WHITE PAPER

Modern External Attack Surface Management:

Optimizing Cyber Incident Response Capacity and Speed

Any discussion of incident response today would be incomplete without first understanding the nature of an organization's external attack surface and the solutions designed to manage and protect them. External Attack Surface Management (EASM) is a critical cybersecurity practice focused on identifying, monitoring, and managing the internet-facing assets of an organization. By providing continuous visibility into an organization's external attack surface, including third parties, supply chains, and other critical assets outside the purview of traditional IT management, EASM helps organizations to proactively detect and remediate security exposures.

With today's rapidly evolving threats, organizations face an increasing volume and sophistication of cyber-attacks. The expanding attack surface, driven by the adoption of multi-cloud environments, distributed applications, and extensive third-party dependencies, makes it challenging for security teams to manage their attack surface and respond efficiently to threats and attacks. Security analysts are inundated with alerts, often exceeding 11,000 per day for large organizations, leading to missed exposures and delayed responses. Traditional threat intelligence tools provide a wealth of data but often lack the context needed to prioritize threats accurately. This overload can have serious real-world consequences, such as the notable breaches at T-Mobile and Acer Philippines, where overwhelmed analysts were unable to prioritize and respond to threats before they became noteworthy incidents.

To address these challenges, organizations are increasingly adopting advanced security tools and frameworks in the hope of enhancing their incident response capabilities. Extended Detection and Response (XDR) integrates various data sources to provide a comprehensive view of the threat landscape, while Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms streamline security operations and incident management. Continuous Threat Exposure Management (CTEM), introduced by Gartner in 2022, is a proactive approach that anticipates threats through a cyclical process of scoping, discovering, prioritizing, validating, and mobilizing. This structured methodology ensures that organizations can identify, understand, and respond to risks in a strategic and proactive manner. However, while these tools and frameworks have significantly improved SOC capabilities, they still require significant effort from analysts to examine, investigate, and validate threats. The sheer volume of alerts, along with the complexity of modern threats, can overwhelm even the most well-resourced SOCs, leading to analyst burnout and reduced effectiveness.

Despite advancements in cybersecurity tools and methodologies, several gaps remain. One significant gap is the lack of actionable, curated intelligence that would help security teams better prioritize and resolve the most critical threats. Traditional threat intelligence sources often overwhelm analysts with data, requiring considerable effort to triage and investigate alerts that might, or might not, be real threats.

Additionally, many security tools lack comprehensive visibility into an organization's external attack surface, leaving blind spots that attackers can exploit. Another gap is insufficient coverage. The dynamic nature of cyber threats means that static, periodic assessments are inadequate, necessitating continuous monitoring and real-time intelligence to stay ahead of attackers. Finally, there is a significant lack of intelligence context between various security tools, leading to fragmented insights and delayed responses. These gaps often result in operational inefficiencies and missed opportunities for early detection and remediation — allowing threats to escalate and cause considerable damage.

TacitRed, developed by Cogility, addresses these challenges and gaps with its modern External Attack Surface Management (EASM) solution. TacitRed empowers security analysts to take immediate, decisive actions to mitigate impactful cyber exposures by providing unparalleled tactical attack surface intelligence that is fully curated, prioritized, and detailed. The SaaS solution uniquely ingests and analyzes global internet and threat intelligence of both entities and adversaries continuously using data stream analytics, offering actionable insights into over 18 million U.S. businesses. Subscribers can examine compromised and at-imminent-risk assets with threat scoring and extensive findings context. The findings are available on-demand, just by entering a target entity's domain name. Analysts can drill down into the details or have them automatically sent via API to enrich the EASM intelligence of their existing SIEM, SOAR and other solutions.

TacitRed continuously monitors and maps an organization's external attack surface, even as it grows and changes over time, providing real-time assessments of its security posture. As part of this process, TacitRed uniquely applies intelligence synthesis, a technique that dynamically analyzes terabytes of proprietary and public internet, threat traffic signal, and intelligence data sources. By identifying active security issues, TacitRed helps security teams understand their overall security posture. The solution categorizes threat findings by severity and attack stage, allowing analysts to focus on the most critical issues. Early attack stage exposures enable teams to take a preemptive response, whereas later stage exposures facilitate containment action. Detailed supporting evidence, including full contextual details of affected machines and users, enables efficient and coordinated remediation of a broad range of threats, including phishing attacks, session hijacking, malware infiltration, account takeovers, and other exploits targeting internet-facing assets.

TacitRed tactical attack surface intelligence delivers fully curated, prioritized, and validated findings – providing comprehensive context on pertinent security issues that sets it apart from conventional EASM tools. The SaaS solution provides visibility to an organization's external attack surface and enumerates active attacks and imminent threats. By negating often irrelevant, inaccurate, and outdated threat data, security teams can more effectively and efficiently streamline investigation, containment, and resolution processes.

TacitRed

Visit **www.tacitred.com** to take a tour, request a demo – or better yet, to register to try TacitRed for free.

TacitRed
15495 Sand Canyon Ave. #150
Irvine, CA. 92618

sales@cogility.com
+1 949.398.0015