WHITE PAPER

TacitRed

Modern External Attack Surface Management:

Enabling Fast and Accurate Cyber Insurance Risk Assessment

As the digital landscape continues to evolve, so do the threats that organizations face. Cyber insurance has become an essential part of risk management strategies, offering financial protection against cyber incidents. However, accurately assessing cyber risk remains a significant challenge for insurance risk assessment managers, making it difficult to optimize premiums and avoid excess claims exposure. Cyber insurance demand continues to grow rapidly, and organizations want timely replies from carriers and agents to answer premium and coverage inquiries. To remain competitive, accuracy must be accompanied by speed and resource efficiency. A modern External Attack Surface Management (EASM) solution can provide a comprehensive approach to address these challenges and optimize risk assessment processes.

The challenges in cyber insurance risk assessment are multi-faceted, from sourcing and managing the volume and complexity of available threat intelligence that is involved in the assessment, to the pressures of responding quickly to inquiries and creating informed quotes. Assessments need to determine the extent of susceptibility to ransomware, denial of service, account takeover, sensitive and personal data exfiltration, and more. This incorporates potential extortion, business liability, and privacy compliance penalties. Cyber threats are continually evolving, with new vulnerabilities and attack vectors emerging at an alarming rate. This dynamic environment makes it difficult for assessment analysts to keep pace and accurately evaluate an organization's risk to cyber-attacks and breach.

Traditional risk assessment methods often rely on a combination of application checklist forms and the use of varying external scanning tools. Applications can provide a wealth of risk factors by asking a variety of organization, governance, certification, and operational security questions, in addition to business details and historical incident information. This use of attestation to gauge cyber risk relies heavily on the accuracy and honesty of responses. While providing an initial risk litmus test to compare against industry data, additional independent, technical security assessment is required. Achieved certifications and compliance does not necessarily equate to low cyber risk.

There are many threat intelligence data sources and security scoring tools to choose from including passive and active vulnerability scanning of internet-facing assets to uncover specific weaknesses. While providing some sense of asset vulnerability risk, the results are only for a point-in-time and often require expertise to interpret. Security scoring and Third-Party Risk Management (TPRM) platforms aim to expand and automate the risk assessment process by periodically aggregating scanning, threat intelligence, and other data sources. Unfortunately, their effectiveness hinges on the quality, depth, and timeliness of their data and analysis, which can leave gaps in understanding an organization's actual risk profile. In many cases, the risk scoring and actual findings are inaccurate, irrelevant, or outdated. These tools often miss newly exposed assets or active attacks and threats — leading to an incomplete, unverified,

and potentially surface-level evaluation that impact cyber insurance risk assessment. When applicants are provided such findings, it also places an added burden on the applicant's IT staff to validate and resolve items that predominantly have low impact on actual risk mitigation. This issue is compounded by the fact that organizations frequently adopt new technologies and expand their digital footprints, further limiting TPRM results.

To address these challenges, cyber insurance risk assessment managers must adopt more advanced and dynamic technical assessment approaches that complement security questionnaires. One effective strategy is the use of modern external attack surface management (EASM) solutions that provide continuous monitoring and real-time analysis.

EASM 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 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 greater security posture intelligence and provides context to proactively mitigate security issues. For the cyber risk insurance analyst, it provides the means to significantly enrich the assessment process.

Automated threat monitoring allows for the detection of new vulnerabilities, threats, and attacks as they emerge, providing a more accurate and up-to-date picture of an organization's risk profile. The ability to aggregate multiple threat intelligence sources enables assessors to more easily view findings that are current and relevant — avoiding more tedious, manual assessment methods. Despite these advancements, conventional TPRM and EASM approaches limit cyber risk assessment efficiency and efficacy.

One significant gap is the lack of comprehensive visibility into an organization's entire attack surface. The periodic scanning and detection of known potential vulnerabilities often miss new assets and active attacks and threats. Another gap is the challenge of validating and prioritizing threats. Many solutions pull threat data, such as potential stolen credentials, from the various sources including the dark web. But much of this data is unsubstantiated. With the vast amount of threat information generated, it can be difficult to distinguish between critical threats and benign exposures — such as outdated SSL certificates. This can lead to an overload of information, making it challenging for risk assessment managers to focus on the most pressing security issues.

Finally, there is often a disconnect between the data generated by risk assessment tools and the actionable insights needed for effective risk mitigation. Many tools provide questionable findings with insufficient context, leaving risk assessment managers, as well as a customer's security staff, to manually interpret and prioritize the findings. This can be time-consuming and prone to errors, reducing the efficiency and effectiveness of the risk assessment process.

How TacitRed Overcomes the Challenges and Gaps

TacitRed, developed by Cogility, is a modern EASM solution designed to address the challenges faced by cyber insurance risk assessment managers. By providing continuous, real-time analysis into an organization's external attack surface and delivering fully curated findings, TacitRed ensures that risk assessment analysts can quickly and easily understand their customer's active security exposures that can be exploited or have been exploited by cyber adversaries.

TacitRed leverages Expert AI and real-time data processing to provide tactical attack surface intelligence. Unlike conventional TPRM and EASM tools, TacitRed processes massive, diverse, streamed data sources in real-time to detect and prioritize impactful 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 risk profiles. These profiles include an overall threat score, as well as extensive security findings.

TacitRed continuously monitors over 18 million U.S. organizations' external attack surfaces, offering a detailed and dynamic view of an organization's risk profile. This continuous monitoring overcomes the challenges of periodic assessments, false positives, and inaccurate threat information. The approach ensures that exposures and attacks are detected with valid, supporting evidence. Cyber risk analysts can literally get a current profile of a business entity, on-demand, just by entering its domain name. Having instant access to this curated threat intelligence expedites and fortifies risk assessment processes. This also allows for more frequent internal review cycles, especially before term renewal, to see if a client's cyber-attack prevention and resiliency efforts have improved or degraded.

Beyond a threat score, subscribers can examine compromised and at-imminent-risk assets with extensive findings context. This includes details of phishing attacks, session hijacking, malware infiltration, account takeovers, data exfiltration, and other exploits targeting internet-facing assets and susceptible users. This allows risk assessment managers to quickly understand the nature and impact of each threat and make informed decisions about the acceptable risk and type of coverage. Additionally, analysts can provide findings with confidence, supported by enough details for their customers and prospects to initiate impactful threat and attack mitigation efforts.

Analysts can drill down into the details or have them automatically sent via API to enrich the EASM intelligence of their existing quoting and other solutions. The seamless integration with existing tools further enhances the efficiency of the risk assessment process, enabling automation and coordinated underwriting response. By addressing these challenges, TacitRed empowers cyber insurance risk assessment managers to optimize their processes, improve the accuracy of their risk evaluations, and offer better-informed policies to their clients. This enhances the competitiveness of cyber risk insurance providers and enhances the protection provided to insured organizations.

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