INSIGHTS | TECH BRIEF

Written By Shawn Murphy
WEI Cybersecurity Solutions Architect

Maximizing Incident Response Effectiveness In The Modern SOC

The cybersecurity landscape is constantly evolving as organizations grow more distributed and migrate to the cloud, leading to an expanded attack surface. The broader perimeter and significant financial incentives to cybercrime has resulted in threats becoming more complex, malicious, organized, and well-funded. While businesses are using AI to strengthen their security posture, threat-actors are also embracing AI-powered tools to craft sophisticated customized attacks. This necessitates a paradigm shift in how Security Operations Centers (SOCs) approach incident response (IR).

Traditional SOCs functioned as reactive entities, primarily focused on identifying and responding to active threats. While detecting and reacting to threats remains a critical aspect of security, modern SOCs must be proactive. Incident response effectiveness is maximized through collaboration between SOC and IR teams, enabling quicker detection and streamlined workflows that facilitate more efficient escalation and containment of security incidents. Strong feedback loops between IR and SOC teams can help establish more effective security measures, reducing cyberattack risk. By proactively hunting for threats through techniques like threat intelligence analysis and leveraging advanced analytics and automation, security teams can identify and neutralize malicious activity before it can inflict significant damage.

This technical brief covers topics explored in an informative conversation between Shawn Murphy, WEI's Senior Cybersecurity Architect and Jeff Cassidy, Security Operations Center Manager at CyberTrust Massachusetts. To listen to the full podcast, visit the WEI Tech Talk Podcast on any major podcast platform.

Evolution Of The SOC

The core mission of the SOC is to detect, prevent, respond to, and recover from security threats by continuously analyzing data from various sources across the organization's network, systems, and applications. As Jeff Cassidy aptly states, "The goal of the SOC is to find the bad." Traditionally, SOCs were on-premises facilities where analysts monitored network activity for suspicious behavior by combing through vast amounts of log data to identify potential threats. Today, SOCs can be virtual, hybrid, or entirely remote, depending on an organization's infrastructure and operational model.

WEI TECH TALK

EP 20: Discussing Modern SOC, Incident Response & Threat Hunting
LISTEN NOW

WEI CYBERSECURITY

SOCs are typically structured with different analyst tiers:

- **Tier One** analysts triage alerts to assess the urgency and relevancy of potential threats and escalate anything requiring further attention.
- **Tier Two** analysts conduct deeper investigation and apply more advanced analyses to assess the legitimacy and origin of threats.
- **Tier Three** analysts are experts with deep knowledge of organizational infrastructure, enabling them to make critical decisions about threats and coordinate complex responses. These analysts also employ their advanced skillset to hunt for threats that may have evaded detection.

Many organizations now outsource tier one responsibilities, and other lower-level SOC operations, to managed security service providers (MSSPs) to reduce costs and ensure 24/7 coverage. This allows internal teams to focus on complex issues and strategic initiatives.

As technology has advanced and attack surfaces expanded, cybersecurity risks have grown in volume and sophistication. The rise of cloud computing, Software-as-a-Service (SaaS), Operational Technology (OT), and the Internet of Things (IoT) have significantly increased the digital footprint that must be monitored and secured. SOCs have had to broaden their focus to encompass a wider range of security domains, including endpoints, cloud environments, and identity management. Data serves as the primary driver of SOC activities, as the volume and complexity of the data that requires analysis has increased significantly.

To address these challenges, SOCs are utilizing a variety of specialized tools and technologies designed to detect and respond to threats across various environments, however, limited integration and interoperability between security tools has increased the workload for SOC analysts. Organizations are facing both a skills gap, where tier one analysts aren't equipped with the necessary skills to effectively utilize the tools, and a knowledge gap, where analysts struggle to tune alerts to prevent recurring false positives and avoid unnecessary escalation. Additionally, the ever-growing volume of data, coupled with the influx of new tools and increased complexity of the networks they protect, often results in alert fatigue.

The Modern SOC: A New Operational Model

The conventional SOC structure is based on the traditional helpdesk approach, with a tiered system for escalating issues. The ticket-based system in legacy SOCs focused on individual alerts without considering the broader context or related alerts, leading to blind spots and delayed response times. Tier one analysts often experienced burnout due to high stress and limited exposure to broader security operations, while the siloed processes created bottlenecks as issues were escalated to higher tiers. The modern SOC represents a strategic evolution from the traditional structure, focusing on flexibility, adaptability, and the integration of advanced and holistic technologies. Transforming from legacy models involves rethinking organizational structures and technology platforms to protect expanding attack surfaces and meet the demands of a rapidly evolving threat landscape.

Integrated And Holistic Platforms

Traditional Security Information and Event Management (SIEM) systems, designed to aggregate logs and generate alerts into separate ticketing platforms, often lack scalability and integration capabilities. Modern SOCs are adopting integrated security platforms that aggregate data and logs from various sources, such as cloud platforms, identity services, and endpoint detection and response (EDR) tools. These platforms incorporate built-in case management to streamline investigation and resolution, AI-driven detection and tuning capabilities, machine learning (ML) algorithms for advanced analytics and better visibility, and User Entity and Behavior Analytics (UEBA) to detect subtle anomalies that might indicate insider threats and compromised accounts. Let's look at some key components of a modern SOC platform:

- **Alert Aggregation and Correlation:** In legacy SOCs, analysts sifted through a deluge of security alerts to try and understand relevance and identify correlations. Modern SOC platforms aggregate and correlate security events by gathering alerts from various sources, finding commonalities, and enriching them with threat intelligence insights, historical context, and information about user behavior patterns.

- **Automation:** Repetitive tasks and routine threats are managed through automation, which improves efficiency and reduces the workload on analysts. Automated workflows streamline processes and ensure consistent execution, reducing errors. Automation leverages AI and ML to rapidly analyze security alert and event data, reducing false positives and accelerating threat detection and incident response times.
- **Advanced Analytics:** AI and ML technologies analyze massive datasets, uncovering hidden patterns indicative of malicious activity, enhancing threat hunting. For example, AI can detect subtle changes in user behavior that might signal a compromised account, enabling timely intervention. Additionally, these technologies can be deployed to counter adversarial AI by detecting refined tactics, such as sophisticated phishing emails, though analysis of message structure and language patterns.

Enhancing IR Effectiveness In The Modern SOC

After analyzing security alerts, the SOC escalates confirmed threats to the IR team. Their missions are complementary: the SOC focuses on "finding the bad" (detecting and analyzing potential threats), while IR handles "containing the bad and getting back to good" (reacting to incidents, containing damage, eradicating threats, and restoring normal operations). Traditionally, SOC and IR teams were closely aligned but separate entities. Integrating the IR function under the same umbrella as the SOC, alongside other supporting functions such as detection engineering, threat hunting, and cyber threat intelligence, has become increasingly common. This approach is particularly advantageous in small SOCs where analysts wear multiple hats. An integrated approach promotes seamless collaboration and handoff from alert detection to incident response, underscoring the critical role of the SOC in supporting and improving the effectiveness of IR.

Comprehensive Incident Context

Comprehensive and accessible information regarding incident context is crucial for the SOC to support IR effectively. This information should clear and concise, covering details such as the triggering alert information, specific security tools involved, observed versus expected network behavior, incident environment, and any initial SOC containment efforts. Given the time-sensitive nature of incident response, the SOC should provide initial system and timeline scope.

- **System Scope** helps IR teams to understand the breadth of an attack by mapping out compromised systems, networks, endpoints, and user accounts. This step assists in assessing the extent of the threat and informs containment strategies.
- **Timeline Scope** entails reconstructing the chronology of the incident to trace the origin and development of the attack. This helps IR teams understand whether the observed activity is recent or part of a longer-term campaign, informing the response approach. Uncovering the timeline aids in root cause analysis, allowing IR to pinpoint the exploited vulnerabilities that enabled the attack.

The Critical Link Between Scoping And Containment

Effective scoping is vital for successful incident containment and remediation. Building on the SOC's initial assessment of system and timeline scope, the IR team delves deeper. This may involve forensic analysis of compromised systems, in-depth endpoint investigations, and leveraging threat intelligence to understand the attacker's methods and potential goals. A well-defined scope, established through collaboration with the SOC, provides the foundation for successful incident containment. Here's how:

- **Understanding the Impact:** Scoping identifies compromised systems, enabling IR teams to isolate them and prevent the threat from spreading. Understanding the impacted business units and which third parties are involved is also crucial. This combined knowledge informs the development of a targeted containment strategy.

- **Mapping the Attack Path:** Understanding the attack sequence, from initial compromise to current state, is essential for containment. Scoping, though log and network traffic analysis, helps reconstruct this timeline and identify containment points.
- **Building a Removal Strategy:** A clear scope is imperative for IR to formulate an effective strategy to remove the attacker from compromised systems. Scoping not only defines the attack footprint but also helps identify the attacker's methods and command and control channels. This intelligence enables IR teams to target their eradication efforts.

By uncovering the full extent of the incident, IR can take targeted action to contain the threat, minimize damage, and ultimately expel the attacker from the network. Containment isn't simply about shutting down systems. It's a strategic process aimed at:

- **Limiting the Impact:** Containment focuses on isolating compromised systems and preventing the attacker from further lateral movement to minimize damage caused by the incident.
- **Preserving Evidence:** Effective containment avoids actions that could destroy or tamper with evidence required for forensic analysis and understanding the attacker's actions.
- **Maintaining Business Continuity:** As Jeff Cassidy states, "There's a fine line between keeping the business running and stopping the bleeding" as over-containment can disrupt business operations. The ideal approach is to contain the threat at a micro-level, targeting only the infected systems.

Closing the Loop for Improved Security

High-functioning SOC and IR teams operate in a symbiotic relationship where feedback loops drive continual improvement. IR feeds its findings back to the SOC, which identifies weaknesses in existing security controls and alerts. This shared knowledge allows the SOC to refine detection and prevention mechanisms, ultimately reducing the number of incidents that reach IR. When recurring incidents trigger IR involvement, such as those caused by unpatched vulnerabilities, outdated systems, or configuration issues, IR needs to engage with the appropriate IT stakeholders, such as cloud engineers or service providers. These communication loops help identify areas where preventative actions can be taken, eliminating persistent weaknesses and making it harder for attackers to gain a foothold in the environment. Leveraging a closed-loop feedback system, where IR findings drive SOC improvements and proactive communication with IT stakeholders, prevents future incidents.

As Jeff Cassidy states, "In the same model that a SOC should only be left to respond to something that could not have been prevented, an IR team shouldn't be left to scope, triage, and respond to impact for something that should have been avoided."

Incident Preparedness: "Train Like You Fight"

While IR involves managing crisis situations, a significant portion of IR teams' time should be dedicated to proactive measures that improve response efficiency. The best way for IR to become more effective is by focusing on preparedness through rehearsals, dry runs, tabletop simulations, and refining playbooks to improve incident response plan coordination. Tabletop exercises provide a controlled environment to simulate various attack scenarios and test responses, with a focus on building muscle memory so that when a real incident occurs, the response is second nature. By leveraging rehearsals and dry runs as a training platform, and by cultivating a worst-case scenario mindset and planning for potential breaches, data loss, malicious encryption, and exfiltration incidents, IR teams can "train like they fight".

Effective training exercises must comprehensively test and validate all aspects of the IR plan, including incident command structures, escalation protocols, and vendor and third-party coordination. Test cases should encompass all technical aspects including IT team preparedness for data backup and recovery. Scenarios need to continually evolve in complexity, themes, and stakeholder participation, extending beyond the technical aspects to include complimentary workstreams such as legal counsel involvement and external communication. This ensures a comprehensive understanding of roles and responsibilities during an incident. By embracing

a holistic approach that includes all relevant parties, IR can create a more robust and agile incident response framework.

Threat Hunting: Getting "Left of Bang"

"Left of bang" is a concept borrowed from military strategy that encourages a proactive approach to cybersecurity. Here, "bang" represents the moment of crisis, whether it's a breach, an attack, or a critical failure. To get "left of bang", organizations must focus on threat hunting to identify and mitigate potential threats proactively. Threat hunting, a relatively new aspect of modern SOC models, leverages cyber threat intelligence (CTI) as a source of truth about adversaries' tactics, techniques, and procedures (TTPs), along with indicators of compromise (IOCs), allowing threat hunting teams to actively search for signs of compromise within the organization's environment. Threat modeling is essential in this process, aiding organizations in understanding the motivations, targets, and methodologies of potential adversaries based on factors such as industry, geographic location, and geopolitical considerations. Leveraging frameworks like MITRE ATT&CK, threat hunters can map out common pathways used by adversaries to infiltrate systems and search for indicators of their presence before an incident is even detected. Since attackers constantly update their tactics, threat hunters must adeptly identify new and emerging threats, focusing on complex and sophisticated IOCs.

The threat hunting process results in two possible outcomes: (1) If no threat indicators are found, the SOC can set up alerts to monitor for them in the future; (2) If the threat is detected, IR is activated to contain and remediate it, while the detection engineering team develops new detection capabilities. Complimenting proactive threat hunting with traditional defensive measures, like firewalls, vulnerability scanning, patch management, and penetration testing, establishes a multi-layered security approach that provides a comprehensive and adaptable defense against threats. Optimizing preventative controls ensures that threat hunting remains a manageable and effective endeavor.

Talk to WEI today

Organizations must modernize their SOCs to navigate the complexities of today's dynamic threat landscape effectively. By actively hunting for threats before they strike, SOCs can minimize incident response workloads and significantly improve overall security posture. This proactive strategy, coupled with seamless collaboration between SOC and IR teams, empowers organizations to maximize incident response effectiveness within the modern SOC framework and stay ahead of evolving threats. The experts at WEI are ready to support your organization in modernizing your SOC and getting "left of bang".

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.