Cyber Startup Observatory®

APAC

September 2022

The Global Cyber Innovation Network

Startups & Scaleups

Advisors

Investors

Community

Enterprises

The Global Cyber Innovation Network

Meet the Observatory Companies

...featured in this edition

Platinum

CYBER RANGES

B5

AIRBUS CYBERSECURITY

STORMSHIELD

senhasegura

IAI ELTA

Gold

ATEMPO preserving data ecosystems

STELLAR CYBER

CYVIATION

Cyber Security Leaders

Amir Siddiqui
CISO
U Microfinance Bank Pakistan Limited

Esti Peshin
VP, General Manager, Cyber Division
IAI - ELTA

Jym Cheong
Deputy Director, Cyber Resilience Systems
ST Electronics (Info-Security) Pte Ltd

The Global Cyber Innovation Network

Cyber Security Leaders

Rizwan Baig
Senior VP and Head of Governance, Risk & Controls
Standard Chartered Bank

Ammar Shareef
Head of Information Security
Keenu

Enes Yildizhan
ICT Security Chief
Tailwind Airlines

The Global Cyber Innovation Network

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

cyberstartupobservatory.com

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

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

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

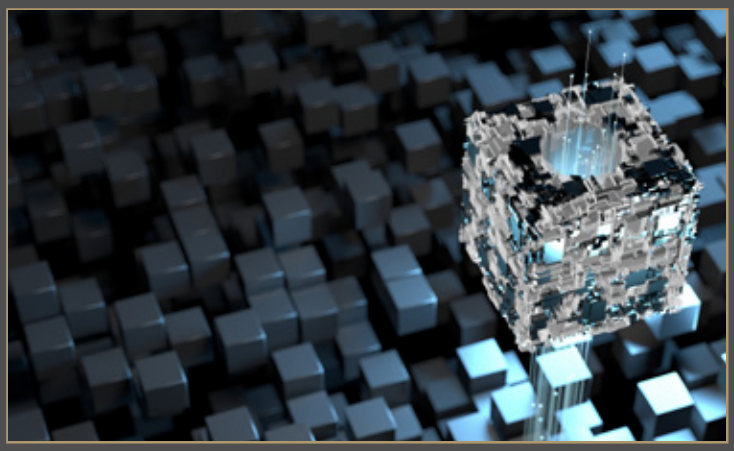
The information provided by the participating startups and companies belongs to them. They remain the sole and exclusive owner of any information provided to Smartev including without limitation, with respect to any intellectual property rights, copyrights and trademarks. Smartrev Analytics Consultants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

Contents

Contents

Contents

Contents



Contents

Overview

It is an honor to present the seventh edition of the **Cyber Startup Observatory APAC.**

Since our first edition we have been able to see the high level of innovation in the region, particularly in markets such as **Singapore, China, Australia, Malaysia and Japan** - although there are also high-quality startups in the rest of the region.

The harsh years of the pandemic imposed significant barriers to innovation - in addition to the untold human cost. This severe event, however, accelerated digitization, generating great opportunities for innovative startups that saw the opportunities.

Ransomware attacks skyrocketed, even targeting critical infrastructure. Cyber security companies and entrepreneurs have played a key role in protecting our society.

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 Seventh Edition Observatory APAC.

2022 will also see us build on the success of last year's Cyber Security 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 two series of events:

- The Innovation Series (i-Series)
- The Bespoke Series

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 Seventh Edition Observatory APAC 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, META Europe, and Africa, 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 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:

Amir Siddiqui, CISO @ U Microfinance Bank Pakistan Limited
Esti Peshin, VP, General Manager, Cyber Division @ IAI - ELTA
Jym Cheong, Deputy Director, Cyber Resilience Systems @ ST Electronics (Info-Security) Pte Ltd
Rizwan Baig, Senior VP and Head of Governance, Risk & Controls @ Standard Chartered Bank
Ammar Shareef, Head of Information Security @ Keenu
Enes Yildizhan, ICT Security Chief @ Tailwind Airlines

The **Seventh Edition Cyber Startup Observatory APAC** 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:

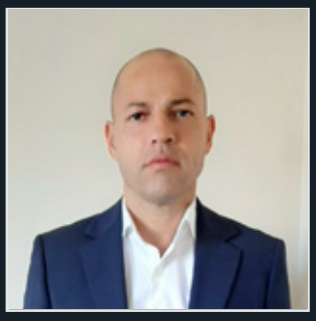
- User Emulation in next-generation cyber range environments
- Addressing Banks' non-financial risks: Moving towards a resilience-based approach
- Cyber Forensics in The Cloud Environment
- Cloud IAM: What Do You Need to Know?
- How Seemingly Insignificant Data Points Add Precision to Open XDR
- Best practices could save you!
- Can we still trust flight instruments in the cyber age?

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

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.

Thanks, as ever, to Unsplash photo repository and its second to none photographers and creators (https://unsplash.com) for the inspirational pictures which have been used in this publication.

Jose Monteagudo
Editor-in-Chief



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

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

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

Sections

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

The APAC CyberSlide

Product

The CyberSlide - Product

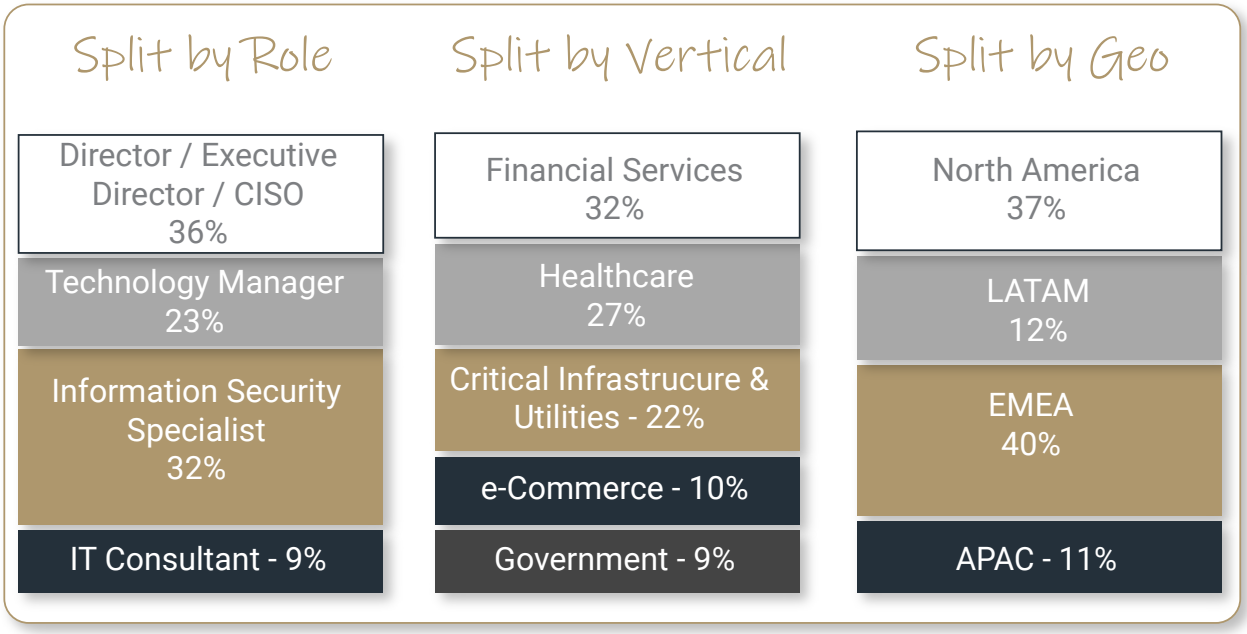
The CyberSlide is dedicated to supporting the extensive cybersecurity market active within the Cyberslide's country, but which has a truly global impact. Cybersecurity has a key part to play not only from the perspective of innovative startups looking to get a foothold in the industry, but also for those 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 Cybersecurity Observatory - most notably the @CSOFinder search engine - which aims to simplify the cybersecurity technology selection process and offer the best solution for any cybersecurity 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.

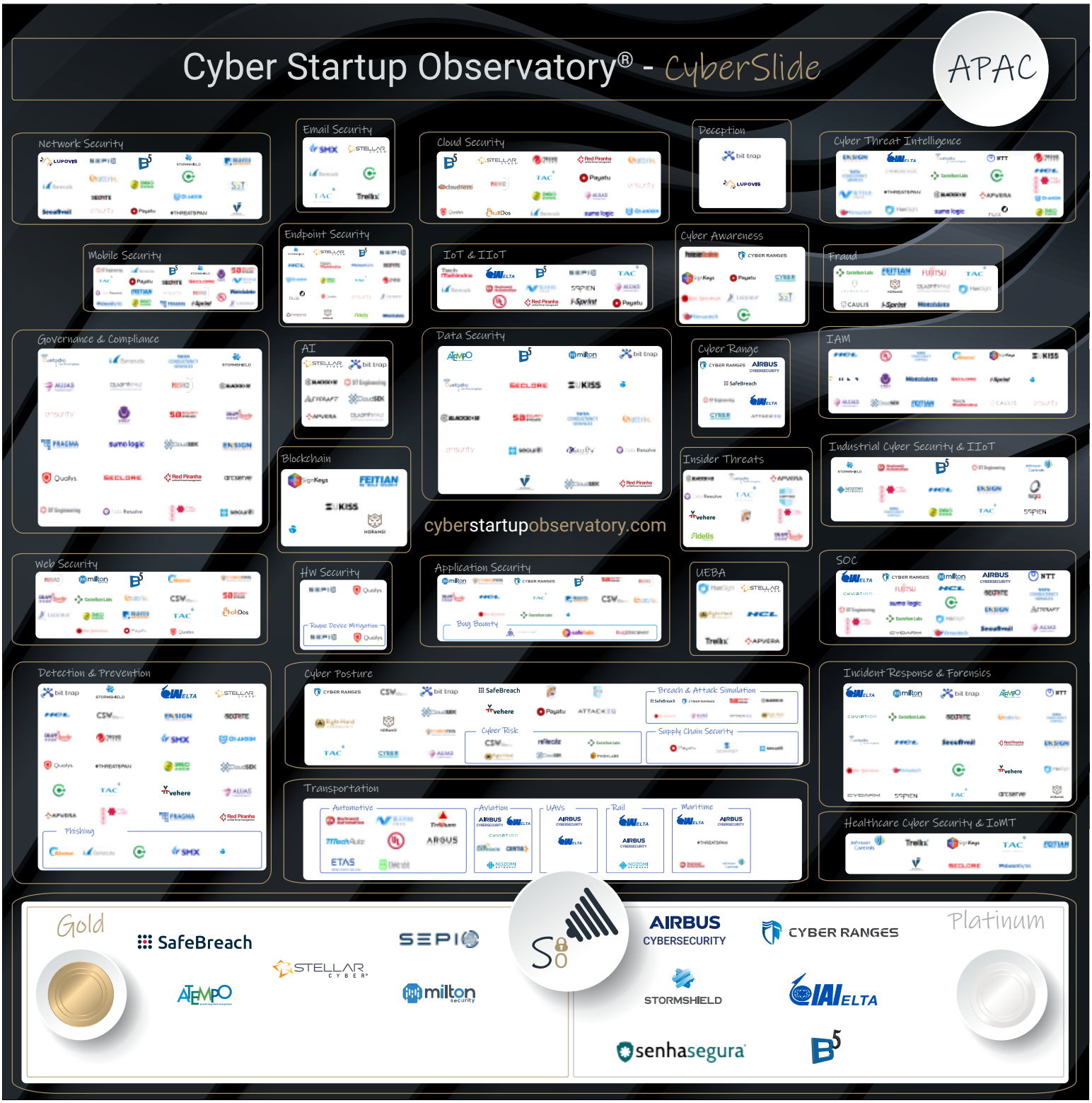
Given the impossibility of including every single one of these companies on the CyberSlide, it's important to mention that all participating companies have been contacted individually in order to ensure the correct categorization process has been negotiated and agreed upon.

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.



A world-class

cyber security ecosystem



200+ Companies featured

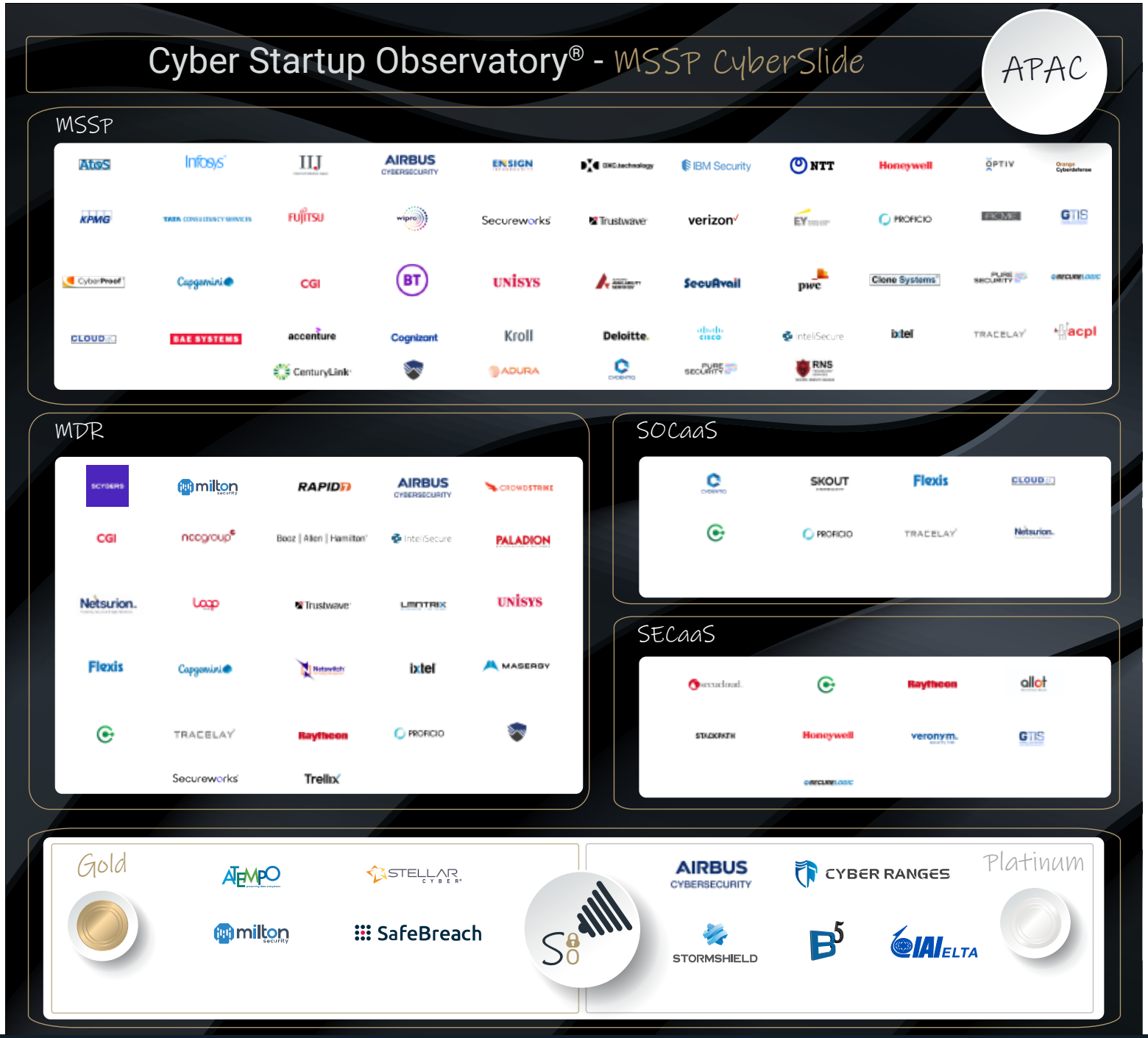
Resources

The APAC CyberSlide

Managed Security Services (MSS)

A world-class

Cyber Security ecosystem



100+ Companies featured

MSSP, MDR, SOCaaS & SECaaS Providers

Amir Siddiqui

CISO @ U Microfinance Bank Pakistan Limited

Amir Siddiqui

CISO @ U Microfinance Bank Pakistan Limited

I am BS (4 Years) in Computer Science from University of Karachi, along with valuable experience of 17+ years in Banks of Pakistan and Retail Sector of Saudi Arabia.

I hold certifications of CISM, CDPSE, Senior ISMS Lead Auditor and CEH. I have experience of 12+ years in Information Security, primarily Heading the IS function with contribution to Governance, Risk and Compliance, alongside with Security Operations, Risk Assessment, Offensive/Defensive Security programs, Business Continuity Planning & Disaster Recovery, etc. I am part time instructor on various cybersecurity courses.

Key achievements include, but not limited to it:

1. *Developed ISO 27001 compliant Information Security Policies and Procedures for 4 Banks, including one 'Big-5' Bank.*
2. *Presented IS Dashboards to Management and Board committees on forums like ITSC, BRMC, BITC, etc., at the quarterly meetings.*
3. *Developed Security Operations Center for 2 Banks, one through MSSP and other on-premises SOC supporting all three Layers from L1, L2 and L3 Analysts.*
4. *Headed CERT and CSIRT for 2 Banks as a CISO, and participated in joint investigation of cybersecurity incidents together with IT and pertaining stakeholders*
5. *Performed Risk Centric Threat Modelling with process for Attack Simulation and Threat Analysis*
6. *Enabled & achieved PCI-DSS for 2 Banks and achieving SWIFT CSF 2019 for 1 Bank.*
7. *Developed Security Operations Manual, with emphasis on Security Alert triage process, Vulnerability Management Program, Cyber-threat Intelligence Program, Red teaming exercises, etc*

8. *Deployed SIEM, EDR, PAM, DLP, IAM, VA Scanners, SOAR and various other cyber-security tools in 3 Banks, including development of Playbooks and Runbooks for effective monitoring as per the design of cybersecurity controls crafted in policies and procedures.*

9. *Developed Security Use Cases for all security tools and appliances with support from international guidelines as MITRE ATT@CK, NIST, CISA, ENISA, CIS, etc.*

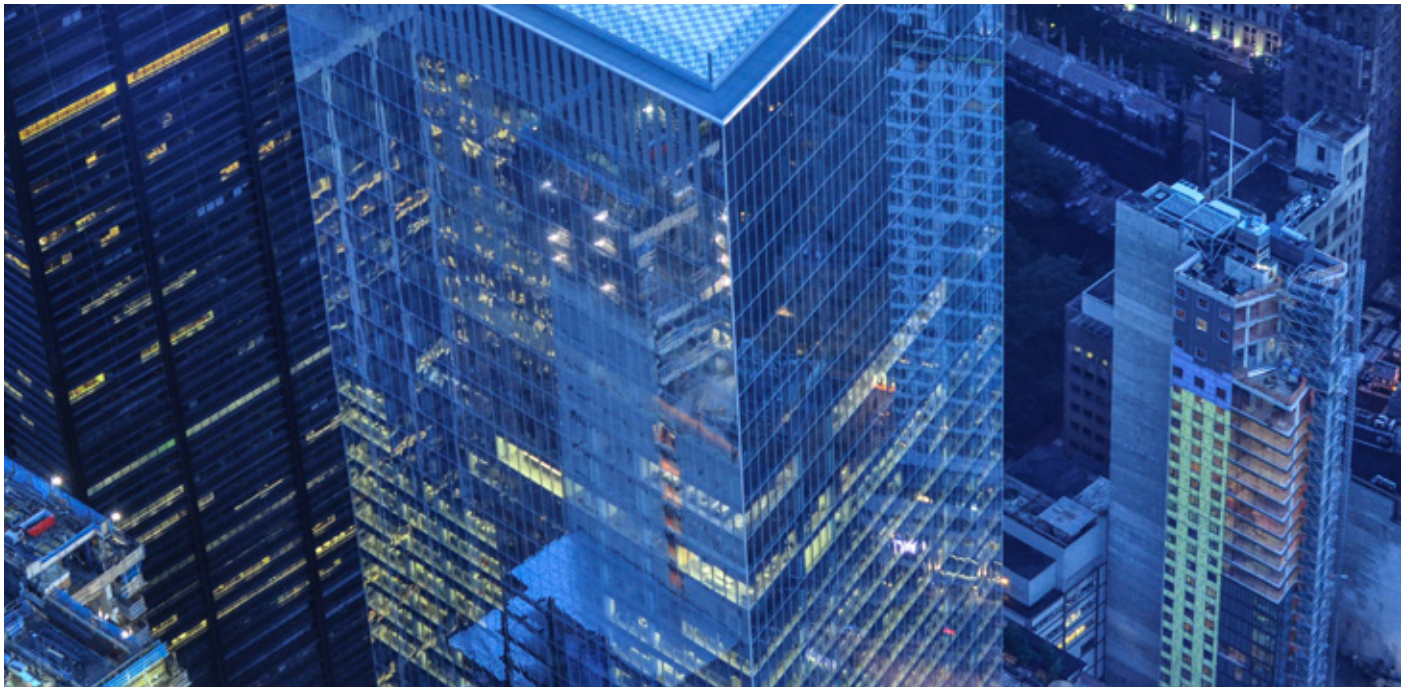
10. *Conducted Enterprise-wide Business Impact Analysis (BIA) and Data & Information Classification activity for 4 Banks including present Bank, performing DPIA (Data Protection Impact Assessment) for current bank.*

11. *Assurance for regulatory compliances for various SBP Circulars and Frameworks issued time to time, that include but not limited to, Payment Card Security Framework 2016, Enterprise Technology Governance and Risk Management Framework 2017, Security of Payment Card - 2018, Digital Onboarding Framework, etc.*

12. *Performed comprehensive IS Risk Assessments for 4 Banks, and maintained Risk Registers for all IS Risks with reporting to KRIs for Operational Risk Department.*

13. *Conducted Information Security Awareness & Training Sessions for regular and technical workforce, for 4 Banks. Conducting subject trainings since 2009.*

14. *Cyber Security Assessment on policies & controls, overseeing Network & Infrastructure appliances for security assessment, facilitating Penetration Testing and Vulnerability Assessment Exercise, etc.*



Why did the role of CISO appeal to you and how do you see the role evolving in the future?

Since I completed my education and stepped into the professional world, I have the instinct to work in security domain of Information Technology. I was associated with an international association of computing in university days, where I learned about the basics of cybersecurity and challenges the world is facing about it, then.

However, those were not the days when digital dependencies of business were that much. Internet was thinly available to the masses and cyber-security roles were not that much popular as well.

The CISO roles appeals to me because of its liveliness, its agility to adjust itself in the new technology ventures and power of its adaptability with all industries.

Most prominently the role gets interesting because of challenges for newly developed cyber threats and everyday complex exploits developments.

CISO role is evolving very rapidly, the one who has more business related responsibilities than the traditionally technical threat hunter.

Usually CISO is considered as a techy, who just knows all about defensive and offensive security along with GRC and International Standards.

However, the paradigm has shifted and now CISOs are considered as business enablers, where they need to understand business strategy, align security strategy accordingly, and deploy security controls accordingly.

Monitor the security controls 24/7 and report results to management and stakeholders to either accept, buy or mitigate the risks. CISO are getting more influential as any other CxO in the organization and have power to enforce security controls, as per the business needs and requirements.

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

CISO is a great interpreter, and treats people the way they want to be treated. Becoming a CISO is a non-traditional career path, and it is still being developed, mainly because it's a relatively new position.

A CISO must be able to go between the two worlds of executives and security engineers, which are two different cultures with their own discrete languages and priorities.

You need a background in one, then seek mentorship in the other. A CISO is somebody who's an executive that understands cybersecurity and can translate it to executives in non-technical strategic terms.

A CISO translates this information so that the executives can understand the risk, make proper decisions, and be held accountable for proper security and/or the impact breaches might have on the organization.

Your mind was created to solve problems. If you don't give it good problems, it will create bad problems.

There are three pieces of cybersecurity, and they are what you should stay focused on:

1. Critical Data and Information
2. Risk Assessment and mitigation techniques
3. CIA triad, Confidentiality, Integrity and Availability

We hear about People, Process and Technology in cyber, but which do you consider the most relevant?

It's hard to decide that which one from People, Process and Technology should be preferred as most relevant. The three are very much dependent on each other and one can't survive without the strength of other. In cyber people are the ones who are the weakest link, the process is the one where the vulnerabilities can found a way without being noticed until you perform audits or assessment activities, and technology, if not properly maintained or configured can expose the organization to unprecedented amount of exposures.

So therefore all three are important and a must. But if asked to choose one of them, my answer would be People. We choose them to protect the organizations, we assign them responsibilities to implement process and the underlying technologies, we assign them the job roles to monitor, and much more. The process and technology will stand idle if we will not train people on the technology and its cons and pros related to misuse or negligence.

Second most important fact of considering people is about monitoring them for their usage of technology and interaction with other processes. It's the people that use the technology to facilitate themselves and other ones who may not or may be part of same or any other process, which makes it a complete cycle of any business case. Human or People being the weakest link can exploit the whole business case, if they are not suitably monitored and reported for necessary actions.

Security Operations should also consider human based use cases that could identify the technology or process misuses.

Are there any common traits as to what makes a successful security program?

The most common traits that I use to make my security program successful is by dividing and ruling the different security domains. The core domains that I focus on are GRC (Governance, Risk and Compliance), Operations and Projects. The core is with GRC, which is being authorized to manage the entire security program.

The top is resided with the Security Strategy, Policy and Procedures, which are inculcated to the security operations, risk assessment, security reviews and compliance programs.

Concluding that, GRC should be the center point of running entire Security Program, where they input to and outputs from GRC should be documented.

The metrics for security operations should be derived from the GRC function and its output should be evaluated by the GRC team, so necessary policy and procedures should be changed or adopted.

Should we be focusing on technological innovation or shift to a more people-centered approach for cyber risk mitigation?

Like any other domain, cyber risks can be reduced but never be eliminated. However, unlike other domains the risks belonging to cyber security can change in a matter of seconds.

So the use of technology in managing and updating the necessary controls and their pertaining risk factors.

There was time when people were using disconnected security appliances and it takes substantial time for analysts to consolidate the data from various sources and then come to a conclusion for the remediation and actions. However, with the passage of time, more advance cyber-attacks are happening, which require immediate actions from cyber security analysts.

Similarly, security tools and appliances also needs to be integrated into a single platform where pre-built or pre-set rules must execute to stop any unwanted action by any adversaries. This has resulted in a concept and evolution of Security Orchestration and Automation with Response (SOAR) components.

Having said that it's the people for whom security is all about. People decide what business they want to use technology for, they decide to focus on the risks that they think are important to evaluate, they learn from the process and adopt new ways to change it. People are the ones that deploy, use or run, patch and maintain the technology and security products.

People are the individuals that review and audit the technology and monitor security tools, and response to the suspicious things. Therefore, it's the people that interact over the conclusions, actions and anticipations from other people.

So, in my opinion Cyber Risk Mitigation should be focusing on People rather than technological innovation.

What new security challenge are arising as business enterprise network are changing and become more complete?

With the advent of new startups and Fintechs coming along, the business models are becoming more integrated with each other and are becoming more complex.

The urge to bring the innovative idea and get into the business as quickly as possible is giving birth to the lot of open source codes into the front end application and interfaces, and it's the place where the risk resides.

If one is not sure about the vulnerabilities of its application and exploits that could happen the application will remain prone to unwanted cyber-attacks.

What do you see, if any, as the gaps in current practices around risk management?

The current practices of risk management roam around the facts of giving more importance to low risk assets rather than reassessing risk score to the assets with respect to growing threats and vulnerabilities. Risk score is very live value that can increase to dangerous level and similarly can be reduced to an acceptable level.

The proper business impact analysis should be an automated and orchestrated exercise that should keep a track on risk value of information assets. The security reviews and audit should be performed on the current risk values not on the results that were available three or six months back.

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

Starting from the Universities and Colleges, we should introduce more and more contents and syllabus into the curriculum, so students have baseline developed for the security field and its sub domains.

Organization should focus more on developing their teams in providing training and certification opportunities. Cybersecurity setups should open up the opportunities for their teams to learn new system and technologies, adopt latest trends.

Train the trainer concept should be brought into the system so people can explore and learn more on cyber security working practices.

Insight

CYBER RANGES

User Emulation in next-generation cyber range environments

CYBER RANGES

User Emulation in next-generation cyber range environments

Authors: Dr. Al Graziano, CEO @ Silensec | CYBER RANGES and Samuel Rodríguez Borines, Offensive Security Lead @ Silensec | CYBER RANGES

At a glance

- 9 minute read
- Actors in a Cyber Range Simulation
- Replicating Benign User Activities
- Current User Emulation Gaps
- Integrating User Emulation and next-generation cyber range environments
- User Emulation with CYBER RANGES

CYBER RANGES

Introduction

In this paper the authors outline the importance of user emulation in the context of a cyber range and more importantly in the context of a next generation cyber range. The ability to emulate user activities and behaviour is pivotal to the delivery of high-fidelity experiential environments for the purposes of cyber security training, assessment of cyber resilience and overall cyber capability development in current and future cyber warfare.

Simulation vs Emulation

In order to understand user emulation, it is important to understand firstly the difference between simulation and emulation as the two terms are often used, erroneously, interchangeably.

Emulation and simulation are terms, which have been traditionally used in the context of replicating hardware devices. In that context, emulation is the process of enabling a computer system (the host) to mimic the hardware and software features of another target device (the guest). In other words, emulation aims to imitate the behaviour of a computer or other electronic system with the help of another type of system. A simulation on the other hand is the process of modelling an environment to mimic the behaviour and configuration of another target device. Compared to emulation, simulation is a lower-fidelity replica of the real system usually used for the purposes of analysis and study rather than for high-fidelity interaction.

Another way of looking at the difference between emulation and simulation is in the context of replicating cyberattacks and threat actors. In such a context, emulation is the process of replicating the behaviour and actions of an attacker in an environment, which behaves exactly like the real one and adheres to all of the rules of the systems being emulated.

In attack simulation, on the other hand, the reproduction of the behaviour and actions of an attacker is implemented differently and does not reproduce all the exact same outputs and effects of a real attack.

Typical examples are phishing simulations or ransomware simulations where the effect of the attack is not to install malware on a phished user or to encrypt the user hard drive after information has been stolen but to show the potential impact of those attacks. And that is why such simulations implement the attack in a safer, hence different, way from the real one.

Actors in a Cyber Range Simulation

When talking about a cyber range and the development of high-fidelity simulation environments, two key components are usually required and they are cyberattacks and user activities. More components can be added or need adding in to achieve high fidelity, depending on the context, such as simulated Internet services, Dark Web, etc. However, for the purposes of this paper, we shall focus on the recreation of user activities.

A typical high-fidelity simulation environment shall usually include different actors. First of all, there are threat actors, either internal or external. Then we have the internal personnel of the fictious target organization being simulated.

Then we have external benign actors such as users interacting with the organization's servers and services.

In order to provide realism to any simulation environment, the cyber range must be able to reproduce (simulate or emulate) the activities of different actors. In this paper we shall focus on the recreation of the activities and action of benign users.

Replicating Benign User Activities

Replicating benign user activities can be done, as we said, through simulation or emulation:

- User Emulation - User Emulation focuses on replicating how a user would interact with a system in real life, including the way a person would use peripherals to interact with a computer system. This way each keystroke, each mouse movement is reproduced exactly the same way it would be performed in real life;

- User Simulation - User simulation replicates the actions and activities of the user but is limited to reproducing only the effects of a user interaction. For example, instead of moving the mouse cursor to close an application window, the simulation would just close the window via an external command, which has the same result, albeit at the cost of lower fidelity;

- User Simulation with Traffic generation – another way of achieving user simulation is to use traffic replay to generate noise in the virtual environment. In a real environment there is usually a lot of user traffic in the network, which can make attacks more difficult to identify. In order to simulate such traffic, simulation software can be used generate network traffic that would simulate different user activities such as Web browsing, video streaming, e-mail exchanges, etc. Once again, such simulation is not high-fidelity as the traffic generated, being simple traffic replay, is not stateful and will not generate logs in the end systems being simulated.

Current User Emulation Gaps

When creating user emulations one of the challenges today is the ability to emulate the user interactions with computer system peripherals such as a mouse or a keyboard, resulting in poor fidelity. A good example of this is the generation of e-mail exchanges in the simulation environment without capturing the keystrokes users would normally generate to create those e-mails, rendering some scenarios such as keylogger-based attacks not possible to simulate. Other gaps exist in the generation of realistic traffic payloads such as sending e-mails with random words, which makes spotting of the actual phishing attack a trivial affair. User emulations should execute actual mouse movement and keystrokes, as well as providing plausible content whenever the user needs to create some text. This can be done with the aid of macro software and AI text-composer tools that can generate coherent text.

Another challenge is the scheduling and orchestration of the emulated user activities. For instance, a real user does not just send e-mails but he/she will also respond to e-mails such as phishing e-mails. The typical user emulation with regards to user activities is based on scheduling specific times or time intervals when such activities occur, making the emulation one-way and not bi-directional such as in a real e-mail exchange and there are not many ways to set up realistic behaviour in response to an event.

When talking about traffic generation there is a similar challenge. The typical approach is based on network traffic recordings and then replaying the traffic mix according to some rules (typically fixed and not adjustable). However, there is a lack of tools that allow for ways to replicate specific traffic at specific times or to generate such traffic in response to specific events during the simulation scenario.

To improve functionality around simulated user interaction, there need to be easy ways to define behaviours with realistic and specific scheduling and reactive capabilities so that users can experience real life-like responses from the simulation scenarios they play. Traffic generation follows similar needs. It needs to be easy enough to set up to emulate all kinds of traffic found in a real environment, with specific scheduling and reactive capabilities so that it provides an environment that mimics actual malicious traffic and attacks.

All such emulations need to be orchestrated to work in a realistic way. The objective is to mix an amount of the three types of user emulation and simulation discussed above to deliver a high-fidelity virtual scenario that allows users to experience the attack in a strictly similar fashion as they would encounter it in real life.

Integrating User Emulation and next-generation cyber range environments

Following on the previous considerations about how a good User Emulation system should be approached, there can be huge improvement on how a cyber range is built and used in order to deliver a realistic experience to a user. These are some key points that benefit of a more robust User Emulation system.

More realistic Cyber Exercises

One of the primary objectives of a cyber exercise or cyberdrill is to simulate attacks, security incidents and other related disruptions to test and teach an organization about its cyber response capabilities. In order to do this in an efficient way, having the most realistic virtual environment possible is crucial. While the emulation of computer systems may be simple, good User Emulation presents some challenges, and a weak implementation can damage the effectiveness of a cyber exercise. There is no point in teaching how to react to certain user behaviours such as e-mails, remote access or even password changes if the simulated environment is not realistic enough.

Emulation of interactions inside and outside the system

A good emulation of behaviours from every point on the network helps to improve fidelity of a scenario. Providing tools to emulate interactions outside the virtual network allows scenario creators to avoid tampering with packets and trying to replicate these behaviours, by just running agents that identify themselves and impersonate IP addresses from the network.

Full control over User Emulation

There are different needs for each type of cyber exercise. Therefore, being able to schedule and run multiple instances of the same User Emulation under a tight control allows for scenarios to be exactly what they need to be in order to obtain the right level of realism and meet the desired outcomes. Not only there is the need to execute User Emulation at a specific time, but sometimes there is the need for multiple executions of the same event from different sources, or at different randomized times.

Ultimately it must be achievable to create user emulations that execute automatically, but those emulations must be customizable in order to have realism. The need for automatic User Emulation cannot be satisfied at the expense of customization. It must be possible to generate new User Emulation templates and then it must be possible to automate the execution of those templates. Many solutions prioritize the former and not the latter objective.

User Emulation with CYBER RANGES

This section illustrates sample User Emulations performed with the CYBER RANGES Injector Engine.

Send e-mail emulating user interaction

The following figures illustrate an example on how to send an e-mail using Outlook via the CYBER RANGES Injector Engine.

The emulation will perform the following actions: open Outlook e-mail client, create a new e-mail, type the e-mail letter by letter and finally send the e-mail.

With this approach it is possible to orchestrate realistic interactions and it possible to repeat them periodically or at a given schedule or in response to specific events.

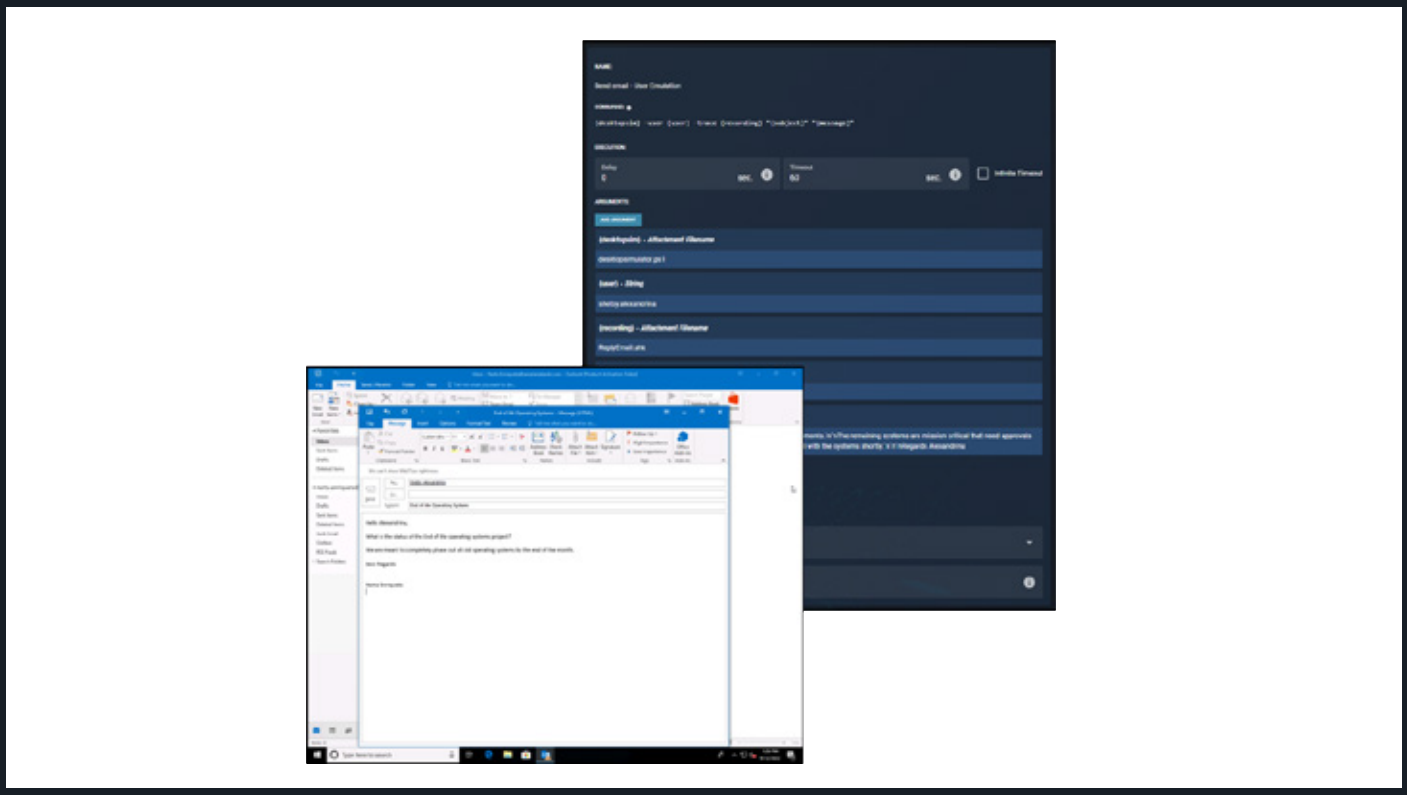


Figure 1: A CYBER RANGES injection to send a custom e-mail message

Replaying Traffic Captures

Using traffic injections, a scenario designer can easily configure the playback of traffic capture attaching it via the web interface.

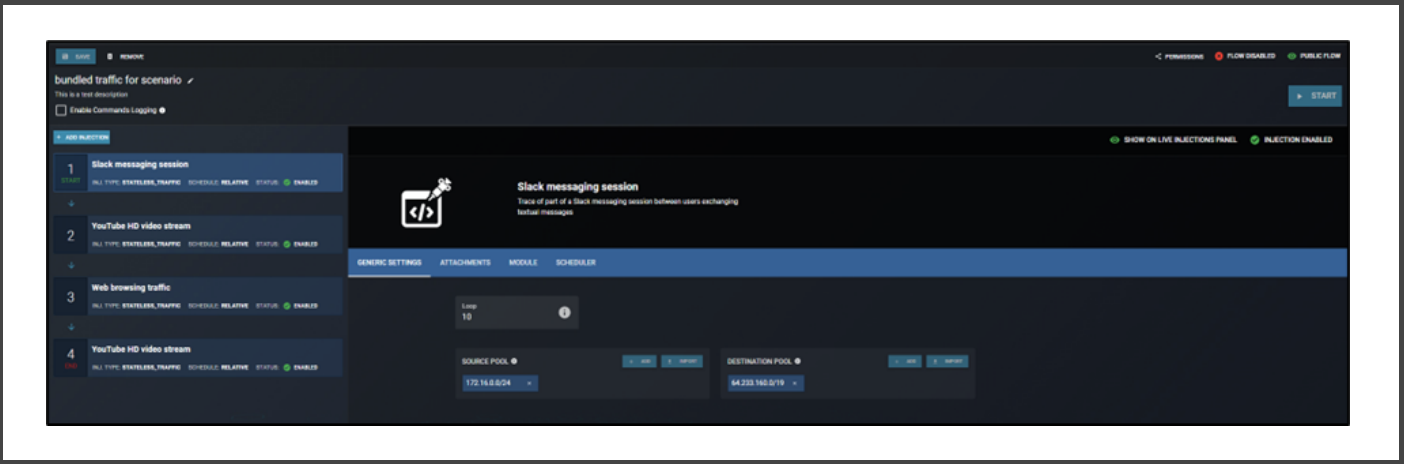


Figure 2: A CYBER RANGES flow of traffic generation injections

Generate and send realistic e-mails using AI

By using in-house developed tools, it is possible to generate realistic e-mails, configuring the type of message that one needs to deliver. This way, human, coherent and cohesive sounding e-mails can be used to feed user emulation scripts further in the execution flow.

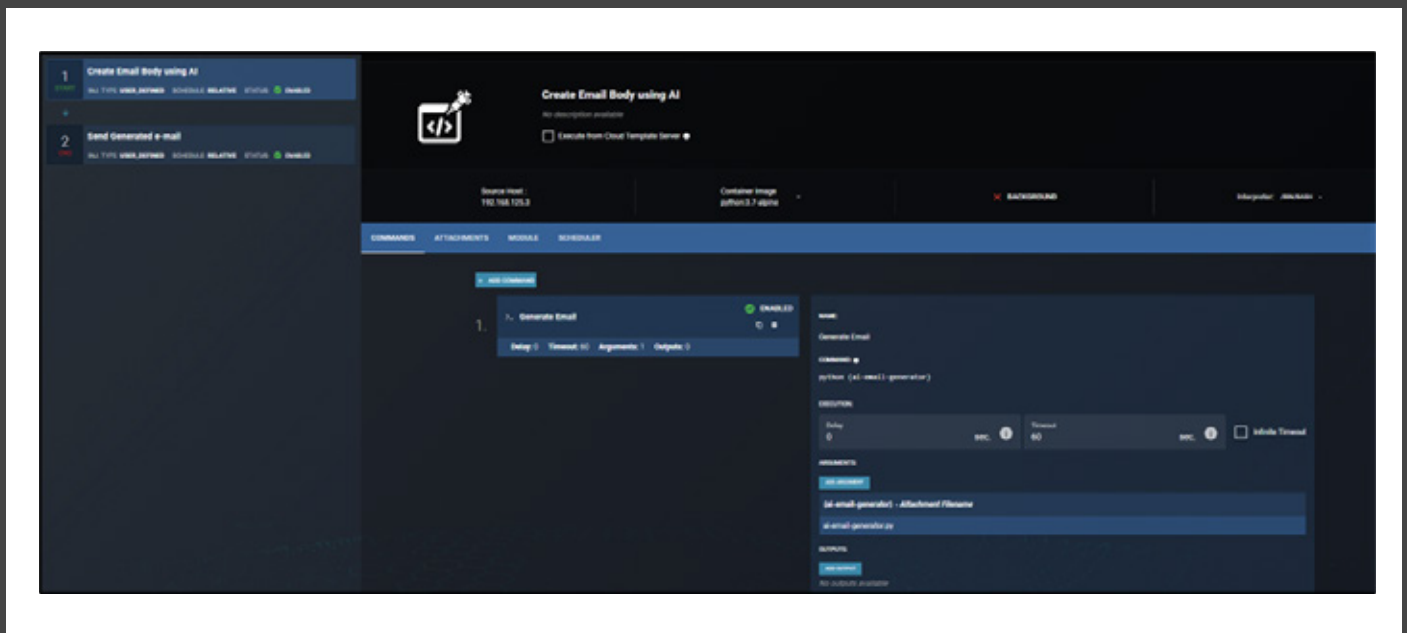


Figure 3: A CYBER RANGES injection that generates an e-mail using AI, and then sends it

Navigate through the Internet emulating user interaction

Similar to sending e-mails, it should be possible to emulate users opening a web browser and then navigating to one or many, randomized places over the internet. This serves both the purpose of generating traffic on the network as well as mimicking actual user behaviour.

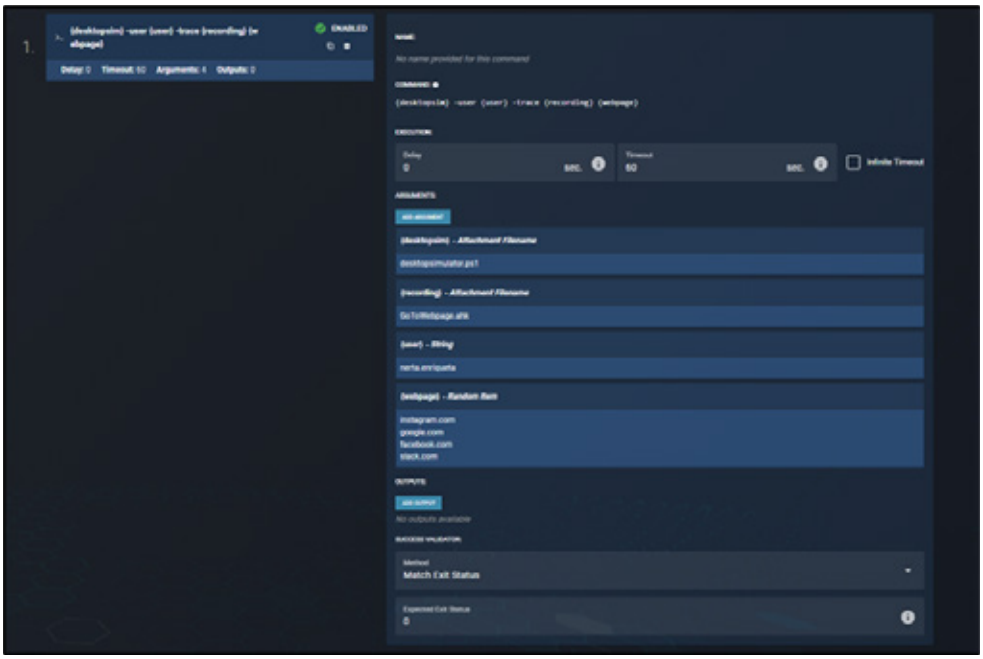


Figure 4: A CYBER RANGES injection showing how to simulate a random navigation to one of the given webpages

CYBER RANGES Injector Engine Scheduler

Scheduling behaviour is a huge part of making a scenario truly believable.

By using the tools provided by the CYBER RANGES platform there are a lot of ways to schedule and configure the behaviour of any given injection.

In the example below a periodic scheduler is used, which provides the means of executing the same behaviour several times (optionally from different sources, automatically) and repeating the execution in a random way.

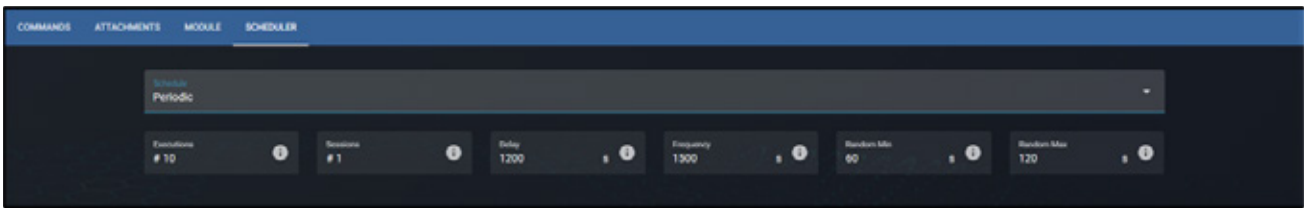


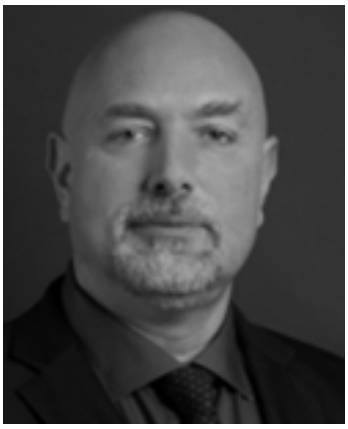
Figure 5: Different settings of injection scheduling in a behaviour that needs repeating 10 times

Conclusions

User Emulation is key to the delivery of high-fidelity cyber exercises and cyber range simulations. While many tools and solutions currently exist, many gaps exist that limit the realism of such simulations.

In this article, we have illustrated some of the current challenges that exist in the market today to achieve realistic User Emulation. We have showcased examples of how some of those challenges are addressed in a next-generation cyber range with the use of its custom-configurable Injector Engine.

About the Authors



Dr. Al Graziano
CEO
Silensec | CYBER RANGES

CYBER RANGES is the ISO27001 certified state-of-the-art next-generation military-grade full-content-lifecycle platform for the validation of threat-informed cyber defence capability and cyber resilience.

Built on cloud technology, CYBER RANGES applies high automation, high orchestration and high scalability to the delivery of even complex large-audience deep-dive C2 drills based on high-fidelity IT/OT infrastructure replicas.

Al actively represents CYBER RANGES as a key member-organization of the European Cyber Security Organization (ECSO), where he co-chairs WG5, i.e. the Working Group on Education, Training, Awareness and Cyber Ranges.

Silensec also leads the sub-working group 5.2 on Education and Professional Training, advancing best practices in the domain of cyber ranges, cyber exercises, cyber security professional training and competency development at European level.

Al is a former UK university course director in information security and currently an accredited ITU cybersecurity expert for cyberdrills.

Samuel Rodríguez Borines, MSc.
Offensive Security Lead
Silensec | CYBER RANGES

Sam leads the CYBER RANGES Injector Engine team, specializing in recreating real-life cyberattacks.

A graduate in computer engineering from Vigo University in Spain, he holds a Masters in Cyber Security from Universidad Europea and a professional certification in ethical hacking from Sentinel One.

Previously with the likes of EY, Deloitte and Amodo, Sam now leads on the design and development of tabletop and technical exercises, the research on APTs, attack campaigns and threat actors, and their replication via CYBER RANGES Injector Engine to automate and support Red Team engagements.

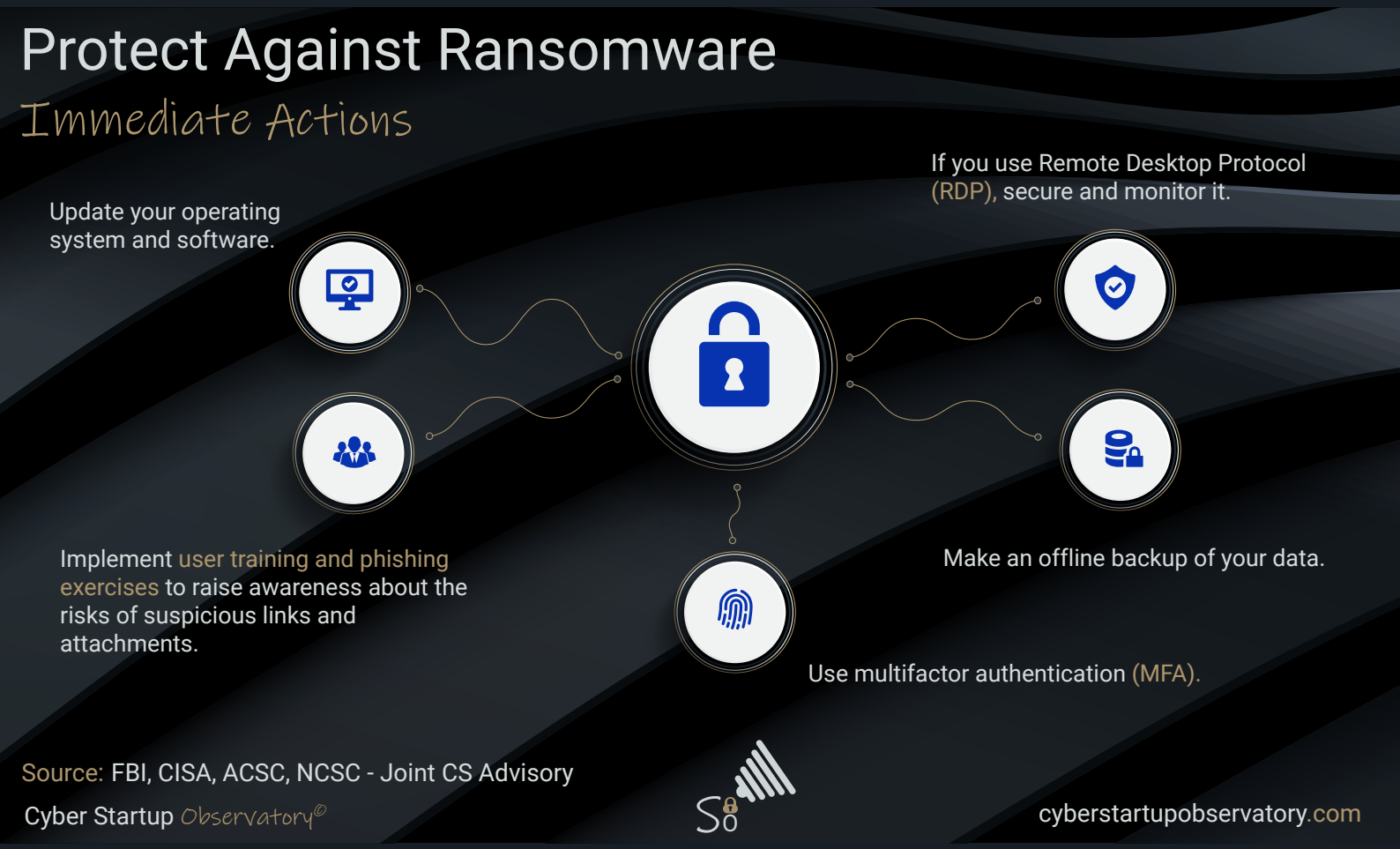
Resources

Infographic

Protect Against Ransomware – Immediate Actions

Protect Against Ransomware

Immediate Actions



Available for download in Press Quality

Infographics - Threats & Attacks

Cyber Startup Observatory - Community

Esti Peshin

VP, General Manager, Cyber Division @ IAI - ELTA

Video Interview

What is ELTA's mission and vision with regard to national level cyber?

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

Esti Peshin

VP, General Manager, Cyber Division @ IAI - ELTA

Insight

BLU5 GROUP

Addressing Banks' non-financial risks: Moving towards a resilience-based approach

Addressing Banks' non-financial risks: Moving towards a resilience-based approach

Authors: Antonio Varriale, Managing Director and Giorgia Somma Business Development Manager @ Blu5 Group

At a glance

- 6 minute read
- Global Payments' overview
- ATM and PoS industry challenges
- Resilience: the new risk-management paradigm for banks
- Zero Trust: Towards business Resilience

The increased digitalisation of advanced economies is affecting the way banks produce and provide financial services to their customers. The capacity to process information and to connect with economic agents are two important results of this process.

In addition to financial risk, digitalisation also poses significant operational risks. Non-financial risks arise from the bank's operations (processes and systems) and are similar to the risks faced by corporates operating in other sectors.

The corporate experience in addressing non-financial risks by moving from a risk-management approach to a resilient-based approach, can provide a model beneficial to banks too. The financial services industry has seen drastic technology-led changes over the past few years. Many executives look to their IT departments to improve efficiency and facilitate game-changing innovation while also lowering costs and supporting legacy systems.

Global Payments' overview

The digitalisation of payment transactions has influenced society and has been playing a role in the change of customers' payment habits, accelerating a series of existing trends.

Global cashless payment volumes are set to increase by more than 80% from 2020 to 2025, from about 1tn transactions to almost 1.9tn. According to a recent analysis by PwC these numbers will nearly triple by 2030.

Asia-Pacific will grow fastest, with cashless transaction volume growing by 109% until 2025 and then by 76% percent from 2025 to 2030, followed by Africa (78%, 64%) and Europe (64%, 39%). Latin America comes next (52%, 48%), with the US and Canada growing least rapidly (43%, 35%).

However, the pace of adoption of cashless transactions differs worldwide, partly because of the different technological approaches, cultural backgrounds and trust.

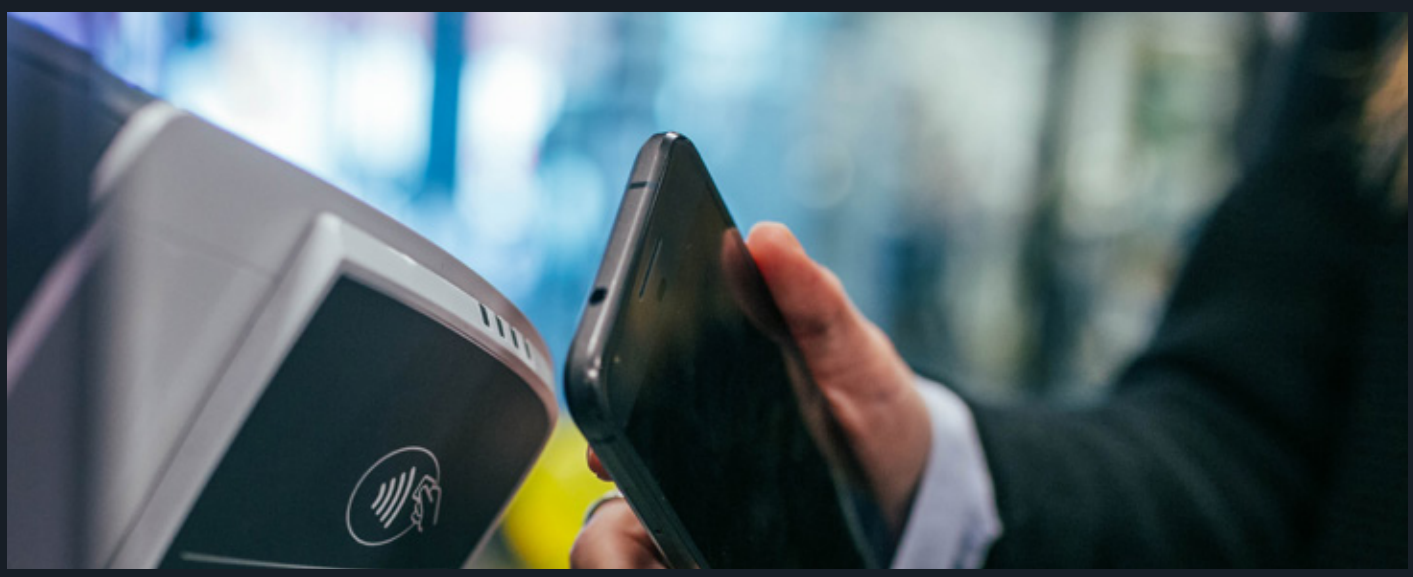
Underneath the shift to cashless lies larger, more profound changes and challenges besides the financial risks. Often underestimated are the risks emerging from transformations events, including fundamental changes in the business model due to digital and technological advances. Non-financial risks are becoming more significant.

[1] The entire infrastructure of payments needs reshaping, with new business models emerging. Many payment providers strive to meet greater efficiency, scale, modularity and global interoperability. Outsourcing of Cloud and platform infrastructure will become increasingly important, too. According to PwC, eight out of ten financial services organisations are expected to have outsourced their infrastructure by 2025. Data privacy and cybersecurity are of major concern. The increased use of online transactions provided an opening for fraudulent purchases, with the average value rising by almost 70% in 2020. Therefore, compliance and data-privacy risks are top priorities for banks, fintechs and asset managers in implementing a fully integrated technology strategy.

ATM and PoS industry challenges

Banks deal with very sensitive things directly related with people's money. Thus, banks have long leaned on leased lines for years since the connection does not carry third party communications. In fact, bank networks are often physically isolated and perimeter-based, relying on high infrastructure costs and dedicated service provider contracts.

Nonetheless, digital transformation and cost savings have accelerated the migration to alternative modern network technologies. As these services slowly increased, the network's capabilities began to fall short.



Many financial institutions already connect their teller stations, check-imaging systems and other PC-based devices via IP. Each branch is configured as a LAN that connects to a WAN at a main branch or other central sites.

Retail chains connect devices such as point-of-sale and credit card terminals, inventory systems and other devices via IP. Each store is a LAN that connects to a WAN at corporate headquarters or another site. Although the availability of more integrated services at ATMs and PoS devices helps financial institutions enhance customer experience and improve a bank's revenue, the industry faces many challenges during the process of transformation which constitutes a major risk of financial loss due to the following forces:

- **Use of third-party vendors:** ATMs and PoS are getting more connected, to the corporate network and public/ private/ partner cloud.
- **Rapidly evolving, sophisticated and complex technologies:** ATMs and PoS are getting intelligent and doing more, leading to more sophisticated software and evolving compliance requirements.
- **Increased use of mobile technologies by customers,** including the rapid growth of the Internet of Things
- **Cross-border information security threats due to increasing cross-border data exchanges:** ATMs and PoS attacks are getting more complex and targeted, limiting the effectiveness of generic solutions

ATM machines and PoS devices are typically connected to the bank's data center using a VPN tunnel through private network for transactions or to check customer balances.

Generally, VPNs are inconsistent: If many users are operating on the network and the users reach the VPN threshold value, this VPN crashes failing to stand up to the load and concurrent transactions. Firewalls or perimeter authentications on their own do not provide sufficient security guarantees. TCP/IP design assume trusted network connectivity. VPNs and DMZ are workarounds with excessive risks and IP addresses are weak identifiers. This excessive implicit trust leads to excessive potential risk.

ATMs are usually placed in shopping malls, gas stations, convenience stores, in new and remote areas, and often case legacy equipment are still a reality.

Not all countries or locations have sufficient and reliable wired Internet access options and VSAT communication is still costly, thus posing a challenge for ATM secure, affordable and reliable connectivity.

Operations and maintenance costs when owning the networks are also a concern for banks whose traditional revenues are shrinking and the increasing regulatory pressure adds to the costs of running daily business.

As a consequence of this pressure and considering the need to invest in technology, IT has become a priority of CEO running IT (cost) transformation projects, since IT contributes to the overall cost increase in the banking sector.

Resilience: the new risk-management paradigm for banks

In light of the present disruptive and rapidly changing business environment, financial institutions expect the IT organisation to do more to help ensure they are well-positioned to succeed in the future.

Hence, risk management cannot be seen as a collection of static practices but must evolve to keep pace with rapidly changing business models. Consequently, financial Institution leaders have started questioning the risk-based management approach and are now calling for new approaches that go toward business resilience.

Resilience entails security and expectations in terms of connectivity, putting networks under even more pressure. The data exchanged is greater than ever, driving increasing network capacity and bandwidth requirements. Banking applications have become feature-rich and data hungry, and a system failure may have severe repercussions regarding reputational damage and compliance.

Zero Trust Secure Virtual Networking is the new approach for financial institutions to achieve business resilience, network efficiency and manageability.

Zero Trust: Towards business Resilience

Today, most financial institutions employ a perimeter-based defence based on costly banks' private networks, in some cases not even an IP network, relying on VPN technology for network access.

After allowing endpoints (users and devices alike) to join their internal network, each endpoint typically enjoys a broad range of lateral movement within the network, regardless of their role. Unfortunately, this approach allows endpoints far more access than required to perform its duties. A flat (non-segmented) network architecture allows a malicious actor, who gains access, the ability to move across a network and get hold of sensitive data. Likewise, automated malware or ransomware targeting the network, can spread laterally across an open architecture damaging critical system functions and availability.

These are the types of risks that Zero Trust architectures address. Zero Trust is a cybersecurity approach that breaks down the myth that all threats come from the outside. Essentially, Zero Trust is based on the concept that no device or user is trusted unless it is identified through fine-grained controls to comply with the organisation's security policies.

ATMs and PoSs are built on several software layers (operating system, hardware software layer…), plus different other tools for operations, monitoring and security. Frequently the software update on these devices is reactive, meaning they happen after a vulnerability was found; hence, malicious actors have found a way into the software. This is where the concept of zero trust makes sense in isolating layers, especially with legacy applications that oftentimes are no longer patchable. A zero-trust strategy should also be extended to the third-party tools and services which also have legitimate access to ATMs and PoSs for example when servicing the devices.

Virtual Networking: Towards network efficiency and manageability

Financial Institutions are pressured to shrink the overall operational costs including IT investments that were kept to the bare minimum and mainly for the critical maintenance needed to assure business continuity.

Due to the above, financial institutions are now facing several problems: (i) maintenance of obsolete hardware without support contracts, (ii) infrastructure complexity with many under utilised systems, (iii) usage of legacy applications and unsupported operating systems (End of Life), and (iv) inability to upgrade and expand provided services due to limitation of physical resources.

The demands for adding new services and products and the pressure to constantly reduce operational costs create the necessity to reform IT procedures and operations. A way to address these demands is to resort to new techniques for virtualisation, centralised management and consolidation.

Virtualisation technology can allow immediate improvements in availability, security and Total Cost of Ownership (TCO). In addition, ATM's will be more compatible with cloud services platforms of the future.

Blu5 expertise in the financial industry can support banks reduce the complexity of their networks for a lower TCO, reduced operational costs and a more sustainable business.

SElink Zero Trust Network Access strategies and secure software-based networking technologies, provide virtualised network segmentation at the service level with the tokenisation of the routes' ID for a more secure, manageable and cost-effective network infrastructure.

Banks can abstract the physical layer of the IT infrastructure to the advantage of reduced hardware needs, faster delivery of services and increased agility. Not being tied down to a physical resource at any particular location, for example, makes it possible for banks with a widespread geographical presence, stretching to remote areas, to troubleshoot and push automatic updates farther and faster in a more reliable and bandwidth-optimal manner.

With **SElink,** banks can say goodbye to pricy leased lines and private network topologies, and migrate to public IP networks and the Cloud to reduce the total cost of ownership as well as operational and management costs. SElink intrinsic security features address the residual security challenges of this migration.

References

[1] BCG; Citi; McAfee; AGU Research; Washington Post; FT; Ivey Publishing; IMF; World Bank; WSJ; Iowa State University; PwC.

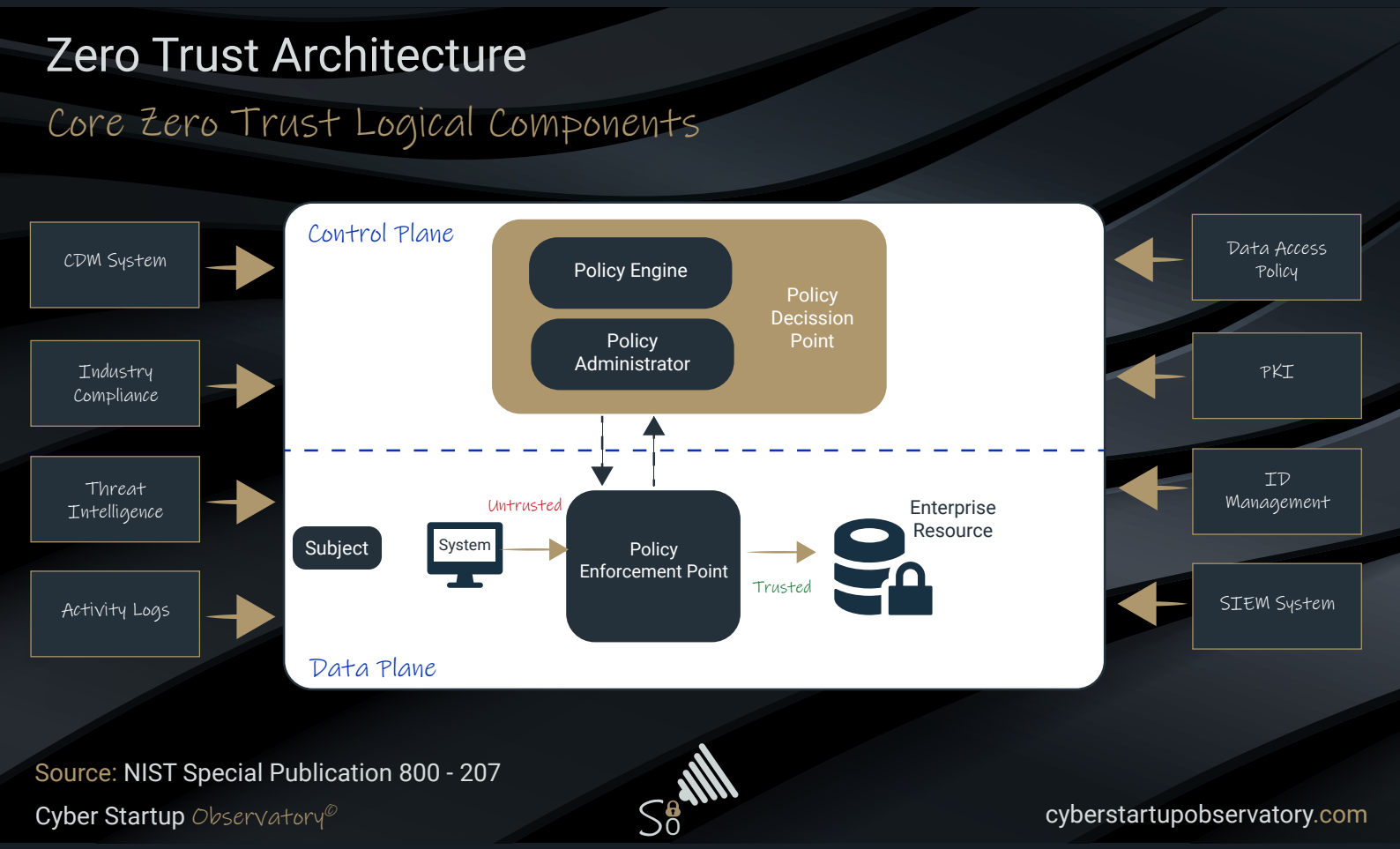
Resources

Infographic

Zero Trust Architecture – Core Zero Trust Logical Components

Zero Trust Architecture

Core Zero Trust Logical Components



Available for download in Press Quality

Infographics - Data Security & Privacy

Cyber Startup Observatory - Community

Jym Cheong

Deputy Director, Cyber Resilience Systems @ ST Electronics (Info-Security) Pte Ltd

Jym Cheong

Deputy Director, Cyber Resilience Systems at ST Electronics (Info-Security) Pte Ltd

Jym is currently an R&D lead with ST Electronics (Info-Security) Pte Ltd. He is also the principal author of Open Endpoint Defense & Response (OpenEDR), an open-source security platform[1].

He has more than a decade of industry experience accumulated from 1various roles in Product R&D, Evaluation and Large-Scale systems deployment and delivery.

His achievements include the design and development of low-cost passport scanners for nation-wide deployments, technical leadership for delivering ST-Engineering Security Operation Center and two government-agencies SOCs.

He spearheaded capability-building of a Test-and-Evaluation group to ascertain the efficacy of existing and emerging security products.

Beyond his technical roles, he advises C-suite Executives who are in turn advisors for their respective boards and forums.

What is your overall approach to information security?

I devised what I termed as Attack-Life-Cycle approach to Cyber-Physical (or CP)[2] Security. The approach starts with the necessary and sufficient conditions of any CP attacks.

Just like fire, CP attacks need a set of conditions to succeed. To mitigate the risk of combustion, we need to disrupt or remove one or more of the three conditions stated in the Combustion Triangle.

Similarly, disrupting one or more of the three conditions of CP attacks will lower the risks of successful attacks. Of these conditions, I will put my focus on Threat Accessibility because:

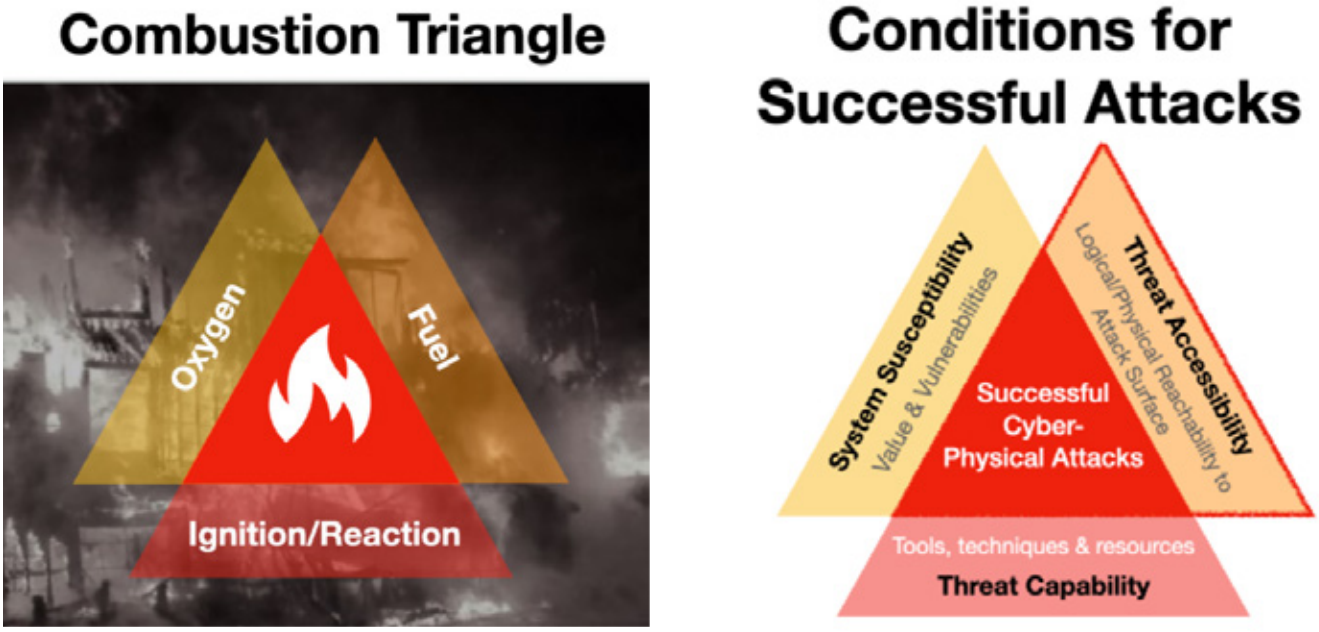


Fig. 1 - Attack-Life-Cycle approach to Cyber-Physical (or CP) Security

Systems Will Always be Flawed - This is not to advocate "No need to patch system vulnerabilities", but don't let your life depend on just patching systems. There's no way to get rid of System Susceptibility. Even tech-companies worth billions-of-dollars can't get it right, let alone smaller organisations and companies.

Threat Actors Have the Upper-Hand in terms of Tools, Techniques and Resources - The amount of FREE tools, techniques and resources (including source-codes) creates an unfavourable imbalance against defenders who have to get it right all the time with high cost, but attackers only need to get it right once with low-cost.

Early Disruption, Containment and Detection of Threat Access Attempts are possible - Better technical controls like Remote Browser Isolation not only disrupts malware delivery and phishing attempts, but increases the attack-effort to control an infected endpoint. Malicious websites that deliver payloads are contained within an ephemeral Remote Browser containment. Even if backdoors were to somehow get into endpoints by other means (eg. USB sticks), establishing the usual malware Command and Control will be harder since there's no direct Internet access. We should free up budgets from ineffective controls (eg. Firewalls & Anti-Virus) to repurpose for better controls that disrupt a broad set of offensive methods. We need to detect infiltrations early with Deception technologies - traditional rule-based detection development will never catch up with agile & motivated Threat Actors.

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

Most drivers know that without a seat belt, the chances of survival are low for higher-speed automotive accidents. Even with seat belts, there is still no such thing as 100% survival since there are other road-users who could be careless or reckless.

Similarly, there is no such thing as 100 percent cybersecurity. Even powered-off equipment can be stolen under our watch (e.g. Hard disk "replaced" from your Multi-functional Printer). We can at best minimize risks by exercising risk management.

How can CISOs better understand a business' needs?

Empathy; put yourself into users' shoes. It is best to learn it first-hand from users who are part of the business. When they can't do their job due to various pain-points related to technical controls, it usually follows that the business will suffer. Or it could be worse, users start to introduce Shadow IT or take risky approaches just to overcome their pain-points. To share a real-world example, after Singapore's SingHealth breach incident, Multi-Factor Authentication or MFA became a mandate for all IT administrators and high-risk endpoints are to be equipped for MFA.

Consider a sterile Operating Room setting, imposing MFA for health-care staff is challenging due to the aseptic requirements, especially for authentication methods that require typing. Cyber Security Agency of Singapore took the lead to consolidate various issues faced by Critical Information Infrastructure stake-holders, specified into requirements and arranged a number of "Call-for-Solutions" engagements with both academia and vendors to work out innovative solutions. I believe all CISOs/Leaders should play such roles within the context of their respective organisations.

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

Limit your exposure to the Internet because most payloads are delivered via the Internet. Install OpenEDR which is free and open-source. It blocks 100% of executable file-based malware without the need for signature-database and mitigates commonly abused "File-less" offensive techniques based on Microsoft-Office macros and scripting to deliver Ransomware and malware alike.

How do you predict the future of authentication?

The future of authentication is Password-less. Passwords are a liability. Offensive methods come in the forms of dirt-cheap fake login interfaces to even "Cracking Password-as-a Service". Passwords are no longer effective as a control and offer very poor usability. We can end up losing our "Digital Identity" over one password because it is hard for users to remember so many passwords, such that users end up reusing the same ones for different digital services. Authentication needs to be secure and user-friendly at the same time. It should be a low-friction framework or service that supports MFA for both users and service providers. As of now, I am putting my bets on FIDO Alliances.

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

It depends on the quality and timing of the information that is being shared. Is the information relevant and actionable? For instance, receiving a technical workaround to mitigate certain system vulnerability before an official vendor patch is available.

But suppose a company is a pure Microsoft-Windows shop, then information related to Linux vulnerabilities are irrelevant. Is it timely? The official patch may already be out earlier than the information for the workaround. Do you have staff to answer the earlier two questions? This is usually the primary challenge for most organisation.

Many don't have manpower or "bandwidth" to deal with such information, which can be in volumes.

Closing Thoughts

As shared earlier, it is possible to achieve early disruption, containment and detection of attacks if we repurpose budgets for better controls and drop ineffective ones. With the "new normal" of working from home due to the current pandemic, **Threat Accessibility becomes even more concerning** because organisational assets are now within the home network, which could already be compromised. These networks are not within your control, Threat Actors can pivot into organisational networks through VPNs, especially when it is poorly configured to allow dual zones; accessing Internet and Intranet at the same time.

References

Insight

IAI - ELTA

Cyber Forensics in The Cloud Environment

Cyber Forensics in The Cloud Environment

Author: David Tayouri, Cyber R&D Manager at IAI - ELTA

At a glance

- 5 minute read
- Cyber Forensics
- Cloud Forensics Challenges
- Cloud Forensics Guidelines
- Summary

The digital infrastructure landscape is evolving towards fully integrated, multifunction, cloud-delivered networking and security platforms. Today's organizations are required to provide customers and employees with immediate, uninterrupted service regardless of where they are physically located. This transformation to digital business requires anywhere, anytime access to applications and services – many of which are located in the cloud. However, with the many advantages, this model affords come a myriad of security concerns.

Enterprises seek to protect their assets from unauthorized entities while maintaining business continuity by allowing trusted devices and users to access applications hosted on-premises or in the cloud. They need to implement cloud-based security technologies in different layers to achieve this. To improve cloud security, we examine the cloud access architecture as presented in the diagram below and consider the context: who is accessing, from where, and what is the access target. For cybersecurity in general and cloud security in particular, different methods should be considered to prevent, detect, analyze, and respond to attacks. Included among them is cyber forensics.

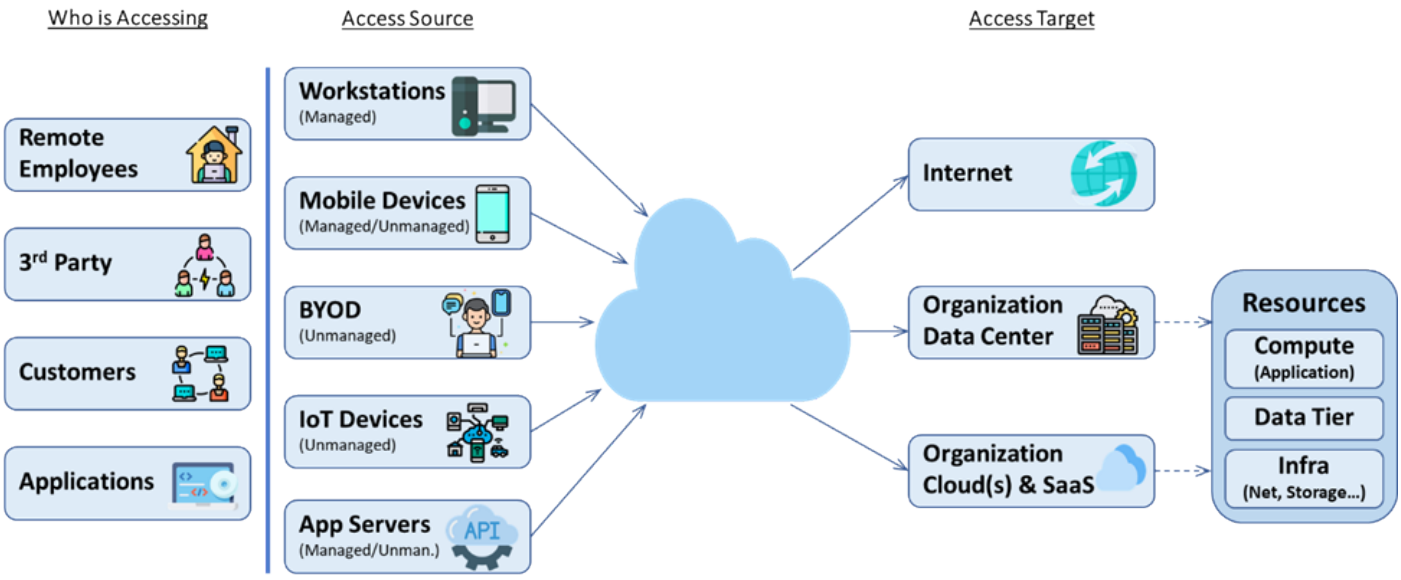


Figure 1: Cloud Access Architecture

Cyber Forensics

Digital forensics is the branch of forensics that focuses on recovering, investigating, and analyzing material found in digital devices.

Cyber forensics focuses on techniques used to track the footprints left by a cyberattack and is widely employed in incident response, malware analysis, data leak protection, and cybercrime investigations.

We refer to cloud forensics when the examined artifacts reside in the cloud.

For digital evidence to be accepted in a court of law, it must be handled in a way that prevents its tampering by cyber criminals.

The forensics process includes five phases:

1. Identification – finding the evidence and noting where it is stored.
2. Preservation – isolating, securing, and preserving the data, including preventing possible tampering with the evidence.
3. Acquisition – retrieving the data from suspected digital assets.
4. Examination – reconstructing data fragments and drawing conclusions based on the evidence found.
5. Presentation – creating a record of all the data to recreate the crime scene and summarizing it for presentation in court.

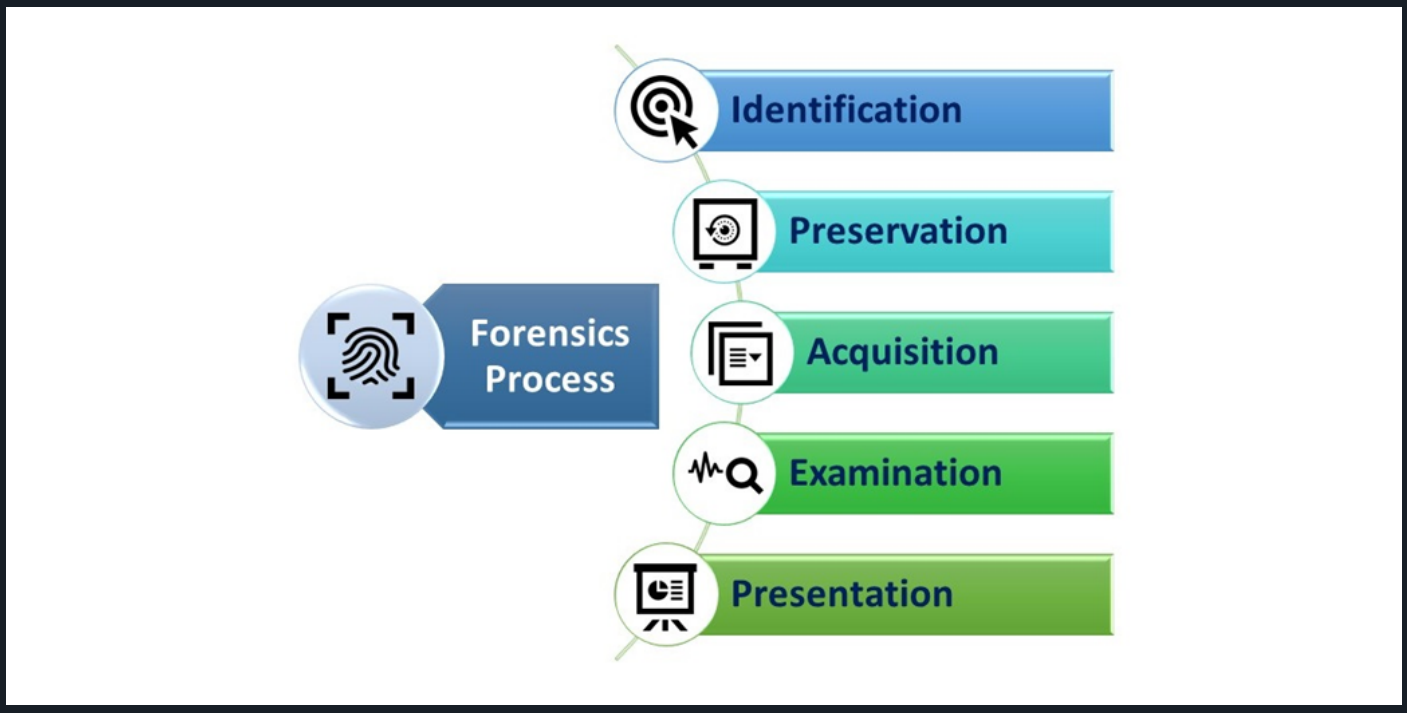


Figure 2: The Forensics Process

Cloud Forensics Challenges

Cloud forensics brings many inherent challenges in all of the above-noted phases. Following are some of the main challenges [1,2,3]:

Identification

Access to the evidence in logs – in some instances, investigators do not know the data's location due to the cloud's distributed nature.

Volatile data – when a virtual machine (VM) is turned off or restarted, all the data is lost unless the image is stored somewhere.

Intelligence processes for real-time investigation are impossible – most providers do not reveal the specifics of their operations.

Evidence identification – in most cloud computing environments, most of the evidence is either unavailable or not generated or stored in the same way as in traditional non-cloud settings. In cloud computing, resources are usually exposed abstractly.

Application details are unavailable – private and confidential information of cloud-based software/applications used to produce records are typically inaccessible to the investigator.

Preservation

Isolating a cloud instance – in the cloud environment, it is hard to isolate the incident environment to prevent any possible evidence from tampering or alteration due to resource sharing between multiple users.

Data integrity – errors may occur in the data preservation stage in the cloud context due to multiple actors who are involved in the process.

Time synchronization – the synchronization of time can be used as a source of evidence, but the date and time stamps of the data are questionable when they are from multiple systems. Moreover, the difference in time zones between cloud servers and cloud clients can affect evidence integrity, reliability, and admissibility.

Live forensics – when evidence is collected in a cloud environment, the suspect system is still running, and data is likely changing as it is being collected. Therefore, data correctness cannot be verified.

Acquisition

Multi-tenancy – cloud service providers (CSPs) use of multiple data centers to serve multi-cloud computing customers may raise many uncertainties about customers' data isolating and retrieving.

Virtualization – extracting sound evidence from a VM is difficult due to malicious code that may circumvent VM isolation methods.

Data deletion – investigating and retrieving deleted data in a cloud computing environment is challenging because the CSPs do not use sufficiently sophisticated methods for retrieving information on deleted data. In addition, deleted data can be overwritten by another user in a shared virtual environment.

Dynamic storage – some CSPs dynamically allocate storage based on the user's current needs. As data is deleted from the system, the storage is reallocated.

Examination

Evidence correlation – the evidence may be spread across multiple digital resources.

Crime scene reconstruction – reconstruction of the crime scene in the cloud environment to understand how illegal activities were committed may be problematic. For example, when adversaries shut down their virtual instances after committing malicious activities, reconstructing the crime scene will be impossible.

Decoupling between cloud user credentials and physical users – binding a cloud username to a physical entity to prove the physical ownership of the data attributed to the cloud username is challenging.

Cloud Forensics Guidelines

The above-mentioned challenges are emphasized due to the multi-national nature of the cloud and the lack of global standards and regulations concerning cloud forensics. Following are some guidelines that will help cope with these challenges [5,6,7]:

Policy & SLA

- Have a well-documented digital forensics process. This can be part of the incident response policy and procedures, but it should cover the complete forensic investigation lifecycle.

- Predefine a set of corporate-approved forensics-enablement tools to be installed as part of any instance deployment in the cloud platform.

- Establish logging requirements for cloud platforms and set the severity level, timestamp format, and retention and rotation periods. Enable logging and auditing in the cloud environment by corporate policy.

- Define with the CSP which logs from the underlay infrastructure can be exposed during forensics examinations and how long the log retention periods are. Specify recoverability after deletion options for each type of log.

- Define data storing location(s) by agreeing with the CSP on the corporate authority to decide where all the data is stored for the deployed environment (country, state, and jurisdiction).

Identification

- Evaluate the service model supplied by the CSP being analyzed: SaaS (Software as a Service), PaaS (Platform as a Service), or IaaS (Infrastructure as a Service). The detection of an incident in a cloud environment may differ according to the model adopted for the services.

- Identify the particular data sought, relevant periods, the involved CSPs, and the utilized services.

- Interact with the CSPs' professionals to map the incident and the extent of the damage.

Preservation

- Implementing preservation techniques may require isolating cloud resources. CSPs should isolate the physical disk connected to an incident, taking into account that data from other customers sharing resources could also be copied.

- The chain of custody must start when the researcher has access to physical media. Implement contracts that allow the investigator access to the evidence, sometimes physically.

Acquisition

- Consider using the Cyber Forensic Field Triage Process Model (CFFTPM), which proposes an onsite approach for identifying, analyzing, and interpreting digital evidence in a short time frame.

- The CSP should be responsible for extracting forensics images of the physical disk or partition, or at least the virtual machine created for the client by handling the hypervisor.

- Sometimes, it may not be possible to shut down a machine to remove the disc or boot via live CD. Therefore, remote collection strategies should be established.

- Document the acquisition process, including system information, methods used, and how the data is received. This step is crucial to assure the process' integrity.

Examination

- Consider timestamping in the collection and analysis phases.

- Regarding the logs, the experts should be familiar with the most used platforms, knowing how logs are generated so they can use a parser efficiently.

Summary

With the surge in the transformation to digital business, many organizations are opting to locate their assets in the cloud. This requires the adaptation of cybersecurity to the cloud environment, particularly implementing the cyber forensics process. The multi-national and distributed nature of the cloud brings many challenges to forensics experts. To assist them in coping with these challenges, global standards and regulations for cloud forensics are required.

IAI's Cyber Division has amassed vast experience and offers a wide array of available solutions to enable investigators to perform the entire cyber forensics analysis cycle efficiently.

References

[1] Cloud Forensics: A Review of Challenges, Solutions and Open Problems,

https://ieeexplore.ieee.org/document/7149635

[2] Digital Forensic Investigation Challenges based on Cloud Computing Characteristics,

https://www.sciencepubco.com/index.php/ijet/article/view/21361

[3] NIST Cloud Computing Forensic Science Challenges,

https://csrc.nist.gov/publications/detail/nistir/8006/final

[4] Cybersecurity Standards for Cloud Access,

https://ieeexplore.ieee.org/document/9718230

[5] Cloud Forensics - Best Practice and Challenges for Process Efficiency of Investigations and Digital Forensics,

http://icofcs.org/2013/ICoFCS-2013-003.pdf

[6] IPCFA: A Methodology for Acquiring Forensically-Sound Digital Evidence in the Realm of IAAS Public Cloud Deployments,

https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1367&context=theses

[7] Scientific Working Group on Digital Evidence, Best Practices for Digital Evidence Acquisition from Cloud Service Providers,

https://www.swgde.org/documents/published

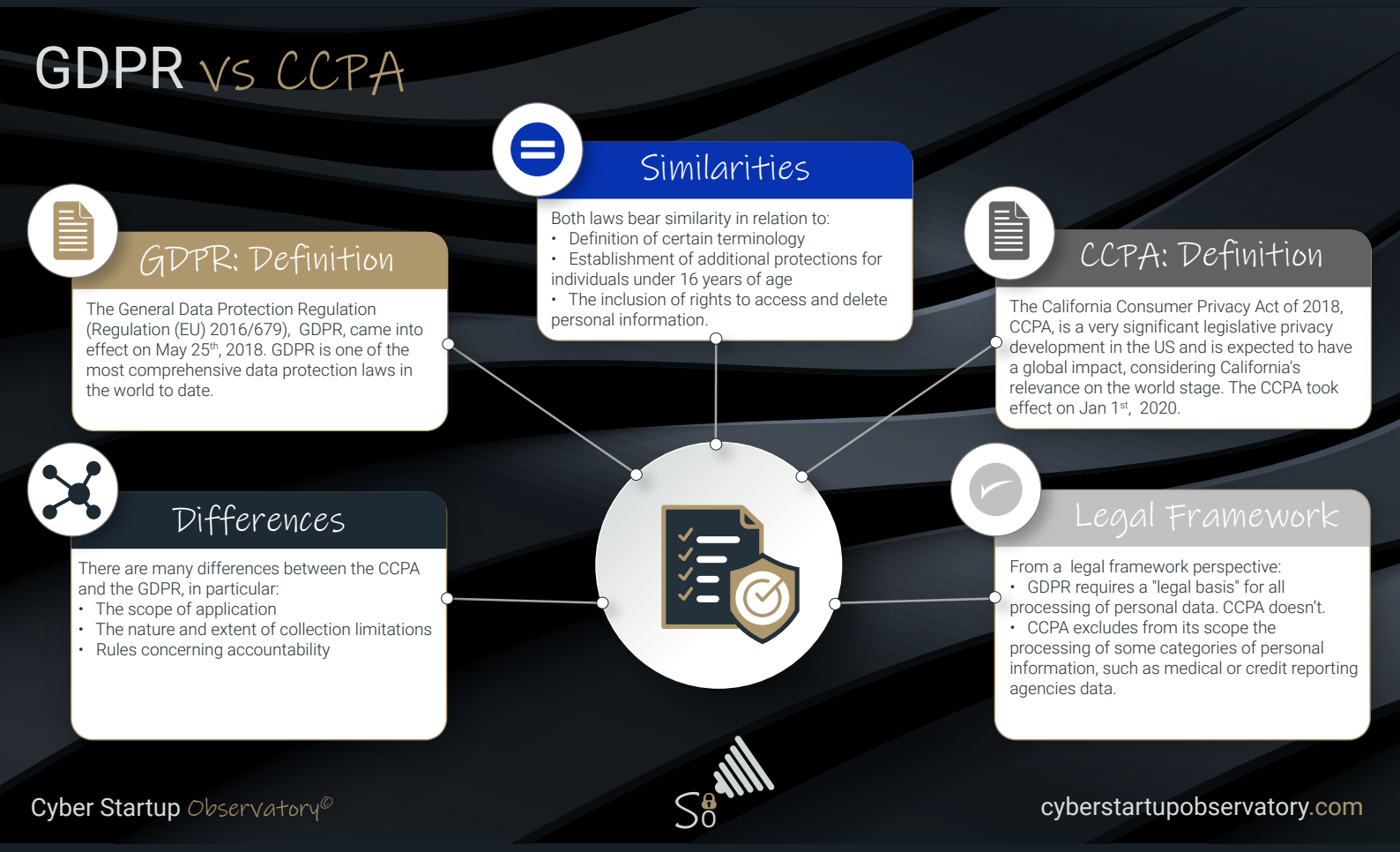
Resources

Infographic

GDPR vs CCPA

GDPR

vs CCPA



Available for download in Press Quality

Infographics - Data Security & Privacy

Cyber Startup Observatory - Community

Rizwan Baig

Senior VP and Head of Governance, Risk & Controls at Standard Chartered Bank

Rizwan Baig

Senior VP and Head of Governance, Risk & Controls at Standard Chartered Bank

Rizwan Baig is the Senior Vice President and Head of Governance, Risk & Controls at Standard Chartered Bank, responsible for strategic direction, vision for Governance, Risk & Controls of Operations and Technology function.

As a seasoned professional with an enriching 10 years of Banking experience, Rizwan is known for driving, leading and nurturing the operational risk fabric across the Operations and Technology function, maximizing operational excellence and delivering financial performance. He is also serving as the Information & Cyber Security (ICS) lead for the Bank where he is responsible for driving the Information and Cyber Security Agenda and orchestrating the country ICS risk posture with being an active security advisor.

Rizwan holds an MBA (Finance) and MS in Economics from the Institute of Business Management and holds an accreditation from Institute of Bankers Pakistan (IBP) for the title of 'Chartered Banker'.

He also holds certifications in the field of Information and Cyber Security (ICS) such as Certified Ethical Hacker (CEH V10), Certified Information System Auditor (CISA) and a Diploma in Information Security from Institute of Business Administration (IBA). Rizwan is married and has a son. In his free time, Rizwan likes travelling, playing chess and performing illusions as a hobby.

> "Any organization without a CSIRP in place should be racing to implement one."

If I gave you an extra Euro / Dollar, how would you spend it on cyber security?

I would spend that extra euro / dollar on strengthening the human firewall in an organization along with streamlining the Cyber Security Incident response plan to equip the organization to respond / prevent to a successful breach. Most organizations are ill-equipped to handle a major cyber security incident, much less amid a global crisis like COVID-19.

A recent global study found that 76 percent of organizations don't have an incident response plan applied consistently across the organization. One in four organizations report not having any Cyber Security Incident Response Plan (CSIRP) whatsoever. An effective CSIRP outlines governance and communications practices across teams.

It also defines response models and details crisis response roles and responsibilities across the organization, such as strategy, technology, operations, and community and government relations. Any organization without a CSIRP in place should be racing to implement one. With breach notification laws and regulations getting stricter around the world even prior to the COVID-19 pandemic, business continuity planning is a long-term strategic capability that can prepare an organization for a host of unexpected contingencies.

By 2023, there will be 3 times more networked devices on Earth than humans, according to a global survey report. And by 2022, 1 trillion networked sensors will be embedded in the world around us, with up to 45 trillion in 20 years.

IP traffic has reached an annual run rate of 2.3 zettabytes in 2020, up from an annual run rate of 870.3 exabytes in 2015. Data is the building block of the digitized economy, and the opportunities for innovation and malice around it are incalculable. Hence the significance of every dollar spent on cyber security is magnified.

What should corporate boards know about conducting information security?

This is indeed an intriguing question. I would like to answer this with the narration to the following quote;

Robert Mueller, who was the FBI director until 2013, once said that there are only two types of companies in the world: those that have already been hacked, and those that will be hacked in the future, then jokingly added that "the two groups can be merged into one category: companies that have been hacked and hacked again".

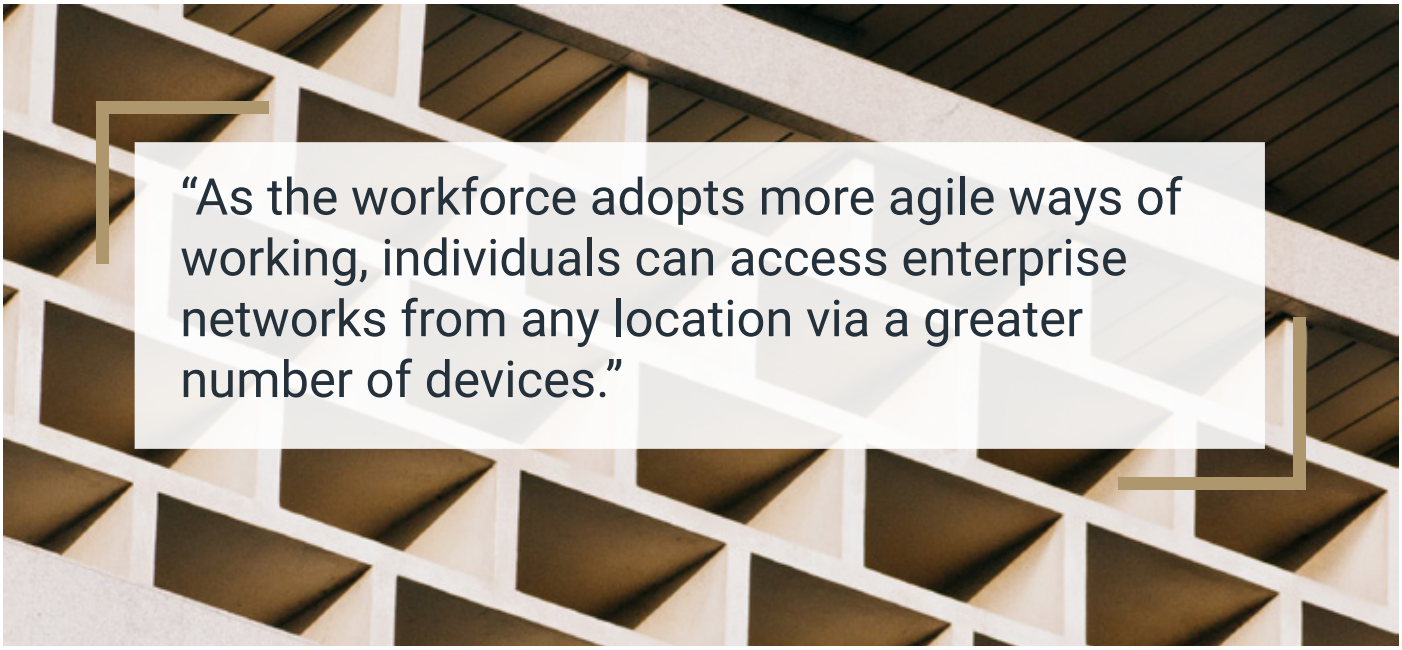
Learning from this we come to the conclusion that we should start researching and finding out which of his two categories his company belongs to: "those who have already been hacked" or "those who will be hacked in the future".

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

For me as the saying goes "Quality is more important than quantity. One home run is much better than two doubles."

The content of the Cyber security awareness program is far more important than the daily frequency of the exercises/ training. I believe that organizations should focus on customized awareness programs to their relevant audience with integrating real life scenarios. Tabletop exercises and breach simulations are an effective way to validate the process and procedures for each of the key functions of your cyber crisis management plan. On a regular basis, conduct full-scale simulation exercises to stress-test teams, leadership, and communications.

The ultimate goal is training the team to "build the muscle memory" to respond effectively, much like first-responder or military teams. Crisis planning needs to accommodate a spectrum of operational disruption and social impacts, which require different approaches to crisis mitigation and response. Cyber resilient organizations operate in a continuous cycle of discovery, learning, adaptation, and iteration. In times of crisis, effective threat remediation comes down to the ability of individuals to work together on complex, often intractable, problems. Techniques such as Live fire, capture the flag competition and the adoption of VR/ AR in the learning process can increase exponentially the learning retention.



In my view, anticipating attacks, responding to them in real time, setting traps to contain them, and protecting assets according to their value can help companies stop sophisticated cybercriminals. Hence, in order to survive in the age of advanced cyberthreats, organizations should resort to / use ‘active defense’.

What unique security challenges does your industry face?

Cyber security spending where more is less, evolving regulatory landscape, digitization, data privacy and emerging third-party risks are generally the main ambits for consideration. As digital becomes business as usual, the threat surface that can be attacked is increasing exponentially. This is largely due to the convergence of information technology (IT) and operational technology (OT), Internet of Things (IOT) sensors, data analytics, and optimization AI.

In addition, as the workforce adopts more agile ways of working, individuals can access enterprise networks from any location via a greater number of devices. This increases the footprint of cloud-based platforms, business solutions and data repositories.

The security of the enterprise perimeter is therefore based on user identity, and companies need to have a “trust by design” strategy embedded to ensure security around how employees are accessing data for both in-house and externally developed applications. Following this, Cyber security investment must be a key part of the business budget cycle and investment decisions must be more evidence-based and sensitive to changes.

The need for a unified, enterprise-wide approach to cyber risk, involving the business and the risk, IT, and cyber security groups is the need of the hour. The leaders of these groups must begin to work together, identifying and protecting the organization’s critical digital assets as a priority. The process of addressing cyber risk will also have to become technologically enabled, through the implementation of workflow management systems.

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

The need for different strategies around innovation and digital banking was apparent in banking well before the pandemic hit. As technology has developed, there has been a rise in customer expectations of banking, not least from the instant and personalized services provided by the leading technology firms. FinTechs have shown what is possible and that all banks need a digital plan.

A rise in digitization is also coupled with enhanced cyber risks which the organizations need to deal with. Although the benefits and advantages of digital transformation are eminent, the journey will not be without challenges emerging from reliance on advanced technologies such as cloud computing, artificial intelligence (AI) and the Internet Things (IoT).

Organizations must break down barriers in their rapid move to scale technology. Organizational leaders face the difficult task of balancing the traditional approach to risk management with the need to respond quickly to a crisis that has created massive changes to their operating environment.

Criminal cyber activity, including fraud and phishing attacks, has increased as more employees work remotely. As organizations shift from crisis mode, their boards need to address new emerging risks, such as video and voice communication surveillance with everyone using virtual communication tools and other platforms, data security controls for the use of personal equipment, and cases of third and fourth parties falling victim to cyber issues. Firms should track and assess the risks they have accepted.

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

In my view it’s a “the more you know” mantra applied to cybersecurity. Intelligence sharing helps expand everyone’s cyber threat intelligence (CTI). Proactive information-sharing about attacks and defensive mitigations builds resilience across organizations participating within a given trust community, evolving herd immunity against attacks that others have seen within their own networks. Some businesses are reluctant to share cyber security information. They may be worried about legal implications, attacker retaliation, or endangering intellectual property. Nevertheless, over the past decade the practice has become more common. Forums have been developed to share information and some intelligence providers have set up secure servers with daily threat updates and intelligence sharing.

Closing Perspective

An innovative cybersecurity strategy based on good risk management principles needs to be applied and while most mining companies have cyber on their enterprise risk register, the “real” cyber risk may be understated or not well defined enough to accurately assess the control effectiveness and residual risk.

The focus should be on how cyber security will support and enable enterprise growth.

The aim should be to integrate and embed security within business processes and build a more secure working environment for all.

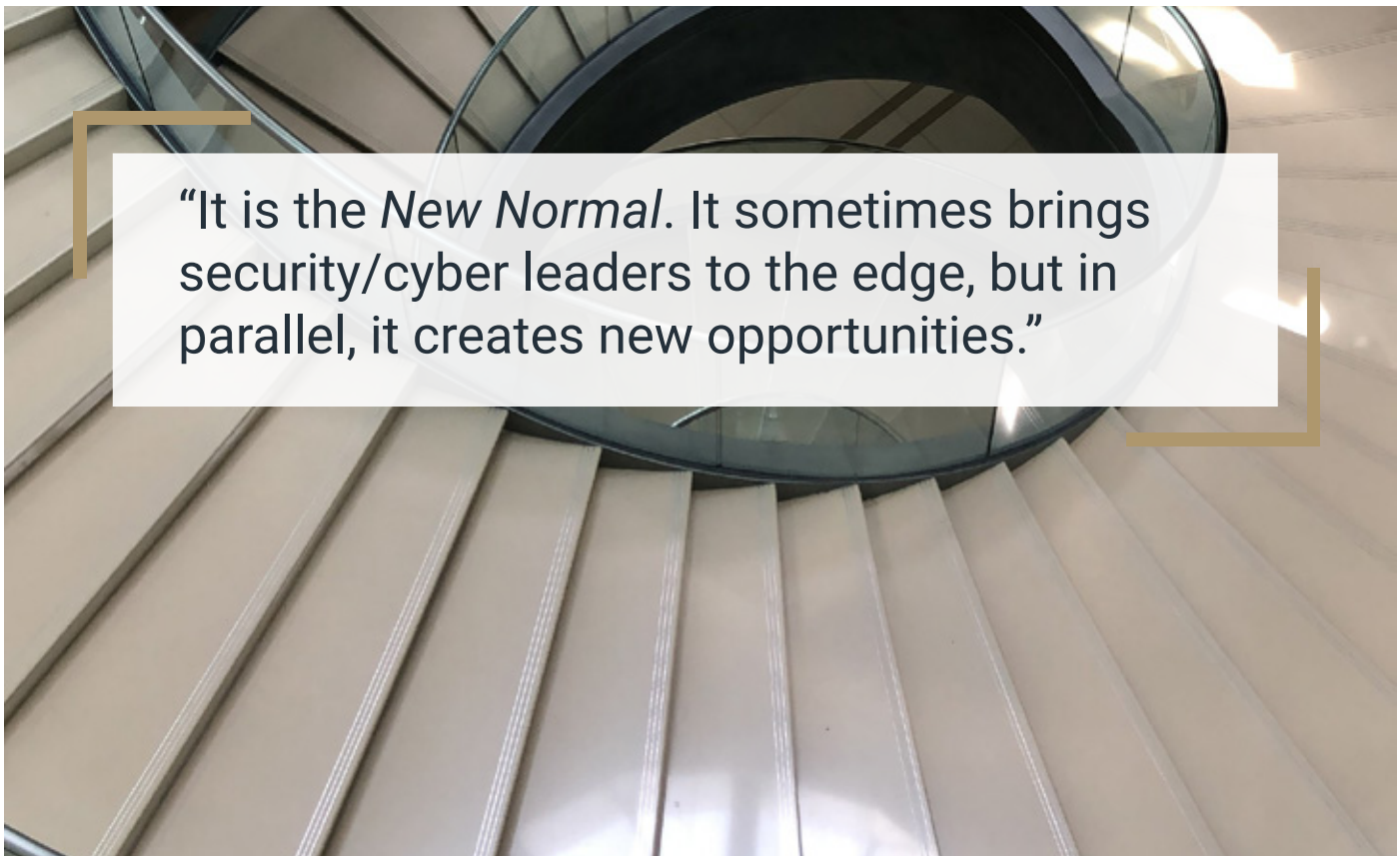
This is particularly important in light of the changing technology landscape, a more agile workforce and the push for technology to be more flexible and "customer focused." Every cyber security transformation should promote three key principles across culture, governance and capabilities:

- Excellence in security fundamentals. Be highly mature at "security basics," practice good security hygiene and optimize your current information security solution capabilities. Security basics include the locking down of highly privileged corporate accounts (e.g., domain administrators), routine patch management and vulnerability management (i.e., penetration testing), multifactor authentication, security awareness, and a cyber crisis simulation.

- Strong governance program and a culture of accountability. This should include adequate progress and performance metrics, the development of a security-savvy culture and a shift in culture to ensure security practices are a part of people's everyday responsibilities.

- Continuous improvement. Adapt to new requirements based on evolving threats and trends and have a plan to regularly assess security posture to remediate gaps. This plan should include policy, standards and a subset of critical controls that can then be built out over time as awareness and adoption grows. It is important to remember that cyber strategy roles and responsibilities are for everyone in the organization, no matter their role.

It is the "New Normal." It sometimes brings security/cyber leaders to the edge, but in parallel, it creates new opportunities.



Insight

senhasegura

Cloud IAM: What Do You Need to Know?

Cloud IAM: What Do You Need to Know?

Author: senhasegura

At a glance

- 6 minute read
- What Is Cloud IAM?
- How Important Is Cloud IAM?
- Advantages of Cloud IAM
- How Does Cloud IAM Work?
- Cloud Types
- The Principle of Least Privilege

With the adoption of remote work by most organizations, the need to join cloud computing and invest in solutions that provide security in this context has also increased.

Therefore, we recommend using Cloud IAM to limit the privilege of users according to their roles, ensuring the protection of data and corporate files in the cloud.

This is only possible through practices such as the use of mechanisms with multi factor authentication (MFA), as we will explain in this article. To facilitate your understanding, we divided our text into topics:

- What Is Cloud IAM?
- What Does IAM Mean?
- How Important Is Cloud IAM?
- Advantages of Cloud IAM
- How Does Cloud IAM Work?
- Cloud Types
- The Principle of Least Privilege in Cloud Environments
- What Is the Difference Between Cloud IAM and ICES?
- About senhasegura
- Conclusion

Enjoy reading!

What Is Cloud IAM?

Identity and access management (IAM) consists of a process structure that enables information technology managers to manage users' access to critical information in their companies.

Its capabilities include privileged access management and mechanisms such as two-factor authentication, multi factor authentication, and single sign-on systems.

All this ensures the security of sharing only the necessary data and also the possibility of storing profile and identity information in a protected manner. You can deploy IAM systems using a cloud-based or hybrid subscription model through the services of a third-party provider. In an IAM system:

- One can protect sensitive information within a system;
- Users and groups can have different levels of access;
- Users and their roles can be added, removed, and updated in the system;
- One can identify roles in the systems and verify their attribution to each user;
- One can identify the users in the system.

What Does IAM Mean?

IAM stands for Identity and Access Management.

It is a technology that allows people to have access to a company's data in a limited way, in order to ensure a higher level of information security.

As mentioned in the previous topic, this is possible through the following resources:

- Single sign-on systems;
- Privileged access management; and
- Multi Factor authentication.

How Important Is Cloud IAM?

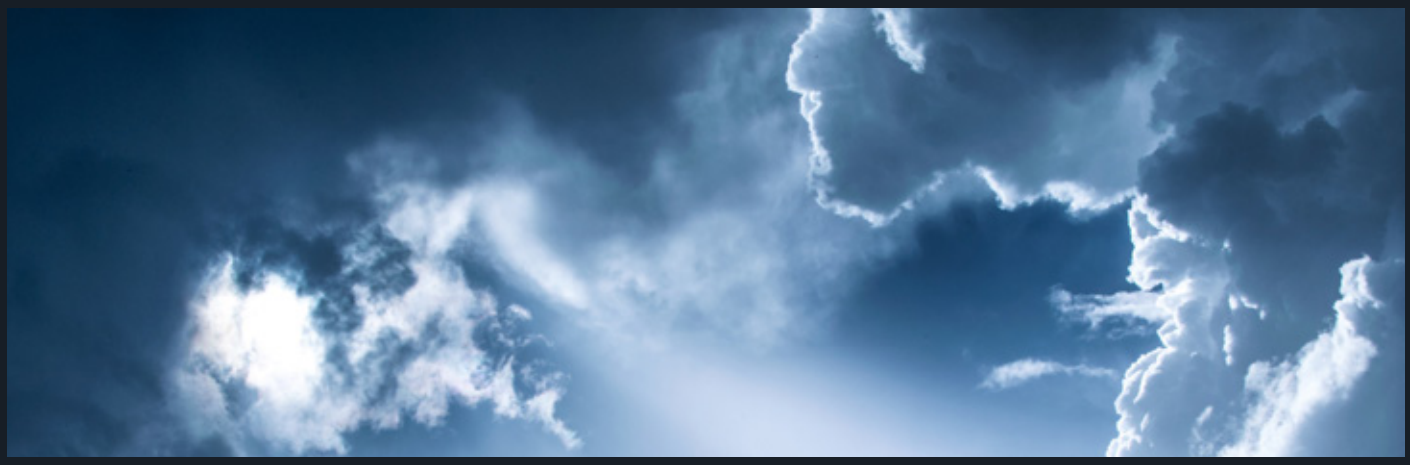
When we talk about cloud computing, we refer to the possibility of accessing data and files from any environment, not just from a company's devices, which is increasingly common with the growth of remote work.

This situation creates great challenges for leaders responsible for protecting corporate documents and data, after all, if access control was made possible based on the network perimeter in the past, today, this is no longer possible.

Thus, what should be considered when granting access to cloud data is the user's identity.

However, manually assigning and tracking user privileges can be quite a risky procedure. With that in mind, we recommend using IAM, an automated solution.

Affordable for businesses of all sizes, it has a wide range of capabilities, including AI, behavior analysis, and biometrics.



Advantages of Cloud IAM

Cloud IAM brings several benefits to the companies that invest in this solution. Check out the main advantages below:

It Contemplates Cloud Services

In the context of digital transformation, organizations prioritize the migration of identity infrastructure to the cloud. With Cloud IAM, this process occurs faster and more affordably, since cloud services do not require investment in staff and hardware.

Performing an upgrade also becomes easier, especially for companies that rely on cloud providers.

It Reduces Operational Costs

With remote work on the rise and professionals using personal devices for work, there is a greater mobilization of IT teams to manage these resources, which increases the costs of hiring experts and purchasing and maintaining equipment.

By investing in Identity as a Service (IDaaS) and Cloud IAM, these costs can be reduced.

Scalability

No matter how many employees a company has to add in a new location or if its website will attract numerous visitors to shop online during a sale: one can scale Cloud IAM solutions easily for new users.

More Security

With Cloud IAM, you can use features such as multi factor authentication, which ensures more cybersecurity for your company. This is possible

because this technology strengthens password security, as it requires more than one authentication factor.

To make the procedure even simpler, eliminating the need for passwords, it is also possible to opt for authentication without using them.

It Saves User Time

Through Cloud IAM, single sign-on allows one to log in and access resources in an agile manner. With this, customers of e-commerce can log in seamlessly and employees can use several applications to perform their activities without wasting time.

It Decreases the Need to Reset Passwords

IAM reduces the need to reset passwords, as well as the occurrence of problems with stolen access. Today, it is believed half of IT technical support tickets are aimed at resetting passwords and each reset would cost about $70.

How Does Cloud IAM Work?

With an IAM solution, one can control people's access to a company's critical data. This control is based on the roles of each user within the organization, defined according to their position, authority, and responsibility.

IAM systems capture and record login information, manage the user identity database, and enable the assignment and removal of access privileges, allowing the oversight and visibility of all user base details.

In addition to managing the digital identities of humans, they manage the identities of applications and devices to ensure more security.

It can work as identity or authentication, and the service provider is responsible for registering and authenticating users and managing their information.

Cloud Types

There are several cloud options available, which allow you to use the one that best suits your business needs and your budget. Check it out:

Public Clouds

They are hosted by cloud service providers, such as Google Cloud Platform (GCP) and Amazon Web Services (AWS).

Private Clouds

They are usually hosted in the organization itself, providing flexibility and security.

Partner Clouds

They are often hosted in a public cloud by a partner who manages the environment.

Hybrid Clouds

They combine different types of cloud to ensure security, flexibility, and value for money.

Multi Clouds

In general, they combine more than one of the top three public cloud providers, Google Cloud Platform (GCP), Microsoft Azure, and Amazon Web Services (AWS).

The Principle of Least Privilege in Cloud Environments

Each cloud provider offers different capabilities for access permissions. Therefore, IT security teams need to control entitlements when migrating the infrastructure to the cloud, following the principle of least privilege.

This is because conventional IAM permission models are not appropriate for cloud environments, but are designed to protect systems and applications deployed in an organization's data center.

Cloud environments are accessed by a larger number of people, from any environment, which makes their management much more complex to monitor.

Unlike traditional data centers, a cloud environment belongs to and is operated by the cloud provider by following a shared responsibility model.

In this case, traditional privileged and non-privileged access designations do not apply to the cloud. Information security makers should extend permission models to cloud environments.

IAM permissions control access to cloud resources such as Kubernetes containers, virtual machine servers and files, and cloud services such as database, virtualization, storage, and network services.

What Is the Difference Between Cloud IAM and ICES?

More and more organizations use public cloud providers to simplify their operations and ensure innovation, with many adhering to multi-cloud solutions in order to increase availability and reduce costs.

In this sense, conventional identity and access management (IAM) practices are not enough to protect these dynamic resources, since they are designed to protect static local applications and infrastructure.

For this reason, cloud services create their own IAM resources to contribute to companies that need to protect cloud environments. Despite this, the diversity, scalability, and dynamism of this solution still generate challenges when it comes to information security.

But with CIEM solutions, one can address these challenges by viewing and correcting incorrect IAM settings and enabling access with the least privilege in this context.

In practice, the difference between Cloud IAM and CIEM is that while CIEM manages privileges (entitlements) and their policies in the environment, Cloud IAM manages, including provisioning credentials such as users and access keys.

About senhasegura

We at senhasegura believe in the importance of promoting digital sovereignty, providing our clients with control over privileged actions and data, and avoiding theft and leaks of information.

When it comes to Cloud IAM, we offer a unique solution in relation to competitors, allowing provisioning, de-provisioning, and access flow for users and access keys.

Conclusion

By reading this article, you learned that:

- IAM is a process structure that enables information technology managers to manage users' access to critical information in their organizations;
- One can deploy IAM systems using a cloud-based or hybrid subscription model through the services of a third-party provider;
- In Cloud IAM, the user's identity is considered when granting access to cloud data.
- Some advantages of this solution are the fact that it includes cloud services, allows cost reduction, provides scalability, security, and saves user time, in addition to reducing the need to reset passwords.
- In Cloud IAM, three authentication factors are usually used. These are: knowledge factor, possession factor, and inheritance factor.
- CIEM solutions allow one to address viewing and fixing incorrect IAM settings in cloud environments and enable access with least privilege.

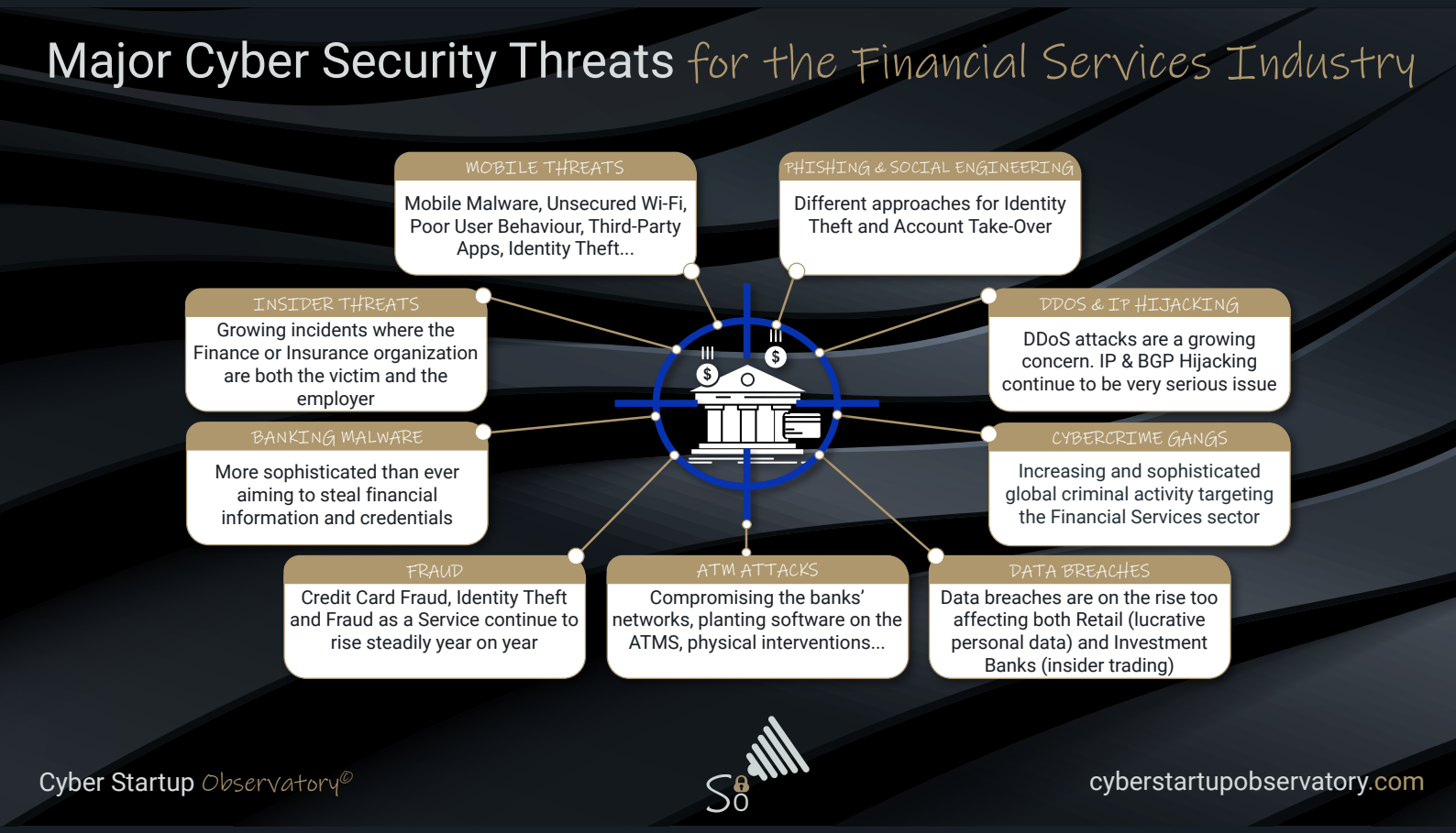
Did you like our article on Cloud IAM? So, share our text with someone else who might be interested in this topic.

Resources

Infographic

Major Cyber Security Threats for the Financial Services Industry

Major Cyber Security Threats for the Financial Services Industry



Available for download in Press Quality

Infographics - Financial Services

Cyber Startup Observatory - Community

Ammar Shareef

Head of Information Security
@ Keenu

Ammar Shareef

Head of Information Security @ Keenu

Ammar is an IT Infrastructure and security professional with diverse experience in the service provider, enterprise and financial sectors.

He joined a Cloud and Datacenter service provider company as systems engineer, where he was part of a cloud team during deployment and post deployment technical support.

Later Ammar joined a financial institute to manage systems and datacenter projects in close coordination with the compliance and audit team.

In 2015 he joined a fintech startup to oversee IT Infrastructure and security projects to enhance the digital posture of the company.

Ammar is currently working in the capacity as Head of Information Security to enable digital services for merchants and consumers.

Are there any common business roadblocks that prevent security practices from being implemented?

A security breach is like a fire that can happen once and will change the company posture for a long period of time. One of the fundamental approaches to avoid any security or "technical glitch" is to avoid some of these common roadblocks:

AWARENESS

One of the common building blocks for an organization's security posture is the awareness program, as no matter how many controls and security programs are implemented, there is always an awareness gap which can bring down a complete system.

> "A security breach is like a fire that can happen once and will change the company posture for a long period of time."

BALANCE

We often see there is a balance issue of processes which are implemented to get things done from a business perspective, which are either too protected or left with loopholes and can become a vector for any adversary to take advantage.

CHALLENGE EVERYTHING

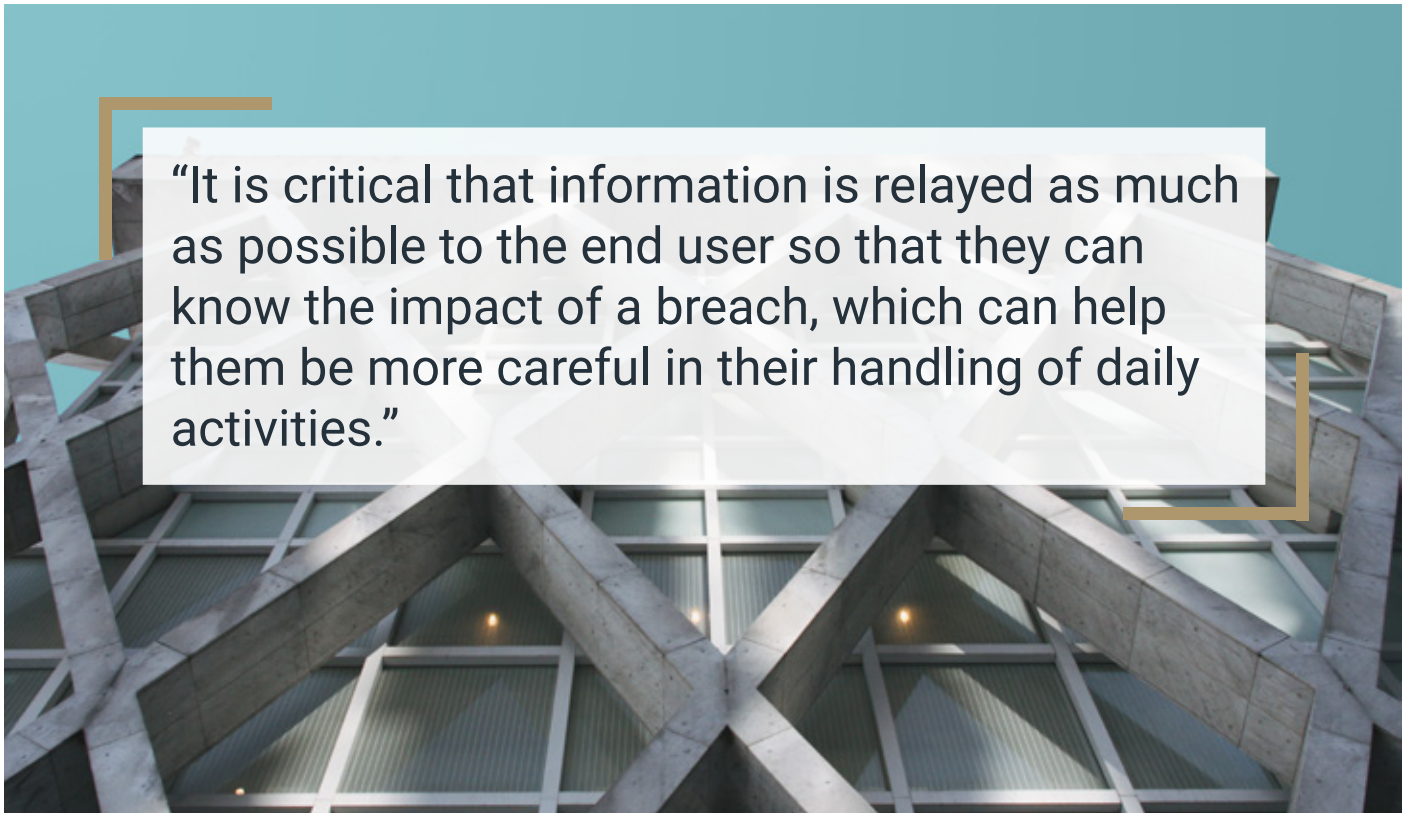
In a larger sized organization there are often norms and process already in place which are never part of the restructuring thought process, and due to organizational focus on business aspects, security and technology is often neglected to rethink how the organization's three-pronged approach of process, people and technology should be adjusted with a changing digital landscape and business models.

What should corporate boards know about conducting information security?

As security is an integral part of any business and considered to be a core item in organization readiness in this digital era, it should be part of a de facto checklist that marks organizations to be ready.

It is essential for the board members to enable space for security programs which can help users to be more aware of security threats and systems to be robust enough to protect the brand image.

The CISO should ensure that all board members are aware of the potential threats that company faces and help draw a road map to ensure that those threats are mitigated.



The best approach is to open the information to board members and ensure that weekly or monthly threat intelligence reports are relayed to board members.

What soft skills can help security executives collaborate better?

Nowadays, being in the infosec department is a demanding job. Often the security executives forget that a normal user has very little knowledge of potential threats and their impact. A major problem in the awareness programs is the gap between the majority of users and people who handle the security department.

From a security standpoint the security executives tend to interact less with the rest of the users, although this should not be the case. It is critical that information is relayed as much as possible to the end user so that they can know the impact of a breach, which can help them be more careful in their handling of daily activities.

Most often the users in high pressure cases can be off-guard and be prone to a phishing attack, which has been a major threat vector and source of information gathering for the attacker.

It is also important to ensure that awareness programs are more user friendly and interactive with simulations so that every user can relate to the simulation and be more aware in real case incidents. Drills can then follow to test the effectiveness of awareness programs.

Threats are everywhere and always changing - how can we address this difficult reality?

It has always been a cat and mouse chase for organizations to ensure that controls are effective against an adversary.

Ideally, we want to make it a 100% secured environment - however no system or organization can claim it to be that effective.

There are a few programs that need to be implemented in order to cater to these fast changing threats: awareness programs, followed by actual drills/ tests to make sure that the members attending these programs are putting the knowledge in practice; also auditing is necessary to ensure that all the logs which are generated by systems are correlated and made use of rather than having them dumped in raw format with no linking of access protocols.

For example, if user A got physical access to Datacenter, however he didn't check-in at the front desk, it means that there is rough inside escalation access which has triggered this alarm.

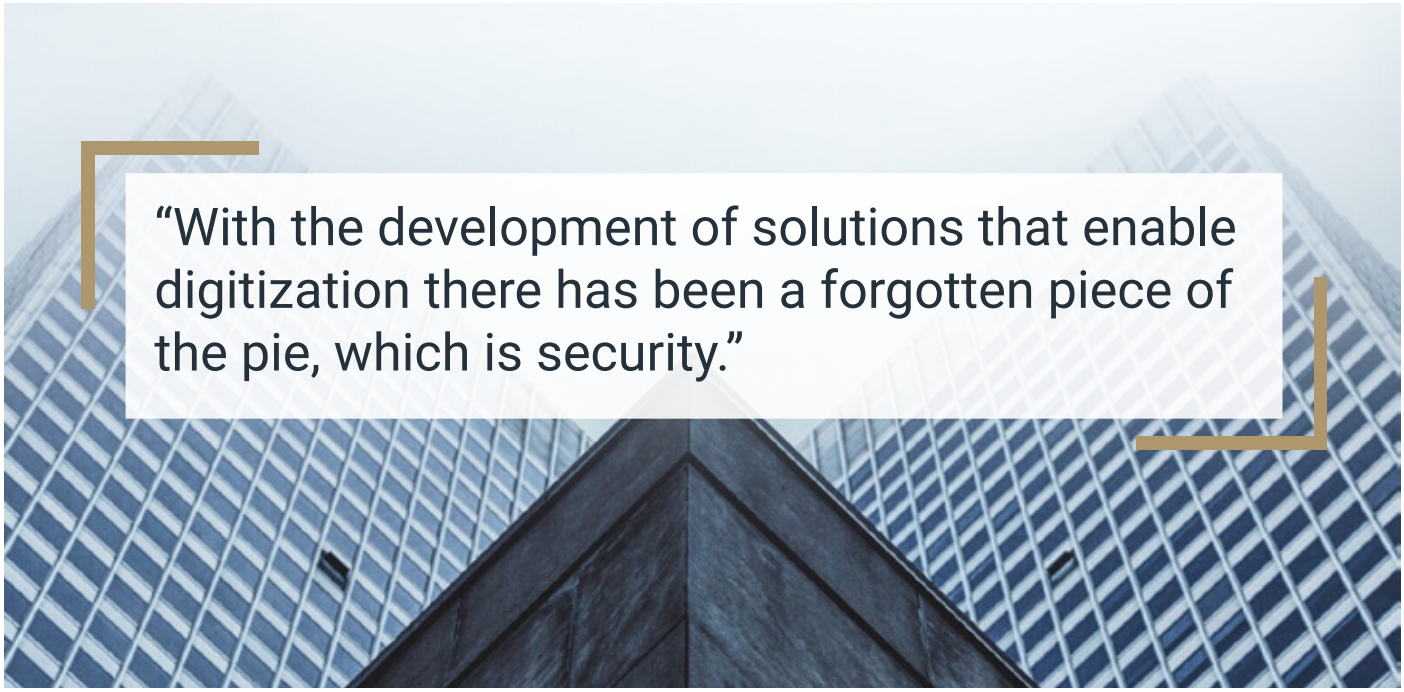
It is the same case with system and software, where audit logs should have a broader view for the SOC team to analyze and ensure that any privilege escalation should raise the alarm in time and be blocked for analysis.

One of the major hindrances which organizations face is the balance between what business wants and what security suggests. This balance needs to be maintained at all times, as sometimes too many restricts can cause an inverse effect where at the time of critical business issues the security considerations are lifted to extreme with no controls left to protect the business.

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

Digitization has been a major player that has changed the way we do business, interact and even make decisions. Its development in all sectors of life has paved the way for great innovation. With the development of solutions that enable digitization there has been a forgotten piece of the pie, which is security.

In recent times the security aspect has been considered thanks to policies such as GDPR which protects the user right and makes sure that solution providers are more thoughtful while designing solutions.



There needs to be international organizations that work as an NGO and enable small solution providers to make more secure applications, as security hardening can be a challenging task for many organizations. This NGO/Body should work at a micro level similar to what UNICEF, USAID and other organizations are doing so that we have a more secure digital space.

How might we address the perception of cyber security holding back the business?

One of the main causes for cyber incidents has been due to a lack of trust on the threats which security teams have been raising with management. This has been the catalyst for a lack of security consideration during designing and implementation.

However, this has drastically changed as adaption of cloud-based workloads and globally connected environments came into existence. However, even today business perceives cyber security as a potential overhead. One of the major plus points from a security standpoint is that the amount of automation and security first approach in the technology department is making sure that this perception is reduced. While protocols are great to have to keep structure, there needs to be a more agile approach for permission related matters as these red tapes become a major nuisance.

Also, systems need to be continuously re-evaluated to ensure that all security protocols placed are effective and have a balanced effect for both business and security. While we all want to be secure, it is critical that business should not suffer due to the over-provisioning of security controls and SOPs.

Closing Statement

In my view there is a gap between a pro-active approach to handling security requirements/incidents and a reactive one which most organizations are currently hooked on. A global consortium/NGO is required which can help organizations to attain a certain level of security with an easy approach so that organizations can elevate their security posture to one of complete information security.

Insight

STELLAR CYBER

How Seemingly Insignificant Data Points Add Precision to Open XDR

STELLAR CYBER®

How Seemingly Insignificant Data Points Add Precision to Open XDR

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

At a glance

- 3 minute read
- The Process of Prioritizing Alerts
- Determining the Role of Minor Alerts
- Every Data Point Matters
- Automating Comprehensive Data Review with Open XDR

With the sheer number of alerts bombarding security teams, even complete triage is not always possible. Expert security analysts scan the alerts and determine the most significant ones.

While their judgment or instinct is generally correct in highlighting alerts that likely indicate significant security events or incidents, smaller, seemingly insignificant findings are often ignored.

Sometimes these are meant to be reviewed later, but that rarely happens if new alerts keep pouring in.

The Process of Prioritizing Alerts

Teams determine top priority alerts based on several factors:

1. The tool creating the alert has already categorized these as their most important category of alert. Harried analysts will first look to these in performing their triage.

2. Security teams prioritize alerts about more important infrastructure or attack surface parts. For instance, an alert that indicates an event inside a data center carries more weight than a general network alert or something happening on an endpoint.

3. And similarly, certain tools carry greater priority over others, particularly in terms of what they monitor and how they operate. Indications of lateral movement have importance over general intrusion detection alerts. Tools using behavioral analytics usually command more attention than those that don't because they help to catch unknown attacks.

4. Analysts want to avoid false positives and will rule out anything that smacks of being erroneous or insignificant.

Even after all these assessments, there are still a considerable number of alerts in a "hard to tell" or "it's probably nothing" category. In an ideal world, these would all be investigated in due time. Unfortunately, with the unrelenting number of new alerts and other demands pressing upon teams, an analyst rarely has the luxury of investigating these, even later. They are quickly forgotten…

Determining the Role of Minor Alerts

It is not wrong how security teams triage and that the more minor alerts get assigned, the lower priority. Should these minor alerts be ignored altogether? The reality is that when push comes to shove and teams are understaffed and overworked, minor alerts remain ignored. Is there value to these alerts? Many are likely of no consequence.

There are some, however, that might make all the difference between finding an attack early or not finding one until after the damage is already done. These lesser alerts may be important in two ways. First, it may be that individually, the alerts cannot convey anything that seems significant. When considered together, however, they may point to attack activity that might otherwise be missed. In this case, the whole picture is far more valuable than the individual alerts or data points.

Every Data Point Matters

however, they may point to attack activity that might otherwise be missed. In this case, the whole picture is far more valuable than the individual alerts or data points.

Putting these data point pieces together may not be intuitive when spread over a large team or part of many findings that a single analyst may have to scan or review. One premise of Open XDR is that every data point matters, and "the more, the merrier" regarding feeding input into the system. Some of these data points may not matter, but including them helps ensure that nothing was missed that could be an important clue. Some may not be important, but others might provide essential context or important corroboration of attack activity. Think of it this way. In a large retail store, a person walking in with a hat, dark sunglasses, or a hoodie may not raise any concerns, but if, within two minutes, ten similarly outfitted individuals walk in, that might warrant attention.

Or, if a person with a hoodie walks in, and then several small disturbances occur (a person falling, something getting knocked over or spilling, etc.) and one of the security cameras mysteriously goes out, that might be a solid clue that something strange and potentially damaging is going on. See More: How Enterprises Can Secure Endpoints With Extended and Managed Detection and Response.

Automating Comprehensive Data Review with Open XDR

The key to an Open XDR system is to utilize advanced machine learning to automatically correlate these findings to find the forest from the trees in a way individuals or teams may not. Such systems welcome data from all sources. Even well-staffed teams with reasonable workloads would not likely handle such volume. Reviewed manually, each data point may be considered minor or insignificant because it might only be slightly anomalous and not close to any threshold of being malicious.

These points provide a more precise picture of attack activity when properly correlated and analyzed. For instance, some alerts may signal a substantial change indicative of something malicious, such as an email click through to a suspicious website or an unknown powershell script executing with high privilege on an endpoint.

Other alerts may look like day-to-day business activities, such as a large volume of data transfer between internal assets or a SaaS app (like Office 365) sharing policy changes.

A second way that lessor alerts might be vitally important is that they may serve as corroborating data or evidence to higher priority alerts that may get some review or assessment but would ultimately have dismissed.

Security analysts are slightly more likely to connect the minor and major findings, but the tendency would be to miss it just because of the volume of alerts, amount of work, and lack of resources. Again, a good Open XDR system should be able to correlate the minor data points with more major ones to increase the precision and speed of finding an active attack.

Whether serving as an individual data point to establish a big picture or as more corroboration, "minor" data points are important for the speed and fidelity of uncovering potential attack activity. The task of finding an active attack quickly and with a high degree of accuracy is difficult.

The odds are overwhelmingly in favor of an attacker not being detected. To vastly change the odds, an entirely new approach to security is needed, one where every data point is important and counts towards finding what might otherwise be hidden.

By moving from complete dependence on individual security tools to centralizing all data and alerts—including the large and the small—such as with Open XDR, organizations can gain new advantages over attackers and no longer be relegated to the losing end. Ideally, data should not be ignored, but, rather considered in total to give organizations an edge in preventing or mitigating attacks.

About the Author

Sam Jones

Vice President of Product Management

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

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

@CSOfinder

Our Global Search Engine for Cyber Security Companies

How It Works

Visit... @CSOFinder

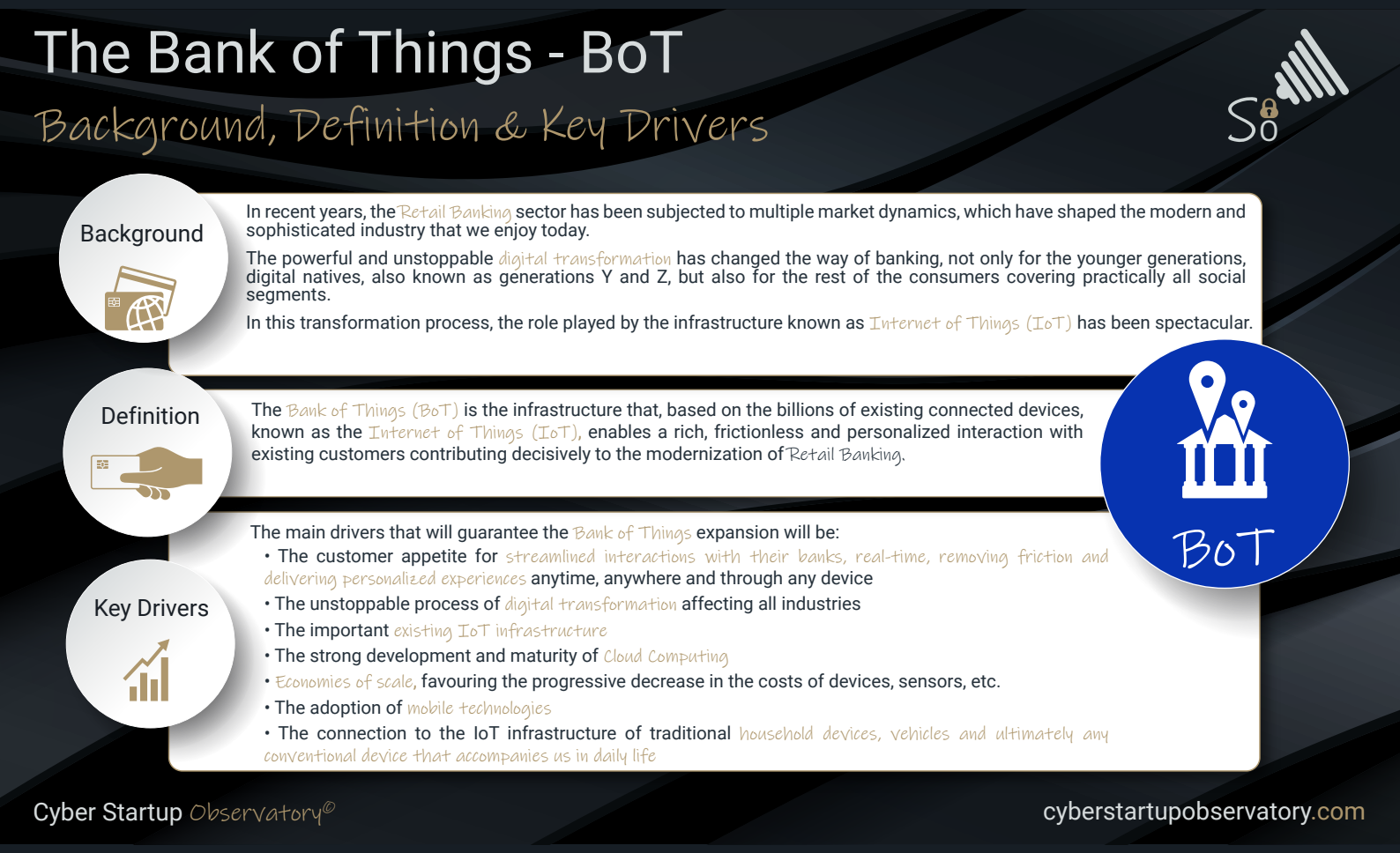
Resources

Infographic

The Bank of Things – BoT

The Bank of Things

BoT



Available for download in Press Quality

Infographics - Financial Services

Cyber Startup Observatory - Community

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.

ATEMPO

Best practices could save you!

preserving data ecosystems

Best practices could save you!

Author: Atempo

At a glance

- 3 minute read
- Best practices could save you!
- There have been several large-scale ransomware attacks in Asia
- Be prepared!
- The good practices to protect data

In a recent blog on this web site, we warned enterprises in Asia of the rolling fire of malicious attacks. The trend is still here and has gotten even worse. According to the IBM 2021 Cost of a Data Breach Report, Asia was the most attacked region that year, concentrating 26% of all cyberattacks, while Europe (24%), North America (23%), the Middle East (14%) and Latin America (13%) were the targets of the remaining attacks. In 2022, the trend of cyberattacks in Asia has continued to increase. According to research by Kaspersky, Jakarta- Indonesia alone experienced more than 11 million attacks in the first quarter of the year. This number reflected a 22% increase from the previous year.

Furthermore, the security company blocked a total of 11,260,643 phishing links across Asia using their anti-phishing systems with most of them being traced to the devices of users in Vietnam, Indonesia, and Malaysia.

There have been several large-scale ransomware attacks in Asia over the last few years.

An eye clinic in Singapore, web hosting services in Malaysia, and insurance companies across Thailand, Malaysia, Hong Kong, and the Philippines have all been victims, indicating the diversity of industries in which attacks took place. Some factors leave organizations vulnerable to these attacks in the first place.

First comes the insufficient knowledge about IT products. Second is the scarcity of security staff.

Unfortunately, some companies underestimate the importance of good security measures until it is too late. They fail to recognize that cybersecurity can be essential to business survival, thereby neglecting to equip themselves or invest in strong security products and solutions.

Be prepared!

When it comes to protecting your business against cyberattacks, you must be prepared. Training and sensibilization of your workforce is the first step that should be taken. Then you must develop a disaster recovery plan to guide you should you be attacked. This plan should answer such questions as: What to do when you are attacked? How to react? How to restore business services?. You need the appropriate solutions to address these issues.

The most important thing is to overcome the impact of the attack. Speed and precision are required on what and how to restore. Once your disaster recovery plan is complete, you should train your employees on how to use the plan. Have them practice the different steps of the plan which will give you the possibility to adjust or enhance the plan.

The good practices to protect data

The 3-2-1 rule is a traditional approach to keeping your files safe and has been adopted by a great number of organizations. This policy, in simple terms, outlines best practices for business continuity. It defines how to avoid data loss.

Keep at least **3** copies of your data

Keep the backed-up data on **2** different storage types

Keep at least **1** copy of the data offsite.

Last but not least, it's better to keep a copy offline ! The 3-2-1 approach should guide your strategy and processes to avoid data loss and reduce the impact of an attack. It could also help you in selecting the appropriate data protection solution for your business. Such solution should assist you in identifying and locating your data rapidly to avoid wasting time when a restore is necessary. In other words, you will not have to look for a needle in a haystack to find and restore the correct data.

Speed and precision are great, but it is important to be sure that the data you restore is safe from infection. **Air gap is the solution.** It is a security measure to ensure that a computer or network is physically isolated from the public Internet or an unsecured local area network. Il ensures that the data you restore was totally isolated from the attacked environment and was not corrupted during the attack. Air gap enhances resilience and provides a starting point of confidence to begin rebuilding after an attack.

Today, backup infrastructure is the first line and the last bastion to defend against ransomwares. It remains the best solution to protect data efficiently. But backups must be sure and protected proactively to avoid being ciphered when an attack occurs. One way to ensure the safety of your backups is to lock the backed up data in a certain state to make it immutable.

There are different ways to do it depending on the storage technology you use. In block technology, WORM (Write Once Read Many) is a way to lock. **Object lock is the most used way to make object immutable.** It's often accompanied by retention locking technology to ensure no user -- even an admin -- can expire, change, or delete the immutable backup until the end of a designated retention period. Also important is securing the access to the solution by a RBAC (Role Based Access Control) tool.

It governs the access for users and administrators of the systems. To avoid intrusions within the backup platform, this simple access role control could be enhanced with a multifactor authentication solution, at least 2 factors.

This technology provides a unique code through a third-party application which is required to access the administration console of the backup solution. It strengthens access control and avoid intrusion even in cases of stolen connection credentials.

Atempo's solutions integrate several features to make backup data immutable. When your backups are on a S3 object storage for instance, you can enable object locking. With this feature, your stored objects become immutable during the defined retention period. Object immutability helps prevent the cryptovirus from encrypting your backups.

All Atempo solutions follow backup best practices to better defend against malicious attacks, particularly ransomware. Best practices do not prevent or avoid an attack, but they can save you from having to deal with the consequences of the attack.

CYVIATION

Can we still trust flight instruments in the cyber age?

CYVIATION

Can we still trust flight instruments in the cyber age?

Author: Nissim Belzer, Chief Technology Officer @ CyViation

At a glance

- 2 minute read
- Can we still trust flight instruments in the cyber age?
- The possibility still exists that instrument failure could lead to more tragic events

cyviation

Trusting the instruments is a fundamental cornerstone of any aircraft's training program. But what happens when flight instruments become unreliable?

Putting your trust in the cockpit's instruments is one of the challenges of learning to fly. Novice pilots can confuse what they see and feel and what their controls tell them.

The way we experience the elements—through our eyes, our inner ear, and our kinaesthetic senses—is usually reliable and trustworthy, serving us well throughout our lives. But this is not the case when a pilot experiences disorientation in the clouds.

A pilot's senses can lead him to believe that an aircraft is flying straight and level when it is veering to one side or even in a steep descent. Fortunately, visual and audible alarms are triggered in such cases to alert the pilot. This system has proven so reliable that pilots are trained to disregard their senses in an emergency and to trust their instruments instead.

On October 29, 2018, and March 10, 2019, two 737 MAX aircraft—Lion Air Flight 610 and Ethiopian Airlines Flight 302, respectively—experienced catastrophic errors that cost the lives of 346 passengers and crew.

The entire 737 MAX global fleet was grounded, pending separate NTSB (National Transportation Safety Board) investigations. The final report, released on October 23, 2019, found that a combination of MCAS (Manoeuvring Characteristics Augmentation System) design flaws and AoA (angle-of-attack) sensor failure had caused the pilots to set the pitch of the horizontal stabilizer to full "nose down" position [ADD citation]. The 737 MAX returned to service worldwide in 2021, with the FAA requiring that all MAX pilots receive MCAS training in flight simulators.

The possibility still exists that instrument failure could lead to more tragic events—instrument failure caused by a cyberattack.

Some research institutes have addressed the human factor during cyberattacks by testing a pilot's reaction time, behavior, corrective actions, etc. The conclusion is that higher workload and weakened trust in the system result in rapid erosion of the basic tenet of pilot training—trust your instruments.

To quote one study, "… cyber-attacks influence pilots' workload, trust in the system, visual information acquisition, behavior, and performance," going on to conclude, "… warning about an impending cyberattack can moderate several of those effects …."

But changing the 'trust the instruments' paradigm is a tough nut to crack. To date, no major cyberattacks have been publicly disclosed. Pilots are not trained for them and may not even be aware their aircraft is under attack because the fleet lacks crucial detection systems. Most pilots aren't even familiar with the cyber QRH (Quick Reference Handbook) and, therefore, can take no predefined actions in the event of an attack.

OEMs (Original Equipment Manufacturers) and airlines are increasingly allocating resources to prepare for future cyber threats. Regulations, such as DO-355/ED-204, address this imperative and urge operators to monitor and train flight crews for the inevitable attack proactively. This training should include IT, OT, simulators, and in-flight IDSs (Intrusion Detection Systems).

It is now widely acknowledged that pilots trust the instruments' training may be insufficient and tragically ineffective during real-life events. Pilots must be trained and prepared to avoid air disasters caused by a potential cyberattack.

Airbus Cybersecurity

European specialist in cyber security

AIRBUS
CYBERSECURITY

01

AIRBUS CYBERSECURITY

Company Description

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

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

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

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

02

Company Information

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

Key Target Verticals:

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

03

AIRBUS CYBERSECURITY

The Product

Product Category: Cyber Range, Detection & Prevention; SOC

Product Stage: Released

Product Names and Brief Description:

- Cyber Range: Training and simulation platform

Services Provided:

- Cyber threat intelligence
- Network security
- Cyber resillience

04

Product in detail: CyberRange

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

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

The main functionalities of our CyberRange are:

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

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

AIRBUS CYBERSECURITY

How does it work?

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

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

Pre-production tests:

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

Operational qualification:

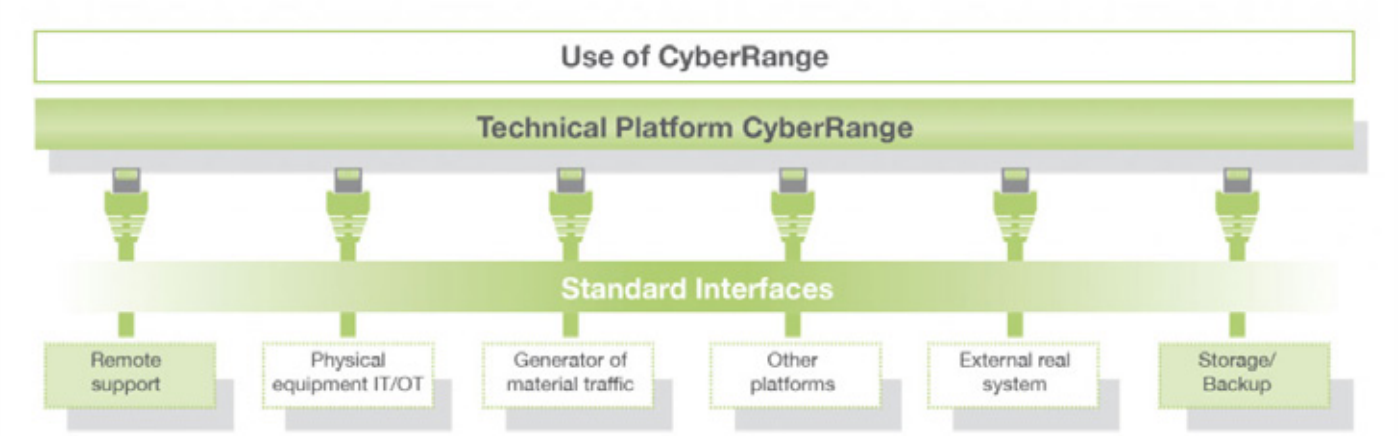
- Assessment of the impact of new equipment on a system
- Study of rule integration or the implementation of new procedures
- Analysis of cyber attack behaviour on its infrastructure without taking any risks

Training

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

Exercices

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



Key Benefits

06

AIRBUS CYBERSECURITY

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

Unique Differentiators

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

Future Functionality

- New scenarios integrated by default
- Various training packages available

AIRBUS
CYBERSECURITY

AIRBUS
CYBERSECURITY

Infographic

Cyber Range

Main Functionalities

Stormshield

A European Leader in Digital Infrastructure Security

STORMSHIELD

01

Company Description

STORMSHIELD

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

02

Company Information

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

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

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

03

The Product

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

Product Stage: Released

Product Names and Brief Description:

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

Services Provided:

- Threat Intelligence, Training, Support

Customer Footprint

Markets with Customers:

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

Relevant Public Success Stories per Key Target Vertical:

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

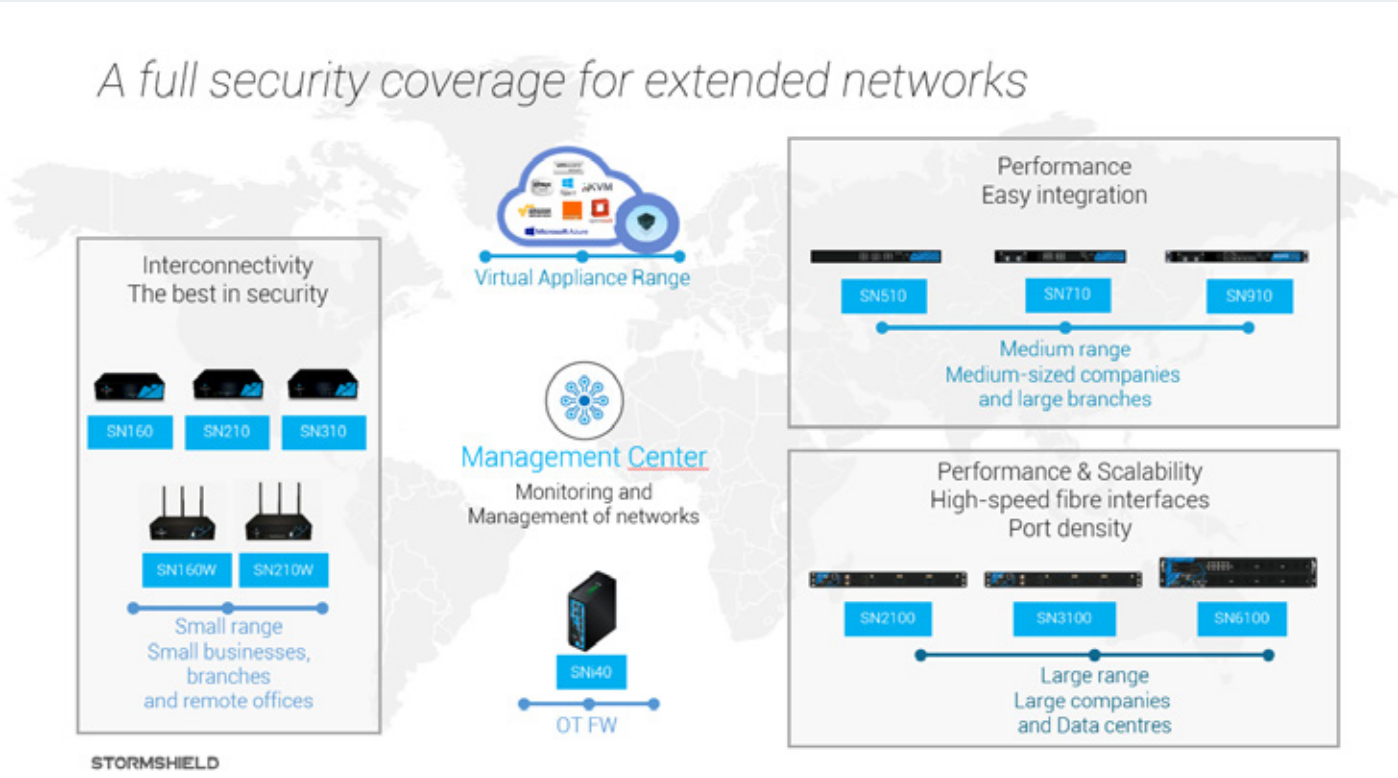
STORMSHIELD

Product in detail

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

How does it work?

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



Key Benefits

STORMSHIELD

Ensure that business activities will remain uninterrupted

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

Protect the internet use

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

Connect employees and remote offices

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

Meet compliance requirements

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

Unique Differentiators

Unrivaled Trust

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

Global Protection for Converged IT/OT Networks

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

Performance

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

STORMSHIELD

Product in detail

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

How does it work?

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

Key Benefits

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

07

STORMSHIELD

Unique Differentiators

Unrivaled Trust

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

Global Protection for Converged IT/OT Networks

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

Performance

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

Future functionality

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

Certifications

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

CYBER RANGES

A Next-generation Cyber Range as a Service

CYBER RANGES

01

CYBER RANGES

Company Description

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

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

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

02

Company Information

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

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

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

03

CYBER RANGES

The Product

Product Category: Cyber Range, Detection & Prevention; SOC

Product Stage: Released & Deployed

Product Names and Brief Description:

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

Services Provided:

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

04

Product in detail: CYBER RANGES

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

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

CYBER RANGES offers you:

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

How does it work?

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

CYBER RANGES

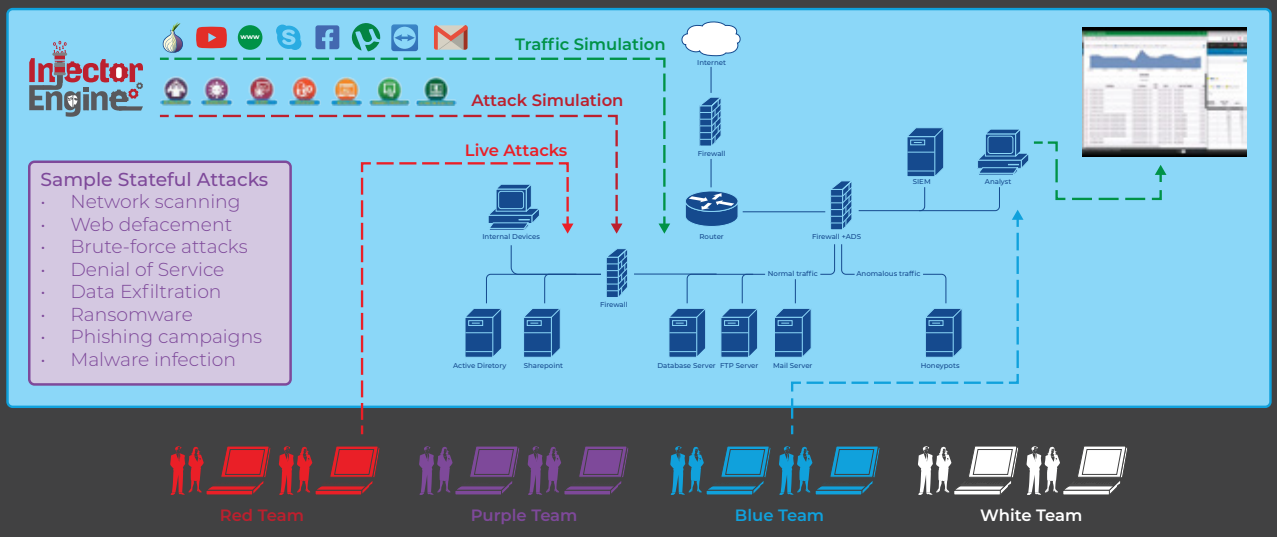
How does it work?

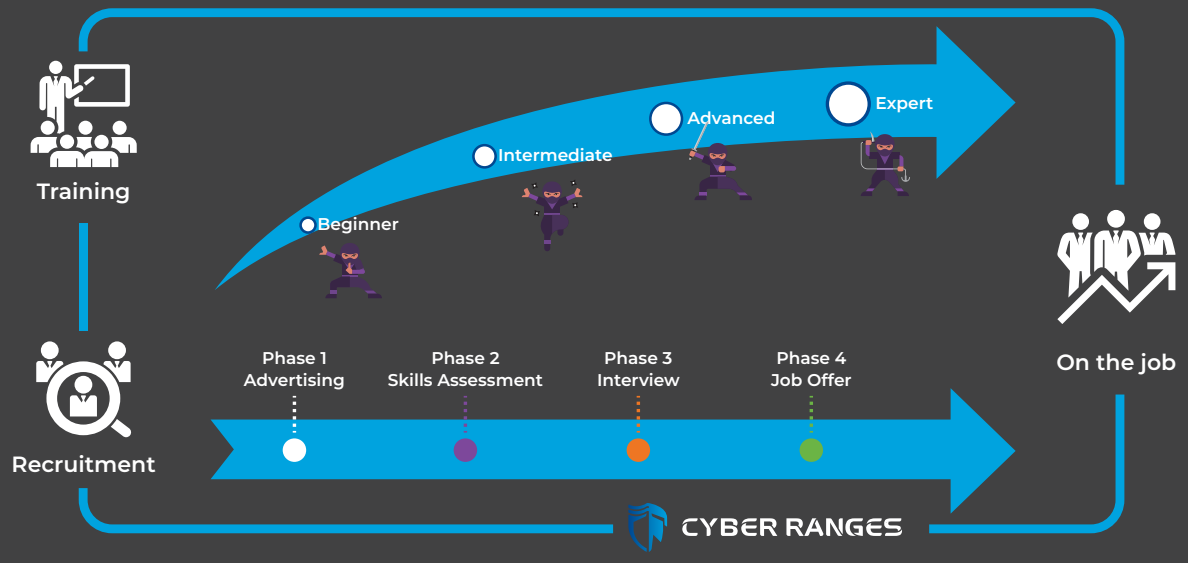
CREATE Design and build custom scenarios, including complex virtual environments, storylines with clear mission/task objectives and cyber challenges.

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

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

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





06

CYBER RANGES

Key Benefits

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

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

07

Unique Differentiators

Key differentiators of CYBER RANGES are:

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

08

CYBER RANGES

Future Functionality

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

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

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

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

09

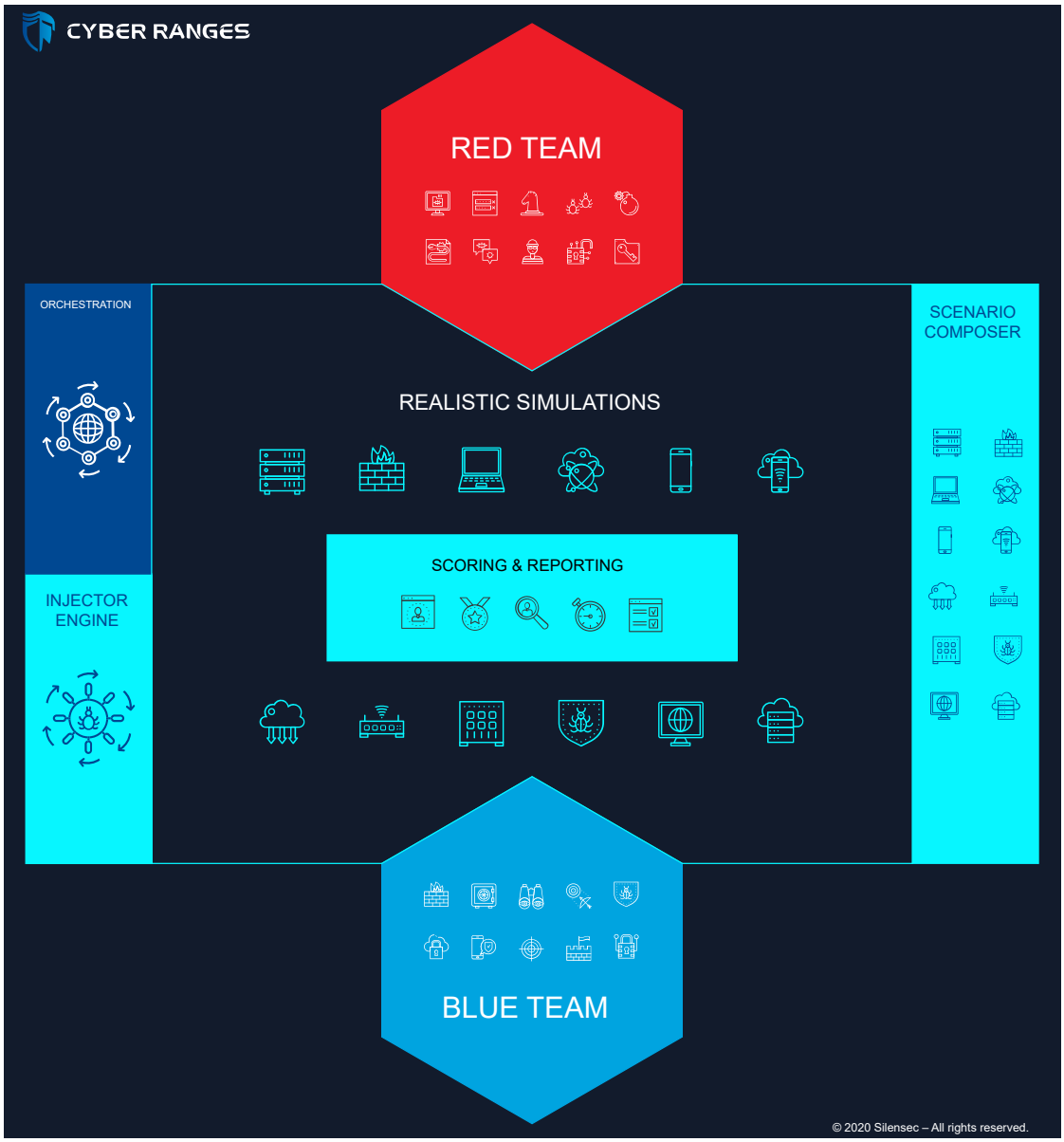
Services provided

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

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

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

Infographic: Red vs Blue Team realistic simulations



Certifications

silensec™ iso27001 Certified

senhasegura

Global Privileged Access Management (PAM) Vendor

senhasegura

01

Company Description

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

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

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

02

Company Information

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

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

03

The Product

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

Product Stage: Released & Deployed

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

Services Provided:

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

04

senhasegura

Product in detail

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

For PASM:

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

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

For PEDM:

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

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

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

05

How does it work?

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

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

06

Key Benefits

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

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

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

07

Unique Differentiators

Features that differentiate senhasegura against our competitors:

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

Other differentials:

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

Privileged information
- Personal vault
- Privileged data

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

Secret Management
- Cloud IAM provisioning

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

Future functionality

08

Our main innovation drivers are:

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

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

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

Video

Blu5 Group

Shaping resilient IT

01

Company Description

Blu5 takes pride in **supporting digitisation teams in the challenge to reduce the surface of attacks, while securing core critical operations.** We engineer hardware and software to address the needs of Critical Infrastructures, IoT, FinTech, BioMedical, Space & Defence.

Resilience is our team keyword. Cost effectiveness, smooth system integration and timely solutions are our daily leads, working hand in hand with our customers to deliver user friendly implementations suitable for their IT infrastructures.

Since foundation in 2007, the Blu5 R&D team, rich of 40+ patents, has been the company's key enabler for generating innovative solutions.

02

Company Information

Company Name: Blu5 Group

Founded: 01/2007

Employees: 30 to 50

Web: www.blu5group.com

Headquarters: Singapore

Key Target Verticals: Government, Defense, Critical Infrastructure, Banking and Finance, IoT, Manufacturing, Telecom

03

The Product

Product Category: Application and Web Security, Data and Endpoint Security, IoT - IIoT, Mobile, Cloud and Network Security

Product Stage: Released & Deployed

Product Names and Brief Description:

- SElink™: layered security protocol to protect data in motion for bandwidth-sensitive applications

04

Product in detail

SElink™

SElink is the solution to protect data-in-motion. By establishing a protected and authenticated channel, SElink allows two or more entities to securely exchange data.

Designed to protect dedicated links independently from the technology and the protocols in use, SElink is the ideal choice to apply a strong security layer on existing systems and networks. Suited for Point-To-Point and Point-To-Multi Point data flows, SElink does not require any dedicated complex connection setups nor dependent upon standard virtual tunnelling protocols or even SSL/TLS for the purpose of protecting data-in-motion.

SAs compared to standard SSL/TLS implementations, SElink requires extremely low bandwidth for link establishments, zero data overhead on encryption and configurable key evolution policies.

SElink is also suitable to be deployed over standard Http, Https connections in a client-server scenario.

Typical use cases for SElink in the IT domain include secure remote-access and authentication to information held in centralised database servers, applications (e.g. Self Service Kiosks - Bank ATMs, vending machines, Business Software, HR, Accounting, etc.) and other online-based services (e.g. e-filing of tax revenue, online gaming, cloud, etc.)

05

How does it work?

When two or more entities need to create a secure communication channel, the SElink library negotiates the session keys and performs encryption, signature, decryption and verification operations on the exchanged data.

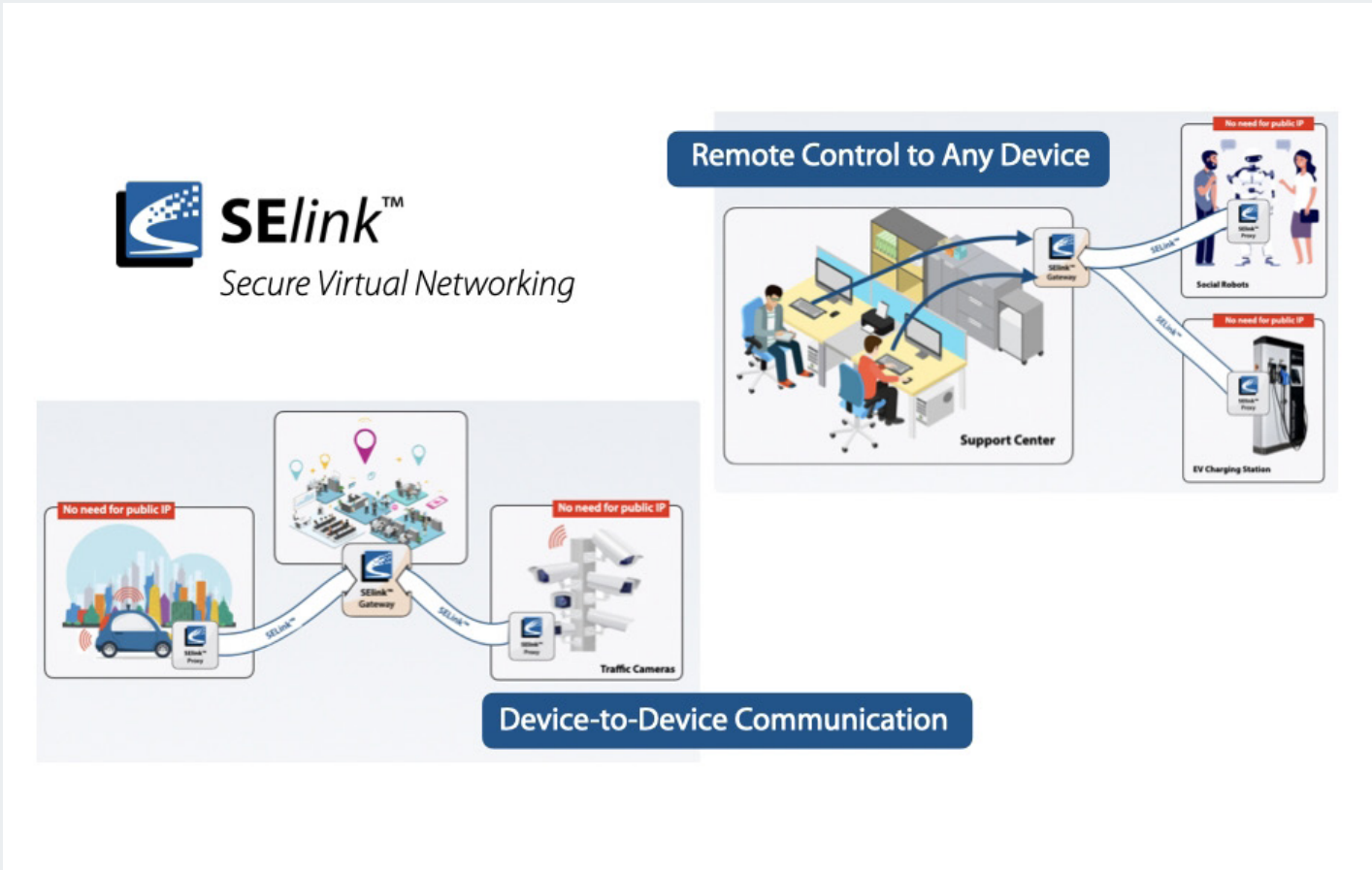
SElink negotiation process aims to create two communication keys (encrypt/Decrypt/verify) on the base of the security policies set on the peers (e.g.supported algorithms, pre-defined communication groups, cryptographic mechanisms…)

How does it work? (Cont'd)

Each Entity can manage several SElink channels at the same time.

Unlike TLS and other standard encryption protocols, SElink™ generates new session keys either every 'N' seconds or every 'M' bytes. By default SElink, is configured to create a new session key every 1.024 bytes and supports variable blocks size cryptographic algorithms.

SElink implementations:
- SDK implemented on Blu5 xSE™ technologies
- OS independent
- SW or HW microSD, USB, chip, SW only
- C/C++ portable code
- Several wrappers available (e.g. JNI, Javascript, PHP, etc.)



Key Benefits

SElink, Secure Virtual Networking, provides layered security for the protection of your data in motion, without impacting on your data flow and IT network performance.

Quantum-safe, Simple, Fast and Versatile, SElink is designed for bandwidth-sensitive operations.

- More Data, less Bandwidth (Zero overhead)
- No personal traffic reaching your company (Split tunneling by design)
- Lockout malicious software (Application access control)
- Stable connections on poor networks (automatic session recovery)
- Dematerialise your network routes (Network Virtualisation)
- Future-proof your network security (Quantum resilient strategies)
- One Tunnel One Application (Centralised Endpoint management)
- Activate multiple tunnels at the same time (Simultaneous multi-site connections)
- Business continuity in one single product (Integrated redundancy and disaster recovery)
- Transport protocol independent (Http, XML, XMPP, CoAP)
- Easy to use (based on less than 10 APIs)

Unique Differentiators

- automatic session recovery (no key renegotiation)
- zero bandwidth overhead
- Quantum-safe
- Split tunnelling by design
- custom and new algorithms injected in real-time (Crypto Agility) ready for implementation of Post-quantum algorithms selected by NIST

Future Functionality

- Unified client-server identity

07

Awards

- Designed in Singapore Awards 2019
- Singapore SME 1000 Company Award 2017
- SME 100 Awards 2017: Singapore's Fast-Moving Companies
- Singapore SME 1000 Sales/Turnover Growth Excellence Award 2016
- Singapore Emerging Enterprise Awards 2014

08

Partners

IAI/ELTA

ELTA Systems, a leading Defense Electronics Company

01

Company Description

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

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

02

Company Information

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

Key target verticals:

National Cybersecurity entities, Government, Army, Navy

03

The Product

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

Product Names and Brief Description:

- CEWC
- Maestro
- Tame Range
- Neptune

Customer Footprint

Relevant Public Success Stories per Key Target Vertical:

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

Product in detail: Cyber Early Warning Center - CEWC

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

How does it work?

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

05

Key Benefits

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

Unique Differentiators

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

Future Functionality

Evolved SOC ecosystem build for land / maritime / aviation

Product in detail: MAESTRO

State of the art automated environment for media investigation

How does it work?

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

Product benefits and unique differentiators

Key Benefits:

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

Unique Differentiators:

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

Future Functionality:

Mobile analysis platform for IR teams for on-site analysis

Product in detail: TAME RANGE

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

How does it work?

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

Product benefits and unique differentiators

Key Benefits:

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

Unique Differentiators:

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

Future Functionality:

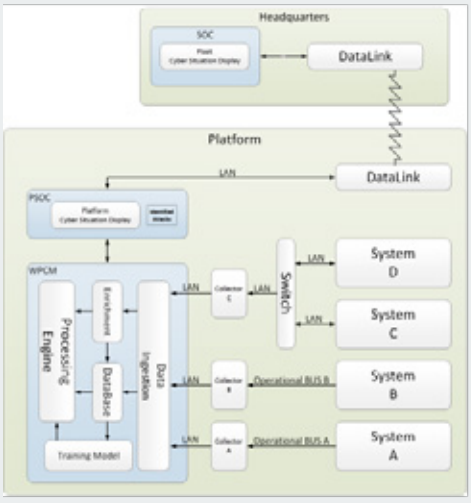
- Support of IOT attack scenarios

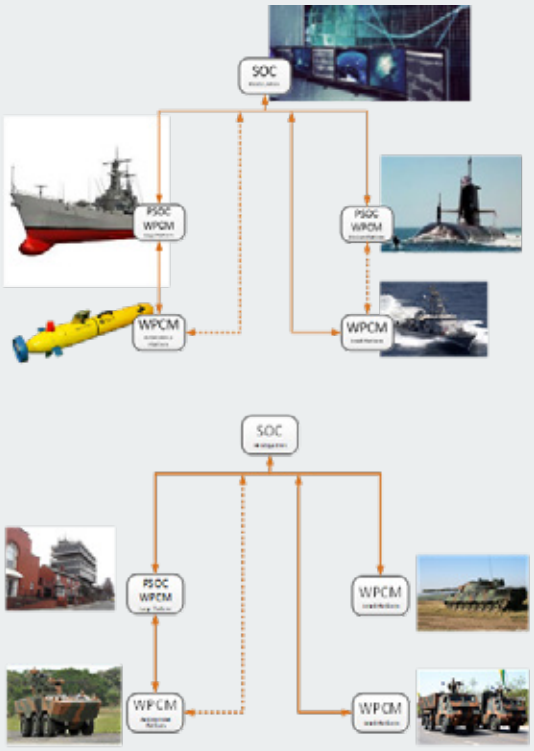
Product in detail: Neptune

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

How does it work?

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





09

Key Benefits

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

Unique Differentiators

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

Future Functionality

- Organizational & Industrial solutions
- Improved detection swiftness

Partners

Israel Cyber Companies Consortium – IC3

Israel Aviation Cyber Companies Consortium – IAC3

Stellar Cyber

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

STELLAR CYBER®

01

Company Description

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

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

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

02

Company Information

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

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

03

The Product

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

Product Stage: Released & Deployed

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

STELLAR CYBER®

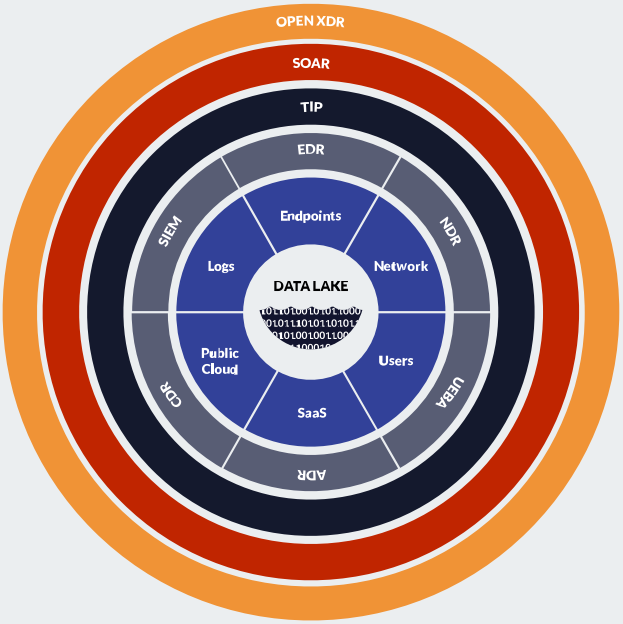
Product in detail

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

How does it work?

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

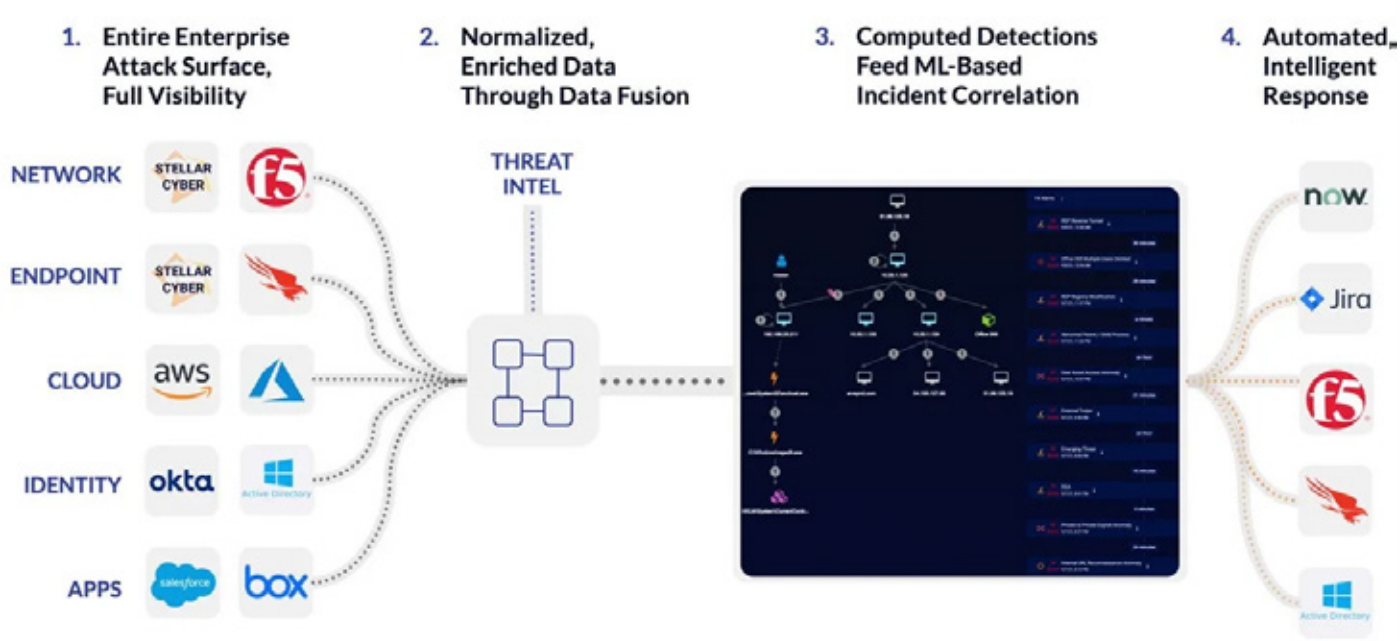
The outcome of Open XDR is protecting your enterprise from threats from a single platform versus multiple tools that have weak or non-existent connections band-aiding it all together. And the ultimate outcome of Open XDR is radically improved detection and response at a price enterprise's can afford.



Stellar Cyber's Approach To Open XDR

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

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



06

Key Benefits

The value of Open XDR:

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

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

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

07

Unique Differentiators

Our unique differentiators are:

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

07

Unique Differentiators (Cont'd)

2. XDR Kill Chain™:

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

08

Videos

Stellar Cyber Incident Correlation

Stellar Cyber XDR Kill Chain

Atempo

Data Protection Solutions

preserving data ecosystems

Company Description

01

Atempo is a leading independent European-based software vendor with an established global presence providing solutions to **protect, store, move and recover all mission-critical data sets** for thousands of companies worldwide. With this feature set and an **extensive range of supported storage technologies and applications**, Atempo is suitable for all centralized or multi-site organizations including those having extreme scale data volumes, petabyte and above.

Company Information

02

Company Name: ATEMPO

Founded: 1992

Employees: 160

Web: www.atempo.com

Headquarters: Massy, South of Paris, France

Other French offices: La Ciotat, Lyon, Toulouse, Vannes.

Worldwide offices: UK, Germany, USA, Singapore, Korea.

The Product

03

Miria: A unique solution to back up and migrate or synchronize billions of unstructured data files between heterogeneous storage.

Tina: Enterprise backup and restore solution for physical and virtual machines, supporting a wide range of operating systems and applications.

Lina: Continuous data protection for desktops, laptops and file servers, offering self-service restore capabilities.

Customer Footprint

Relevant Public Success Stories:

- Public Administration
- Healthcare
- Research & Higher Education
- Industry & Manufacturing
- Media & Entertainment
- Other

Product in detail: Miria

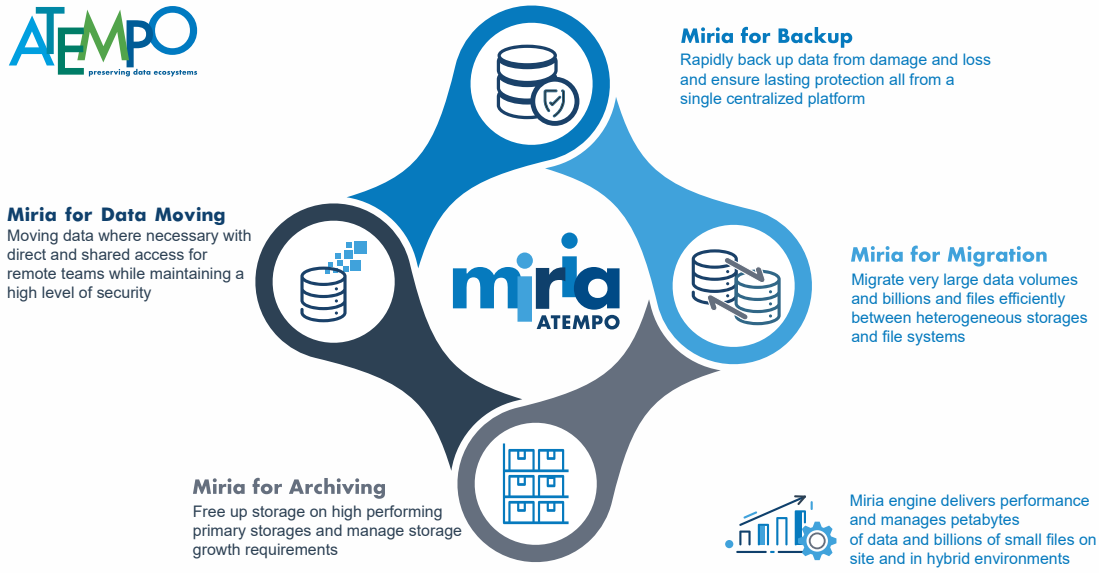
Miria is a powerful and scalable backup, archive, copy/move, migration and synchronization solution for petabyte scale unstructured file-based storages.

How does it work?

Miria for Archiving allows organizations to cost effectively manage the growth of their file-based data, particularly for data-intensive industries.

Miria for Archiving is a high-performance file management software for large file-based data sets that delivers:

- Cross-platforms backup and restore capability for large scale-out NAS, parallel file systems and file servers
- Express post-disaster restart for protected NAS by offering direct use of the backup target for read/write use
- File and folders on-going synchronization between heterogeneous storages with ACLs and remote sites support
- Automated permanent storage migration between heterogeneous platforms with ACLs preservation
- End-User driven or automatic Archiving via simple drag-and-drop interface allowing end-users operations without IT staff assistance And much more...



Key Benefits: Miria

05

- Efficient backup and restore for petabyte-scale volumes and billions of files:
  - Fast-scanning large storages for new, modified or deleted files
  - Complying with backup windows constraints
  - Preserving users rights/groups (ACLs)
- Making migration or synchronization of very large data set of files between heterogeneous storage simple and efficient

Unique Differentiators

- Heterogeneous platform integration that preserves ACLs across storages, operating systems and platforms
- User driven or automated workflows
- Fast data movement due to heavy parallelization and leveraging scalable groups of data movers

Future Functionality

- **SnapStor –** New capability to leverage a GPFS storage as a backup target that enables direct and immediate restart of production directly from the backup in case of disaster – as well as empowering the rebuilding of the storage platform once ready to restart

Product Video

Product in detail: Tina (Time Navigator)

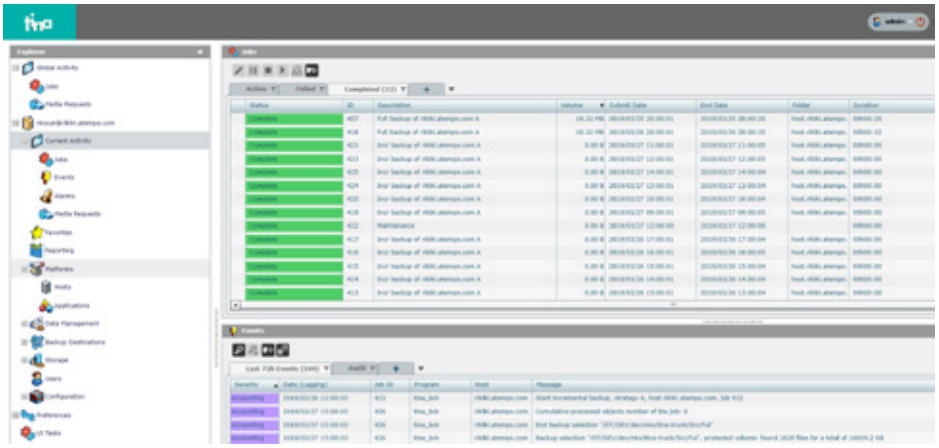
Built for **complex, heterogeneous enterprise environments, Tina** offers complete data protection, whether you manage a single work group or multiple data centers. Time Navigator makes it easy to **meet backup windows, to ensure digital security and to manage tiers of backup storage**, regardless of the platform, application or media.

How does it work?

Tina transforms backup by focusing on what matters in your business: recovery of data. Whatever the platform, restore is always based on three simple concepts:

1-Select data.
2-Choose date & time.
3-Restore.

Restore-centric solution that provides visual access to the file system in real-time showing not only files and directories but also deleted files. The user never needs to worry about where the data has been saved. Data is tracked throughout its lifecycle and can be restored with just 3-clicks regardless of the complexity of its backup history. Tina provides a common interface that displays the files in the same way regardless of platform.



Key Benefits: Tina

- **Security and compliance:** encryption, digital certificates, key management and activity trails can be applied to specific sets of protected data.
- **Unique restore:** no need to know where the data resides, only the date/time to restore back in time. File restore operations are made easier by providing a unique restore interface across a wide support of platforms and infrastructure.

Unique Differentiators

- **Tina** - A unique approach to data restoration locates and restores individual files from any point in time and from any tier of storage, enabling both IT staff and end users to quickly restore lost files.
- **Tina** is the ONLY solution able to visualize all files, including deleted ones (from physical and virtual machines) and restore them with the same 3-click approach through a simple interface.

Future Functionality

- Support of VMware vSphere
- Enhanced security for data encryption
- Fine granular restore of Active Directory
- Deduplication for all applications and Operating Systems
- Oracle RMAN script configuration wizard

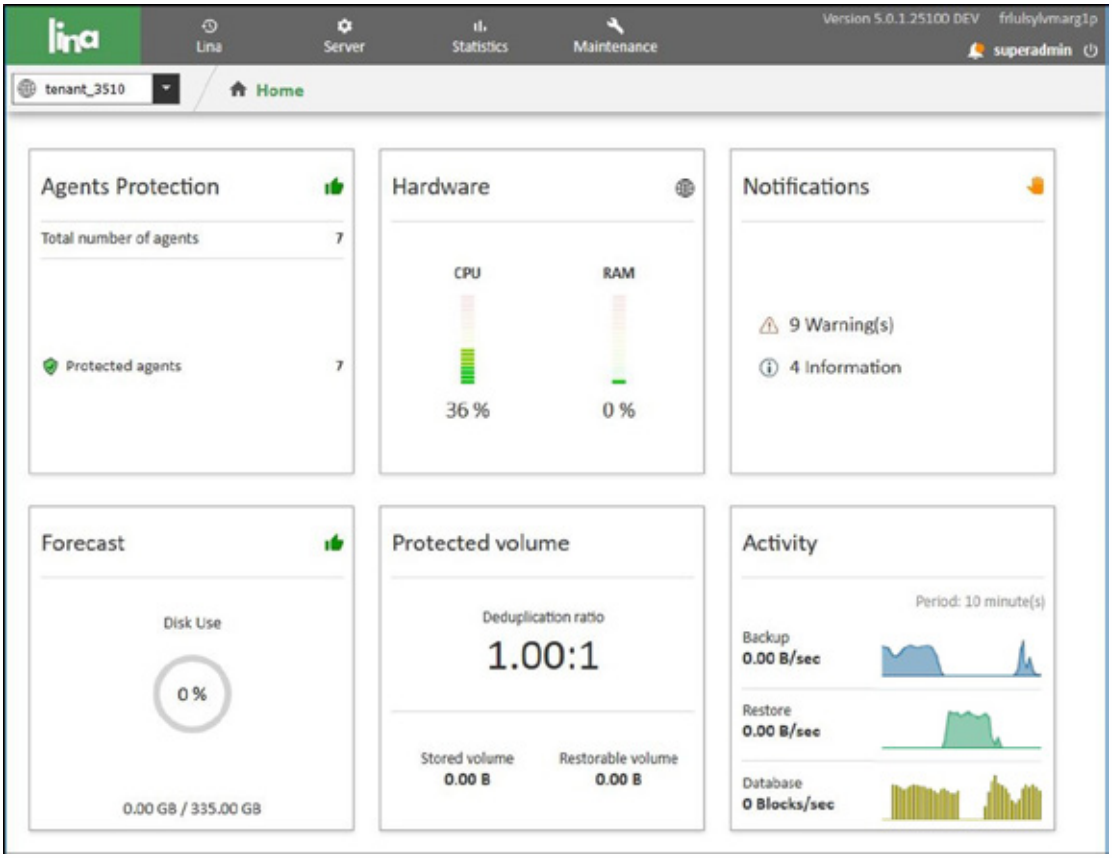
Product in detail: Lina

Lina provides a standalone, continuous data protection solution with advanced data de-duplication for remote offices, workstations, file servers and laptops.

How does it work?

With more and more critical data being stored on laptops, data protection is essential to protect the business. **Lina** provides continuous data protection for files residing on desktops, laptops and file servers, offering self-service restore capabilities.

With **Lina**, administrators just need to roll-out data protection policies across the enterprise and end users are empowered to restore data, through a wizard or a web browser.



Key Benefits: Lina

- End-users benefit from seamless protection of their data. There is no need to ask the administrator for the restore
- Administrators save time by not having to deal with numerous end-user restore requests
- Infrastructure managers benefit from reduced storage costs and optimized network performances
- Continuous data protection, no need to schedule backups, no risk of exceeding backup windows

Unique Differentiators

- **Lina** offers wizards to restore, but also advanced restore features (Time Navigation, cross restore).
- **Lina** can protect laptops and file servers with millions of files.
- De-duplication mechanism reduces storage space and network use.

Future Functionality

- Multi-servers Architecture
- Encryption
- Fail over Replication
- Restore Audit Trail

Certifications & Awards

Label France CyberSecurity identifying French Cybersecurity quality solutions which respects the highest level of computer security requirements.

Atempo is also participating actively to the French Government Program, to bring assistance to cyberattack victims, through the **Cybermalveillance.gouv.fr platform**.

Based on our ability to back up, protect, manage, and recover data, the most valuable asset of all business, to ensure data security and business continuity, Atempo has been named by the Insight Success Magazine one of the 10 Most Reliable Cybersecurity Solution Providers - 2020.

AI Global Media Ltd has put the Cyber Security Awards in place to honour companies that have gone above and beyond in this highly competitive sector. Atempo has been named: “Best for Data Protection & Restore Software - Europe”, as recognition of our outstanding performances within the sector.

MyTechMag, a pioneering tech magazine has acknowledged Atempo—a leading independent European-based software vendor with a global presence, offering Disaster Recovery solutions to protect, store, move and recover all your data—one among the **“Top 10 Promising Disaster Recovery Solution Providers 2020**" who are transforming companies with their unique solutions.

11

The Atempo.Wooxo Group has been selected to join the Alumni **French Tech 120** program, designed to nurture 25 unicorns by 2025.

Luc d'Urso has been named "**Best Cyber Security CEO**" in Europe in the 2020 European competition, in recognition of his active role in the fight against cybercrime.

Institutional Partners

Feedback and suggestions

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

We appreciate receiving compliments

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

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

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

You can contact us at:

info@cyberstartupobservatory.com

The Global Cyber Innovation Network

The Cyber Startup Observatory®

The Cyber Startup Observatory®

APAC - 7th Edition