Cyber Security Observatory®

META

March 2023

Innovation - Insight - Leadership

Startups & Scaleups

Investors

Advisors

Community

Enterprises

Innovation - Insight - Leadership

Featured Companies

Cyber Security Leaders

...featured in this edition

Dr. Aloysius Cheang
Chief Security Officer
Huawei Middle East & Central Asia

Aaditya Bhagra
Associate Partner, MEA Security Services
IBM

Innovation - Insight - Leadership

Cyber Security Leaders

...featured in this edition

Madan Mohan
Director - Technology Risk
BDO UAE

Enes Yildizhan
ICT Security Chief
Tailwind Airlines

Innovation - Insight - Leadership

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.

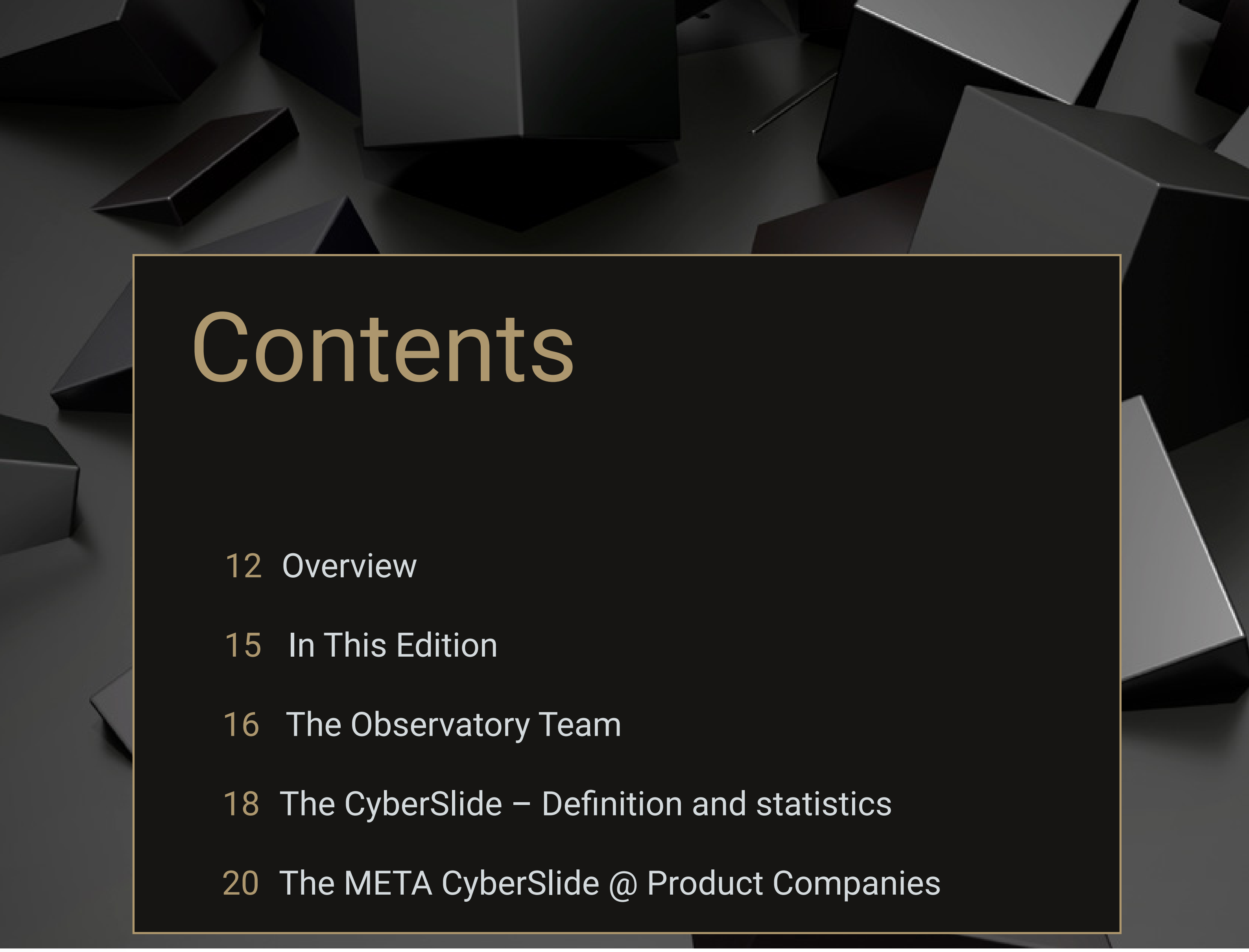
In this document, **“Cyber Startup Observatory”, "Cyber Security Observatory"** and **“Smartrev Cybersec”** refer to trademarks belonging to Smartrev Analytics Consultants SLU.

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.

© 2023 Smartrev Analytics Consultants SLU. All rights reserved.

Cyber Startup Observatory®

- Financial Services
- Healthcare
- Critical Infrastructures
- e-Commerce
- Public Sector
- Manufacturing
- SME
- Technology & Consulting
- Law Enforcement
- Universities & Education
- Automotive
- Aviation
- Rail & Metro
- Maritime



Contents

12 Overview

15 In This Edition

16 The Observatory Team

18 The CyberSlide – Definition and statistics

20 The META CyberSlide @ Product Companies

22 The Israel CyberSlide @ Product Companies

24 The Africa CyberSlide @ Product Companies

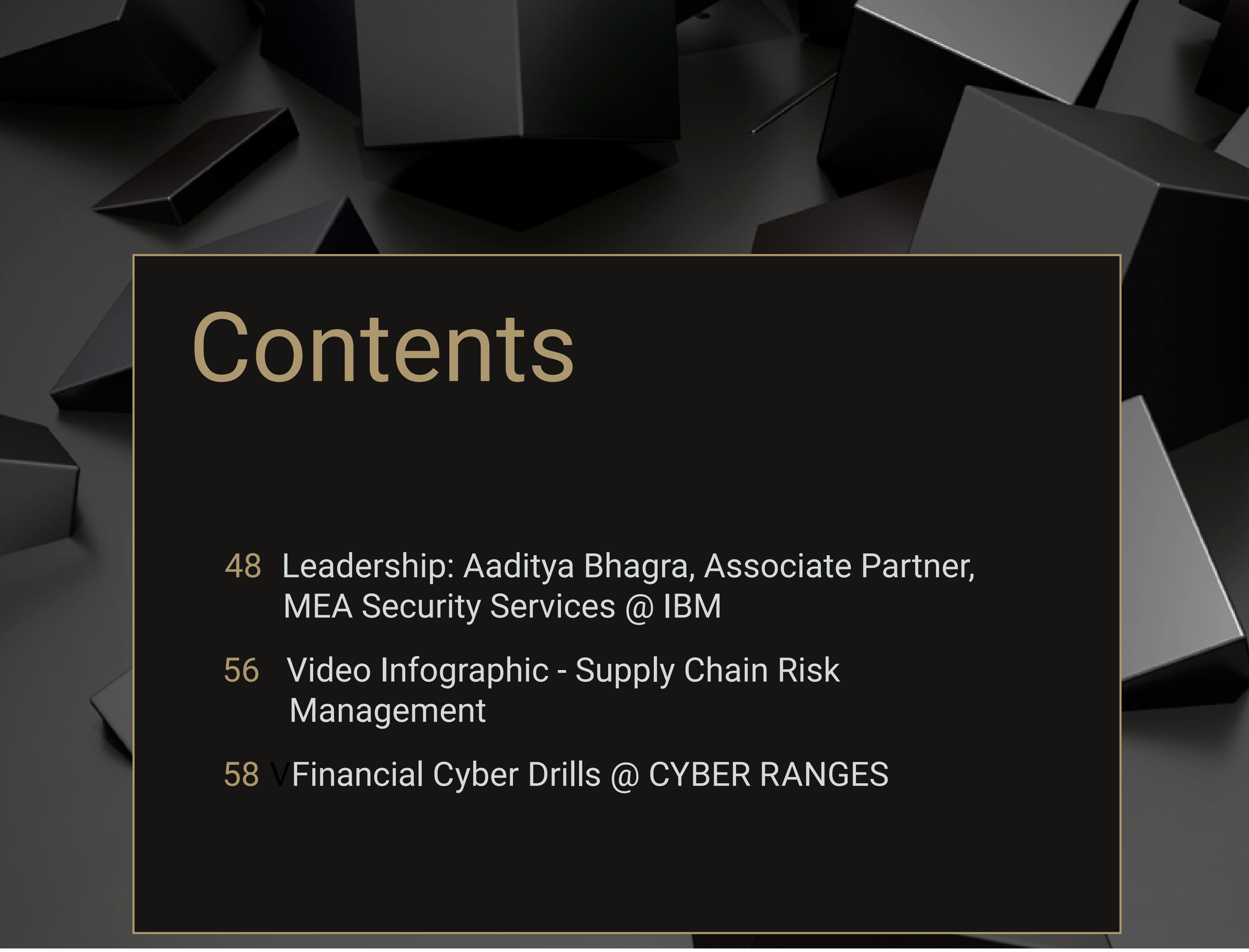
26 APAC CyberSlide @ Product Companies

28 The Airport of Things (AoT) @ Cyber Startup Observatory

33 Leadership: Dr. Aloysius Cheang, Chief Security Officer, Huawei Middle East & Central Asia

35 Video Infographic - Protect Against Ransomware - Immediate Actions

37 How Do You Choose the Best Cybersecurity Project For Your Company? @ senhasegura



Contents

48 Leadership: Aaditya Bhagra, Associate Partner, MEA Security Services @ IBM

56 Video Infographic - Supply Chain Risk Management

58 VFinancial Cyber Drills @ CYBER RANGES

74 Leadership: Madan Mohan, Director - Technology Risk @ BDO UAE

83 Video Infographic - Potential Significant Changes in NIST CSF 2.0

85 Making Co-Managed Security Services a Win-Win @ Stellar Cyber

88 Leadership: Enes Yildizhan, ICT Security Chief @ Tailwind Airlines

94 Video Infographic - Immediate Steps to Improve OT Cyber Security

96 Power Grid Cybersecurity, Where Are We Now? @ Cyber Startup Observatory

Contents

Pages 28 - 32

The Airport of Things (AoT)

Pages 37 - 47

How Do You Choose the Best Cybersecurity Project For Your Company?

Contents

Pages 58 - 73

Financial Cyber Drills

Pages 85 - 87

Making Co-Managed Security Services a Win-Win

Contents

Pages 96 - 101

Power Grid Cybersecurity, Where Are We Now?

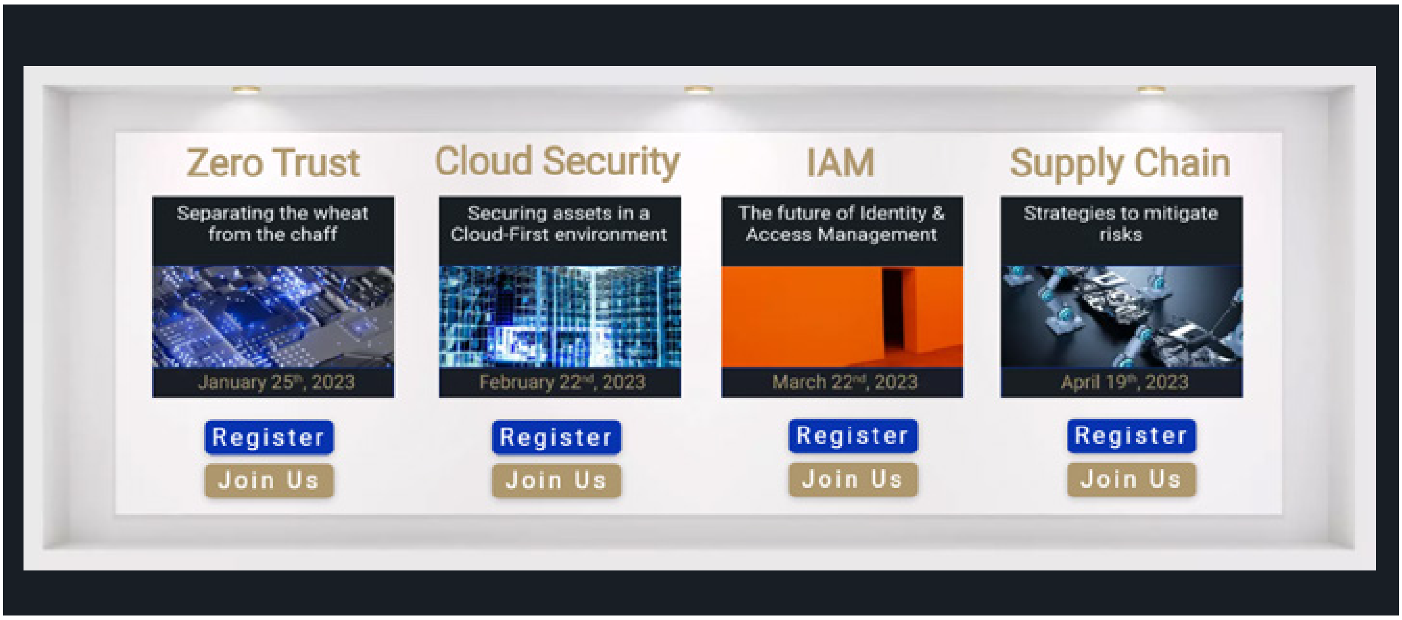
Overview

The **Cyber Security Observatory Middle East, Turkey and Africa (META) - 4th Edition** kicks off with a look at the cyber security ecosystem in the UAE, Israel, Turkey and Africa, dynamic markets we keep coming back to with renewed enthusiasm for its innovators, expertise and shear scope for growth within the cyber security industry.

Of course, the last twelve months have not been without their challenges for these countries - cyber security risks all increased manyfold with the ongoing geopolitical conflicts and the war, exposing ever expanding threat surfaces, and high-profile breaches and ransomware cases making headlines yet again. On the front-line, defending businesses, public bodies and institutions and indeed, individual citizens, we find both established companies and burgeoning start up innovators, and we are proud and honored to be able to shine a light on some of the amazing work being put into practice by them in this 4th Edition of the Cyber Security Observatory META.

2023 will also see us build on the success of last year's Cyber Innovation Summits - our series of virtual events covering an extensive list of cyber security topics - and we are delighted to announce that this year we will offer **12 brand new events** covering the following topics:

- Zero Trust - Separating the Wheat from the Chaff
- Cloud Security - Securing Assets in a Cloud-First Environment
- The Future of Identity & Access Management (IAM)
- Supply Chain Security - Strategies to Mitigate Risks
- Ransomware - Steps to Help Prevent This Massive Problem
- Improving the Efficiency and Effectiveness of the SOC
- Data Protection and Privacy Laws - Global Trends
- Securing a Remote Workforce - Challenges and Best Practices
- Enabling the Human Firewall
- Effectively Managing your Attack Surface
- Leverage the Power of CTI to Improve your Security Posture
- Key Considerations for Implementing DevSecOps

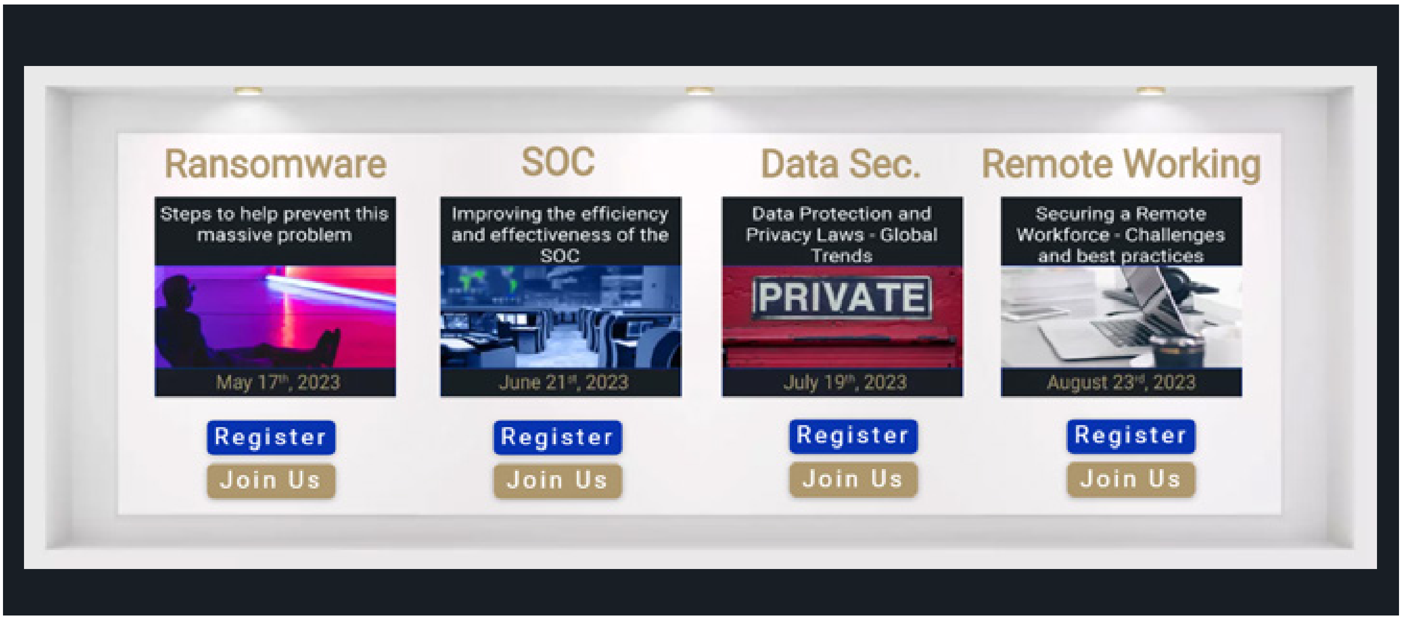


Zero Trust
Separating the wheat from the chaff
January 25th, 2023

Cloud Security
Securing assets in a Cloud-First environment
February 22nd, 2023

IAM
The future of Identity & Access Management
March 22nd, 2023

Supply Chain
Strategies to mitigate risks
April 19th, 2023

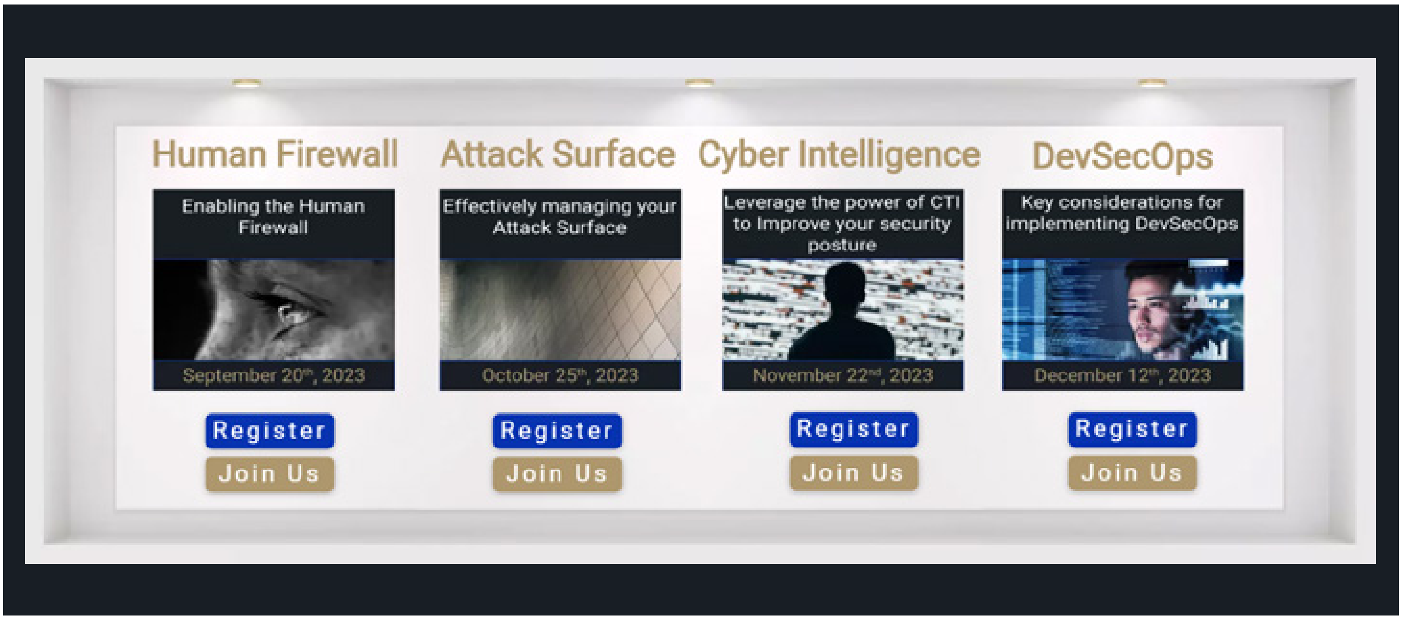


Ransomware
Steps to help prevent this massive problem
May 17th, 2023

SOC
Improving the efficiency and effectiveness of the SOC
June 21st, 2023

Data Sec.
Data Protection and Privacy Laws - Global Trends
July 19th, 2023

Remote Working
Securing a Remote Workforce - Challenges and best practices
August 23rd, 2023



Human Firewall
Enabling the Human Firewall
September 20th, 2023

Attack Surface
Effectively managing your Attack Surface
October 25th, 2023

Cyber Intelligence
Leverage the power of CTI to Improve your security posture
November 22nd, 2023

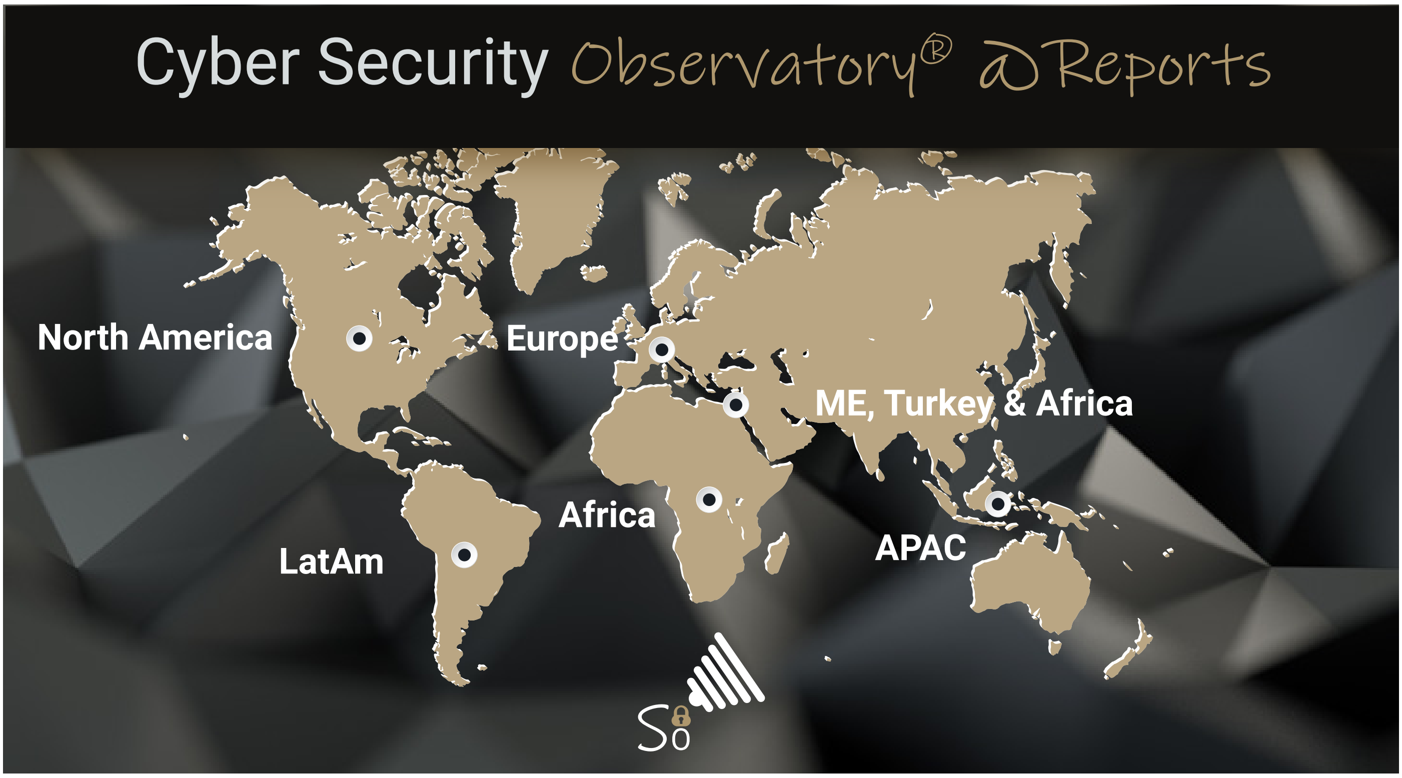
DevSecOps
Key considerations for implementing DevSecOps
December 12th, 2023

We are confident they will be of great interest and value to both CISOs and Cyber Security companies alike, and which will also support The Observatory in sharing and promoting its three key elements:

- Worldwide promotion of cybersecurity innovation
- Information sharing and collaboration across the industry
- Fostering leadership among cybersecurity practitioners

Putting together this 13th Edition Observatory North America has provided us with an opportunity to connect with yet more companies in the industry and we are grateful to them all for sharing their vision and experience.

Together with our Regional Observatories covering **North America, LATAM, Europe, Africa,** and **APAC,** we now have in place a comprehensive program on a truly global scale.



In This Edition

One of the fundamental elements of the Observatory program is the way in which we have built up close relationships with some of the most highly-regarded Cyber Leaders and Innovators in the industry. We believe this is crucial in order for us to present a trustworthy overview of the state of play within Cyber Security, regardless of the sector in which it is applied.

In this edition we are once again honored to share the views and insights of another fine selection of Cyber Leaders who have managed to spare us the time to share their thoughts on the crucial role they play within their organizations.

So we would like to extend our sincere thanks to:

Dr. Aloysius Cheang, Group Chief Security Officer @ Huawei Middle East & Central Asia, UAE
Aaditya Bhagra, Associate Partner, MEA Security Services @ IBM, UAE
Madan Mohan, Director - Technology Risk @ BDO, UAE
Enes Yildizhan, ICT Security Chief @ Tailwind Airlines, Turkey

The 4th **Edition of the Observatory META** sees us publishing articles offering the insight, vision and solutions of top companies playing a major part in the cyber security landscape across the country.

We feature articles covering the following fascinating topics:

- The Airport of Things (AoT)
- How Do You Choose the Best Cybersecurity Project For Your Company?
- Financial Cyber Drills
- Making Co-Managed Security Services a Win-Win
- Power Grid Cybersecurity, Where Are We Now?

We hope that the material included in this **Observatory META** will contribute to the goal of locking cyber security into our thinking, as we head into another year of challenges and opportunities.

The Observatory Team

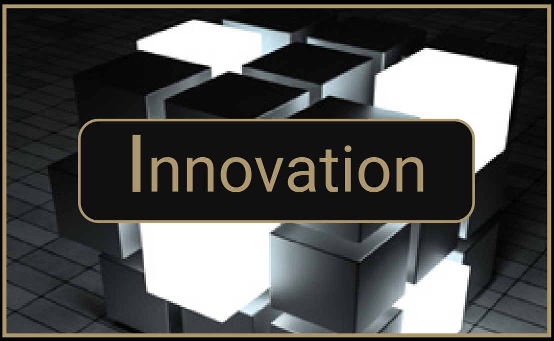
It just remains for me to thank my team here at the Observatory Program - Co-editor, Maite Ortega, German Duarte, our CTO, our Research Manager and Consulting Director, Alicia Peña for their infinite patience and support in the preparation of this publication.

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


Innovation

Insight

Leadership

Resources

Training

Trends

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

Resources

The CyberSlide

Definition and Statistics

The CyberSlide

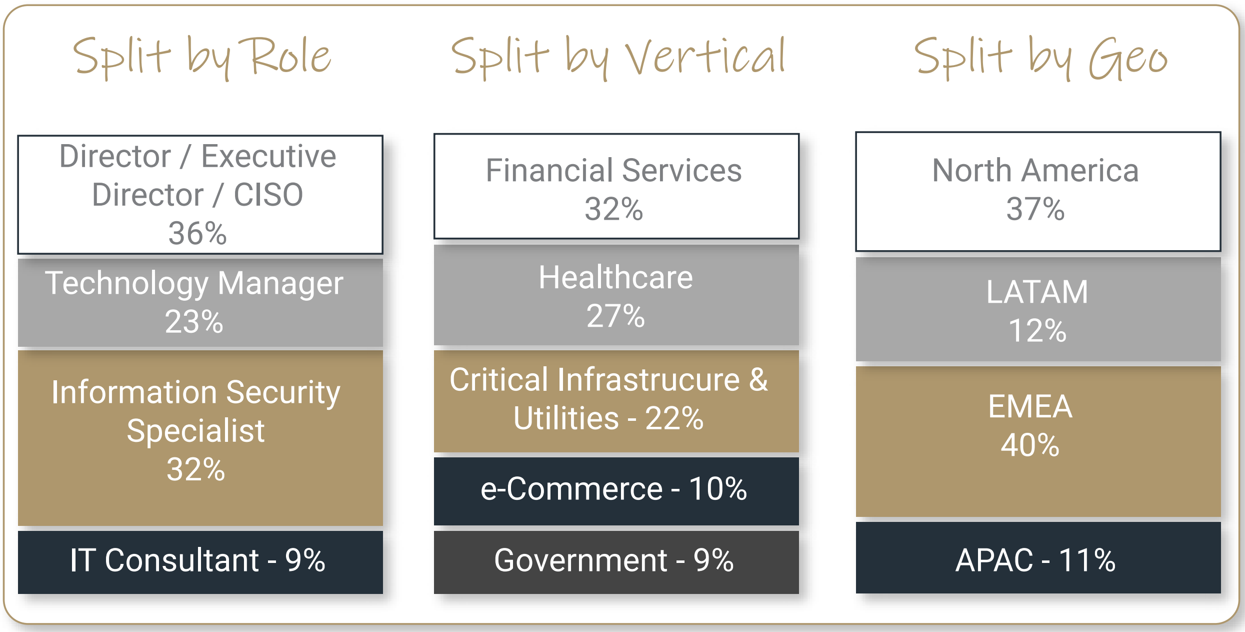
The CyberSlide is dedicated to supporting the extensive cybersecurity market active within the Cyberslide's country, but which has a truly global impact. Cybersecurity has a key part to play not only from the perspective of innovative startups looking to get a foothold in the industry, but also for those 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.



Split by Role

Director / Executive Director / CISO 36%

Technology Manager 23%

Information Security Specialist 32%

IT Consultant - 9%

Split by Vertical

Financial Services 32%

Healthcare 27%

Critical Infrastrucure & Utilities - 22%

e-Commerce - 10%

Government - 9%

Split by Geo

North America 37%

LATAM 12%

EMEA 40%

APAC - 11%

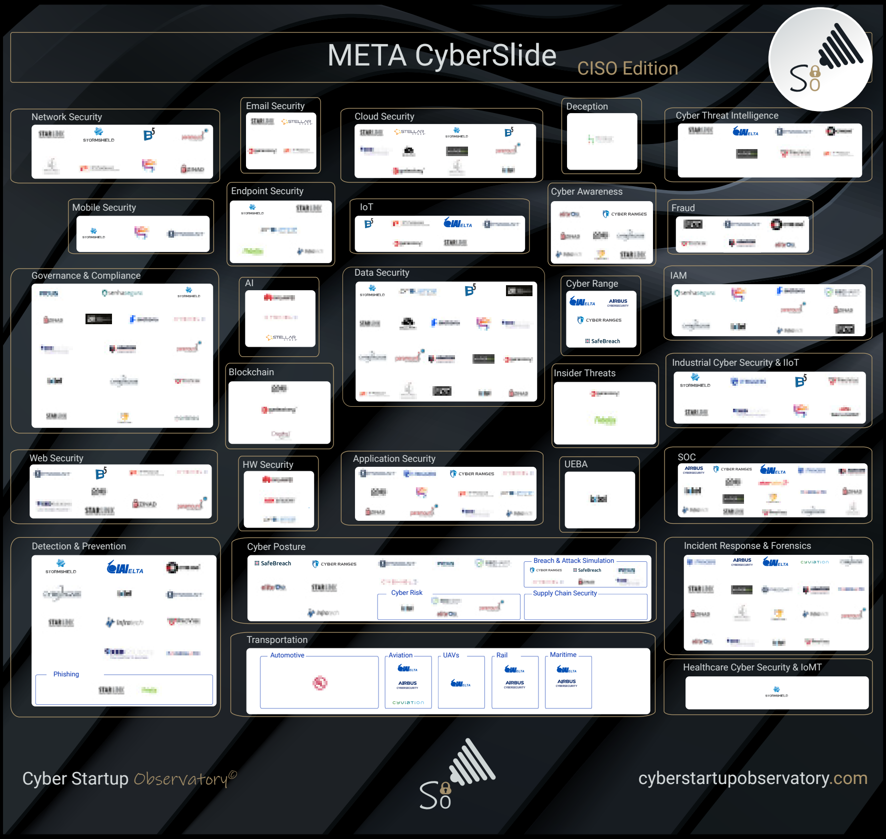
Resources

The META CyberSlide

Product Companies

META CyberSlide

Please click on the image below to download in Press Quality PDF:



META CyberSlide CISO Edition

Network Security

Email Security

Cloud Security

Deception

Cyber Threat Intelligence

Mobile Security

Endpoint Security

IoT

Cyber Awareness

Fraud

Governance & Compliance

AI

Data Security

Cyber Range

IAM

Blockchain

Insider Threats

Industrial Cyber Security & IIoT

Web Security

HW Security

Application Security

UEBA

SOC

Detection & Prevention

Phishing

Cyber Posture

Breach & Attack Simulation

Cyber Risk

Supply Chain Security

Incident Response & Forensics

Transportation

Automotive

Aviation

UAVs

Rail

Maritime

Healthcare Cyber Security & IoMT

Cyber Startup Observatory©

cyberstartupobservatory.com

META CyberSlide

- CISO Edition (100+ Product Companies)
- 90% Startups, 10% Scaleups
- Updated & Promoted Weekly Globally
- Available for download in Press Quality PDF
- Companies featured in our Global Search Engine for Cyber Companies, the @CSOfinder

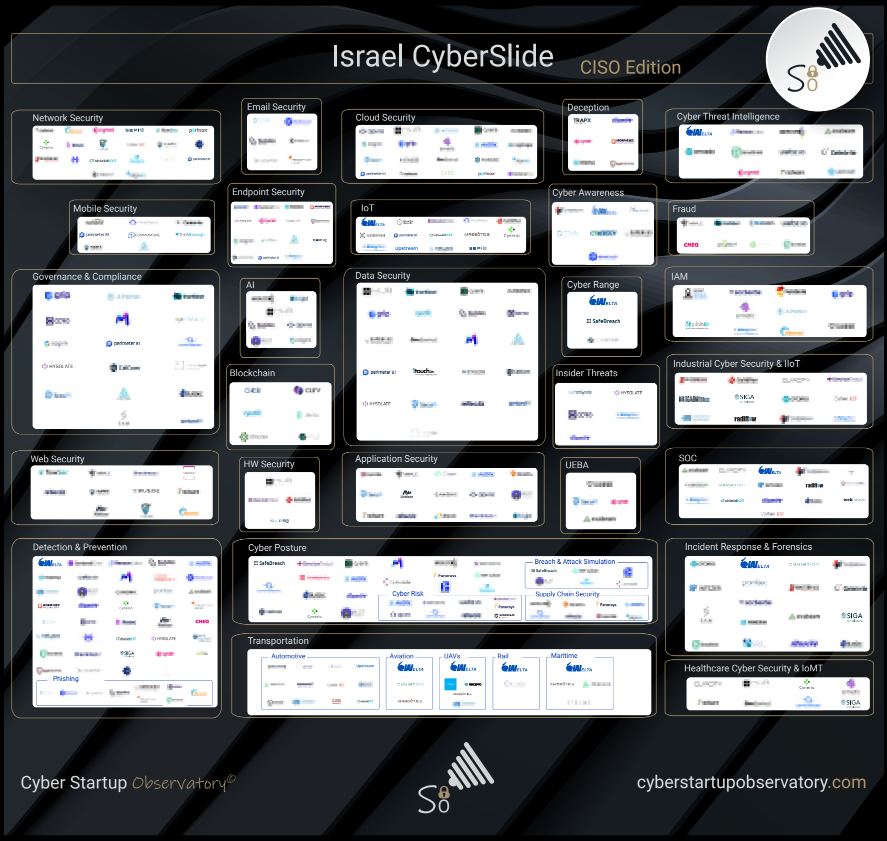
Resources

The Israel CyberSlide

Product Companies

Israel CyberSlide

Please click on the image below to download in Press Quality PDF:



Israel CyberSlide

- CISO Edition (200+ Product Companies)
- 90% Startups, 10% Scaleups
- Updated & Promoted Weekly Globally
- Available for download in Press Quality PDF
- Companies featured in our Global Search Engine for Cyber Companies, the @CSOfinder

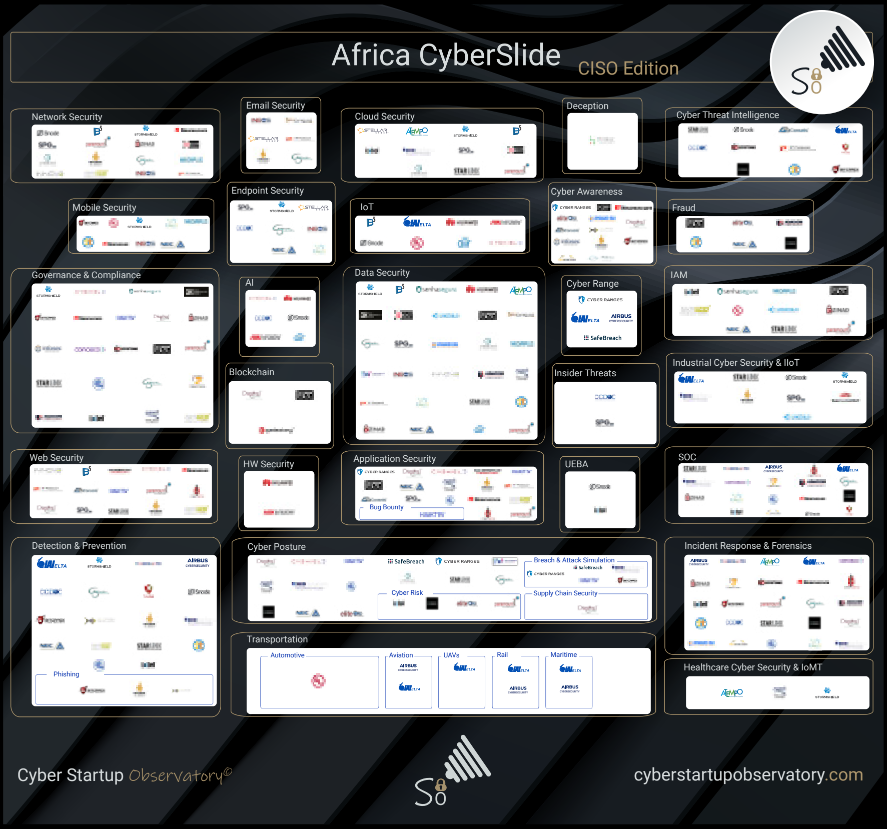
Resources

The Africa CyberSlide

Product Companies

Africa CyberSlide

Please click on the image below to download in Press Quality PDF:



Africa CyberSlide CISO Edition

Network Security

Email Security

Cloud Security

Deception

Cyber Threat Intelligence

Mobile Security

Endpoint Security

IoT

Cyber Awareness

Fraud

Governance & Compliance

AI

Data Security

Cyber Range

IAM

Blockchain

Insider Threats

Industrial Cyber Security & IIoT

Web Security

HW Security

Application Security

Bug Bounty

UEBA

SOC

Detection & Prevention

Phishing

Cyber Posture

Breach & Attack Simulation

Cyber Risk

Supply Chain Security

Incident Response & Forensics

Transportation

Automotive

Aviation

UAVs

Rail

Maritime

Healthcare Cyber Security & IoMT

Cyber Startup Observatory©

cyberstartupobservatory.com

Africa CyberSlide

- CISO Edition (100+ Product Companies)
- 90% Startups, 10% Scaleups
- Updated & Promoted Weekly Globally
- Available for download in Press Quality PDF
- Companies featured in our Global Search Engine for Cyber Companies, the @CSOfinder

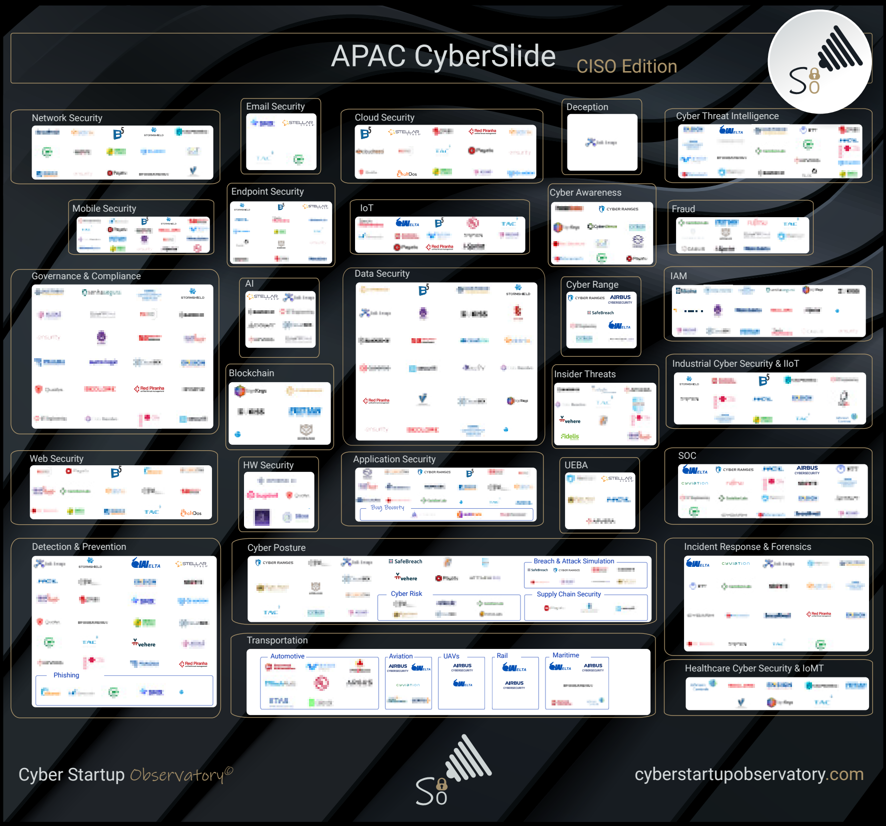
Resources

The APAC CyberSlide

Product Companies

APAC CyberSlide

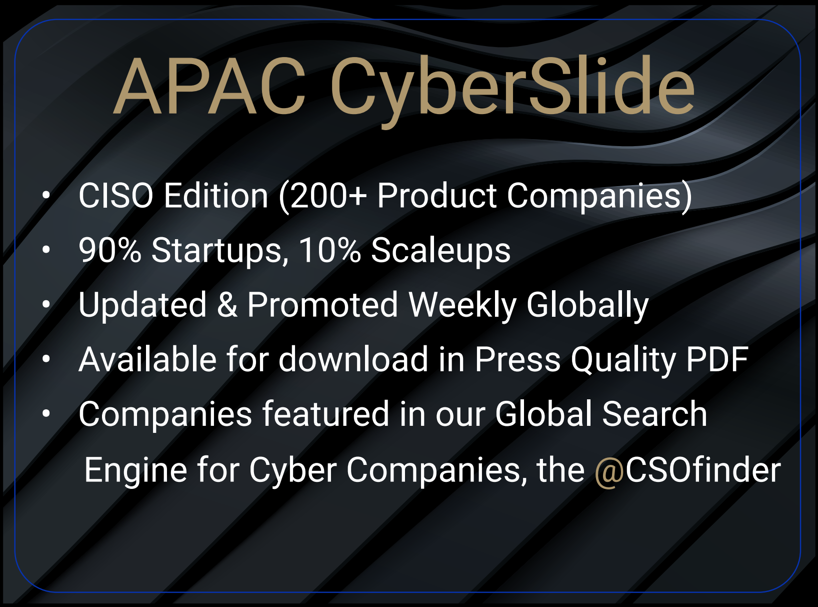
Please click on the image below to download in Press Quality PDF:



APAC CyberSlide CISO Edition

Cyber Startup Observatory©

cyberstartupobservatory.com



APAC CyberSlide

- CISO Edition (200+ Product Companies)
- 90% Startups, 10% Scaleups
- Updated & Promoted Weekly Globally
- Available for download in Press Quality PDF
- Companies featured in our Global Search Engine for Cyber Companies, the @CSOfinder

Insight

Jose Monteagudo

Founder & Chief Analyst @ Cyber Startup Observatory

The Airport of Things (AoT)

The Airport of Things (AoT)

Author: Jose Monteagudo, Founder & Chief Analyst @ Cyber Startup Observatory

At a glance

- 4 minute read
- Background
- Understanding the role of IoT and IIoT devices
- Summary and Conclusions
- About the author

Background

Airports all around the world have experienced a deep transformation during recent years.

Connectivity has been implemented in almost every aspect of the airport daily activity and procedures leading to:

- **Substantially improved passenger and employee experience** and convenience by offering self-services, avoiding queues, providing timely notifications, connectivity and collaboration, leisure, congestion management, digital guided navigation, shopping and retail offers, to name just a few.

- **Operational excellence and efficiency** for shared services facilities.

- **Drive workforce productivity** and real-time collaboration for ground staff.

- **Innovative, value-added revenue generating services.**

- **Asset tracking with improved transparency, visibility and reliability.**

- **Sustainability:** smart energy, emissions, water and waste management.

- **Smart security,** including biometrics, track & trace systems, video surveillance & analytics, smart security gates and smart healthcare services.

The eruption of the IoT has been massive too, adding new functionality, simplifying monitoring, maintenance and operations of traditional airport and aviation systems.

But there is always a price to pay. Increased connectivity through the digitization of everything and the ubiquity of IoT devices is a double-edged sword and although it enables new security solutions as referred to previously, it also creates new threats by increasing the attack surface.

Moreover, IoT devices, due to their limited hardware and software capabilities, might pose a substantial risk if not managed properly. The aviation industry is aware of these cybersecurity challenges and is working very hard to address them.

Understanding the role of IoT and IIoT devices

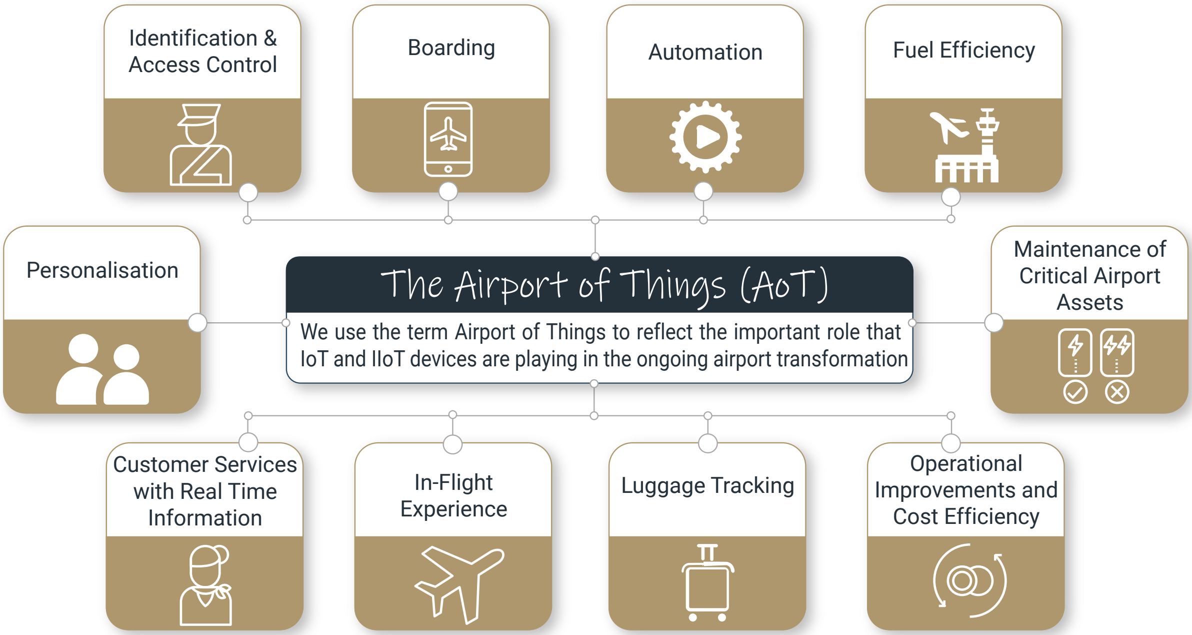
The airport represents a key element in overall aviation industry safety and security. In this article we are going to shed some light on the deep transformation that is taking place at the airports, involving a fascinating journey from traditional legacy infrastructures to state of the art Airports of Things (AoT).

We use the term Airport of Things to reflect the important role that IoT and IIoT devices are playing in this transformation.

The potential opportunities for IoT to add value to the airport ecosystem are countless improving passenger experience while at the same time increasing revenue for the airlines, operators and concessionaries. Let's take a look:

- **Streamlined access control, passenger identification and departure processes:** use of advanced biometrics will simplify identification, even eradicating the need for travel documents. A series of biometric touchpoints which recognize passengers at any checkpoint such as baggage drops, security checkpoints and immigration clearance. This will hugely simplify airport access, streamlining security checkpoints, reducing queues, as well as optimizing check-in processes.

- **Personalisation:** leveraging IoT sensors and devices, biometrics, behavioral analytics and geolocation, airports will be able to deliver a completely personalized experience to both passengers and employees at the airport.


Identification & Access Control
Boarding
Automation
Fuel Efficiency
Personalisation
The Airport of Things (AoT)
We use the term Airport of Things to reflect the important role that IoT and IIoT devices are playing in the ongoing airport transformation
Maintenance of Critical Airport Assets
Customer Services with Real Time Information
In-Flight Experience
Luggage Tracking
Operational Improvements and Cost Efficiency

- **Improve customer service with real-time, relevant Information:** passengers can get real-time updates about estimated waiting time at security lines, locations of specific airline check-in counters, gates, baggage belts, restaurants, shops, etc. Moreover, detailed and accurate information about flight delays, parking availability, emergencies could be delivered in a convenient and personalized way. The opportunities to reduce friction at the airport and to boost the customer experience are countless.

- **Boarding:** will become a self-service process with passengers just needing to pass through an automatic electronic barrier.

- **In-Flight experience:** IoT sensors might be integrated in the aircraft seats, measuring multiple passenger variables to increase safety and comfort level.

- **Luggage tracking:** IoT beacons and RFID tag technology might be used for luggage tracking providing real-time information about luggage location.

- **Operational improvements and cost efficiency:** IoT and IIoT will simplify the management and maintenance of a variety of devices such as heating, ventilation and air conditioning (HVAC) systems, information boards, kiosks etc, offering greater visibility on an enterprise-wide scale.

- **Maintenance of critical airport assets:** sensors on critical airplane and airport elements will be able to provide maintenance staff with real-time information with regards to the part status and when it needs to be replaced or repaired.

- Fuel efficiency: IoT applications might improve the overall fuel costs and consumption, which have substantial impact in the airline's bottom line.

- Automation: improving operational efficiency, lowering costs and simplifying the overall operation.

Summary and Conclusions

The opportunity to leverage IoT and IIoT technologies to modernize airports is obvious. They are playing a key role now and will continue being instrumental in the transition to the Smart Airport or the Airport of Things as we purposely named it.

Nevertheless, leveraging these opportunities brings new challenges and risks.

We need to assure that these devices are properly secured before they are plugged in and the risk of an increased attack surface, properly addressed.

About the author

Jose Monteagudo is the Editor-in-Chief of the Cyber Startup Observatory, a project he founded in 2018 after more than 20 years in product, consulting and leadership roles in technology companies in the US, UK, France, Japan, Singapore and Spain. He holds a Bsc in Aeronautical Engineering and an MBA from ESIC.

Leadership

Dr. Aloysius Cheang

Chief Security Officer, Huawei
Middle East & Central Asia

Video Interview

Cyber Security Leaders

Please click on the image below to watch the video

Dr. Aloysius Cheang

Chief Security Officer, Huawei Middle East & Central Asia

Interviewed by

Jose Monteagudo

Editor-in-Chief @ Cyber Startup Observatory

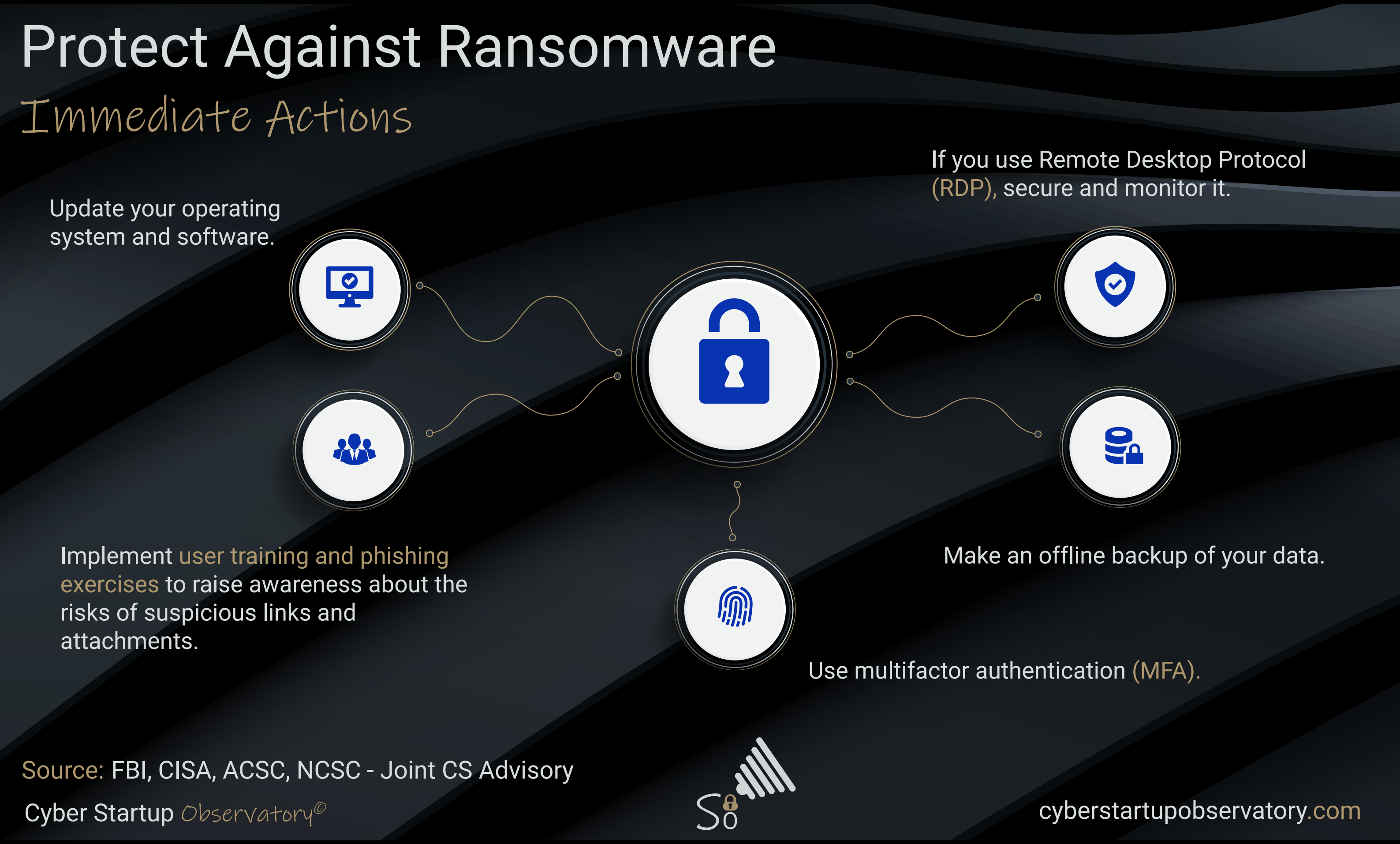
HUAWEI

Resources

Video Infographic

Protect Against Ransomware -
Immediate Actions

Protect Against Ransomware - Immediate Actions



Protect Against Ransomware

Immediate Actions

Update your operating system and software.

Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.

If you use Remote Desktop Protocol (RDP), secure and monitor it.

Make an offline backup of your data.

Use multifactor authentication (MFA).

Source: FBI, CISA, ACSC, NCSC - Joint CS Advisory

Cyber Startup Observatory©

cyberstartupobservatory.com

Please follow the link below to visit all our Video Infographics:

Cyber Startup Observatory - Video Infographics

Insight

senhasegura

How Do You Choose the Best Cybersecurity Project For Your Company?

How Do You Choose the Best Cybersecurity Project For Your Company?

Author: senhasegura

At a glance

- 10 minute read
- Cybersecurity Project: What Is It, and What Is Its Importance?
- The Five Types of Cybersecurity
- People, Processes, and Technology
- Guidelines for Prioritizing Cyber Security Projects

senhasegura

The IBM Cost of a Data Breach 2022 report brought a lot of information that shows the importance of choosing a good cybersecurity project for your organization.

According to information extracted from this document which included interviews with more than 3,600 people working in companies that had their data violated, it was possible to find alarming conclusions.

First, 83% of the organizations surveyed suffered some kind of breach between March 2021 and March 2022. Also, 60% of these attacks increased prices for customers.

It has also been identified that 79% of critical infrastructure organizations have not implemented a zero-trust plan to prevent cyber threats, and 19% of violations occur due to a compromised business partner.

Faced with so many digital security gaps, it can be diffcult to know where to start deploying a cybersecurity project. Therefore, we address this issue here. To facilitate your reading, we divided our text into topics. These are:

- About Cybersecurity
- Importance of Cybersecurity
- Cybersecurity Project: What Is It, and What Is Its Importance?
- What Are the Five Types of Cybersecurity?
- People, Processes, and Technologies: Crucial Elements for the Success of Every Cybersecurity Project
- Guidelines for Prioritizing Cyber Security Projects within a Company
- Key Cyber Threats Faced by Companies
- About senhasegura

Conclusion Enjoy the read!

About Cybersecurity

When we talk about cybersecurity, we refer to a set of technologies, procedures, and methods used to prevent attacks on devices, programs, data, and networks, avoiding the activity of hackers and ensuring the privacy of a company's data, which must be protected from insider and external threats and natural disasters.

However, accelerated by the Covid-19 pandemic, digital transformation has brought several vulnerabilities, such as those related to remote work. As a result, there was a significant increase in data leaks, phishing emails, and account invasions.

Importance of Cybersecurity

Currently, processes in companies are migrating to the online world due to digital transformation, which can "facilitate" the loss of information of great importance to a business.

Thus, organizations need to invest in cybersecurity in order to ensure their operations and prevent threats, such as malware, viruses, and phishing.

One should also be aware that malicious attackers have been improving their techniques over time, so it is increasingly challenging to maintain data security and avoid compromised business.

Another novelty is data protection laws, which have been holding organizations accountable for the exposure of sensitive information from their customers, employees, and business partners, generating million-dollar sanctions.

In practice, these legislations have several requirements to be respected in order to avoid accidental or intentional data loss.

That is, investing in a good cybersecurity project is the recommended measure to avoid inconvenience, financial losses, loss of credibility, and closure of companies.

Cybersecurity Project: What Is It, and What Is Its Importance?

Cybersecurity projects are aimed at promoting digital security within any company. Its importance lies in the possibility of avoiding cyber threats, such as hacker invasions. It also contributes to the fact that errors -whether deliberate or not, of employees or third parties – have fewer impacts on the organization and reduce the possibility of losses, such as: loss of data, credibility, millionaire sanctions imposed by data protection laws, which can even cause the end of a business. And in small companies, this is even more crucial: according to a Cisco study, 60% of organizations affected by a cyberattack shut down operations within 6 months of the incident.

What Are the Five Types of Cybersecurity?

There are five types of cybersecurity. These are:

- Critical Infrastructure Security;
- Application Security;
- Network Security;
- Cloud Security; and
- Internet of Things (IoT) Security. Check out each of them in detail below:

Critical Infrastructure Security

What Is It?

When talking about critical infrastructure security, we refer to the area that contemplates the security of systems, networks, and assets in industries that are essential to ensure the security of a country's economy, health, and public services. These sectors include the chemical, communications, utilities, energy, and financial industries.

What Are the Challenges?

A major challenge for critical infrastructure is the security issues its systems present versus the limited protection features.

Application Security

What Is It?

Application security is essential as these programs have increasingly become targets for hackers. It consists of practices adopted to make them more secure, which occurs during their development and then after their implementation.

What Are the Challenges?

Ensuring application security requires tracking all the tools developed for these applications. It is also important to be aware of the future needs of a company, which may require software aimed at a more complex infrastructure.

Network Security

What Is It?

Network security is a term that refers to hardware and software solutions, as well as procedures aimed at protecting the network and data against cyberattacks. In practice, this concept includes network analysis, application security, access control, and antivirus software, among other factors.

What Are the Challenges?

The main challenge of network security is to maintain protection in increasingly complex structures, with a large volume of cyber threats and several functionalities used in corporations, which also represent new problems.

Cloud Security

What Is It?

As companies suffer the impact of digital transformation, they become more dependent on cloud solutions and need to adopt measures that ensure digital security in this context.

This is because outsourced providers may even be responsible for infrastructure management, but the accountability for any exposed data remains with the organization as well.

What Are the Challenges?

The challenges of companies adopting cloud solutions are related to the ability to meet security criteria in a dynamic environment, which can generate a lack of visibility in accessing and using data.

Internet of Things (IoT) Security

What Is It?

Internet of things security is associated with protecting devices connected directly to the cloud in gadgets, such as surveillance cameras. Its function is to protect designed devices, without taking into account aspects of cybersecurity and data protection.

What Are the Challenges?

The greatest challenge associated with the internet of things security refers to human activity. In practice, with the increased connectivity of these devices, it is necessary to instruct users on the change of default passwords and the need for updates, for example. On the other hand, many users do not see these devices as targets of attacks and end up ignoring best security practices during their development and use.

People, Processes, and Technologies: Crucial Elements for the Success of Every Cybersecurity Project

People

When it comes to cybersecurity projects, investing in cutting-edge technology is not enough. It is essential to train users to respect security protocols and ensure the protection of company data.

In practice, your employees increase security risks in a variety of ways. Among them, we can highlight:

- Clicking on URLs and Opening Suspicious Emails

It is necessary to make your employees aware of the risks involved in this practice and encourage the exclusion of emails from fake addresses to protect sensitive data.

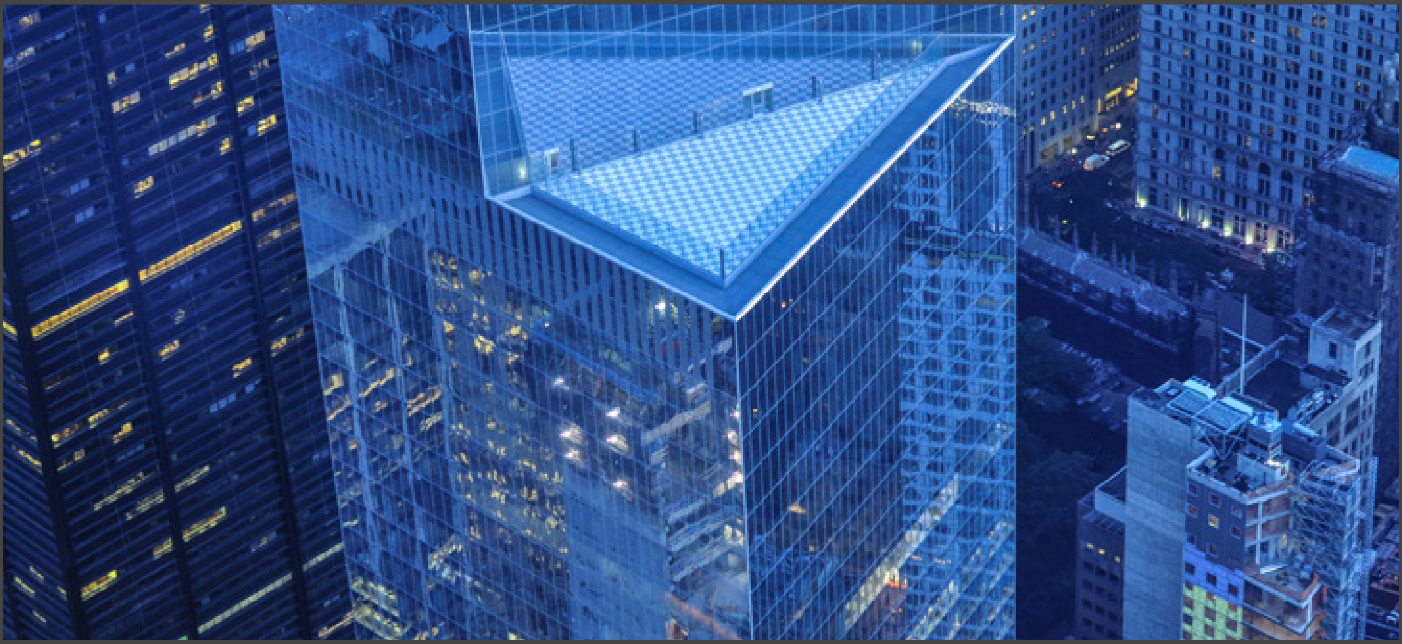
- Keeping the Same Password for a Long Period

To ensure the security of your company, employees' passwords must be changed regularly. In addition, strong combinations should be used, and it is not recommended to reuse the same password in different services.

Due to the difficulty in memorizing so many passwords, we also recommend the use of a password vault, which will only require the memorization of a single code.

- Personal Browsing

Many people use the devices of their companies for personal purposes, such as accessing social media, shopping, or paying bills. The big problem is that this behavior facilitates the work of malicious agents who want to collect information. Therefore, ask your employees to use their own devices, not corporate ones, for personal browsing.



- Lack of Backups

Many people still fail to perform backups when finishing their tasks. Nevertheless, it is of paramount importance to back up the system files. So, employees should understand they need the help of the IT team with these functions.

- Unattended Devices

Leaving devices on desks unattended and without blocking them is a fairly common practice, which can also cause damage to the security of a company. For this reason, it is essential to make employees aware of the importance of preserving data contained in these devices and maintaining their control.

Processes

Information security professionals use numerous processes to protect sensitive data. In practice, they need to identify and combat cyber threats, protecting information and responding to incidents.

Besides being implemented, these processes must be documented to save time and financial resources, and preserve customer confidence in cases of cyberattacks.

To counter cybersecurity-related risks, we recommend using the Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce, after former U.S. President Barack Obama signed an executive order in 2014.

Technology

After the deployment of security processes, it is indispensable to assess the tools available to avoid cyber threats.

For this, you must consider two types of technology: those that will help you prevent and combat attacks, such as antivirus, DNS filtering, and malware protection; and those that need protection, including computers, routers, and the cloud.

Previously, we could rely on security perimeters. Now, migration to cloud environments, remote work, and policies like Bring Your Own Device (BYOD) have made it easier for hackers to work.

Cybersecurity Project: What Is It, and What Is Its Importance?

A cybersecurity project is essential to not overwhelm IT staff with unnecessary work and to ensure the company's ability to deal with a cyberattack.

However, to create and run your cybersecurity project, you must take some action. They are as follows:

Understanding Your Company's Goals

Each organization has its strategic goals, which should guide the creation of the cybersecurity project. Therefore, it is important to evaluate the company's vision and its business and cybersecurity strategies.

This information will provide a basis for the development of the project and will be a guide to gradually know if it is, in fact, efficient.

To understand the strategic goals of the company, read documents related to the subject and talk to top management to know their priorities.

Discovering the Reason Behind the Project

Cybersecurity projects can be motivated by several reasons, although all of them need to prevent and combat cyber incidents in common.

In practice, the project can be an awareness and training campaign on cybersecurity, the implementation or updating of a security system, compliance with new laws and regulations, etc.

Understanding what the project's motivation is will certainly contribute to establishing priorities, directly impacting the company's operations.

Determining the Value of the Project

Here, when we talk about value, we are referring to the importance of a cybersecurity project for an organization.

That is, it is convenient to analyze how it will impact stakeholders and what its real importance is to the business. A project that adds great value must necessarily be prioritized.

Analyzing the Urgency

It is important to assess the urgency of the cybersecurity project to determine whether it should be prioritized or can wait. But remember that priorities can and should be modified as changes occur.

Detailing the Aspects that Affect the Project's Success

A successful cybersecurity project depends on a number of factors, including budgets, deadlines, and return on investment (ROI), among other things.

On the other hand, it is often impossible to execute a project due to unfavorable circumstances. Therefore, it is advisable to know what can affect the project's success in advance.

Ranking the Cybersecurity Project According to the Priority

With the information on goals, objectives, and possibilities of success in hand, it is time to establish an order of priorities through an overall classification, which can be score-based.

Defining How Many Projects Can Be Executed at a Time

Probably, the organization will not be able to assume all priority projects at once. Thus, the solution is to work on them in a phased manner, creating a queue of plans to execute.

Another recommendation is to run the fastest ones first and then the ones that require more time and effort.

Sharing Findings with Top Management

Before starting the cybersecurity project, it is essential to meet with leaders and share the information gathered. This is because the findings can serve as insights to change the order of priorities of the projects, requiring top management to be on board.

Working Flexibly

Working with cybersecurity projects requires flexibility, after all, priorities can be modified according to context. By the way, this occurred in most companies after the beginning of Covid-19, which accelerated the mass adoption of remote work and brought new demands to security teams.

Key Cyber Threats Faced by Companies

The following are the main cyber threats that should be considered by a cybersecurity project:

- Ransomware;
- Phishing;
- Attacks on Mobile Devices;
- Attacks Using QR Codes;
- Denial-of-Service (DDoS) Attacks; and
- LotL and AVT Attacks.

See the detailed explanation of each of them below:

Ransomware

This type of cybercrime works like this: the attacker blocks a network or system and asks for millionaire amounts in exchange for the release of information, which may not be returned, but sold to other criminals. Due to the lack of efficient cybersecurity mechanisms in companies, this tactic is very common.

Phishing

Another common crime in the virtual environment is phishing, which consists of sending counterfeit emails, and pretending to be a legitimate organization. With this, malicious agents convince their victims to share personal information or take action to their benefit. There are also some types of very sophisticated phishing attacks, such as very realistic audio recordings produced through artificial intelligence.

Attacks on Mobile Devices

With many people working remotely, the use of personal devices for corporate purposes and the use of corporate devices for personal purposes tend to occur more frequently.

This increases security vulnerabilities, especially in the face of malware attacks on devices.

Attacks Using QR Codes

Currently, cybercriminals use QR Codes to deploy malware applications, infecting their victims' phones and stealing their bank details.

For this reason, it is advisable to check the code provided by the company before accessing it.

Denial-of-Service (DDoS) Attacks

This type of attack occurs when the hacker overloads a machine with traffic, disrupting its normal operation and making a service unavailable to users. In practice, the attack is performed through a single computer.

LotL and AVT Attacks

Less known, Living off the Land (LotL) attacks do not need to create malicious files to access a company's systems because they use gateways that already exist.

Advanced Volatile Threat (AVT) attacks allow access to an organization's data as quickly as possible.

About senhasegura

We, from senhasegura, are part of MT4 Tecnologia, a group of companies specializing in digital security, founded in 2001 and operating in more than 50 countries.

Our main objective is to ensure digital sovereignty and security for our clients, granting control over privileged actions and data and avoiding theft and leaks of information.

For this, we follow the lifecycle of privileged access management through machine automation, before, during, and after accesses.

These are also our commitments:

- Avoid interruptions in the activities of companies, which may impair their performance;
- Automatically audit the use of privileges;

- Automatically audit privileged changes to identify privilege abuses;
- Provide advanced PAM solutions;
- Reduce cyber risks;
- Bring organizations into compliance with audit criteria and standards such as HIPAA, PCI DSS,
- ISO 27001, and Sarbanes-Oxley.

Conclusion

In this article, you saw that:

- Cybersecurity is a set of technologies, procedures, and methods used to prevent cyberattacks;
- Digital transformation has brought new vulnerabilities to IT structures;
- Companies should invest in cybersecurity to prevent threats, such as malware, viruses, and phishing;
- Data protection laws hold organizations accountable for the exposure of sensitive information of their customers, employees, and business partners;
- Cybersecurity projects are aimed at promoting digital security within any company;
- There are five types of cybersecurity: critical infrastructure security, application security, network security, cloud security, and Internet of Things (IoT) security;
- People, processes, and technology stand out among the crucial elements for the success of a cybersecurity project;
- To define the priorities of cybersecurity projects within a company, one needs to understand the organization's objectives, find out the reason for each project, determine its value, assess its urgency, detail aspects that interfere with its success, rank projects in order of priority, define how many projects it is possible to execute at a time, share the findings with top management, and work flexibly;
- The main threats faced by companies are ransomware, phishing, mobile device attacks, attacks using QR Codes, denial-of-service (DDoS) attacks, and LotL and AVT attacks.

Leadership

Aaditya Bhagra

Associate Partner, MEA Security Services @ IBM

Aaditya Bhagra

Associate Partner, MEA Security Services @ IBM

Addy is an accomplished cybersecurity and consulting leader with a wealth of experience spanning over 13+ years.

He is currently an Associate Partner with IBM Security Services in the Middle East & Africa, having previously held a range of positions with leading consulting and industry organizations including Accenture, PwC, AXA, and AOL Time Warner. He has strong cross-domain functional skills and is an expert in cyber security strategy, cyber security transformation, cloud security, and cyber incident response.

Some of his notable accomplishments include serving as interim CSO for a major insurance company in the Netherlands, where he established their information security function. Building and operationalizing the cyber incident response plan for a leading European aviation company and leading the network security transformation for a large financial services firm across 20 global locations. Since joining IBM, Addy has played an instrumental role in establishing their security transformation practice in the UK&I and has led several complex security transformation programs for clients within the Financial Services and Aviation industries.

Addy holds a double Master's in Management from The London School of Economics and Political Science and Bocconi University, as well as a degree in Computer Science and Engineering from RNS Institute of Technology, Bangalore. He is also a passionate mentor and is committed to developing high-performing talent in consulting and cybersecurity.

What new cybersecurity challenges are arising as business enterprise networks are changing and becoming more complex?

In the previous decade, cybersecurity for the most part followed a castle and moat model with a well-defined cybersecurity perimeter secured by firewalls and with data residing within a corporate datacenter.

However, the last decade has seen several paradigm shifts in technology with the advent of software defined infrastructure and networking, cloud, mobile, and edge computing, as well as in ways of working with more and more employees now working either in a hybrid or remote working model (accelerated by the COVID 19 pandemic).

These shifts have created new challenges for cybersecurity leaders, since they need to

1. **Secure users and devices accessing** corporate applications and data from multiple locations and not just within the data center.

2. **Secure applications and data** that reside across both on-premises and cloud environments (IDC predicts that by 2025, 49% of the worlds stored data will reside in public cloud environments)

3. **Secure the networks and connectivity** between these distributed systems

4. **Maintain and operate the increasing number of cybersecurity tools** required to protect the distributed environment (as per IBM, 85 is the average number of cybersecurity tools within an enterprise organization)

It also means that cybersecurity leaders can no longer rely on the old perimeter-based cybersecurity model and require a new model like Zero Trust. A Zero Trust model is based on the principles of least privilege, continuous verification and assumed breach and means that no user, device or connection is trusted.

However, depending on the organization’s current maturity, achieving a Zero Trust cybersecurity posture can be a considerably long journey. My recommendation therefore is that organizations start small and focus on a particular domain or use case that is relevant to their interests. For e.g., if you have a significantly large hybrid workforce, then focusing on securing a remote workforce may be a good Zero Trust starting point.

How would you justify cybersecurity investment to your board?

I highly recommend cyber risk quantification as a means of justifying cybersecurity investment to the Board. Whilst we have seen this being used by organizations in the Banking and Financial Services industry, I believe that the current economic landscape, competing business priorities and limited budgets has made using cyber risk quantification imperative for CISOs in all industries.

By leveraging cyber risk quantification, CISOs can put an objective dollar value against each of their cyber risks and provide the Board with a cost/benefit analysis of how the requested investments will help mitigate the risk.

Talking in dollar value terms, makes cyber risk quantification an effective language for communicating cybersecurity across the Board (which may include a diverse mix of leaders from Legal, Audit, HR, IT and Finance backgrounds) that may not necessarily understand the nuances of requested cybersecurity investment itself. It also helps cybersecurity leaders in prioritizing their own initiatives since it adds consistency and objectivity to the process.

Today organizations can leverage existing standards for quantifying cyber risk like those from the FAIR institute. There are also tools available like RiskLens and ThreatConnect that help automate cyber risk quantification and reporting. Additionally, for organizations that haven't employed cyber risk quantification in the past, utilizing the services of trusted consulting and systems integration provider is a good option to help them transform their risk management processes at scale.

Another important lever for the justification is where the cybersecurity investments directly relate to compliance with an industry regulation or standard. It's important for CISOs to communicate to the Board, the organizational costs of non-compliance and the associated financial, legal and operational impacts.

What are some of the barriers preventing organizations from implementing personal data and privacy protection initiatives?

I personally feel one of the main barriers for organizations has been the lack of understanding of this domain. This is both from a skills (i.e., resources that specialize in privacy) and from an awareness perspective (i.e., the applicable privacy laws and regulations that they need to comply with).

Moreover, whilst previously there were several data privacy laws and regulations, these did not have any associated guidelines and standards for organizations to help understand the specifics of what needed to be implemented. This has changed over the last few years and the development of standards like ISO 27701 and the NIST Privacy Framework are certainly welcome developments.

A second barrier is the lack of accountability and sponsorship for this domain (especially in organizations that may not have a Chief Privacy Officer), to establish, implement and maintain a privacy information management system. Privacy programmes require collaboration across the legal, risk, cybersecurity teams and will often fail without strong sponsorship and accountability from the top. Additionally, even with clear R&Rs and sponsorship, it is important that organizations set the right tone from the top and communicate periodically to build the culture of privacy across the organization.

Finally, another factor has been the lack of enforcement of privacy regulations in certain geographies. This has meant that certain organizations have either delayed implementing or chosen to not implement privacy related controls as part of their ongoing projects.

In an ever-changing threat landscape, how do you adapt your cybersecurity posture?

Firstly, I believe its important that both cybersecurity leaders as well as the Board are abreast of the latest cybersecurity threats to their industry as well as the organization.

These threats must be incorporated as an input to cybersecurity risk assessments as well as cybersecurity strategy planning, so that leaders can prioritize their initiatives accordingly.

Secondly, organizations must ensure that they have an architecture that is resilient to cybersecurity attacks and follows a Zero Trust model. This means having defense in depth with multiple layers of cybersecurity controls and high availability to reduce the impact of a successful attack, as well as wrapping cybersecurity with context around every user, every device and every connection.

Organizations must also ensure that they have well documented cyber incident response plans and playbooks in place for the most prevalent information cybersecurity threat vectors like phishing, ransomware, web exploitation etc. It is also important that they regularly battle test these plans both through technical adversary simulation (red, blue, purple teaming) and crisis simulation exercises. Use of breach and attack simulation tools is also a good way to regularly identify and remediate exploitable weaknesses in the organizations IT and cloud environment.

Finally, humans can be both the strongest or weakest link in the cybersecurity chain, and organizations must invest in regular cybersecurity awareness of all their employees, contractors and third parties.

When pushing forward with digital transformation, many companies will migrate to the cloud. What are the main risks to consider when doing so?

Data residency risk is crucial, and it's important that organizations understand where the cloud providers will store the data and whether this is in line with the local country regulations and organizational requirements.

Another significant risk is cloud security and specifically cloud misconfiguration. Whilst speed of deployment and lower costs are a promised benefit, rapid deployment without ensuring the security of cloud landing zones, and virtual and containerized cloud workloads, can often lead to painful data breaches. In fact, cloud misconfiguration has been one of the notable reasons for cloud related data breaches in the recent years. Organizations must therefore ensure they establish secure landing zones for cloud deployments and build security into their DevOps processes on the cloud. Utilizing an industry standard like CSA Cloud Controls Matrix for gap analysis can be a useful exercise in understanding cloud security control gaps for cloud from a people, process and technology perspective.

Additionally, organization risk loss of some control when moving to the cloud. Depending on the cloud deployment model (IaaS, PaaS and SaaS), organizations will need to operate on a shared responsibility model with the cloud provider and must ensure that there are no responsibility gaps between them and the provider. Vendor lock-in is another risk associated with relying on a single cloud provider. If organizations rely heavily on a single cloud provider, they could risk becoming locked in and may find it difficult or expensive to switch to a different provider if needed. Organizations therefore need to consider using a multi-cloud or hybrid cloud approach to avoid vendor lock-in.

Lack of skills is another risk that organizations need to plan for when moving to the cloud. Depending on the market maturity in their region, organizations may need to either hire or upskill their own resources for managing and operating their cloud resources.

Finally, while cloud migration offers cost savings, it can also lead to unexpected expenses if the cloud resources are not managed properly. To manage costs effectively, organizations must have a clear understanding of their cloud expenses and implement cloud Financial Operation (FinOps) management strategies for monitoring and optimization.

What do you think are the right steps to reduce cyber risks when working with third parties?

To effectively manage third party risks, I would firstly recommend that organizations clearly establish their own cybersecurity and compliance requirements. When working with third parties, it is important that these cybersecurity and regulatory compliance requirements are mandated as part of the contracts (including right to audit) and are clearly communicated to them. For e.g., if the third party will process any personal data of your customers, then your contract must clearly outline the need to comply with the relevant privacy regulation.

Organizations must also establish a third-party risk management framework and regularly conduct third party risk assessments for all their vendors. The third-party risk assessment questionnaire must also be part of your vendor onboarding process. Auditing third parties may be necessary if they implement changes to their IT environment that might introduce new cybersecurity risks to your organization.

From an access perspective, third party access to your organization's systems and data must be limited to only what is necessary and must be granted on a need-to-know basis.

Additionally, from a data perspective, organizations must continuously monitor where their data resides, how it is secured and what it is being used for. Organizations must also be clearly aware if any of their data flows from third parties to other fourth parties, and what if any risks it may create for them.

Finally, organizations must include and test their third-party incident response procedures, escalation protocols, and communication plans as part of their overall cyber incident response plan.

Closing Statement

In order to keep up with the changing cybersecurity threat landscape, security leaders need to periodically review and update their own cybersecurity strategy to ensure it prioritizes initiatives that help counter the evolving threats to their organizational assets.

Leveraging a zero-trust security model, having a cyber resilient security architecture, fostering a security aware culture and regularly battle testing their cyber preparedness are some of the key steps that will help security leaders in continuing to safeguard their organizations.

Disclaimer

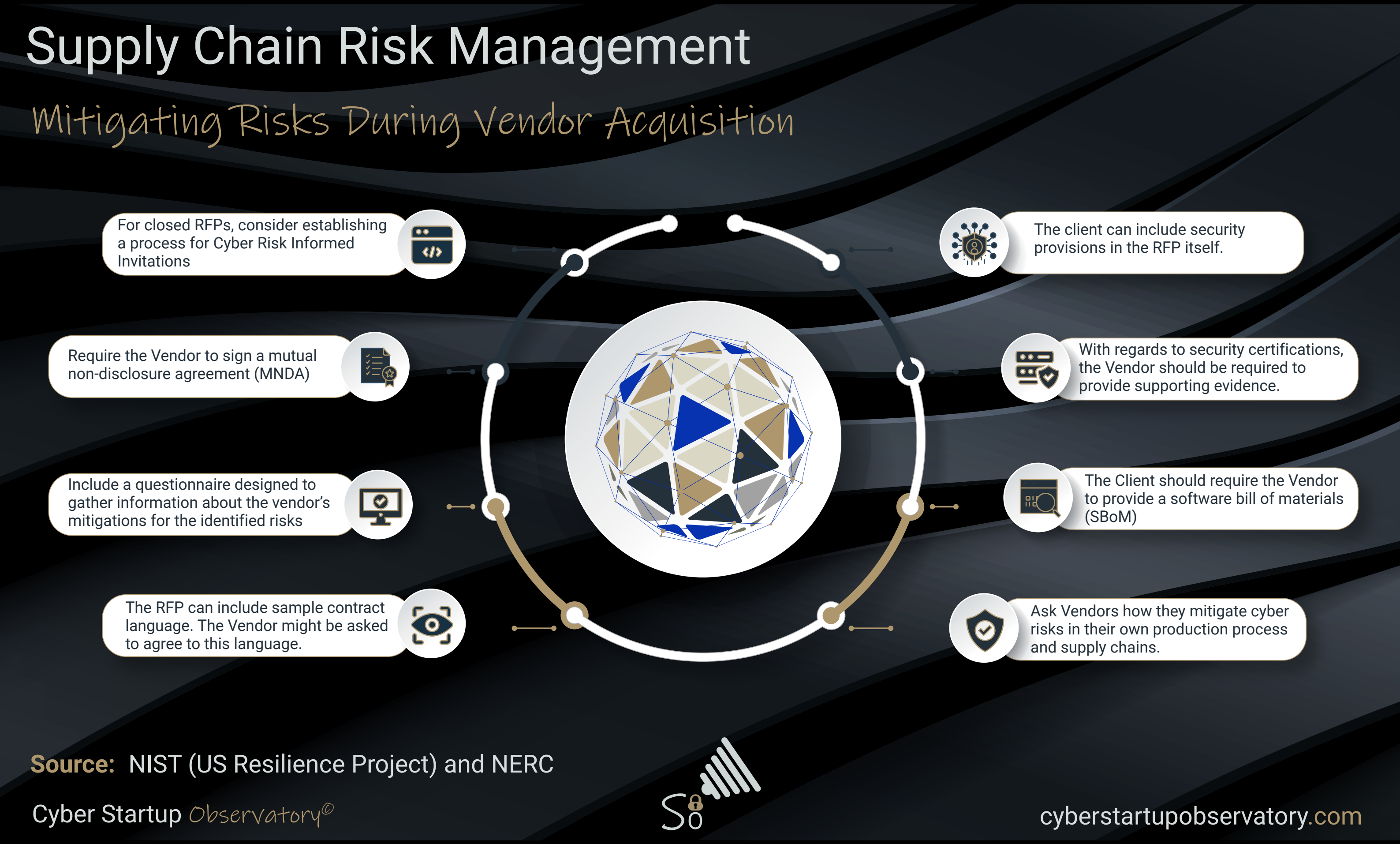
The views expressed in this interview belong solely to the author, and not necessarily to the author's employer, organization, committee or other group or individual.

Resources

Video Infographic

Supply Chain Risk Management - Mitigating Risks During Vendor Acquisition

Supply Chain Risk Management - Mitigating Risks During Vendor Acquisition



Supply Chain Risk Management

Mitigating Risks During Vendor Acquisition

- For closed RFPs, consider establishing a process for Cyber Risk Informed Invitations
- Require the Vendor to sign a mutual non-disclosure agreement (MNDA)
- Include a questionnaire designed to gather information about the vendor's mitigations for the identified risks
- The RFP can include sample contract language. The Vendor might be asked to agree to this language.
- The client can include security provisions in the RFP itself.
- With regards to security certifications, the Vendor should be required to provide supporting evidence.
- The Client should require the Vendor to provide a software bill of materials (SBoM)
- Ask Vendors how they mitigate cyber risks in their own production process and supply chains.

Source: NIST (US Resilience Project) and NERC

Cyber Startup *Observatory©*

cyberstartupobservatory.com

Please follow the link below to visit all our Video Infographics:

Cyber Startup Observatory - Video Infographics

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:

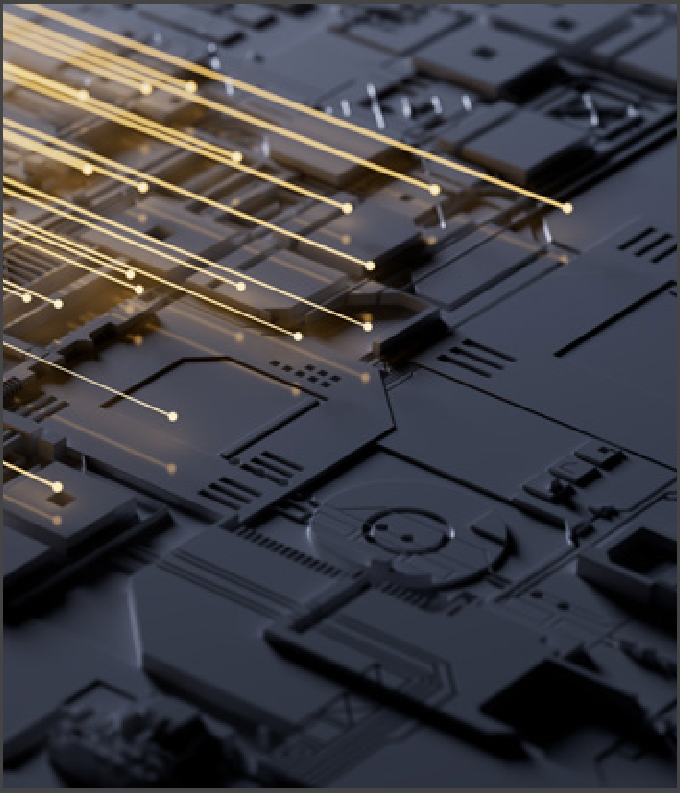
"All men make mistakes, but only wise men learn from their mistakes."

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.

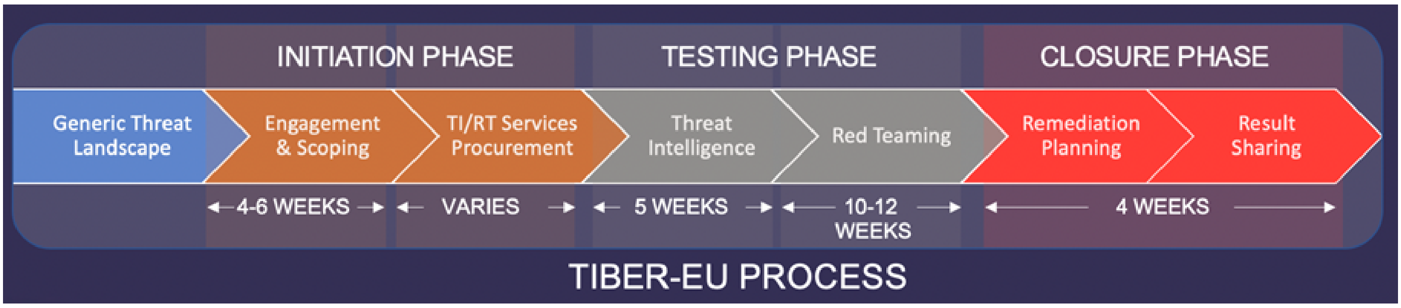
- It is delivered on production systems – Because of the live production systems being targeted, Red Team Testing engagements have to somewhat limit the realism of the attack simulation in order to limit the risk of unforeseen negative impact on the business.

Cyber drills

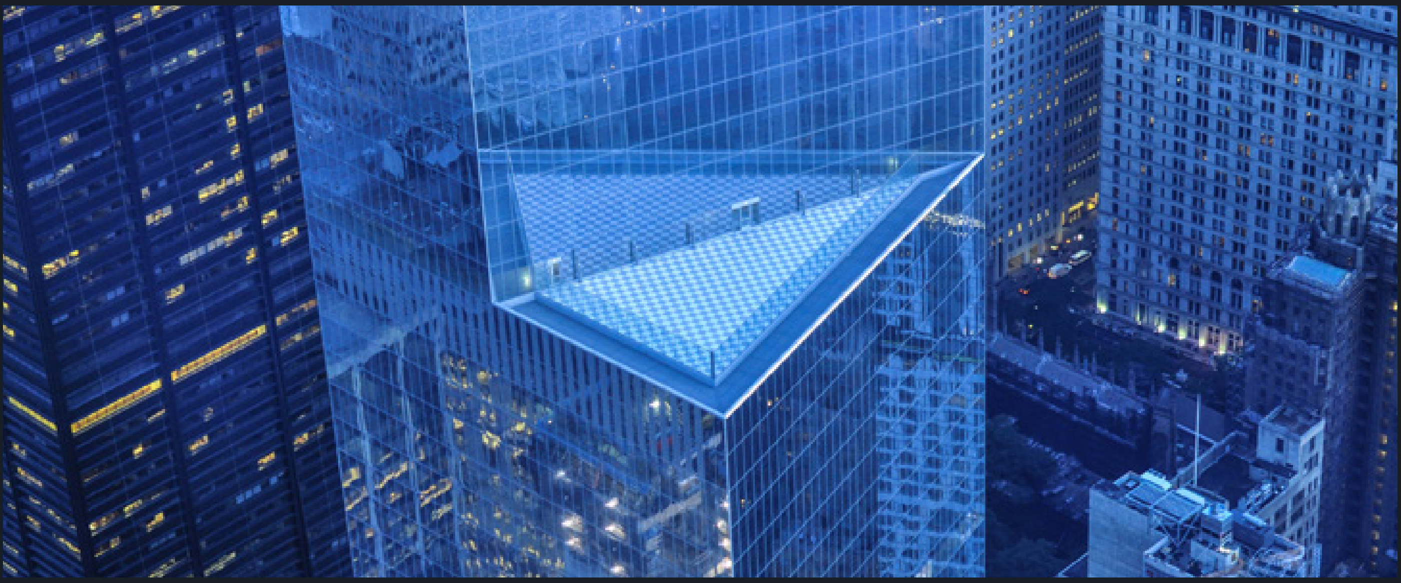
A cyber drill is a planned event during which an organization simulates cyberattacks, information security incidents or other types of disruption to test the organization's cyber capabilities, from being able to detect a security incident to the ability to respond to it appropriately and minimize the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

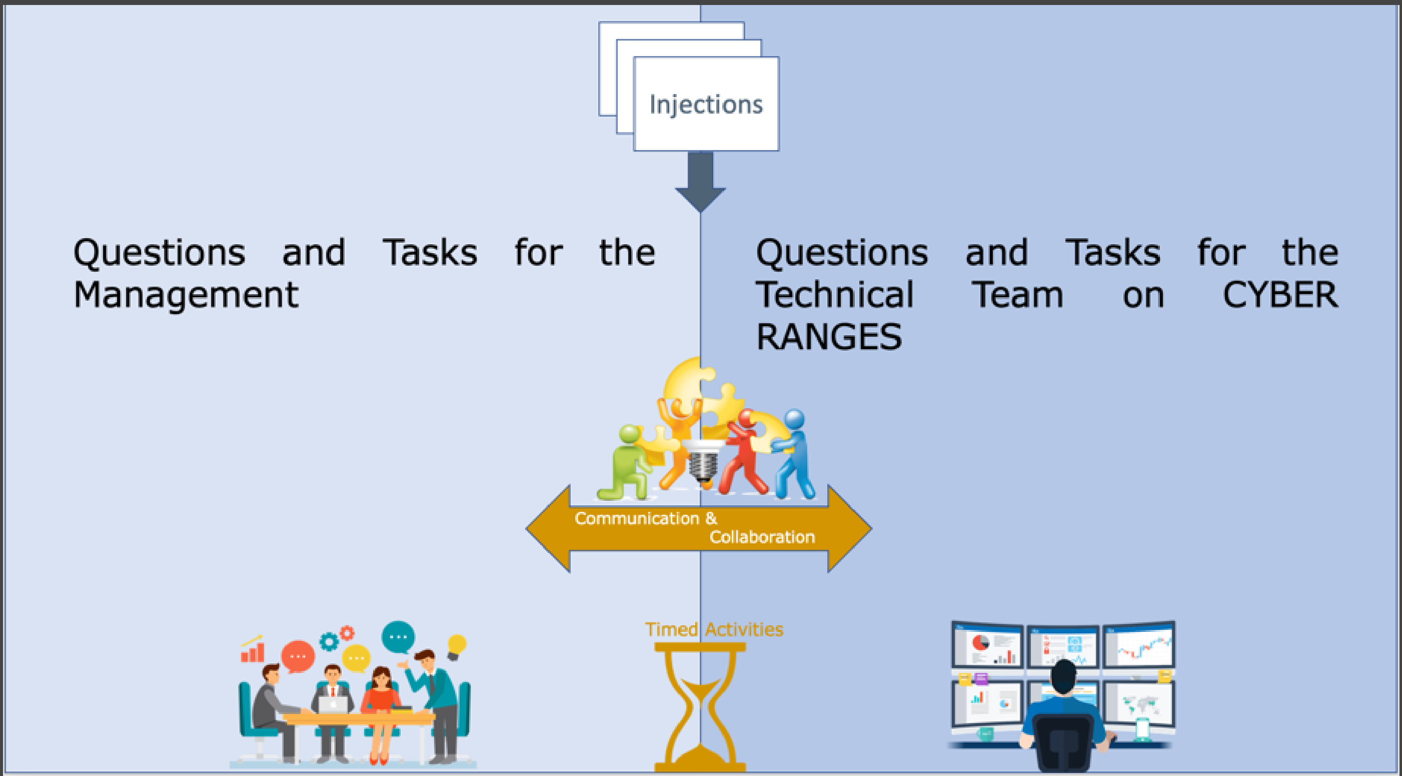
Operational Exercises - Operational exercises have been run successfully for many years across many different business sectors. However, Operational Exercises come with the following shortfalls:

- 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.

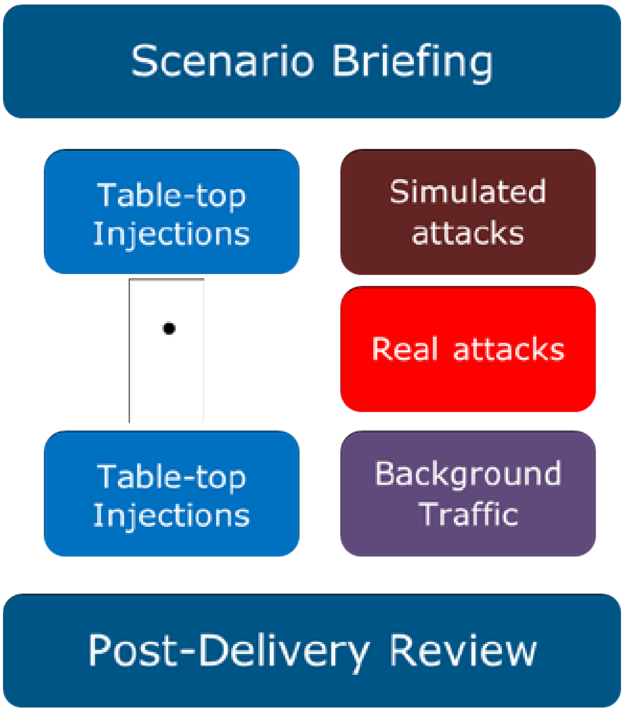
A Better Approach: Cross Cyber Drills (C2 Drills)

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.


Injections
Questions and Tasks for the Management
Questions and Tasks for the Technical Team on CYBER RANGES
Communication & Collaboration
Timed Activities

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.

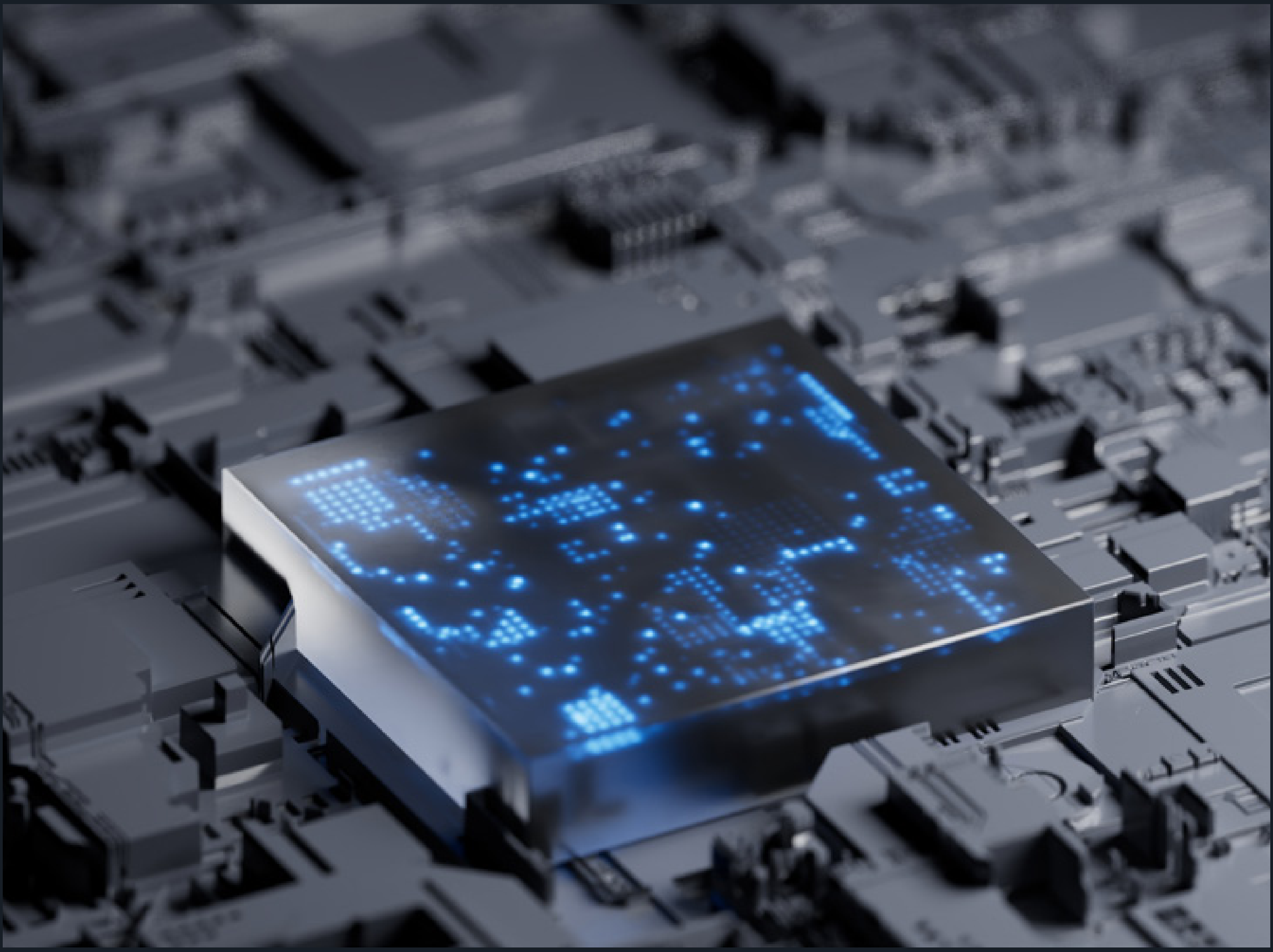
Participants are divided into two groups. Group one includes all the participants involved in the technical hands-on exercises. Group 2 includes the management involved in the table-top simulations.

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:

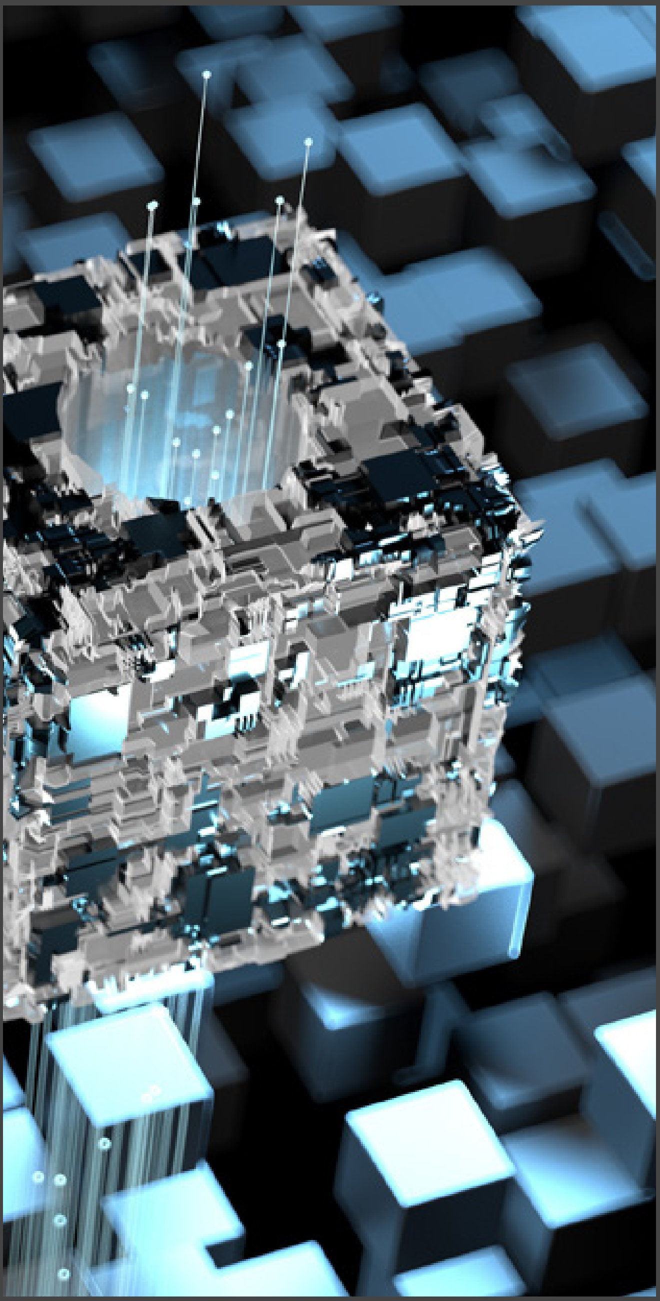
- Management Workflow of Simulation Environments
- Attack Simulation/Emulation
- Management of interactions amongst multiple stakeholders (e.g., management and technical staff).

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.

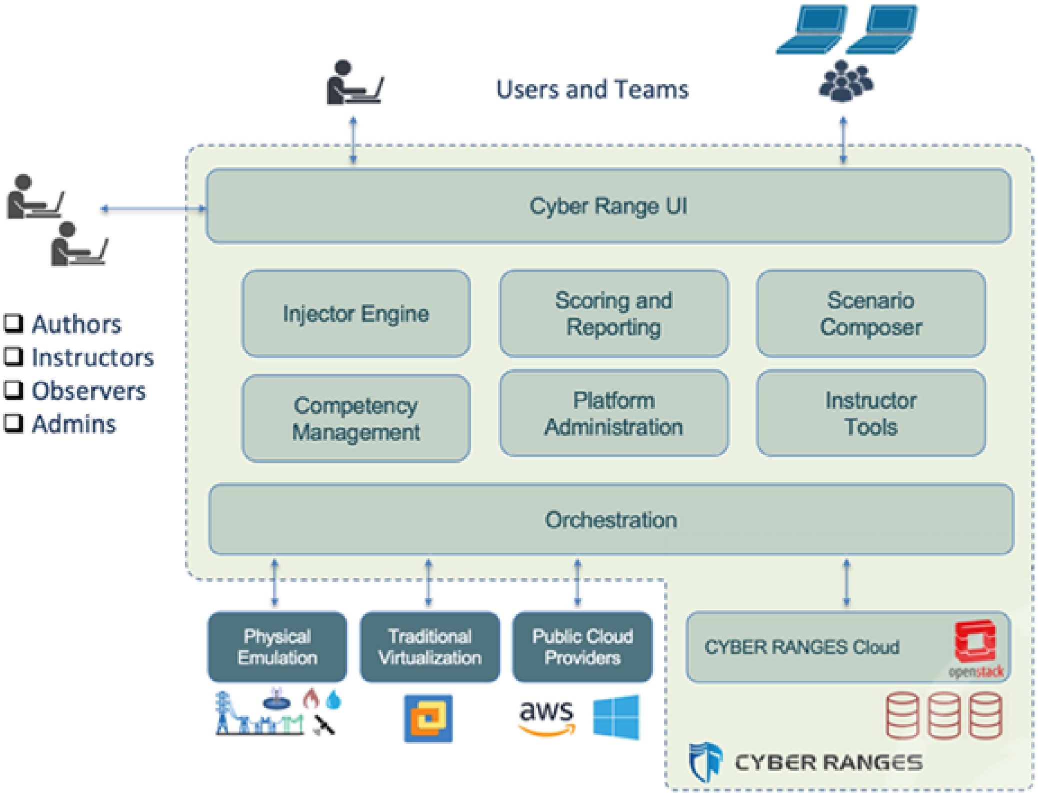
Using a Next-Generation Cyber Range for Improving Cyber Drill Automation

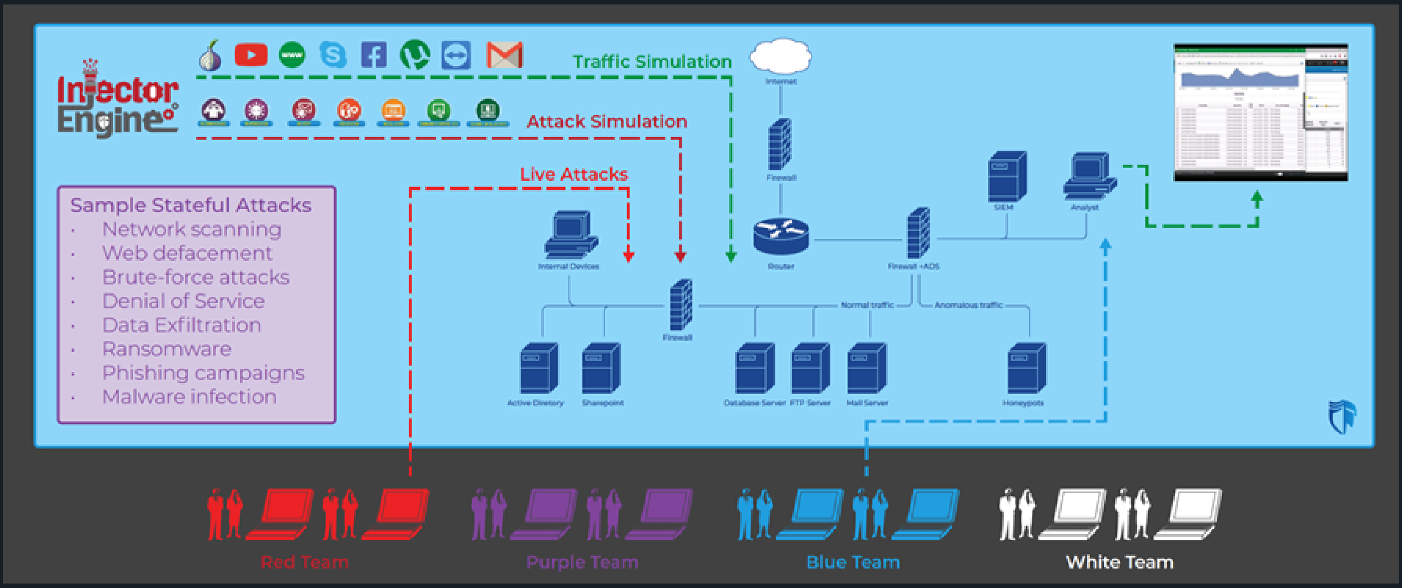
Since every organization is different, assessing cyber resilience will never be a fully automated process. However, there is light at the end of the tunnel that is bound to change this limitation for the entire financial sector and other industries alike.

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

[1] MITRE 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

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

[4] Bank 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

[5] Saudi 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

[6] The 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

CYBER RANGES

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.

Leadership

Madan Mohan

Director - Technology Risk @ BDO UAE

Madan Mohan

Director - Technology Risk @ BDO UAE

Madan Mohan is a Director in BDO UAE's Technology Risk Advisory Services practice, having more than 19+ years of experience in providing Cybersecurity, information technology (IT), data security and IT risk management consulting services to global organizations.

He is responsible for growing and delivering the technology advisory services including Cybersecurity, Cyber & Information security consulting, Managed security services, Cyber regulatory compliances and internal audits.

At a leadership level, he is responsible for managing relations, value delivery, business development, building partnerships and alliances (local and global), proposals, bid management, quality and risk management

He has received Top 50 CISO awards; recognized his contribution in enhancing the IT security landscape and securing company's digital assets.

Received Top 100 CIO awards, in recognition of exemplary contribution in Info Sec.

Received best data protection strategy of the year award 2019

Professional qualifications:

- IIM – Management & Leadership Program
- Bachelors of Engineering in Computer Science
- C|CISO certified
- CISA certified
- CISM certified
- CDPSE (Privacy) certified.
- Certified Privacy Lead Assessor (DCPLA)
- ISO 27001 LA from BSI UK
- ISO 25999 LA from BSI UK

How can a CISO enable business, maintain competitiveness and still provide reasonable security?

Disruption is the 'new normal' for businesses globally, from pandemic and trade re-negotiations to cyberwars. Investing in cybersecurity can be a powerful business enabler, helping you protect critical assets, streamline compliance, modernize your IT infrastructure and build trust with Regulators, customers & other internal/ external stakeholders.

The CISO's primary responsibility is to allocate rare resources effectively and efficiently, maximizing the value of every dollar spent to reduce the corporate cyber risk profile. To achieve this, the CISO must rush into execution mode, and conduct a deep dive to understand the business value chain, digital crown jewels, customer segments, the most profitable business lines and top management priorities. The CISO must also dig deep into audit reports, penetration test results, red teaming exercises, executive tabletop exercises, third party assurance reports, data breach root cause analysis reports, risk registers and board reports to have a good grasp on the most critical cyber risk exposures.

Once CISO gained a deep insight into the organizational road map, digital strategy, existing capabilities and key risks, formulate a strategic plan that prioritizes the areas of highest risk and quick wins. Organisation's top priorities will naturally need the required budget and additional resources to bolster the existing team.

How would you justify security investment to your board?

Even in today's climate of constant threat of cyber attack, IT may still encounter challenges in getting the cybersecurity message across to their board of directors.

We know, there is no such thing as 100 percent secure and as data breaches continue to hit the headlines, investments in IT security never seem to be quite enough. When it comes to budgeting, the role of a Chief Information Security Officer (CISO) is to prioritise available resources based on the IT risks the organisation faces and justify additional investments when and where needed to executives.

Here are some strategies for helping to raise visibility, support for cybersecurity initiatives & justify security budget at your organization:

- Assess IT risks

Before requesting additional investments, CISOs should first assess whether current resources are allocated correctly in order to address the actual risks that firms are exposed to; whether those risks are prioritised well and what the level of remaining risk exposure is.

Risk assessments enable CISOs to determine which risks are sufficiently addressed by current IT controls and what security gaps remain that require additional efforts and investment management. With that information, CISOs are therefore better able to prioritise risks and allocate resources wisely.

By accurately assessing risks for organisations and the industry in general, companies will be able to prepare a roadmap for eliminating the critical security gaps in their environment and build a coherent argument for additional budget.

- Effective Communication

CISOs are well-advised to start with their security status, briefly describing the IT risks roadmap and explaining exactly what they are doing to address current risks, demonstrating that they are effectively using existing technologies and human resources. During the communication with the board, CISOs should avoid technical acronyms or using terms such as “the infrastructure”; they should instead reference business processes and real-life scenarios, ideally examples of incidents in the national press.

At this point it is important to highlight the most acute security gaps that leave a company vulnerable to current threats and request money to address them. The key to success is to clearly explain and, whenever possible, quantify the business impact of the security incidents that could result if those security risks are left unaddressed.

- Highlight Solution Benefits

This stage involves providing a clear, actionable plan for how the CISO will use the budget requested to reduce the IT risks identified to a level acceptable to the business. This plan must include resources – people, technologies, etc. – deadlines and a detailed budget that sets out how much money will be spent on what.

To support the argument, it is important to estimate the expected return on security investment (ROSI) for planned investments in order to prove their effectiveness in balancing risk and cost. CISOs can base this calculation on direct prevention of financial losses. Apart from the losses, it is great to translate the value that security projects can bring to the business. In other words, presenting budget requests to the board as opportunities for assisting in meeting their business objectives, such as reducing costs, increasing revenue or increasing the company’s value on the market.

How can a company create a data privacy culture in the workplace?

The organization itself must view privacy as a business imperative; after all, reputational damage may be the least of the concerns among regulatory, revenue and expense implications when privacy is breached. More than just setting procedures and investing in a strong privacy leader, each individual at the organization should be trained in privacy policies, processes and principles. Enterprises are living entities, and their culture helps them survive in today's fiercely competitive business environment.

Deploying Data privacy culture requires the board of directors and senior management to decide to support and enable a privacy shield to mitigate the risk associated with data privacy. As a result, enterprises should answer this critical question: "Should we develop and implement a data privacy culture to reinforce personal data protection of our stakeholders?"

Perhaps such a question needs to be evaluated by senior executives who manage data privacy projects. These executives must also assess whether the development and implementation of a data privacy culture should be done before establishing data protection technology and processes.

Importance of Data Privacy Culture

Implementing a data privacy culture enables:

- Empowering people—Data Privacy culture empowers people with the sociological and psychological skills that are required to work with Data Privacy policies and procedures.
- Projecting Data privacy meaning—Within the enterprise, the importance of the people, technology and processes of Data Privacy is understood. The consequences of ignoring Privacy's social, legal and financial risk are addressed.
- Establishing stakeholder partnership and collaboration of key players—A network of data privacy stakeholders is defined and managed. Stakeholders include employees, managers, government agencies, senior executives, boards of directors, technology providers, consulting providers, and education and training providers.
- Providing an education and training road map—An appropriate education and training program that encompasses the people, technology and processes of Data privacy is integrated and delivered.

What measures can help organisations protect themselves against ransomware?

Ransomware attack can be avoided by protecting organizations with multiple controls as part of a defense-in-depth strategy, which means implementing good cybersecurity practices and designing systems accordingly. Fortunately, there are countermeasures that organizations can implement to combat this ongoing threat.

- Keep Systems Up-To-Date
- Implement Whitelisting Technologies
- Implement Email Security Technologies
- Use Updated Malware Scanners
- Implement Multifactor Authentication for Admin Access
- Implement Good Access Controls.
- Have Good and Secure Backups
- Implement Cyberdeception Techniques

In the face of growing regulatory pressure, where do you see the line between compliance and security?

Compliance and security complement each other in various aspects. However, being compliant does not necessarily mean that an organization is covering all aspects of security required to protect infrastructure.

There have been significant known breaches of many companies that were considered "compliant." An effective security program integrated with an efficient compliance plan will strengthen overall security infrastructure and ensure compliance.

The overall objective for security controls is to support the organization's services and infrastructure by identifying risks, improving the security level, and enabling rapid detection and response to security attacks.

It is also true that, in practice, no organization can place all the security controls against every cyberattack by itself. Consequently, it is now a growing practice that many organizations leverage a hybrid model for their security controls. For example, organizations put in place onsite or locally deployed security controls in the form of people, process and technology, together with cloud-based security controls.

On the other hand, risks, regulatory and compliance requirements drive business values of highly regulated industries, such as financial services and healthcare. Therefore, using a hybrid model for security controls in highly regulated industries raises compliance implications. Especially for highly regulated industries, the multitude of risk, regulatory and compliance requirements, such as ADHICS, PCI DSS, SOX, HIPAA, GDPR and many others related to privacy and sensitive data, are increasing. There is more complexity, cost and operational overhead in the infrastructure – consequently, cloud-driven security controls are a natural choice for many organizations to address complexity, cost and operational issues. However, this also leads to new challenges to remain compliant with ever-increasing requirements.

Organizations must analyze technological aspects of particular compliance requirements – for example, how encryption/decryption will be performed inside or outside a particular jurisdiction, and where and how the data (alerts, logs) will be stored and handled. While decrypting traffic externally, who will have access to that decrypted data? More importantly, in the case of a breach or data leakage, how will accountability be established and how will fines be paid that are imposed by regulatory authorities?

What do you think are the right steps to reduce cyber risks when working with third parties?

The SolarWinds example highlights the interconnectedness of cyberspace and the need for collaboration at the sectorial, national and global ecosystem levels to develop effective cyberdefenses.

The security of an enterprise not only relies on its own employees, suppliers, and contractors, but it also on those from other organizations in its own geography and in the wider global economy. An enterprise may exhaust its resources dealing with challenges in securing its systems, but to ensure that similar security is governing other users of cyberspace requires a global security defense mechanism, which means open communication with other partners and even competitors.

To improve cyberdefenses, it is vital that defense measures are defined appropriately, along with defense policies and procedures. Enterprises must communicate their defense measures effectively and openly and ensured that they understand the cyberdefenses of their third-party suppliers and, thus, have ensured effective cybersecurity in the organization. The key to achieving a transparent and tough attitude toward cybersecurity is for organizations and third-party suppliers to work together.

There are numerous recommendations that can help reduce cybersecurity risk when working with third-party suppliers:

- Ensure that third parties are required to meet enterprise cybersecurity standards and that the same standards are imposed on any subcontractors.
- Ensure that regular testing (e.g., penetration testing) or exercises testing technical systems are conducted regularly.
- Ensure that access controls are such that a user's access is dependent on their need to do their job based on their roles; no other access is given to them and there is widespread use of zero trust in the enterprise.
- Implement enterprisewide use of multifactor authentication (MFA) for all high-level access.
- Implement systems to detect possible security threats and notify the appropriate contacts upon detection.
- Study and prepare for third-party supply chain attack scenarios.
- Prepare team members through mandatory security training and certification opportunities.
- Specify security requirements in third-party contracts (e.g., service level agreements [SLAs], escalation protocols) and work with the procurement function to integrate these elements into any supplier contracts.
- Ensure that cybersecurity expectations from smaller suppliers are fairly balanced between security and the effective use of available resources.
- Ensure that if any issues are identified, they are corrected, customers are duly informed and risk mitigation procedures are followed.

Closing Statement

Layered Security Approach

Digital transformation, hastened by the onset of COVID-19, has escorted in a new era of technological innovation and digital processes unlike anything the IT industry has ever seen before. And the risks have increased exponentially. Layered security is the only approach that provides measures corresponding to protection, detection, and response. Layers are beneficial for many reasons. Each layer provides an additional level of defence so that with each extra layer of security that can be added, it becomes more challenging to find ways to infiltrate the system. While each layer in and of itself is not an adequate defence mechanism, layering them together improves each one's efficiency until the last layer nearly completely blocks out the hacker's ability to gain access. Instead of trying to rely on just one or two levels of defence, like access cards and two-step identification, multiple layers of security will lower the risk of a breach and make it easier to respond to legitimate inquiries and requests.

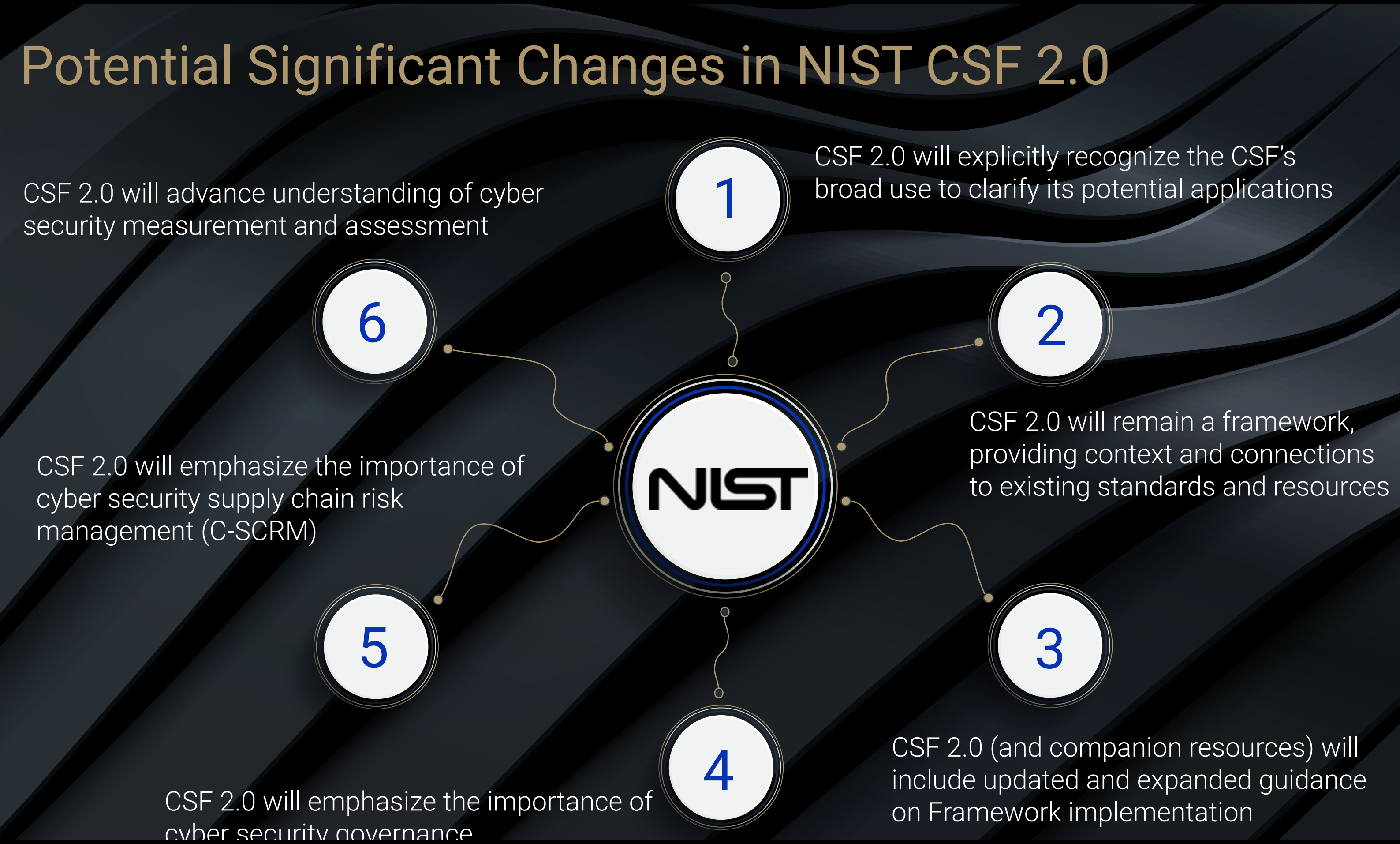
Layered approach provides multi-levels of defence that both identifies and eliminates threats on many different levels. With each added layer, it compounds level of protection until a wall of security is created that is almost impenetrable. The increased risk of loss associated with cyberattacks cannot be denied, so it's vital that a security approach is followed which takes many different types of threats into consideration and deals with each one quickly and efficiently.

Resources

Video Infographic

Potential Significant Changes in NIST CSF 2.0

Potential Significant Changes in NIST CSF 2.0



Potential Significant Changes in NIST CSF 2.0

1 CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications

2 CSF 2.0 will remain a framework, providing context and connections to existing standards and resources

3 CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation

4 CSF 2.0 will emphasize the importance of cyber security governance

5 CSF 2.0 will emphasize the importance of cyber security supply chain risk management (C-SCRM)

6 CSF 2.0 will advance understanding of cyber security measurement and assessment

Please follow the link below to visit all our Video Infographics:

Cyber Startup Observatory - Video Infographics

Insight

STELLAR CYBER

Making Co-Managed Security Services a Win-Win

Making Co-Managed Security Services a Win-Win

Author: Stellar Cyber

At a glance

- 3 minute read
- What to Tell Prospective CIOs and CSOs
- Ensuring Your Own Success
- Conclusion

Organizations like to work with MSSPs for co-managed security services for lots of reasons. The trick is to make sure the arrangement works for you as well as it does for your clients.

Of course, co-management brings you added revenue and payback for the security services in which you have invested. For your clients, it enables them to enhance their security by offloading it to experts whose mission in life is to stay up to date on the latest hacks and remedies.

What to Tell Prospective CIOs and CSOs

There are several specific co-management selling propositions for MSSP services. The most important one is that you close their security knowledge gap to reduce risk and make the client's infrastructure safer than ever.

But there are others, including:

- Shorter time to a solution. Rather than having to hire and train new analysts of their own, prospects can simply work with you. If you have the right SOC platform, you should be able to get a new client up and running within a few days.

- Workload reduction. Co-management helps a company right-size IT workloads for an overworked in-house analyst staff. Maintaining a leaner in-house IT staff also reduces the burden on IT management.

- Reduced turnover. By reducing the workload and enabling the client's IT staff to focus on areas they know well, you also boost morale for their analysts and IT managers, which minimizes burnout and turnover.

- Retained control. The big objection to partnering with an MSSP is a loss of control, but it's easy for clients to retain control because they're the ones making the choice about which functions to outsource.

- 24/7 support. One of the biggest advantages of outsourcing security is continuous monitoring and support. IT managers can sleep more peacefully and even go on vacation knowing there's someone minding the store.

Ensuring Your Own Success

Here are two strategies for ensuring your own quality of service, service agility and overall margins:

- Use the right SOC platform. You won't be able to service clients properly or maintain high margins if your SOC platform doesn't give you service flexibility or requires more attention than an Italian sports car. Make sure your SOC delivers full visibility into the client's infrastructure, that it's flexible enough to integrate with the security tools your client wants to keep, and that it's easy for your team to use. Having built-in multi tenancy will also make it easy to on-board new customers. Finally, automation and ease of use are important if you want to maintain a lean team of your own to minimize expenses.
- Maintain client satisfaction. Provide regular reports to the client and give them access to your dashboard so they can see for themselves that you're on the ball. Make sure you deliver statistics on threats found and stopped – those will impress upper management and help justify your budget.

With these ideas in mind, you'll ensure a win-win for your clients and your own firm, establishing a long-term relationship that can grow over time. To learn more reach out to Stellar Cyber

www.stellarcyber.ai

Leadership

Enes Yildizhan

ICT Security Chief @ Tailwind Airlines

Enes Yildizhan

ICT Security Chief @ Tailwind Airlines

First of all, a big thank you to the Cyber Security Observatory and Smartrev Cybersec for including me in such an organization.

I am Enes, I am both a senior and a passionate professional in the Cyber Security and Information Security industries with over 7 years of manager, team leader, advisor, pre-sales & post-sales engineer experience combining engineering skills with excellent communication skills.

Currently, I have been working as ICT Security Chief at Tailwind Airlines and I am responsible for the management of security solutions, hardening vulnerabilities, incident detection and response, forensic analysis, information security management and compliance, cyber threat intelligence and social engineering.

How might the issue of the cyber security skills shortage be addressed?

Today, there is a shortage of qualified cyber security specialists and this problem is increasing day by day. The increase in cyber security job postings compared to previous years proves this. According to data from global research companies, the cost of cybercrime is estimated to reach $6 trillion worldwide by the end of the year. That's why the demand for skilled cybersecurity professionals is higher than ever before. All these experiences have increased the need for experienced cyber security personnel.

I think the gap of cyber security skills can be minimized as follows;

1. Especially before graduating from the university, successful internships should be done and entry-level certificates should be obtained that will facilitate entering the business life.

2. Those who are just starting out in the field of cyber security should specialize in the basics of cyber security, especially with training.

3. Cybersecurity is one of the fastest growing areas in IT industries. In this case, what can you do to keep up to date with the latest information? The answer is very simple: Read, read and read more. Make a list of cyber leaders on Twitter and other social media channels and follow news and analysis on emerging cyber threats.

4. Specialization is important to success in your career. For those who want to be a cyber security leader, they must have decided in which field they want to advance.

How would you justify security investment to your board?

For years cybersecurity spending has experienced stratospheric growth. Then COVID-19 hit and forecasts took a grim turn. As a result of the economic impact of the pandemic, Gartner predicted a reduction in global security spending and was right. That being the case, I can recommend the following, based on my experience, to persuade the board of directors to invest in security:

1. Categorize security solutions that require investment by priority level by running a risk process.

2. Use security performance metrics and reports to justify funding.

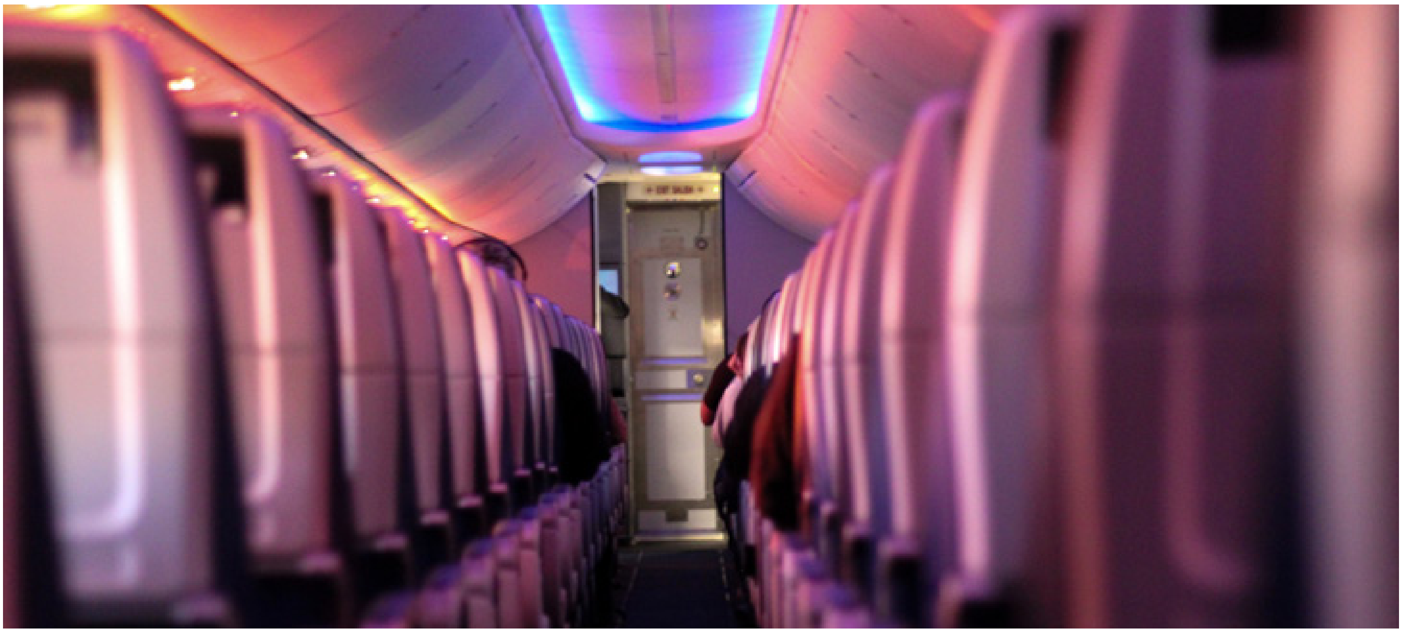
3. Benchmark security performance to prioritize investments.

4. Uncover the risks, especially in the remote office environment, which is the new work norm.

5. Emphasize that the "new normal" requires a new approach.

How often do you think security drills and exercises should be employed in order to maintain the profile of cyber security within the company?

Cyber security exercises have an important place in efforts to increase awareness on cyber security, as well as to improve the level of expertise, implement information security standards and user trainings among initiatives to ensure cyber security.



Because the purpose of cyber security exercises; to improve their ability to resist cyber attacks, to improve their internal and inter-institutional coordination against cyber attacks, and to increase the level of awareness about cyber security.

Considering the threat vector, which changes moment by moment, in order to keep awareness constantly alive; At least 1 broad and 2 narrow scope pentests (Internal, External, Web and DDoS) per year, social engineering once every 3 months and if possible 1 Red Teaming work per year will reinforce this vitality.

Is Zero Trust the solution to defend against ransomware?

Over the past year, there have been a number of successful ransomware attacks that have made online security a hot topic across the globe. Ransomware attacks continue to rise, putting companies without proper security measures at risk of data breaches. To prevent such attacks, organizations are relying on a Zero Trust model to protect both on-premise and cloud assets. Zero Trust ensures relevant least-privilege and secure access to corporate resources, limiting the attack surface and decreasing the chances of ransomware attacks.

By controlling all aspects of network security with a Zero Trust solution, IT managers can significantly reduce the risks of online threats across their organizations.

Zero Trust allows IT managers to segment user access, so each user can access only specific company resources, without exposing the network at large.

This is critical for decreasing the severity of ransomware attacks. With Zero Trust, even in the case of a vulnerability, hackers are limited to the few resources open to the specific user they hacked instead of the entire corporate network.

Zero Trust, the overall security posture; Considering that it has developed in Network Segmentation, Trust Zones and Infrastructure Management, we can say that it is a solution to protect against ransomware.

When pushing forward with digital transformation many companies will migrate to the cloud. What are the main risks to consider when doing so?

Many businesses are now starting to use cloud computing because it provides them a far more flexible and dependable IT infrastructure that is primarily intended to simplify business operations. Because simplifying and streamlining business operations helps companies to sell and expand quickly. However, bringing a business into the cloud is easier said than done.

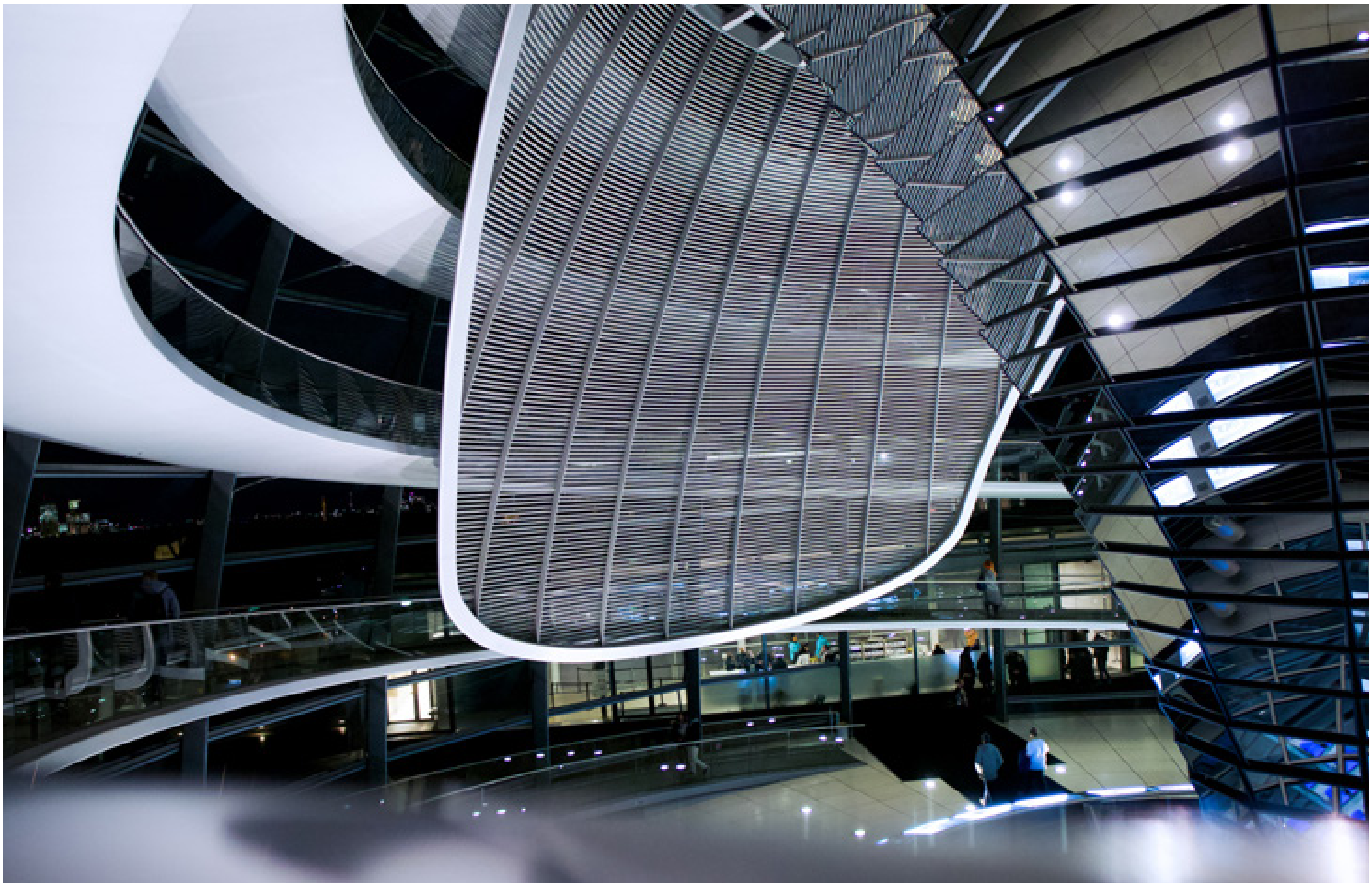
To successfully move your business into the cloud, here are the top cloud migration risks you should avoid:

1. No Concrete Plan in Place - You must first decide if you will use a single cloud provider or manage numerous cloud platforms, determine what you will send to the cloud and what will remain on your local data storage.

2. Cloud Compatibility to Existing Business Systems - Adequate IT capabilities

3. Loss of Data - Before you begin migrating, create a backup of your data, particularly the files you will be moving.

4. Security - Compliance violations, contract violations, unsafe APIs, provider difficulties, misconfigured servers, malware, external attacks, unintentional bugs, insider threats, etc. You should choose a platform that has no security concerns.



What channels are available for fostering the exchange of information and ideas among the CISO community?

I think that most cybersecurity professionals today are more willing to share information and exchange ideas than in the past.

I think that LinkedIn is the most used channel to encourage the exchange of information and ideas. The shares made here, the groups created and the newsletters support this. In addition, reaching thousands of people helps this situation by expanding its network.

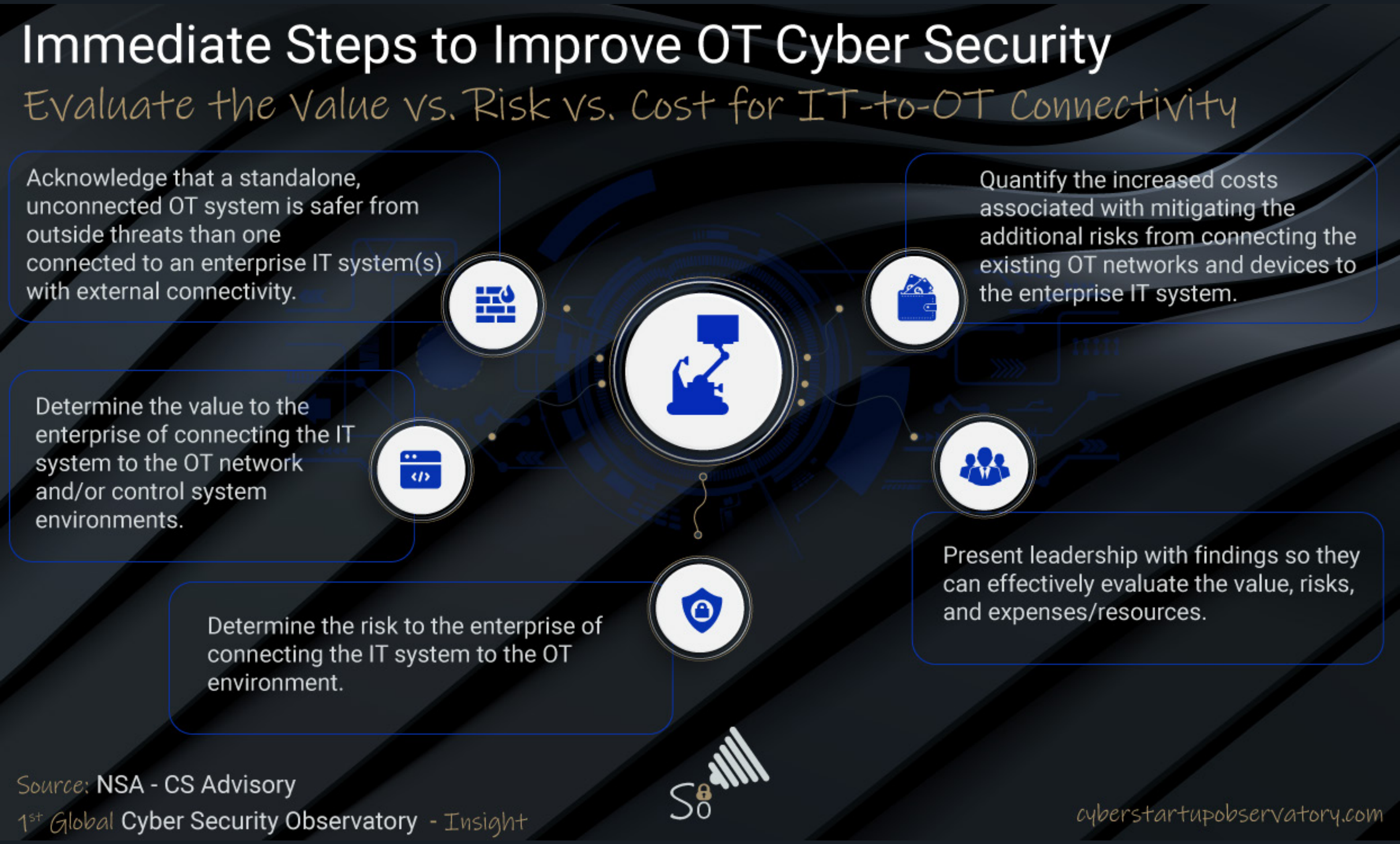
As a result; From the smart watch on our arm to the smart cleaning robot in our home, the number of devices connected to the internet is increasing day by day. Therefore, we can say that cyber security has become an integral part of our lives. I believe that cyber security experts and high-aware end users who see this picture will shape the future.

Resources

Video Infographic

Immediate Steps to Improve OT Cyber Security

Immediate Steps to Improve OT Cyber Security



Immediate Steps to Improve OT Cyber Security

Evaluate the Value vs. Risk vs. Cost for IT-to-OT Connectivity

Acknowledge that a standalone, unconnected OT system is safer from outside threats than one connected to an enterprise IT system(s) with external connectivity.

Quantify the increased costs associated with mitigating the additional risks from connecting the existing OT networks and devices to the enterprise IT system.

Determine the value to the enterprise of connecting the IT system to the OT network and/or control system environments.

Present leadership with findings so they can effectively evaluate the value, risks, and expenses/resources.

Determine the risk to the enterprise of connecting the IT system to the OT environment.

Source: NSA - CS Advisory

1st Global Cyber Security Observatory - Insight

cyberstartupobservatory.com

Please follow the link below to visit all our Video Infographics:

Cyber Startup Observatory - Video Infographics

Insight

Jose Monteagudo

Founder & Chief Analyst @ Cyber Startup Observatory

Power Grid Cybersecurity, Where Are We Now?

Power Grid Cybersecurity, Where Are We Now?

Author: Jose Monteagudo, Founder & Chief Analyst @ Cyber Startup Observatory

At a glance

- 4 minute read
- Background
- The next generation power systems: The Smart Grid
- Cybersecurity challenges, threats and risks
- About the author

There are many voices raising concerns about the fact that the quickly evolving threat landscape is outpacing protection measures and defences in the energy sector and notably in the power grid.

There are no shortcuts or easy ways to address this problem. Electricity grids are complex infrastructures that have been deployed during the last few decades. These grids are far more than generating stations, high voltage transmission lines, transformers and finally distribution lines that connect individual customers.

The overall architecture of the grid includes seven different components which interact at different levels. These seven components will determine the ability of the power grid to change to address technical, operational, cybersecurity, market, regulatory or end-customer requirements.

These components are:

- **Electric component:** this is the most well-known piece of the jigsaw. It includes generators, transformers, switches, protection circuits, transmission and distribution lines to portray it in a simplistic way.
- **Industry component:** including a huge number of utilities and other organizations interacting through operations, planning and markets. The structure of the markets will differ from region to region and will have important impact on the desire and ability to change.

- **Control component:** including all the control systems, protection circuits and synchronization systems which are critical to safety, operational efficiency and performance.

- **Digital component:** composed of the information and communications systems (ICT) that allow monitoring and control of all the devices on the grid. The Digital layer is crucial for almost all business processes.

- **Convergent networks:** electricity generation will rely heavily on other networks that at a first glance seem to be un-related. This is the case of hydrocarbon fuels and natural gas pipelines, both critical for power generation.

- **Regulatory component:** as we might expect, the power industry is heavily regulated on multiple levels. The regulatory architecture will vary depending on the country and will also have an important effect on all operational aspects and in particular on cybersecurity which is the specific area of interest of this article.

- **Coordination framework:** for coordination and control of all the different elements and assets that make up the system, including some that are not owned by electric utilities.

From a topology perspective, the traditional power grid system is centralized and radial, where power is generated and delivered from one end to the other.

As we may see, there is huge complexity in the overall architecture of the power grid. There are many moving pieces that interact together and that have been built over the last few decades.

Moreover, this infrastructure wasn't designed with cybersecurity in mind. Engineers at that time didn't have to address the challenges that have been brought to the table by the new approach: connectivity everywhere.

So now we understand the architecture of the power grid a little bit more, the key question is how we can shape its evolution to cope with the very dynamic threat landscape.

The next generation power systems: The Smart Grid

The smart grid represents a major improvement over legacy power infrastructure. Leveraging state-of-the-art ICT technologies, it will enhance the efficiency and reliability of power systems, bringing distributed intelligence and demand response.

As we have discussed before, the topology of legacy power infrastructures was centralized and radial. Nevertheless, conventional methods for unidirectional power flow will no longer be effective to control renewable energy sources implemented at the consumption sector. Consequently, new strategies are needed to facilitate the bidirectional flow incurred by power production of the distributed energy resource units. The transformation will require intelligent distribution automation by means of decentralized power management as well as information and communications technologies.

With increased connectivity comes the major concern of cybersecurity. Arguably, we couldn't have foreseen the cybersecurity challenge at the time of design of legacy electricity infrastructures. But in the case of the Smart Grid the situation is different. We have been well aware of the status quo with regards to the threat landscape. So, the question is, are next-gen electricity grids ready to face the current cybercrime reality?

Let's take a look at the architecture of the Smart Grid to discuss the key security requirements and security challenges.

The Smart Grid can be structured in four different layers:

- **Physical Layer:** including Generation (cycling coal and natural gas-fired power plants with CCS, grid-based renewables, wind farms, nuclear power plants), Transmission, Distribution, Consumption and Grid-based Storage. The electrical flows are limited to this layer.

- **Communication Layer:** including home area, neighbourhood, access & black-hole, core, office and external networks.

- **System Integration Platform:** computing infrastructure, networks and security management, application and data integration.

- **Software layer:** meter data analysis (MDA), billing, outage management, load control, consumers and field engineers' devices interface, GIS, wide area management systems, consumer information systems.

Additionally, we will also find the Industry and Regulatory elements as well as the Coordination Framework as in the case of legacy electricity utilities.

The security requirements for the Smart Grid are covered by the CIA Triad (Confidentiality, Integrity and Availability).

The CIA triad applies to both the General-Purpose Information Technology Systems (ICT Component) and the Industrial Automation & Control Systems (ICS Component).

Nevertheless, when it comes to managing the risks, prioritization and strategy, it is important to differentiate between the ICT component and the Industrial Control Systems (ICS) component.

Let's discuss the CIA Triad in detail:

- **Availability:** focuses on identifying and assuring data and services that need to be available. This is a critical aspect for Smart Grids systems supporting the Smart Grid automation, for example for SCADA servers of Distributed System Operators (DSO) or Transmission System Operators (TSO).

- **Integrity,** ensuring the fidelity of the information, which means identifying and preventing data to be modified without authorization. An example might be to guarantee that control commands and power control readings have not been modified during their transmission.

- **Confidentiality,** preventing unauthorized access to private information. This is less critical when considering grid automation systems (SCADA) but absolutely crucial for end consumers.

There are two other security dimensions that need to be considered: authentication and non-repudiation.

Authentication has been considered implicitly in the CIA Triad and deals with making sure that someone or something really is who or what it claims to be.

Non-repudiation refers to being able to prove that an action has been taken by the entity really responsible for that action.

These two components are equally important for Industrial Automation & Control Systems (SCADA) and General-Purpose Information Technology Systems.

Cybersecurity challenges, threats and risks

Considering that ICT layers constitute roughly three quarters of the Smart Grid architecture, the major challenges below will be easily understood:

- **Connectivity:** as the topology of the Smart Grid is decentralized, all the elements require a high level of protection. The communication network, while allowing for significant advantages, also brings with it risks and challenges. It is key to striking a balance between internetworking and data security.

- Trust: consumers are no longer assumed to be trustworthy

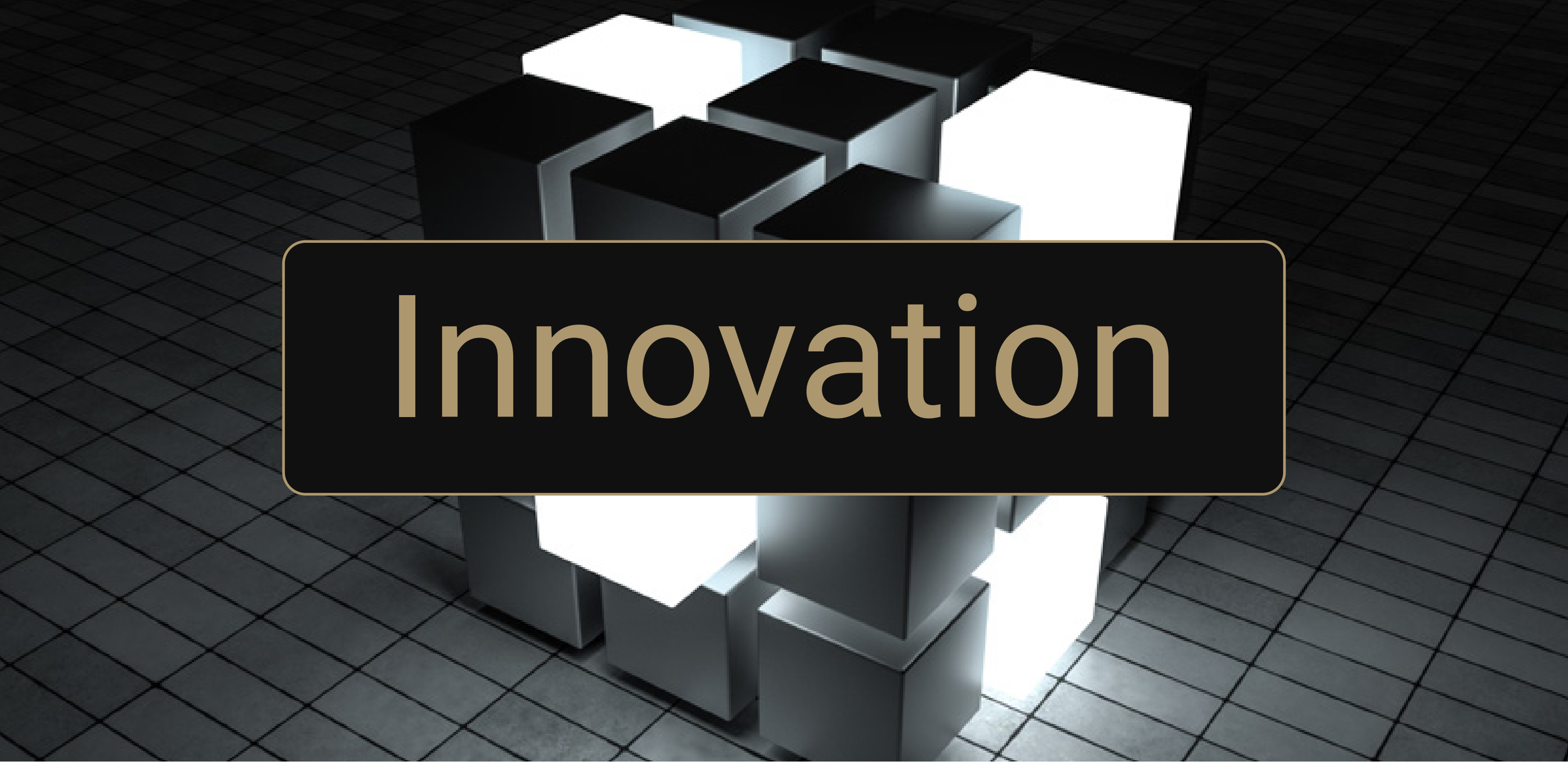
- Privacy: the introduction of smart meters brings important challenges in terms of consumers' information privacy.

- Software vulnerabilities: it is especially important to protect SCADA systems from malware, malicious updates as well as having a strict patching policy.

Cybersecurity in the Smart Grid must address not only deliberate attacks, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software and alter load conditions to destabilize the grid in unpredictable ways.

About the author

Jose Monteagudo is the Editor-in-Chief of the Cyber Startup Observatory, a project he founded in 2018 after more than 20 years in product, consulting and leadership roles in technology companies in the US, UK, France, Japan, Singapore and Spain. He holds a Bsc in Aeronautical Engineering and an MBA from ESIC.



Innovation

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.

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:

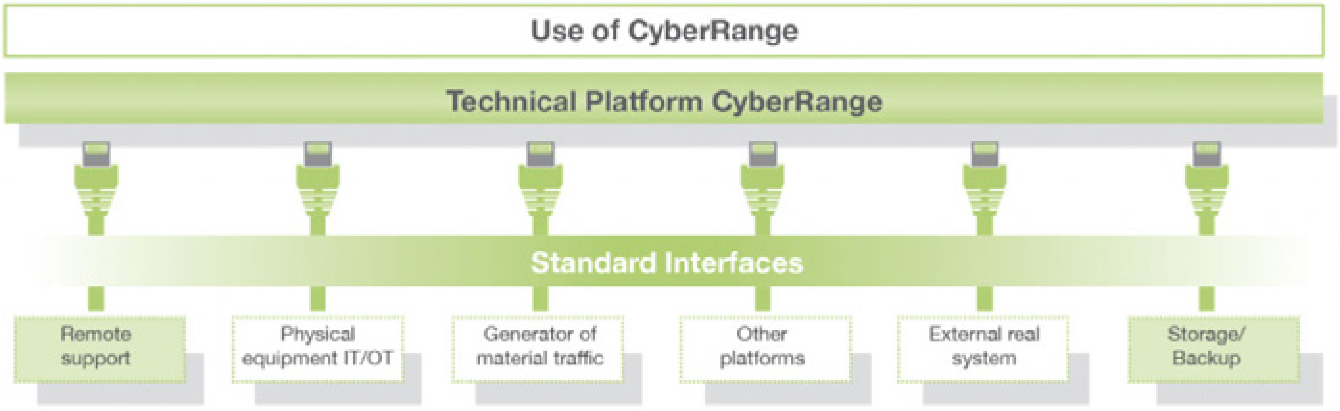
- Assessment of the impact of new equipment on a system
- Study of rule integration or the implementation of new procedures
- Analysis of cyber attack behaviour on its infrastructure without taking any risks

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



06

AIRBUS
CYBERSECURITY

Key Benefits

- **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

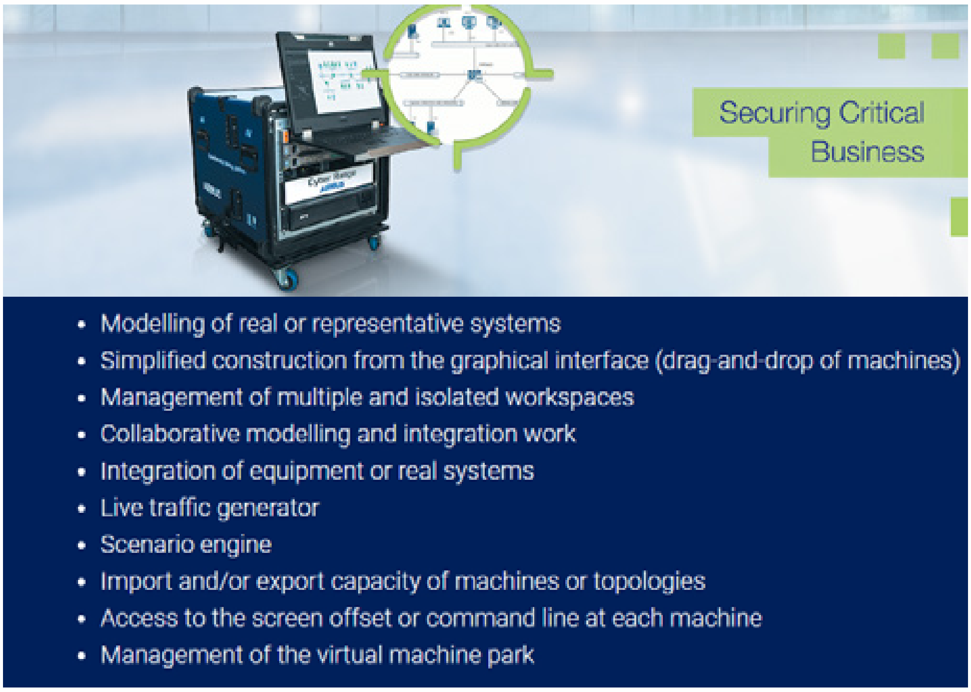
- New scenarios integrated by default
- Various training packages available

AIRBUS
CYBERSECURITY

Infographic

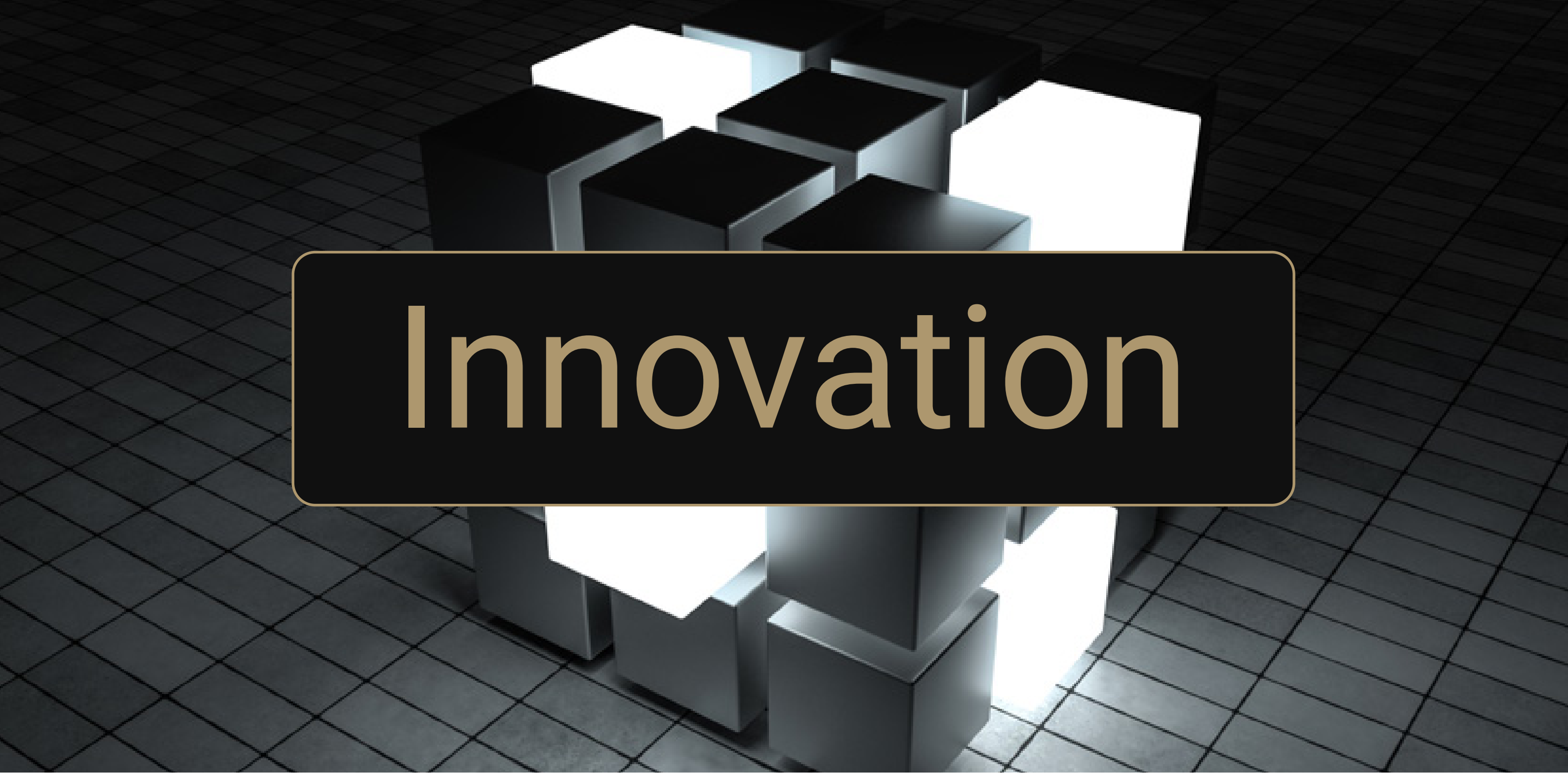
Cyber Range

Main Functionalities



Securing Critical
Business

- 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



Innovation

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:

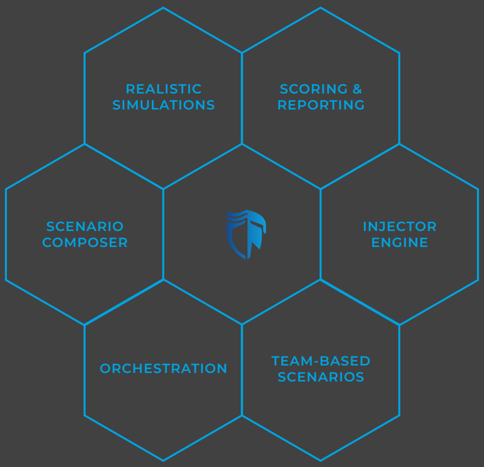
- an environment for on-tap individual training practice with an ever-growing library of simulation scenarios.
- a service for blue/red team exercise platform for SOC/IR teams.
- your own platform, hosted/on-premise according to your organisation's mission, to model even true replicas of your live or 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?

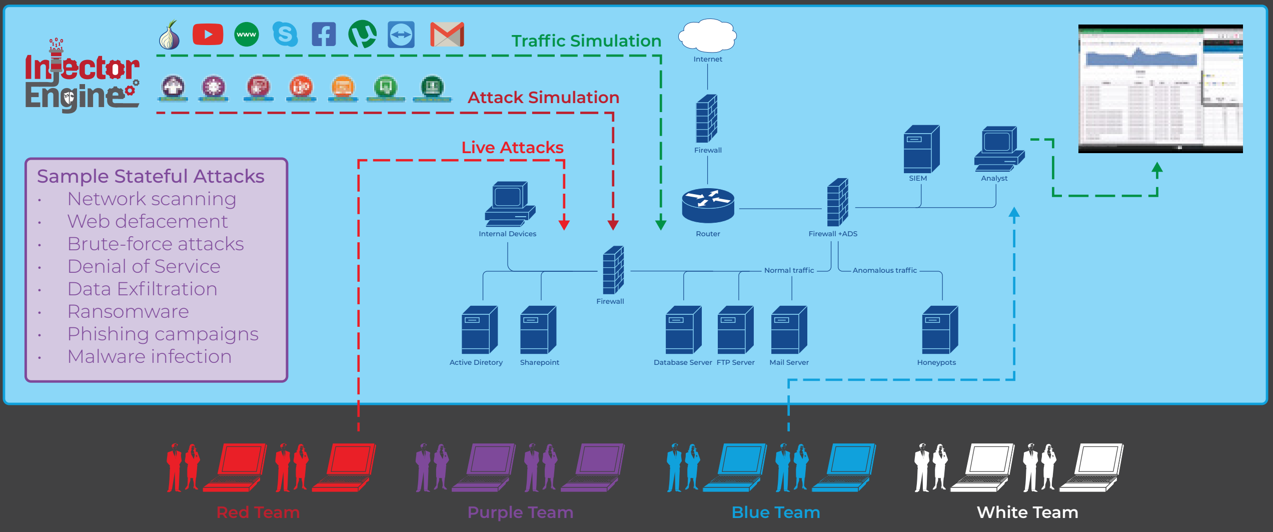


CREATE Design and build custom scenarios, including complex virtual environments, storylines with clear mission/task objectives and cyber challenges.

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.

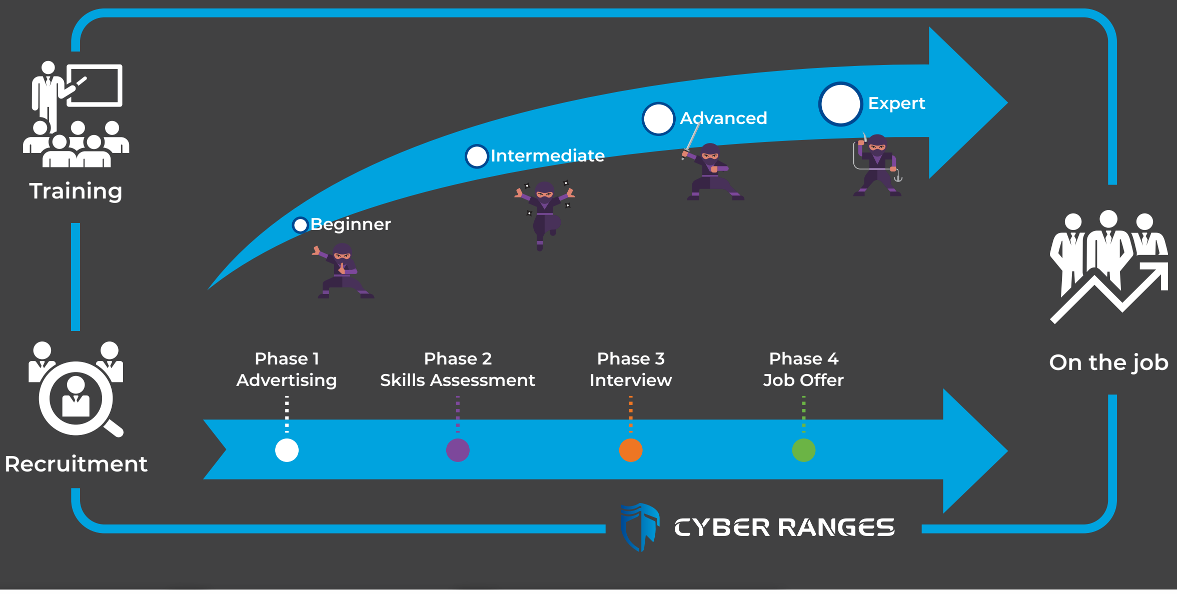
USE Set up and run cyber exercises from the extensive library within minutes, using nothing but a few clicks.

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



Sample Stateful Attacks

- Network scanning
- Web defacement
- Brute-force attacks
- Denial of Service
- Data Exfiltration
- Ransomware
- Phishing campaigns
- Malware infection



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

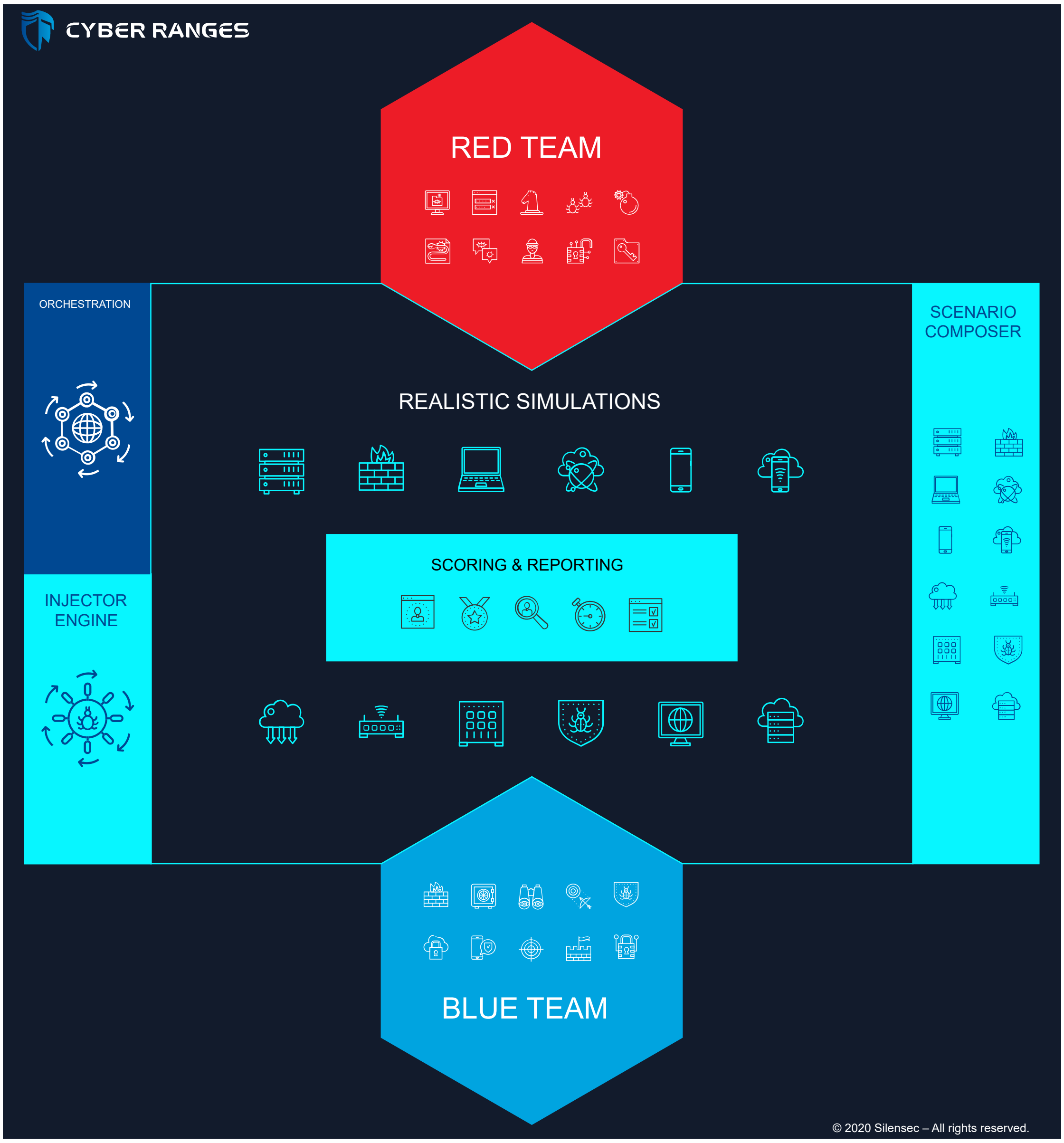
Services provided

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:

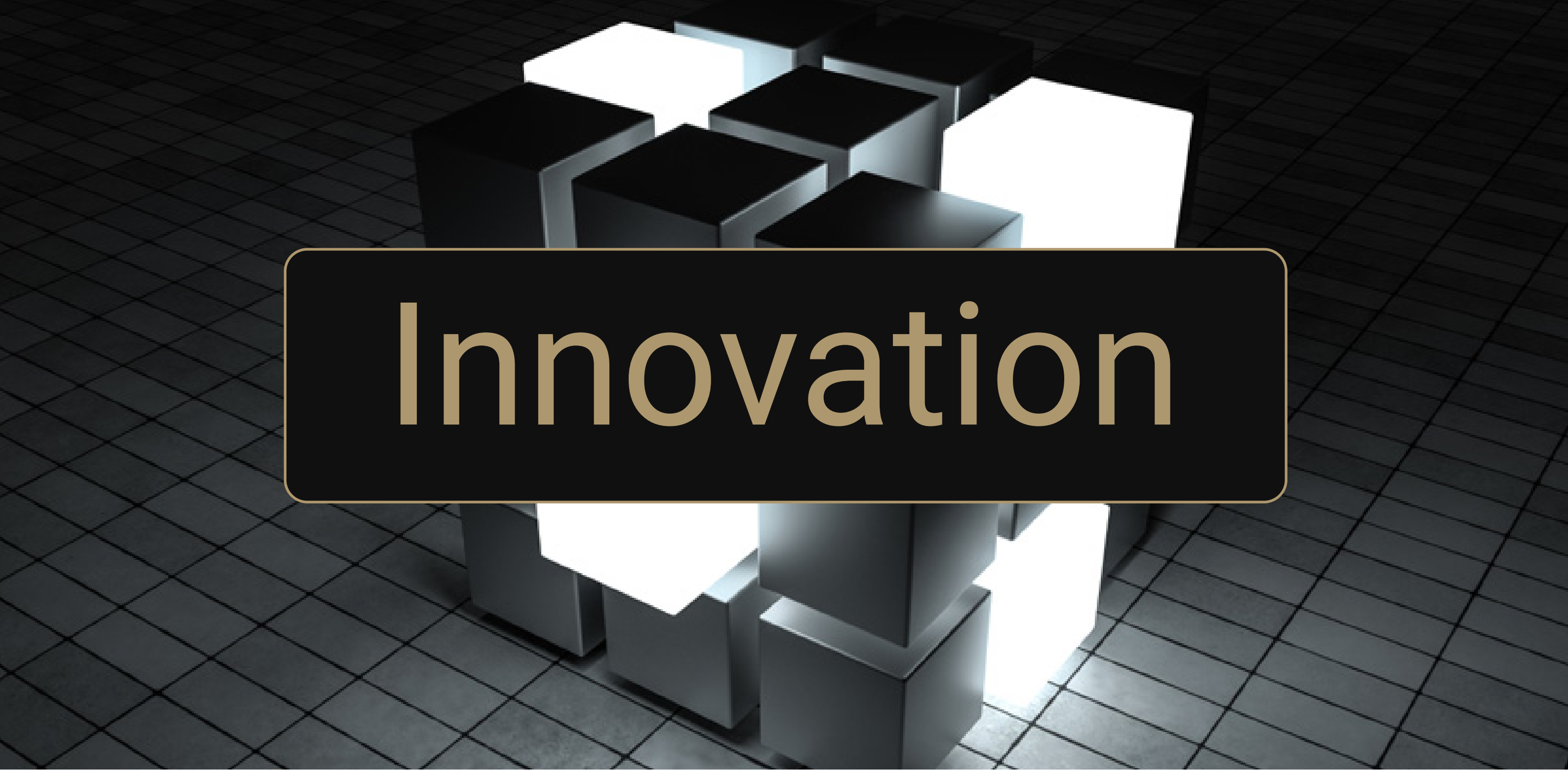
- Advanced scenarios including APT and cyber threat simulation
- Custom simulation replicating the target organization’s environment
- Delivery of cyber drills and hybrid table-top hands-on simulation exercises
- Large-scale security personnel selection and recruitment based on hands-on competence assessmentScoring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

Infographic: Red vs Blue Team realistic simulations



Certifications

silensec™
iso27001 Certified



Innovation

senhasegura

Global Privileged Access Management (PAM) Vendor

senhasegura®

01

senhasegura

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

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

senhasegura

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

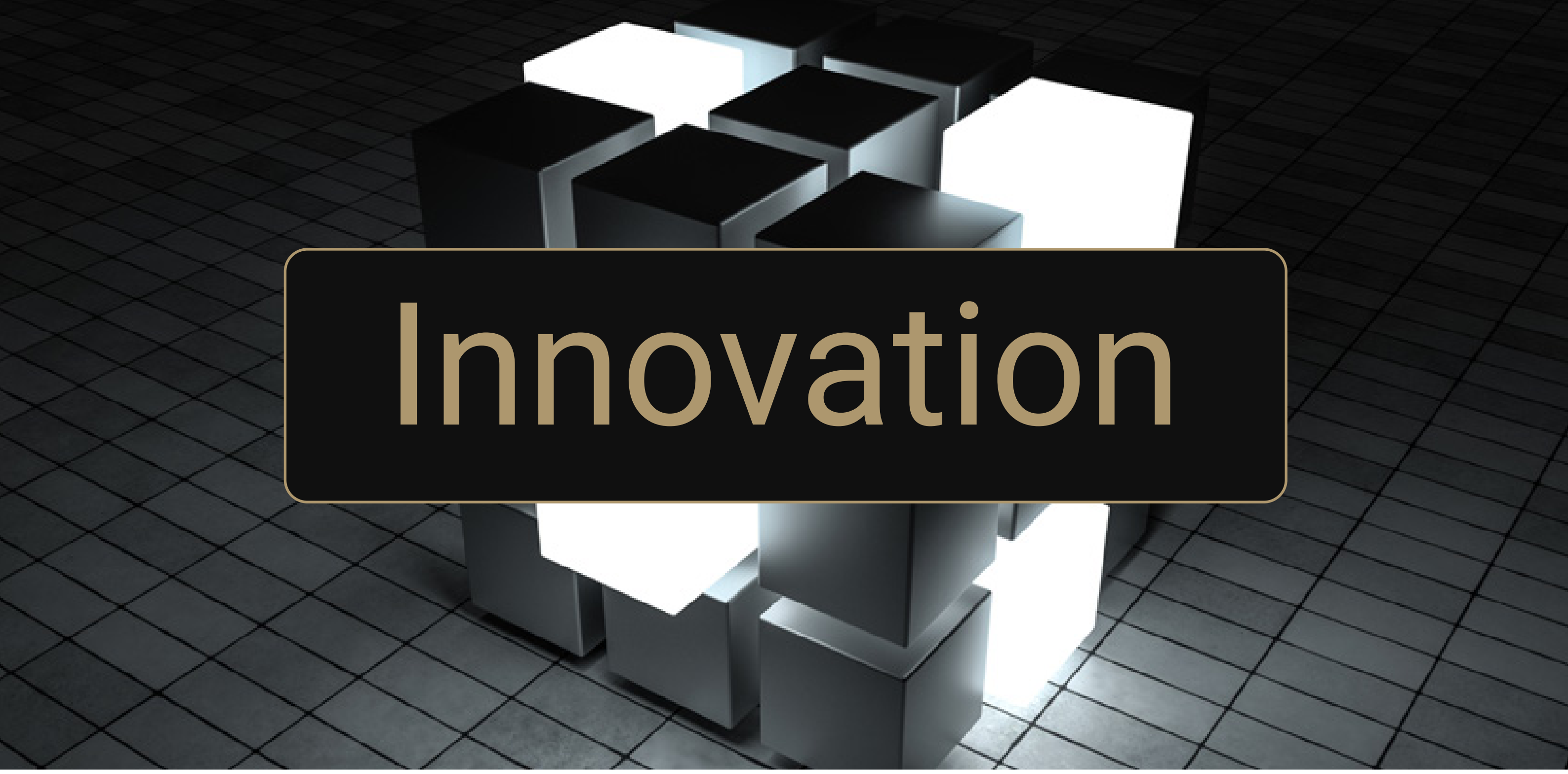
08

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



Innovation

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:

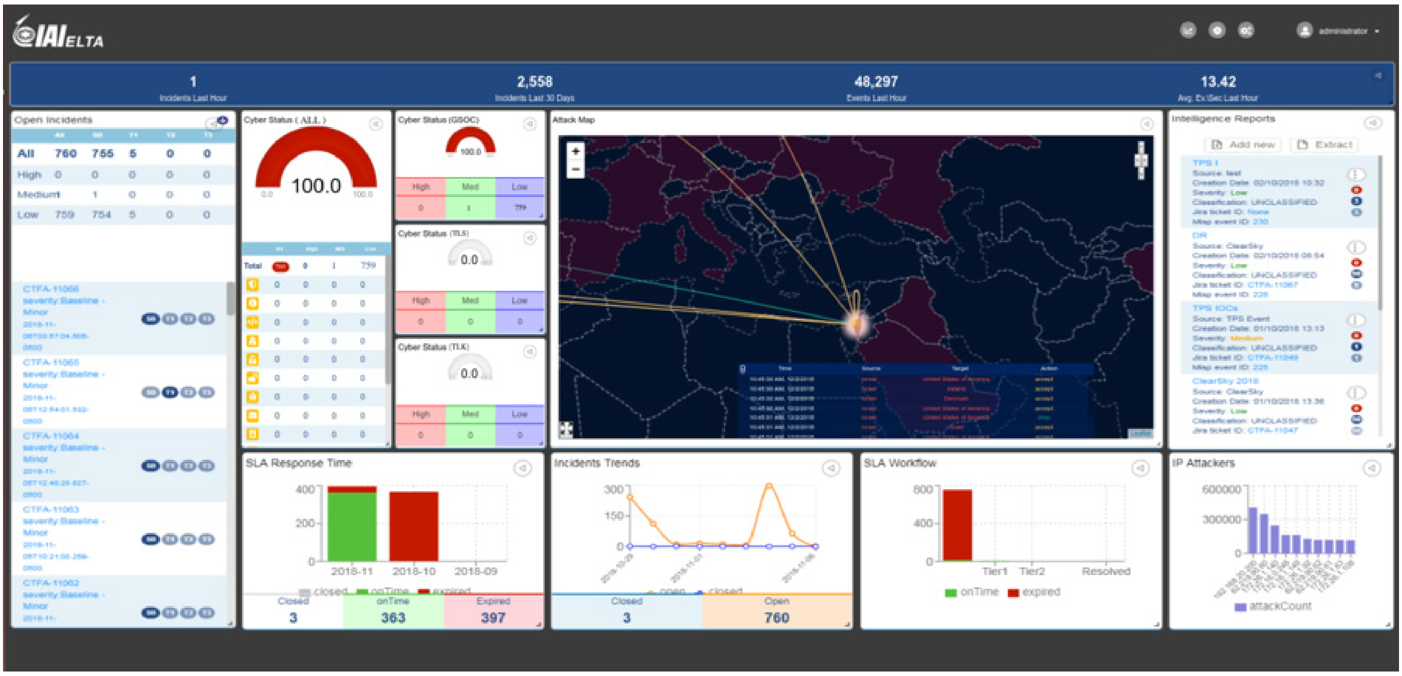
- Government
- Financial Services
- Critical Infrastructures
- Manufacturing
- Law Enforcement & Intelligence Agencies
- Other

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



BACK TO CONTENTS

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

06

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

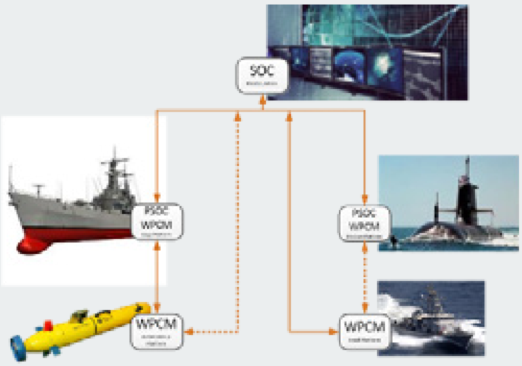
08

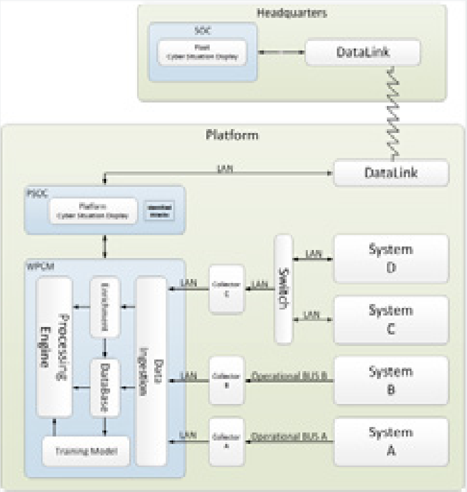
Product in detail: Neptune

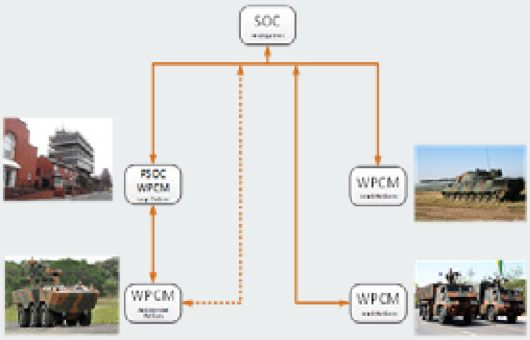
Neptune system detects and reports anomaly behavior of platforms (Maritime, Aviation, UAVs, Automotive, etc.) and systems (e.g. Warfare, C4I, IT Systems, etc.) and generates intuitive, flexible and adjustable cyber situation view.

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

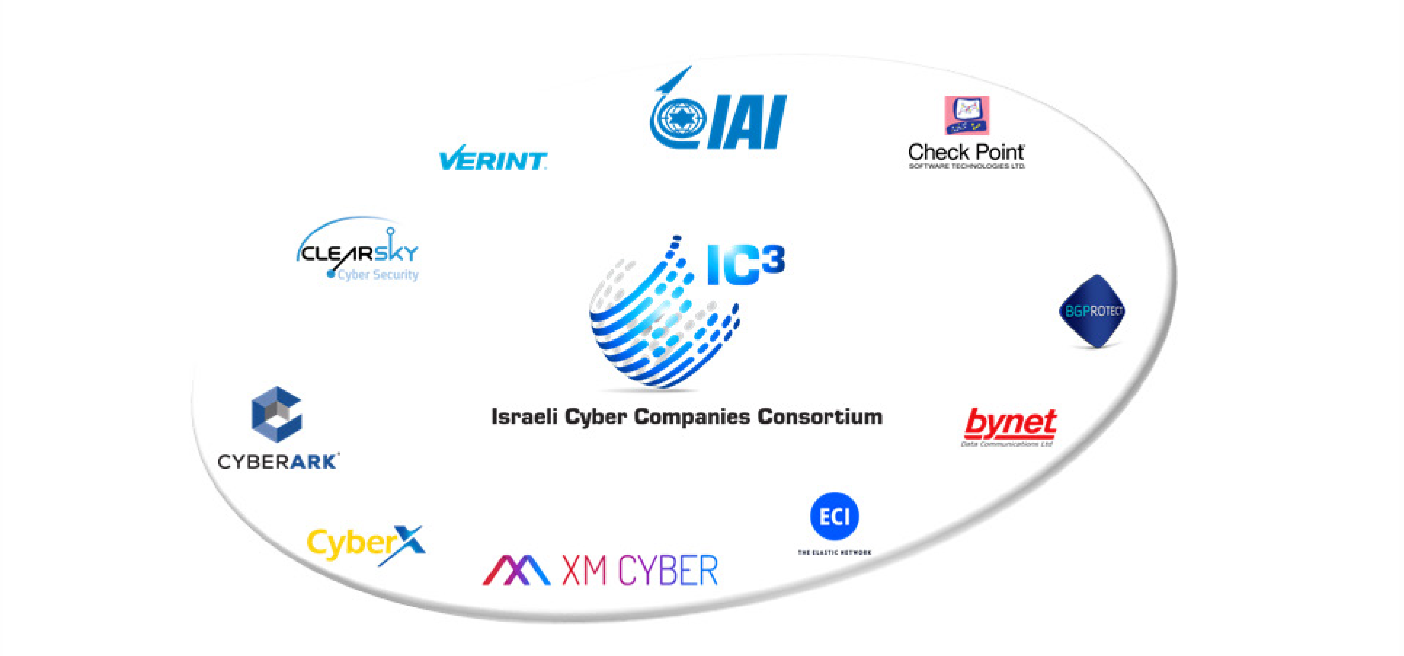
Unique Differentiators

- 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

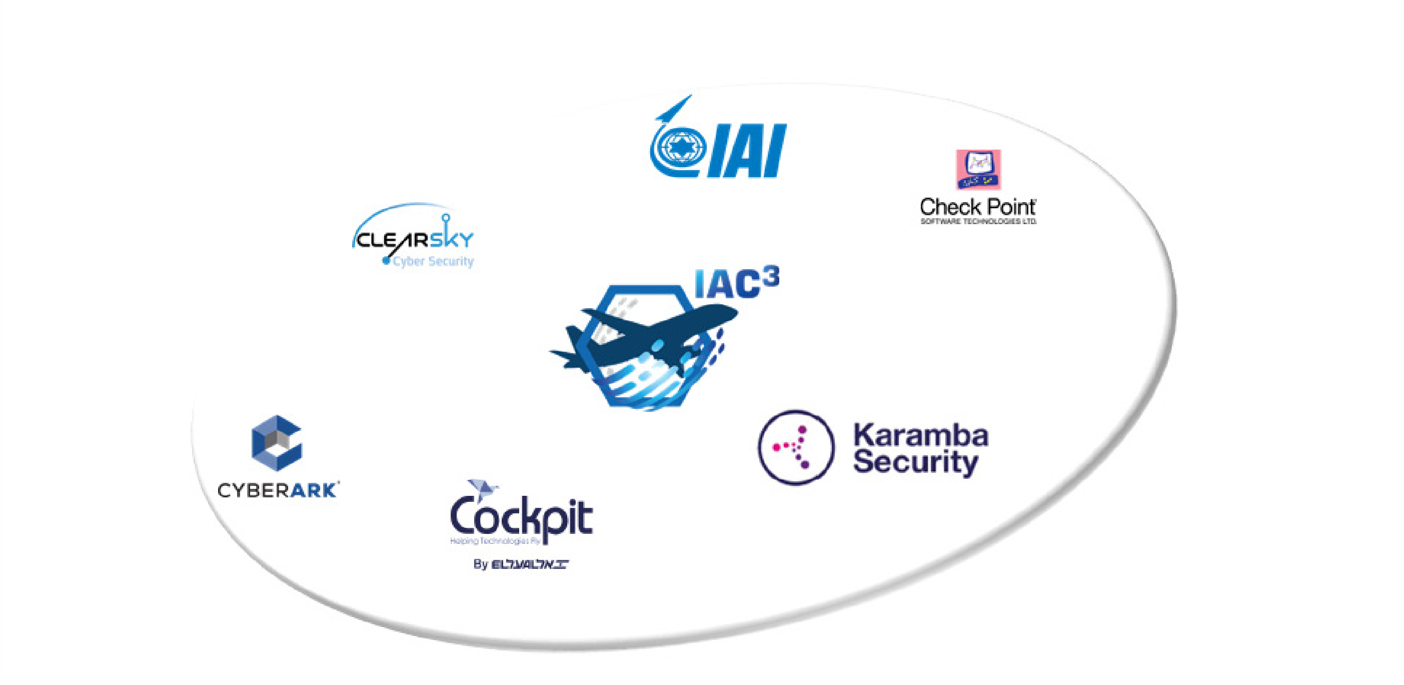
Future Functionality

- Organizational & Industrial solutions
- Improved detection swiftness

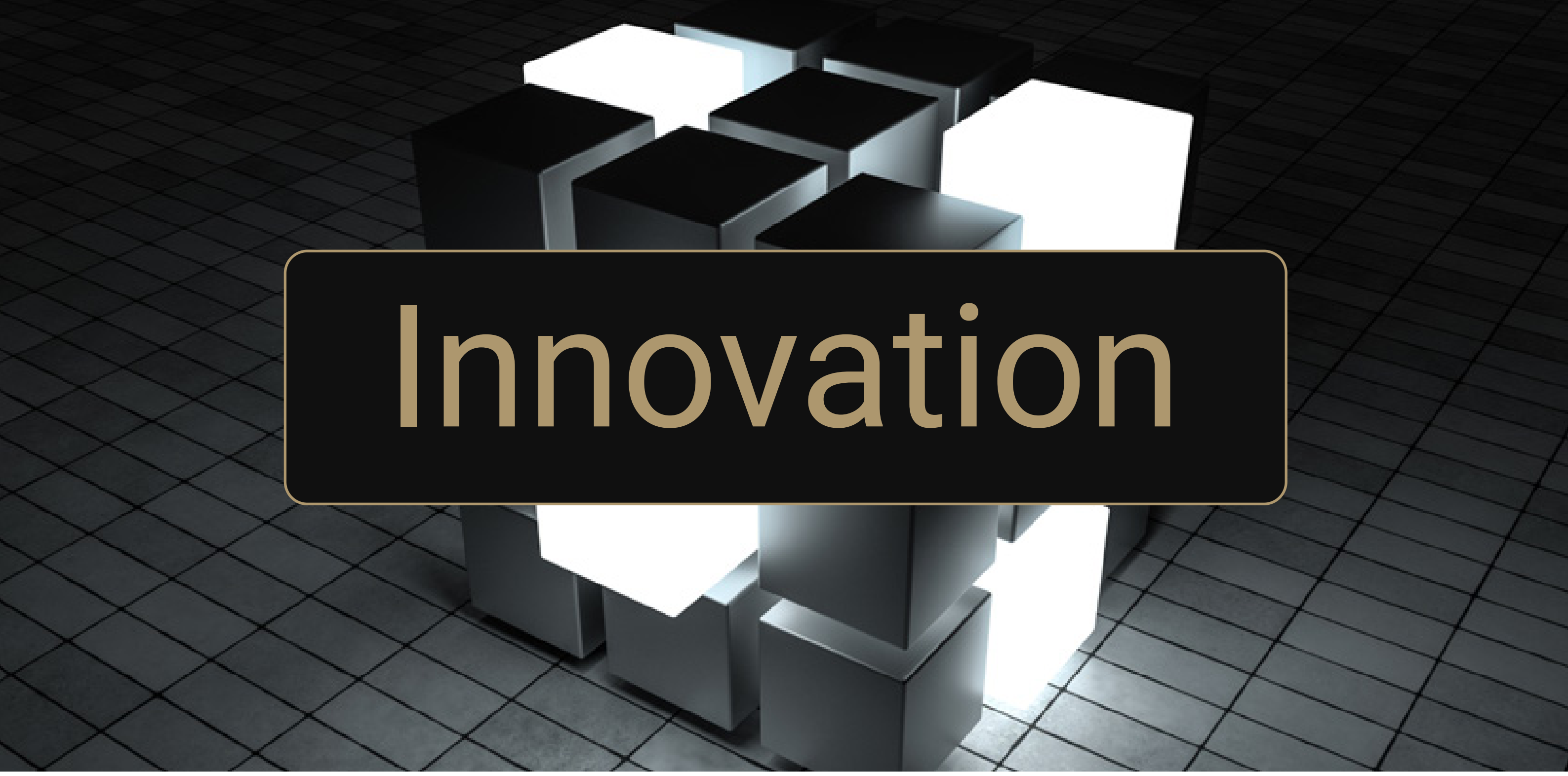
Partners



Israel Cyber Companies Consortium – IC3



Israel Aviation Cyber Companies Consortium – IAC3



Innovation

Stellar Cyber

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

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.

04

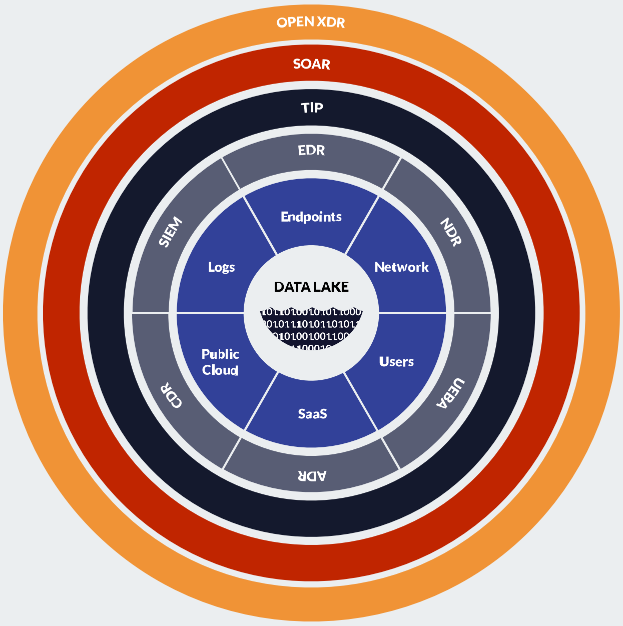
Product in detail

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.

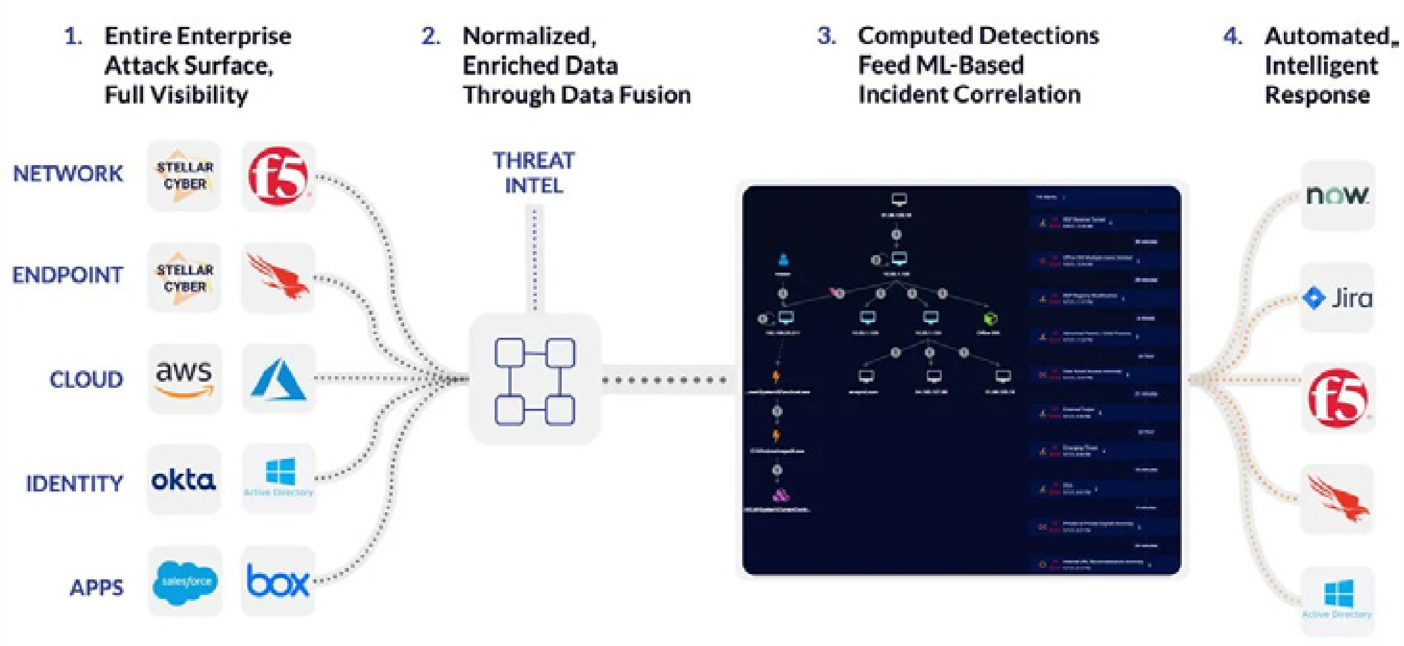
The outcome of Open XDR is protecting your enterprise from threats from a single platform versus multiple tools that have weak or non-existent connections band-aiding it all together. And the ultimate outcome of Open XDR is radically improved detection and response at a price enterprise's can afford.



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.


1. Entire Enterprise Attack Surface, Full Visibility
2. Normalized, Enriched Data Through Data Fusion
3. Computed Detections Feed ML-Based Incident Correlation
4. Automated, Intelligent Response
NETWORK
STELLAR CYBER
f5
ENDPOINT
STELLAR CYBER
CLOUD
aws
IDENTITY
okta
Active Directory
APPS
salesforce
box
THREAT INTEL
now
Jira
f5
Active Directory

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 Incident Correlation

Stellar Cyber XDR Kill Chain

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

© 2023 Smartrev Analytics Consultants SLU. All rights reserved. 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.

Innovation - Insight - Leadership

Cyber Security Observatory®

Cyber
Startup
Observatory®

META - 4th Edition