Gorilla Guide®
Foundation Edition

The Journey to an Intelligent SIEM/SOC

Maurice Stebila, Former CISO of Harman by Samsung
Lawrence Miller

Inside the Guide

- A Day in the Life of a Security Analyst
- The Benefits of Adding Intelligence to Security Ops
- 5 Steps To Evolving Your SIEM or SOC

ActualTech Media
STELLAR CYBER®

The Journey to an Intelligent SIEM/SOC

Maurice Stebila, Former CISO of Harman by Samsung
Lawrence Miller

TABLE OF CONTENTS

ActualTech Media

6650 Rivers Ave Ste 105 #22489 | North Charleston, SC 29406-4829

www.actualtechmedia.com

Introduction

It's a jungle out there! The Internet has never been a more hostile environment as the volume, scope, and scale of cyber-attacks and breaches continues to soar. Recent FireEye and SolarWinds breaches show a comprehensive cybersecurity strategy necessarily includes robust prevention, detection, and response capabilities, but as the constantly evolving threat landscape makes a successful cyberattack or breach ever more likely, enterprises and managed security service providers (MSSPs) are increasingly focusing their efforts on effective detection and response. The Stellar Cyber intelligent security operations platform helps organizations throughout their journey.

According to the 2020 Cost of a Data Breach Report (IBM Security), the average time to identify and contain a breach is 280 days, with an average total cost of $3.86 million.

The security analysts on your security operations team juggle a multitude of complex, expensive security tools from multiple vendors while trying to keep their heads up in a massive quicksand pit of security alerts. The last thing they need is another siloed point solution to cobble together. This daily

Security Operations Taxonomy

Where are you on the journey to an intelligent SIEM or SOC?

	Log Management	SIEM	SOC
Use Cases	Compliance Data lake Threat investigation	Query-driven Detections (Rules + UEBA)	Threat Hunting with Automated Response (SOAR)
Security Team Focus	Focused on Governance and Compliance	Focused on threat identification	Focused on complex threat detection and response
Security Team Structure	Co-owned by IT	Security director/CISO with a small team	Dedicated SOC team
Challenges	Cost, want security with limited budget and resources	Complexity and limited expertise and resources	Confidence in detections and productivity

Figure 1: Typical security operations team use cases, focus, structure, and challenges

struggle is real, whether you have a security information and event management (SIEM) platform or a security operations center (SOC)—or are thinking of building one. Use the information in **Figure 1** to help you determine where your security operations team is on its journey.

Enterprise Strategy Group conducted a recent survey of CISOs to identify their biggest challenges and the results are in:

- **Threats on the rise (76 percent)** – Threat detection and response is more difficult today than it was just two years ago, and current detection and response tools aren't keeping up.

- **Data and alert fatigue (70 percent)** – It's difficult for my organization to keep up with the volume of security alerts generated by our security analytics tools.
- **Visibility gaps (75 percent)** – It's difficult to synthesize different security data telemetry for security analytics.
- **Security tool failure (75 percent)** – My organization has deployed one or more security analytics technologies that haven't lived up to expectations.
- **Skills gap (75 percent)** – The cybersecurity skills shortage has impacted security analytics and operations in my organization.

Today's enterprise security environments consist of physical, virtualized, and containerized workloads in on-premises data centers and public, private, and hybrid clouds. This creates huge coverage challenges and an overwhelming volume of unactionable alerts. In this untenable state, it's extremely difficult for security teams to efficiently respond to alerts and identify critical threats before valuable data is stolen or damage is done.

Clearly, a better early warning detection platform is needed: a scalable, artificial intelligence (AI)-powered security operations with the right data and armed with the ability to automatically detect, hunt, and respond to threats.

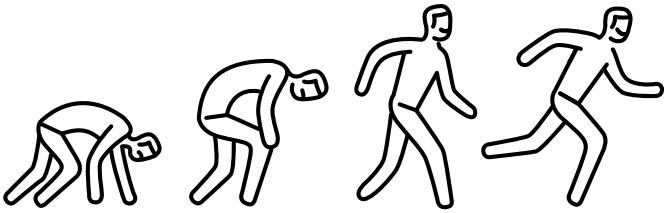
The Cost (Benefit) of Security Automation and Incident Response

According to the *2020 Cost of a Data Breach Report* (IBM Security), the average time to identify and contain a breach is 280 days, with an average total cost of $3.86 million. Rapid detection and response are key to reducing the cost of a breach. With rapid detection, the average cost of a breach is reduced from $3.86 million to $2.74 million for breaches identified and contained in less than 200 days.

For organizations with fully deployed security automation (artificial intelligence, machine learning, analytics, and orchestration) to augment or replace human intervention, the average time to identify and contain a breach is 175 days with an average total breach cost of $2.45 million (versus $6.03 million for organizations with no security automation). Effective incident response (as demonstrated by the existence of an IR team and IR plan testing) reduced the average breach cost to $3.29 million (versus $5.29 million for organizations without an IR team or IR plan testing).

Crawl, Walk, Run: The Evolution to the Intelligent SIEM / SOC

Evolving from a traditional SIEM/SOC to the Intelligent SIEM/SOC follows a familiar pattern for most bipeds: crawl, walk, run. But for our maturity model there are actually five levels, so let's add "slither" and "soar" to the beginning and end of the model.



- **Level 1 (Perimeter – network):** The organization has deployed traditional perimeter-based security tools such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), endpoint protection platforms (EPP), and vulnerability management. The Stellar Cyber Intelligent next-gen security operations platform, powered by Open eXtended Detection and Response (Open XDR), leverages nearly 300 integrations with existing tools to correlate their data. This lowers costs by 4x and broadens labor options while adding new capabilities, including firewall traffic analysis (FTA), machine learning IDS (ML-IDS), sandbox, and data streaming to legacy SIEMs.
- **Level 2 (Coverage – more data):** The enterprise or MSSP has deployed a security information and event management (SIEM) tool with log data as its primary sources. It is ostensibly for early attack detection, investigation, and response to complex attacks. Wait, your SIEM doesn't do all that? Don't worry, you're not alone – setting up and properly tuning a SIEM platform is complex. As more applications have moved from on-premises infrastructure to the cloud, you may also be using a cloud access security broker (CASB) to manage risks for the SaaS

applications used by your organization. The Stellar Cyber security operations platform brings next-generation SIEM (NG-SIEM) and cloud detection and response (CDR) to the party, providing comprehensive visibility across on-premises, public cloud, and SaaS applications such as Office 365.

- **Level 3 (Intelligence – advanced analytics):** The organization is gaining valuable insights through data collected leveraging advanced analytics such as behavior analysis and machine learning to bring speed and fidelity to detection and response. The Stellar Cyber security operations platform supports user user and entity behavior analysis (UEBA), and network traffic analysis (NTA). It leverages advanced analytics by tuning the data to reduce noise through advanced ML algorithms.

- **Level 4 (Coordination – orchestrated response):** The organization has used security orchestration, automation, and response (SOAR) functionalities. The Stellar Cyber security operation platform has built-in automated response capabilities to further reduce your response time.

- **Level 5 (Prediction – single pane of glass):** The organization leverages a single platform to detect, correlate, investigate, and respond to critical events in the environment. The Stellar Cyber security operations platform is the only security platform that delivers complex attack detection and response across the entire attack surface with a comprehensive, kill-chain-aligned GUI that improves mean time to detect (MTTD) by 8x and mean time to remediate (MTTR) by 20x.

An organization with a traditional SIEM/SOC can be at any of these five levels. However, the Stellar Cyber security operations platform, powered by Open XDR, can modernize and elevate your organization to the highest level while helping turn an ordinary security analyst into a security expert.

As more applications have moved from on-premises infrastructure to the cloud, you may also be using a cloud access security broker (CASB) to manage risks for the SaaS applications used by your organization.

Welcome to the Jungle: A Day in the Life of a Security Analyst

To gain a better understanding of the challenges your security teams face, it's sometimes helpful to trek a mile in their shoes. The various tiers of security analyst responsibilities can be summed up using the analogy of the heroes in another one of today's jungles, a hospital emergency room.

In traditional security operations, there are typically three levels of security analysts:

- **Level 1 (trauma nurses):** triage specialists who monitor and evaluate incoming alerts and identify suspicious activities that merit attention, prioritization, and further investigation.
- **Level 2 (emergency room doctors):** incident responders who perform the more advanced analysis and investigation of alerts, assess the scope of an attack, and identify and research indicators of compromise (IOCs) for blocking or mitigation of identified threats.
- **Level 3 (specialists and surgeons):** threat hunters who conduct malware analysis and network forensics and work to proactively identify attacker tactics, techniques, and procedures (TTPs) and advanced persistent threat (APT) activities. They also work with key stakeholders throughout the organization to implement remediation plans.

The key activities of the security teams can be broadly classified into four areas: collect, detect, investigate, and respond.

COLLECT

In a traditional SIEM/SOC, thousands of events are collected every day, and alerts are generated daily by endpoints, firewalls, servers, applications, and various other security tools deployed across the organization. Without proper context, this onslaught of information leads to alert fatigue, causing potentially critical events to be missed or ignored.

In the Intelligent SIEM/SOC platform, these same events are collected from the same systems, but they're automatically normalized and enriched with contextual information like users, assets, and built-in threat intelligence, and correlated to incidents so that only relevant and actionable alerts are generated for the security analysts, enabling easy triage and investigation. Leveraging AI and machine learning (ML), the Intelligent SIEM/SOC is constantly improving the accuracy of correlations and reducing alert "noise" to enable human security analysts to focus on critical events.

DETECT

Detection of critical events can be hit-and-miss in a traditional SIEM/SOC. It's frequently a matter of correctly fine-tuning all of the instrumentation throughout your environment: too much tuning and the analysts won't get enough event information and alerts (false negatives); too little tuning and they'll be overwhelmed with extraneous and inconsequential alerts (false positives). Even after you've spent the time and effort to correctly tune the instrumentation, it comes down to the skills and experience of individual analysts to manually detect critical events amid all of the chatter—which may take days, weeks, or much longer.

The key activities of the security teams can be broadly classified into four areas: collect, detect, investigate, and respond.

In the Intelligent SIEM/SOC platform, critical alerts are quickly and automatically surfaced through advanced ML, and in many cases remediated. When remediation isn't possible through automation and orchestration, security analysts can quickly take manual action or escalate alerts, as appropriate.

INVESTIGATE

Investigation in a traditional SIEM/SOC typically requires analysts to leverage numerous tools for simple tasks like geo-locating an IP address, identifying users and/or assets, researching threat intelligence databases, and much more.

In the Intelligent SIEM/SOC platform, many common investigation tasks have been automatically completed by the platform itself. Security analysts can perform many other tasks directly in the same console with all the data in a unified data lake, using a Google-like search capability, and associate the investigation results with the alert, thereby saving valuable time for analysts at different levels throughout the investigation process.

RESPOND

Looking back at that IBM Security *2020 Cost of a Data Breach Report*, 73 days of the 280 average total days to identify (collect, detect, investigate) and contain (respond) a breach were spent on containment. That's a measure of the traditional SIEM/SOC's incident response capability.

In the Intelligent SIEM/SOC platform, many response activities are automated and orchestrated, reducing containment and remediation to minutes instead of days or weeks. Critical events that can't be automatically contained and remediated can be responded to quickly by the SOC's incident response team, armed with timely, actionable information and recommendations about the threat.

Realizing the Advantages of the Intelligent SIEM or SOC

The Intelligent SIEM/SOC delivers dramatic improvements to a company's ability to protect itself from ongoing attacks. It consolidates and analyzes information from across all security tools, correlating detections from multiple sources, and presenting actionable attack information and remediation options in a single dashboard.

Enterprises and MSSPs see the advantages of the Intelligent SIEM/SOC firsthand when performing external penetration testing and red team adversary simulations to validate that their security operations platform is correctly optimized for detecting and identifying alerts. There has been some discussion as to whether AI and ML will start to replace human security analysts, but industry experts agree that these deep learning tools complement, augment, and improve your security operations staff's ability to perform analysis and investigation to detect advanced threats. The intelligent SOC

also delivers significant improvements in threat hunting, detection, and forensics analysis. These enhanced capabilities lead to reduced dwell time, MTTD, and MTTR.

The Intelligent SIEM/SOC delivers dramatic improvements to a company's ability to protect itself from ongoing attacks.

Call to Action: In the Jungle, the Quiet Jungle, the CISO Sleeps Tonight

Traditional SIEM/SOCs see thousands of isolated alerts on various endpoints, firewalls, and other tools, or in server and application logs (possibly all under the umbrella of a SIEM), causing blind spots instead of enabling situational awareness and effective response.

Security analysts are overwhelmed with alert fatigue and the complexity that comes from having to use a dozen or more discrete tools. Stellar Cyber's intelligent next gen security operations platform gives you a 360-degree view of your entire attack surface from a single interface, allowing analysts to detect complex attacks in seconds and respond within minutes.

Stellar Cyber's platform offers readily available, pre-built, high-fidelity correlated detections in one console so your analysts don't have to spend time integrating multiple tools and tuning noisy rules. Its readable, searchable, and actionable records of every event provide human-friendly evidence and easy-to-digest details that level-up your analysts into threat hunters.

Traditional SIEM/SOCs see thousands of isolated alerts on various endpoints, firewalls, and other tools, or in server and application logs (possibly all under the umbrella of a SIEM), causing blind spots instead of enabling situational awareness and effective response.

The platform works with the existing SIEM and other tools you already trust, ingesting their data to rapidly detect threats. It is operational within hours and offers a broad range of capabilities that allow you to sunset existing tools (such as NDR, CASB, UEBA, SIEM, SOAR) to save on licensing fees. Stellar Cyber:

- Radically improves efficiency by creating context around data, reducing attack identification time, and allowing improved resource allocation for other security tasks

- Dramatically improves detection accuracy with Artificial Intelligence and reduces resolution time
- Integrates with over 270 and growing security solutions to ingest, normalize, correlate and respond to threats quickly
- Is a single-license platform with easy deployment on premises, in public clouds, or in hybrid environments

No matter where your security team currently stands on the journey to the intelligent SIEM or SOC as shown in Figure 1, Stellar Cyber's XDR platform can help you move one or two steps toward the ending goal with effectiveness, efficiency and efficacy to overcome the challenges your security team is facing.

Don't lose another night's sleep in the Internet jungle! Get started today with a product tour at https://stellarcyber.ai/products/product-tour/. Then see Stellar Cyber's Intelligent next gen security operations platform in action by requesting a demo at https://stellarcyber.ai/request-a-demo.

About Stellar Cyber

Stellar Cyber's high-speed, high-fidelity detection and automated response platform gives you 360-degree visibility across the entire attack surface through normalized and enriched data from ANY source. It reduces attack detection time from days to real time, allowing improved resource allocation for other projects. Pre-built detections improve analyst skillsets, enabling them to detect and respond to complex threats and making them far more productive by dramatically reducing alert fatigue. It is also easy to use, incorporating many native security tools under a single pane of glass, and enables you to sunset stand-alone tools to reduce licensing costs and complexity.

ABOUT THE AUTHOR

Maurice Stebila is the Founder and CEO of CxO InSyte,[1] a cybersecurity information exchange and professional network event consortium for CISO/CIOs. Previous, Mr. Stebila was the Chief Information Security Officer of Harman by Samsung, responsible for Digital Cyber Security, Compliance and Privacy across Harman's global enterprise.

[1] https://cxoinsyte.com/

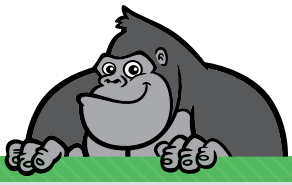
About ActualTech Media

ActualTech Media

ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.



If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit https://www.gorilla.guide/custom-solutions/