CyberProof®
A UST Company

Guide to SecOps for Financial Organizations

Building consumer trust and optimizing technology

Contents

The Challenge Of Technological Diversification & Dispersal

The rapid growth we are currently experiencing in technological innovation brings the promise of new services that enhance the user experience and can reduce costs. But this comes at a price if cyber resilience is not embedded as part of the organization's day-to-day operations.

According to a recent report,[1] organizations in the Financial Services (FS) industry identified compliance and regulation, AI threats, and ransomware as their top cyber security challenges.

As new, cutting-edge technologies are adopted, FS companies are facing an ecosystem of unprecedented complexity (see Figure 1). The implementation of cloud and mobile technology, an expanded supply chain, new payment platforms, application-driven environments and more, means that the attack surface has been extended significantly.

Technology diversification and dispersal mean that a strong security operations framework is needed to drive customer confidence.

Organizations in the FS industry are faced with a wide range of threats, from supply chain risk to identity theft and data manipulation. Change is the name of the game – but in the current IT landscape, one constant remains: ensuring critical data and infrastructure assets, regardless of where they are situated, are monitored and well protected.

1 GrantThorton, Top cyber themes for financial services in 2024, March 20, 2024

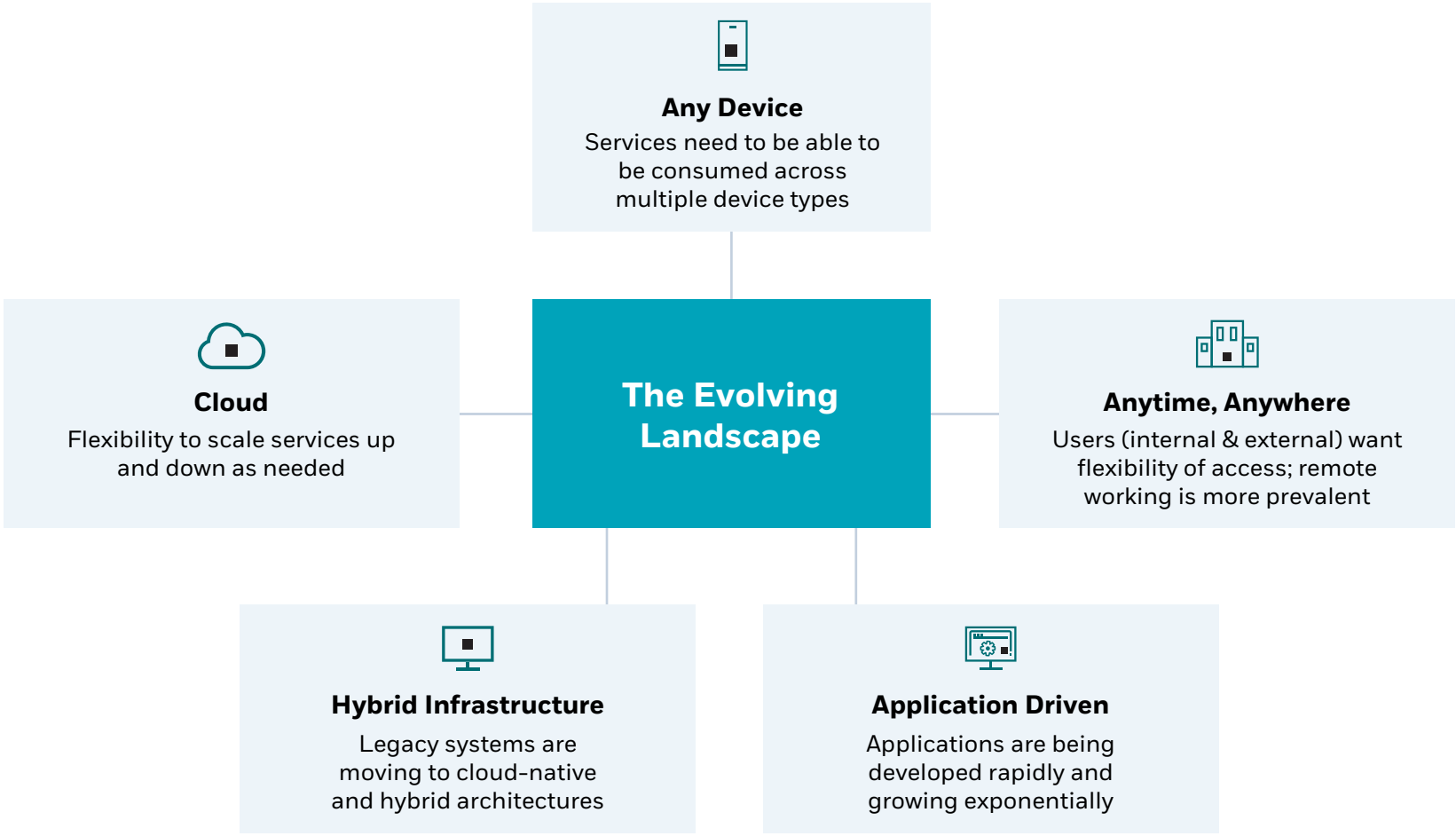


Figure 1: Dispersed interconnecting systems creates an expanded attack surface

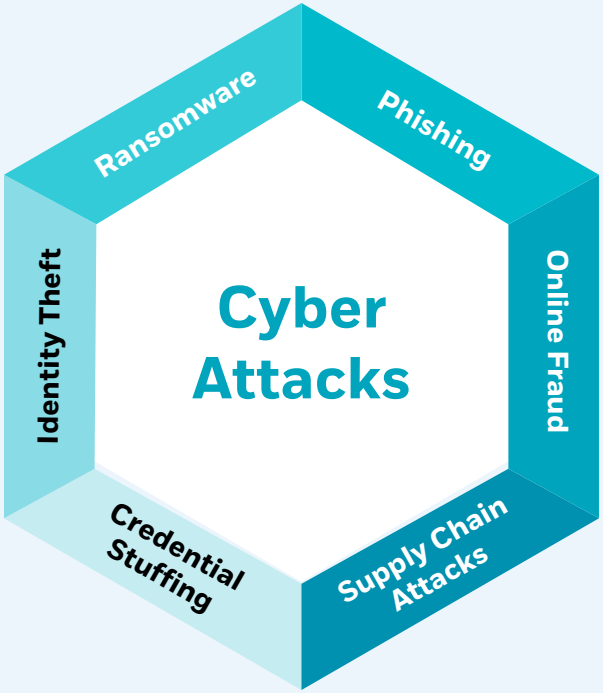
To achieve this end, effective security operations including scalable and real-time security monitoring, actionable threat intelligence capabilities, threat-centric vulnerability management, and agile detection and response all play an important role in reducing cyber risk.

The SOC Is Key To Consumer Trust

The Security Operation Center (SOC) is playing an increasingly important role in reducing the impact of an incident and consequently determining the success or failure of a business.

The most common types of cyber threats targeting the Financial Services industry such as ransomware, credential stuffing, supply chain attacks, identity theft, online fraud and phishing are a daily occurrence. Therefore, the SOC team needs to be vigilant 24/7 and understand the key detection and response times it needs to meet to stay within their defined window of acceptable risk.

The need to maintain confidence and trust is a critical consideration for potential customers and will be carefully evaluated by anyone wanting to do business with you. Cyber threats – whether direct network attacks, or disinformation being purposely disseminated - undermine trust.



In the FS industry, proactive security operations that implement industry best practices will provide an organization with a competitive edge.

More than that – it can be a driver in your organization's continued growth.

Four Ways To Augment Your Soc

Whether your customers are other businesses, end consumers, intermediaries or others – a proactive security practice is viewed as a crucial aspect of any FS organization. But achieving this can be difficult given limited resources, shortage of skills, overburdened teams and inability to monitor diverse environments.

There are four key areas that should be considered to sustainably augment your current SOC capabilities and ultimately improve your security posture:

Adopting a Hybrid Resourcing Model

Streamlining Operations and Improving Efficiency of Human Analysts

Improving Visibility of Threats and Vulnerabilities

Managing Risk Through Personalized Use Cases

Let's have a closer look at how each of these could be applied:

1 Adopting A Hybrid Resourcing Model

According to a recent report,[2] the average cost of cyberattacks has been ballooning. Respondents to the survey indicated they were spending about $4.88 M per data breach on average, a 10% increase over last year and the highest total in history.

Yet, despite the critical impact of these attacks, organizations across all industries and sectors agree that they are suffering from a severe lack of resources. The cyber security skills gap is getting worse in many markets, and the human resources and financial investments necessary for effective risk management are increasing.

So, how do you leverage your resources optimally – ensuring your team is spending its time on high impact tasks? And how do you augment your resources with the right skills from a third-party or outsource specific time-consuming operations without losing control or visibility?

Scenario 1

The Problem: Let's say that there is an FS company that relies heavily on the services of a Managed Detection & Response (MDR) provider to monitor their network for suspicious activity and escalate priority incidents to your internal SOC. The company is particularly concerned about threats that frequently target the FS industry, such as the Cl0p ransomware gang – a particular group that can carry out significant attacks and is capable of evading detection if a SOC does not have clear transparency into its' operations.

The security provider working with this company augments the organization's in-house capabilities. However, the SLAs that the MDR team provides do not support fast enough responses. Moreover, the services that the MDR provider delivers are "black box" and do not allow the company's in-house team to be engaged in what's going on.

The Solution: In this scenario, it's important to rethink your current approach to outsourcing security. The company might want to consider adopting a hybrid SOC model in which the resources of the MDR provider sit alongside those of the company – both in terms of day-to-day operational support and in terms of governance.

The average data breach cost

$4.88M

per breach

2 IBM, Cost of a Data Breach Report, 2024

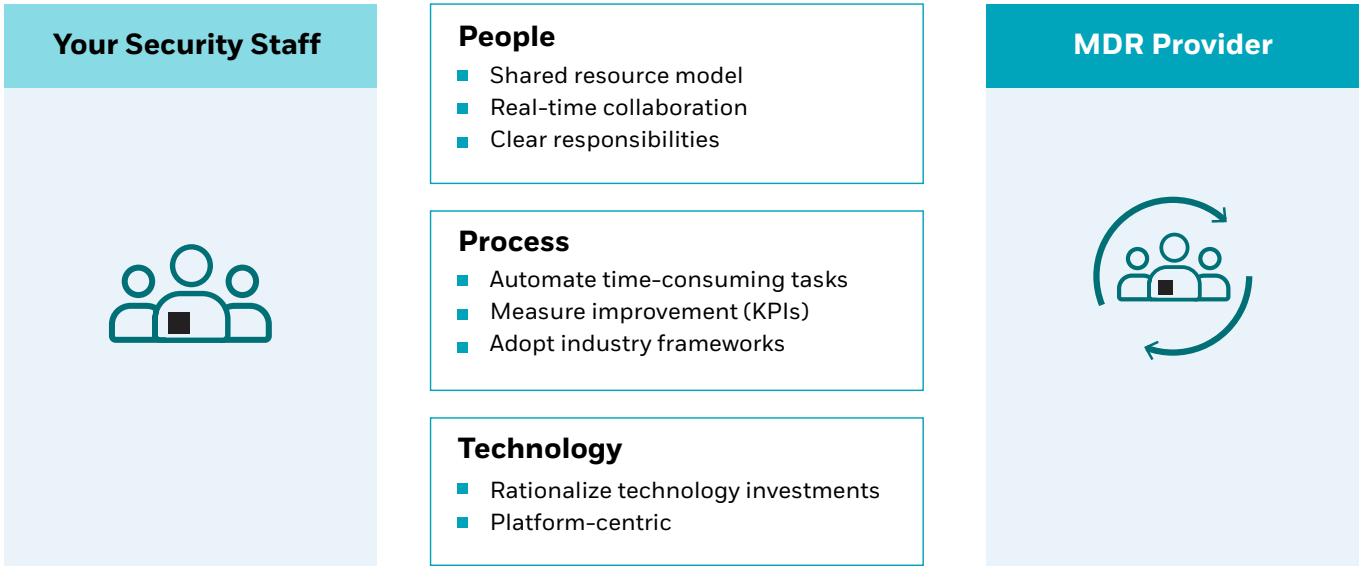


Figure 2: A hybrid engagement model

Companies should ensure that they are getting continuous transparency into their security operations, so they continue to see exactly what is being done by the outsourced team at all times.

In this type of arrangement, companies should ensure that they are getting continuous transparency into their security operations, so they continue to see exactly what is being done by the outsourced team at all times.

If they are working with a more advanced MDR provider that is platform-centric, the company would also be likely to gain increased visibility with a transparent approach of operations that leverages their providers investments in automation, orchestration, and threat intelligence. They might also provide features that allow analysts and internal stakeholders to utilize AI data tools, chatbots, and collaborative interfaces to communicate in real time. These abilities have a huge impact in shortening incident handling time.

In terms of governance, adopting a Hybrid SOC model would ensure accountability is shared and expectations are met across the life of a project.

This approach facilitates collaboration between the company and provider's stakeholders through a committee structure at the technical, operational and executive level – with the provider bringing across key stakeholders to act as an extension of their organization such as a SOC lead, service delivery managers, security architects, customer success managers and security engineers.

In terms of the SOC architecture, a hybrid model would also improve flexibility in resource allocation and help fill gaps where needed, while making the most out of existing resources. For example, the company's SOC might completely outsource security monitoring and use case development to the provider but could then work alongside their level 2 (incident responders) and level 3 (threat hunters) team to support incident response and forensics activities.

2 Improving Visibility Into Threats and Vulnerabilities

Organizations continue to seek and adopt innovative solutions in order to achieve and maintain market leader status.

The use of innovative technologies can also create a complex infrastructure and, invariably, these changes lead to new kinds of cyber risk. Therefore, it's crucial to put processes in place that allow you to successfully monitor multiple environments in real-time and focus your efforts on threats that matter to the business. Basic questions need to be addressed such as:

- How do you maintain full visibility into both on-premises, cloud-native, and distributed environments?
- With so much data available, how do you prioritize security activities?
- How do you know where to invest time, effort, and financial resources?

Bottom line: With a plethora of new technologies being implemented – and the attack surface so vast – today's IT ecosystem demands simplification, in order to be effective.

> **In the financial services industry, being interconnected is essential - but it also represents new risks, such as greater supply chain threats and new software vulnerabilities.**

Scenario 1

The Problem: Let's say a particular FS company is unable to provide effective monitoring of threats or carry out timely response actions. The company's SOC team is overwhelmed by the amount of data being generated by systems for banking activities, ATMs, online transactions, customer profiling, and more.

The company is concerned about ransomware attacks that target corporate computer networks, encrypt found files, and demand that a cryptocurrency payment is made in order to regain access to the encrypted data. These ransomware techniques, like those utilized by Cl0p, are likely to be used for multiple, multi-layered extortion attempts into the company network.

The company's SOC feels that the sheer quantity of information prevents them from making well-informed decisions that can enhance the organization's security posture. Their historic investments in multiple security tools are creating too many alerts to identify the proverbial "needle in the haystack."

The Solution: With the disparate and sensitive nature of these assets, it would be best to implement a security monitoring infrastructure that can scale and handle large volumes of data without requiring additional infrastructure investment. The core components of this would include:

- A scalable data collection and normalization capability
- Cloud-native Security Information and Event Management (SIEM) and security data lake
- An intelligent data management layer that filters and tags data before it is sent to the SIEM
- Enrichment sources such as vulnerability intelligence, threat intelligence, user information and network topology context

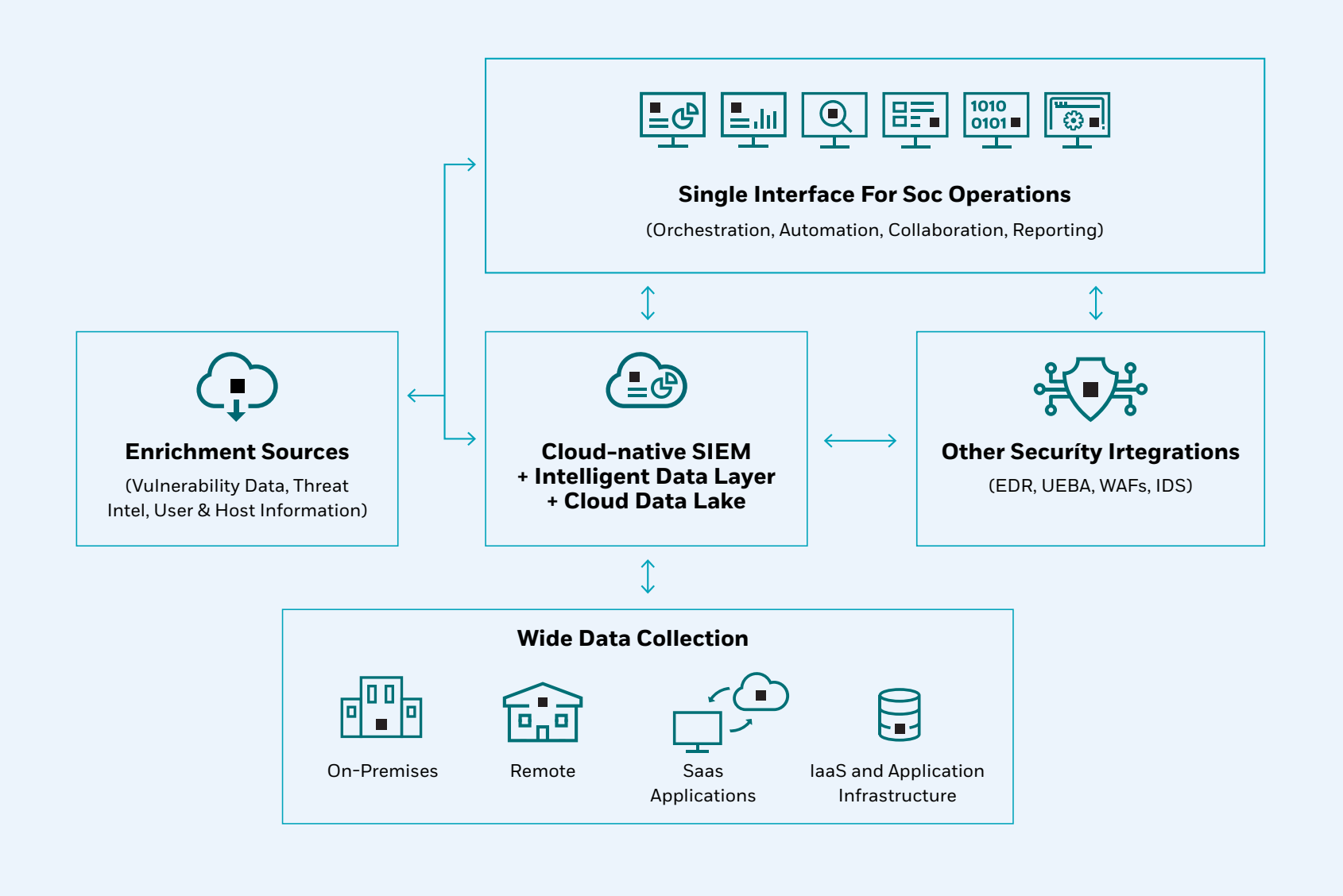
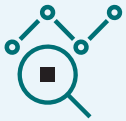


Figure 3: Modernized security monitoring infrastructure that can handle large volumes of data from different sources

Depending on the company's specific objectives, an approach to cyber security of this nature could cover all or part of the following:



Discovery – Carrying out continuous collection and aggregation of a wide net of data, including vulnerability data, patch data, asset groupings, CMDB data, security controls and threat intelligence. It is vital to bring this data collection as close as possible to real-time, continuous scanning to avoid missed information.

Prioritization – Utilizing an intelligence data layer to filter through large volumes of data can help security teams prioritize alerts. Prioritizing data ingestion with tags and filters mapped against threat intelligence allows you to go from having a list of millions of known vulnerabilities to focusing on a more manageable list – i.e., in the dozens, not the millions.

Simulation – Conducting validation to understand the attacker path. A simulated attack tests if the controls that have been put into place are configured correctly. This is often where new vulnerabilities emerge, as new attack techniques continue to outgrow security updates.

Remediation – Mitigating critical risks by arming both IT, IT Security, and the SOC with multiple remediation options. These include reinforcing policies, upgrading systems, isolating machines, and optimizing response plans.

The company would gain an additional advantage by adopting an ongoing, threat-centric approach to vulnerability management. Given the persistent threats of credential fraud and data exfiltration attacks targeting the financial services sector, vulnerabilities will inevitably be targeted.

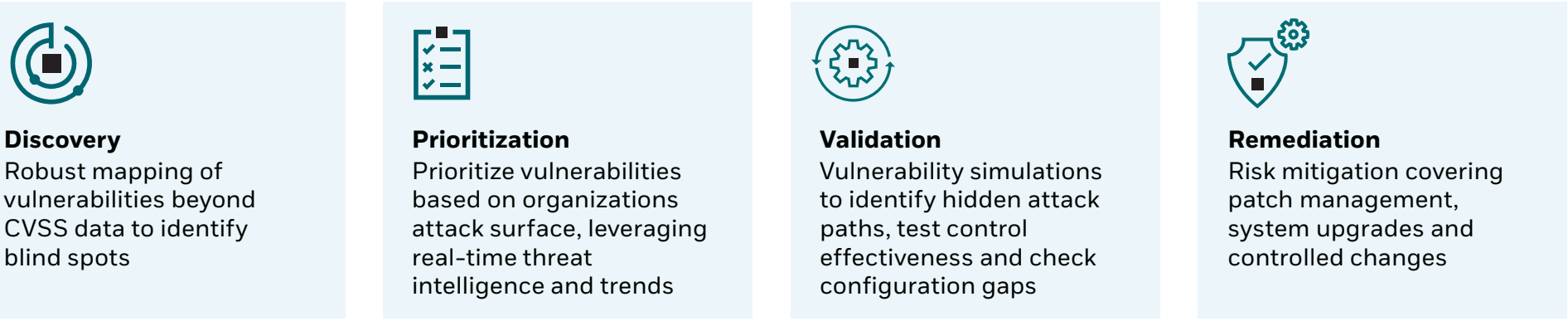


Figure 4: A threat-centric approach to vulnerability management

The identification, prioritization, and management of vulnerability risks can be time consuming and inefficient. But by adopting a threat-centric approach that ensures continuous visibility and centralized control, you can regain the ability to make swift decisions regarding incident response and management. Moreover, leveraging the capabilities of AI tools working as an inherent part of security operations would automatically provide analysts with threat intelligence and vulnerability-related context to alerts. These AI tools would also handle some of the activities usually conducted by human analysts, such as enriching event data, automatically handling low-risk alerts, and responding to analysts' requests with actionable information and event summaries.

By adopting a threat-centric approach that ensures continuous visibility and centralized control, you can regain the ability to make swift decisions regarding incident response and management.

3 Streamlining Operations & Improving Efficiency Of Human Analysts

With the skills gap looming and in-house teams overworked, the way forward in a highly challenging ecosystem involves implementing a combination of artificial intelligence and human intelligence.

A combination of AI and human intelligence provides support for all aspects of security, from threat intelligence to vulnerability management, and reduces the risk of cyber incidents to provide overall strength in depth.

> **Identifying which types of tasks can be accomplished faster and better with AI tools and which tasks are best left to humans – can help an organization deliver more efficient security operations.**

Scenario 3

The Problem: Let's say that a particular FS company needs to effectively handle a variety of supply chain risks but, the company finds that its security operations team is facing a number of increasingly problematic and time-consuming issues that is preventing them from responding to alerts of supply chain compromises. Too much time is spent carrying out manual tasks such as monitoring alerts, creating correlation rules, enriching alerts, and documenting and configuring playbooks – there simply aren't enough hours in the day. Moreover, time to respond is not fast enough, and this increases the organization's risk.

The Solution: The company could consider increasing the speed and efficiency of security operations and lightening the workload of its team by integrating greater automation into its work processes.

For example, leveraging the support of integrated AI tools that can support the work of your human analysts could potentially automate up to 90% of L1 SOC activities including alert enrichment, extracting key observables, automatically handling low-risk incidents, investigation actions, and report generation.

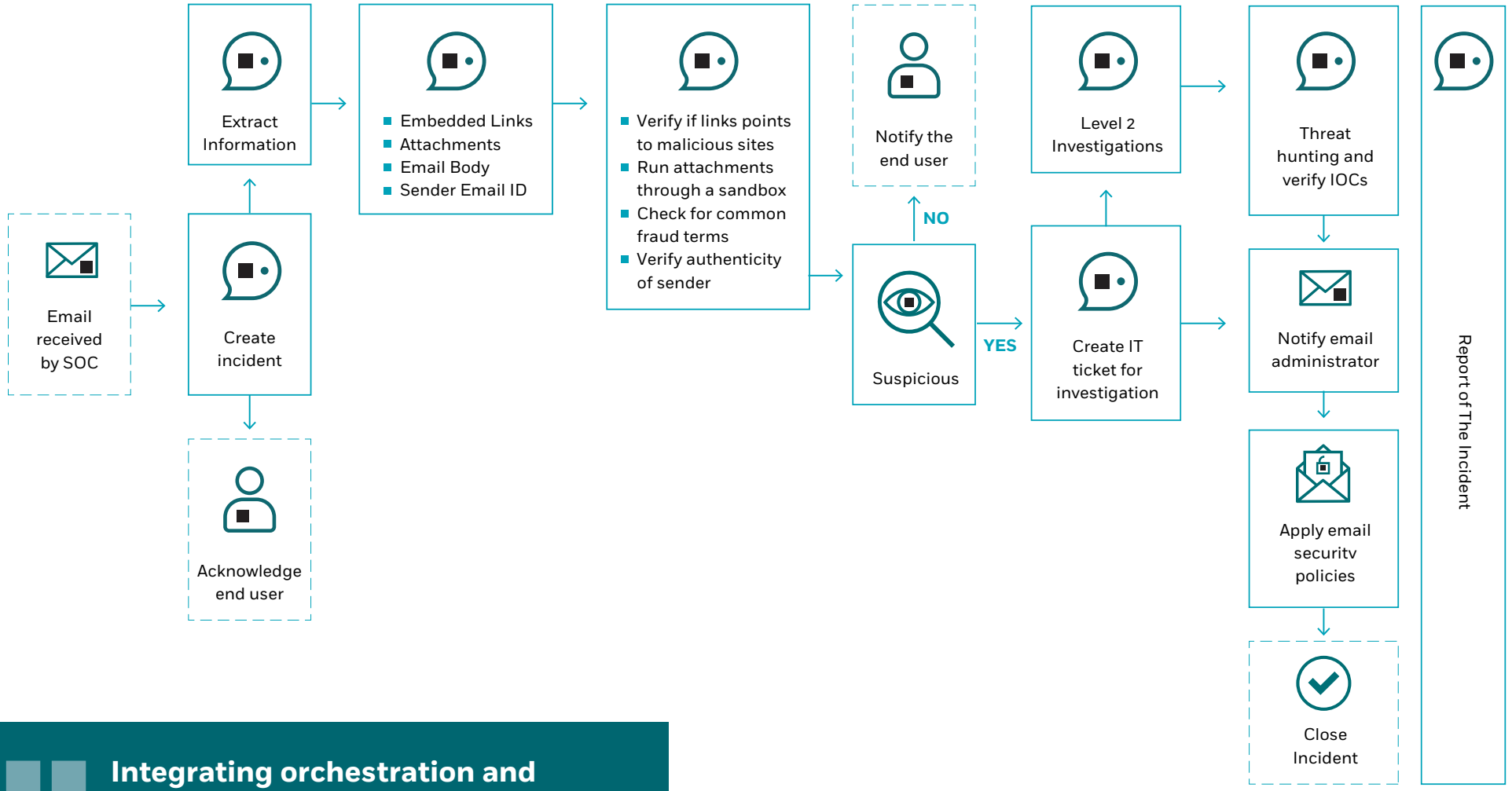


Figure 5: Example of a phishing playbook using a virtual analyst to automate key steps

Integrating orchestration and automation delivered by a virtual analyst, the company's security analysts would be able to make more informed decisions and fetch data or ask requests in a timely manner.

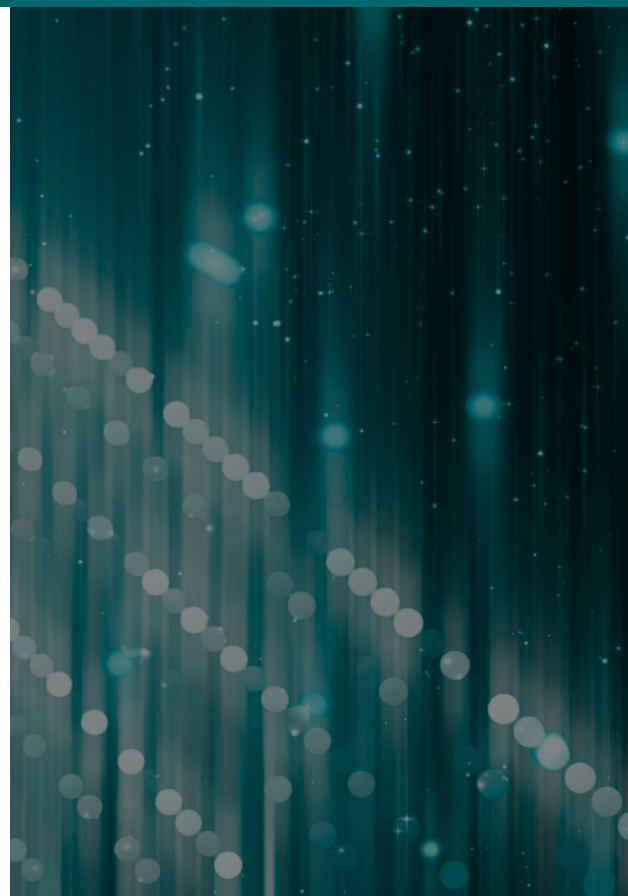
This would lead to significantly reduced detection & response dwell times and provide context for the SOC team so that high-value human resources can focus on high priority incidents.

By maximizing automations with AI tools, the company's security analysts would be able to make more informed decisions and focus in on high-risk threats. In addition, this would free up time needed by the team to build more efficient operations.

An MDR provider that already has a strong foothold in the FS industry and already invested in these capabilities could provide added value, helping develop AI-powered playbooks that include actions customized to specific threats, such as the LockBit Ransomware as a Service (RaaS) group, that is notoriously targeting FS organizations. The MDR provider could assist in mapping to industry frameworks such as MITRE ATT&CK – and in optimizing the organization's Incident Response (IR) processes and procedures.

Playbooks can be maintained by the MDR provider's security experts and continuously updated to align with changing threat vectors facing the FS industry and improve the organizations' response capabilities. These playbooks could be partially or fully automated and function as an integrated aspect of the company's security operations to facilitate the fastest possible response.

Playbooks can be maintained by the MDR provider and continuously updated to align with changing threat vectors



4 Managing Risk Through Use Cases

Attacking risk management “head on” involves first identifying the nature of the problem – then exploring ways to address it. In other words, getting serious about risk management means first asking some basic questions: Where do your critical assets reside? Who is trying to attack these assets? What is the best means of protection – particularly, given the extent of dispersal on the network?

The MITRE ATT&CK framework – a powerful foundation for developing threat models – can be used to map clearly where an organization is protected, and where it’s vulnerable, according to the matrix.

Once these gaps have been defined, reducing and managing risk requires making some strategic decisions.

Scenario 4

The Problem: Let’s say that an organization is concerned about data theft and online fraud and therefore invests money in vulnerability scanning tools, fraud detection technology, and periodic penetration tests. But it still lacks the agility it needs to detect and respond to this type of threat within a window of acceptable loss to the business.

The Solution: This company should start by carrying out a baseline assessment of their detection and response gaps and mapping against the MITRE ATT&CK matrix. By leveraging this knowledgebase

in an effective way, they can create a heatmap of the attacker techniques and tactics used for committing online fraud and data theft such as spear-phishing or brute force. They can then prioritize detection and response requirements that allow them to mitigate those specific attack scenarios as quickly and efficiently as possible.

Carrying out this exercise should not be a one-time initiative but a continuous process, as attackers are always developing new ways to achieve the same goal, which means security teams should be continuously optimizing their detection and response processes.

However, continuously optimizing detection and response capabilities can be a costly process if you don't have the right resources in place. This process typically requires an Agile use case development team.

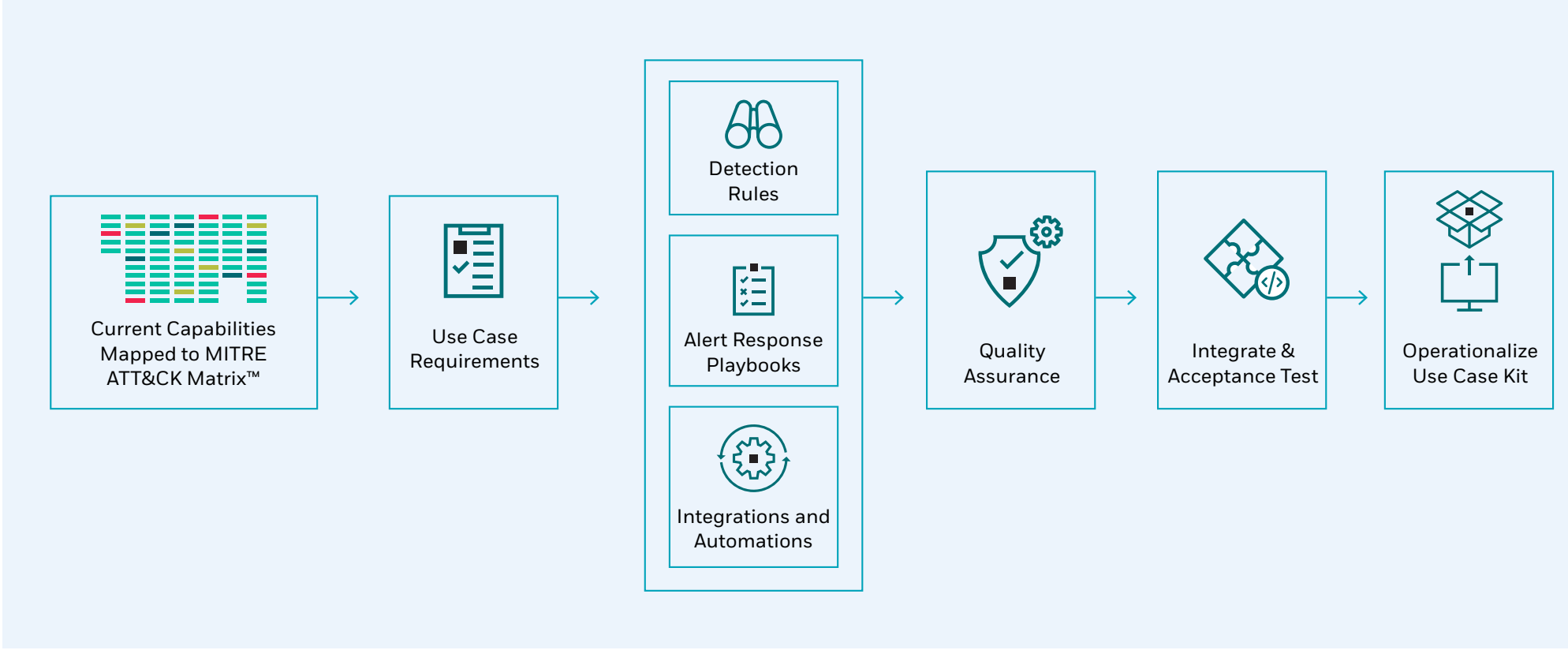
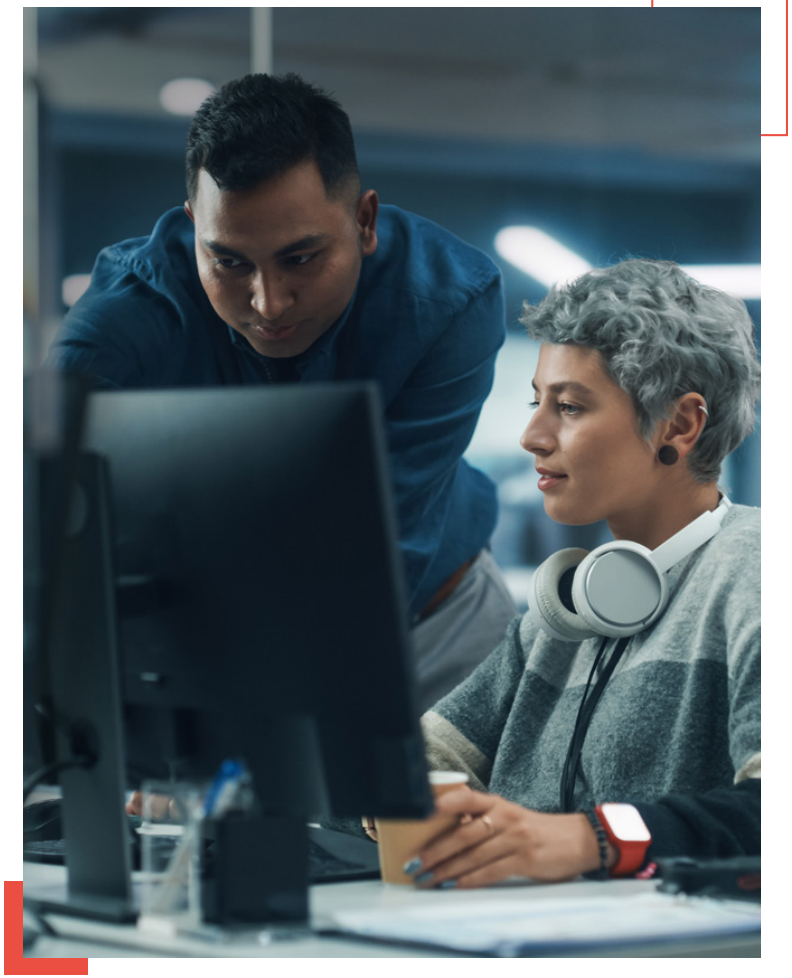


Figure 6: An agile process for developing and operationalizing use case kits

An Agile development supply chain involves the following steps:

- Collecting key business risk and threat intelligence inputs
- Developing detection rules
- Developing automated/manual response playbooks
- Configuring integrations with systems and security technologies (firewalls, SIEMs, enrichment sources, etc.)
- Building automations and training AI tools to speed up repetitive processes
- Conducting quality assurance testing
- Deploying these use cases into operations

Each of these steps requires a range of resources such as technology integrations and access to the right skilled experts such as rule developers, incident response specialists, and playbook automation engineers. If the company opts to work with an advanced MDR provider, the provider's security team could carry out the process on their behalf and automatically compile and deploy use case kits – a package consisting of detection rules, response playbooks, integrations, and automations with security technologies that is deployed in their environment to mitigate this specific type of attack. This would give the organization the ability to stay ahead of the changing threat landscape and allow it to focus its time and effort on responding to the most important threats.



2 IBM, Cost of a Data Breach Report, 2024

Conclusion

The traditional infrastructure of the FS industry has been disrupted by the rapid growth and adoption of a range of innovative technologies – from the cloud and mobile to payment platforms and application-driven environments – which have both diversified and dispersed organizational assets and data.

Maintaining customers' trust is more important today than ever before. The FS industry is faced with a wide variety of threats, including supply chain risks, credential and identity theft, data theft, and specific threat actors such as the Cl0p ransomware group, LockBit RaaS group, BlackCat/ALPHV, and more.

In this complex and uncertain reality, organizations looking to drive business growth are encouraged to take the necessary steps to enhance their security posture – and this means augmenting the capabilities of the SOC by leveraging human resources optimally, simplifying cyber security processes, augmenting capabilities with automation and AI, and reducing and managing risk through effective cyber security decision- making and implementation.

Customers – be they businesses or consumers – value organizations with a strong security culture and are attracted to those players in the FS industry that make this a priority.

2 IBM, Cost of a Data Breach Report, 2024

CyberProof®
A UST Company

About CyberProof

Fortify your enterprise with cloud security transformation. CyberProof, a UST company, helps enterprises migrate to cloud-native security operations with advanced Managed Detection & Response services that allow you to protect, detect, and respond to new and existing cyber threats faster and more effectively. Our team of nation-state trained experts together with our AI virtual assistant SeeMo challenge the status quo in the cybersecurity industry with a risk-based approach that helps mitigate the potential threat to your business. Our mission is to empower your organization to anticipate, adapt, and swiftly counter cyber threats – with our global security operations centers, in-depth expertise, and a portfolio of services including Tailored Threat Intelligence, Advanced Threat Hunting, Use Case Management, and more.

For more information, visit www.cyberproof.com.

Locations

Barcelona | California | London | Singapore | Tel Aviv | Trivandrum

cyberproof.com