Criminal IP ASM

Criminal IP

Proactive Prevention Through
a Risk-Based Response Strategy

Why Attack Surface Management (ASM) is Essential for Cybersecurity

What is Attack Surface Management (ASM)?

Attack Surface Management (ASM) is a comprehensive security strategy designed to identify all digital assets within an organization, continuously detecting and managing externally exposed vulnerabilities in real time. The proliferation of cloud technologies, IoT devices, and remote work has rapidly expanded digital assets, creating new opportunities for hackers to target hidden assets and services.

ASM evaluates and prioritizes asset risks, enabling the efficient allocation of security resources to proactively prevent security incidents. It also enhances regulatory compliance and supply chain security while minimizing potential damage through real-time detection and response. ASM goes beyond simply enhancing security; it plays a pivotal role in fostering business con dence and maintaining competitiveness.

Why Should Attack Surface Management be Implemented?

The cloud transformation and expansion of digital infrastructure have induced global distribution of organizations' IT assets, continuously exposing unexpected ports and services. In such a complex environment, accurately pinpointing and managing the location and condition of all assets has become increasingly difficult.

Gartner and Forrester emphasize the importance of Continuous Threat Exposure Management (CTEM), noting that organizations implementing Attack Surface Management (ASM) typically discover that over 30% of their assets were previously unrecognized ones.

Attack Surface Management (ASM) mitigates security risks by identifying undetected assets and potential threats in real time, prioritizing them based on risk, and proactively addressing them.

Gartner

« "ASM is a new solution that helps organizations identify risks associated with internet-connected assets and systems that they may be unware of."
"The organizations that prioritize security investments based on CTEM programs by 2026 can reduce two-thirds of all security incidents." ».

「Gartner Top 10 Strategic Technology Trends for 2024」

FORRESTER

« "Some ASM tools discovered several hundred percent more cloud assets than organizations thought they were using, and on average, attack surface management tools initially discover 30% more cloud assets than security teams know they have" ».

「2022 ASM Report: Find and Cover Your Assets with Attack Surface Management」

What Elements can Attack Surface Management Detect?

Attack Surface Management (ASM) offers comprehensive detection of a diverse range of assets and potential vulnerabilities, both externally and internally within an organization.

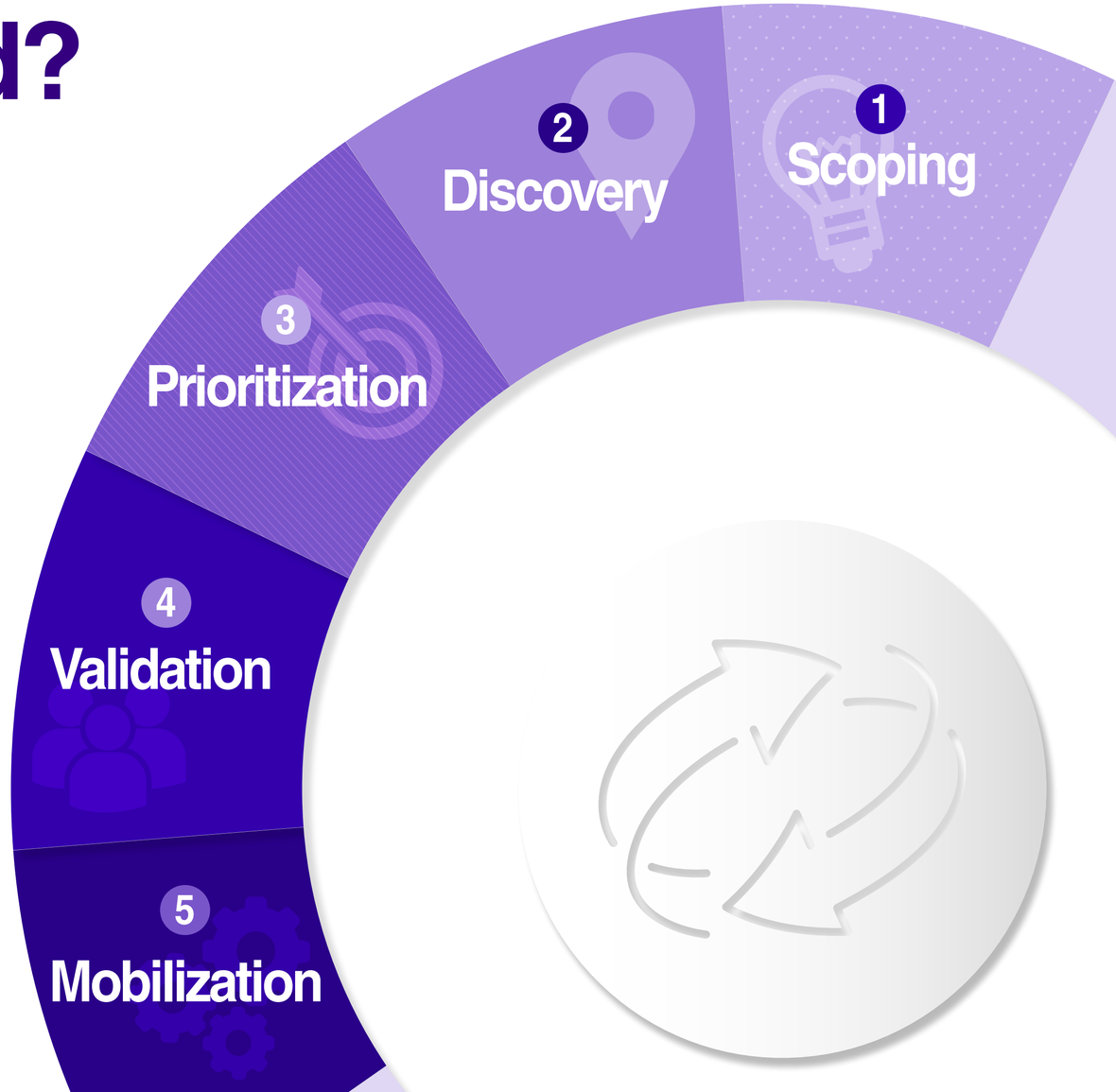
ASM enables a proactive security response by detecting a wide range of blind spots that are difficult to identify through traditional security assessments.

How are Threats Detected?

Attack Surface Management (ASM) is an **AI-powered automation technology** that operates 24/7/365, detecting all assets and vulnerabilities within an organization in real-time. Even if a server is deployed in a **hard-to-reach location**, ASM will **detect the asset the following day** and issue warnings regarding potential security risks.

Automated scanning tools, **Open Source Intelligence (OSINT) techniques, cloud API integration, web crawlers, AI-powered data analytics,** and other technologies work together to quickly and accurately detect hidden assets and vulnerabilities.

This **continuous and intelligent detection** identi es blind spots often overlooked in traditional security checks, enabling a proactive response.



Differences Between Attack Surface Management and Vulnerability Assessment

Attack Surface Management (ASM) and Vulnerability Assessment share the same security objectives, but they differ in their approach and scope.

Scope & Operational Approach

Vulnerability assessments focus on already identified assets, whereas ASM continuously detects and manages the entire asset landscape, including hidden ones, using automation tools operating 24/7 in real time.

Detection Target

While vulnerability assessments focus on CVE-based vulnerabilities, Attack Surface Management (ASM) addresses a broader range of threats, including domains, cloud assets, third-party resources, misconfigurations, and exposed sensitive information.

Supply Chain Security

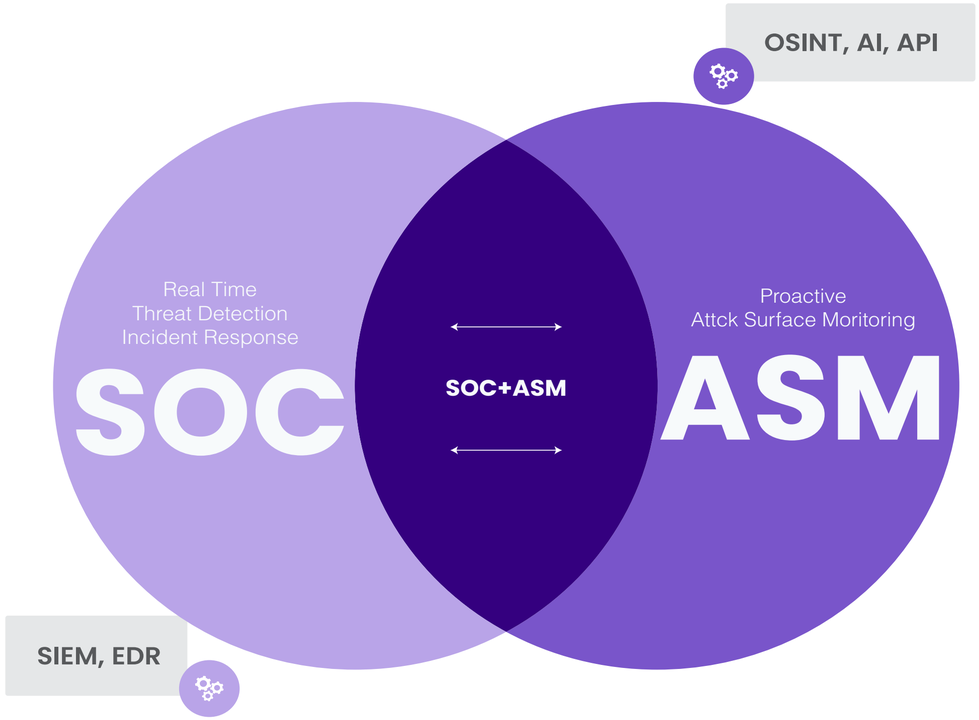
While vulnerability assessments focus on internal assets, Attack Surface Management (ASM) also includes assets from subsidiaries, partners, and third-party vendors, offering a comprehensive approach to supply chain risk management.

ASM is a comprehensive security strategy that addresses the limitations of vulnerability assessment and proactively manages organizational security risks.

Understanding the Relationship Between SOC and ASM

The Security Operations Center (SOC) is responsible for monitoring **real-time security events**, detecting abnormal behavior, and managing incident response. Attack Surface Management (ASM), on the other hand, continuously detects and **proactively prevents** vulnerabilities in an **organization's assets, both external and internal** through automation tools and AI.

While SOC, **SIEM, and EDR** tools focus on reactive security responses, ASM emphasizes **proactive measuresusing** technologies such as **OSINT, cloud API integration**, and other advanced tools. SOC focuses on **internal security events**, whereas ASM manages the **entire attack surface, including external assets and supply chains**. SOC focuses on real-time threat detection and incident response,whereas **ASM** is a proactive security strategy that emphasizes asset discovery ASM complements the proactive areas that SOCs may overlook, providing a more comprehensive view of an **organization's security posture and strengthening its defenses.**

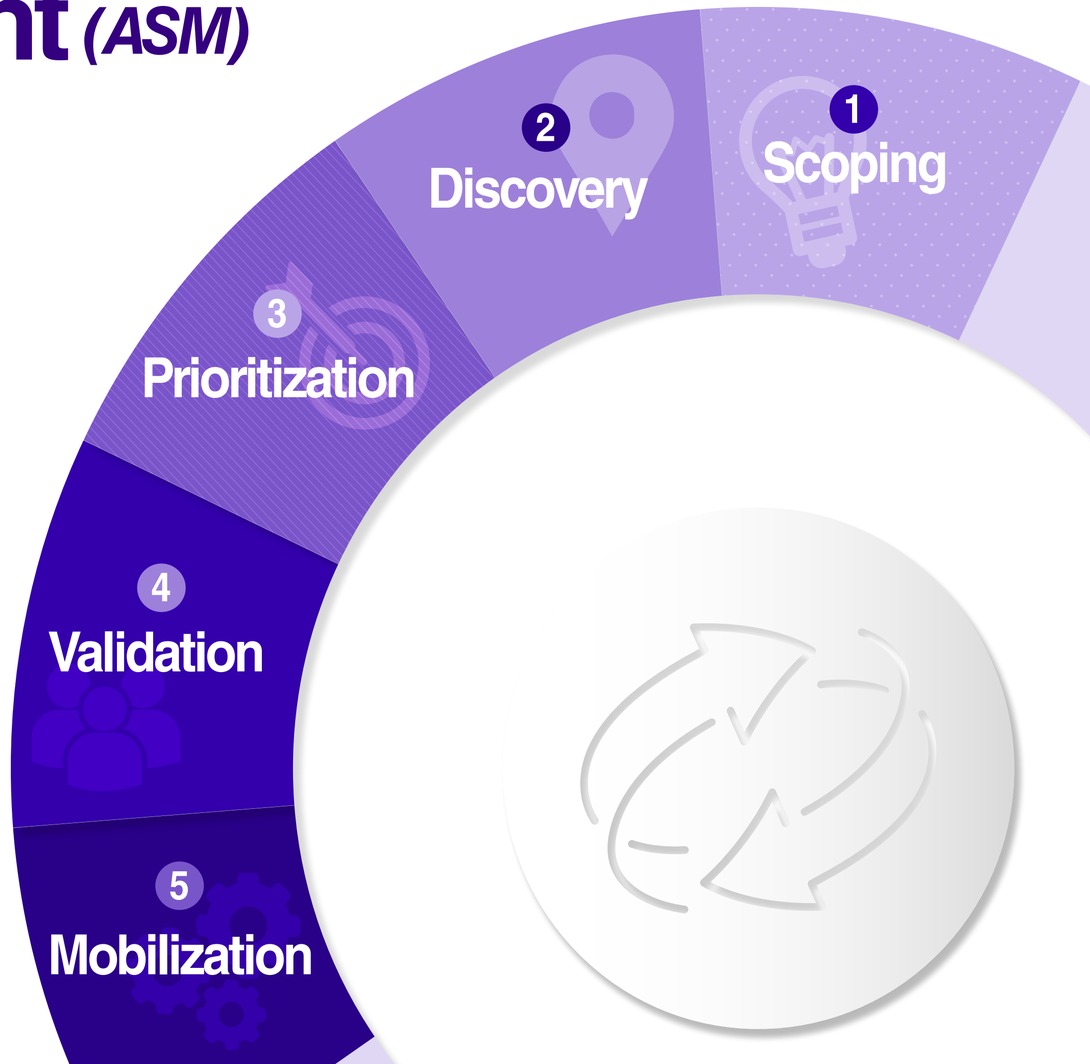


Proactive Security Strategy for the Future: Attack Surface Management *(ASM)*

With cloud transformation and the expansion of digital infrastructure, organizations' assets are becoming increasingly distributed worldwide, while security threats are rising at a rapid pace. Traditional security postures are insufficient for managing all assets and vulnerabilities in the rapidly evolving cloud environment.

Attack Surface Management (ASM) is a crucial security strategy that detects and proactively addresses hidden assets and potential threats in real time, even within complex environments. In the era of cloud computing, Attack Surface Management (ASM) is no longer a luxury but **an essential cornerstone of cybersecurity.**

By adopting ASM, organizations can build a stronger, more adaptive security posture to meet the challenges of a dynamic threat landscape.



Criminal IP ASM

About Criminal IP

Criminal IP is an OSINT search engine specialized in attack surface assessment and threat hunting. It offers extensive cyber threat intelligence, including device reputation, geolocation, IP reputation for C2 servers and scanners, domain safety, malicious link detection, and APT attack vectors via search and API.

Learn more at criminalip.io

Thank You

Why Attack Surface Management (ASM) is Essential for Cybersecurity

Proactive Prevention Through a Risk-Based Response Strategy

Terms of Use

Privacy Policy