CyberProof™

THE ULTIMATE GUIDE TO AUTOMATING YOUR SOC

HOW AI CAN IMPROVE SOC EFFICIENCY AND REDUCE RESPONSE TIMES

TABLE OF CONTENTS

KEY TAKEAWAYS 3

INTRODUCTION 4

PROCESS-RELATED CHALLENGES 5

ALERT FATIGUE 5

LACK OF STANDARDIZATION 5

TECHNOLOGY CHALLENGES 6

EVOLVING ATTACK SURFACES 6

THE CONVERGENCE OF OT AND IT 7

RISK ASSESSMENT AND MEASUREMENT 8

THE IMPORTANCE OF ORCHESTRATION AND AUTOMATION 9

BOT MEETS HUMAN 9

THE POWER OF ORCHESTRATION 10

DEFINING USE CASES AND INCIDENT RESPONSE WORKFLOWS 10

CONCLUSION 11

ABOUT CYBERPROOF 12

KEY TAKEAWAYS

1. Alert fatigue and a general lack of standardization make it difficult for SOC teams to operate effectively in securing an organization's data, team, and integrity.

2. A whole plethora of new security challenges have developed due to rapid change of organizations attack surface and the growing sophistication of cyber criminals – and the explosion in cyber products often creates more confusion for organizations.

3. For computing power to be successfully harnessed, a four-pronged strategy Is required that includes: training bots in attack pattern recognition; using AI to cut detection and response time; leveraging reinforcement learning – based on the activities of expert human analysts; and consolidating data in a single data lake.

4. SOAR (Security Orchestration, Automation and Response) solutions are key in increasing SOC automation and reducing the time required for detection and response. They require a high level of integration that demands robust workflows and established use cases.

5. Sometimes the term "use case" simply refers to SIEM threat detection rules. But a use case actually should include – in addition to the threat detection rule – a playbook that provides details of how the SOC analyst should respond when an alert is triggered, enrichment and dashboards.

6. No security system is 100% foolproof in identifying potential threats in a timely manner. The emphasis must be placed not just on detection but on reducing dwell time and speed of response. Putting into place smart capabilities to cut Mean Time to Respond (MTTR) provides greater cyber maturity and lowers an organization's degree of risk.

INTRODUCTION

The adoption of innovative technologies is crucial in today's business environment – driven by the ongoing pressure to acquire more customers by launching new services in a faster and more convenient way. But adopting new technologies always brings with it a slew of security challenges, making it harder to maintain a secure working environment that provides protection from cyber threats.

Therein lies the rub: Innovation or security? Efficiency or protection? It is an ongoing challenge for any dynamic and productive organization to find the right balance between these frequently conflicting needs.

For many organizations it's the security team that is most impacted by this kind of deliberation. When senior management opts to purchase new technologies, it is the security operations team that must find ways to monitor, identify, and intercept any anomalous behaviors or vulnerabilities that could be indicative of a cyber attack.

It's a moving target – and it's not the only challenge security teams deal with on a daily basis. There's also the challenge of a continually changing threat landscape, with new kinds of attacks and different threat actors cropping up daily.

Moreover, the number of alerts that security teams are expected to handle on a daily basis is expected to continue to grow. And the sheer number of alerts leads to "alert fatigue" on the part of security teams, who can't keep up with the workload. The answer to this problem lies in leveraging automation, which plays a key role in lightening the load and improves efficiencies and accuracy – providing enrichment from both internal and external sources, the contextual information needed for analysts to identify and prioritize which alerts are high risk and need to be handled first.

This eBook takes a look at the issues facing today's Security Operation Centers (SOC) – and assesses how AI and automation can help you meet these challenges and successfully provide organizations with greater cyber resilience.

PROCESS-RELATED CHALLENGES

Operating an SOC successfully involves implementing effective and sustainable processes that a team can comfortably maintain. But the challenges to maintaining good processes are complex – and technology issues are aggravated by problems related to process such as alert fatigue and a lack of standardization.

Alert Fatigue

The term "alert fatigue" refers to the sheer exhaustion that comes from having too many alerts coming in, and not enough people to monitor them effectively.

There has been an explosion in alerts in recent years, as security tools become more sophisticated at identifying potential threats and organizations take a zero trust approach to log collection. According to research by Imperva, 27% of IT professionals say that their organizations receive more than 1 million security alerts daily. Clearly, this is not sustainable.

Lack of Standardization

In large organizations, the issue of alert fatigue is compounded by a lack of standardization across different business units. Security and IT methodologies and processes differ from site to site – and when companies are acquired or merge, they tend to bring with them their own set of technologies and policies.

How can an SOC team manage security effectively when faced with this complex mix of standards, processes, and network architectures?

Organization-wide policies reduce the degree of inconsistency. But often the SOC team is overworked and understaffed so there is little time available to invest in process improvement.

There are several factors that contribute to this problem:

High Rate of False Positives

Many of the alerts that come in that don't reflect "real" problems. There's a lack of accuracy – meaning lots of issues are being flagged by the SIEM and other log management tools that don't actually require the SOC team's attention. Yet the SOC team still needs to weed through them and determine which ones are the real threats that require attention.

Lack of Enrichment

The alerts that are coming in don't have the right maturity of information. They are missing the necessary contextual background and lacking the enrichment from internal and external sources that helps analysts make an informed decision. CyberProof's research shows that, today, 80% of the SOC analyst's work involves enrichment. That means enrichment is a massive resource drain for the SOC team.

Not Enough Experts

As explored by Forrester, the growing skills gap in the security industry means it is practically impossible to maintain the human resources you need for effective SOC operations. There are more jobs than people; according to Brian NeSmith in Forbes, by 2021 there might be as many as 3.5 million unfilled positions in the cyber security industry. That makes it increasingly difficult to find professionals with the necessary experience.

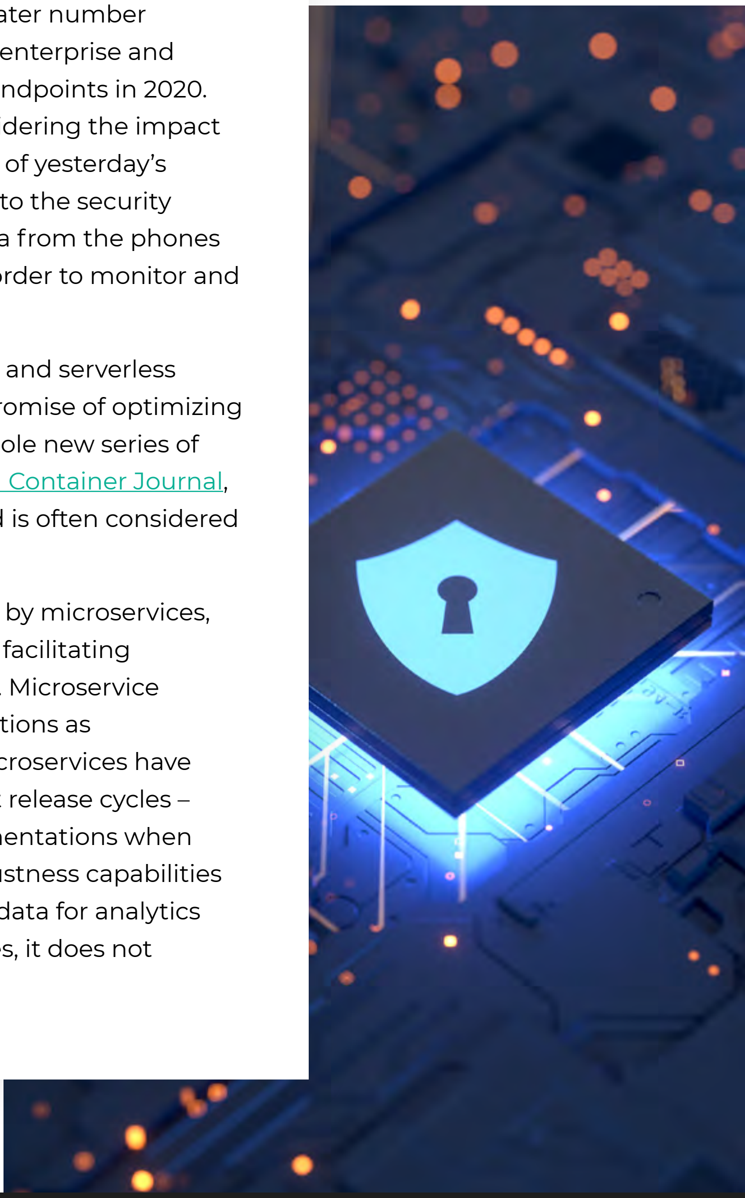
TECHNOLOGY CHALLENGES

Gone are the days when IT was focused on a bunch of servers and cables. Certainly, the architecture was simpler back when data actually 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 a continuously changing attack surface. So SOC teams are often left in the dark with little idea of what is happening across the organization and even less of an ability to respond when something bad happens.

Evolving Attack Surfaces

SOC teams are faced with the infinitely more complex IT environment that has become the norm – created by more sophisticated attack actors and the widespread adoption of new technologies such as:

- **Transition to the Cloud –** The widespread adoption of IoT and the cloud makes the environment difficult to secure because of its distributed architecture and exponentially greater number of endpoints. Gartner recently predicted that the enterprise and automotive IoT market would grow to 5.8 billion endpoints in 2020. The significance of this can be illustrated by considering the impact of cell phones, which are more powerful than any of yesterday's desktops. Cell phones provide serious challenges to the security landscape, as security teams must obtain the data from the phones – and from all of the other available systems – in order to monitor and protect the organization.
- **Containers –** The growing adoption of containers and serverless networks, while offering businesses the golden promise of optimizing hardware utility and efficiency – also creates a whole new series of security issues. As pointed out by Sam Bocetta on Container Journal, container security has been widely neglected and is often considered only as an afterthought.
- **Microservices –** Further complexity is introduced by microservices, hailed for enabling cloud-native deployment and facilitating the rapid delivery of services on an ongoing basis. Microservice architecture describes a way of designing applications as independently deployable services. And while microservices have the advantages of requiring shorter development release cycles – problems are common with microservice implementations when developers neglect to design-in security and robustness capabilities into their services. Also, extracting security event data for analytics from microservices often is not easy; in most cases, it does not provide any useful data.



The Convergence of OT and IT

The operational technologies (OT) and information technologies (IT) defined years ago were far apart from each other, with different methods of connectivity and different languages. But now, IoT is quickly changing the systems and environments that rely on OT.

In manufacturing plants, hospitals, power stations, rail systems, and many industrial environments that require the use of computers to monitor or alter the physical state of a system – IoT is shrinking the gap.

As Gartner has been talking about for years (see this article), IT and OT are on a path toward convergence, old systems that supported industrial control processes (and other specialized applications) are quickly being replaced. Instead of the traditional operational technology systems that relied on legacy machine-to-machine (M2M) systems – advanced applications can now intelligently monitor and control remote sensors, mobile devices, and smart machines – and multiple systems are connected to create flexible, interoperable environments that are IP-based.

For example, both large and small systems are being built using the SCADA (Supervisory Control and Data Acquisition) concept. SCADA uses computers, network data communications, and graphical user interfaces while also using peripheral devices to interface with machinery. Today, it integrates new kinds of connector system involving IoT.

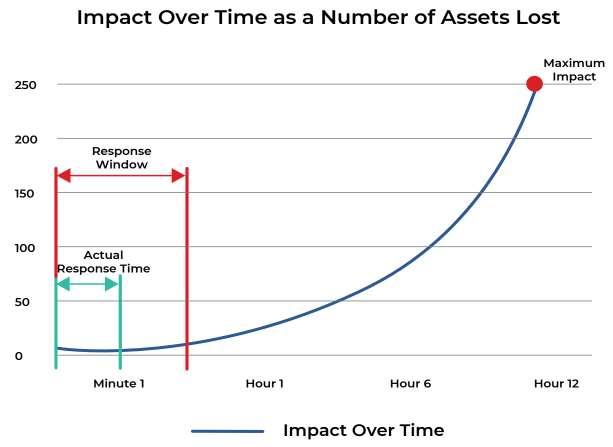
While the unification of OT and IT systems eliminates inefficiencies, and can improve automation in manufacturing environments, the use of IoT-based technologies means there are new vulnerabilities and higher levels of cyber risk.

RISK ASSESSMENT AND MEASUREMENT

Many of the issues facing SOCs can be addressed through a combination of automation and human intervention. Leveraging the distinct power and capabilities of computers – which have the advantages of speed, reliability, and ability to process vast volumes of data – is the path forward in reducing the time required for detection and response. At the same time, human intervention is still required to deal with many complex analysis and assessment tasks that computers are less well equipped to handle.

For the power of computers to be harnessed in security operations, the following methodologies need to be deployed:

- **Attack Pattern Recognition:** To find the one event that's crucial, an SOC must be able to assemble the alerts into an attack pattern – identifying which ones might be indicative of an attack and prioritizing which ones could potentially cause serious damage. Algorithms can be used to facilitate this kind of anomaly detection, which allows the preemptive detection of an attack and assesses probabilities in order to define what represents the highest risk. The bot has the advantages of speed and longer recall – and can scan data across the Internet to gain information about the origin of an attack and provide context over time. The bot also leverages an awareness of all attacks currently available – something humans do not have the ability to do.
- **Definition of the Response Window:** In assessing the risk associated with cyber attack, it is possible to define a minimum period of time after which the impact of the cyber attack becomes exponentially greater. In other words, the magnitude of loss associated with cyber attack is directly related to how long it takes to detect and respond. Thus, speed and agility are the name of the game.



- **Adoption of Reinforcement Learning:** Computers are only as good as the humans they learn from. Reinforcement learning means that computers mimic the actions of experts – of expert, human analysts – and then automate the process they've "learned." Through an ongoing process of reinforcement learning, an organization can successfully leverage AI bots to get faster at preempting, identifying, and mitigating subsequent attacks.
- **A Single Data Lake:** The consolidation of data into a single data lake allows the same data to be used in parallel by multiple teams within an organizations: business analysts can use it for analytics around business activities, IT can use it for IT-related analytics, and security teams can leverage it for running security analytics. The use of this data by multiple groups and its consolidation in one single data lake facilitates better analysis, providing additional context for security alerts that helps analysts make informed decisions.

Leveraging AI to work faster and minimize damage means:

- Detection approaches real time
- Response deploys automation
- Continuous learning & improvement

THE IMPORTANCE OF ORCHESTRATION AND AUTOMATION

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

In an increasingly automated SOC, the interaction between humans and bots[1] 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 operation that require new workflows and use cases.

Bot Meets Human

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 could be carried out by the smart bot. At the point where a smart bot is not capable of further pursuing the response activities, the alert must be handed over to human security analysts.

At CyberProof, this handover is a part of the collaborative process that is defined by our playbooks. For example, a machine might complete the first few steps of the playbook before assigning the next step to the human analyst.

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 an 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.

[1] The term bot refers here to an intelligent agent, defined by Wikipedia as follows: In artificial intelligence, an intelligent agent (IA) refers to an autonomous entity which acts, directing its activity towards achieving goals (i.e. it is an agent), upon an environment using observation through sensors and consequent actuators (i.e. it is intelligent).

The Power of Orchestration

Gartner's recent report Market Guide for Security Orchestration, Automation and Response Solutions defines orchestration, stating: "The complexity of combining resources involves coordination of workflows with manual and automated steps, involving many components and affecting information systems and often humans as well."

Gartner's report underscores the growing importance of SOAR solutions in improving the efficiency of an SOC and reducing the time required for detection and response. SOAR solutions aim to converge security orchestration and automation tools, security incident response, and threat intelligence platforms – creating a single solution that is fully integrated with SIEM and log management systems.

SOAR technologies facilitate SOC automation – allowing the collection of data about cyber threats from multiple sources, and automatically responding to certain kinds of events without human assistance. This fills security gaps, frees up some of the time spent by human analysts, and can significantly improve the efficiency of security operations.

Defining Use Cases and Incident Response Workflows

To constantly improve detection abilities and stay up to date with emerging threats, SOCs should continuously design and build robust use cases.

People tend to associate a use case as a SIEM detection rule, but in this context, a use case is much more than that, including:

- Collecting the right security data to perform security analytics
- Orchestrating security monitoring & incident response technologies
- Enriching security alerts for better contextualization
- Developing incident response playbooks and incident response workflows
- Automating responses by enabling integration with network and security controls
- Creating dashboards & reports for real-time visibility

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 & services used, and more.

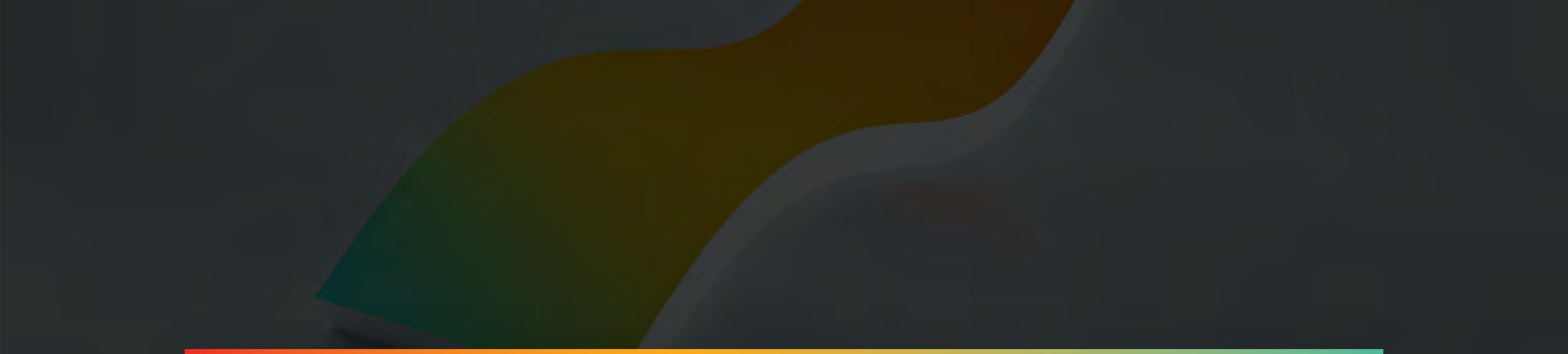
CONCLUSION

The challenges facing today's SOC include process and technology challenges that can make attempts to improve efficiency feel like a losing battle. Alert fatigue and a general lack of standardized methodologies can make it tough to operate effectively, and the rapidly evolving attack surface create a never-ending series of new challenges.

In this environment, SOC automation using AI provides a way forward, improving the security posture of enterprises – and allowing an organization to detect new attack situations and techniques faster.

Smart bots can be used not just to prioritize detection but to recognize patterns and anomalies, preempt attacks and predict the next stage of attack. In addition, better analytics can be obtained by consolidating data in a single data lake and this can provide the additional context that's so sorely needed in assessing new threats. SOAR solutions are also a piece of the puzzle, but to be implemented effectively they require the right experts with the right skills to gain the full potential of this powerful platform.

In today's rapidly evolving threat landscape, the emphasis must be placed not just on detection but on speed of response. No security system is going to have 100% success in identifying potential threats – and putting into place AI tools that effectively cut Mean Time to Respond (MTTR) provides greater cyber maturity and lowers an organization's degree of risk.



ABOUT CYBERPROOF

CyberProof is a security services company that intelligently manages your incident detection and response. Our advanced cyber defense platform enables operational efficiency with complete transparency to dramatically reduce the cost and time needed to respond to security threats and minimize business impact. SeeMo, our virtual analyst, together with our experts and your team automates and accelerates cyber operations by learning and adapting from endless sources of data and responds to requests by providing context and actionable information. This allows our nation-state cyber experts to prioritize the most urgent incidents and proactively identify and respond to potential threats. We collaborate with our global clients, academia and the tech ecosystem to continuously advance the art of cyber defense.

For more information, see: www.cyberproof.com

LOCATIONS

Aliso Viejo | Barcelona | London | Tel Aviv | Trivandrum | Singapore