Cybersecurity
INSIDERS

Transforming SOC Operations:

How TacitRed Curated Threat Intelligence Boosts Analyst Efficiency and Delivers Tactical Attack Surface Intelligence

The increasing sophistication, targeting, and volume of cyber threats facing organizations, coupled with attack surface management dynamics, requires cybersecurity solutions to move towards curated findings that help security teams become more efficient in handling the increased likelihood of exposures, attacks and breaches. This does not necessarily mean building out a bunch of AI prompts.

Modern security tools like Extended Detection and Response (XDR) have significantly improved SOC capabilities over the years. These tools progress detection and response by integrating various data sources and providing a comprehensive view of the threat landscape. Additionally, advancements in Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms have streamlined security operations, allowing for enhanced incident management .

Today's Cybersecurity Challenge

Despite substantial investments in cybersecurity tools, the number of successful attacks is increasing. Over 80% of cyber breaches result from external threat actors conducting phishing, session hijacking, account takeover, and malware attacks - putting organizations under mounting pressure to improve their security posture and automate cyber response. This increase in successful attacks stems from an ever-expanding attack surface combined with increasing coordination and advancement of attack methods.

Factors contributing to the expanding attack surface include the use of multi-cloud services, distributed applications, unaccounted-for internet-facing assets, siloed technology acquisitions across business units, and broader supply chain dependency - all introducing more potential attack points for cyber adversaries. Criminal and state-sponsored adversaries are taking advantage of attack surface soft spots with increasingly AI-gen augmented attack methods to exploit susceptible users and vulnerabilities in systems to accomplish their objectives.

The sheer size, scope, and velocity of attacks and issues are inundating security analysts with alerts—often exceeding 11,000 per day for large organizations—leading to missed exposures, delayed action, and analyst burnout. Conventional threat intelligence tools provide security teams with relevant information, but still requires analysts to exert consideration assessment, research, and inference workload. Even with alert reduction capabilities, analysts must exert effort to examine, investigate, and validate. This overload has real-world consequences, as seen in notable breaches where overwhelmed analysts were unable to prioritize and focus on the most serious threats. For example, in the case of the 2023 T-Mobile data breach, crucial threats were missed due to the SoC team struggling with prioritizing alerts and managing threats, leading to data exposure that affected millions of customers. Other breaches, such as the 2024 Mintlify and Acer Philippines, demonstrate threat actor sophistication and third-party risk.

Continuous Threat Exposure Management (CTEM)

Given this reality, organizations are adopting more proactive processes and advanced security tools that enable security operations teams to respond faster and enable their companies to become more resilient against rapidly evolving threats. One innovative approach is Continuous Threat Exposure Management (CTEM), which focusing on workflows processes to mitigate potential threats before they escalate.

Introduced by Gartner in 2022, CTEM addresses the limitations of reactive vulnerability management by proactively anticipating threats. In a nutshell, CTEM operates through a cyclical process of five key stages: Scope, Discover, Prioritize, Validate, and Mobilize. This structured methodology ensures that organizations not only identify and understand their attack surface but also respond to risks and remediate vulnerabilities in a more strategic and proactive manner.

- **Scope:** Define the organization's total attack surface and risk profile, including internal and external vulnerabilities.
- **Discover:** Utilize advanced tools to identify potential threats and vulnerabilities within the defined scope.
- **Prioritize:** Rank threats based on their likelihood of exploitation and potential impact on the organization.
- **Validate:** Confirm the existence and severity of identified threats using techniques like automated penetration testing and breach simulation.
- **Mobilize:** Implement remediation measures for validated high-priority threats, ensuring alignment with business objectives and effective communication across departments.

Balancing Security Posture and Defense

CTEM strikes an important balance between maintaining a robust security posture and being capable of dynamic response. This balance is crucial because a purely defensive stance may leave organizations vulnerable to novel attack vectors, while a focus solely on response may lead to unaddressed vulnerabilities and missed threats. By integrating posture and response, CTEM enables organizations to prioritize and address the most critical vulnerabilities in real time, aligning security efforts with business objectives and operational realities.

The Need for a Better Approach

As discussed earlier, traditional threat intelligence sources and assessment tools fall short in refining the signal-to-noise ratio, covering the extended attack surface and managing threat volume and sophistication. This still leaves analysts coping with how to more efficiently triage and respond to the deluge of often irrelevant, inaccurate, and outdated alerts and intelligence data – often missing truly critical findings.

To bridge this gap, TacitRed was developed by continuous intelligence solutions provider Cogility to empower security teams with tactical attack surface intelligence. Unlike traditional tools that often overwhelm analysts with data, TacitRed delivers fully curated, prioritized, and detailed findings on pertinent cyber issues. This allows security teams to take immediate, decisive actions on compromised and at-imminent-risk assets to mitigate exposures.

Tactical Attack Surface Intelligence with TacitRed

TacitRed continuously monitors, maps, and analyzes an organization's external attack surface, offering an on-demand assessment of an organization's security posture and providing curated, valid, and detailed active threat findings.

As a turnkey, Software-as-a-Service (SaaS) solution, TacitRed automatically maps an organization's external attack surface and correlates connections and threat activity between its digital presence, cyber adversaries, and third-party entities.

Security operations, security analysts, and risk analysts can instantly examine curated attack surface risks and active issues of over 18 million U.S. entities on demand by simply entering a business domain name. Users can examine compromised and imminent target assets and novel attack findings categorized by severity, threat type, and cyber kill chain stage. The on-demand, accurate, and actionable intelligence with full contextualization sets TacitRed apart from conventional, query-based external attack surface management tools.

Attack Surface Intelligence Process

TacitRed's approach to attack surface intelligence can be summarized in five key steps that are closely aligned with the principles of Continuous Threat Exposure Management (CTEM) model discussed earlier, which serves to anticipate and mitigate potential threats before they can escalate:

- **Inventory:** Continuously maps and analyzes internet-facing assets, while dynamically monitoring the connections and threat activity and active exploits.
- **Discover:** Identifies compromised and at-imminent-risk assets, helping security teams understand the overall security posture of their organization's external attack surface. A calculated Threat Score based on active threat actor activity informs analysts about the extent of assets that are compromised or are at imminent risk and require priority action.

- **Investigate:** Provides comprehensive, curated findings enabling analysts to readily examine compromised and high target assets with full contextual details of affected machines and users, prioritized by severity and categorized within the cyber attack chain stage. This allows analysts to focus their investigation on valid security issues with high fidelity.
- **Respond:** Expedites mitigation efforts by sharing curated findings with incident response teams, including asset severity rating and detailed exposure evidence. The system enables the integration of active attack surface asset enumeration and threat findings to existing SIEM, SOAR, and IT Asset Management tools via API.
- **Extend:** Enables security teams to assess their extended attack surface of third-party entities, such as subsidiaries, partners, suppliers, agents, and service providers. By sharing threat scores and critical security insights, organizations can facilitate corrective actions to reduce supply-chain risk.

An Example of How AI Unleashes the Full Potential of Threat Intelligence

Leveraging Expert AI and event stream processing technologies, TacitRed is able to deliver accurate, actionable threat intelligence at scale. At the heart of TacitRed is Cogility's patented Hierarchical Complex Event Processing (HCEP) analytic. It applies pattern-matching logic at machine speed to dynamically process billions of streamed records each hour through its cloud-scaled event stream processing engine - while maintaining state. By synthesizing available industry threat intelligence with proprietary sources, such as domain and internet routing registries, malware and botnet logs, bulletproof hosting, C2 node identification, and internet traffic sampling, TacitRed provides the best possible curated threat insights that can enable organizations to respond to and prevent incidents. The Expert AI behavioral analysis identifies active cyber attacks, including threat actors, targeted entities, exposed assets, compromised credentials and sessions, and malware activities. Additionally, TacitRed evaluates third-party risks and presents actionable results with similar details as first-party risk assessments.

> "The interface is straight-forward and purposely uncomplicated. The speed, depth, and usefulness of threat detail from TacitRed is astonishing – saving us considerable time and potential claim loss," according to Ross Warren, VP of E&O and Cyber at ATRI Insurance Services.

This is presented in a simple, intuitive SaaS GUI allowing analysts to ascertain risk, examine active compromised and target assets, and mobilize mitigation efforts using detailed threat contextualization – or to push findings to other internal systems via API.

Conclusion

TacitRed is a game-changer in delivering tactical attack surface intelligence that can help organizations realize the promise of Continuous Threat Exposure Management. The SaaS solution's ability to provide continuous, curated, prioritized and detailed active security findings empowers security teams to assess active threats faster and mitigate them more efficiently. By enhancing security analyst capacity and capability, the tool can help fortify the way SOC operations manages external attack surface risk.

For more information, visit https://tacitred.com and check out their free 30-day trial at https://tacitred.com/trynow

Holger Schulze – founder and principle analyst, Cybersecurity Insiders
Scott Gordon (CISSP) – chief marketing officer, Cogility Software