Deloitte.

Adaptive Defense: Custom Alerts for Modern Threats

Introduction

As cyber threats rapidly evolve, the need for resilient and adaptive security measures has not been more critical. Traditional Security Operations Centers (SOCs) have long counted on out-of-the-box (OOTB) alerting systems—preconfigured software tools that come equipped with generic, signature-based detections—to identify known threats. However, as cyber adversaries continually refine their tactics, techniques, and procedures (TTPs), these standard alerting tools often fall short of effectively detecting sophisticated attacks. This white paper explores the imperative shift towards intelligence-led threat detection (ILTD) within the framework of a next-generation SOC (next-gen SOC) in Cyber Operations, emphasizing the limitations of conventional OOTB alerting mechanisms and the enhanced capabilities offered by tailored intelligence-driven approaches.

Next-gen SOCs represent a paradigm shift in how cyber threats are managed, prioritizing a proactive and strategic use of intelligence to anticipate, identify, and respond to threats before they manifest into breaches. To remain a step ahead of advanced threat actors, SOCs should consider integrating ILTD as a core component of their operational strategy. By leveraging customized threat intelligence, these centers can enhance their detection capabilities, improve response times, and reduce the risk of significant damage. ILTD is a qualitative approach, building detection rules based on their alignment with adversaries' real-world behavior. This approach contrasts with the traditional quantitative methods that focus merely on the volume of signature rules implemented.

The average company leverages **76** security tools, generating billions of events a day.[1]

Methods to implement ILTD for next-gen SOCs

Security teams cannot realize next-gen SOCs without ILTD. Therefore, transitioning from OOTB alerting systems to an ILTD approach involves several strategic steps that can significantly enhance an organization's cybersecurity posture.

Initially, organizations should conduct a current-state assessment of their security infrastructure and detection capabilities, identifying gaps and areas of improvement. This assessment should include an evaluation of the existing threat landscape specific to the industry and the vulnerabilities of the business. By combining organizational telemetry with threat intelligence, detection engineers can fill security gaps and write relevant detection use cases for an organization's environment, based on the threats targeting their assets while leveraging and maturing existing toolsets.

In Deloitte's experience, organizations too often focus only on a small subset of assets, the crown jewels (e.g., intellectual property, valuable data, or critical systems required to perform business operations), lacking a thorough overview of the threat landscape. Although we advocate that these assets require ample protection, they may not be the intended target of a sophisticated attack. For example, businesses might not consider client usernames and passwords to be crown jewels per se compared to intellectual property, but cybercriminals target usernames and passwords to use in credential stuffing attacks. This leaves the organization exposed to advanced threats with gaps in coverage.

Therefore, the development and integration of a tailored threat intelligence framework is crucial. This framework should leverage both external data sources (e.g., open-source information and community sharing groups about emerging threats) and internal data sources (e.g., internal vulnerabilities, risks, and operations) to build a detailed threat database that is continuously updated and refined. Intelligence analysts who excel in their role understand their organization, business operations, and what constitutes threats to it, allowing them to find and associate threat intelligence with the requirements of detection engineers and security personnel in next-gen SOCs. Therefore, training the cybersecurity team in the nuances of intelligence analysis is another critical step, honing an analyst's tradecraft to effectively interpret and act on the intelligence gathered.

A survey found that a lack of visibility or context from security tools resulted in **47%** of attacks being missed in a 12-month period.[2]

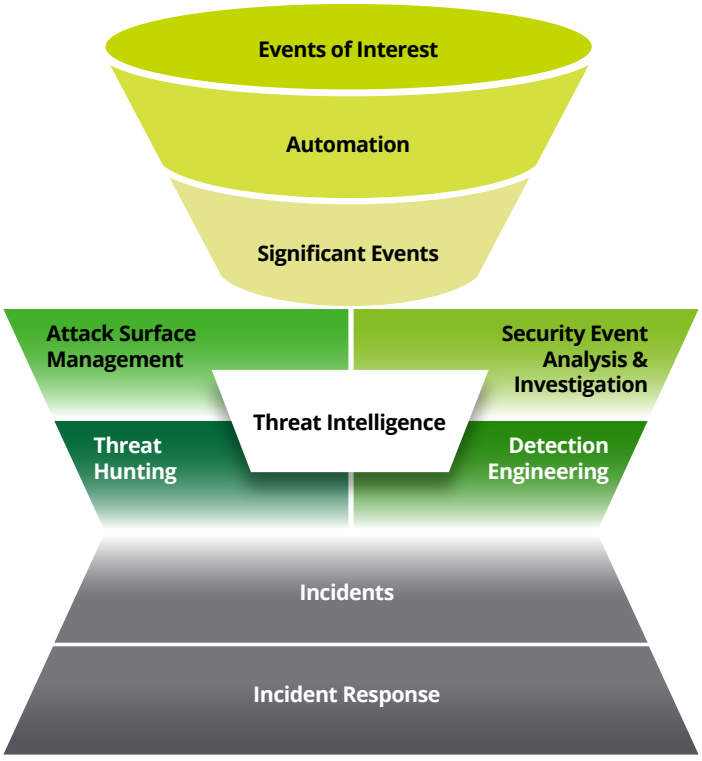


Figure 1: *A skills-based SOC with threat intelligence at the forefront*

Fostering collaboration across departments and with external entities can enhance the contextual understanding of threats and improve the organization's overall security posture. It is essential to establish a feedback loop between cyber threat intelligence and detection engineering, where insights from detected threats are utilized to refine detection strategies and intelligence operations.

When intelligence analysts prioritize applicable threats to build ILTD systems, they follow a meticulous process that combines risk assessment with strategic intelligence analysis. This begins with identifying and categorizing threats based on their potential impact and the likelihood of occurrence, tailored to the specific business context and industry vulnerabilities. Analysts utilize a rich mix of sources, including historical incident data, current threat landscape analysis, and predictive intelligence, to forecast pertinent threats. The prioritization process often employs a scoring system that weighs factors such as threat severity, asset value, and organizational readiness, enabling a quantifiable approach to threat ranking.

The intelligence provided allows detection engineers to develop alerting thresholds combined with risk scores to trigger alerts for specific threat actor behaviors. This allows security analysts in next-gen SOCs to better manage and prioritize alerts, which is crucial because a single behavior associated with a threat actor might trigger thousands of alerts that in hindsight are only part of normal baseline activity. It is only by synthesizing various alert thresholds that a clearer picture emerges, indicating the presence of an adversary within the environment, reducing alert fatigue, and mitigating advanced threats.

Next, continuous monitoring of the cyber environment allows analysts to adapt and recalibrate their priorities based on emerging trends. This dynamic approach makes certain that the ILTD framework remains responsive and aligned with the evolving nature of cyber threats, focusing resources and defensive measures on significant and probable risks.

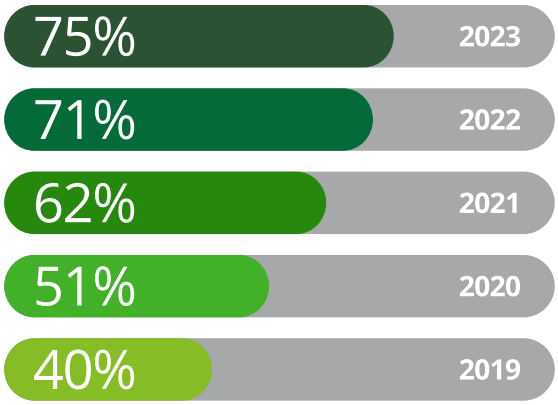
To measure the effectiveness of the ILTD approach, we emphasize monitoring through continuous consumption of threat intelligence and efficient client case management strategies that address false positives or misleading and unclear rules. The effectiveness of a rule may vary significantly from day to day as the threat landscape evolves and less sophisticated threat actors enhance their tactics. Owing to the qualitative vs quantitative analysis that is crucial for SOCs. Therefore, security teams collaborate closely, periodically updating detection strategies with new threat intelligence to maintain relevance in a dynamic threat environment.

91% of businesses believe a far-reaching and catastrophic cyber event is “at least somewhat likely in the next two years” due to global geopolitical instability.[3]

Case studies

Deloitte urges organizations to not underestimate our adversaries' motivations and to match proactive defense strategies with threat actors' relentless pursuits. While defenders may have the chance to correct mistakes, threat actors depend on their achievements for their livelihood, fueling a high level of determination.

When determining the below case studies, we highlight two prominent state-sponsored threat actors over cybercriminals (and ransomware groups). State-sponsored threat actors are more difficult to detect as they relentlessly pursue exclusive target sets, and they operate with stealth and persistence; whereas cybercriminals are easier to detect since they prioritize opportunistic attacks on a broad array of victims with speed for financial gain.



Malware-free activity[4]

Volt Typhoon

Posing a significant threat to US national security, Volt Typhoon is a regional Chinese threat group that is observed targeting the US defense and critical infrastructure sectors, including energy, telecommunications, and water systems. Volt Typhoon employs various techniques to achieve its objective, exclusively leveraging living-off-the-land (LOTL) techniques and hands-on-keyboard activity. These techniques blend into normal network traffic, making malicious activity extremely difficult to detect and mitigate, especially when depending on standard OOTB detections. This trend continues to grow, as malware-free activities increase. Threat actors are trending to identity-based attacks (e.g., phishing, social engineering, and access brokers) and exploitation of vulnerabilities and valid accounts.

Next-gen SOCs implementing ILTD work across teams to address Volt Typhoon's advanced capabilities. Threat intelligence teams, analyze and assess these activities, sending detection engineers indications and warnings of Volt Typhoon's TTPs. Detection engineers then develop alerting thresholds combined with risk scores for monitoring Volt Typhoon's malicious behavior. This supports prioritizing alerts and confirming certain thresholds are met before triggering an alert. Ultimately, this allows security analysts in next-gen SOCs to better manage and prioritize alerts, which is crucial as a single event associated with a threat actor's behavior can trigger thousands of alerts, contributing to longstanding alert fatigue issues that have long plagued traditional SOCs. It is only by understanding the behaviors of an advanced threat and synthesizing various alert thresholds that a clearer picture emerges, indicating the presence of an adversary within the environment.

90% of cybersecurity professionals find it is harder to detect an insider threat vs an external threat.[5]

This is a significant finding as advanced threats leverage valid accounts and LOTL techniques.

Sandworm

Sandworm (aka APT44) is a threat actor that is attributed to the Russian General Staff Main Intelligence Directorate (GRU) military agency. Sandworm is known for its aggressive attack capabilities across political and military contexts that present a significant threat to global governments and critical infrastructure where Russian interests intersect. Sandworm's destructive capabilities, risk tolerance, and far-reaching mandate to advance Russia's interests, place governments, civil society, and critical infrastructure operators at risk of advanced attacks with short notice. Sandworm tends to use exploits to compromise edge infrastructure and infiltrate into a target environment. Like Volt Typhoon, Sandworm will then deploy open-source tools and use LOTL techniques to perform reconnaissance, move laterally, and collect information from target systems.

In one instance, Deloitte defenders identified Sandworm activity after detecting an anomalous instance of a masqueraded TeamViewer binary. TeamViewer is a maintenance software tool that uses remote access and remote control. The defenders determined it was malicious after observing that the binary was executed from a temp directory, which is inconsistent with the known operational behaviors of legitimate TeamViewer software. The discovery of Sandworm activity followed the consumption of intelligence reports that provided defenders with indicators of compromise (IOCs) and behavioral analysis that were crucial to setting up initial detection parameters.

Future outlook

Moving forward, organizations will increasingly leverage cyber threat intelligence with detection engineering functions to improve their cybersecurity posture. Emerging technologies also provide several use cases that can advance ILTD. For instance, artificial intelligence (AI) can comb through massive amounts of data about a threat actor's activities inside a network, enabling quick analysis of a threat actor's prevalence within an environment.

Additionally, AI can explain how dozens of seemingly unrelated activities translate into threat actor behavior, speeding up the process of identifying behavioral facts about the threat and allowing defenders to focus time and attention on defense strategies across targeted environments.

Lastly, automating the generation of attack scenarios and running simulations can confirm the effectiveness of the detection rules. This not only streamlines the confirmation process but also affirms that the detections are concentrated and can handle variations of the attack. These are use cases leveraging new technologies that will advance the interaction between cyber threat intelligence and detection engineering that is ILTD within a next-gen SOC.

69% of executives say they will use generative AI for cyber defense in the next 12 months.[6]

At Deloitte, Threat Intelligence is our compass in navigating the ever-evolving landscape of cyber threats. It's the distillation of evidence-based knowledge about both existing and emerging threats. Our Cyber Threat Intelligence (CTI) services help clients turn data into timely, actionable, relevant, and predictive intelligence to defend against advanced and persistent threats.

Connect with us

Lead authors

Will Burns
Deloitte US
Cyber Leader
Managing Director
Deloitte & Touche LLP
wburns@deloitte.com

Clare Mohr
Deloitte US
Cyber Threat Intelligence Leader
Vice president of solution delivery
Deloitte & Touche LLP
clmohr@deloitte.com

Stanley Parret
Deloitte US
Detection Engineering Manager
Deloitte & Touche LLP
sparret@deloitte.com

Emily Notariano
Deloitte US
Cyber Threat Intelligence Advisor
Senior Consultant
Deloitte & Touche LLP
enotariano@deloitte.com

Contributors

Alex Smith
Deloitte US
Detection Engineering
Senior Consultant
Deloitte & Touche LLP
alexandersmith8@deloitte.com

David An
Deloitte US
Cyber Threat Intelligence Manager
Manager
Deloitte & Touche LLP
davidan3@deloitte.com

Taryn Campion
Deloitte US
Hunt and Incident Response
Next-gen SOC Consultant
Deloitte & Touche LLP
tacampion@deloitte.com

Deloitte.

Endnotes

1 Staff, "Security Leaders Peer Report, Panaseer," 2022. [Online]. Available: https://panaseer.com/reports-papers/report/2022-security-leaders-peer-report/ [Accessed: 28 June 2024].

2 Staff, "CRA Business Intelligence, the research arm of CyberRisk Alliance, 2022. [Online]. Available: https://www.cyberriskalliance.com/press-release/cyberrisk-alliance-releases-2022-cybersecurity-year-in-review-report [Accessed: 28 June 2024].

3 Staff, "Global Cybersecurity Outlook," January 2023, World Economic Forum, [Online]. Available: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf [Accessed: 28 June 2024].

4 Staff, "CrowdStrike 2024 Global Threat Report," n.d. [Online]. Available: [https://go.crowdstrike.com/global-threat-report-2024.html [Accessed: 28 June 2024].

5 Staff, "Insider Threat Report," Securonix, 2024. Online. Available: https://www.securonix.com/resources/2024-insider-threat-report/ [Accessed: 28 June 2024].

6 Staff, "Global Digital Trust Insights," PwC, 2024. Online. Available: https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html. [Accessed: 28 June 2024].