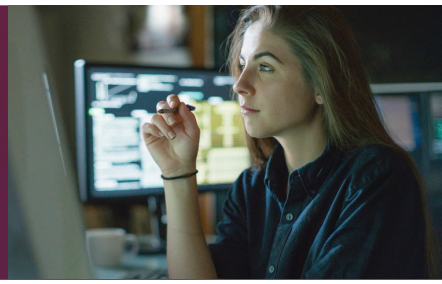
CHECK POINT

STRATEGIC CONSULTING GROUP

External Risk Management



External Risk and Importance of EASM

The cybersecurity threats are increasingly sophisticated and pervasive, organizations must be vigilant in managing their external attack surface – the aggregate of all the possible entry points or vulnerabilities through which an unauthorized user can enter an organization's digital environment. External Attack Surface Management (EASM) focuses on identifying, analyzing, and securing these vulnerabilities from potential cyber-attacks, thus forming a crucial component of an organization's cybersecurity strategy.

Managed External Attack Surface Assessment

Continuous and automated asset discovery and contextualization are essential due to the diverse and evolving nature of digital assets exposed to the internet. Comprehensive visibility into an organization's digital footprint, including assets owned by subsidiaries and third parties, mitigates the risk posed by unknown or untracked digital assets, which represent the most common threat vector.

Managed EASM as a service , solves these issues by providing real-time insights and enabling scalable, accurate, and timely responses to emerging threats, without consuming SOC resources. The service is delivered by experienced security analysists part of the Red Team, through the frequent reports sent or contacting in case of critical vulnerability is being discovered. This dramatically reducing manual effort and leading to more effective vulnerability management and risk prioritization.

How to Analyze an Attack Surface

The analysis of the attack surface involves several steps, starting from the external asset inventory and the acquisition of context, which is continuously updated. Then, payloads tailored to asset specifications are developed to meet risk detection requirements. These payloads are sent to the asset via a distributed network of test systems. Finally, the results are validated, compiled, and made available through accessible interfaces. These processes are automated, consistent, and scalable, thus increasing the depth and breadth of cyber security assessment.

Main Features:

1. **Discovery:** Utilizes extensive open-source intelligence (OSINT) to identify digital assets and build a comprehensive globalnetwork view of an organization's attack surface. This includes identifying subsidiary companies, cloud resources, and otherinterconnected entities.
2. **Contextualization:** Offers insights into the business context of identified assets, including their role, sensitivity, andrelevance to the organization. This helps in understanding the asset's importance and the potential impact of itscompromise.
3. **Active Security Testing:** Employs over 25,000 attacks, including significant coverage of common vulnerabilities like the OWASP Top 10, to evaluate assets' security. This approach, combined with discovery and contextualization ensures testing across the entire external asset inventory without any impact on asset resources.
4. **Prioritization:** Allows security teams to identify and prioritize vulnerabilities based on the asset's business context,discoverability, attractiveness to attackers, and other critical metadata. This targets efforts toward the most significantrisks, imroving efficiency.
5. **Remediation Acceleration:** Facilitates faster issue resolution through continuous, automated testing providing organizations the confidence in their remediation efforts and reducing the mean time to remediation.

Assessment: Inputs, Process, and Outcome

The assessment starts with the input of the organization's digital landscape's data into the system. The primary domain name is enough to start, though additional information (i.e. about cloud environments) can additionally improve results.

This data undergoes analysis through steps including reconnaissance, discovery, contextualization, vulnerability analysis, and active security testing. The process involves the automated gathering and classification of assets, generation of payloads, testing, and evidence collection, all supported by machine learning (ML) and natural language processing (NLP) technologies for scalability and accuracy.

The outcome is an in-depth and consistent understanding of the organization's external attack surface, highlighting vulnerabilities and misconfigurations for prioritization and remediation. This systematic approach provides a high-confidence level in the organization's cybersecurity posture, ensuring that security teams can focus on the most meaningful issues, enhancing operational efficiency, and significantly reducing the risk of breaches.

The External Attack Surface Assessment can be delivered as an one-time test or continues annual subscription to the service.

Assessment Phase	Activity
1. Business Scoping	Uncover and map organizational structure
2. Recon / Discovery	Uncover IP ranges and domains Typical scope Scan IP ranges and build asset inventory Gather OSINT on assets Classify assets Add business context to assets Add attribution (organizational ownership) to assets
3. Vulnerability Analysis	Identify CVEs through software versions (CPEs)
4. Prioritization	CVSS Asset discoverability Asset attractiveness Threat intelligence
5. Testing / Exploitation	Payload-based active tests / DAST Assets tested (typical) Classify data sensitivity High risk exploitation activities
6. Reporting / Recommendations	Findings list and Executive summary Remediation planning