WHITE PAPER

TacitRed

Modern External Attack Surface Management:

Simplify, Automate, and Reduce Third-Party Risk

Organizations increasingly rely on third-party vendors and partners to support various business functions. While these collaborations drive innovation and efficiency, they also introduce significant cybersecurity risks. Third-party risk management (TPRM) is crucial to protecting access to sensitive resources and information. This is where External Attack Surface Management (EASM) solutions come into play. This paper explores the challenges of assessing third-party risk, the approaches to managing it, the gaps within existing tools, and how TacitRed by Cogility addresses these challenges and limitations effectively.

Let's start with a brief description and basic expectations of EASM. External Attack Surface Management is a security best practice focused on identifying and monitoring an organization's internet-facing assets and detecting their vulnerabilities and active exposures. By providing continuous monitoring and assessment of an organization's external attack surface, as well as those of third parties which are outside the purview of IT management, EASM helps security teams gain security posture intelligence and context to proactively mitigate security issues.

An organization's external attack surface comprises not only the assets they own and threats they must manage themselves, but also extends to subsidiaries, partners, and supply chain members that have some business or digital connection to the primary organization. Many organizations struggle to monitor and evaluate the cybersecurity posture of their third-party vendors at all, let alone continuously. This lack of visibility can lead to blind spots, allowing unidentified exposures to create entry points for cyberattacks that may ultimately lead back to the primary organization.

Another significant challenge is the sheer volume of data and analysis during the assessment process. Large organizations can have anywhere from a few hundred to thousands of third-party relationships. Each third-party entity, just like the primary organization, has a dynamic digital footprint that can be vulnerable to being exploited. For example, a third-party threat, such as compromised credentials, can result in unauthorized system access and account takeover. Their exposure can lead to a direct attack on the primary organization. The constant evolution of cyber threats and cyber adversaries further complicates this process, as new vulnerabilities and attack methods can emerge rapidly.

Conventional approaches to automate TPRM are varied but have significant limitations. Manual audits based on compliance checklists and security questionnaires can provide a wealth of risk insight, but are labor-intensive and time-consuming. Extending this method to third parties and partners similarly employs compliance certifications and attestations. This approach can only be attempted periodically and relies heavily on the accuracy and honesty of responses, often resulting in inconsistent or incomplete data. Passive vulnerability scanning of internet-facing assets can uncover specific weaknesses, but this testing still requires resources and expertise for effective management. TPRM platforms aim to automate the process by aggregating scanning, threat intelligence, and other data sources, but their effectiveness hinges on the quality, depth, and timeliness of this data and analysis.

Unfortunately, findings from conventional TPRM and EASM tools often yield irrelevant threats and partial details. Without sufficient threat context, organizations remain uncertain about the severity of security issues. This requires additional validation that burdens security teams. As organizations expand their third-party relationships, these challenges also magnify. Worse, these tools don't provide enough useful context for the third-party to take meaningful action. Conventional TPRM and EASM tools still fall short on providing up-to-date, accurate, and comprehensive insights into an organization's dynamic external attack surface.

TacitRed leverages Expert AI and real-time data processing to provide tactical attack surface intelligence. Unlike conventional EASM, TacitRed processes massive, diverse, streamed data sources in real-time to detect and prioritize active cyber issues at machine-speed. It applies an intelligence synthesis technique, whereby terabytes of proprietary and public internet, threat traffic signals, and threat intelligence data sources are assessed. This results in accurate and timely third-party risk profiles. These profiles include an overall threat score, as well as extensive security findings.

TacitRed continuously monitors and analyzes the external attack surfaces of over 18 million U.S. business entities. Organizations can readily obtain on-demand findings of their partners, subsidiaries, and suppliers, just by entering a company's domain name. This up-to-date threat intelligence, combined with fully curated, validated, and detailed findings, allows teams to assess third-party risk with greater speed, depth, and scalability.

TacitRed significantly reduces the noise, errors, and accuracy issues that plague conventional TPRM and EASM tools. The solution automatically prioritizes active compromises and imminent threats, presenting curated findings that include the type of attack, its exploitation stage, and full contextualization. This enables security analysts to skip the laborious process of filtering and validating data to streamline security risk assessment. It also enables the organizations to inform third-party vendors of security issues with details that are valid, pertinent, and actionable. This allows security analysts from the organization and the third-party to communicate more effectively to expedite threat response. This benefits third parties and bolsters the overall security posture of the primary organization.

TacitRed also addresses the issue of scalability. As organizations add more third-party vendors, their digital footprint expands, and the volume of threat data to be analyzed increases. TacitRed's advanced technologies ensure that the solution can scale to accommodate this growth without compromising on finding integrity or performance.

In summary, third-party exposures are the conduit for unauthorized access and cyber-attack. TacitRed overcomes the challenges and limitations of current TPRM and EASM tools by offering continuous external attack surface monitoring, analysis, and active threat detection — with greater risk insight, threat context, and scalability. The curated, prioritized, and detailed findings automate and fortify risk assessment capabilities without further burdening security teams. More so, it allows organizations to share pertinent findings with their third-party security counterparts to effectuate overall risk reduction

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

sales@cogility.com
+1 949.398.0015