WHITE PAPER

TacitRed

MSSPs Considerations for Evaluating EASM Solutions

As Managed Security Service Providers (MSSPs) seek to expand their service offerings and enhance the efficiency of their security operations, the selection of a modern External Attack Surface Management (EASM) solution becomes crucial. With cyber threats evolving rapidly, MSSPs must address various challenges while leveraging advanced technologies to remain competitive in the service business. This paper explores the key considerations for MSSP business managers when evaluating EASM solutions, focusing on the challenges, existing approaches, gaps, and how TacitRed effectively addresses these issues.

MSSPs face several challenges in maintaining and enhancing their security services. First, acquiring and retaining clients is an ongoing concern. Clients are seeking MSSPs with extensive service offerings that allow organizations to outsource a wide variety of operational security risks. MSSPs must be able to offer strategic advice, while managing popular security tools owned by the customer and provide innovative tools and services that cover cyber defense gaps.

As cyber threat actors are constantly devising new tactics, techniques, and procedures to breach defenses, it is imperative for MSSPs to stay ahead of these threats and deliver confidence to their clients. The reality is that MSSP customers will be attacked and exploited. These customers rely on their MSSP to demonstrate security posture improvement but will gauge their MSSP on mean time to detect (MTTD) and mean time to remediate (MTTR) incident response.

Another significant challenge is the scarcity of skilled cybersecurity professionals. Hiring and retaining qualified security analysts is increasingly difficult, leading to resource constraints within MSSP operations. This shortage of talent can result in overburdened analysts who must manage vast amounts of alerts, threats, and intelligence data, often leading to inefficiencies and potential oversight — and turnover.

Moreover, limited visibility into a client's dynamic external attack surface is a significant hurdle which is exacerbated by the associated risks introduced by their partners, agents, and suppliers. MSSPs must ensure they have accurate and real-time insights into pertinent attacks and threats against a clients' internet-facing assets, susceptible users, and supply chain. External Attack Surface Management (EASM) solutions aim to provide this intelligence that is typically outside the purview of IT management.

Traditional approaches to attack surface management typically involve extensive data collection and analysis. Analysts are encouraged to gather as much attack surface and threat intelligence data as possible to support risk assessment and threat response. However, this approach often leads to an overwhelming volume of data, making it difficult and time consuming for analysts to efficiently identify and prioritize genuine threats. In-house built internet scanning tools and threat intelligence sources to map attack surfaces and detect vulnerabilities can identify some of a client's internet-facing asset exposures, but this method is often inconsistent and may not provide accurate or up-to-date details. More so, it requires expertise and maintaining different tools to support the process.

Several gaps exist in conventional EASM approaches. One significant gap is the high noise level generated by outdated, inaccurate, and irrelevant threat data. Analysts must spend considerable time sifting through this noise to identify, investigate, and validate potential exposures, which hampers their ability to respond swiftly to pertinent security issues. Furthermore, it often presents irrelevant signals that pale in significance to active, high-priority attacks. This results in wasted resources and delayed responses.

Additionally, conventional EASM solutions do not adequately address the risks introduced by third-party and supply chain entities, leaving organizations vulnerable to indirect attacks — and in turn, blindsiding MSSP analysts.

The above challenges underscore the need for a modern EASM solution that can optimize analyst productivity and enhance threat detection and response capabilities.

Enter TacitRed.

TacitRed, a tactical attack surface intelligence solution from Cogility, offers a transformative SaaS approach to addressing these challenges and gaps. Unlike conventional EASM solutions, TacitRed provides fully curated, prioritized intelligence that enables MSSPs to take immediate, decisive action.

TacitRed leverages Expert AI and real-time data processing to analyze massive, diverse, streamed data sources 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 advanced approach eliminates the noise by delivering only validated signals, allowing analysts to focus on active exploits and imminent threats.

TacitRed provides full contextual details that enable efficient mitigation of a broad range of threats, including phishing attacks, session hijacking, malware infiltration, account takeovers, and other exploits. This enables MSSP analysts to streamline investigation, containment, resolution, and prevention processes. By reducing the volume of irrelevant data and providing fully curated intelligence, TacitRed enhances analyst efficiency and accelerates response times.

One of TacitRed's key strengths is its ability to provide continuous, real-time monitoring of over 18 million U.S. business entities. MSSP analysts can readily obtain findings of their client's attack surface, including third-party and supply chain risks, on demand. This provides MSSPs tremendous flexibility to offer immediate and on-going external attack surface insights for their clients.

TacitRed offers a straight-forward analyst dashboard, allowing clients and MSSP analysts to easily see threat scores and drill down to examine threat details. Furthermore, TacitRed can integrate with existing MSSP systems, like SIEM, SOAR, and other tools to enable greater operational efficiency and a cohesive defense strategy. These integrations ensure that attack surface intelligence is shared across tools and teams, enhancing coordinated threat detection, analysis, and response workflows.

In summary, TacitRed enables MSSPs to extend their service portfolio to existing and new customers. It empowers MSSPs to overcome the limitations of conventional EASM approaches by providing continuous, curated, and comprehensive threat intelligence and comprehensive visibility into external attack surfaces. By automating the detection, prioritization, and enumeration of active attacks and imminent threats, TacitRed enables MSSPs to optimize their security operations, enhance analyst productivity, and accelerate mitigation effectiveness – to the benefit of their organization and their clients.

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