Cyber Startup Observatory®

Africa

November 2022

The Global Cyber Innovation Network

Startups & Scaleups

Community

Enterprises

The Global Cyber Innovation Network

Meet the Innovative Companies

Featured in this Edition

CYBER RANGES

AIRBUS CYBERSECURITY

senhasegura

STORMSHIELD

IAI ELTA

STELLAR CYBER

LUPOVIS

Cyber Security Leaders

Dr. Almerindo Graziano
CEO
CYBER RANGES

Olayemi Agbeleye
CISO
Central Securities Clearing System Plc

Tarek El-Sherif
Head of IT Risk
Abu Dhabi Commercial Bank

Stanley Mwangi Chege
CEO
Digital Transformation Experts

Cyber Security Leaders

Gift Medi
CIO
Medical Aid Society of Malawi

Nuno Marques
CIO
Banco BIR

Illyass Ankouz
Global Head of Cyber Security
OCP S.A

Youssef Saidi
CISO / RSSI
Société Générale Maroc

The purpose of the **Cyber Startup Observatory®** is to collaborate to build a safer society and to help solve important problems leveraging cyber security innovation. Find out more and tell us what matters to you by visiting us at:

cyberstartupobservatory.com

This publication has been prepared for general guidance on matters of interest only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice.

No representation or warranty is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Smartrev Analytics Consultants SLU, its members and employees do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

In this document, **"Cyber Startup Observatory", "Cyber Security Observatory"** and **"Smartrev Cybersec"** refer to trademarks belonging to Smartrev Analytics Consultants SLU.

The information provided by the participating startups and companies belongs to them. They remain the sole and exclusive owner of any information provided to Smartev including without limitation, with respect to any intellectual property rights, copyrights and trademarks. Smartrev Analytics Consultants SLU have received explicit written permission to publish all the information included in this report.

Contents

Contents

Contents

Contents

Contents

Overview

It is an honor to present the fourth edition of the **Cyber Startup Observatory Africa.**

Since the first launch of the Observatory dedicated to the region, we have had the pleasure of collaborating with CISOs and other executives from the region and we have seen the high professional and human level.

However, the region faces significant challenges. Digital transformation has reached levels unprecedented in European or North American economies, with some countries such as Kenya, Nigeria or South Africa with online population percentages of 83%, 60% and 56% respectively.

This level of digital penetration has enabled the population to be equipped with advanced digital services but as always, there is a second side of the coin that is somewhat darker.

Online crime has skyrocketed, seriously affecting the more than 500 million internet users in Africa.

In its study "African Cyberthreat Assessment Report, October 2021" Interpol identifies five main risks:

- Online scams: fake emails or text messages claiming to be from a legitimate source are used to trick individuals into revealing personal or financial information;
- Digital extortion: victims are tricked into sharing sexually compromising images which are used for blackmail;
- Business email compromise: criminals hack into email systems to gain information about corporate payment systems, then deceive company employees into transferring money into their bank account;
- Ransomware: cybercriminals block the computer systems of hospitals and public institutions, then demand money to restore functionality;
- Botnets: networks of compromised machines are used as a tool to automate large-scale cyberattacks.

Cybercriminals take advantage of the lack of awareness of the citizens and SMEs to commit these attacks.

From a business point of view, although there is top-notch talent in Africa, it is difficult to find personnel qualified in the latest technologies, difficulting recruitment processes, which are key to maintaining cybersecurity teams that can deal with cybercrime.

Ongoing training is another area for improvement. Although there are great public and private initiatives in various countries in the region, much remains to be done.

From a regulatory standpoint, and although there have been working groups to create common data protection and privacy policies, the region is still very heterogeneous with large initiatives underway.

Some of the most noteworthy are:

- South Africa - The National Cybersecurity Policy Framework (NCPF), December, 2015, calls for greater cooperation, coordination and partnerships to increase the cybersecurity posture in South Africa.
- The Nigerian Cybercrime Act which was signed into law in May 2015.
- Kenya - The Government of Kenya launched the National Cybersecurity Strategy on August 5th, 2022 as a roadmap to address the new challenges and emerging threats in the cyber domain.
- Mauritius - National Cyber Security Action Plan (2014-2019)
- Ghana - Cybersecurity Act, 2020 (Act 1038)
- Morocco - General Guidelines for the Digital Development of Morocco by 2025 and the National Directive on the Security of Information Systems

We believe that great things are being done, but as is always the case, much remains to be done as cyber criminals are opportunistic and constantly on the prowl.

Some examples of recent cyber attacks in the region:

- Transnet (South Africa) became a victim of a ransomware attack forcing the company to declare force majeure at several key container terminals, including Port of Durban, Ngqura, Port Elizabeth and Cape Town.
- City Power (South Africa), a ransomware attack hit Johannesburg electricity supply
- Shoprite Holdings - Large supermarket chain in southern Africa hit with ransomware
- Nigerian betting platform Bet9ja hit by a ransomware attack

Faced with a particularly sensitive situation as described above, the Observatory Africa will monitor the region in detail in the dedicated African launches planned for 2023.

We will also continue to work with our members and partners, in Africa to foster innovation, share valuable industry insight and promote the leadership of African cyber security professionals.

With this goal in mind, we have created the Observatory's global infrastructure, supporting African startups and scaleups in their growth not only in their home market but also in Europe, Middle East, North America, LATAM and APAC.

Finally, I would like to thank all our Observatory members, governmental institutions, partners, industry thought leaders, members of the academic community and entrepreneurs who have supported us since the first launch of the Observatory in 2018 and motivated us to keep growing globally.

This new Observatory Africa is dedicated to them.

References

- Interpol – African Cyberthreat Assessment Report, October 2021 (Link)

Visit the Observatory

Click on the link below to visit the Observatory's Global Infrastructure

In This Edition

The fourth edition of the Cyber Startup Observatory Africa covers key topics for the industry.

We begin by presenting solutions to prepare the financial institutions in Africa to fight cyber crime.

From **CYBER RANGES,** we present the article **"Financial Cyber Drills".**

We continue with one of the global leaders in the Privileged Access Management space, **senhasegura** covering a fascinating topic **"Principle of Least Privilege: Understand the importance of this concept".**

Then, **Stellar Cyber** shares with us a great piece discussing the topic **" What is a Lean Security Team, and how to know if you are part of one",**

The healthcare industry has been severely hit by ransomware attacks and more targeted cyber crime. I share in this edition my own analysis of the state-of-the-art of cyber security in the Healthcare industry with my article **"Healthcare cyber security – state-of -the-art".**

Our winner of the latest Cyber Startup Competition, Lupovis, brings us a interesting article shedding some light on the fascinating topic of Cyber Deception " How Cyber Deception helps CISOs meet their cyber security goals".

The industry is frustrated by a dual reality: on the one hand, a steady increase in cybersecurity budgets that is failing to stop, and on the other hand, a steady increase in the volume and severity of cyber crime.

Our latest article in this observatory covers this issue and is entitled "Cyber Resilience and our proven inability to stop cyber attacks".

In addition to the articles we present our renowned CyberSlides dedicated to Africa. As always, the reader will find the Product and Managed Security Services ver-sions. In future Observatories we will start to include country-specific versions for each country in the region.

As in the rest of the Observatories, we also feature high-quality infographics to raise awareness on important issues for the cyber professional community.

We present in this new edition eight top leaders. We are proud to share in this Observatory Africa our exclusive interviews with:

- Dr. Almerindo Graziano, CEO @ CYBER RANGES
- Stanley Mwangi Chege, CEO @ Digital Transformation Experts Ltd
- Olayemi Agbeleye, CISO @ Central Securities Clearing System Plc
- Tarek EL-Sherif, Head of IT Risk @ Abu Dhabi Commercial Bank
- Gift Medi, Medical Aid Society of Malawi
- Nuno Marques, CIO @ Banco BIR
- Ilyass Ankouz, Global Head of Cyber Security @ OCP S.A
- Youssef Saidi, CIO @ CISO / RSSI @ Société Générale Maroc

I find it difficult to present a group of cyber security leaders with similar levels of credibility, experience and reputation in Africa or globally.

I want to explicitly share our appreciation and respect for the great work they do to keep our governments, enterprises, and in general our society cyber secure.

I hope you enjoy Observatory Europe 4th Edition.

Welcome!

Jose Monteagudo

Editor-in-Chief

Cyber Startup Observatory

The Observatory Team

It just remains for me to thank my team here at the Observatory Program - Co-editor, Maite Ortega, German Duarte, our CTO, our Research Manager and Consulting Director, Alicia Peña for their infinite patience and support in the preparation of this publication.

Jose Monteagudo
Editor-in-Chief
josem@smartrev-cybersec.com

Maite Ortega
Co-Editor
maiteo@smartrev-cybersec.com

German Duarte
CTO
german.duarte@smartrev-cybersec.com

Sections

This methodology is also applied to our web cyberstartupobservatory.com and will be consistent in future editions of the observatory.

Resources

The CyberSlide

Definition and Statistics

The CyberSlide

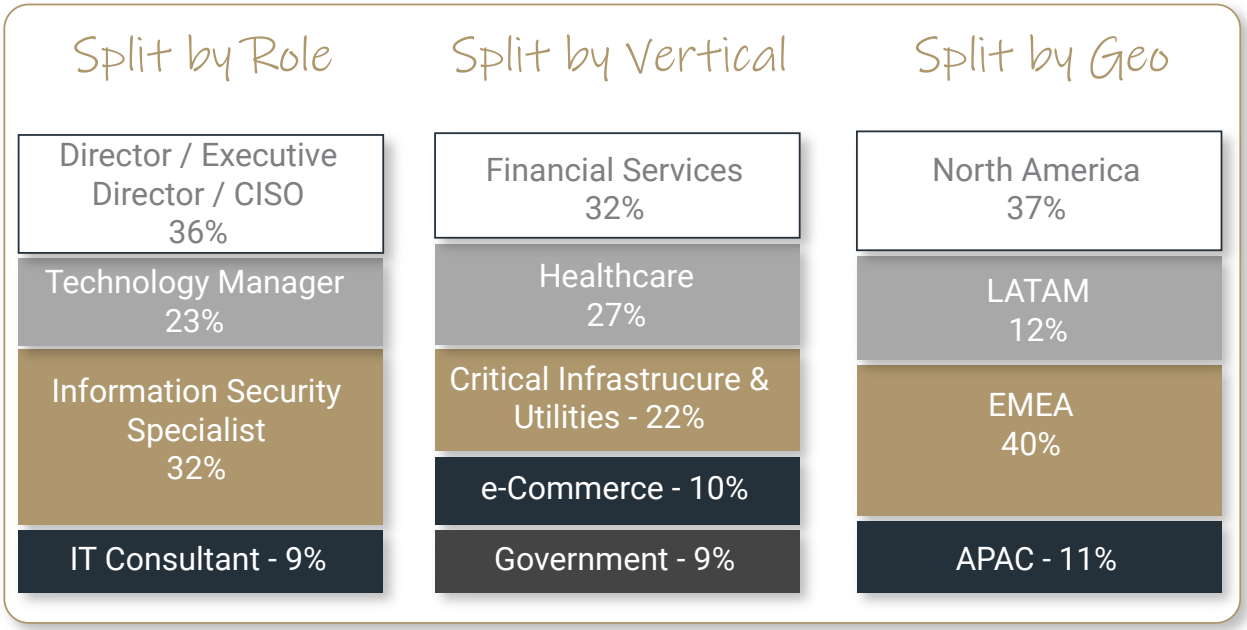
The CyberSlide is dedicated to supporting the extensive cybersecurity market active within the Cyberslide's country, but which has a truly global impact. Cybersecurity has a key part to play not only from the perspective of innovative startups looking to get a foothold in the industry, but also for those established companies who are already major players in the field. The solutions such companies provide form an integral part of our everyday security regime and highlight the fact that we cannot rest on our laurels in the fight against the bad guys.

The CyberSlide is part of a suite of solutions created by the Cyber Startup Observatory - most notably the @CSOFinder search engine - which aims to simplify the cybersecurity technology selection process and offer the best solution for any cyber security issue.

The @CSOFinder showcases the featured companies using a clear categorization that is standardized across the 100+ markets currently on our radar. As a result, a CISO from APAC, Europe, North America, LATAM - anywhere in the world, in fact - can identify companies more easily, helping them to navigate this ocean of complexity in which 1000s of new companies spring up every year.

Given the impossibility of including every single one of these companies on the CyberSlide, it's important to mention that all participating companies have been contacted individually in order to ensure the correct categorization process has been negotiated and agreed upon.

Furthermore, we are one hundred percent committed to keeping the CyberSlides updated, to promote them regularly, to educate the community and to provide the most effective support possible to these industry innovators and their mission.



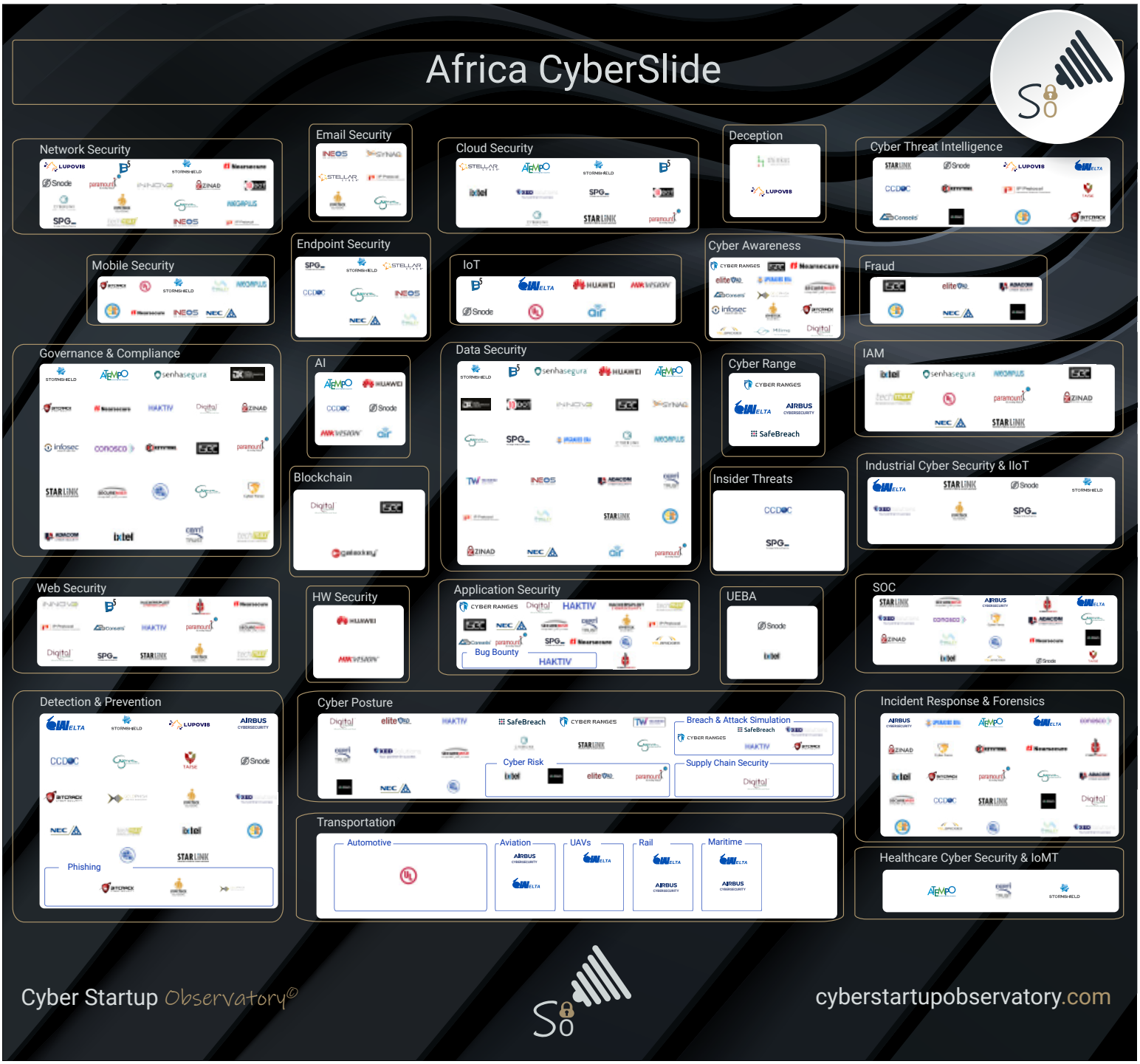
Resources

The Africa CyberSlide

Product Companies

A world-class

cyber security ecosystem



125+ Companies featured

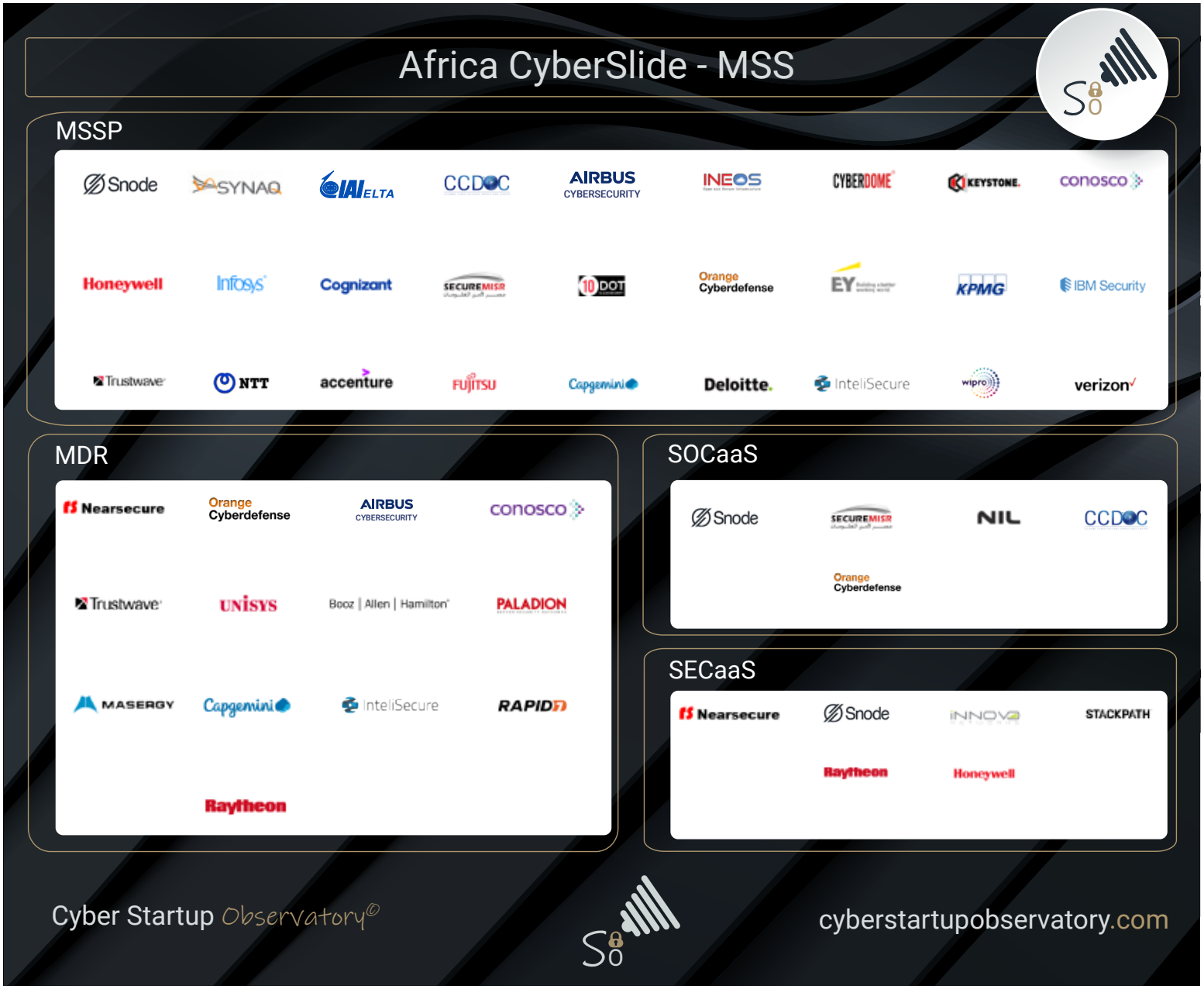
Resources

The Africa CyberSlide

Managed Security Services (MSS)

A world-class

cyber security ecosystem



75+ Companies featured

MSSP, MDR, SOCaaS & SECaaS Providers

@CSOfinder

Our Global Search Engine for Cyber Security Companies

How It Works

Visit... @CSOFinder

Leadership

Dr. Almerindo Graziano

CEO @ CYBER RANGES

Almerindo Graziano

What is TOAR and How Does TOAR Help Build Cyber Capability?

Please click on the link below to watch the interview...

Insight

CYBER RANGES

Financial Cyber Drills

CYBER RANGES

Financial Cyber Drills

Author: Dr. Al Graziano, CEO at Silensec | CYBER RANGES

At a glance

- 12 minute read
- Introduction
- Assessing cyber resilience
- A better approach: Cross Cyber Drills
- The role of Next-Generation Cyber Ranges
- Conclusions

CYBER RANGES

Introduction

Cybercrime statistics concur that financial institutions have become the number one target of cyberattacks. Besides the immediate financial rewards, financial institutions are also custodians of a wealth of information about their customers, which once stolen can be re-sold and/or used to commit other cybercrimes, financially motivated or not.

Never like today must financial institutions be able to minimize the impact of cyberattacks, whether it is through the use of cyber threat intelligence, the development of advance detection and response capabilities, or the development of a strong security posture.

Regardless of the chosen solutions, the human talent component continues to play a pivotal role that many financial institutions struggle to address also because of the still increasing shortage of competent security professionals.

Attacks and security breaches have become the third unequivocal constant in every CISO's life after death and taxes. CISOs have increasingly turned their attention to improving the cyber resilience of their organizations in order to minimize the impact and disruption of cyberattacks on their business. But how can CISOs assess their organizations' cyber resilience?

In this paper, I analyze the different methods that financial institutions have at their disposal for assessing their cyber resilience, emphasizing the need for regular cyber exercises. I also elaborate on one specific type of cyber exercises, which we at Silensec have developed and call Cross Cyber Drills, which are proving – also with financial institutions – to be very effective in assessing cyber resilience beyond the resilience of systems (engineering approach) and encompassing people and processes.

Finally, I put forward a number of guidelines to help financial institutions plan and execute effective cyber exercises.

Cyber Resilience

In recent years the term Cyber Resilience (or Cyber Resiliency) has gained great interest from CISOs from around the world. Such factors as remote working, digital transformation, ecosystem, supply chain risk management, cyber-physical convergence, cloud migration and shortage of competent workforce, increase the complexity of managing the security risk of the organization, especially when talking about large multinational financial institutions.

While CISOs do not shy away from the security challenge, they have begun to look for new ways to validate how well their organizations will withstand an attack on their cyber infrastructures before those attacks occur. The term resilience has already been used for many years in different contexts[1], from National Security to Critical Infrastructures and more recently with reference to cyber security. NIST provides the following definition of Cyber Resilience (SP 800-160 Vol. 2):

"The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."

On the other hand, Gartner defines organizational resilience as:

"The ability of an organization to resist, absorb, recover and adapt to business disruption in an ever-changing and increasingly complex environment to enable it to deliver its objectives, and rebound and prosper" (a slightly modified version of the ISO 22136:2017 definition).

Regardless of the actual definitions, everyone can agree that cyber resilience addresses organizations as a whole and it is not just a matter of security posture and security controls being in place.

Also, the underlying message within the term cyber resilience is about the growing reliance of organizations and society as a whole on cyber resources, a reliance that is only going to grow deeper and wider with the increasing adoption of cyber-physical systems. At a high-level, a cyber resilient organization must be able to:

- **Anticipate Attacks** – This ability is often related to the development of threat intelligence capabilities and the associated capability of the same organization to create plans and deploy security controls to minimize the risks of impending threats (e.g., by addressing the targeted vulnerabilities).

- **Withstand Attacks** – Despite the best effort and good security posture, attacks will still manage to get through the organization's defences and sometimes they stay resident as in the case of APTs. The ability of an organization to withstand an attack is linked to its monitoring and detection capabilities and to the effectiveness of the overall incident response process.

Obviously, an organization must also continuously improve and learn lessons from experience and from reflecting on it. As Sir Winston Churchill quoted:

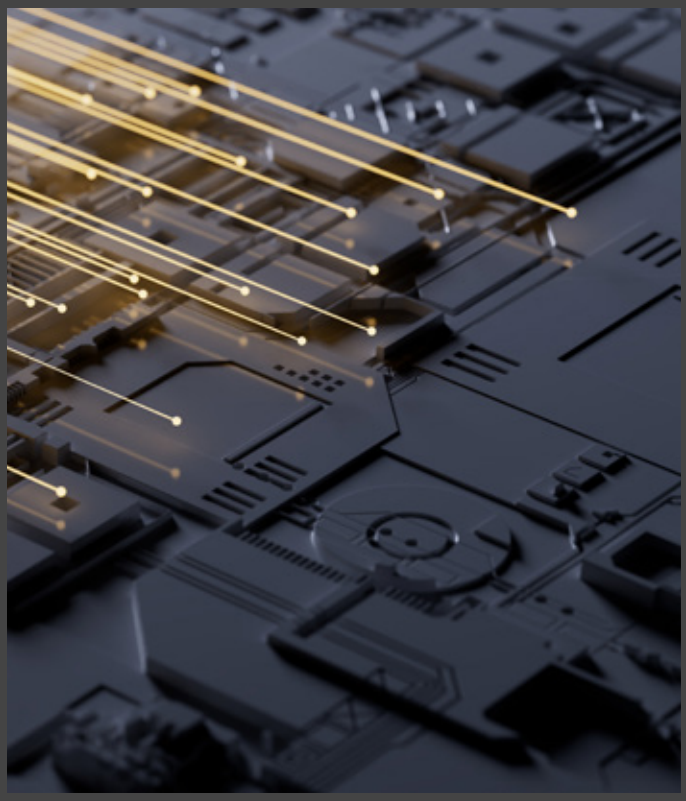
"All men make mistakes, but only wise men learn from their mistakes."

However, more recently, Warren E Buffett, an American business magnate, philanthropist, and one of the most successful investors in the world (CEO and Chairman of the Omaha-based multinational conglomerate company Berkshire Hathaway), better articulated it as follows:

"It's good to learn from your mistakes. It's better to learn from other people's mistakes."

In the financial sector, a pivotal publication recognizing the importance of cyber resilience is the CPMI-IOSCO guidance on cyber resilience for Financial Market Infrastructures (FMIs), published in June 2016[2] . In this document, the authors call for FMI to establish a comprehensive cyber resilience framework that includes a testing programme to validate its effectiveness.

Specifically, understanding (through testing) the overall effectiveness of the cyber resilience framework in the FMI and its environment is essential in determining the residual cyber risk to the FMI's operations, assets, and ecosystem. Such testing must simulate tactics, techniques and procedures (TTPs) of current and relevant cyberattackers as gathered from threat intelligence.



Assessing Cyber Resilience

While many CISOs focus on improving the cyber resilience of their organizations, the testing and assessment of such cyber resilience remains an integral part of the overall digital risk management strategy.

International best-practice security standards, such as ISO 27001, require organizations to plan and execute regular audits every year. Similarly, organizations should develop annual programmes to test their cyber resilience regularly and to use the outcomes of those assessment for improving their cyber resilience.

Most importantly, the assessment of cyber resilience should include internal and external stakeholders playing different roles within the organizations, including senior management, operational personnel, regulators, ecosystem partners, and financial authorities.

Today, CISOs wishing to assess the cyber resilience of their organizations use, or are looking to apply, one of the following methods (please bear in mind that not every method is appropriate for assessing cyber resilience and some are more appropriate than others):

Breach and Attack Simulation (BAS)

Breach & Attack Simulation (BAS) tools and solutions have become widely popular in the industry in recent years. Attack simulation refers to the ability to simulate a threat actor's tactics, techniques and procedures (TTPs).

The business focus of most attack simulation tools and platforms is to provide a (semi) automated means of obtaining the attacker's view or perspective of the target organization. While traditional vulnerability scanning technology focuses on the identification of systems, networks and application vulnerabilities, BAS solutions go the extra mile by allowing to simulate the different phases of the security kill-chain, while at the same time providing recommendations on how to secure the organization.

Sample features of BAS solutions include:

- Agent-based install on the production environments
- Provide an automated attacker's view of an organization's environment
- Provide recommendations to mitigate gaps
- Map assessment findings to MITRE ATT&CK.

BAS solutions are fundamentally audit solutions to understand the organization's exposure to cyberattacks across the entire cyberattack surface, helping the organization to prioritize risk mitigation strategies and improve its security posture. In that respect, BAS solutions help by increasing the ability to anticipate and withstands attacks.

However, when it comes to assessing an organization's cyber resilience, BAS solutions have the following shortfalls:

- **BAS solutions only simulate attacks** – BAS solutions are deployed on production systems. As such they limit themselves to only simulating the attacks.

  For instance, when simulating a ransomware attack, the files that the BAS agent tries to write on disk in the production systems are harmless files, which simply contain hashes of known malicious entities.

  This way, a SIEM might flag such files if they are even allowed to be written, while endpoint security controls deployed on the machines might quarantine the actual files.

  From a cyber resilience perspective, BAS will help organizations identify configuration gaps and help improve the security posture of the organization but it will not address the human factor side of the resilience, leaving the CISO wondering "what if…" with no strong assurance or confidence.

- **BAS solutions only address the system side of the organizational resilience** – Cyber resilience includes the ability of the organization to detect, respond and mitigate the impact of attacks affecting the cyber resources of the organization. In other words, a cyber resilient organization will have mature and effective processes and competent staff in place in order to be able to detect attacks that have slipped through the hardened net of security controls - it will then be able to respond to such attacks in order to minimize their impact on the business.

BAS solutions are here to stay and to become a permanent solution for CISOs of all organizations. However, they only address the system aspects of the cyber resilience, leaving aside the human components of talent and security processes.

Red Team Simulation

A Red Team Simulation is an engagement where the tactics, techniques and procedures (TTPS) of real-life attackers are simulated on real production environments in order to reveal the strengths and weaknesses of the organization being tested, enabling it to reach a higher level of cyber maturity.

Red Team Simulations are tailored to an individual organization to simulate an attack on the critical functions of that organization and its underlying systems (i.e., its people, processes and technologies).

Several Red Team Testing frameworks have been developed around the world. Notable examples include:

- The European Union Threat Intelligence-Based Ethical Red Teaming framework (TIBER-EU)[3].
- The CBEST framework in the United Kingdom, developed by the Bank of England[4]
- The Intelligence-led Cyber Attack Simulation Testing (iCAST) by the Hong Kong Monetary Authority ("HKMA")
- The Financial Entities Ethical Red-Teaming (FEER)[5] by the Saudi Arabian Monetary Authority

- The Adversarial Attack Simulation Exercises (AASE)[6] developed by the Associations of Banks in Singapore.

The **figure below** illustrates a typical process for the execution of Red Team Testing, from procurement, scoping up to execution, according to TIBER-EU.

Other frameworks provide a similar structure. Overall, the following considerations can be made with regard to Red Team Testing and cyber resilience assessment:

- Costly Engagement – A red Team Testing exercise is a multi-stakeholder engagement carried out on production environments. As such it requires considerable planning and resources.

- Long process not suitable for many iterations – Due to its nature, a Red Team Testing engagement is usually a once-a-year activity at best. In reality, many financial institutions do not even carry them out annually.

- Organizations have to wait for the next iteration to assess any applied improvements.

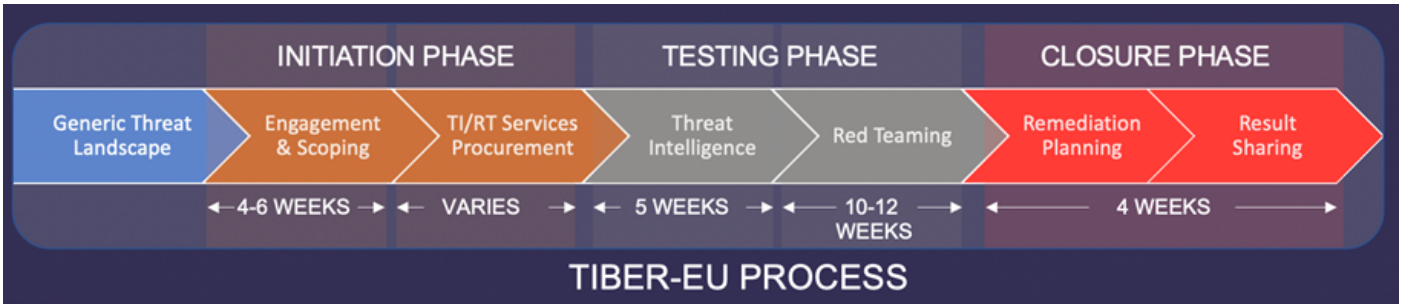
- It is delivered on production systems – Because of the live production systems being targeted, Red Team Testing engagements have to somewhat limit the realism of the attack simulation in order to limit the risk of unforeseen negative impact on the business.

Cyber drills

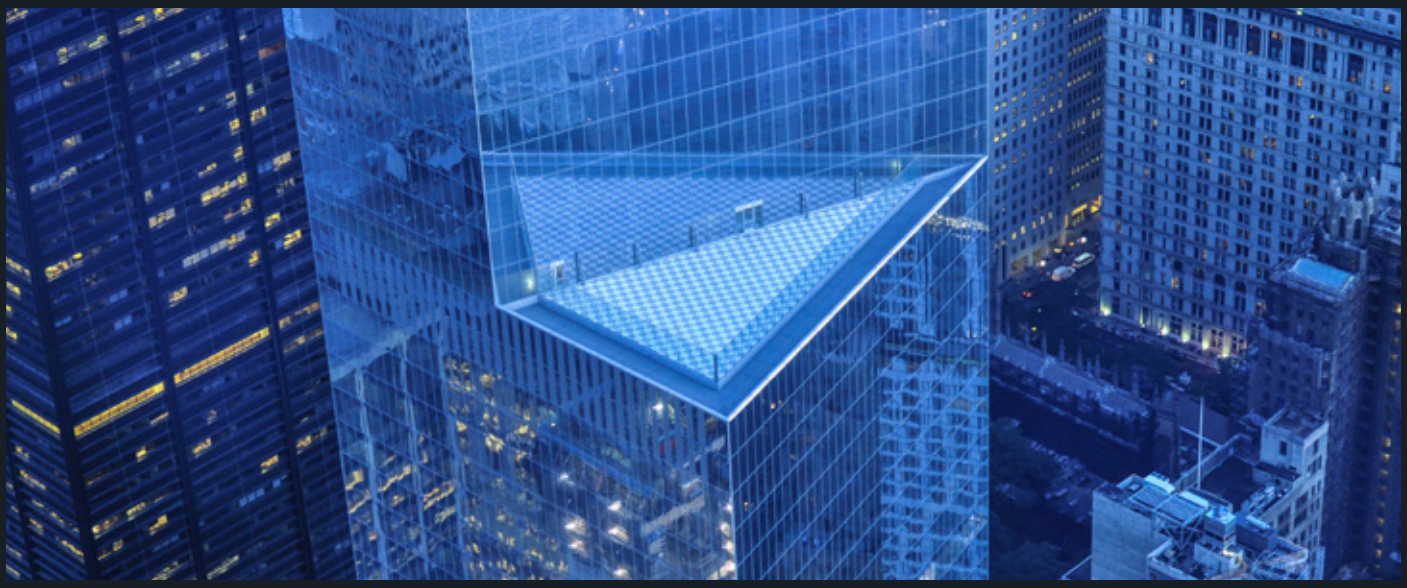
A cyber drill is a planned event during which an organization simulates cyberattacks, information security incidents or other types of disruption to test the organization's cyber capabilities, from being able to detect a security incident to the ability to respond to it appropriately and minimize the impact on the organization's business.

Such simulations are captured into what is normally called a scenario, which includes a storyline, a simulated environment, some challenges and much more, depending on the scenario. Overall, cyber drill scenarios fall under one of the following two types:

Table-top (TTX) – These are discussion-based scenarios, where participants usually role play to simulate their reactions in real-life situations.



The execution of Red Team Testing



During TTX exercises, a facilitator guides participants through a series of "injections", i.e., fictitious events such as, for instance, receiving a threatening email or the news of a critical vulnerability or a declaration by a hacktivist group. TTX are best suited for testing security processes.

- **Operational (Hands-on)** – In these exercises participants are required to interact with simulated systems and test their ability to carry out typical cybersecurity tasks such as identifying and responding to a security incident, performing malware analysis, carry out some computer forensics etc.

Table-top exercises - Table-top exercises are great - they will always play an important role in the CISO tool chest but they have the following shortcomings:

- TTXs are not inclusive – In the majority of cases, TTXs only involve the management side of the organization and not its technical side. When they do involve operational staff, TTX are simply simulating threats to elicit responses from the audience and to validate the decision-making processes. For instance, when simulating ransomware the TTX may require the SOC team to choose from a list of available options or to suggest alternative actions. In no case will anyone be required to perform an activity of malware analysis or log analysis or any other practical activity.

- Processes and not Operations – TTX are a great way of testing the knowledge and understanding of processes, but they fall short in the validation of the process execution since everything is simulated with little to no operational engagement.

As an example, a TTX may help validate if an organization's incident response process is sound and if it has been developed according to best practice. It may even help validate to what extend staff follow the process.

Operational Exercises - Operational exercises have been run successfully for many years across many different business sectors. However, Operational Exercises come with the following shortfalls:

- Operational Exercises are not Inclusive – Just like TTXs were not inclusive of the operational staff, Operational Exercises are not inclusive of the management roles. Responding to security incidents requires sound technical competencies but it also impacts on the business and thus it requires communication, escalation, and coordination with other entities, involving Management up to the Board to take important decisions which can affect the execution the of the incident response process.

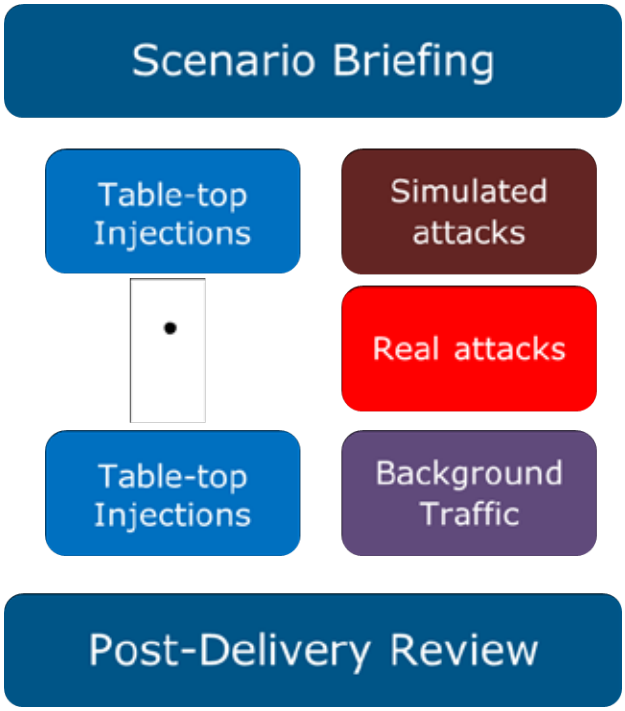
- Lack of Business Context – Operation exercises tend to focus on the technical side to assess the abilities of the operational staff in dealing with specific phases of the incident management process or across the entire lifecycle of a security incident. Yet the focus is on "can you do it" and "can you fix it" type of questions rather than "do you understand the impact this has on the overall organization" and "are you able to effectively collaborate and communicate with non-technical staff" to minimize the impact of the security incident to the business.

A Better Approach: Cross Cyber Drills (C2 Drills)

While traditional cyber drills fail to capture the communication and collaboration aspects within an organization and between different organizations, C2 Drill scenarios are designed to include both table-top and hands-on exercises simultaneously, allowing the participants with different roles and responsibilities to interact with one another, simulating the entire business and its operational relations within the organization and its ecosystem, as and if involved.

C2 Drill Approach

The following figure illustrates the typical delivery plan for each scenario in a C2 Drill:



Scenario Delivery Format

Each scenario begins with a briefing session to introduce it, its objectives and to explain the rules of engagement. Information about the simulation environment and how to access it is also provided in order to ensure all participants are ready to begin the cyberdrill.

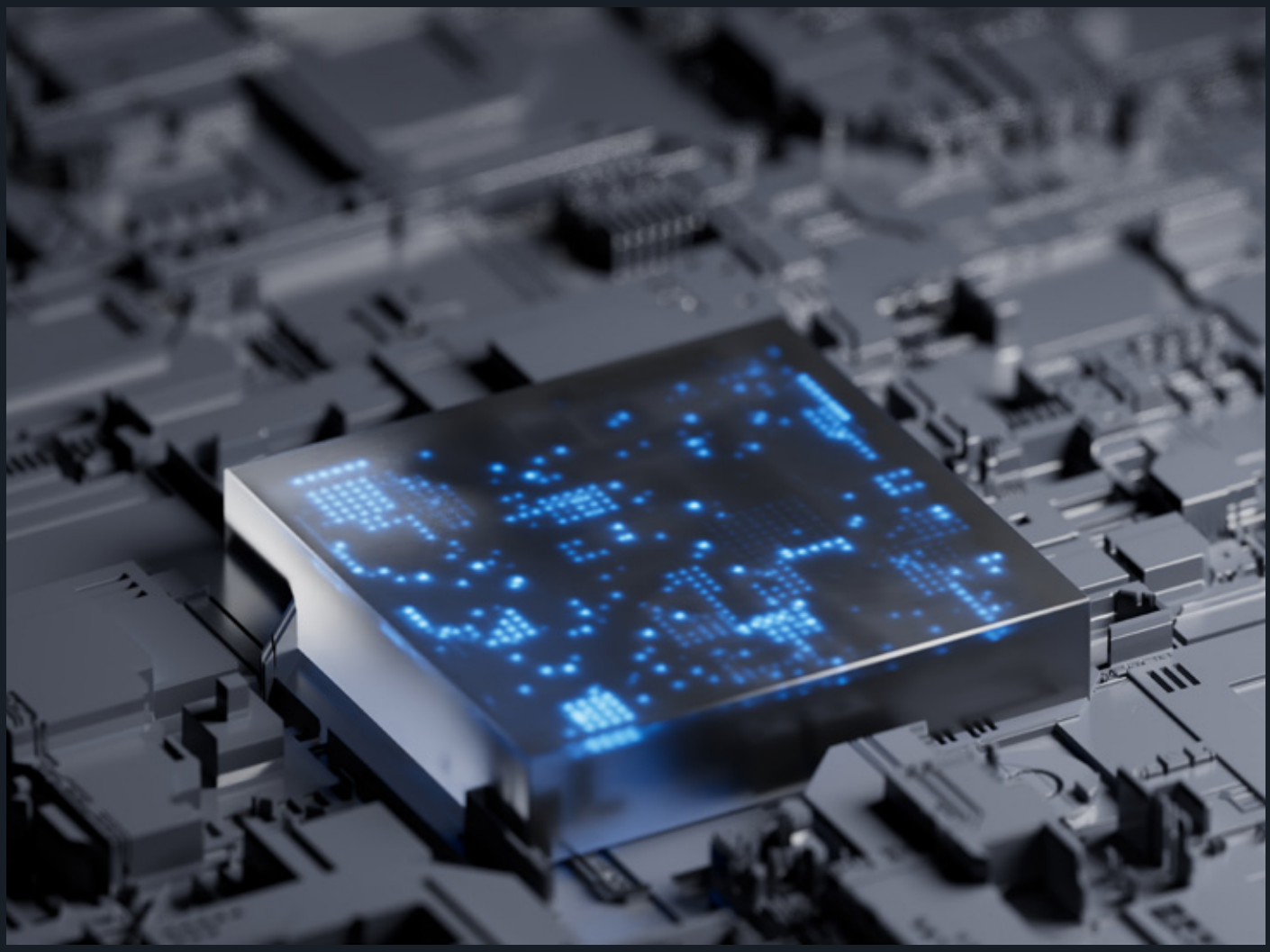
Participants are divided into two groups. Group one includes all the participants involved in the technical hands-on exercises. Group 2 includes the management involved in the table-top simulations.

Each scenario is designed to require hands-on responses and activities with, at the same time, management reflections, discussions and decision points. Furthermore, each scenario requires the two different groups to interact with one another at different stages, simulating the typical interactions and communications of a real-life scenario.

Planning a Cross Cyber Drill

Whether it is a TTX, an Operational Exercise or a Cross Cyber Drill, the truth is that cyber exercises should be taken on a regular basis and more than once a year. Unfortunately, the main reason why this does not happen is costs!

The high costs are explained by the customization of the exercise for the target organization. Let's take ransomware as an example. A generic TTX on ransomware will have little to no value to an organization of a certain maturity level. A more mature organization will most likely require the TTX to be customized to take into account the organization's security processes, incident response playbooks, organizational structures and more. All this drives the costs up. Then again, once run, the TTX loses its value. Similar considerations can be made for other types of exercises.



Other reasons affecting the regular execution of cyber exercises include:

- **Lack of Established Assessment Frameworks and Methodologies** – Unlike Red Team Testing Frameworks, cyber exercise frameworks are less established. Cyber exercises in the commercial sector are less mature in that respect. Organizing a cyber exercise, especially involving many stakeholders is not an easy task and the delivery of the exercises often leaves the organizations wanting.

- **Maturity of tools and technology** – Automation means lower costs, greater speed of execution and increased realism. Most tools and technologies used in cyber exercises today lack automation and are heavily dependent on security professionals and facilitators to run the show on stage and at the back. Setting up and maintaining simulation environments is still expensive.

- **Maturity of assessment frameworks** – Everyone wants the assessments to identify the gaps and shortfalls that need addressing. However, there is no click-and-run type of cyber exercises, and there is no click-and-run type of assessments that will just observe the actions and responses of the people participating in the cyber exercise and spit out the organization's scorecard. At least not just yet.

The Role of a Next-Generation Cyber Range in Cyber Exercises

Much of the costs associated with the regular assessment of cyber resilience are related to the inability to automate the tasks and activities that can and should be automated, such as for instance:

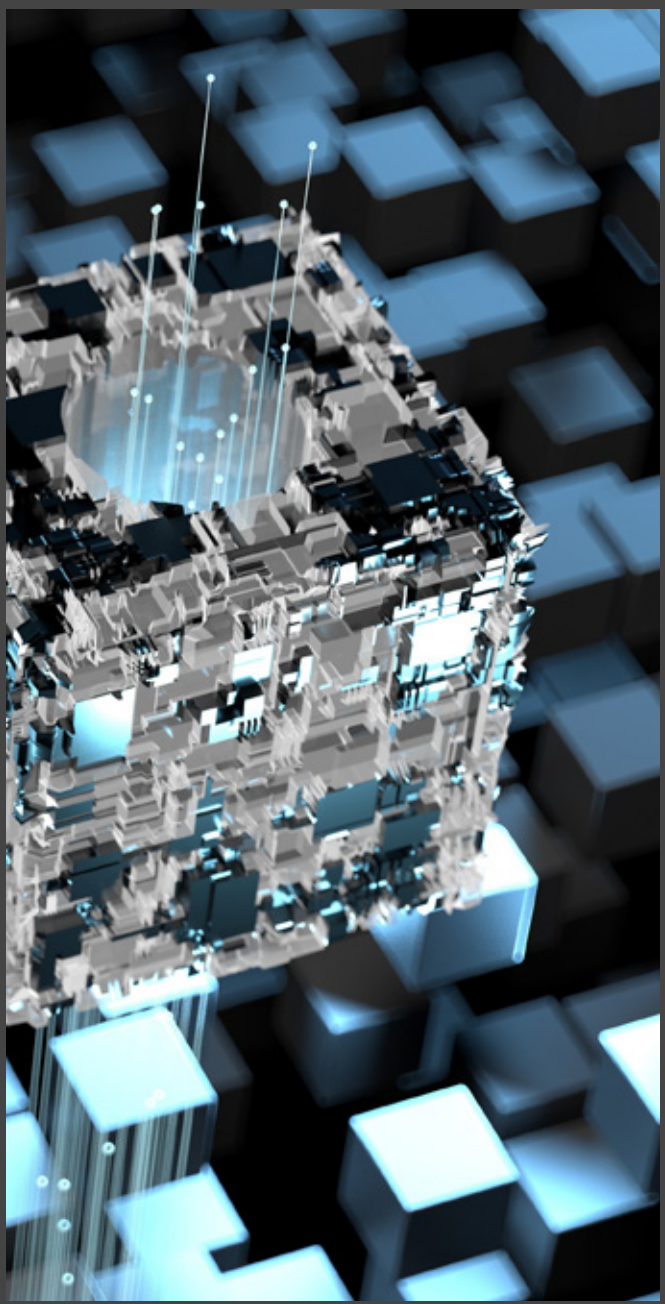
- Management Workflow of Simulation Environments
- Attack Simulation/Emulation
- Management of interactions amongst multiple stakeholders (e.g., management and technical staff).

What is a Next-Generation Cyber Range?

When talking about cyber ranges and trying to understand the difference between traditional, old-generation cyber ranges and next-generation cyber ranges, the key point is about the ability of a cyber range to address both the aspects of scaling the exercise and the experiential learning methods applied in a manner that is cost-effective for the organization.

Next-generation cyber ranges address both scale and method, simultaneously. Next-generation cyber ranges come with the following characteristics:

- High orchestration to scale both skills development and application of such skills in realistic simulation environments
- Integrated functionalities to support different use cases
- User Activity and Attack Simulation/ Emulation
- Ability to easily add experiential learning content for both the development of skills and the application of such skills in realistic deep-dive simulation environments
- Ability to be deployed on cloud or on premises with comparable costs
- Click-and-play ease of use even for complex high-fidelity simulation environments
- Integrated learning management system to manage users' upskilling progression and experience.



The figure below illustrates the architectural components of a next-generation cyber range. Compared to traditional ones, next-generation cyber ranges integrate multiple functional components, on top of the traditional ICT/OT simulation, to provide the end user with automated functionalities, which heavily reduce the resource requirements to execute cyber drills and to simulate and denotate attacks, providing users with a practical and effective one-click experience.

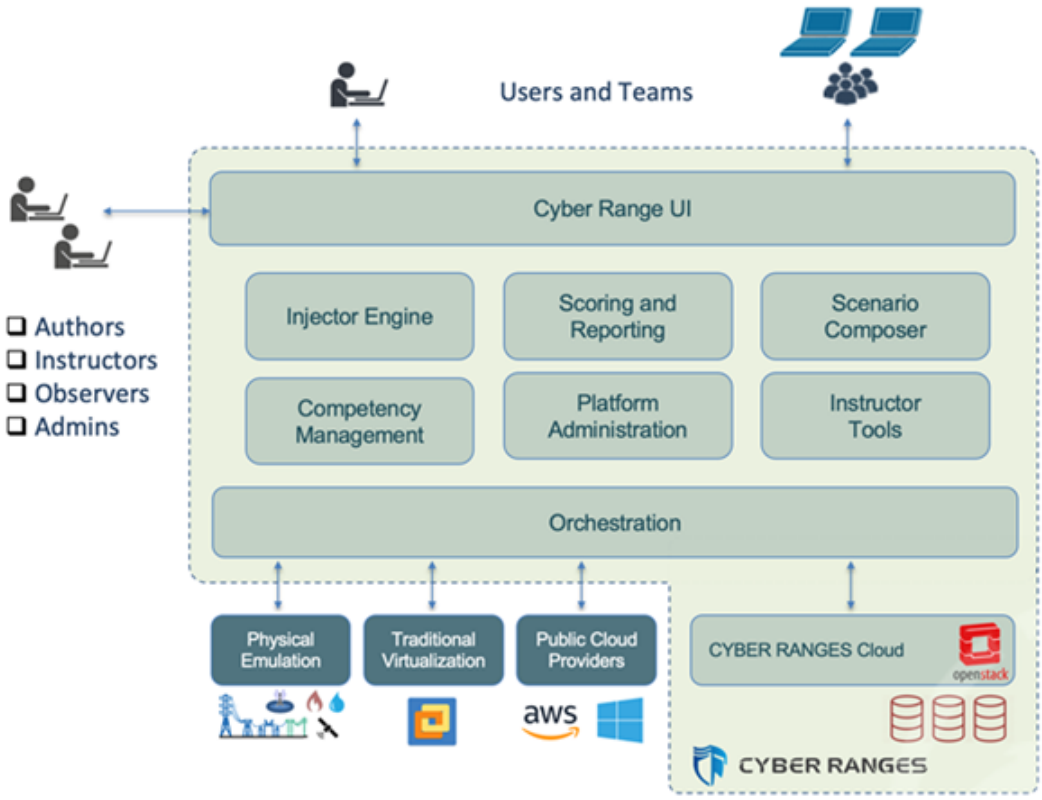
Using a Next-Generation Cyber Range for Improving Cyber Drill Automation

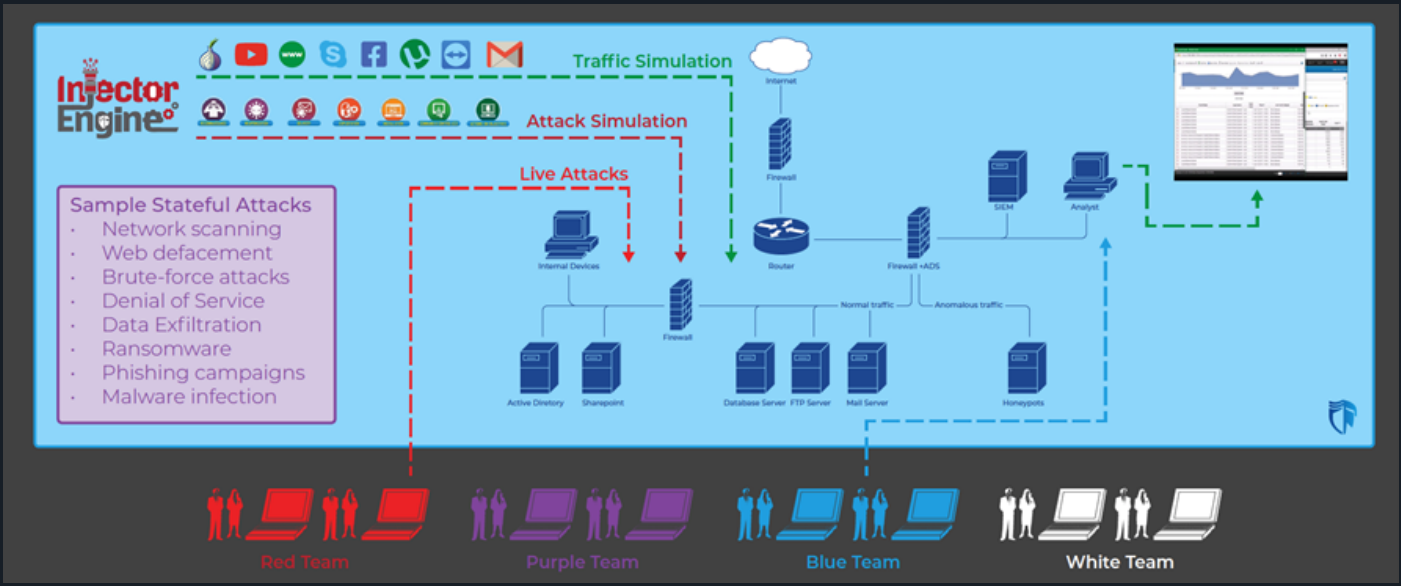
Since every organization is different, assessing cyber resilience will never be a fully automated process. However, there is light at the end of the tunnel that is bound to change this limitation for the entire financial sector and other industries alike.

Many organizations are beginning to look at next-generation cyber ranges to heavily cut down on the costs of execution of cyber exercises and to integrate both TTX and Operational Exercises into a single platform for a comprehensive end-to-end assessment of cyber resilience.

Assessing cyber resilience with a next-generation cyber range includes the following steps:

1. **Development of Replica Environments** – The replica environment must be representative of the organization's infrastructure, including the same security controls and infrastructure assets in order to facilitate a confident appreciation of the organization's response to the attack simulation. The set-up of the replica environment should also be based on the analysis of the organization's security processes, incident response playbooks and reflect the security maturity of the organization.





Cross Cyber Drill on CYBER RANGES – a simplified setting

2. **Development of attack simulations based on threat intelligence** – Once the replica environment has been set up, attack simulations can be developed on the basis of current and relevant threat intelligence.

2. **Click-and-play execution of threat simulations** – In this phase, the environment is ready to be used for fast execution and against limited resources to test and evaluate the cyber resilience of the organization.

2. **Semi-Automatic capture of actions and responses** – Stakeholders' interaction is captured and observations documented by the facilitators of the cyber exercise.

2. **Value-Added Reporting on Cyber Resilience** – A report is produced capturing the level of cyber resilience, mapping the organizational response to specific cyberattacks.

Naturally, the above process relies heavily on two aspects:

- The use a of next-generation cyber range

- The use and integration of a cyber resilience assessment framework, which the cyber range will help automate to the extent possible, leaving the "humans" in charge of the tasks of planning and executing the exercise, and analyzing its results in terms of cyber resilience assessment.

The current maturity of some next-generation cyber ranges, such as CYBER RANGES by Silensec, has already reached a level that allows financial institutions to comfortably deploy them for the running of Cross Cyber Drills.

The cyber resilience assessment frameworks, in relation to the use of cyber ranges, are still maturing but are expected to reach maturity in the near future, as more and more organizations begin to use a next-generation cyber range for comprehensive exercises and to contribute to the development of best practice.

Conclusions

Financial institutions should begin to look at alternative methods of assessing cyber resilience, which require lower costs and allow for more frequent execution and comprehensive deep-dive test activities.

Specifically, organizations should consider the adoption of Cross Cyber Drills, powered by a next-generation cyber range to improve the automation of exercises, reduce their costs and integrate the regular assessment of their cyber resilience into the organization's digital risk management strategy.

References

1MITRE Cyber Resiliency FAQ https://www.mitre.org/sites/default/files/PR_17-1434.pdf

2(2016) Guidance on cyber resilience for financial market infrastructures, https://www.bis.org/cpmi/publ/d146.pdf

3European Central Bank (2018). TIBER-EU FRAMEWORK https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

4Bank of England (2021). CBEST Threat Intelligence-Led Assessments. https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf

5Saudi Arabian Monetary Authority (2019). Financial Entities Ethical Red-Teaming. https://www.sama.gov.sa/ar-sa/Laws/BankingRules/Financial_Entities_Ethical_Red_Teaming_Framework-AR.pdf

6The Associations of Banks in Singapore (ABS)(2018). Red Team: Adversarial Attack Simulation Exercises. https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1-06766a69f299c69658b7dff00006ed795.pdf

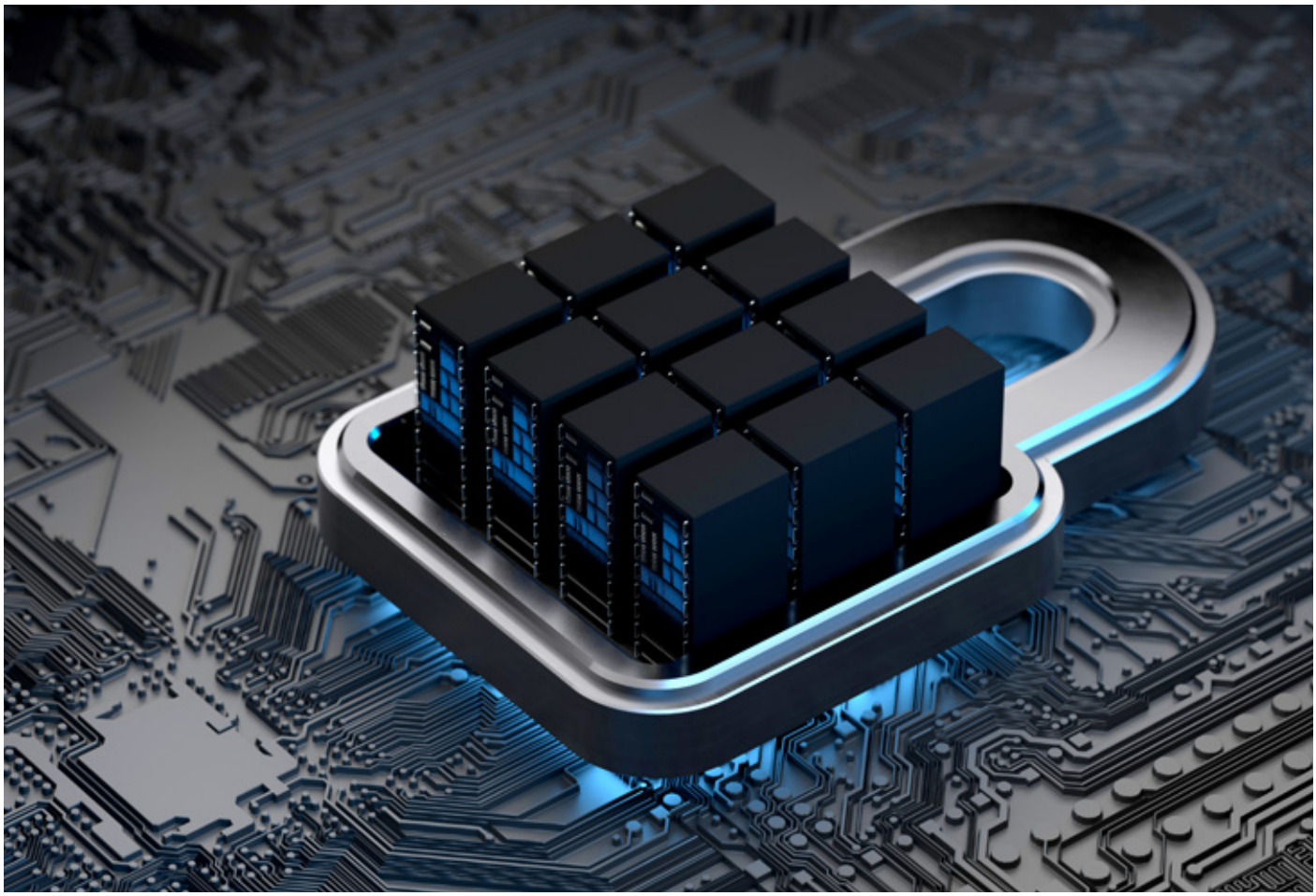
About the Author

Dr. Al Graziano, CEO, Silensec | CYBER RANGES

Dr. Al Graziano founded Silensec in Sheffield (UK) in 2006, after a successful career as the university course designer and then director of the first UK MSc. Information Security programme. An ISO 27001 certified cyber security solution provider, Silensec has been delivering hands-on cyber drills to national CERT/CSIRT since 2014 in collaboration with the UN's International Telecommunication Union. Silensec has developed the latest ITU Cyber Drill Framework. CYBER RANGES by Silensec is the only next-gen cyber range platform with its full feature set available on premises, on private and public cloud, and portable.

Silensec is a member of the European Cyber Security Organization (ECSO) and co-chairs the ECSO Working Group WG 5 on cyber ranges, cyber exercises and training, and also at sub-WG 5.1 (cyber ranges) and sub-WG 5.2 (education and training), furthering the best practice in the area of cyber ranges and cyber exercises.

Silensec is also a Premium Partner of the Global Cyber Alliance (GCA), based in New York, London and Brussels and focused on cooperation between industries and governments in tackling cybercrime.



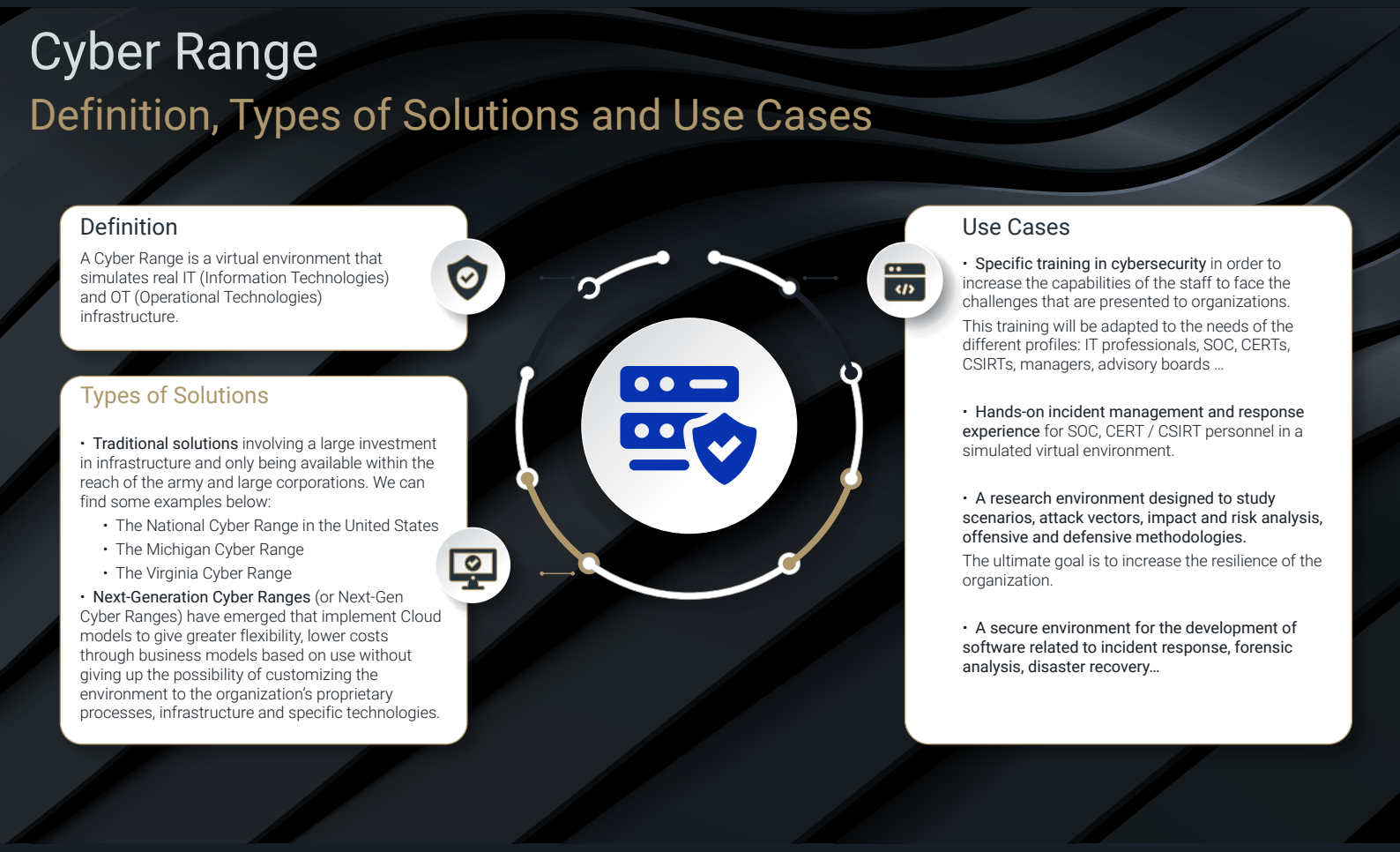
Resources

Infographic

Cyber Range - Definition, types of solutions and use cases

Cyber Range

Definition, types of solutions and use cases



Available for download in Press Quality

Infographics - Cyber Range

Cyber Startup Observatory - *Community*

Stanley Mwangi Ghege

CEO @ Digital Transformation Experts LTD, Kenya

Stanley Mwangi Chege

CEO @ Digital Transformation Experts LTD, Kenya

Please click on the link below to watch the interview...

SENHASEGURA

Principle of Least Privilege: Understand the importance of this concept

senhasegura

Principle of Least Privilege: Understand the importance of this concept

Author: Senhasegura

At a glance

- 5 minute read
- What is the Principle of Least Privilege (POLP)?
- Why is the POLP important?
- 10 benefits of the Least Access Principle
- How to implement the POLP
- Examples

Granting administrator access to a user who does not even have time to explain why they need this permission is not an efficient way to solve a company's problems but rather to harm its security.

This is because sensitive data can fall into the wrong hands through a cyber invasion, in addition to the organization's own collaborator posing a threat due to the possibility of human, accidental, or purposeful errors.

In this context, it is recommended to apply the **Principle of Least Privilege**, which grants these users only the necessary permissions to perform their tasks.

In this article, we explain in detail this concept and its importance, among other information on the subject.

What is the Principle of Least Privilege?

Also known as Least Access Principle, the Principle of Least Privilege (POLP) refers to a concept of cybersecurity according to which users should receive only the necessary permissions to read, write, and execute files indispensable to their operations.

In practice, the Principle of Least Privilege integrates the security policy of companies and restricts access to applications, systems, and processes only to privileged users.

Depending on the system, it is possible to base these privileges on the roles of professionals within organizations.

Why is the Principle of Least Privilege Important?

First, the Principle of Least Privilege is critical to reducing the attack surface, preventing the action of malicious users. This is extremely important, since privileged credentials are among the main targets of attackers.

That is, by limiting superuser and administrator access through the **Least Access Principle,** one can protect a company from intrusions. Moreover, it helps prevent the spread of malicious software, such as malware.

However, it is essential to be aware of the need to apply the **Principle of Least Privilege** to endpoints. This helps prevent hackers from using elevated privileges to increase their access and move laterally across the IT framework.

The need to keep companies in compliance with strict auditing standards also explains why the **Principle of Least Privilege** is important.

10 Benefits of the Least Access Principle

The main benefits of the Least Privilege are:

- Elevation of privileges when necessary
- Restriction of access to applications
- Restriction of access to system settings
- Control of the data used
- Smallest attack surface
- Reduction of human failures
- Malware containment
- Enhanced data security
- Protection against common attacks
- Compliance with audit criteria

Here are more details on these benefits:

Elevation of Privileges When Necessary

It is necessary to apply the Least Access Principle (POLP) whenever one needs to elevate the privileges of an employee to a particular application for a specific time to operate.

Restriction of Access to Applications

Another purpose of the Principle of Least Privilege is to prevent an administrator from changing the settings of equipment by installing applications and exposing the organization's network to cyber threats

Restriction of Access to System Settings

The Principle of Least Privilege also has the function of reducing administrative privileges by restricting access to system settings.

Thus, a user may have administrative privileges without being able, for example, to change firewall settings, since the control of the environment is intended for the administrator.

Control of the Data Used

Through the Principle of Least Privilege, one can record and store detailed information about each access granted and obtain greater control of the company's data.

Smallest Attack Surface

If a malicious agent breaks into a user account with limited permissions, their attack will compromise only the resources accessed by that user. In contrast, if the hacked account is an administrator, the hack will impact the entire network.

This means that, in order to reduce the attack surface used by hackers to harm a business, it is recommended to keep the minimum number of administrator accounts.

Reduction of Human Failures

In addition to hacking, applying the Principle of Least Privilege in your organization helps prevent problems caused by human errors. After all, users with access to resources that go beyond what is necessary to perform their tasks can, unintentionally or even purposely, delete or reconfigure something.

Malware Containment

The Principle of Least Privilege helps prevent your network from getting infected by malware. This is because an administrator with many accesses can spread malware to multiple systems, while it is possible to count its dissemination on networks where Least Privilege applies.

However, it is not enough to restrict users' access, as the same must be done in relation to applications in order to prevent this type of attack on your network.

Enhanced Data Security

You may remember when Edward Snowden leaked millions of classified NSA (National Security Agency) files to the media due to his privileged access. The incident has caused many problems, which could be avoided if his permissions were limited to the scope of his work.

Applying the Least Access Principle is an efficient way to limit the number of users with access to sensitive data, reducing the possibility of internal leaks and strengthening digital security.

Moreover, in the event of a violation, the restrictions imposed by the Principle of Least Privilege allow for easier tracking of the cause.

Protection Against Common Attacks

Applications with high privileges are often targeted by hackers, who insert malicious instructions into SQL statements to control critical systems. However, this type of attack can be avoided through the Principle of Least Privilege (POLP), which impacts the possibility of elevating permissions.

Compliance with Audit Criteria

Applying the Least Access Principle allows organizations to operate in accordance with the most stringent audit requirements, making it possible to avoid threats and reduce the downtime and losses generated by a potential attack.

How to Implement the Principle of Least Privilege

Some practices are recommended when the goal is to apply the Principle of Least Privilege. Some of them are:

- Conduct an audit of the accounts;
- Establish the Least Privilege into new accounts;
- Elevate privileges for a limited time;
- Ensure that elevations of privileges are appropriate;
- Track all user actions on the network; and
- Conduct periodic audits.

Check out these items in more detail below:

Conduct an Audit of the Accounts;

The first step in implementing the Least Access Principle is to audit all existing privileges in accounts, programs, and processes, ensuring that users are only granted the necessary permissions to perform their activities.

Establish the Least Privilege Into New Accounts

Next, it is important to keep in mind that new accounts must be created in compliance with the Principle of Least Privilege, regardless of whether they are used by company managers or IT staff.

After all, if any of these users require a higher level of access afterward, it may be granted temporarily.

Elevate Privileges for a Limited Time

The privileges granted must be temporary whenever a user needs to raise the level of access for a specific project. In such cases, to ensure even greater security, it is possible to use single-use credentials.

Ensure that Elevations of Privileges Are Appropriate

Before applying the Principle of Least Privilege to accounts that already exist, you should assess which roles require elevated access and whether users actually rely on this elevation of privileges to perform their operations.

This assessment should be carried out periodically, including new tasks that may require privileged access.

Track All User Actions On the Network

To apply the Principle of Least Privilege, it is also important to monitor and track all user actions on your network.

This monitoring will allow you to detect over-privileged users, track suspicious activity, and identify evidence of an intrusion before it causes incalculable damage.

Conduct Periodic Audits

To ensure that permissions are always at the appropriate level, periodic audits are required. Keep in mind that performing this type of maintenance is much easier than starting to implement the Principle of Least Privilege policy from the beginning, saving you time and ensuring more security for your company.

Principle of Least Privilege: Example

Here are some cases where the use of POLP is indispensable:

- Social Media

We advise the conscious and responsible use of social media through the application of the **Principle of Least Privilege.**

In other words: to offer only the information necessary to make use of these media and not to share sensitive data with other user profiles.

In addition, it is important to configure privacy and security options in order to restrict users' access to your publications.

- Mobile Devices

Many applications request unnecessary permissions to perform their functions, such as telephone, location, and contacts, and can even be used to steal the banking details of the victims.

Therefore, it is also essential to apply the Principle of Least Privilege in this case in order to avoid damage caused by malicious apps.

- Health System

A receptionist of a health insurance plan should not have access to the clinical and confidential data of patients. This is because, without the Principle of Least Privilege, if a malicious user invades your computer, they will have access to these files.

- Manufacturing Companies

A manufacturing company should also grant its employees only the level of access needed to perform their tasks, rather than giving access to your entire ICS. This is because remote access to industrial resources and interconnectivity generate security vulnerabilities for the organization.

- Retail

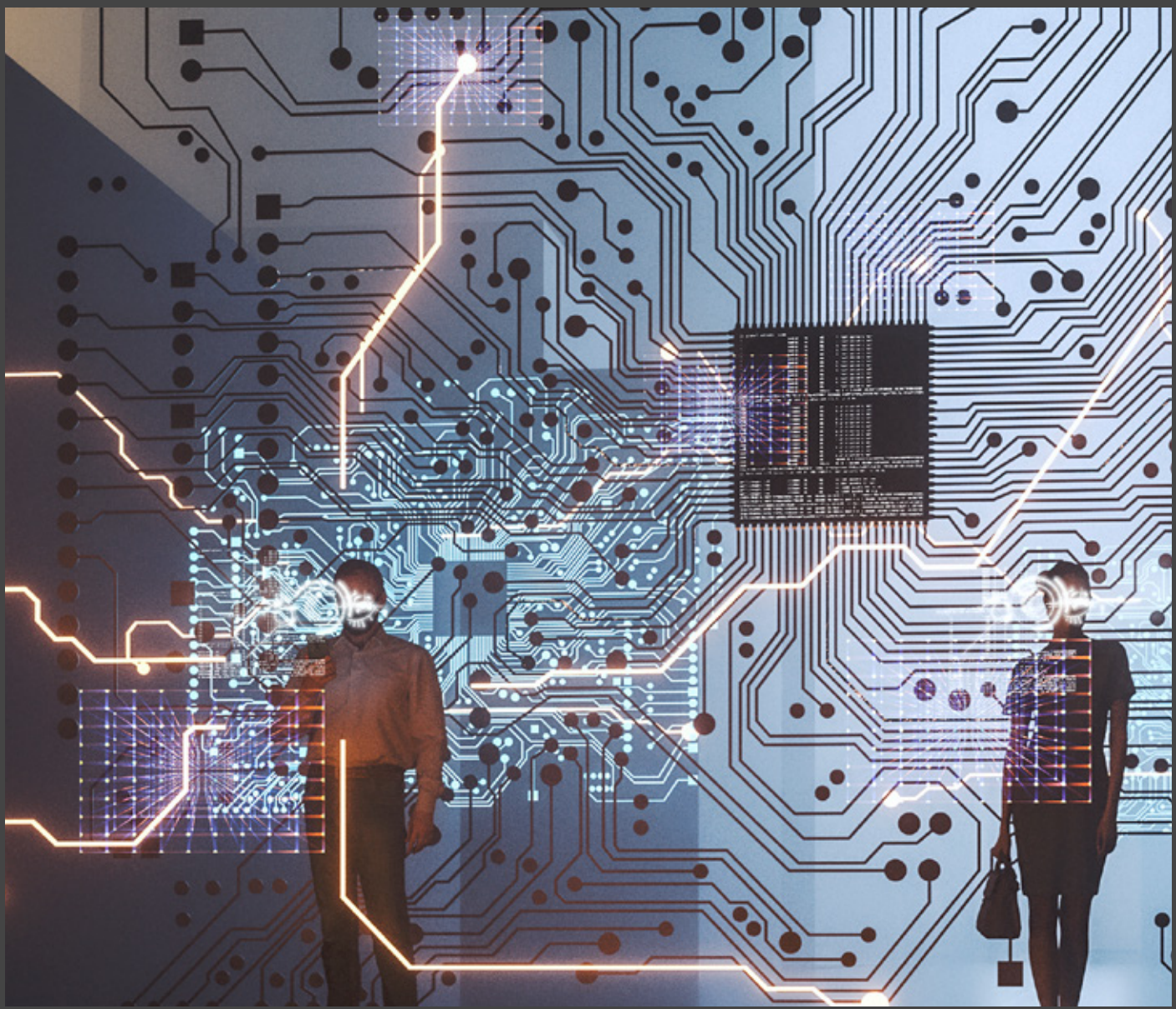
The retail sector usually has a high turnover of employees, which can be a problem if there is no control over the levels of access granted. For this reason, companies in the segment must apply the Principle of Least Privilege to ensure that only the right people have access to their data and resources.

- Financial Services

Professionals working in financial services deal with millions of customer files daily. To reduce risks, it is appropriate to apply the least access principle (POLP) in that context.

- Outsourced Activities

Many corporations outsource services such as CRM systems, HR, and databases. When they need technical support, it is advisable to apply the Principle of Least Privilege, ensuring that outsourced professionals have access only to the system they need to repair, which reduces risks to the company.



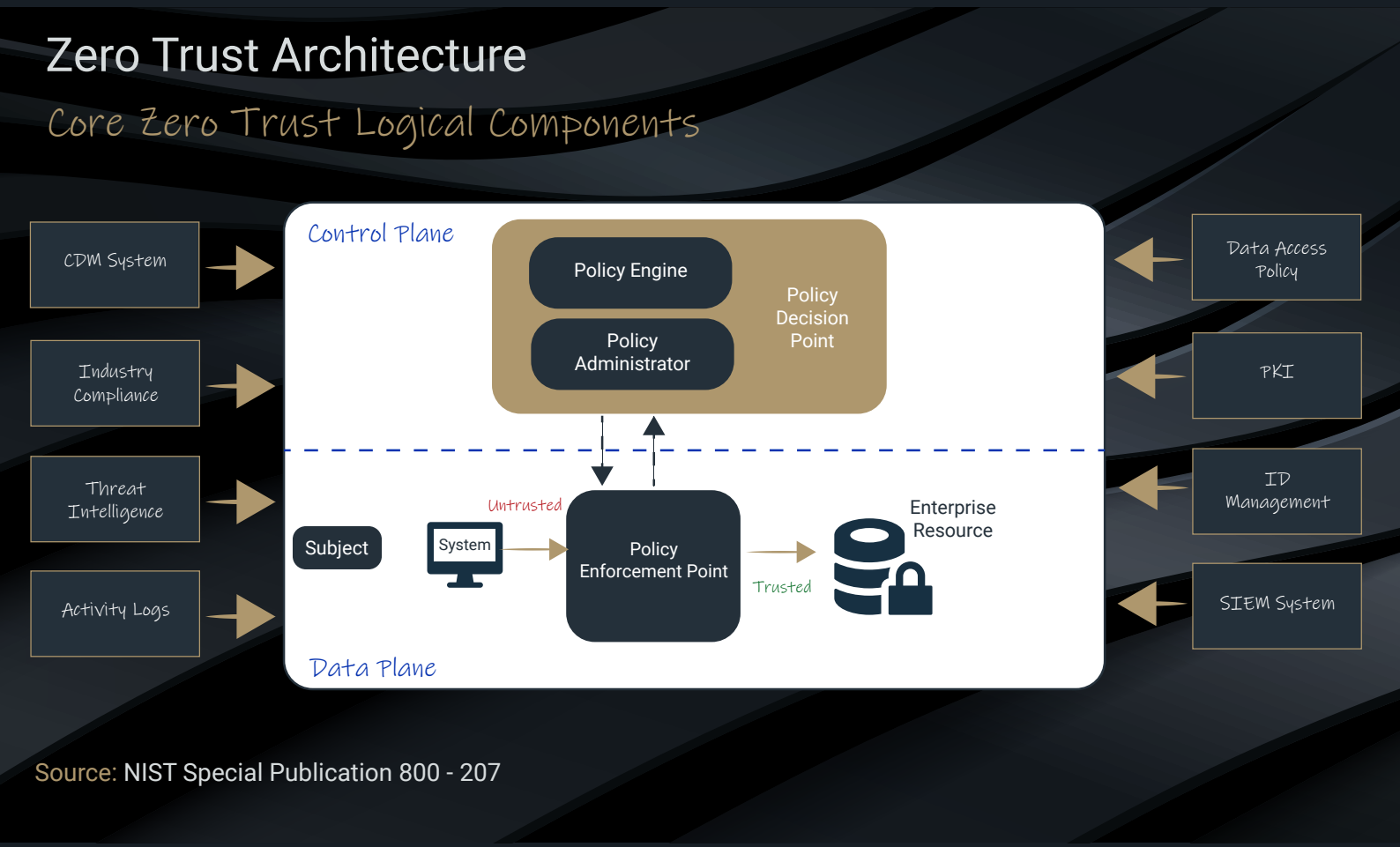
Resources

Infographic

Zero Trust architecture

Zero Trust architecture

Core Zero Trust logical components



Available for download in Press Quality

Infographics - Data Security

Cyber Startup Observatory - Community

Olayemi Agbeleye

CISO @ Central Securities Clearing System Plc

Olayemi Agbeleye

CISO @ Central Securities Clearing System Plc

Olayemi is a cyber security professional with experience in Cyber Resilience, Information Security, Technology Risk, Defense in depth, Security Operation Center.

With over 9 years' experience within the Banking sector, Fintech and the Capital market, he has been instrumental in the setting up of two Security Operation Centers.

His experience in multiple industrial sectors provides a deep experience and knowledge that has helped in cost effective implementation of complex security solutions.

Olayemi holds a degree in computer science from Olabisi Onabanjo University. He was recently awarded the Senior Lead Cybersecurity Manager and Senior Lead Incident Manager by the Professional Evaluation and Certification Board.

What is your overall approach to information security?

My approach personally has always been to identify the uniqueness of the industry in which I find myself. While information security best practice is a good practice in all industries, it is important to perform a proper risk assessment of the industry or business to identify the specific need of the industry or the business.

> "I approach security from all possible points of exposure, starting from endpoints connecting to the network either wired or wireless, traffic in and out of the network, vulnerability assessments on the network and potential insider threat."

In general, I approach security from all possible points of exposure, starting from endpoints connecting to the network either wired or wireless, traffic in and out of the network, vulnerability assessments on the network and potential insider threat.

Cyber vigilance and incident management are also tools that I see as important as every other aspect of Information Security.

How important is to have the CEO thinking that security matters?

Having a CEO who thinks and appreciates security concerns is the dream of any Chief Information Security Officer.

The best way to implement an enterprise security best practice is the top-down approach which requires the establishment of a management framework sponsored and supported by the C-level executive including the CEO.

Once the CEO supports the information security concerns within an organization, communicating the importance of security policies and procedures to other members of the organization becomes easier. Having a CEO who understands and support security initiatives also helps tremendously in getting security budget approved.

Understanding the implication from security threats not only provides the needed support in pushing security initiatives but also provides the needed management commitment in closing out identified vulnerabilities on the network as a result of the CEO's understanding of the potential impact of an exploit of such loopholes.

Almost everybody agrees that organizations need a culture of security. How can security leasers help facilitate that type of culture?

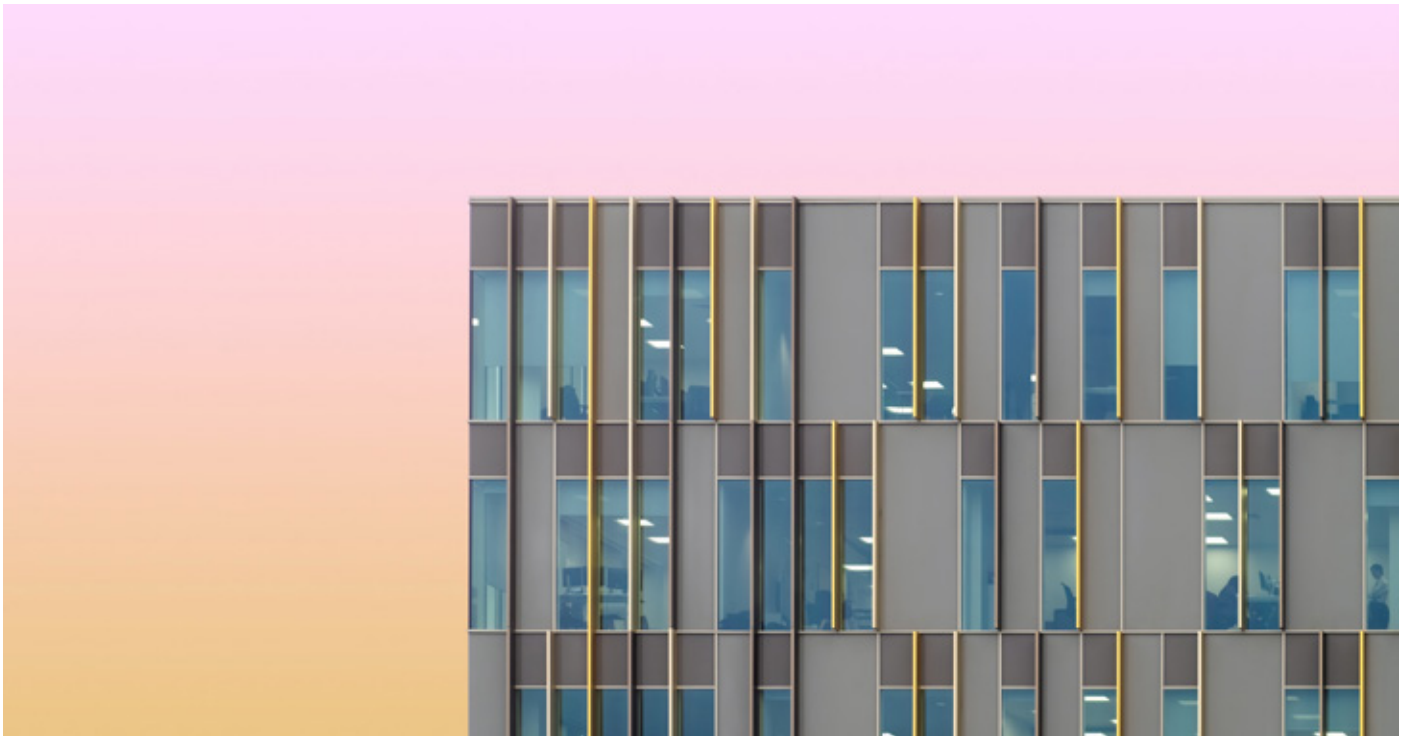
Creating a security culture within an organization begins with everybody understanding the risk to the company business objectives if such objectives are derailed by cyber actors. Understanding that it takes only one careless decision on the part of ONE employee to roll out the red carpet for hackers and scammers, security becomes the responsibility of every employee.

The first step in creating a security culture is to train employees on the importance of protecting the company against cyber-attacks and that the responsibility doesn't just rest with the security team but with all staff; by communicating in clear terms to show that the employees are not the security problem but are part of the solution; by educating and empowering all stakeholders to beat the cyber threats they face with the right security awareness materials and solutions; by communicating through awareness content that speaks to the audience (employee) in a way they understand.

With clear management support to information security programs and a good understanding of the risk faced by the organization, a security culture can easily be created with well-informed employees.

Ransomware and phishing are among the risks that have threatened all industries recently. From your perspective, how should companies mitigate these risks, and what has worked for you?

Over the years, Ransomware and phishing attacks have proved to be an effective tool for the cyber actors, mostly easy to launch and readily available to be purchased as a service on the dark web.



According to multiple sources (Verizon, IRONSCALES Email Security report etc.), over 90% of successful cyber-attacks begin with a phishing attack.

With the global cybercrime damages predicted to reach $6 Trillion annually by 2021 according to the Cybercrime magazine, organizations need to take a second look at their controls around thwarting phishing and ransomware attacks.

Because these attacks leverage on users to click on links or open malicious attachments, having an informed employee who can spot a phishing attempt is key in winning this battle.

Continuous security awareness must be put in place to ensure employees understand the risk posed by clicking on links or opening unknown attachments. Phishing simulation exercises must be incorporated into security awareness programs to ensure employees are tested on how to identify a phishing email.

While the human training is important, having technology in place which can detect phishing emails and ransomware attacks is as important. A good email security solution should be in place which can inspect the content of emails (attachments and links) to spot cases of phishing emails, as is having an anti APT solution at the edge of the network to inspect network traffic in and out of the network for malicious network content.

When the business is steaming along and wants to introduce new products or services, how do you make sure that security is plugged in?

Knowing that the role of security is to understand the business and provide the necessary support as a business enabler to ensure the business objective of the organization is not impacted negatively from cyber-attacks helps in balancing security with the business need.

Ensuring that the product development team are in sync with the security team is key in building security requirements into new products and services. It is also key to ensure that identified risks are not only treated but are brought to the attention of the decision makers.

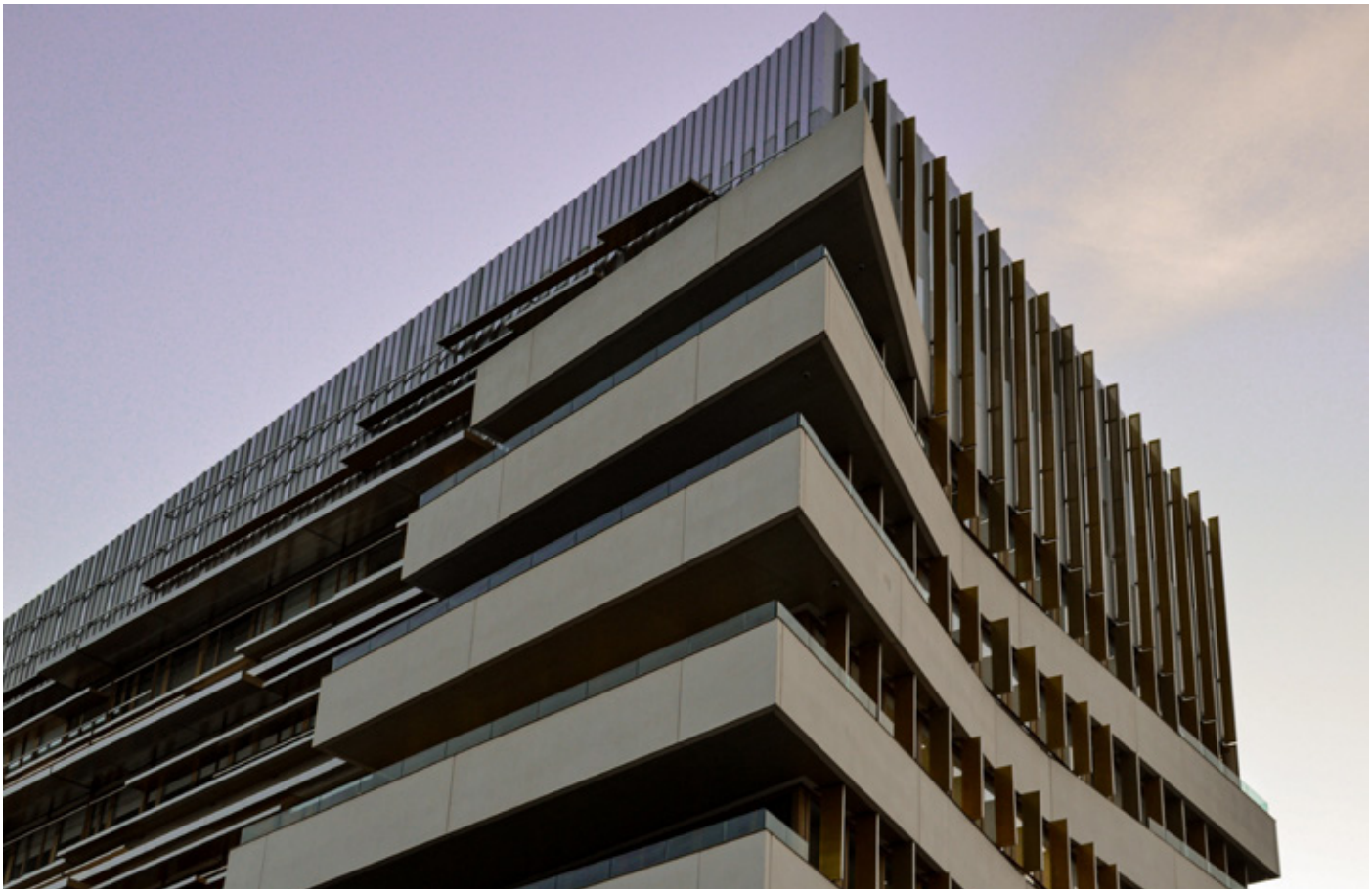
As much as security teams need to educate the business on the security issues, they also need their own education around corporate goals. This will ensure alignment of objective between the business leaders and the security team.

How has industry co-operation had an impact on cybersecurity?

We know today that cybercriminals are highly motivated and often change the rules of the game. They're also often willing to share their information freely so that new techniques spread rapidly among criminal communities. Organizations within similar ecosystems have also begun sharing cyber-attack information. Proactive information-sharing about attacks and defensive mitigations builds resilience across organizations participating within a given trust community. While a lot of companies still feel reluctant to share cybersecurity information because of legal implications, attacker retaliation etc., we have seen a lot more co-operation emerging in the last decade.

Closing statement

While the job of the CISO has become extremely difficult especially with the work from home as a result of the this pandemic, by consistently leaning new techniques and technologies, by adopting defense-in-depth strategy to protect our assets, I am sure we can always protect our organization's business objectives from cyber actors.



Insight

STELLAR CYBER

What is a Lean Security Team, and how to know if you are part of one

STELLAR CYBER®

What is a Lean Security Team, and how to know if you are part of one

Author: Sam Jones, Vice President of Product Management @ Stellar Cyber

At a glance

- 3 minute read
- What is a Lean Security Team
- A few questions you can ask yourself
- A few quick considerations

Recently I wrote a blog about what makes a lean security team tick, however, after I posted, it occurred to me that I probably should have spent a few minutes talking about the different types of security teams we run into and how to determine if you fit into the lean security team category.

You might say, well, why do I care if I am on, or manage, a lean security team or not? Great question. Let me answer that question with a short story from my personal experience.

I have worked for seven different cybersecurity startups, from very early in their lives to very late in the startup lifecycle. At each company, the resources available to the marketing team varied widely.

For instance, at company A, if I wanted to produce a video, I would do it all myself, from recording to editing to posting. However, at company B, for that same video, I would provide the content while a team of others would work on the editing and publishing. You could say company A had a lean marketing team while company B had a complex marketing team.

Was one approach better than the other, that is debatable. What is clear to me is that by understanding the resources I had available at the company, I knew what could and could not be done, especially when bringing technology in-house.

Now back to the world of cybersecurity. Over the years, I've worked with hundreds of security teams, from the team of 1 to teams with the ability to bring in every new piece of technology they wanted.

If you drew a spectrum, those two examples would represent the furthest extremes. Most teams lay somewhere in between these polar opposites. Here are a few questions you can ask yourself to determine where you and your team fit into the security team continuum.

- Are you a security "jack of all trades"?
- Do you, or anyone on the security team, moonlight as IT, or vice versa?

- Does the team manager (aka SOC or SecOps Manager) also work cases?
- Do triage alerts yourself?
- Is automation a big part of your team's strategy (even aspirationally)?

If you answered "Yes" to the majority of the questions above, then congratulations, you are more than likely on a lean security team. No what? As I mentioned, the whole reason to understand the type of team you are on or managing is to inform expectations and how you properly enable your team. So, if the more you think about it, the more you feel like you are indeed managing a lean security team, here are a few quick considerations.

Monitor Morale: While a lean security team can be just as effective as a more complex, more resourced security team, you, as a manager, need to pay close attention to your team members' morale. If you see someone's productivity drop, do not jump to conclusions. Take a few minutes to "check in" and see if they might need a break. While it's not ideal to have members out for a day, maybe you can offer a shorter shift one day or a longer lunch, just something to let the team member know you recognize their efforts and care about their well-being.

Mix it Up: While most lean security teams do not have specialists who only work a certain types of cases, there are some interesting things you could offer to break up the monotony that can occur over time. Maybe you offer shift changes once a quarter or even try a new shift structure that enables someone who might have always worked late at night to pull some afternoon duty. Small changes can keep things lively and recharge a worn-down security team.

Smart Enablement: We all need the right tools to complete our jobs. This is especially important for the lean security team, where time is the "coin of the realm". If your team is saddled with manually intensive legacy processes, now might be a good time to consider making some tooling changes. There are new options in the market that enable you to automate those manual processes, giving your team back precious time to catch and eradicate more threats. We focus on delivering products that help lean security teams to maintain a competitive advantage over attackers. When you have five minutes free, I recommend exploring our solution for yourself.

As I stated before, lean security teams can be just as effective as large, complex teams if expectations are managed correctly, and the team is enabled to be as effective as possible. To learn how Stellar Cyber can help your lean security team contact us today.

About the Author

Sam Jones

Vice President of Product Management

Sam is an experienced product development leader with a track record of building AI and security products that customers love. He has a strong background in AI/ML, data infrastructure, security, SaaS, product design, and defense.

Sam has held product and engineering positions at companies including Palantir Technologies and Shield AI, and worked for the US Air Force on cyber defense strategy. Sam earned his Bachelor's degrees in Electrical and Computer Engineering from Cornell University.

Resources

Infographic

Ransomware attacks, overview

Ransomware Attacks

Overview

Ransomware Attacks - Overview

WHAT IS RANSOMWARE?

- Ransomware is a type of malicious software that gains access to the victim's files or systems and blocks user access to them or releases the data for public download
- It uses different techniques but the most common is to encrypt the victim's files, making them inaccessible and demanding a ransom payment to decrypt them
- Recovering the files without the encryption key is an intractable problem (it would require huge resources and consequently is considered infeasible)

RANSOMWARE FACTS

- The global attack volume jumped by 151% during the first six months of 2021
- Over 90% of ransomware attacks are delivered via email phishing
- The total recovery cost from a ransomware attack has increased from $761,106 in 2020 to $1.85 million in 2021
- Healthcare, Financial Services, IT and Critical Manufacturing are the most targeted industries in 2021

HOW DOES IT WORK?

1.- **Delivery Vectors:**
- Most ransomware is delivered via email (phishing emails with ransomware payloads) when the victim clicks a link or downloads an attachment that delivers the malicious software
- Other delivery mechanisms are drive-by-download attacks on compromised or malicious websites, bespoke Remote Desktop Protocol (RDP) attacks and social engineering leveraging social networks messaging
- Generic ransonware is rarely individually targeted

2.- **The Process:** most ransomware variants encrypt the files on the affected system, making them inaccessible and demanding a ransom payment using cryptocurrencies to make it difficult to trace and prosecute the perpetrators

BIGGEST ATTACKS

Bigger, better and more sophisticated strains are popping up. The most important ransomware attacks have been:

- **SamSam**
- **REvil or Sodinokibi**
- **SimpleLocker**
- **WannaCry**
- **Cerber**
- **Ryuk**
- **TeslaCrypt**
- **NotPetya**
- **Katyusha**
- **PewCrypt**
- **LockerGoga**
- **Bad Rabbit**
- **Jigsaw**
- **GandCrab**
- **Dharma**

PROTECTING AGAINST IT

1.- Reduce the risk of a ransomware attack:
- Principle of Least Privilege: restrict users' permissions and conduct proper credential tracking
- Education and security awareness training
- Proper endpoint hygiene with proper configuration, regular updates and patches
- Leverage existing advanced threat prevention solutions to address all the delivery methods
- Up to date asset inventory and file integrity monitoring

2.- Limit the fallout in case of attack:
- Frequent and reliable backup and recovery
- Clear and regularly tested recovery plan
- Crisis management preparation, strategy and procedures

Available for download in Press Quality

Infographics - Threats & Attacks

Cyber Startup Observatory - Community

Tarek EL-Sherif

Head of IT Risk @ Abu Dhabi Commercial Bank

Tarek El-Sherif

Head of IT Risk @ Abu Dhabi Commercial Bank

Tarek has gained a wide experience in distinguished multinational banks in Egypt in the fields of information technology and information security, as well as developing policies, procedures and relevant governance frameworks for information security risks in the banking industry.

During this practical experience, he participated and supervised the implementation of a large number of effective projects in information technology innovative, security solutions.

Tarek holds a master's degree from the Arab Academy for Banking and Financial Sciences with a major in Business Administration (MBA).

He certified as a Chief Information Security Officer from EC-Council, and was recently honored as a top IT leader of Egypt, recognized at The World CIO 200 Summit.

How do you articulate the three-pronged approach of people, processes and technology?

People, processes and technology are the main pillars of performing any activity as they are the cornerstone of maintaining effective business management and achieving the goals of the organization and, based on the nature of each industry, this approach has its own model.

However, many organizations believe that by applying and implementing the latest security technology techniques, they will be able to handle all security incidents - which is not the real situation, as without structured processes and high awareness for people, technology cannot be effective and efficient.

"Many organizations believe that by applying and implementing the latest security technology techniques, they will be able to handle all security incidents - which is not the real situation."

That is why the efforts of security leaders often focus on improving the organization's information security strategies, enhancing processes and building a strong awareness program.

The right balance between these pillars gives us a solid foundation to build on, subject to them being consistent together.

Despite that, the crucial element is people, as the computers do exactly what we ask them to do, while the right people with the right attitude, experience, expertise and qualifications will help to identify and develop the adequate processes and put them in the right place to ensure that the technology is implemented in fruitful ways.

How important is to have the CEO thinking that security matters?

Information and data have become a key corporate asset today, and information security has become a major strategic priority.

CEOs and executive management should be concerned with information security as a strategic issue and vital function and not just a technical problem and deal with it as a serious issue related to enterprise risks.

Moreover, when security leaders are given the required authorization and delegation of authority necessary to confront security incidents and power to report the risks of information security issues directly to members of the Board of Directors.

At this moment, information security leaders have the encouragement needed to fulfill their mission, the ability to implement information security policy and obtain the necessary resources (facilities, budget, information technology tools and human resources) to overcome obstacles, make things happen and realize the benefits of the information security program - in addition to ensuring that information security management is included as part of the organization's business goals and incorporated into the organization's culture.

Almost everybody agrees that organizations need a culture of security. How can security leaders help facilitate that type of culture?

Security culture comes primarily from organizations. The challenge is with the people who respond to phishing emails by clicking on the links they receive and believing what anyone says to them.

Keeping enterprise information secure is a huge challenge and faces enormous difficulties such as lack of knowledge or carelessness.

Even well-intentioned employee mistakes can leave the company vulnerable to cyber-attacks, cause information security problems and may affect the services that organization provides to its clients, which certainly harms the organization's reputation and financially as well.

In general, people within the organization must understand the correct thing to do and basic security concepts that should be in place, such as maintaining the confidentiality of data, keeping passwords secret, avoiding social engineering and refraining from discussing confidential topics outside the workplace or with unauthorized persons.

For this reason, security leaders should address this challenge with appropriate measures by establishing an ongoing security program that focuses on enforcing security policy approved by top management and implementing appropriate controls, as well as monitoring and auditing program consistency and effectiveness.

In addition, the awareness program should motivate and encourage employees to report not only the full incidents, but even the suspicious things they face.

Everyone should feel like a security person, and by engaging employees, the security issues will be discovered more easily, and you will be better able to respond faster.

Moreover, the organization must build and protect its own security culture and ensure its sustainability and invest in it, in order to create a better security awareness culture. When a culture of security is sustainable, it transforms security from a one-time event to a life cycle that generates returns forever.

What unique security challenges does your industry face?

Lack of budget, violation of compliance regulations, breach of data privacy and third-party risks are generally the main obstacles. However, the financial industry always faces an increasing number of challenges, especially in the digital transformation era as technology empowers banks to innovate in digital services such as online banking, mobile banking, mobile wallet and increased dependence on digital money.

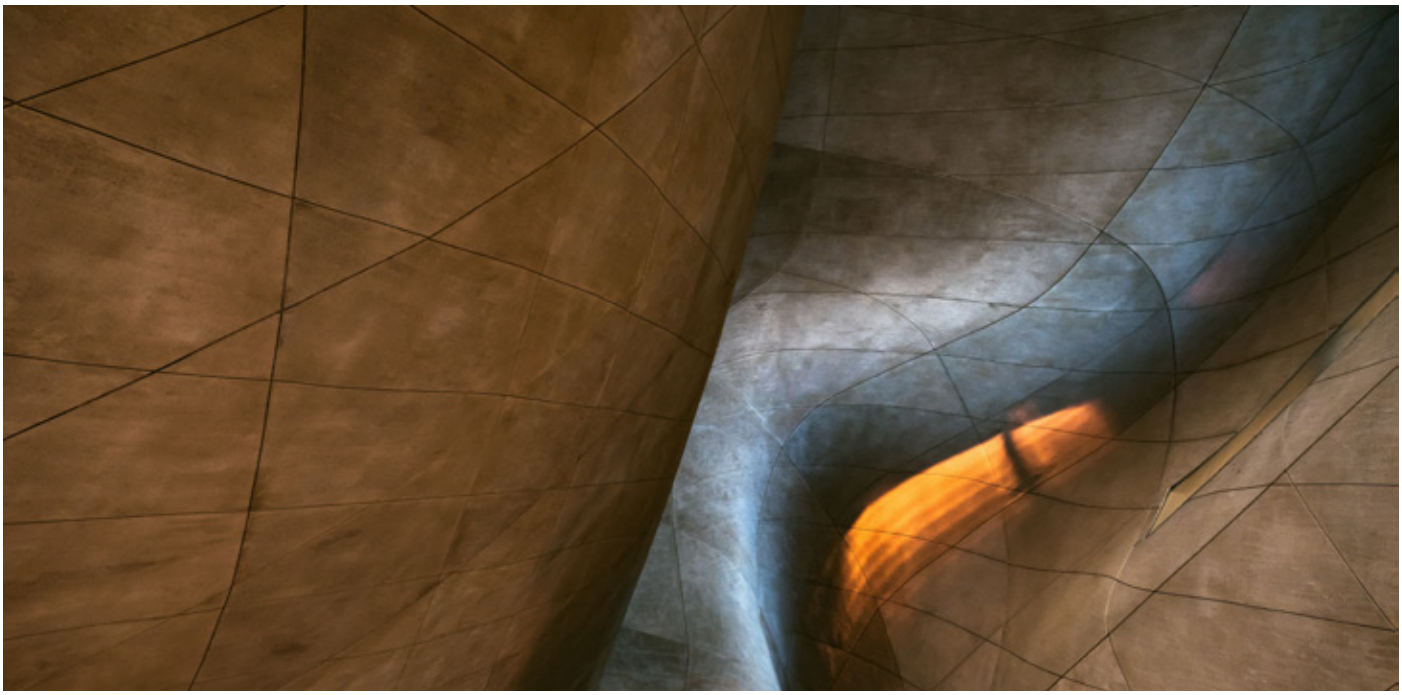
At the same time, organizations suffering from cyber-attacks, which are among the most important barriers in implementing digital transformation agendas as most cyber security technologies used today can be sufficient solutions at the present time but any potential new wave of fraudulent schemes could bypass existing security controls completely.

Given that the financial industry is a victim of increasingly sophisticated cybercriminal tactics, it may be more expensive compared to cybercrime in other industries.

Accordingly, security leaders struggling to secure customer data and develop proper risk mitigation strategy to prevent unauthorized activity, focus on emerging threats and vulnerabilities and try to bridge existing security gaps by deploying the best security solutions and developing additional security measures and layers to address rapidly developing cyber security attacks.

Digitalization is a double-edged sword, offering incredible benefits but also entailing serious risks. What are your thoughts on this inevitable development?

Digital transformation is an indisputable fact that we have to deal with. In the digital transformation era, innovation is happening everywhere, and all entities are accelerating with each other on the digitalization path.



Although the benefits and advantages of digital transformation are clear to see, the journey will not be without challenges or obstacles because the implementation of new digital technology requires not only the modernization of existing IT systems, but also other changes that rely on advanced technologies such as cloud computing, artificial intelligence (AI) and the Internet Things (IoT).

Consequently, emerging cyber security solutions should have new features such as security automation and artificial intelligence for cyber security solutions as a key to dealing with the increasing number and sophistication of cyber security threats and the ability to detect attack patterns through the full implementation of machine learning systems.

Blockchain technology also revealed the capabilities of technology towards decentralizing and securing transactions across IT systems and devices in a secure manner that maintains privacy.

What is the best way to foster an image of information security being there to help support the business rather than just being about the raw technology?

Information security exists to support business and facilitate its mission, and most security leaders realize this and aim to integrate information security and its different tiers into the business, and they should provide this meaning to all organizations' levels.

Moreover, the internal units should be kept aligned with the information security program and provide more insight into cyber security issues within the organization to ensure the best integration.

Insight

Jose Monteagudo

Healthcare cyber security – state-of -the-art

Healthcare cyber security – state-of-the-art

Author: Jose Monteagudo, Editor-in-Chief, Cyber Startup Observatory

At a glance

- 5 minute read
- Where is the industry now?
- Understanding the levels of Health IT
- Security, confidentiality and privacy
- Major threats for the industry

Where is the industry now?

Good health and well-being are one of the UN Sustainable Development Goals, the United Nations' new roadmap to improve people's lives by 2030.

In most developed countries healthcare systems are involved in a transition process – the digital transformation – from paper-based to Electronic Health Systems.

In 2017, 8.8 % of the gross domestic product (GDP) of most developed nations (OECD countries) was spent on healthcare – an enormous part of a country's economy.

This referred digital transformation not only has important implications in terms of operational excellence and costs, but also in terms of Privacy, Confidentiality and Data Integrity.

The healthcare industry still struggles with interoperability challenges

Here are the six key challenges related to EHR interoperability (US Government Accountability Office – GAO):

1. **Complex ecosystem with a myriad of stakeholders:** the healthcare ecosystem is extremely complex. In figure 1, below, we show a simplified view of the key stakeholders. Please note that the architecture might be much more complex.
2. **Insufficiencies in interoperability standards.** While standards for electronically exchanging information exist, the industry recognizes they are insufficient for achieving full interoperability.

3. **Privacy rules are varied.** Privacy rules vary across states, countries and regions. This represents a burden for the major players involved, including healthcare providers, software and IT companies and other stakeholders.

4. **Accurately matching patient records.** Patient matching presents an issue for interoperability because different systems use different demographic information to match individuals to their health records. Doing so may yield inaccurate results, as patients may have the same names, birthdates and ages. Thus, trying to corroborate identities between systems that use different demographic data is not possible because systems intake different data.

5. **Prohibitive costs.** System costs and legal fees can deter providers from achieving interoperability. Some EHR systems require multiple customized interfaces to work with other platforms, and providers have to pay the costs associated with building those interfaces.

6. **Lack of governance and trust among entities.** Establishing trust between entities that are needed to support interoperability was noted as a challenge, largely because agreements and organizational policies don't always align between parties.

The diagram below portrays a simplistic view of the healthcare ecosystem including some of the most common messaging standards:

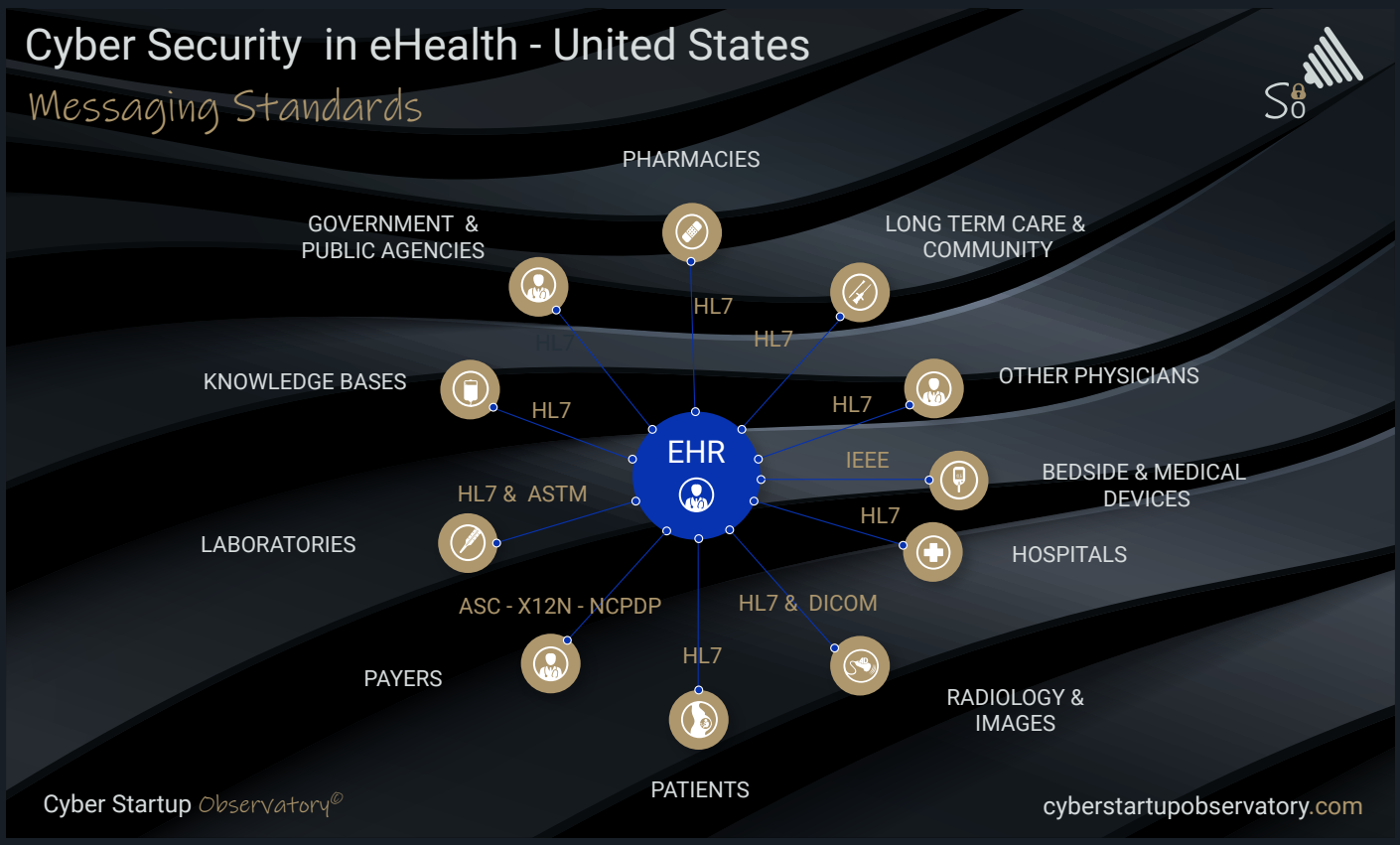


Figure 1: The healthcare ecosystem: key stakeholders and messaging standards

Framework for understanding the levels of Health IT

We have covered the major challenges related to EHR interoperability. Before delving deeper into the major cybersecurity threats faced by the industry, let's shed some light onto the different levels of health IT. A general framework for understanding those levels from a technical perspective is as follows:

- Application Level
  - Computerized Provider Order Entry (CPOE), Clinical Decision Support (CDS), Electronic Prescribing (e-prescribing), Electronic Medication Administration Records (eMAR), Results Reporting, Electronic Documentation, Interface Engines, and so on
- Communication Level
  - Messaging Standards HL7, ADT, NCPDP, X12, DICOM, ASTM, and so on
- Coding Standards
  - LOINC, ICD-9, CPT, NDC, RxNorm, SNOMED CT, and so on
- Process Level
  - Health Information Exchange (HIE), Master Patient Index (MPI), HIPAA Security/Privacy, and so on
- Device Level
  - Tablet PCs, Application Service Provider (ASP) models, Personal Digital Assistants (PDAs), Bar Coding, and so on

Security, Confidentiality and Privacy

Privacy Standards and Security Standards are necessarily linked. Any health record system requires safeguards to ensure that the data is available when needed and that the information is not used, disclosed, accessed, altered, or deleted inappropriately while being stored or retrieved or transmitted.

Security Standards work together with Privacy Standards to establish appropriate controls and protections. Health sector entities that are required to comply with Privacy Standards must also comply with Security Standards.

We need to pay close attention to the electronic systems which manage Patient Identifiable Information.

Some of those systems are detailed below. Please note that this is not an exhaustive list and there are many others:

- Electronic Health Records and Electronic Medical Records that capture and store patient information
- Laboratory Information Management Systems
- Prescription Information Management Systems
- Patient Registration and Scheduling Systems
- Systems for Aggregation and Reporting Information, Monitoring Health Programs and Tracking Patients' status
- Clinical Decision Support Systems
- Systems for Medical Research

Major cybersecurity threats for the industry

Overall, limited spending on cybersecurity is the number one threat among small to mid-sized health delivery organizations, even among larger systems.

Hospitals must make numerous risk management decisions against resource constraints and cybersecurity has historically not been given the attention it requires — for the integrity and availability of their data, the reliability of their clinical operations and most importantly, patient safety.

Some of the protocols and standards discussed in this article were created when cybersecurity wasn't even a concern.

Nevertheless, considering the huge impact on patient safety and the damages caused, cybersecurity in healthcare must be a top priority.

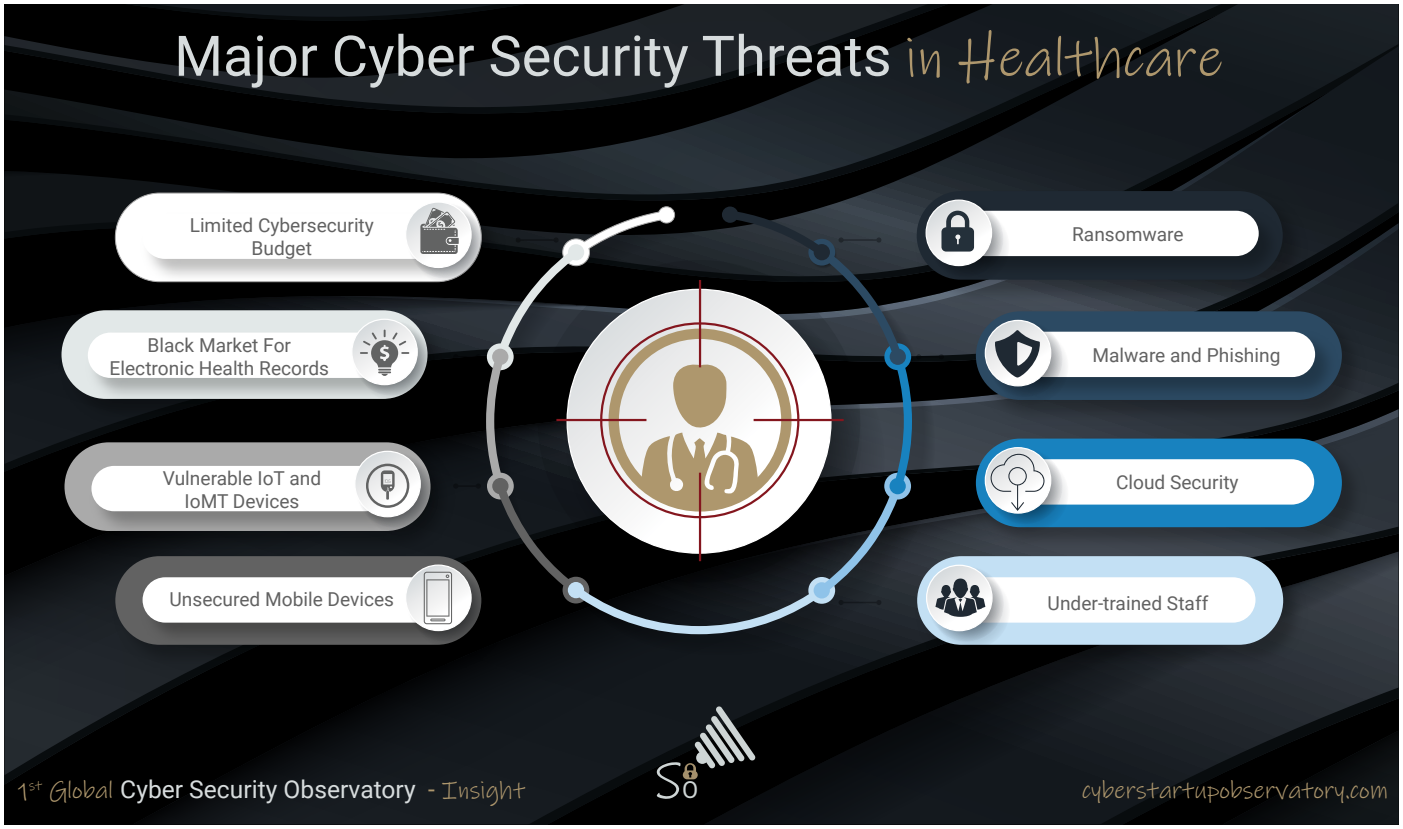


Figure 2: Major Cybersecurity Threats for the industry

Another massive threat is ransomware. It is a type of malware that infects systems and files, rendering them inaccessible until a ransom is paid. When this occurs in the healthcare industry, critical processes are slowed down or become completely inoperable. Typically, ransomware infects victim machines in one of three ways:

- Through phishing emails containing a malicious attachment
- Via a user clicking on a malicious link
- By viewing an advertisement containing malware (malvertising)

Ransomware has become such an issue that in the US, the MS-ISAC, along with their partners at the National Health Information Sharing and Analysis Center (NH-ISAC) and Financial Services Information Sharing and Analysis Center (FS-ISAC), have teamed up to host training sessions around the country on how to defend against it.

As an example, we may consider the WannaCry ransomware attack that hit over 230,000 computers in over 150 countries in May 2017. Organizations that had not installed a Microsoft security update from April 2017 were affected by the attack.

In the UK, the National Health Service (NHS) was seriously impacted. According to NHS England, the WannaCry ransomware affected at least 80 out of the 236 trusts across England, because they were either infected by the ransomware or turned off their devices as a precaution. A further 603 primary care and other NHS organizations were also infected, including 595 GP practices (Investigation: WannaCry cyber attack and the NHS).

As discussed, cybersecurity events in healthcare are particularly critical due to the impact on patient safety. In the case of the WannaCry attack, although the NHS was not the specific target, the impact was massive.

According to the Department of Health investigation, thousands of appointments and operations were cancelled and in five areas patients had to travel further to accident and emergency departments. Between 12 May and 18 May, 6,912 appointments had been cancelled, and it is estimated that more than 19,000 appointments would have been cancelled in total, based on the normal rate of follow-up appointments to first appointments.

Even though the impact was huge, this incident could have caused more disruption if it had not been stopped by a cyber researcher activating a "kill-switch".

But ransomware is just one of the key cybersecurity threats faced by the industry.

We should add to this dangerous mix:

- **High demand for Healthcare Records:** as electronic health records (EHR) are far more valuable than financial data, there is huge demand on the black market, fuelling the numerous cyber-attacks that are damaging the reputation and finances of healthcare operators.
- **Vulnerable IoT, IIoT and IoMT devices:** there is a correlation between the proliferation of IoT, IIoT, IoMT and other connected devices and the increasing risk for the data they collect, manage, store and transmit.
- **Unsecured Mobile Devices:** considering the ubiquitous presence of mobile devices in the industry, especially with the Bring Your Own Device (BYOD) trend among healthcare companies, once these devices are connected to the healthcare infrastructure, a plethora of new threats arise. This is particularly acute once we add to the cocktail both the fact that healthcare employees have not been traditionally educated in cybersecurity risks and the extremely high sensitivity of the data managed.
- **Cloud Security:** healthcare organizations are moving to the cloud at full throttle, with some statistics showing that nearly two thirds of the organizations are leveraging the cloud in some capacity. The top cloud security concerns are the risk of unauthorized access and the risk of malware infiltrations.

In addition to the referred concerns, a key question arises. Who is responsible for the critical data being stored on the cloud?

On the cloud model, there is a shared responsibility. While cloud providers are responsible for protecting their service, responsibility over regulatory compliance, data access and user credentials for the huge trove of medical records and other sensitive data falls to the healthcare IT team. It is crucial for IT teams to fully understand the delineation of this responsibility.

- **Under-trained Staff:** healthcare employees have easy access to patient sensitive data.

Training your staff is critical, but just as important as training is getting them to truly understand the potential impact of their actions.

It is beneficial to continue to enhance your training to focus on healthcare security as well as specialized role-based training. It is a fine balance to do so when clinicians' priority is patient care, but through thoughtful, ever-changing awareness training and scheduled phishing exercises, more awareness can be brought forward.

Another angle to this discussion is Insider Threat.

- Malware and phishing:

One of the most significant threat vectors for a cyber event is phishing. It is essential to train people to recognize common phishing attempts. Cybersecurity and awareness training cannot be underestimated, even though we continue to implement technical controls in managing phishing threats.

Having said that, we have seen sophisticated attacks lately for which purposely designed phishing awareness programs might prove useless. There are sophisticated solutions on the market to help companies address sophisticated phishing attacks leveraging state-of-the-art artificial intelligence, in particular machine learning and other technologies such as computer vision.

- **Third Party Risks:** there is a complex ecosystem of third-party vendors and it's by no means trivial to limit their access to healthcare systems, computers and other devices. While patient data should be highly protected from external personnel, it might be difficult to guard all points of access.

- **Lost, stolen or inadequately disposed-of old hardware:** lost or stolen devices, as well as inadequately disposed-of old hardware, represent a huge risk. In the first case, the risk comes from the devices still having access to the healthcare network and potentially valuable data. In the case of old hardware, especially that containing storage or hard drives, it is extremely important to destroy them properly in order to assure that sensitive information, for example patient data, cannot be recovered by criminals. Companies should stay up to date on HIPAA compliance to ensure that they are following the most recent guidelines.

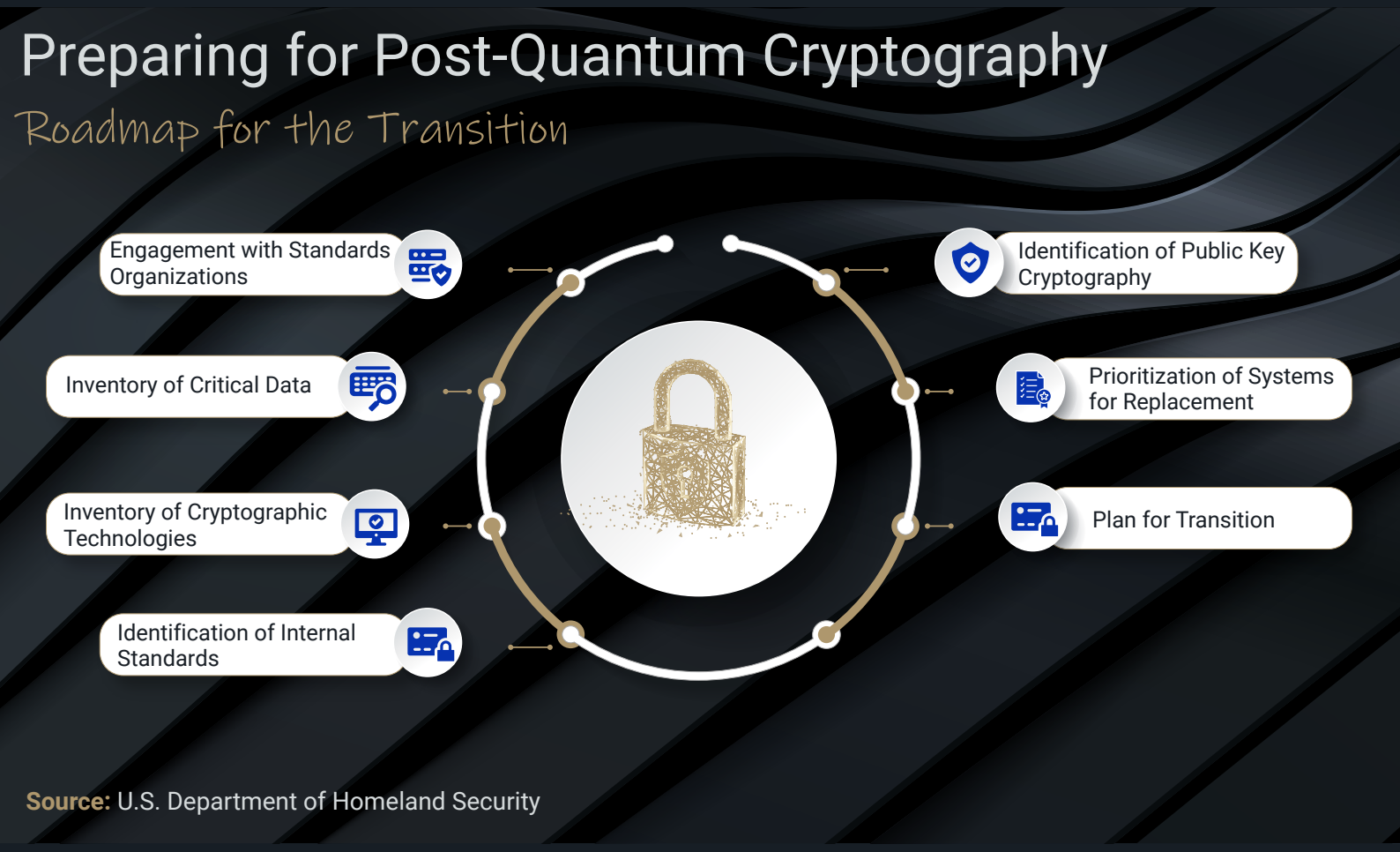
Resources

Infographic

Preparing for Post-Quantum Cryptography

Preparing for Post-Quantum Cryptography

Roadmap for the transition



Available for download in Press Quality

Infographics - Data Security

Cyber Startup Observatory - Community

Gift Medi

CIO @
Medical Aid Society of Malawi

Gift Medi

CISO at Medical Aid Society of Malawi

Gift is an ICT professional mainly focusing on digital transformation strategies and management. His core technical strength is in distributed systems architecture and software development.

He is very well versed in business processes and the relevance of technology as an enabler.

Gift has 15 years industry experience, an ITIL v4 Managing Professional (ITIL Expert), DevOps Certified practitioner, and ISO22301 BCMS Lead Implementor.

He holds a BSc. Computer Networks from University of East London, MSc. in Information Technology from LCMIT and an MBA from MANCOSA.

What is your overall approach to information security?

In simple terms, information security is the safeguarding of information from unauthorized access or destruction. Access to information leads to data manipulation, copy or loss.

With the above understanding, one needs to have an approach to ensure information is secure. The approach that I have applied throughout the years has been a **"Risk based approach".**

From my perspective, this is an approach that sets out to first understand the ecosystem in place, the players in the ecosystem, the strategy and vision which needs to be achieved by the ecosystem, the pain points of the ecosystem and the overall changing environment (PESTLE) in which the ecosystem operates.

Once understood, risk profiling can be done and prioritised.

Meaningful information security can then be implemented which addresses specific needs and looks out for specific breaches. ITIL and BCMS (ISO22301) have greatly come to my aid as enablers of this approach.

By using a Risk based approach:

1. Information is identified and classified;

2. Threats, vulnerabilities and risks in the ecosystem are identified and classified;

3. Stakeholders are identified and classified on a needs and need to know basis;

4. Measures are identified through cost benefit and analysis process;

5. The right information security measures are then implemented on a well worked out plan of approach that meets the need;

6. All that happens is monitored for responding to security incidents in a proactive and reactive manner and also for continuous improvement.

In summary, my overall approach is one of a Risk based approach using ITIL v4 (Service Management) and ISO22301 (Business Continuity Management).

How do you communicate information security issues to the board?

Let me start by saying, NEVER USE TECHNICAL jargon, unless it is brought up and you are asked to explain for their understanding. And when you do happen to explain, approach it as if talking to a layman.

The board's mandate is to do three things in relation to the strategic vision, direction and the objectives set out:

1. Monitor performance,

2. Evaluate performance,

3. Direct next steps from what is monitored and evaluated.

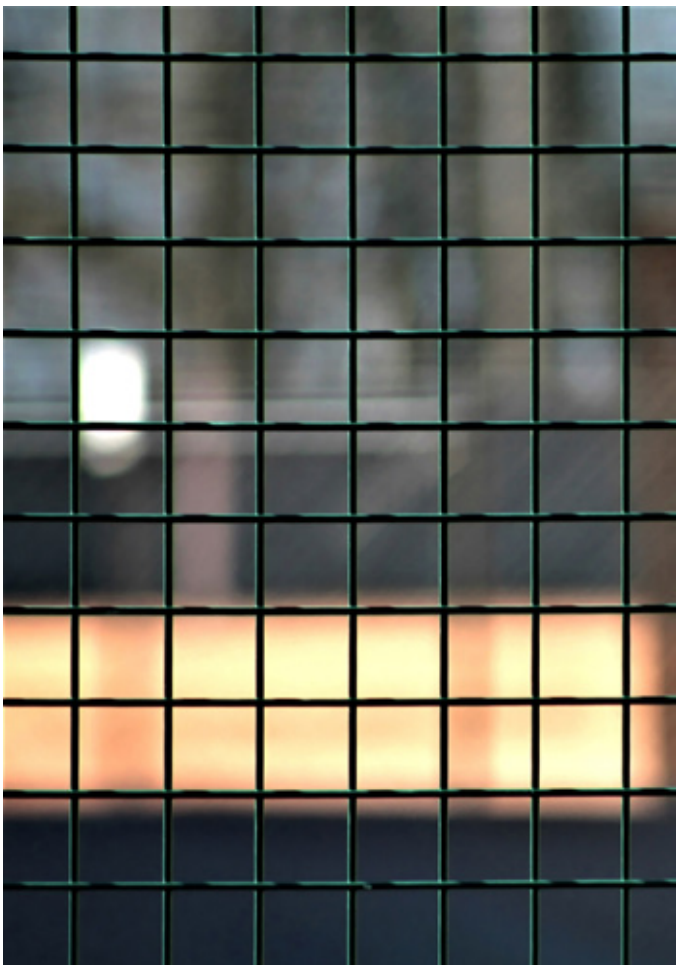
Through these points, the board further ensures that stakeholders' interests are protected i.e., shareholders, customers/clients, employees, third-parties etc. So, if one is to communicate information security, the above should be the line of thinking.

What strategic value will information security add to the overall objectives and vision?

From my personal experience, I have used a particular approach to communicate information security issues to my board. I first tend to refer to certain information security breaches in the country and the impact these breaches had on the organization, its shareholders, customers and employees. I go further to make the board understand what caused the breach and what should have been done to either reduce the impact or for it to not have happened at all. I then relate to our environment, so they understand where the gaps are and if these gaps are left unattended, then the risk factors are higher.

I then propose the plans we as ICT intend to implement for Information security in support of the vision.

In summary, communicate information security to the board by translating it into a language which they will understand.



Almost everybody agrees that organizations need a culture of security. How can security leaders help facilitate that type of culture?

I also agree with this statement. To have a culture of security simply means to have people be aware of the security scope in which they are supposed to be working in and stick to the confines of that scope. People should also know how to react when unusual things happen within their security scope. This will ensure their safety and any potential unauthorized access to information.

Therefore, to facilitate a security culture, security leaders must do several things:

1. Understand the environment in which people work and tailor make security workshops.

2. Consider appointing champions in every department who ensure the fundamental security protocols are followed.

3. Have monitoring tools coupled with procedures and report any potential security lapses or breaches that may arise.

4. Use the breaches as case studies for practical continuous learning and improvement during workshops or when informing stakeholders via email, notice boards, policy updates etc.

5. Congratulate stakeholders for keeping security breaches at a low to help ensure there is continued motivation and vigilance.

Just to use an analogy of a grocery store. It opens 8am and closes 7pm. During opening times, there is a cashier behind the counter who serves customers. The cashier is backed by automatic doors that can be locked electronically, CCTV, a panic button and a baseball bat. The CCTV is a deterrent and used to record events for investigation purposes, the panic button is used to call for support, the baseball bat is for self-defence. Within the grocery environment, if the cashier does not know and understand these security features and should there be a security breach, the potential for loss is very high. Use of the different security features depends on the level of the security breach. The cashier needs to know the right security feature to apply given different scenarios. Repetitive workshops and practical exercises are key to achieving this.

In summary, a security leader can facilitate a security culture by ensuring practical know how on a continuous basis through them first and then through champions as the process matures. The essence of culture is to involve more and more people, so they become self-managing.

What are the biggest challenges you face in the year ahead?

We have embarked on the implementation of an all-digital environment. This means updating our infrastructure and the ICT operating environment. This further means we MUST take all stakeholders onboard with us as we transition into a data-centric environment. In other words, our people need to become the digital culture that we seek

As we implement these changes, we have incorporated information security from the onset. From the end-user, through all the applications and down to the network. The reason for this audacious transition is because of what Covid has brought to the table and our understanding is that this world will return to normal, but will never be the same again. The need to transact digitally seems to have been embedded in the minds of every stakeholder. There is therefore time to think outside the box and respond to business unusual. To borrow a leaf from ITIL v4, we are dealing with VUCA (Volatility, Uncertainty, Complexity and Ambiguous) situations, which we must face head on.

Given this path, there are several challenges:

1. How do we transition and keep our environment secure, our stakeholders satisfied and secure?

2. How do we ensure a seamless and well controlled transition for stakeholders into a digital culture?

3. How do we ensure we maintain focus for ICT to continue being an enabler of the strategic vision?

4. How do we securely integrate with all our third parties?

5. How do we maintain regulatory compliance?

6. Can we achieve all this within the set deadlines given the Covid situation where delivery of resources has become a challenge due to travel restrictions?

7. Are we making the right investment?

These questions must be answered through practical realisation of a working environment.

The key to achieving this fit is a blessing first from the Board, then the availability of resources and capable human resources to carry out the work.

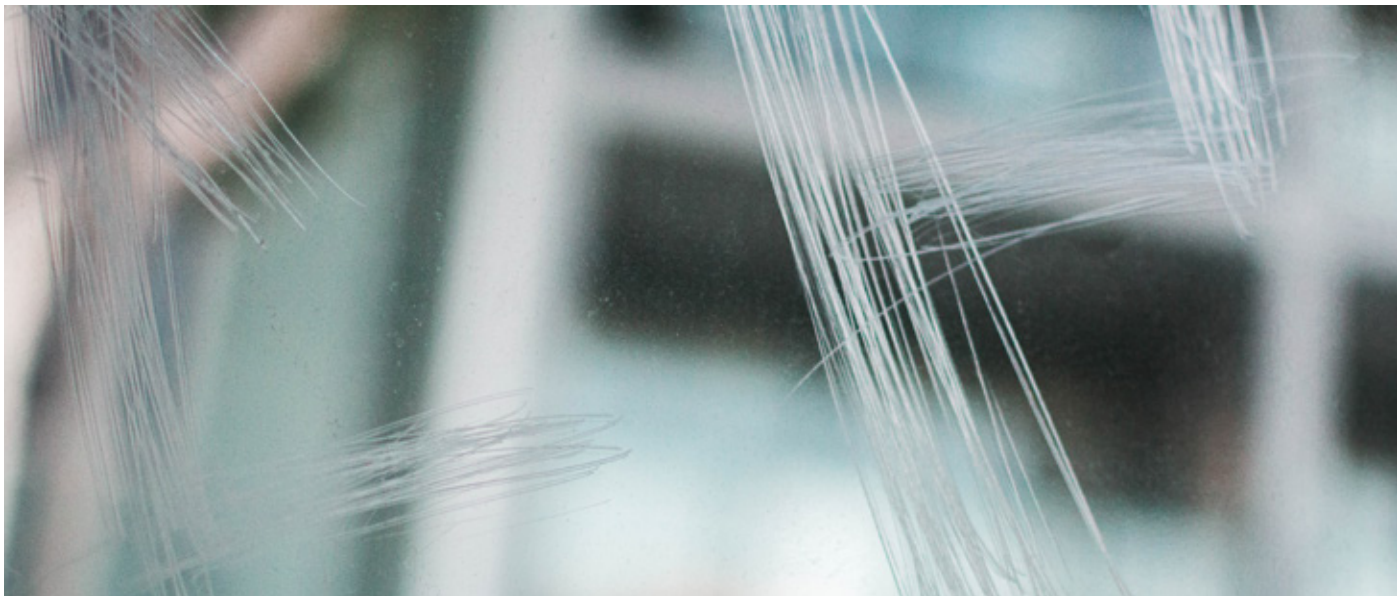
In summary, the biggest challenge is transforming into a digital environment to remain relevant and competitive as a business, manage costs and improve efficiencies. And all this must be done during Covid related challenges.

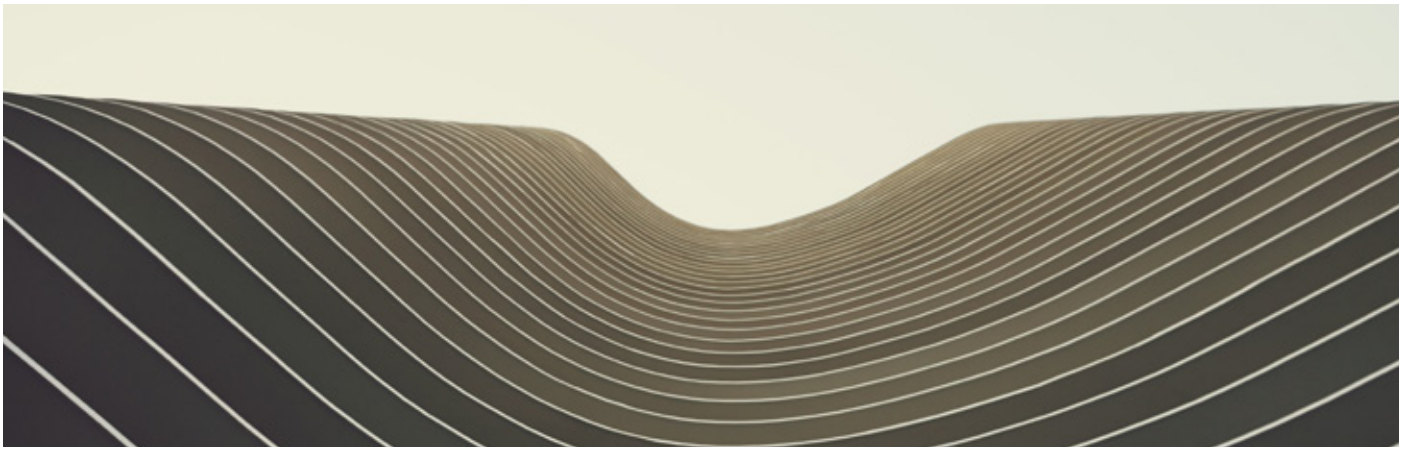
How do you make sure you know what new projects are on the road map and that security is baked in from the process side?

For every strategy, there are objectives that need to be implemented. These objectives are divided into short, medium and long-term timelines. Objectives are then achieved through initiatives, which are essentially programmes and projects. The successful implementation of these initiatives inches us closer to achieving a vision.

A security leader must therefore be part of the strategy process. By virtue of being part of the strategy process, one has access to the programmes and projects set out on the road map. Further to having access, a security leader can contribute towards the formulation of the strategy, the objectives and the details of the new projects.

The security leader must further understand the current situation and relate this to how new projects will be slotted into the working environment.





This requires a deep and thorough understanding through a gap analysis process.

During strategy reviews, the security leader must be part of the process to ensure there is clear alignment of all endeavours. Where projects are being reworked, first-hand knowledge and input will be critical.

Throughout this whole process, the security leader must ensure they are making all relevant stakeholders understand the importance of security from the outset and detailing how it will fit into the overall big picture.

The security leader must also be part of the team that translates and defines the strategic projects to tactical projects to ensure that all requirements are factored in.

In summary, a security leader must be part of the strategy process for them to know about the new projects on the road map.

How important is information sharing within the sector to keep abreast of new threats and cyber security best practices?

Personally, I think information sharing is extremely important. So long as there are boundaries in terms of managing what is sensitive and at what level such sensitive information can be accessed and shared.

We live in an interconnected information age where systems are integrated, and information is shared almost everywhere possible or permissible. Because of this interconnectedness and the sharing of information, cyber threats may transition from one environment to another.

It therefore becomes important to set agreed security standards in how threats can be dealt with.

We recently integrated with third parties to process real-time transactions. During the kick-off meetings, questions were asked on the type of security technologies used, standards of security, use of audit trails, incident response, potential risks, threats and vulnerabilities etc...All these were necessary to ensure both parties charter a common understanding.

ICT experts within the country were invited by the ICT regulator to deliberate on the draft electronic transactions and cyber security regulations act. This follows an earlier deliberation on the data and information regulations act. The expectation is that these documents get passed into parliament, so they are enacted as law. During these deliberations, experts shared information from various industries as they contributed to the draft documents. The representation from different industries clearly highlighted that security must be a joint effort because of the interconnectedness of our systems and interdependence we have from the information shared.

In summary, information sharing should ideally go beyond sectors. A cell phone today can access services from different sectors, a sign that we are all in this together to ensure cyber security best practices are coherently developed and agreed upon. And this can only be achieved if information is adequately shared.

Closing statement

Today there is an overdependence on the use of technology. One way or another, we all want to access a certain service online and this has become the new norm. The cyber space is predominantly our playground. Unfortunately, in every playground, we tend to get those who are bullies and those who are up to no good.

As we cannot do without technology, we need to find continuous ways to make it safe, make it more efficient, make it more accessible. The very fact that we continually integrate and share information tends to raise more security concerns. The case of continuous integration is driven by the need users have of wanting everything at their fingertips.

Security leaders MUST therefore be agile and strategic enough to plan and implement solutions and aim to mitigate risks.

Today we have ML AND AI, which allows automated ways of analysing and responding to cyber threats. The security professional today should have this ability wired into their skillset if they are to stay on top of things.

Insight

LUPOVIS

How Cyber Deception helps CISOs meet their cyber security goals

LUPOVIS

How Cyber Deception helps CISOs meet their cyber security goals

Author: Lupovis

At a glance

- 5 minute read
- What is Cyber Deception
- CISOs' challenges
- How can Cyber Deception help CISOs?
- Deceptive assets
- Events and alerts
- Leading on with breadcrumbs and lures
- Conclusion

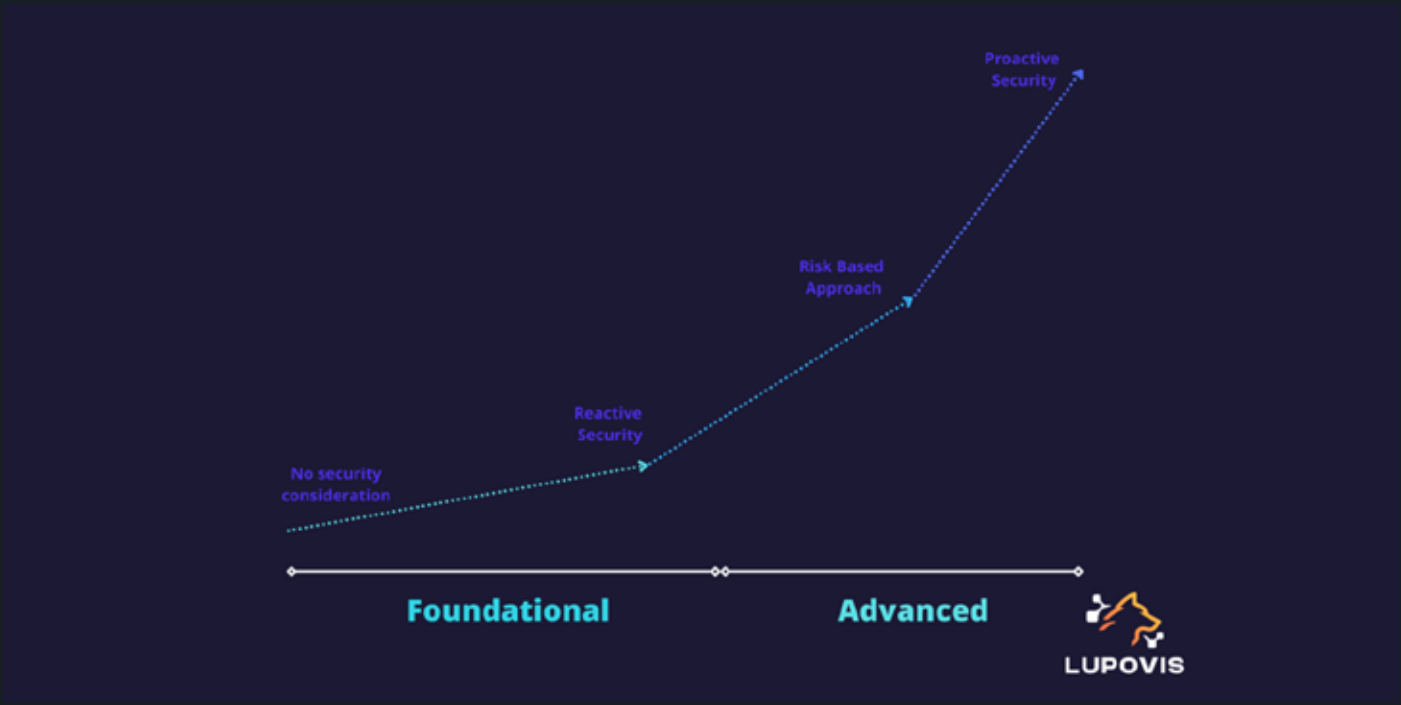
LUPOVIS

CISOs are under constant pressure to secure their organizations' data and systems from ever-evolving cyber threats. As the number and sophistication of attacks continue to grow, traditional security measures such as firewalls and antivirus software and even EDR are no longer enough. This is where cyber deception comes in.

What is Cyber Deception

Cyber Deception is a technique used to consistently trick an adversary during a cyber-attack. It works by deceiving adversaries with fabricated services and fictitious documents. Fabricated services are called Honeypots. They deliberately imitate services such as SSH, FTP, RDP, to create uncertainty and confusion in the adversary's mind. The aim is to influence the adversary as early as possible and turn the tables in favor of the defender.

The use of cyber deception to strengthen cybersecurity defenses is relatively new. Cyber deception involves fooling attackers into thinking they have succeeded in breaching a network, when in reality they have only accessed a monitored environment, allowing CISOs to identify and deflect the attackers. By doing so, CISOs, and SOC teams can buy themselves valuable time to detect and respond to the attack. In addition, cyber deception can provide valuable contextual threat intelligence about adversaries' tactics, techniques, and procedures. This information can be used to improve the organization's overall security posture. As the benefits of cyber deception become more widely known, CISOs are increasingly turning to this proactive security measure to help protect their organizations from harm.



CISOs' challenges

One of the biggest challenges faced by CISOs is managing the increasing complexity of IT security. CISOs need to have a deep understanding of a wide range of technologies in order to secure enterprise networks and technology stacks.

This comes with challenges such as:

- The inability to detect a breach in the network early
- Understand the attack surface
- Detect insider threats in a timely manner

In addition, CISOs need to be able to effectively communicate with both technical and non-technical stakeholders about the risks posed by new technologies and the steps that need to be taken to mitigate those risks.

This comes with challenges such as:

- Obtain funding the for the SOC and CTI teams
- Increase the cyber security maturity of the organization
- Avoid technical challenges

With the COVID-19 pandemic and the uptake in remote work, CISOs have faced challenges is managing security in an increasingly remote world. With more employees working remotely, CISOs needed to find new ways to secure enterprise data and systems without restricting employee productivity.

- This came with its own challenges:
- Reduce false positives generated by the current technology stack in place
- Miss key alerts
- Meet regulatory demands for breach detection and investigation

Finally, CISOs need to have a good overview of the threats their organization is facing.

- Detect threats with valid credentials / insider threats
- Detect APT and zero-day threats

These challenges, alone, make the job for CISO extremely complex, and these challenges are then deferred to their SOC team and threat intelligence teams.

Every action will impacting the entire organization.

To summarize the main pain points of CISOs are:

- The inability to detect a breach in the network early
- Understand the attack surface
- Detect insider threats
- Reduce false positives generated by the current technology stack in place
- Avoid missing key alerts
- Reduce Mean Time to Detect
- Reduce Mean Time to Respond
- Meet regulatory demands for breach detection and investigation
- Detect APT and zero-day threats
- Reduce alert fatigue
- Reduce SOC personnel turn over

Each of these pain points can increase the risk of a successful data breach, costing the organization millions of dollars in damages.

It is key for the leadership team to define a cohesive strategy to manage risk appropriately and proactively.

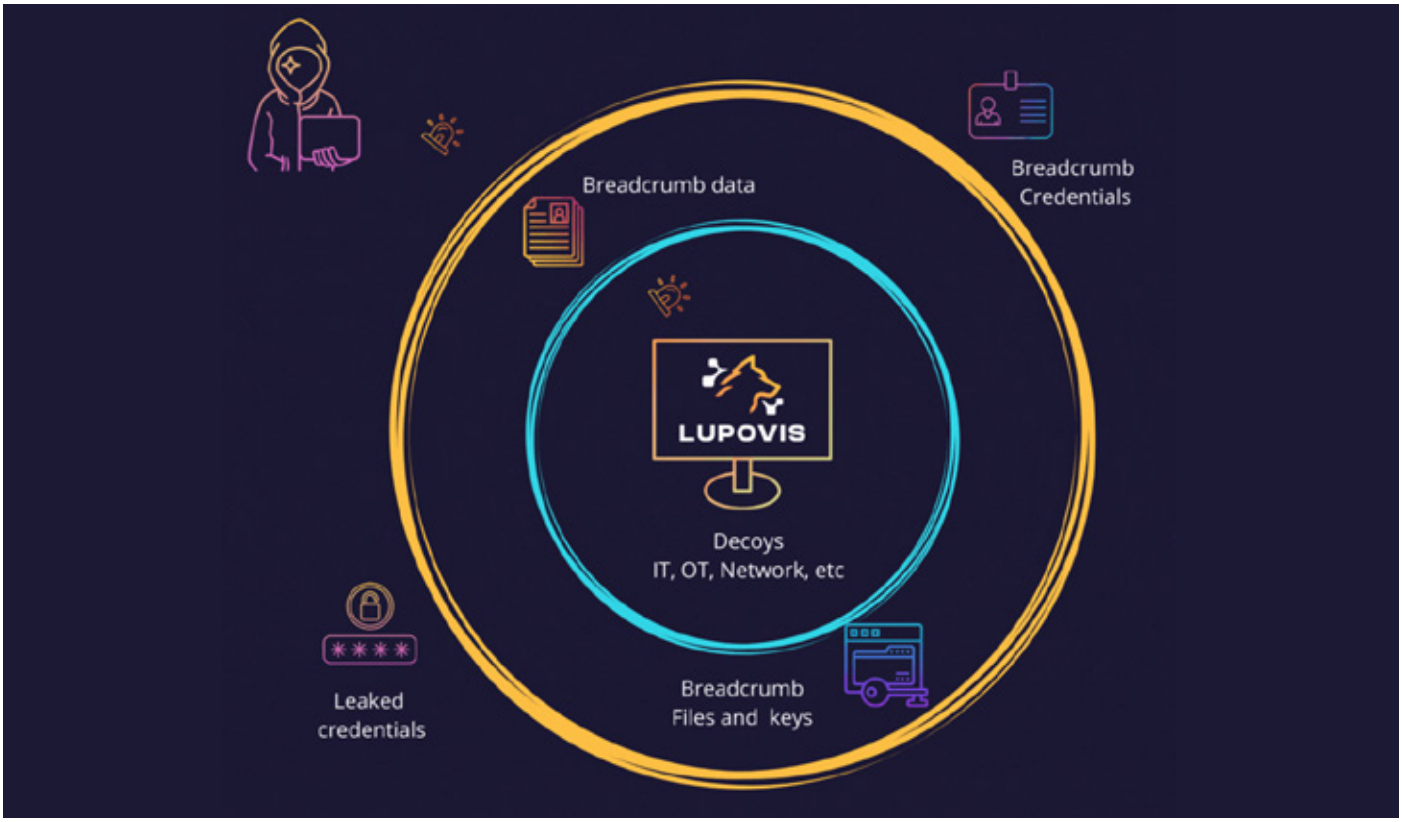
How can Cyber Deception help CISOs?

As the use of cyber deception technologies continues to grow, it is important for CISOs to become familiar with the different cyber deception products. While all vendors offer some basic features, there are significant differences in terms of functionality, price, and deployment model. As a result, it is important to choose a vendor that best meets the needs of your organization. One vendor may offer a better price, but another may offer more features. It is also important to consider the deployment model, as some vendors offer on-premise solutions while others offer cloud-based solutions. By taking the time to learn about the different vendors and their products, CISOs can ensure that they choose the right solution for their organization.

Deceptive Assets

The deception platform must have a wide range of deceptive assets and provide excellent telemetry. This telemetry is essential for obtaining contextual information on the attacker. Without this information, it can be difficult to accurately identify the source of an attack. Additionally, the platform must be able to rapidly deploy new assets in response to changes in attacker tactics.

This agility is essential for keeping ahead of the attacker and protecting the network. By carefully designing the deception platform and selecting the right assets, it is possible to obtain the information needed to identify attackers and protect networks.



Deceptive assets deployed outside of the network will also lead to contextual threat intelligence. Unlike threat feeds that are often too broad, deception assets mimic authentic assets within the organization, leading to a threat that is directly actionable by the team.

Events and Alerts

In the world of security, false positives are a major issue. A false positive is when an event is incorrectly flagged as suspicious when it is actually benign.

This can cause a lot of wasted time and resources as SOC teams frantically try to track down a non-existent threat.

Analysts also often suffer from "alert fatigue" due to the high volume of false positives generated by security tools that are triggered unnecessarily, wasting the analysts' time and energy. In some cases, false positives can even lead to burnout.

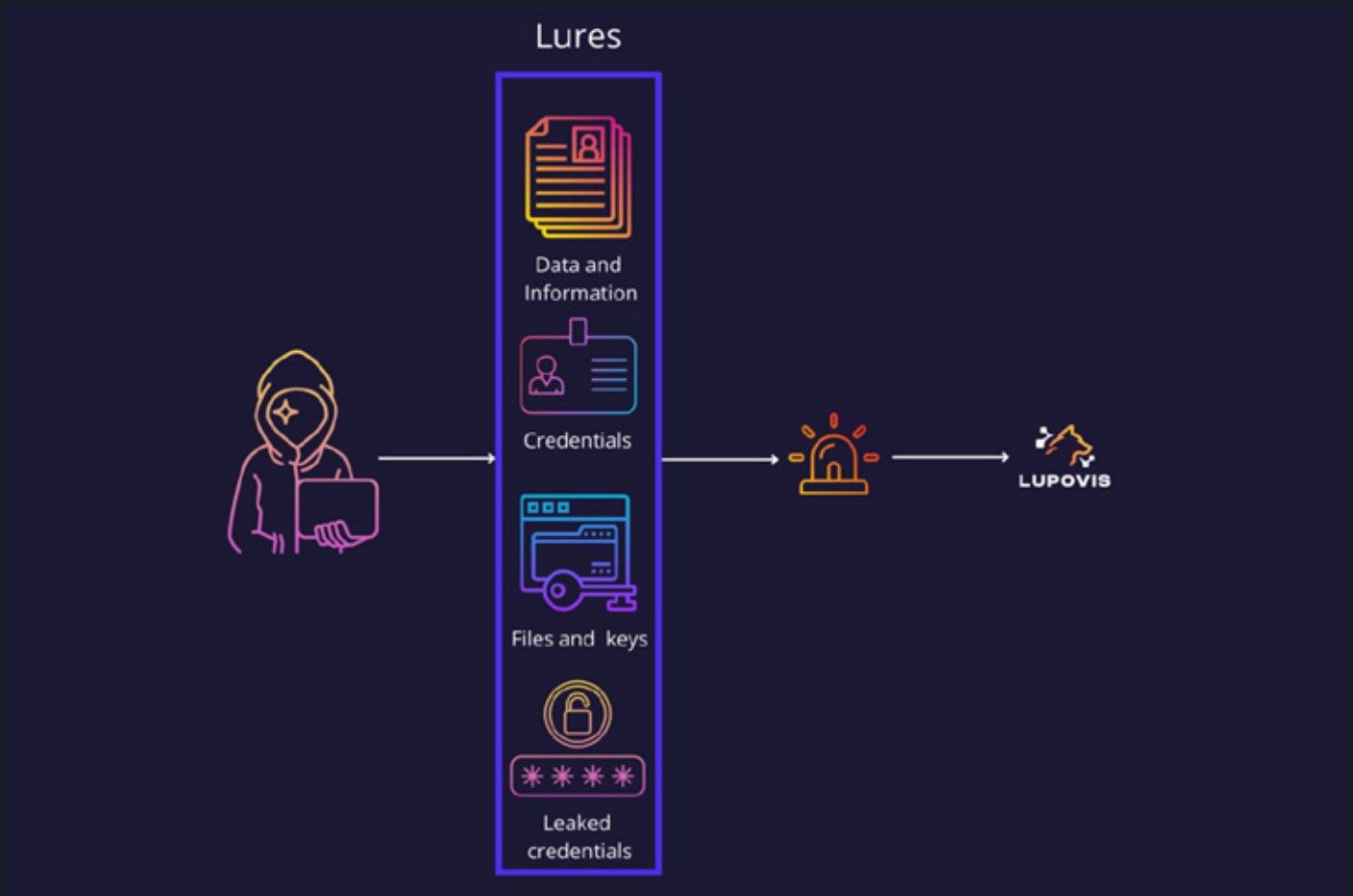
Deception assets must be designed to produce zero false positives; therefore, the event alerting must be concise, clear and feature-rich. By eliminating false positives, SOC teams can be confident that they are only looking at real threats, which will save a lot of time and effort in the long run.

Leading on with Breadcrumbs and Lures

A cyber deception breadcrumb is a small piece of information left behind for an adversary to use and trigger an alert.

Deception breadcrumbs can be placed by security teams inside and outside the network in order to bait attackers to reveal themselves.

By following the breadcrumbs, attackers unwittingly expose themselves and their methods, leading to high alert fidelity.



By using breadcrumbs, organizations can detect adversaries early and take action to mitigate the threat. Breadcrumbs can also be used to track activity and uncover patterns.

They can be left behind by SOC teams and can be used to detect changes in behavior or unusual activity.

By monitoring breadcrumbs, organizations can detect malicious activity early. This will lead to reduced MTTD and MTTR, improving the overall operations.

Breadcrumbs also have the potential to distract and mislead attackers, making it more difficult for them to succeed.

Conclusion

Cyber Deception is a powerful tool for CISOs looking to solve a variety of regulatory challenges, increase visibility in their network, and reduce the number of false positives their SOC team is facing.

When an attacker takes the bait, they are revealed and can be stopped before causing any damage.

Deception has become an increasingly popular solution for CISOs as it offers a number of advantages and is an incredibly effective way to comply with a variety of regulations, such as GDPR and HIPAA.

Ultimately, cyber deception can help to reduce the probability of a data breach, regardless of the source and in turn reputational damage.

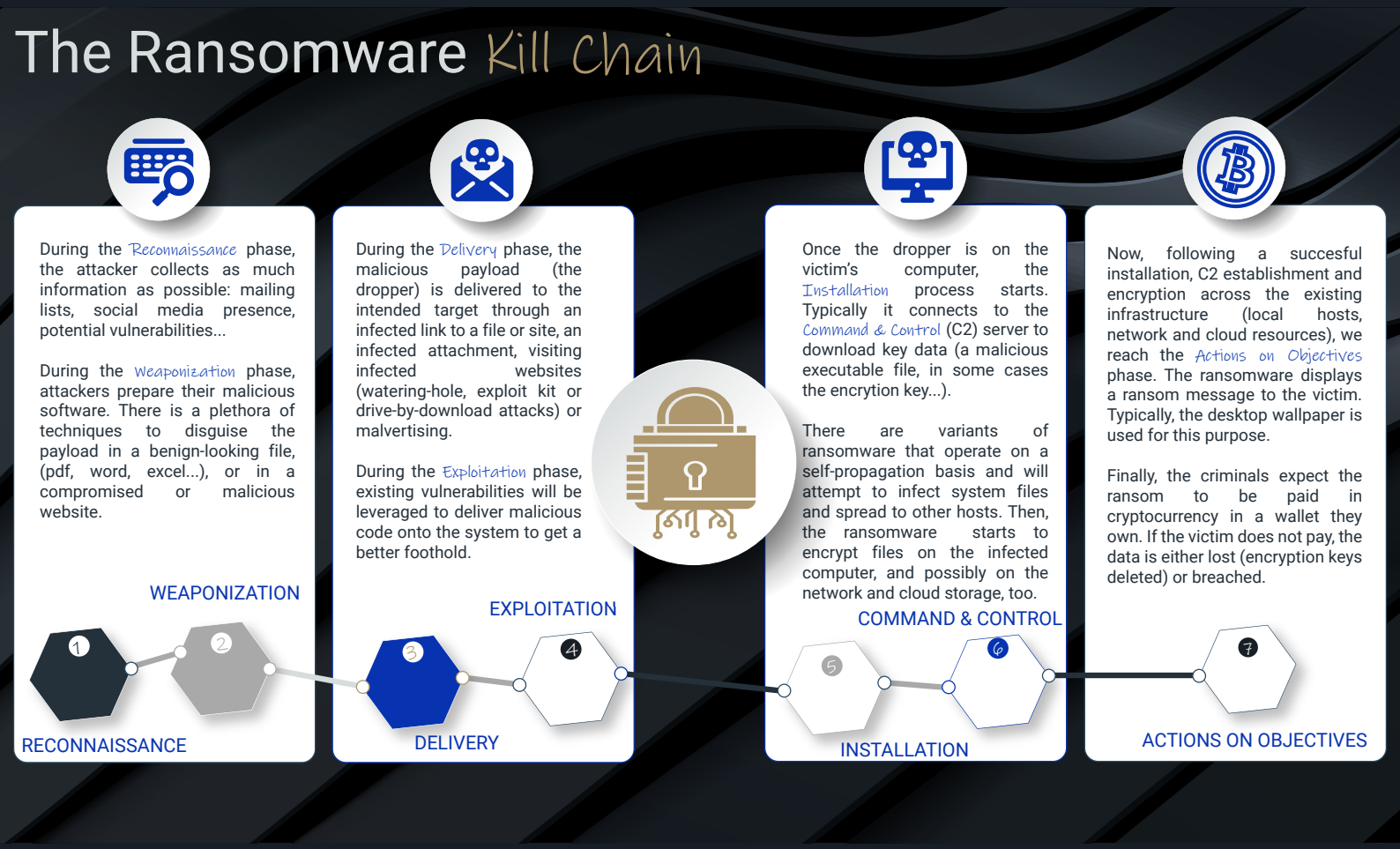
For CISOs, this is a vital consideration, as any data breach can have serious consequences for an organization. As such, the use of a deception platform should be considered as part of any comprehensive data security strategy.

Resources

Infographic

The ransomware kill chain

The ransomware kill chain



Available for download in Press Quality

Infographics - Threats & Attacks

Cyber Startup Observatory - Community

Nuno Marques

CIO @ Banco BIR

Nuno Marques

CIO at Banco BIR

Nuno Marques is the CIO of Banco BIR and has almost 20 years of experience in the operation and management of technological projects in the banking area.

He holds an MBA in Business Management and a Masters in Corporate Compliance and is transitioning to CISO certification focusing on security and data protection processes, having recently completed the DPO.

Nuno has led multiple projects in implementing, managing, and migration for: security solutions, Data Centres, disaster recovery, business continuity and digital platforms on four banks and one insurance company. He puts the success of these projects down to the fact that he had excellent teams to achieve these goals.

What is your overall approach to information security?

About two years ago, the world completely changed its information management paradigm. In previous years and as a result of weaknesses, like the massive leak of classified information from governments, multinationals, and all kinds of organizations, we were struggling with security issues.

However, this situation has gone from a scale of high importance to becoming the focus of all institutions. One thing is certain, the world will not be the same as before 2019 and the deficient concern with information security will dictate the future of organizations!

> "The deficient concern with information security will dictate the future of organizations!"

Therefore, the engagement on this matter must be general and transversal to all organization areas.

I see continuous training in matters related to information and cyber security as the core for each organization, to keep employees aware and prepared to manage the challenges, on storing and disposing the information available to them. Currently, any miscalculated step can cause untold financial or reputational losses.

How can security executives get that "buy-in" from the top?

Information security, from my point of view, has become a commodity, a product of excellence that should be disseminated by institutions that seek the security and privacy of their customers on a daily basis.

CEOs who do not follow this trend will see their institutions lose market, because in an environment of all the insecurity we live with today and, especially, in the case of banking services, it's not only the financial gains that attract customers, but the online services' availability and secure use of these services, without risking the data or financial transactions exposure. In my case, the approach has been to highlight all the work around information security as a way of elevating my institution in the financial market.

How do you assess the responsibility of the CISO for educating the workforce?

Being responsible for the three pillars of information security and for the standards implementation aimed at global security in the organization, the CISO/Leader is the first entity to understand the risks and dangers of poor information management.

It's his responsibility to provide teaching content transversal to the organization, through lectures, cases and practical situations or random knowledge tests, to understand the level of perception and employees' alertness to topics related to information security. Only then will it be possible to understand how collaborators interpret themes such as network intrusions, accidental information disclosure, viruses, spam, spyware, or phishing.

Knowledge and dissemination, when well aligned, bring high reputation results for the organization, equally translated into financial return.

Education in this case should be seen as an immediate and direct investment in the organization's results.

The biggest threat to your institution is already inside the building. Studies show that 60 percent of cyber-attacks come from inside the company. What are the key strategies to address this challenge?

Training employees on security issues must be the first strategy!

We can implement all security systems, internal solutions, limitations, and processes for segmented information access;

we can even implement ISO27001 by the book, but if we don't have the employee's commitment, there's no organization that can resist the security challenges.

Effective research, evaluation and implementation of solutions, processes, and alerts by the security teams in order to mitigate or minimize the security risk should be a parallel step.

Another step is to address the security risks that users who hold the potential for greatest damage represent, and the critical assets they access. So, we should monitor IT admins, top executives, supporting partners, and at-risk employees.

Why do some CISOS use technology for its 'cool' factor instead of for securing or enabling the business?

To attract Generation Z employees and customers in general, leaders have sought to invest in apps and gadgets that are cognitive and flashier. Unfortunately, they forget that these solutions aren't always compatible with the security issues and can weaken organizations. Nevertheless, most of the time it goes this way, and then becomes a subject for the security teams to deal with.

The security solutions in some cases suffer from the same condition, there's a variety of security system on offer, with beautiful aesthetics and lot of dashboards, but after checking the facts and on daily basis, they don't always meet the needs for which they were initially intended.

That's why it's so important to make the proper procurement, considering the real security intentions, even if that means investing in a tailor-made solution.

Personally, it has been this path that I have taken and mainly because having access to the business vision discussed by the board of directors, it's easier to define the best strategies to adopt.

How important is information sharing within the sector to keep abreast of new threats and cyber security best practices?

Knowledge is one of the most important resources we have, and experience is undeniably an asset today! Metrics and standards are just guidelines, we must think that threats with which we are confronted are changeable and quite creative.

Cybersecurity threats evolve at a frenetic pace, so the possibility of being aware of continuous improvements as well as attacks that have occurred, can be dealt proactively through sharing knowledge and experiences.

Promoting information sharing within the same sector and at the level of cyber security improves threat intelligence, as well as coordination of incident response and better prevention of cyber-attacks.

It's through the challenges overcome, in my specific case, by the banking sector and sharing information about the problems we faced, that others prepare themselves for the probability of non-occurrences in their organization.

Closing statement

Due to the limitations we live within, cyber security has become the trend topic for debate evaluation and study.

For organizations' business continuity, boards of directors will have to rethink their strategies and adapt their products and services to a market that is less and less present, focused on convenience and quick responses. However, it's only through knowledge and general engagement of employees that it will be possible to reach levels of security and information protection that no system, norm, procedure, or rule by itself will allow us to do.

We must also be aware that sharing knowledge and experiences will help us to be closer to reality at every step of management.

Insight

Jose Monteagudo

Cyber Resilience and our proven inability to stop cyber attacks

Cyber Resilience and our proven inability to stop cyber attacks

Author: Jose Monteagudo, Editor-in-Chief, Cyber Startup Observatory and CEO at Cyber Innovation Summits

At a glance

- 5 minute read
- Where is the industry now?
- Understanding the levels of Health IT
- Security, confidentiality and privacy
- Major threats for the industry

Barely a week goes by without a ground-breaking story of how another major organisation has been attacked by cyber criminals, breaking previous records in terms of both severity and amount of data breached.

Whether millions of IDs were stolen, or personal data compromised, it's clear that no business, irrespective of the money they throw at security solutions, is safe.

Cyber-resilience - Definitions

Due to the complexity of the topic, in particular when applied to sectors or nations, it's important to start with some definitions.

The **National Institute of Standards and Technology (NIST)** defines cyber-resilience as: the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enable by cyber resources. Cyber resilience is intimately related to other disciplines:

- Information Security and Privacy, which is basically the organization's ability to safe-guard data from unauthorized access or modification while ensuring availability, confidentiality and integrity.
- Business Continuity: ensuring that an organization will have the capability to operate its critical business functions during emergency events.
- Organizational resilience: the capability of an organization to anticipate, respond and adapt to incremental change and sudden disruption in order to survive and prosper.
- Fault Tolerance: the property that enables a system to continue operating properly in the event of the failure.
- Reliability: the quality of being trustworthy and performing consistently well.
- Safety: the condition of being protected from or unlikely to cause danger, risk, or injury.

- **Resilience and Survivability:** in engineering, survivability is the quantified ability of a system, subsystem, equipment, process, or procedure to continue to function during and after a natural or man-made disturbance.

The concept of cyber-resilience not only covers IT systems, but also critical infrastructure, societies, business processes, organizations and nation-states.

According to NIST, a key fundamental assumption of cyber- is the fact that a sophisticated adversary cannot always be kept out of a system or be quickly detected and removed from that system, regardless of the quality of the design, functional effectiveness of the security components and trustworthiness of the selected components.

Additionally, the NIST continues that cyber-resiliency assumes that the adversary presence in the system may be a persistent and long-term issue and recognize that the stealthy nature of the APT makes it difficult for an organization to be certain that the threat has been eradicated.

It also recognized that the ability of the APT to adapt implies that mitigations that were previously successful may no longer be effective.

What are the existing frameworks?

There are multiple frameworks purposely designed for different entities, sectors or environments, such as critical infrastructure, territorial governments, engineering systems and CERTs. Some of these frameworks are listed below:

1. Department of Homeland Security (DHS) – Cyber Resilience Review (CRR): a voluntary examination of operational resilience and cyber security practices offered at no cost by DHS to the operators of critical infrastructure and state, local, tribal and territorial governments. The CRR is offered in a facilitated workshop format and as a self-assessment package.

2. The National Institute of Standards and Technology (NIST) offers a framework for engineering secure and reliable systems-treating adverse cyber events as both resiliency and security issues (NIST Special Publication 800-160-Volume 2).

3. MITRE has developed its cyber resilience engineering framework (CREF) to support the development of structured and consistent cyber resiliency guidance.

4. Cyber Resilience Evaluation Method and the CERT® Resilience Management Model (CERT-RMM).

How do we measure cyber-resilience?

Considering the previous assumption that independently of the measures taken we might not be able to prevent an entity being breached, it is absolutely crucial to assure that we are able to measure its cyber resilience and to guarantee that it is appropriate and kept appropriate in a quickly changing threat landscape.

We need to define the different scopes and the metrics applicable for each one:

- Systems and Missions: metrics would be related to either how well the system or mission handles disruption or to their architectural properties.

- Organizations: metrics are sought in the contexts of cybersecurity, contingency planning and overall risk management.

- Sectors: metrics can be defined using a framework based on risk metrics, relying on a resilience analysis process.

- Nations and transnational entities: this is very complex due to interdependencies among organizations, systems, and critical infrastructures, as well as significant differences between preparedness and response for different types of disruptions and consequent present major challenges to resilience assessment for regions or communities.

This article is designed for general guidance and the definition of specific metrics will require a detailed analysis which might in some cases become very complex, particularly for sectors, nations and transnational entities.

Ways to improve cyber-resilience

As recent global cyber-attacks have demonstrated, it is crucial for our increasingly interconnected society to strengthen its cyber security and resilience.

There are different approaches to improve cyber-resilience. Among them:

- Build a strong foundation: Identify high-value assets and harden them (customer data, IP rights, personal information of staff, etc). Prioritize legacy systems and prepare for the worst.

- Implement a strong risk management practice: be cognizant of the new threats associated with new technologies like IoT-IIoT, Cloud, mobility and adjust your cyber posture to these new threats.

- Address the People risk by properly educating your staff and by putting procedures and policies in place to ensure that all angles are covered in the event of an incident.

- Pressure test resilience like an attacker. Enhance both red attack and blue defense teams with player-coaches that use threat intelligence and communicate closely to provide analysis on where improvements need to be made.

- Employ breakthrough technologies. Automate defenses. Use automated orchestration capabilities and advanced behavioral analytics.

- Be proactive and use threat hunting. Develop strategic and tactical threat intelligence. Monitor for anomalous and suspicious activity.

- Implement a good crisis management strategy

- Evolve the role of CISO. Progress the next-generation CISO—business adept and tech-savvy.

Conclusions

Let's not forget the key fundamental assumption that in today's world, a sophisticated adversary cannot always be kept out of your organization or be quickly detected and removed.

Moreover, it is very important to understand that cyber-resiliency cannot be achieved without planning and resources.

Finally, leadership, governance and accountability are absolutely crucial ingredients.

References

1. Building Cyber Resilient Systems, MITRE

2. Cyber Resilience Metrics: Key Observations, MITRE

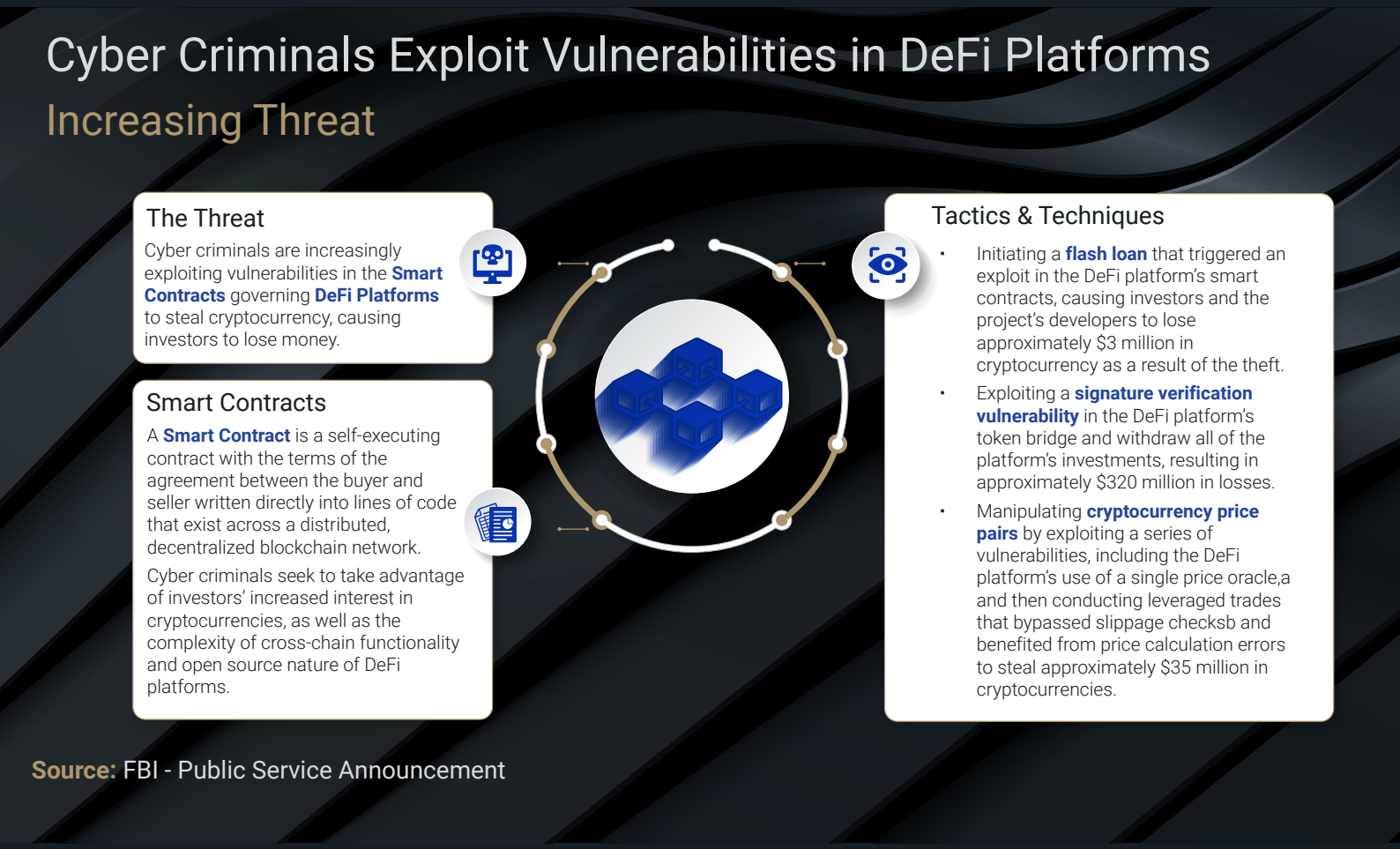
Resources

Infographic

Cyber criminals exploit vulnerabilities in DeFi platforms

Cyber criminals exploit vulnerabilities in DeFi platforms

Increasing Threat



Available for download in Press Quality

Infographics - Financial Services

Cyber Startup Observatory - Community

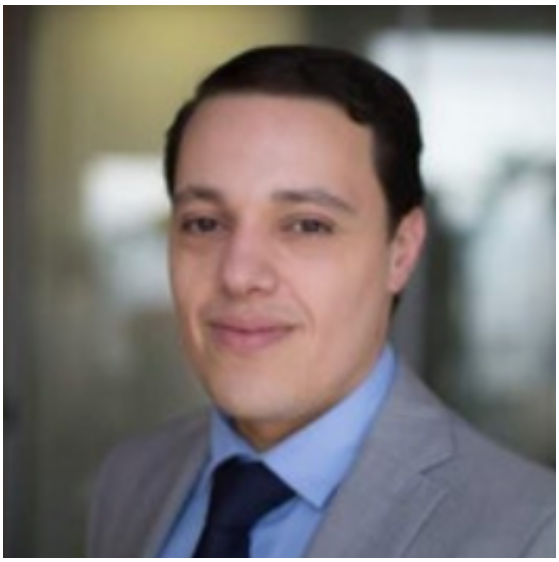
Ilyass Ankouz

Global Head of Cyber Security @ OCP S.A

Ilyass Ankouz

Global Head of Cyber Security at OCP S.A

Ilyass ANKOUZ is a passionate Cyber Security, Business Resilience and GRC professional with over 12 years of experience on both sides of the aisle - consumer and consulting side - developing, managing and delivering large scale multi-country, cross-regulatory programs across Europe, Asia Pacific and Africa.



Ilyass ANKOUZ is a graduate engineer from the "ENSEEIHT - INP Toulouse" engineering school, specialising in Information Systems Security, and holds a master's degree from the "CentraleSupélec" school in program management complemented with several certifications in Information Security & Digital Transformation.

He joined OCP Group in 2019 as Head of Cyber Security to define & develop the group's cyber resilience program.

The CISO role is very high pressure, high stakes job, what is the right profile for this job?

As Stéphane Nappo stated: "It takes 20 years to build a reputation and a few minutes of a cyber incident to ruin it".

What makes CISO's mission difficult is to understand and remain up to date about strategic decisions and operations within the organization.

This "Must Know" need, coupled with the sophistication of cyber threats and the severe damage they can inflict on an organisation makes CISO's role very high pressure and high stake to safeguard the organization's assets.

> "What makes CISO's mission difficult is to understand and remain up to date about strategic decisions and operations within the organization."

Before the digital edge, the CISO role required strong operational security skills to succeed in the mission, leveraging strong and air gapped defence toward the external world. The operational impacts of cyber attacks were also limited, as new technologies were not use in the core operations of the organization.

With the advent of new technologies in the organisation, the CISO role has evolved rapidly to play a direct and active part in the board's business strategy. CISOs are now key players in the business transformation, involved in wide range of committees such as Enterprise Risk, Regulatory & Compliance, and Human Resources Training Programs.

To succeed in their mission, CISOs need strategy and flexibility, passion and patience, hard work and confidence. In my view, these elements are as important as technical and communication skills. I have known several highly skilled and experimented security leaders that could not succeed in their CISO role, as they were missing some of these abilities.

The Human Resources Learning Department should add Coaching programs to CISO's training to enable them to fulfil their role.

How can you convey to the board the message that with regards to cybersecurity – you can minimize the risk but you ae never going to be 100 percent secure?

It is not unusual to hear board members stating that cyber security is a technical issue that CISOs are expected to address with technologies and security experts.

CISOs have to remember that Board members take wild range of risks continuously as part of their decision-making process. Zero tolerance toward cyber risk is a clear sign that board members do not understand those cyber risks.

Therefore, CISOs need to translate the cyber risks into enterprise risks and incorporate them into the enterprise risks map.

With this illustration, board members can compare cyber risks to other enterprise risks like financial risks and understand that zero tolerance toward cyber risk is not compatible with the business goals.

Some materials CISOs may need to prepare ahead of this meeting with the board committee are:

1. Build a strategic cyber risks map of the organisation: CISOs are accustomed to elaborate technical and operational cyber threats maps to manage security operations. CISOs should adopt same approach and build strategic cyber risk maps for C-suite and board members.

2. Formalize your cyber risk appetite through your cyber risk appetite statement: in other words, you need to know how your stakeholders want you to balance cyber risks and business goals. To achieve this goal, you need to develop a formal risk appetite statement tailored to your business model, risk landscape and culture, defining when to "mitigate & accept" risks and when to "reject the risks".

3. Showcase cyberattacks: in the past, sophisticated and destructive cyberattacks have hit organizations from different sizes, industries and regions. CISOs should analyse these external threats to evaluate the potential damage for the organization and integrate it to the board's committees.

With this Cyber Risk toolbox, CISO-board meetings will tend toward enterprise risk – board meetings articulated around risk tolerance & risk appetite that board members master.

What advice do you have for security leaders?

It is common within organisations that security practitioners are seen, as technical experts that block business innovation and monitor employees' activities.

These clichés can delay the integration of cyber security into the culture of the organisation.

To eliminate these clichés, security leaders should adopt the following approach:

1. Enabler instead of blocker: Council near the businesses on cyber security related matters and act as business enabler

2. Leader instead of manager: close to operational teams, supporting them versus controlling them

Your business is only as strong as your weakest partner. Can you trust that your partners are keeping your data safe from attackers and how can we manage third party risk?

In recent years, we have seen major companies with a mature cyber security posture being hit by destructive cyberattacks via their supply chain of partners and service providers.

It is safe to say that the number of this type of attacks will continue to grow with the digital transformation of the organisations. In my view, CISOs must incorporate cyber security requirements in the company's Third Party Risk Management Framework deployed working together with the procurement & back office departments.

For companies with large ecosystems, implementing efficient Third Party Risk Management can be a challenge for the CISO and procurement teams. It is important to adopt a risk-based approach:

1. Start with the classification of the partners based on the sensitivity of the data they manipulate and the sensitivity of the business processes the partners are supporting.

2. Establish the frequency of Cyber risks assessments, based on the sensitivity of the provider.

3. Use adequate tooling to maintain third party risk management overtime; CISO & procurement teams should leverage existing cyber security risk scoring platforms to industrialize their processes.

CISOs following a zero trust cyber security strategy should consider third party as an asset which will simplify & standardize the cyber security risk management framework.

Digitalization is a double edges sword, offering incredible benefits but also entailing serious risks. What are your thoughts on this inevitable development?

Digitalization and technology risks are two faces of the same coin. In the past, technology risks were consistently within the top ten risks on the world economy due to the significant impact that cyber attacks have on organizations, from financial, reputational and operation perspectives.

Implementing a Technology Risk Management (TRM) Framework helps to keep under control the technology risks introduced by the adoption of disruptive innovation within the organisation.

For organisations with mature Technology Risk Management Frameworks, CISOs should engage with enterprise architecture and enterprise risk management teams to integrate cyber risks within the TRM processes.

If TRM is not in place, then CISOs need to drive the implementation of TRM committees as an additional control to handle cyber risks.

Why are some industries more open to sharing information than others?

Cyber attacks can severely damage the reputation of organisations with regards to their customers and their ecosystem of partners and authorities. Therefore, it is natural that organisations are not willing to communicate or share information with their peers and competition.

This is where regulatory agencies play an important role to establish trustworthy environments and sharing policies for the different actors to exchange cyber threat information in a safety manner.

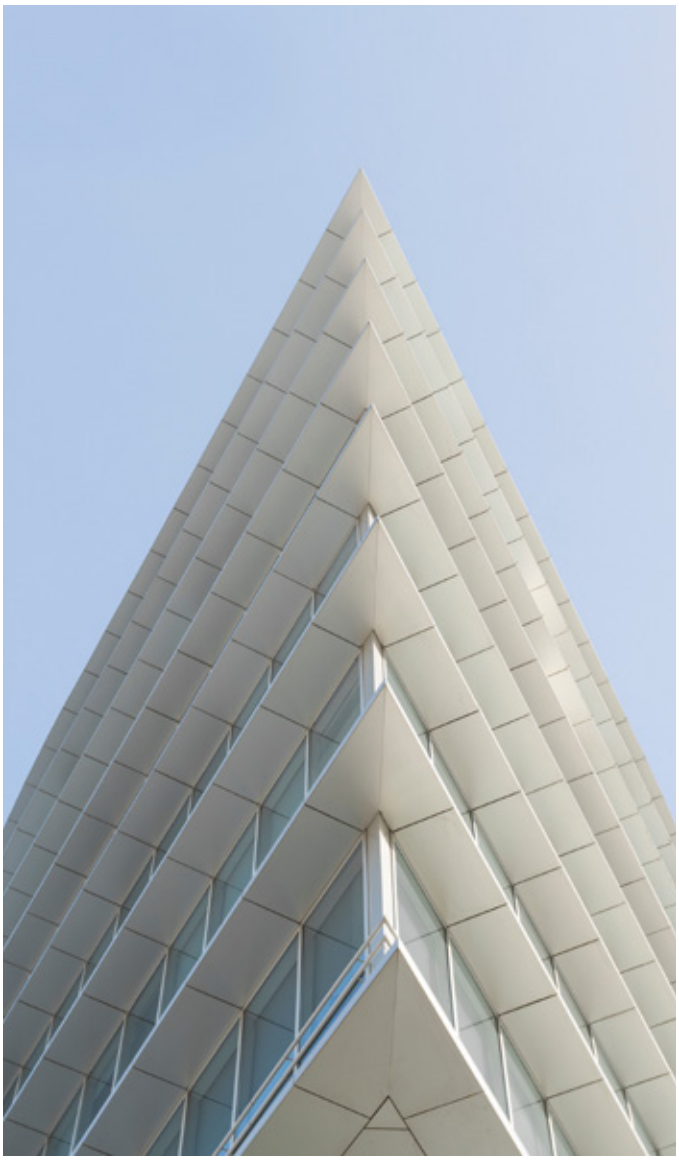
F&I sector is a model where regulators succeed to establish information sharing communities that prevented wild cyberattacks from spreading cross sector.

I believe that each industry should have its specific information-sharing framework aligned with its particularities and needs to be regulated by government authorities.

Closing statement

To keep pace with this fast evolving and sophisticated world, cyber security leaders need to define their cyber security vision with an honest view of their capabilities and a realistic risk-based strategy to achieve their goals.

CISOs should leverage every opportunity to explain their vision to all employees as every employee has its role to play in achieving cyber resilience. All connected, all concerned, all responsible.



Youssef Saidi

CISO / RSSI @
Société Générale Maroc

Youssef Saidi

RSSI / CISO at Société Générale Maroc

Youssef Saidi joined Société Générale in 2002 following a scientific education and an advanced academic training. He obtained a PhD (Doctorate) in Physical Science at the University Mohammed V in Rabat in 1999. The computer component was already present in his PhD work.

In 2001, he further strengthened his knowledge and skills and obtained an engineering degree in IT and Computer Science from the ORT (organization in France). He joined Société Générale to work on the Internet Access Point. In such a role, he observed the risks of the web and the damage cyberattacks can cause to businesses and customers.

He then got interested in the security of the internal systems and in 2006 started to work on the risk analysis of bank's projects. He has contributed to and supported all the bank's transformations since 2002.

In 2008, he became responsible for the IT security. In 2014 he was appointed deputy CISO (RSSI). Since 2018, he has had role of the bank's CISO and head of the Risk and Security department.

The job of CISO is never going to be an easy one. The bad guys only have to be right once. How do you deal with that seemingly impossible challenge?

Any security breach or incident has a significant impact on the image of the company and may result in substantial damage. The mission of the CISO is to anticipate, prepare and protect the company against any potential incident. The challenge is indeed difficult, but it is also motivating and rewarding.

> "The mission of the CISO is to anticipate, prepare and protect the company against any potential incident. The challenge is indeed difficult, but it is also motivating and rewarding."

The biggest challenge is that threats are in continuous evolution. Overcoming today's threats is not a guarantee against future ones. The digital transformation initiated by companies in recent years has increased the potential entry points for cybercriminals.

There is an increasing number of systems in the company, generating large amounts of data and information, and it has become very challenging to detect malicious activities among the large volume of information available.

It is therefore crucial to have a global strategy relying on the human element as well as the processes. Technologies used or developed are aimed to support this effort rather than being an end goal.

To succeed in his mission, the RSSI must:

- Put people at the center of the strategy. The human element is often the weakest link in a security process. Yet, colleagues remain the greatest asset against external threats. Having them central to the IT security strategy allows them to leverage their ability and intuition that no automated security tool can offer. Well trained collaborators remain alert to timely cascade up relevant information to allow targeted actions. When employees ignore or fail to identify suspicious activities and messages that the IT system displays for them this represents missed opportunities to timely identify, properly act and quickly adapt to security breaches.
- Remain up to date with the evolution of the field of cybersecurity and associated technologies. The most efficient way to fight cybercriminals is to remain well informed and to timely access to the latest developments.

For security executives who don't have a strong relationship with their board, how can they improve it?

Given the impact of cyber security on the activity of the company, the CISO-Board interaction has intensified a lot in recent years. This led to an evolution of the role of the CISO.

The latter is in contact with various stakeholders and therefore has to adapt the communication and translate technical matters into messages that can be used for decision making. In doing so, the CISO has to move away from the technical comfort zone to better understand the business, the interdependencies and the risks.

Building a good relationship with the board and streamlining communication and exchange is central to the success of the cybersecurity strategy in the company. On the one hand, it is essential that the CISO knows the expectations of the board, their questions and concerns.

On the other hand, the board should be guided to understand the risks, the strategy and the financial figures. It is therefore critical that a CISO speaks about cybersecurity in business terms and presents quantifiable metrics and measurable outputs.

In summary, for a fruitful collaboration with the board, it is key to:

- Have regular meetings for exchange and establish a process for the Security governance
- Fully understand the expectations
- Be transparent
- Provide an accurate assessment: what is the current status and where do we aim to be?
- Help target investments to areas where the risk is highest
- Limit the use of technical terms
- Be solution-driven
- Translate the investments in cybersecurity into tangible added value to the Business.

Each of these points could be the subject of a paragraph.

Some people call for daily security drills and exercises at all levels of an organization to help reinfornce defensive strategies. What is your take on this?

An important pillar of the cyber security strategy is a clear and efficient awareness program. To be successful, such a program must involve all employees regardless of their hierarchical position or job level.

Research indicates that the majority of security incidents were triggered by human errors generally due to either ignorance, naivety or negligence. Employees have become a prime target for cybercriminals to enter corporate networks and awareness campaigns are necessary.

However, for example, daily awareness campaigns can be counter-productive and are difficult to maintain in time. To achieve the desired outcome, the awareness program should be suitable in its style and content.

An awareness program is effective when it comes in a dynamic and interactive format, and when delivered using various means. Ideally, each format puts the emphasis on a specific issue. The program is most successful when spread over the entire year and when it targets all users. Dedicated sessions to target a specific audience are also recommended.

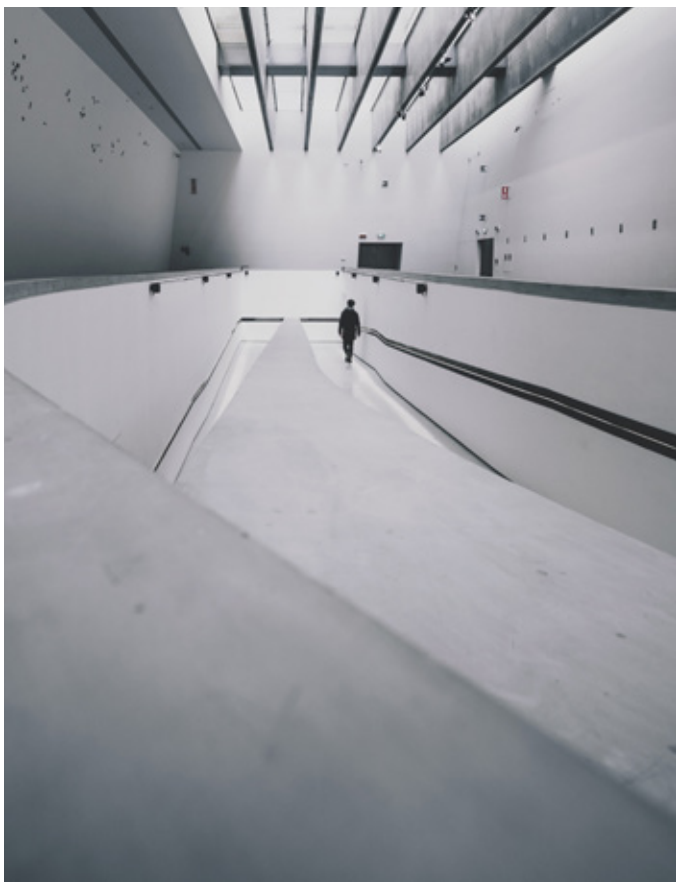
For example, employees of the HRD will not face the same risks as those of the IT team. Each functional entity must be aware of the value of the data and classification of the information it handles. It is therefore essential to support all employees and help them fully understand the risks associated with the data they handle.

Threats are everywhere and are always changing. How can we address this difficult reality?

First of all, one should be fully compliant and inflexible with the basics of security. For example, it is not sufficient to deploy a patch, it must be deployed on 100% of the available resources. It is not sufficient to have a good anti-virus, you need to have it on 100% of the assets. The security basics, if fully implemented, allow us to be protected from most threats.

Regarding the more sophisticated and evolving threats, these are often carried out by organized and highly motivated groups. To adequately face these threats, one must adopt the principle of "zero trust": double check everything and trust nothing. Put controls on the whole chain of connection; make the applications "self-resistant". We can summarize "zero trust" by the following:

- Ensure secure access to all resources regardless of their level of connection to a network (exposure via the Internet or internal network)
- Adopt the principle of least needed privilege
- Control (filter) the entire traffic



Recently, some solutions based on artificial intelligence and behavioral analysis have been developed to help to detect and fight more sophisticated cyberattacks. Despite showing some limitations, these new solutions hold a promising future in the fight against cyberattacks.

How do you predict the future of authentication?

The authentication means are continuously evolving. This is due to the evolution of the threats as well as the growing complexity of the IT environments.

In contrast to that, users request more flexibility and ask for user-friendly access and ease of use. They request secure access to their personal space but view complex authentication as a hurdle.

Today, access using password is dominant. This way of authentication is less used for sensitive or high privilege access. In my view, the access using password will remain the norm for some time yet, even if several experts announce that it will be abandoned.

Strong authentication (2FA), which has brought strength to the classical authentication, seems popular and has a bright future in the coming years. 2FA offers a good compromise between the user experience while ensuring a decent level of security. This method also shows certain limitations and was at the center of recent incidents of cyber fraud. Still, 2FA, remains an acceptable means to be protected against basic attacks.

The biometric authentication, existing for several years now, offers a fast and simple means of authentication. It was originally predicted to overtake the other methods, but its wide use was held back by several issues, mainly ethical considerations. Its further development and future use are therefore questioned.

A single (one-time) authentication (like a single door one can go through) is no longer sufficient to ensure a good level of access security. Ideally, the control of identity should remain continuous.

Recently, a new sort of behavioral authentication emerged as an alternative. It consists of a continuous control of many contextual elements of information which can inform on a person's true identity. Everyone is different and unique, which makes the way an individual carries out daily tasks also unique. It is therefore possible to define the behavioral imprint of a user.

It may consist of the usual connection times, the tools used, or documents/ resources accessed, the keyboard typing speed, the movement of the mouse, etc... Consequently, a malicious user entering the system will deviate from the usual behavior and rapidly trigger an alert.

Further development of machine learning and artificial intelligence science will certainly help such authentication to dominate the coming years. It is likely the future development anticipated for authentication to undergo.

How important is information sharing within the sector to keep abreast of new threats and cybersecurity best practices?

Timely information sharing and keeping up to date with the latest developments, security breaches and emerging threats is essential to adequately fight against cybercrime. Yet, even that information sharing can by itself create vulnerable spots and cause security risks.

One of the concerns is the risk of revealing companies' confidential information or sensitive data on their customers. This risk can be mitigated by implementing a standardized formal and secure process to allow the community to exchange while preventing malicious access.

This open exchange between companies is unfortunately not yet fully leveraged. Various professionals are still trying to find the right and safe balance between information sharing and confidential data protection.

Companies have a legal obligation to report incidents to the authorities. Yet, this remains a limited bilateral process and does not benefit the whole community.

It is evident that more effort would be needed to improve on this aspect.

Closing statement

The field of cybersecurity, as well as our profession, evolves rapidly. The cybersecurity strategy should be continuously reviewed to be able to keep up with and follow any developments.

It will therefore be essential to adapt and rapidly react to emerging priorities in order to balance risk management and business performance.

Airbus Cybersecurity

European specialist in cyber security

AIRBUS
CYBERSECURITY

01

AIRBUS CYBERSECURITY

Company Description

Airbus CyberSecurity is a European specialist in cyber security. Our mission is to protect governments, militaries, critical national infrastructure (CNI) and enterprise from cyber threats, in full compliance with the cyber protection measures required by national institutions.

We are a fully owned subsidiary of Airbus Defence and Space, with over 900 cyber professionals based across offices in Europe, including Security Operations Centres (SOCs) in France, Germany, the UK and Spain. Our main offices are located in Paris, Munich and Newport; however we also have several other offices in our home countries. Additionally, our organisation includes Stormshield, a France-based subsidiary which offers security products to enterprise and government clients.

With over 30 years of experience providing reliable cyber security products and services, we have become one of the most advanced sovereign cyber security players in Europe. Having protected Airbus Defence and Space's complex systems and networks with our SOCs for years, we have leveraged our Airbus DNA to develop products and services for customers facing similar challenges as us, based on state-of-the-art trusted technologies.

We provide a global cyber defence approach that dynamically protects, detects and responds to cyber threats with a portfolio that includes managed security services, design and integration solutions, industrial control system offerings, encryption, key management and consultancy services.

02

Company Information

Company Name: Airbus
Founded: 2011-1
Employees: 500 up to 1000
Web: airbus-cyber-security.com
Headquarters: France
Other Offices: Germany, UK, Spain

Key Target Verticals:

- CNI (in France, Opérateurs d'Importance Vitale)
- Transport
- Manufacturing
- Defence
- Public institutions

03

AIRBUS CYBERSECURITY

The Product

Product Category: Cyber Range, Detection & Prevention; SOC

Product Stage: Released

Product Names and Brief Description:

- Cyber Range: Training and simulation platform

Services Provided:

- Cyber threat intelligence
- Network security
- Cyber resillience

04

Product in detail: CyberRange

The Airbus CyberSecurity CyberRange is an advanced simulation solution that allows customers to easily model IT/OT systems composed of tens or hundreds of machines and to simulate realistic scenarios including real cyber attacks.

It is used by administrators, integrators, testers, trainers and more to design virtualised or hybrid networks, emulate unit activities such as communications between two machines or to launch complex scenarios reproducing a realistic activity (file exchange, email, web traffic and potentially real cyber attacks).

The main functionalities of our CyberRange are:

- Modelling of real or representative systems
- Simplified construction from the graphical interface (drag-and-drop of machines)
- Management of multiple and isolated workspaces
- Collaborative modelling and integration work
- Integration of equipment or real systems
- Live traffic generator
- Scenario engine
- Import and/or export capacity of machines or topologies
- Access to the screen offset or command line at each machine
- Management of the virtual machine park

The CyberRange is available in a mobile box, in a bay or accessible from our cloud.

AIRBUS CYBERSECURITY

How does it work?

The CyberRange is a unified technical platform on which teams can work together or share elements–such as machine models or scenarios. In order to meet the constraints of a complex environment, the platform is open to interface with external equipment such as a physical industrial control system, a hardware traffic generator or a real physical or virtual system.

There are endless use cases for the highly realistic environment recreated on our CyberRange:

Pre-production tests:

- Easy access to an integration platform
- Collaborative work in isolated or shared environments
- Testing new safety equipment and procedures in a realistic environment

Operational qualification:

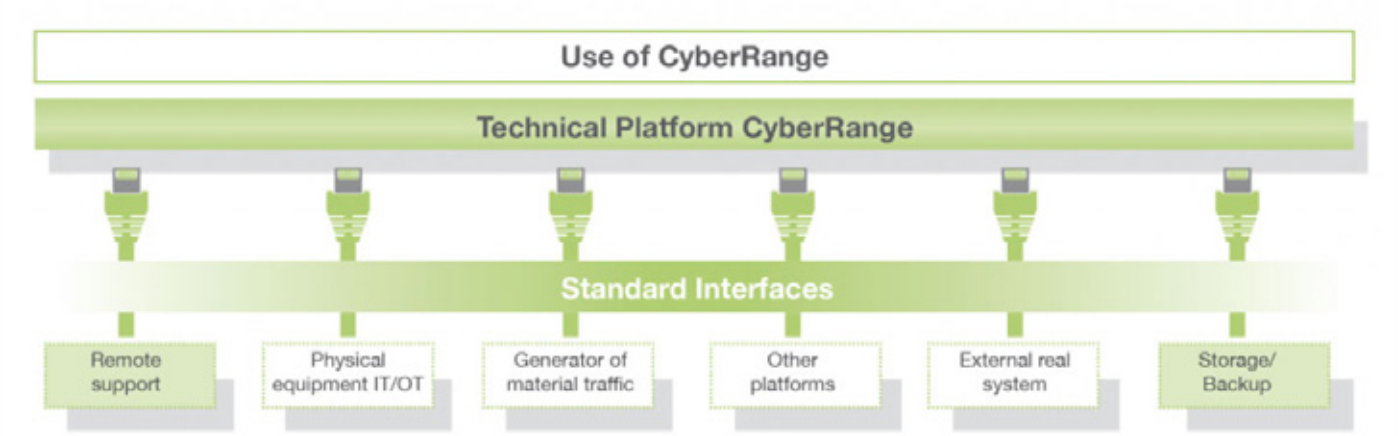
- Assessment of the impact of new equipment on a system
- Study of rule integration or the implementation of new procedures
- Analysis of cyber attack behaviour on its infrastructure without taking any risks

Training

- Awareness training for all staff and training on cyber security best practices
- Development of skills of cyber teams or knowledge retention to face new threats

Exercices

- Training of teams as part of operational exercises close to their daily environment
- Evaluation of the effectiveness of its security system as part of a cyber crisis management



Key Benefits

06

AIRBUS CYBERSECURITY

- **Realistic Simulations:** Immersion in complete IT/OT systems and animation with a complex scenario framework
- **Capacity:** Possibility to create complex systems composed of tens or hundreds of VMs or containers
- **Productivity:** Save time on configuration and integration to focus your business objectives
- **Agility:** Work alone or in a team in the same workspace or in parallel in different spaces
- **Safety:** Perform operations in an environment isolated from production systems
- **Scalability:** Possibility to complete the hardware configuration to increase the capacity

Unique Differentiators

- Easy environment to simulate highly complex networks with up to hundreds of virtual machines and thousands of dockers
- Perfect tool to train professionals at any level and improve skills of cyber experts
- Range of pre-defined cyber attacks
- Available both as a mobile box or through an online access
- Reliable customer service from an established cyber supplier

Future Functionality

- New scenarios integrated by default
- Various training packages available

AIRBUS
CYBERSECURITY

AIRBUS
CYBERSECURITY

Infographic

Cyber Range

Main Functionalities

Stormshield

A European Leader in Digital Infrastructure Security

STORMSHIELD

01

Company Description

STORMSHIELD

A European leader in digital infrastructure security, Stormshield offers smart, connected solutions in order to anticipate attacks and protect digital infrastructures. Stormshield offers innovative end-to-end security solutions to protect networks, workstations and data.

02

Company Information

Company Name: Stormshield
Founded: 01/16
Employees: 300+
Web: www.stormshield.com
Headquarters: Issy les Moulineaux

Other Offices: Lyon, Villeneuve d'Ascq, Toulouse, Munich, Madrid, Milan, Dubai, Warsaw

Key Target Verticals: Industry, Energy, Transportation, Manufactoring, Healthcare, Education, Administration, Defence, CNI

03

The Product

Product Category: Network security, (Cloud Security), Endpoint Security, ICS/SCADA, Information Privacy (Compliance and Data Leakage Prevention)

Product Stage: Released

Product Names and Brief Description:

- Stormshield Network Security (Network protection/Firewall/ UTM/Industrial cybersecurity)
- Stormshield Endpoint Security (workstations protection)
- Stormshield Data Security (data confidentiality and privacy)

Services Provided:

- Threat Intelligence, Training, Support

Customer Footprint

Markets with Customers:

- EMEA Market (France, Germany, Italy, Spain, Benelux, Poland, Hungaria, UK, Switzerlands, Nordics, Saudi Arabia, UAE, Jordania, ...),
- APAC Market (Thailand, Vietnam, Malaysia, Singapour, Taiwan,...)

Relevant Public Success Stories per Key Target Vertical:

- Université de Cergy Pontoise
- Rossman
- Port Boulogne Calais
- More References Available Upon Request

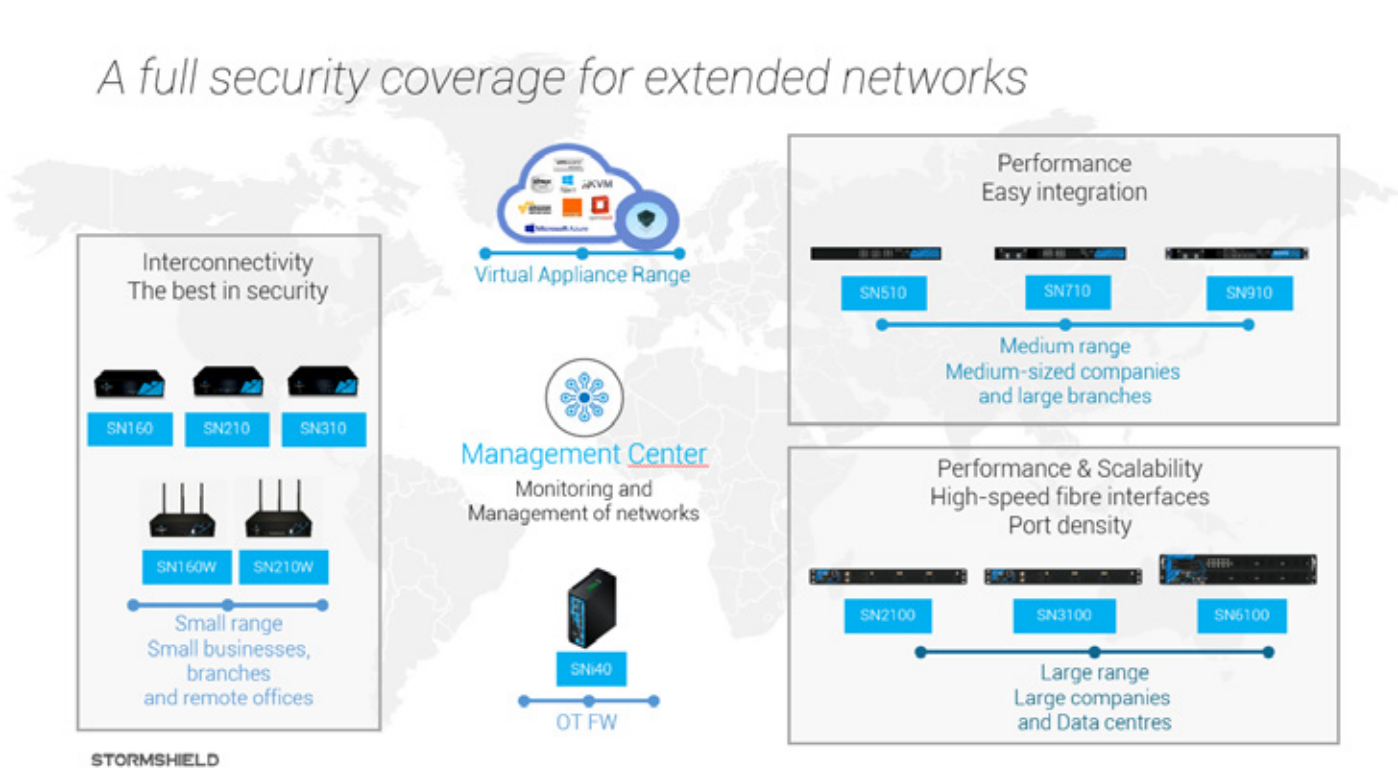
STORMSHIELD

Product in detail

The Stormshield Network Security (SNS) range is designed to protect IT & OT infrastructure against all types of threats transparently for users and administrators. These Unified Threat Management Solutions and Next Generation Firewalls combine all network security functions in a single hardware device or virtual appliance.

How does it work?

- **SNS appliances are available in different form-factors** (physical, ruggedized, virtual) in order to provide extended protection of hybrid environments (IT/OT/Cloud).
- **SNS appliances offer multi-layer traffic analysis and control based on Security Policy Management and Filtering up to layer 7**, Host and IP Reputation, IPSec/SSL VPN, Intrusion Prevention, Malware Prevention, Web and Email Control, Sandboxing, Security Reporting,...
- **SNS appliances can be managed in different ways:** embedded web interface, centralized management console, CLI, or orchestrated using an open API.



05

Key Benefits

STORMSHIELD

Ensure that business activities will remain uninterrupted

Our solutions include all of the protection technology needed to hold out against even the most sophisticated attacks.

Protect the internet use

Monitor internet usage, manage threats from the wild and control the impact on your business applications.

Connect employees and remote offices

Employees have secure access to the company's resources, no matter where they are and what device they're using.

Meet compliance requirements

Ensure your compliance with access control standards, regulations, and norms (PCI-DSS, ISO 27001, NIS, GDPR, LPM, etc.).

Unique Differentiators

Unrivaled Trust

The highest-level of European certifications to ensure integrity and transparency

Global Protection for Converged IT/OT Networks

A unique platform to inspect and control IT and Industrial-related traffic

Performance

An optimized system to ensure maximum performance when security engines are activated.

STORMSHIELD

Product in detail

The Stormshield Data Security (SDS) ensures the confidentiality of sensitive data and integrates transparently into usual communication tools so that business teams can create secure collaborative environments, whatever the media (email, USB keys, etc.), terminals (workstation, mobile) or applications (collaborative, intranet, collaborative cloud platforms, etc.).

How does it work?

- **Encryption everywhere:** Encryption is performed end-to-end and is exclusively controlled by the company. The file comes with its own security and can be shared with total peace of mind on various Cloud platforms or within the company as it is an agnostic solution. This means that the encrypted file remains accessible regardless of where it is stored.
- **User-oriented:** The user is central to data security. They can decide who has permission to access their information and can create workspaces in which we collaborate securely.
- **The keys belong to the company:** Data protection management is completely independent of its storage. Thus, the system administrator manages solutions and storage while sensitive data can only be accessed by authorised users. Furthermore, where outsourced storage such as the Cloud is concerned, the company is still the owner of the protection keys.

Key Benefits

- **Comprehensive protection suite:** Stormshield Data Enterprise ensures the confidentiality of all data, from local file to email protection and including a company's internal collaborative spaces. This solution is easily integrated whether or not it has an Active Directory or a PKI.
- **Easy management of zones of confidence:** Easily integrated into collaborative or communication tools, this encryption solution is scalable and especially suited to global deployment, commercially or by projects (BU or transverse services) or to safeguard exchanges with subcontractors.
- **Compliance:** In accordance with the GDPR* and the ANSSI requirements, a geolocation feature enables blocking of the application depending on the risk associated with the country where the user might be: confidential documents do not have unencrypted access.

STORMSHIELD

Unique Differentiators

Unrivaled Trust

The highest-level of European certifications to ensure integrity and transparency

Global Protection for Converged IT/OT Networks

A unique platform to inspect and control IT and Industrial-related traffic

Performance

An optimized system to ensure maximum performance when security engines are activated.

Future functionality

Agentless Encryption for external collaboration: A protected file can be shared with an external recipient without the need to install a local agent.

Certifications

- ANSSI Qualification (Standard Level)
- VISA ANSSI
- UE Restricted Classification
- NATO Restricted Classification
- EAL3+/EAL4+ Common Criteria

CYBER RANGES

A Next-generation Cyber Range as a Service

CYBER RANGES

01

CYBER RANGES

Company Description

Silensec is an international Information Security Management, Training and Technology Company with offices in **Cyprus (HQ), England, Kenya and Canada** and worldwide clients and partners. Silensec specializes in the delivery of services in IT Governance, Security Audits and Assessments, Value-Added Systems Integration, Managed Security with a 24x7 SOC, Security Training.

Established in England in 2006, Silensec is ISO 27001-certified by the **British Standards Institute (BSI). CYBER RANGES** is a wholly owned subsidiary of Silensec for the development and operation of **ISO 27001-certified** cyber range platforms and services.

CYBER RANGES, a.k.a. Silensec Cyber Range, is a next-generation military-grade full-content-lifecycle cyber range for the individual and team development of cyber capabilities, competencies assessment of competencies, organizational cyber resilience. CYBER RANGES is available as a public subscription-based/private managed service and as On-Premise and Portable deployment options.

02

Company Information

Company Name: CYBER RANGES
Founded: 2006-2
Employees: 50 up to 100
Web: cyberranges.com
Headquarters: Limassol, Cyprus
Other Offices:
Sheffield, UK
Nairobi, Kenya
Calgary, Canada

Key Target Verticals:
CYBER RANGES by SIlensec is used by:

- government agencies
- military entities
- higher education institutions
- training providers
- financial institutions, incl. central banks
- telcos and utilities
- consulting firms

03

CYBER RANGES

The Product

Product Category: Cyber Range, Detection & Prevention; SOC

Product Stage: Released & Deployed

Product Names and Brief Description:

- Next-generation Cyber Range as a Service on public/private cloud or as On-Premise and Portable

Services Provided:

- Immersive simulation training, cyber capability building and assessment, cyber resilience testing

04

Product in detail: CYBER RANGES

CYBER RANGES is the world-renowned platform by Silensec for immersive simulation training, cyber capability building and assessment, cyber resilience testing. Government and military entities, large companies, telcos and utilities, central banks and universities successfully use CYBER RANGES.

Since 2017 the UN's International Telecommunications Union (ITU) has used CYBER RANGES to run cyber drills around the world, such as the ITU 2020 Global Cyber Drill with over 210 participants, organised in teams from both technical and management roles, from 57 national CERTs/CSIRTs. This exercise ran over 2 weeks with 6 complex scenarios designed/developed together with industry partners using the CYBER RANGES content suite for scenarios authoring, infrastructure virtualization, traffic & attack injections, external technologies integration.

CYBER RANGES offers you:

- an environment for on-tap individual training practice with an ever-growing library of simulation scenarios.
- a service for blue/red team exercise platform for SOC/IR teams.
- your own platform, hosted/on-premise according to your organisation's mission, to model even true replicas of your live or target infrastructures (technologies - OT/SCADA/ICS etc. - tools, processes, etc.) and to run your capability and product testing exercises in secure conditions, even with safe online access.
- comprehensive data capture to measure the performance of individuals, teams, processes, tools and products towards ultimate capability evaluation.

How does it work?

- CYBER RANGES has led on the innovative use of cloud technology for cyber-ranging.
- CYBER RANGES can scale up to 1,000s of concurrent users and VMs.
- With a user interface designed according to gamification principles, CYBER RANGES provides user and administration support for individual and red/blue/white/... team-based exercises.
- CYBER RANGES offers the ability to design, develop, host and run custom virtual environments and a variety of multi-format simulation scenarios to meet specific objectives and according to many performance criteria.
- CYBER RANGES offers the ability to integrate third-party technologies and tools in the virtual environment besides its library of pre-built infrastructure assets.
- CYBER RANGES contains advanced technology for user traffic and attack simulations according to the latest exploits and vulnerabilities (e.g. MITRE ATT&CK).
- CYBER RANGES provides support of standard (e.g. NIST NICE) and custom competency frameworks for scoring and assessment, with start-to-finish performance metrics.
- CYBER RANGES is available in all deployment options for clear cyber-ranging economics: public cloud or hosted, on-premise and even portable.
- CYBER RANGES offers real-life situational practice in on-the-job like conditions.
- Many cyber ranges are designed to deploy at a physical location. CYBER RANGES PORTABLE supports cyber-range-in- a-room. it takes your cyber range to users rather than users to it, incl. remote places or in-theatre, for several even complex use cases.

CYBER RANGES

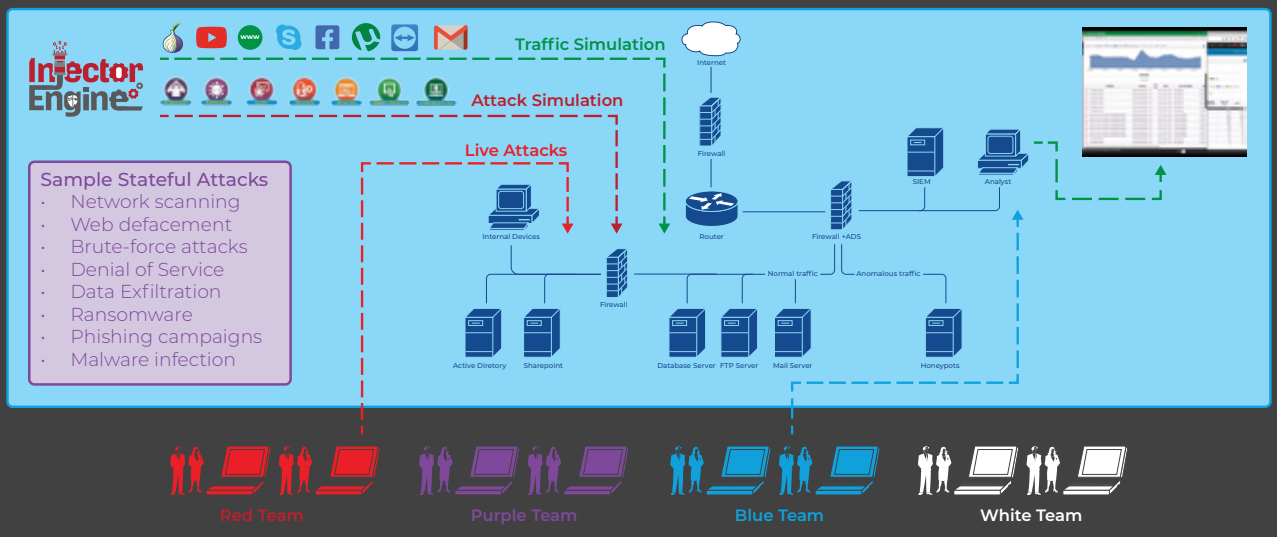
How does it work?

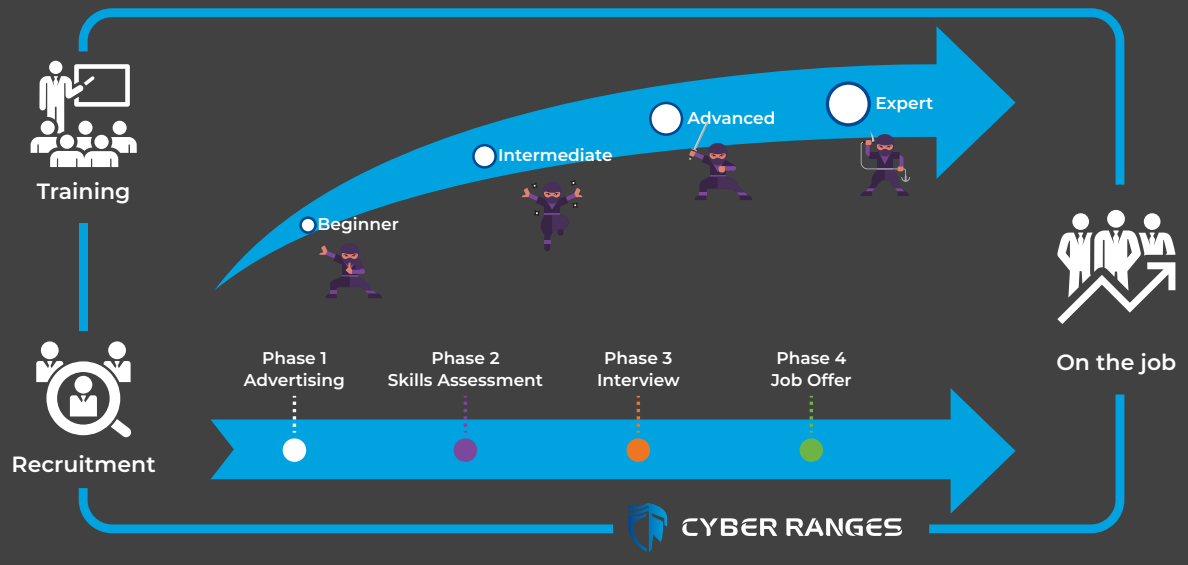
CREATE Design and build custom scenarios, including complex virtual environments, storylines with clear mission/task objectives and cyber challenges.

PUBLISH Make your scenarios available on CYBER RANGES for continuous, easy and on-demand access by users, anytime anywhere, even on pay-as-you-go terms.

USE Set up and run cyber exercises from the extensive library within minutes, using nothing but a few clicks.

ASSESS Assess the competencies of individuals or teams using standard or custom competency frameworks against the latest attacks, threats and vulnerabilities.





06

CYBER RANGES

Key Benefits

CYBER RANGES delivers the following benefits according to the chosen deployment option:

- Continuous security competencies development for your team at a fixed cost
- On-demand deep-dive hands-on security labs anywhere anytime
- Several security tracks, expert-defined, objective-based and mapped to different security roles and career paths to cover all your competence needs in your SOC/CSIRT/CERT/business ecosystem/etc.
- Visibility of individual and team capabilities to know about the areas of strength, weakness and improvement of your personnel's hard and soft cyber security skills
- Advanced traffic and red-team simulation engine for realistic blue-team training scenarios
- Competence-based assessment to support your staff hiring and on-boarding
- Validation of cyber security training and certification programmes against actual real performance
- Training/testing securely on live/planned infrastructure replicas
- Testing the cyber resilience of your organization against current and future threats.

07

Unique Differentiators

Key differentiators of CYBER RANGES are:

- **Orchestration**, i.e. managing great numbers of users and scenarios, even large/complex ones
- **Collaborative authoring tools** for scenario design, development and re-purposing
- **Agent-based user traffic and attack simulations**, also based on MITRE ATT&CK
- **Support of Competency Frameworks** and other performance criteria (custom or industry-specific)
- **Scoring and reporting**
- **All the benefits on a portable system too!**

08

CYBER RANGES

Future Functionality

The CYBER RANGES innovation is backed by a highly focused Research & Development team, whose architects are regularly engaged in large-scale research projects with academic, industry and government partners.

Silensec operates an ecosystem of partners, leaders in their own industries and subject matter experts. This ecosystem already provides those organisations choosing CYBER RANGES, with additional access to:

- specialist knowledge
- engaging simulation scenarios
- focused consultancy services for CYBER RANGES powered cross-team exercises
- integration of CYBER RANGES with domain-specific systems and technologies, such as LMS, HCM and OT/SCADA/ICS and more.

Direct research, partner ecosystem, and active participation in such international industry associations as the European Cyber Security Organization (ECSO) and the Global Cyber Alliance (GCA) help position CYBER RANGES as one of the few most robust long-term committed vendors in the cyber range and cyber exercise market.

09

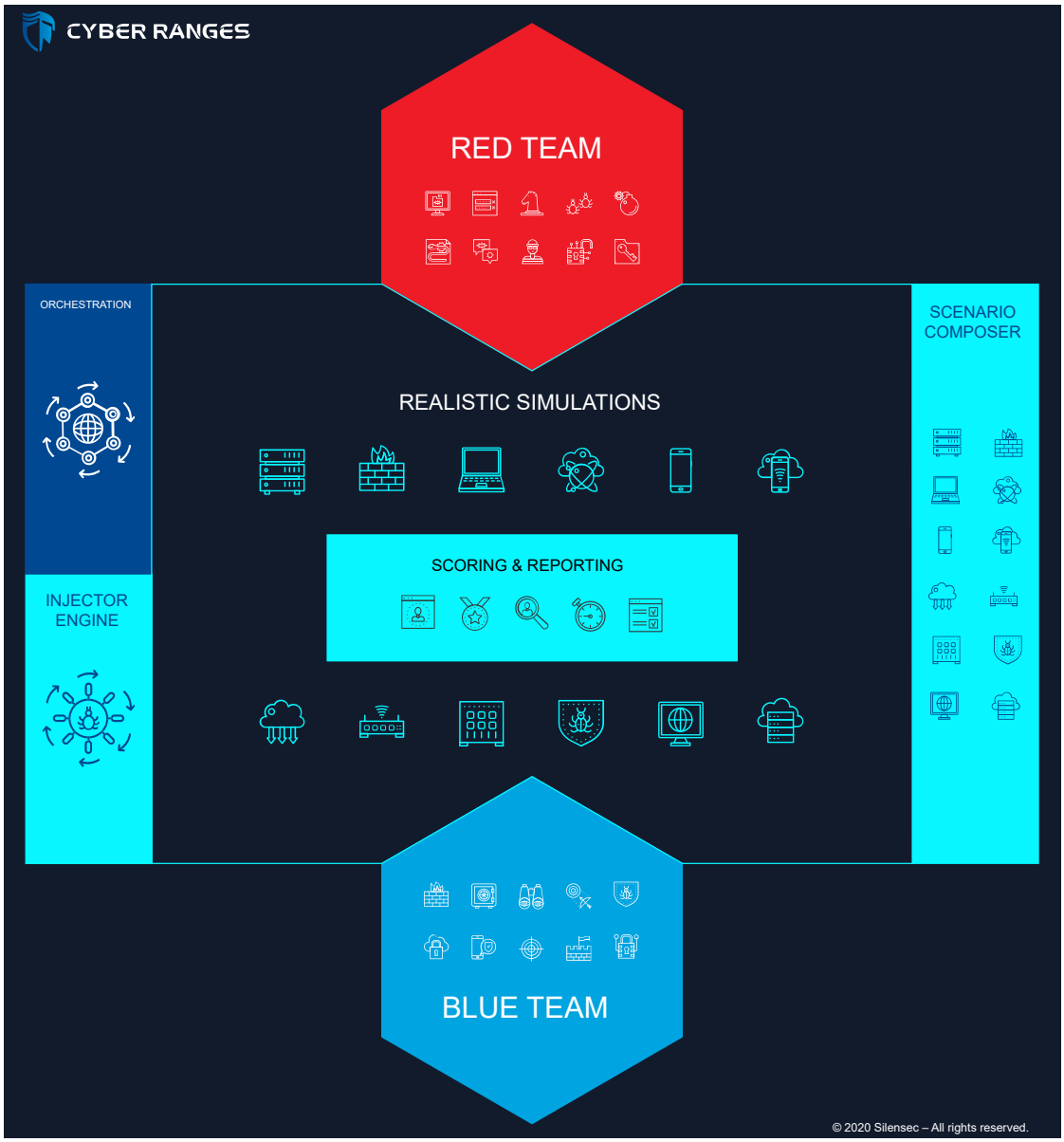
Services provided

CYBER RANGES comes with a comprehensive set of Value-Added Services, provided by Silensec and its Industry Partners, to deliver you and your organization a unique high-return use experience based on the CYBER RANGES capabilities.

Such value-added services can be accessed no matter whether you have opted for a cyber range on pay-as-you-go/subscription terms, hosted/MSSP terms, on-premise or portable:

- Advanced scenarios including APT and cyber threat simulation
- Custom simulation replicating the target organization's environment
- Delivery of cyber drills and hybrid table-top hands-on simulation exercises
- Large-scale security personnel selection and recruitment based on hands-on competence assessmentScoring and reporting
- All the benefits on a portable system too!

Infographic: Red vs Blue Team realistic simulations



Certifications

silensec™ iso27001 Certified

senhasegura

Global Privileged Access Management (PAM) Vendor

senhasegura

01

Company Description

senhasegura is a global Privileged Access Management (PAM) vendor.

Our mission is to eliminate privilege abuse in organizations around the globe and build digital sovereignty. To accomplish this, senhasegura works against data theft through the traceability of privileged actions of both human and machine identities on assets such as network devices, servers, databases, Industry 4.0 and DevOps environments.

In 2020 and 2021, senhasegura has been recognized as a Challenger in the Gartner Magic Quadrant (MQ) report. In the same year Gartner also placed us among the three best PAM Technologies in the world in their Critical Capabilities PAM report. In January 2021, we were one of the only two companies in the world that received the Customers' Choice stamp in the 2021 Voice of the Customer report by Gartner Peer Insights. In the same portal our customers' reviews offered a 97% recommendation rate*, the highest one among all PAM vendors.

02

Company Information

Company Name: senhasegura
Founded: 2010-3
Employees: 50 up to 100
Web: senhasegura.com

Headquarters: São Paulo, Brazil
Key Target Verticals:
Energy & Utilities; Finance; Telco; Healthcare; Legal & Government; Retail

03

The Product

Product Category: Cloud Security, Gov. & Compliance, IAM, Healthcare

Product Stage: Released & Deployed

Product Names and Brief Description: senhasegura Privileged Access Management platform - PAM 360º, an advisory process developed by senhasegura that identifies an organization's maturity level in terms of privileged credential management.

Services Provided:

- Assessment 360º to evaluate the privileged access management process;
- Top down approach starting from a broad view of business

04

senhasegura

Product in detail

senhasegura is a Privileged Access Management platform composed by the following product families:

For PASM:

- senhasegura PAM Core: https://senhasegura.com/en/products/access-management-pam/
- senhasegura DevOps Secrets Management (DSM): https://senhasegura.com/en/security-and-risk-management/devops/
- senhasegura Domum - Remote Access: https://senhasegura.com/en/products/domum/
- senhasegura PAM Express SMB

PS: All PASM components run on Linux Virtual Machine but this is totally transparent to the customer

For PEDM:

- senhasegura Privileged Escalation Delegation Management for Windows, also referred as senhasegura.go for Windows: https://senhasegura.com/en/products/endpoint-privilege-management/endpoint-privileges-windows/
- senhasegura Privileged Escalation Delegation Management for Linux, also referred as senhasegura.go for Linux: https://senhasegura.com/en/products/endpoint-privilege-manageme
- senhasegura Certificate Management: https://senhasegura.com/en/products/certificate-management/
- senhasegura PAM Multi-Tenant: https://senhasegura.com/en/security-and-risk-management/cloud-security/
- senhasegura PAM Load Balancer: https://senhasegura.com/en/products/pam-infrastructure/pam-load-balancer/

PS: All Others run on Linux Virtual Machine but this is totally transparent to the customer

- senhasegura PAM Crypto Appliance: https://senhasegura.com/pam-crypto-appliance/

05

How does it work?

senhasegura is a privileged access management software solution that stores, manages and monitors all credentials, such as passwords, SSH keys and digital certificates, in a secure digital vault. Using encryption mechanisms, the password vault offers users the ability to use only one password to access a series of credentials registered in the solution.

Additionally, senhasegura can be used to access all network resources through SSH and RDP protocols, storing all records of their use for audit and compliance analysis purposes. Its intelligence allows for real-time analysis of actions taken by users and alert generation to identify fraud or inappropriate action.

06

Key Benefits

- Operational gain in the password change process.
- Guaranteed password delivery in a secure and controlled manner.
- Transparent authentication on the target system or network device without displaying the password to network administrators or third parties.
- Greater security maturity in DevOps environments (DevSecOps).
- Reduced security risks and better governance.
- Reduction of security risks and improper access to sensitive data.

senhasegura allows segregation for access to sensitive information, isolating critical environments and correlating environments with and without correlation. Taking this into account, it is important to avoid data breaches, the biggest challenge in the management of privileged users.

Overcome the challenges of implementing regulations such as PCI, ISO, SOX, GDPR, and NIST, with automation of privileged access controls to achieve maturity in the audited processes.

07

Unique Differentiators

Features that differentiate senhasegura against our competitors:

- SaaS-based solution of intelligently distanced Privileged Access that is agentless and VPN-less
- Exclusive native feature of creating and executing Ansible playbooks as a tool for building new privileged tasks
- AI & ML Powered User Security Posture Rating
- DevOps - Secret Automation
- Certificate Management
- Change Audit
- AWS OpsWorks Integration

Other differentials:

Governance and Administration
- built-in SCIM connector for IGA integration
- built-in MFA App

Privileged information
- Personal vault
- Privileged data

PEDM Windows
- offline credential take-out
- file integrity monitoring
- application sandboxing

Secret Management
- Cloud IAM provisioning

Ease of Deployment
- All-in-One virtual machine with no need of 3rd licenses

Future functionality

08

Our main innovation drivers are:

1. Use of AI to predict frauds instead of reporting them
- AI DevSecOps Analysis
- AI PEDM Threat Analysis
- AI Cloud Entitlements Analysis

2. PAM as a SaaS
- Open billing Process: It gives more transparency to legal sponsors of product
- Flexibility to increase or reduce license: which results in greater customer flexibility
- Easier support, community and documentation access: to improve customer experience to solve issues faster

3. DevOps Integrations In 2021 our innovation team will continue to close gaps in market demands, working to accelerate the development of unique and differentiated functions or improving our functions in relation to the competition. We will drive the market even more than we have in the coming years.

Video

IAI/ELTA

ELTA Systems, a leading Defense Electronics Company

01

Company Description

ELTA systems LTD, a group and subsidiary of **Israel Aero Space Industries**, is one of Israel's leading Defense Electronics companies and a global leader in the fields of **Radar, Electronics Warfare, Cyber and Communication**.

IAI ELTA operates as a Defense systems house, based on Electromagnetic Sensors (**Radar, Electronic Warfare and Cyber Communications**) and **Information Technology.** IAI ELTA's products are designed for intelligence , Surveillance , Target Acquisition and Reconnaissance (ISTAR), Early Warning and Control (AEW&C), Homeland Security (HLS) , Cyber, Self-Protection and Self-Defense.

02

Company Information

Company Name: IAI ELTA
Founded: 1967-01
Employees: 100 up tp 500
Web: www.iai.co.il
Headquarters: Ashdod, Israel

Key target verticals:

National Cybersecurity entities, Government, Army, Navy

03

The Product

Product Category: Detection & Prevention, Incident Response & Forensics, Cyber Intelligence, Cyber Range, IoT, Training & Education, SOC, UAVs, Aviation, Rail & Metro, Maritime

Product Names and Brief Description:

- CEWC
- Maestro
- Tame Range
- Neptune

Customer Footprint

Relevant Public Success Stories per Key Target Vertical:

- Government
- Financial Services
- Critical Infrastructures
- Manufacturing
- Law Enforcement & Intelligence Agencies
- Other

Product in detail: Cyber Early Warning Center - CEWC

National level monitoring and detection platform fusing data from internal and external sensors automatically **creating a situational awarness picture for SOC analysts and decision makers.**

How does it work?

- **Data Collection** – cross platforms and cyber threat intelligence
- **Correlation** – between IT & OT events, indicators and national cross organizations incidents
- **Advanced analytics** – identifying sophisticated attacks
- **Situational awareness** - state-level picture of national cyber hygiene status

05

Key Benefits

- Enhancing deployed cyber solution into one holistic platform
- Automated kill-chain investigation
- Full incident response cycle management
- Open architecture

Unique Differentiators

- Seamless orchestration of all cyber sensors into a single point of analysis
- Unified management and display for SOC automation
- Tailor-made technological and methodological solution fitting customer cyber threats

Future Functionality

Evolved SOC ecosystem build for land / maritime / aviation

Product in detail: MAESTRO

State of the art automated environment for media investigation

How does it work?

- Automated extraction of all media types
- Automated analysis-based, operator-defined workflows
- Central display of forensic analysis results
- SDK for integration of new forensic tools

Product benefits and unique differentiators

Key Benefits:

- Automated investigation
- Definition of workflows
- Central display of forensic analysis results
- Shared analysis environment for multiple operators
- Retention of forensic investigation processes

Unique Differentiators:

- Workflows running in parallel tools
- Easy integration of new forensic tools
- Secured environment assuring containment of threats

Future Functionality:

Mobile analysis platform for IR teams for on-site analysis

07

Product in detail: TAME RANGE

Advanced cyber competency center training security professionals with authentic, real-world cyber attack campaigns

How does it work?

- Virtualized, private-cloud based Cyber Lab simulating a real environment
- Assignment of trainees to classes
- Automatic injection of attacks
- Tracking of trainees' progress in attack investigation
- Scoring and assessment of trainees

Product benefits and unique differentiators

Key Benefits:

- Authentic, real-world cyber attack campaigns
- Learning Management System
- Hands-on experience with the tools, techniques and team skills
- Controlled, isolated and customizable network environments
- Simulation of OT devices

Unique Differentiators:

- Full attack automation
- Team training
- Auto-scoring function
- Multiple simultaneous courses

Future Functionality:

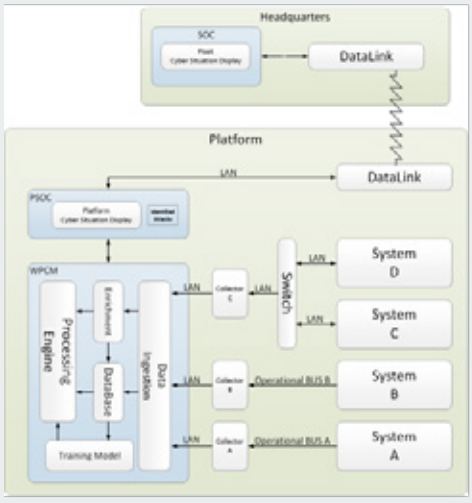
- Support of IOT attack scenarios

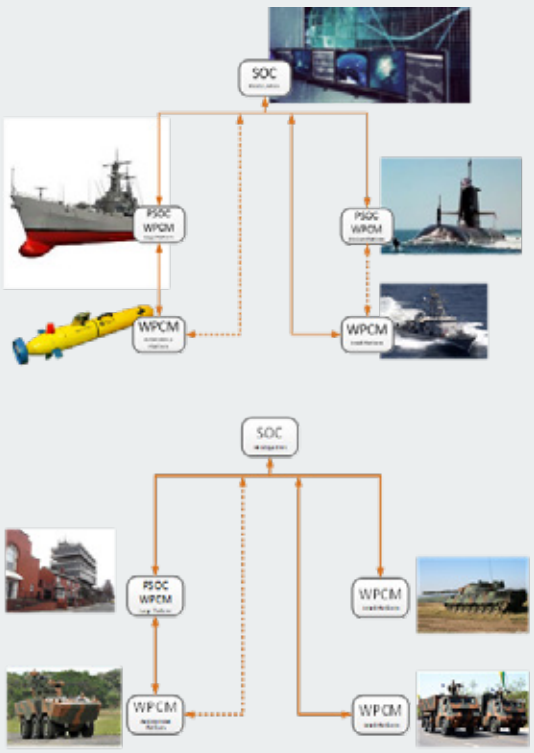
Product in detail: Neptune

Neptune system detects and reports anomaly behavior of platforms (Maritime, Aviation, UAVs, Automotive, etc.) and systems (e.g. Warfare, C4I, IT Systems, etc.) and generates intuitive, flexible and adjustable cyber situation view.

How does it work?

- The system is composed of:
  - **WPCM** (Warfare Platform Cyber Monitoring)
  - **PSOC** (Platform SOC)
  - **SOC**
- The WPCM Collects data from all the monitored systems
- Performs data normalization and enrichment
- Analyzes the data with respective data model using advanced Machine Learning Anomalies Detection Algorithms
- Alerts are being generated toward the PSOC / Central SOC upon events detection
- Feedback on false alarms (False positives) can be generated from the PSOC/SOC, by the user, to improve future detection





09

Key Benefits

- Combine both rule-base and machine-learning
- Able to detect both known and unknown cyber-attacks
- Advanced semi-supervised anomaly detection algorithm incorporates mission/process context considerations
- Multiple systems event correlation
- Outbound system monitoring
- Seamless integration on legacy platforms
- Able to integrate third party systems and sensors
- Detection of technical failure
- Cyber events report to multiple security centers (on-board and off-board) using very low bandwidth
- Intuitive and flexible mission adapted cyber situation view

Unique Differentiators

- Unique and advanced ML algorithms considering mission/process context
- Deep packets inspection normalization and analysis
- Multisystem cyber events correlation and detection
- No affect on systems behavior and performance
- Technical failure detection
- Generic architecture applicable to a variety of platforms – Maritime, Aviation, UAVs, Automotive and more
- HQs central cyber situation awareness viewing cyber status of subordinate platforms

Future Functionality

- Organizational & Industrial solutions
- Improved detection swiftness

Partners

Israel Cyber Companies Consortium – IC3

Israel Aviation Cyber Companies Consortium – IAC3

Stellar Cyber

High-speed high-fidelity detection and automated response across the entire attack surface

STELLAR CYBER®

01

Company Description

Stellar Cyber was founded in 2015 by Aimei Wei (Senior VP of Engineering) on a mission **to transform security operations,** changing the conversation from analyzing data to correlating incidents, covering the entire attack surface and bringing the right intelligence, while retaining investments.

Today, Stellar Cyber is the **leading Open XDR** (Everything Detection and Response) platform for enterprises and MSSPs, unifying all currently disjointed security tools and data sources to fully visualize and automatically detect, investigate and respond to all attack activities.

We continue our relentless drive to enhance the platform through ongoing research and development.

02

Company Information

Company Name: Stellar Cyber
Founded: 2015
Employees: 70 up to 100
Web: stellarcyber.ai

Headquarters: Santa Clara, CA
Key Target Verticals: Enterprise : Manufacturing, Finance, Education, Government, Healthcare

03

The Product

Product Category: XDR, Cloud Security, Detection & Prevention, Email Security, AI, Endpoint Security, Network Security, Orchestration & Automation, UEBA

Product Stage: Released & Deployed

Product Names and Brief Description: Stellar Cyber's Open XDR platform delivers **Everything Detection and Response** by unifying all currently disjointed security tools and data sources to fully visualize and automatically detect, investigate and respond to all attack activities. organization's maturity level in terms of privileged credential management.

STELLAR CYBER®

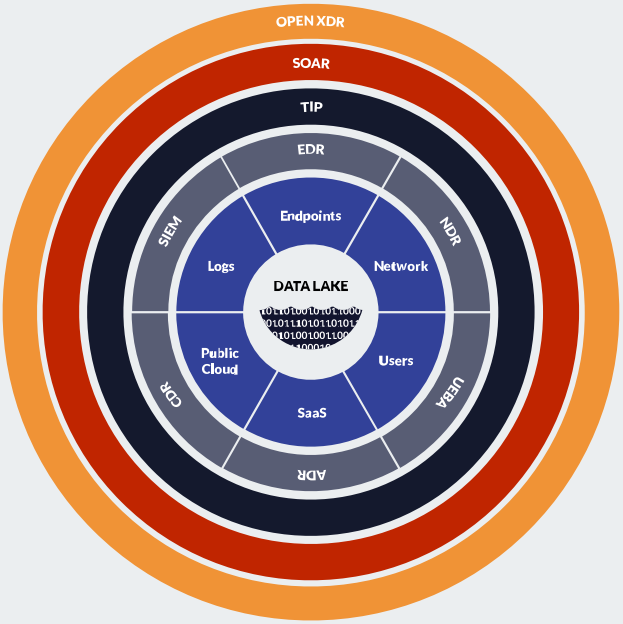
Product in detail

Open XDR is a unified, AI-powered approach to detection and response, that collects and correlates all existing security tools, to protect the entire enterprise attack surface effectively and efficiently. **Open XDR is Everything Detection and Response,** more than eXtended Detection and Response, because it must defend against all threats across the entire attack surface. The only way to do this is by integrating with existing security tools.

How does it work?

Architecturally, Open XDR is about **unifying and simplifying the entire Security Stack** for the purpose of radically improving detection and response. At any given enterprise, a Security Stack will consist of numerous capabilities like SIEM, EDR, NDR, SOAR and more. These capabilities were never designed to work with each other, and teams spend too much time managing multiple tools, which is what leads to the problems of today – too many tools, not enough people, not right data. That's where Open XDR comes in – unify all capabilities together, correlate alerts from individual tools into a holistic incident, simplify by reducing administrative overhead. AI and automation comes in as the only technically feasible way of protecting the entire attack surface effectively and efficiently, which is why it is a key architectural attribute of Open XDR.

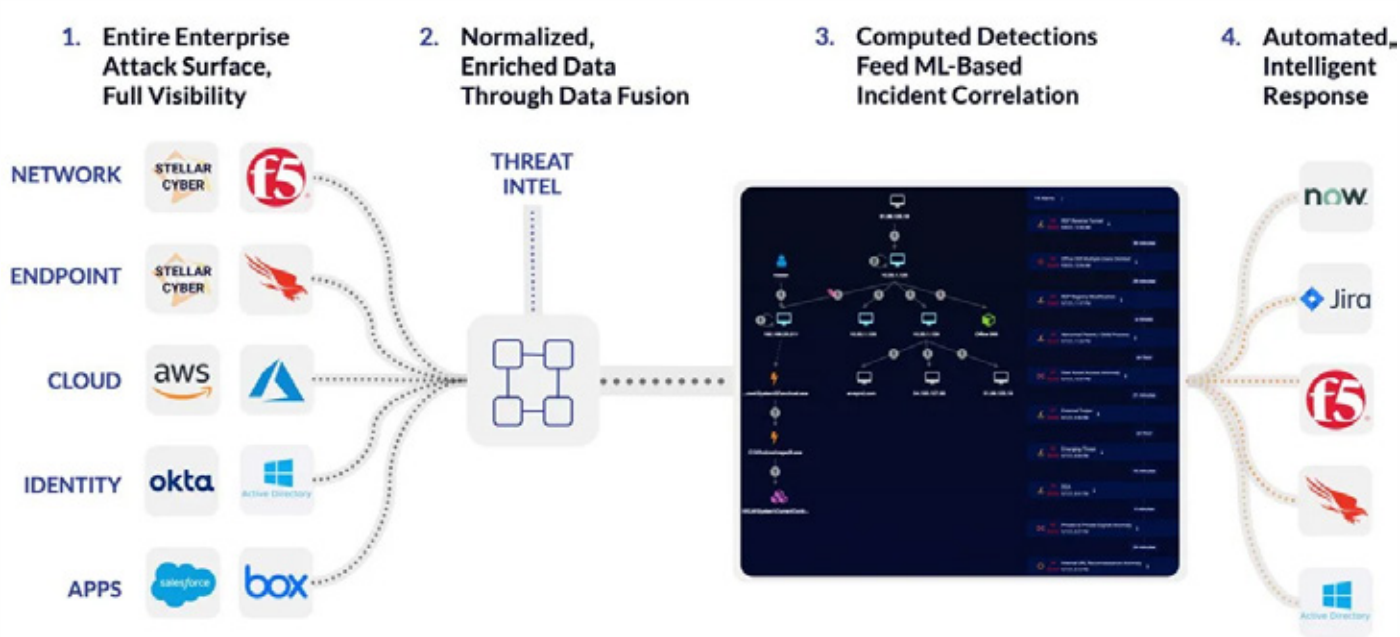
The outcome of Open XDR is protecting your enterprise from threats from a single platform versus multiple tools that have weak or non-existent connections band-aiding it all together. And the ultimate outcome of Open XDR is radically improved detection and response at a price enterprise's can afford.



Stellar Cyber's Approach To Open XDR

While integrating with your existing security tools as part of our open platform, Stellar Cyber's Open XDR Platform also packages together multiple capabilities, all built on core technology that enables the outcome of Open XDR – radically improved detection and response at a price enterprise's can afford. In our view, it's not enough for Open XDR to be "eXtended", that is a marginal improvement over status quo, and today's security environment demands something dramatically different, which is why we believe Open XDR is Everything Detection and Response.

From a technology standpoint, we believe the right approach to XDR is Open-first, partially-Native. If an Open XDR platform is only a "correlation layer" on top of existing tools including a SIEM, that does not deliver a unified experience and does not simplify the Security Stack. Conversely, a Native-only XDR platform requires an enterprise to move their entire infrastructure to one vendor. The Open-first, partially-Native approach to XDR is core to our Open XDR platform. The Stellar Cyber Open XDR Platform works with whatever you have already, gives you better visibility where you don't yet have it, and helps you consolidate multiple capabilities under one platform if you choose to do so.



06

Key Benefits

The value of Open XDR:

- Radical Performance
  Unification of the Security Stack, with AI powered detection and response, translates a faster, better approach to security opeartions.

- No Vendor Lock-in
  Open XDR leverages existing security tools, not forcing you to migrate your Security Stack to a single vendor's firewalls, SOAR, EDR, etc.

- Economics
  Simplification and consolidation of security products reduce the number of licenses, tool training and overall capital required to run a security operations program.

07

Unique Differentiators

Our unique differentiators are:

1. Automated Incident Correlation:
   - Automatically groups related alerts into incidents that show the progression of an attack – reducing the investigation effort from the number of alerts to the number of incidents, orders of magnitude reduction.
   - Automatically combines related alerts into incidents with high fidelity – reducing the noise from the false positive of individual alerts – an order of magnitude improvement in accuracy.
   - Automatically prioritizes incidents to clearly identify the most serious attacks – shows analysts exactly where and how to respond.
   - Leverages telemetry from existing security tools as well as its own sensors – preserves existing security investment and provides 360-degree visibility by filling in the gaps.
   - Feeds the AI engine with normalized and enriched quality data to initiate instant and effective responses – AI works better when it has the right data to work from.

07

Unique Differentiators (Cont'd)

2. XDR Kill Chain™:

- First new kill chain invented in years – designed specifically for XDR detections, where threats can attack any point in theinfrastructure.
- Loop interface prioritizes detections into five phases: initial attempts, persistent foothold, exploration, propagation, and exfiltration / impact – analysts can easily see attacks as they happen and respond to the most emergent needs first.
- Captures the progression of complex attacks – alerts appear in the context of the five-phase kill chain so analysts can easily prioritize them without getting lost in details.
- Incorporates commonly used MITRE ATT&CK framework for detailed analysis and adds new tactics and techniques beyond the MITRE ATT&CK framework.

08

Videos

Stellar Cyber Incident Correlation

Stellar Cyber XDR Kill Chain

Feedback and suggestions

Your feedback is extremely important to us and we value and appreciate receiving your suggestions or comments to help us improve our content, services and the way we communicate.

We appreciate receiving compliments

If you are satisfied with the Cyber Startup Observatory, please let us know. It helps us to know that we are delivering our services effectively and provides us with an opportunity to recognize our team's valuable effort.

Suggestions on cyber security topics, news, solutions and innovations are a valuable input

We strive to cover relevant topics, provide valuable resources and to shed some light on important issues. The team welcomes your contribution as a way to widen our vision, the quality of the content and the depth of our knowledge.

You can contact us at:

info@cyberstartupobservatory.com

The Global Cyber Innovation Network

The Cyber Startup Observatory®

The Cyber Startup Observatory®

Africa - 4th Edition