CyberProof®
A UST Company

A buyer's guide to modernizing your security operations center

An eBook from CyberProof and Microsoft

Contents

Introduction

Having a security operations center (SOC) is no longer a privilege of large organizations. With the growing number of cyberattacks and a changing technology landscape, all companies are now beginning to understand the risks and consequences of cyberattacks. All companies, irrespective of their size, that handle critical client data and payment details, or are adopting digital transformation, are also considering building centralized security operations.

Many current solutions are not architected for today's – or tomorrow's – demands:

- Legacy on-premises security tools require powerful hardware and extensive maintenance that make them expensive to operate.
- Storage and compute needs to increase dramatically during an incident, which is difficult for an on-prem. footprint to accommodate.
- The move to the cloud has enabled a new degree of enterprise scale-out, and with the explosion of cloud-born data, legacy Security Information and Event Management (SIEM) platforms and security tools are less and less able to cope with the demand.
- IT and OT are on a path toward convergence; old systems that supported industrial control processes (and other specialized applications) are quickly being replaced. Consequently, this presents new vulnerabilities and higher levels of risk.

Let's have a more in-depth look at some of what SOCs are struggling with today, and how a Smarter SOC would address these issues.

Addressing common SOC challenges

To help you reduce the risk of a cyber incident in the today's fast-paced, complex IT environment, it's important to optimize your security operations strategy in terms of the people, processes, and technologies that can help you achieve your goals.

People

According to a 2020 survey by the Ponemon Institute, for an average organization, three SOC analysts will be fired or resign in one year. The same report also revealed that on average, nearly eight months is required to find a new SOC analyst (3.5 months) and train him or her (3.8 months). This shows why organizations across all industries and sectors agree that they are suffering from a severe lack of resources. The cybersecurity skills gap is getting worse in many markets, and the human resources and financial investment necessary for effective risk management are increasing. In addition, SOC teams have to face the day-to-day challenges that affect the productivity of security operations:

- Alert fatigue caused by a high volume of noisy alerts
- Investigations that are complex and time consuming
- Security skills are in short supply
- Lack of standardization across business units and regions

To alleviate these challenges, organizations often look to outsource SOC services to a Managed Dectection & Response (MDR) provider. However, the services provided are often "black box" and do not allow the company's in-house team to have visibility into operations. They may get tied into a standardized engagement driven by Service Level Agreements (SLAs) that allow for limited flexibility.

Adopt a hybrid engagement model to facilitate more effective collaboration between your team and those of a third-party service provider.

Security operations should be transparent between both insourced and outsourced teams, i.e., a service provider should assist and augment your work but without requiring you to relinquish knowledge or control. A hybrid engagement model enables you to bring the resources of the MDR provider alongside those of the client's teams – both in terms of day-to-day operational support and in terms of governance. In this model, the client is able to communicate with the provider's remote analysts in real time so they get continuous transparency into the provider's operations, allowing them to continue to see exactly what is being carried out by the outsourced team at all times.

This type of model also allows the client to flex which capabilities are fully insourced or fully outsourced or to use a combination of resources, such as augmenting Level 2 teams with specialist capabilities and knowledge in areas such as Incident Handling, Threat Hunting, Threat Intelligence Monitoring, Use Case development, etc. With the threat landscape constantly evolving, it's important to access skills that are agile enough to adapt to these changes.

Process

Without implementing sustainable and effective processes that a team can comfortably maintain, the investments you make in people and technology will only cause more complexity. Adopting processes that are aligned to industry frameworks such as NIST is a good start, but this isn't as simple as using it as a template for your organization. Your business needs tailored processes that fit your architecture and unique goals.

The common challenges to maintaining good processes include:

- High rate of false positives
- Lack of enrichment from internal and external sources
- Sophistication and volume of threats
- Many disconnected products that are hard to view and control

To alleviate these challenges, organizations often look to outsource SOC services to an MDR provider. However, the services provided are often "black box" and do not allow the company's in-house team to have visibility into operations. They may get tied into a standardized engagement driven by Service Level Agreements (SLAs) that allow for limited flexibility.

Continuously improve prevention controls, detection rules, response playbooks, and technology integrations and automations.

While adopting processes that are aligned to industry frameworks such as NIST is a good start, you also need customized processes that fit your organization's architecture and unique goals.
Use cases should be tailored and aligned to meet your organization's needs and targeted risk appetite.

In order to adopt a proactive threat detection approach, organizations can map their threat detection abilities to the MITRE ATT&CK Matrix to create use cases for developing and updating their threat detection rules and automated response. The goal of use cases is to reduce business risk for specific attack scenarios/cyber loss events by developing an Agile Detection and Response process that drives down attack impact by rapidly identifying and mitigating those attacks. The use case detection rules and playbooks developed should be mapped to your threat profile, IT landscape, control gaps, and risk appetite.

Technology

Gone are the days when IT was focused on a bunch of servers and cables, when the architecture was simpler and data sat inside the perimeter on physical servers, desktops, and laptops – and effective security involved monitoring a single firewall and other on-premises systems to obtain data. Today's SOCs are faced with complex challenges that result from:

- **Evolving Attack Surfaces** – SOC teams are faced with complex IT environments caused by the widespread adoption of new systems with new vulnerabilities layered on top of legacy systems.
- **Outdated Monitoring & Analytics** – legacy SIEMs are functioning only as aggregators and don't increase response capabilities, adding cost at every step.
- **Transition to the Cloud** – the adoption of IoT, mobility of users and remote working has increased demand for cloud scalability for a more distributed architecture.
- **Application-Level Insight** – traditional monitoring and analysis approaches aren't built to provide enough insight into threats targeting agile development processes involving containers, serverless networks.

Implement the technologies necessary to provide enrichment in order to detect & respond to threats across your estate.

When building or augmenting your SOC, you should consider incorporating some key technologies to improve enrichment, detection, and response capabilities. Be mindful that evaluating the right technologies requires an extensive time investment and you may save that time by working with a partner who is familiar with the available technologies – and can help you select which offering can best future-proof your defense.

- **Cloud Native SIEM** – Traditional SIEMs have proven to be expensive to deploy, own and operate, often requiring you to commit upfront capacity and incur high cost for infrastructure maintenance and data ingestion. With a cloud-native SIEM, there are no upfront costs; you pay for what you use. It helps you collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds, and incorporates Threat Intel and other sources of enrichment. Reduced management efforts and automatic updates help shift talent to concentrate on value-adding initiatives.
- **Automation and Orchestration** – This enables a birds-eye view across the enterprise, alleviating the stress of increasingly sophisticated attacks, growing volume of alerts, and long resolution time frames. Automation and orchestration capabilities include collection of software solutions and tools that allow organizations to streamline security operations in three key areas: threat and vulnerability management, incident response, and security operations automation.
- **Threat Intelligence** – Threat intelligence is evidence-based knowledge about an existing or emerging threat to assets that can be used to inform decisions regarding the subject's response to that threat. There are 3 levels of Threat Intelligence: Strategic, Operational, and Tactical. Strategic looks at the changes in the broader threat landscape and is primarily aimed at executives. Operational seeks to understand how an organization could be attacked by outlining Tactics, Techniques, and Procedures (TTPs). Tactical covers the details of an attack with the shortest lifespan, such as Indicators of Compromise (IOCs) that are usually fed into the SIEM or firewalls.
- **Vulnerability Management** – Organizations need to build and manage the entire vulnerability management lifecycle covering asset discovery, vulnerability identification, issue prioritization, remediation planning, and risk mitigation along with the entire end-to-end governance. This includes 4 stages: Vulnerability Scanning, Vulnerability Intelligence, Vulnerability Simulations (aligned to the MITRE ATT&CK matrix and Cyber Kill Chain methodologies), and Vulnerability Remediation.
- **Endpoint Detection and Response** – EDR combines real-time continuous monitoring and collection of endpoint data with rule-based, automated analysis and response capabilities. Integrating it with your SOC gives security teams a centralized platform for continuously monitoring endpoints and responding to incidents as they arise, often via automated response.
- **Cyber Deception** – With deception technology, security teams do not need to wait and react to an attack. Instead, they can deploy bait, lures, and decoys such as fake servers and users designed to derail attacks early and throughout the attack lifecycle. These decoys can run in a virtual or real operating system environment and are designed to trick the cybercriminal into thinking they have discovered a way to escalate privileges and steal credentials.

Be sure to work with an MDR provider who has obtained a clear understanding of your ecosystem, to avoid unnecessary expenditure.

You will also want to work with the MDR provider in identifying the best ways to integrate any new technologies – so that you can create a single-pane-of-glass view of security operations for your organization, without additional capital investment.

Building a smarter SOC

Adopting next-generation SOC components enables proactive detection and response and helps your team maintain a detailed action plan, enabling them to respond quickly to an attack.

The SOC should function as a driver of your security program – rather than just responding to incidents in a defensive or reactive process.

The process of implementing a smarter SOC includes the following layers of development:

- **Define Log Collection** - what needs to be included?
- **Tackle to data side** - collection, management and storage
- **Security Analysis** - leveraging the capabilities of a SIEM
- **Implement** orchestration, automation, and collaboration

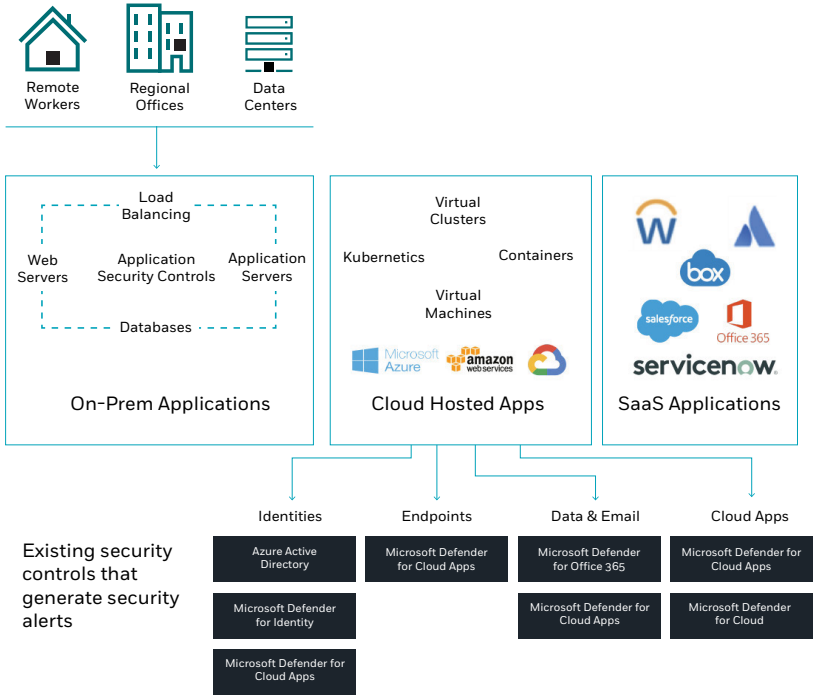
We'll now explore these areas in more detail.

Define log collection – what needs to be included?

Building a Smarter SOC first involves identifying which assets, tools, technologies, and applications need to be integrated.

The log collection layer covers on-prem. applications, cloud-hosted apps, and SaaS applications. It should extend to all of your organization's log sources – including those connected to regional offices, remote workers, and data centers (where relevant).

If you are using components of Microsoft XDR (Extended Detection and Response), also known as Microsoft Defender, the range of existing security controls generating security alerts include identities, endpoints, data, email, collaboration, IoT, OT, cloud infrastructure and cloud applications – all of these data sources must be included in the log collection layer.



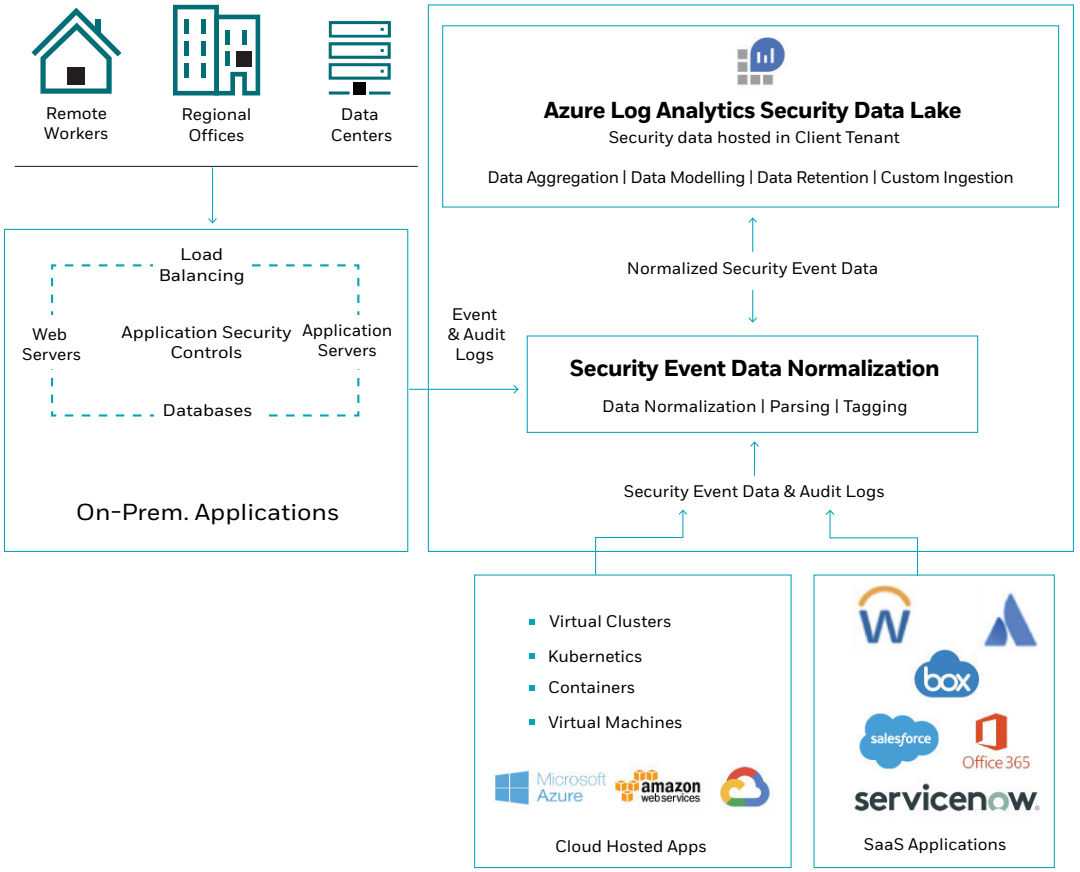
Tackle the data side – collection, management and storage

Once the log collection layer is defined, it becomes possible to implement effective log collection, data management, and data storage.

Finding ways to simplify this process is essential. By using a SIEM native to the cloud, for example, you can gain the advantages of easy collection from cloud sources and auto-scaling.

For some SOCs, part of the data management and storage process involves the ability to parse the data before it goes into a security data lake. Particularly for the enterprise, it might be necessary to look at tagging and filtering data – particularly since the cost implications of using a data security lake include the cost of ingestion and storage.

At CyberProof, we leverage Azure Log Analytics and CyberProof Log Collector (CLC) SaaS technology to pull logs from all sources of data. These include a client's existing Microsoft investments – including on-prem., SaaS, and Microsoft assets – and existing Microsoft security controls that generate alerts across identities, endpoints, data and email, and cloud apps.

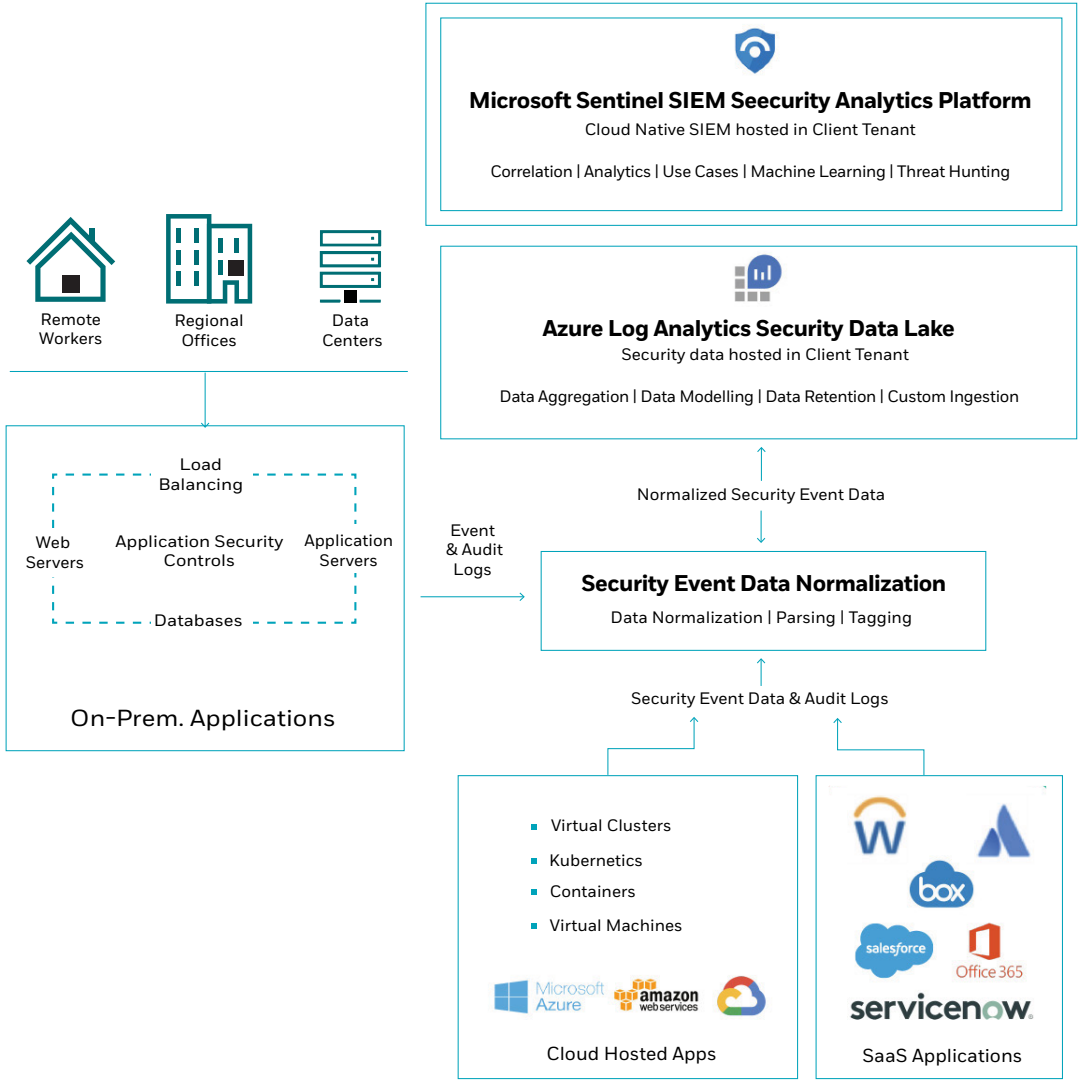


Security analysis – leveraging the capabilities of a SIEM

Conduct analytics using the Security Information and Event Management (SIEM), which utilizes detection rules in identifying anomalies while also monitoring whether your log sources are operating correctly.

The SIEM's activity is crucial in reducing time to acknowledge and remediate to respond – making sure that attackers do not operate freely until remediated. A well-tuned SIEM can help the SOC team catch real detections and avoid wasting time on false positives.

Organizations are increasingly adopting solutions such as Microsoft Sentinel – a cloud-native SIEM that supplies correlation, analytics rules, and filtering of massive volumes of events to obtain high-context alerts. Microsoft Sentinel uses Machine Learning to proactively find anomalies hidden within acceptable user behavior and generate alerts. In addition, it includes the use of Azure Logic Apps to build playbooks and connectors, enabling you to automate workflows with other Microsoft services and other tools such as ticketing systems or instant messengers.



Implement orchestration, automation, & collaboration

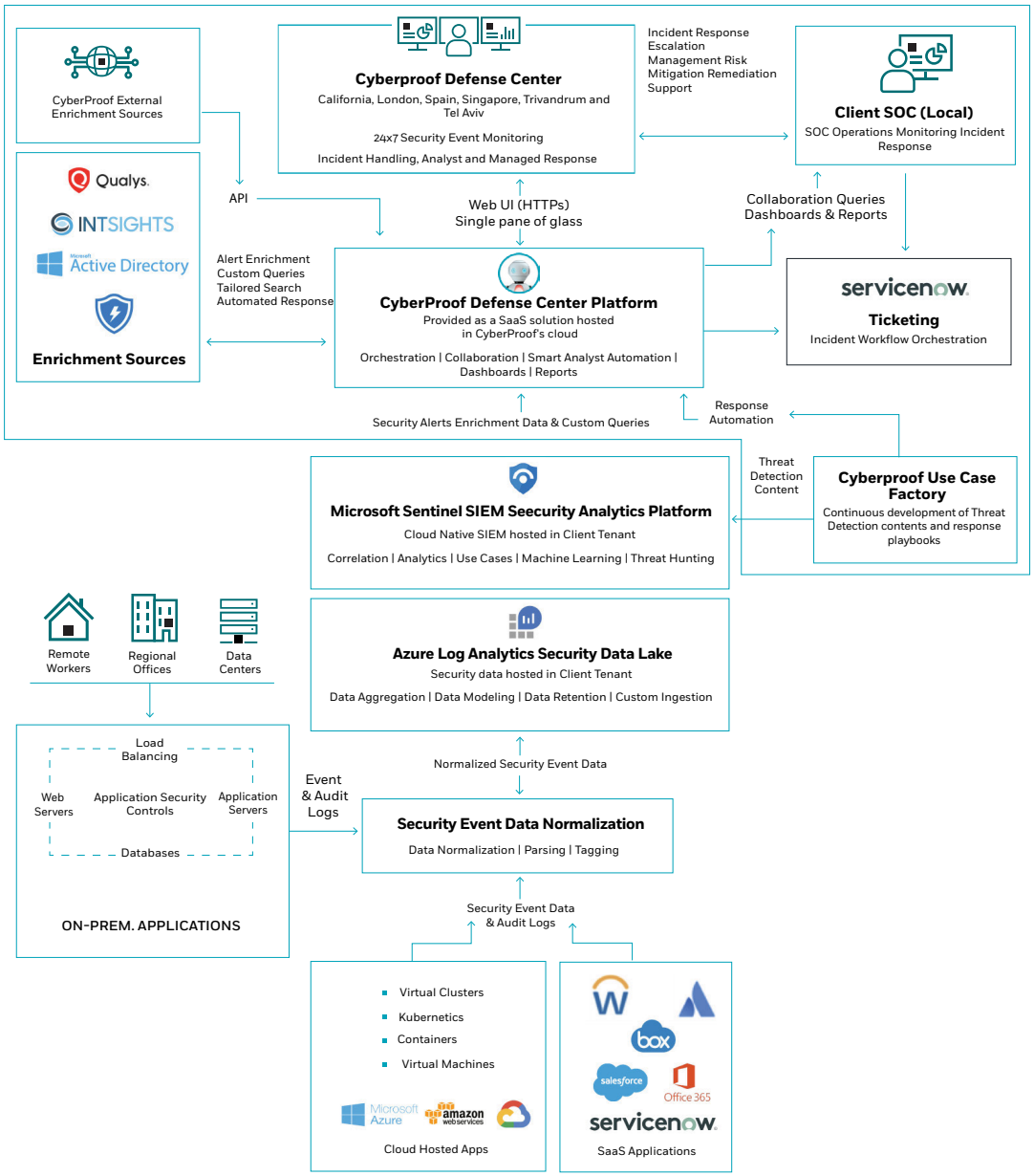
Greater adoption of orchestration, automation, and collaboration provides a key element to productivity.

The push toward orchestration and automation is partly due to the need to alleviate global staff shortages. We simply don't have enough cyber experts to meet the growing need. Organizations are looking for a leaner team - particularly if their SOC analysts, wanting to move up in their careers, are interested in doing more of the higher level work such as threat hunting and level 2 or level 3 investigation.

Greater orchestration and automation is also important due to the continued evolution of threats. It allows the SOC to work faster in enabling incident resolution and facilitates efficiency by supporting a centralized view of threat intelligence through a single pane of glass.

Collaboration features such as ChatOps that allow real-time communication with both internal and external stakeholders also help to speed up remediation of critical incidents.

At CyberProof, we provide clients with access to our CyberProof Defense Center Platform (CDC) – a service delivery platform that provides clients with access to our IP in areas such as automation, orchestration, collaboration, and AI, but "as a service." As part of the platform, our virtual analyst, SeeMo, takes much of the manual strain away from analysts by automating routine SOC tasks such as alert triage, event enrichment, investigation, issue containment, and execution of response playbooks.

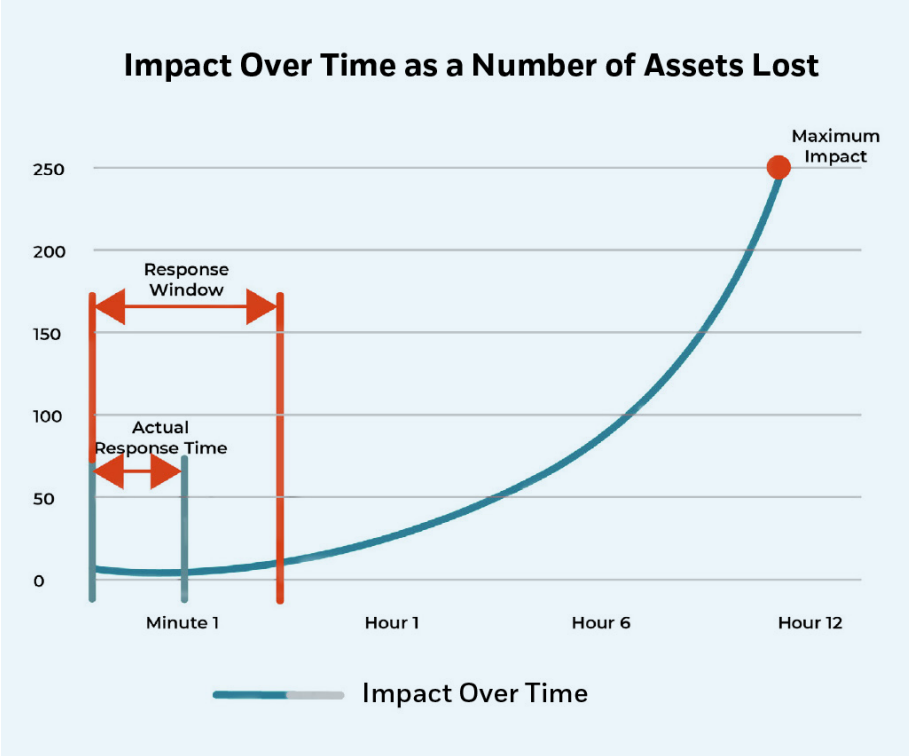


Metrics and measurement of SOC success

Ensuring the success of your SOC and business safety requires continuous measurements of its performance. Here are some of the key metrics to check:

- **Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)** – By putting into place AI tools, you can effectively cut MTTD and MTTR, lowering your organization's degree of risk.
- **Time to mitigate** – Reduce the time necessary to remove an immediate risk to the business. This helps you measure how quickly your team can stop or slow down an active threat.
- **Reduction in false positives** – If a SOC has well-tuned detection rules and use cases, you should see a drop in the number of false positives over time.
- **SOC team productivity** – Leveraging orchestration & automation and utilizing enrichment sources allows you to shrink the time to triage, qualify an incident, and recover from the incident.
- **Number of use cases, playbooks, and detection rules** – Lessons learned during incident response and threat hunting processes should be shared with the use case team, who can fix any of the security gaps that were identified. This either prevents the recurrence of incidents or, alternatively, ensures that if the incident recurs, detection and response happen automatically.

For every attack scenario, there is an impact curve that defines the amount of loss over time. By defining the response window – the minimum period after which the impact of the cyber attack becomes exponentially greater – you can lessen the risk associated with a cyber attack. Because the magnitude of loss is associated with how long it takes to detect and respond, speed and agility are crucial.



Industry Trends

Cloud-native security analytics

Security operations is a continuous battle for relevance, resources, speed of detection, and response.

Therefore, it's preferable to have all of your security talents as productive as possible and focused on added-value tasks. Deploying and maintaining a classic SIEM infrastructure is probably not one of those. Let's look at some of the benefits of cloud-native SIEM.

Cost reduction
Leveraging a cloud-native SIEM saves you from installing and maintaining a physical infrastructure. From a financial perspective, it also allows you to move from capital expenditure to operational expenditure where you pay only for what you use. With resource reservations, you can leverage predictable pricing, and with cloud elasticity you can adapt and manage your costs from month to month.

Scalability and elasticity
A cloud-native SIEM can easily handle the increased volumes of logs coming from your expanding perimeter, including cloud-generated data which can be ingested close to where they were generated. Storage and computing resources are adapted automatically for you and scale as your business scales.

Faster deployment and evergreen
It's much faster to deploy a cloud-native SIEM than a traditional on-premises one. New services are provisioned quicker and the latest technologies are made available automatically enabling you to keep an up to date, state-of-the-art solution.

Community benefits
The provider of your cloud-native SIEM has unique optics about the threats that benefit all of their clients by mutualizing the learnings about the current threat landscape. Some analytics rules or behavior analytics can be updated for all participants to benefit and learn from prior attack situations, without having to personally endure them.

Automation & orchestration

There are so many aspects of SOC operations that computers can do better than humans. But, the concept of creativity – the ability to think laterally, find innovative solutions to new kinds of attacks, and the ability to make thoughtful decisions - remains uniquely human.

The Advent of Smart Bots in the SOC

In an increasingly automated SOC, the interaction between humans and bots (enabled and run by playbooks) needs to be carefully unified. This crucial area of collaboration should be defined in playbooks and in the development of approaches based on Security Orchestration, Automation & Response (SOAR) to SOC operations that require new workflows and use cases.

CyberProof's research shows that 95–98% of SOC alert triage can be automated, reducing human effort. But the remaining alerts do need human support.

For every alert received in the SOC, a number of initial triage activities can be carried out by the smart bot. At the point where a smart bot is not capable of continuing the response activities, the alert must be handed over to human security analysts.

Leveraging automated capabilities allows a security team to accelerate its response and handle emerging threats fast enough to assure the resilience of its systems.

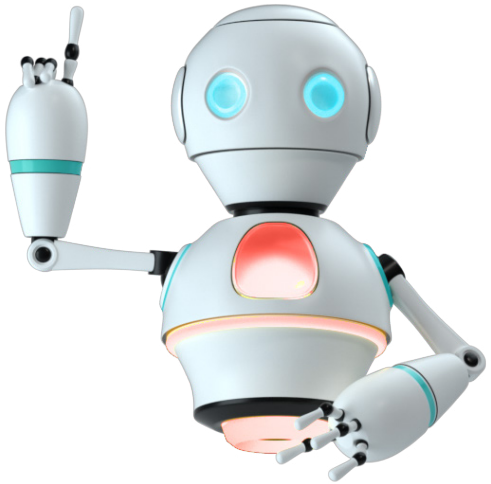
The usage of smart bots means a SOC can automate tasks such as: enriching event data, proactively querying external sources, responding to analysts' requests by providing contextualized and actionable information, automatically creating incidents without human intervention (based on collation and context), and automatically executing non-intrusive steps in digitized playbooks.

By automating some of the SOC's tier 1 & 2 activities, smart bots can help reduce false positives and shrink dwell time, i.e., the period beginning when a threat actor has undetected access to a network and ending when a threat is completely removed.

Use Cases and Playbooks

To constantly improve detection abilities and stay up to date with emerging threats, SOCs should continuously design and build robust use cases and playbooks. Every organization needs tailor-made use cases, which should reflect the organization's unique requirements and threat profile, the threat landscape based on its industry vertical, the types of assets owned, its operating regions, applications and services used, and more.

Workflow integration is critical to ensuring that alerts are prioritized and properly escalated for timely remediation. Use cases help in enriching security alerts for better contextualization, developing incident response playbooks and incident response workflows, and automating responses by enabling integration with network and security controls.



Conclusion

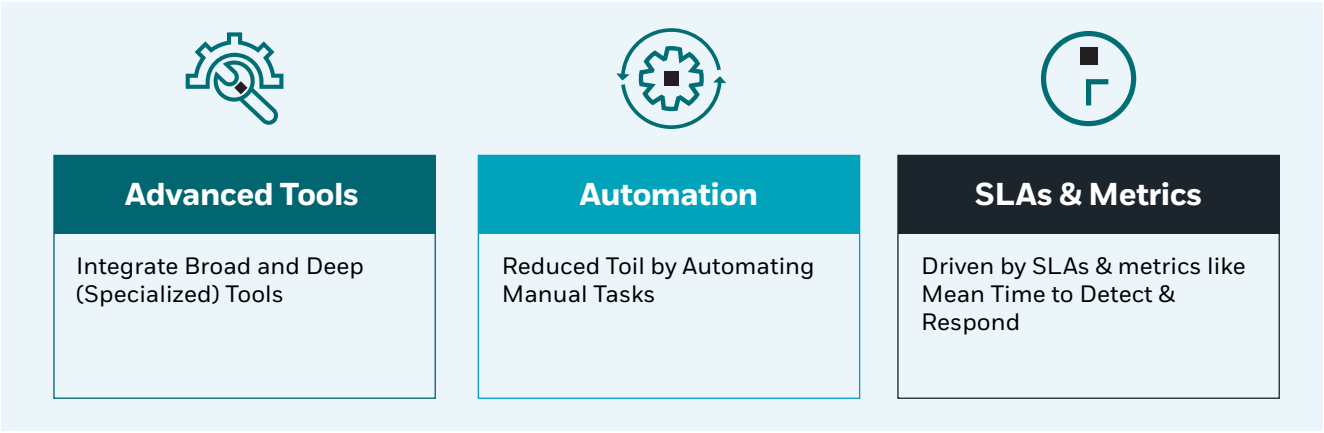
Gaining greater cybersecurity efficiency through the implementation of a Smarter SOC boils down to three keys attributes:

- **Visibility into what matters** – How do I obtain continuous visibility of the threats that are most significant?
- **Collaboration with the right skills, at the right time** – How do I access the expertise I need to solve complex issues quickly?
- **Continuous improvement** – How do I future-proof my defenses?

For companies that do not want to build an in-house, 24x7 SOC, an advanced MDR provider like CyberProof can provide these capabilities. MDR providers can build and manage the SOC and add next-generation SOC components to help you mature your security processes.

If you are working with an MDR provider, you should always define SLAs and communication processes that ensure that the MDR provider does not operate in a "black box."

CyberProof uses its CDC platform to offer full collaboration between clients and the CyberProof SOC team. Clients access the platform to monitor, review, and define client reporting formats and dashboards that track service levels and success.



When an organization does not have an efficient SOC workflow, vulnerability to cyberattacks increases, making it impossible to mitigate risks effectively.

Working with an MDR provider allows you to improve security strategies and stay a step ahead of malicious actors, enabling you to access the latest security capabilities and improve your cybersecurity posture.

CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts. Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics. Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations.

For more information, visit www.cyberproof.com.

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

cyberproof.com