EASM Solution Brief

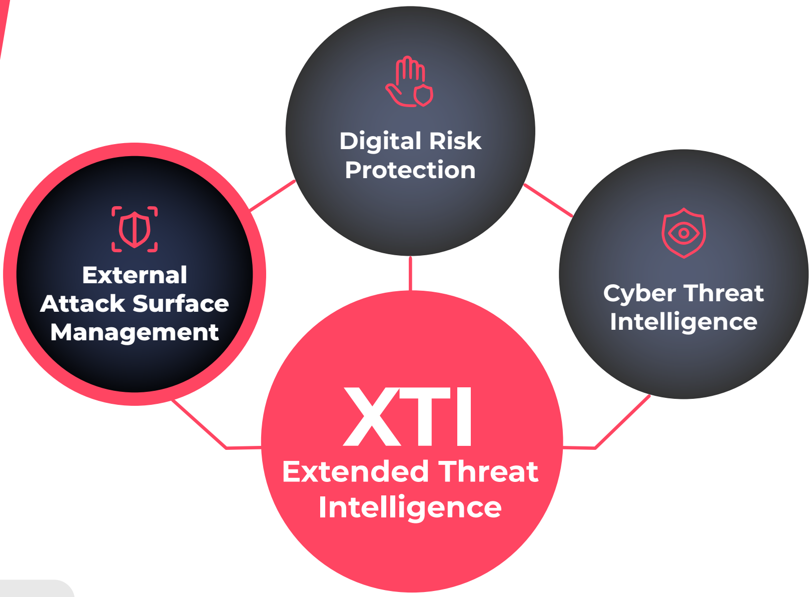
External Attack Surface Management

Gain Visibility with Hacker Mindset

External Attack Surface Management (EASM) is a cybersecurity practice of **identifying, assessing** and **mitigating** vulnerabilities with potential attack vectors that exist outside of an organization's perimeter. The process involves conducting regular security assessments, implementing appropriate security controls, monitoring external systems to **proactively hunt potential threats** and **regularly patching software systems** to address known vulnerabilities.

As the digital landscape continues to evolve, organizations are extending their presence across multiple platforms and mediums, leading to an expansion of their attack surface. This growth not only includes official channels, such as corporate websites and applications, but also **social media platforms, cloud configurations** and **third-party services. The rise of digital touchpoints** has made **External Attack Surface Management (EASM)** increasingly vital. By implementing **EASM,** organizations can **proactively identify vulnerabilities** in their expanding digital footprint and take the necessary steps to **mitigate potential threats,** thereby **ensuring robust cybersecurity** in a rapidly evolving digital world.

External Attack Surface Management


Digital Risk Protection
External Attack Surface Management
Cyber Threat Intelligence
XTI
Extended Threat Intelligence

EASM aims to reduce an organization's **exposure to cyber attacks** while minimizing the impact of security incidents by identifying and addressing weaknesses that attackers could potentially exploit. The **digital assets,** linked to the internet, carries a potential risk of exposure that can cause a **data breach.** To mitigate the threats against those attacks, organizations must **ensure the convenient security practices** to reduce the number of vulnerabilities that attackers can exploit. By constantly monitoring the **evolving and expanding attack surface,** organizations can significantly **lower the risk** of a successful attack with EASM.

By employing our **External Attack Surface Management (EASM)** solution to analyze your organization's attack surface, you gain comprehensive insight into a diverse array of **assets, including websites, applications, cloud configurations, social media platforms** and **third-party services.** This empowers organizations to accurately assess the threat level of their **external-facing assets** and adopt the **most effective cybersecurity practices** to mitigate risks.

Organizations must assume a **proactive stance** in their defense strategy by persistently managing and reducing their external attack surface. This strategic approach effectively **thwarts potential intrusions, preemptively obstructing malicious attempts** before they can compromise the organization's cyber security. Effective External Attack Surface Management requires a **proactive** and **comprehensive approach** to identifying, assessing, prioritizing, and mitigating risks to ensure the security and integrity of an **organization's systems and data.**

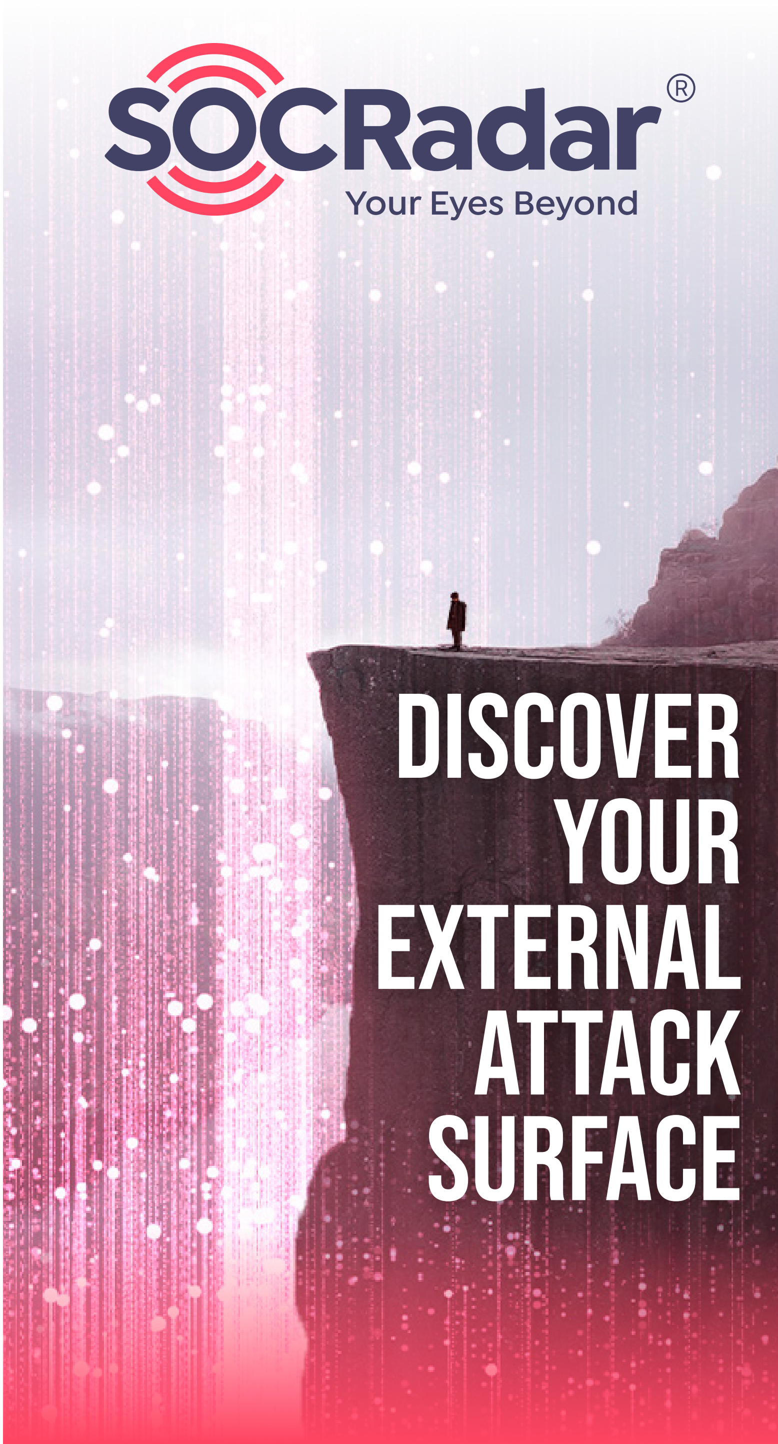
A lack of comprehensive External Attack Surface Management (EASM) implementation, or lapses in its execution, can expose organizations to a multitude of risks, including **data breaches, service disruptions, malware infections** and **phishing attacks.** These security incidents can result in significant **financial losses** and **long-lasting reputational harm,** emphasizing the importance of a robust and well-executed EASM strategy for protecting your organization's valuable assets and maintaining stakeholder trust.

SOCRadar's EASM

Discover, Prioritize and Remediate

SOCRadar's **Extended Threat Intelligence (XTI) provides EASM** service that can help organizations **reduce their attack surface, prioritize their security efforts** and **proactively manage** their cyber risks with a **hacker mindset.** The platform identifies and manages their **digital assets, including websites, web applications, APIs, cloud instances** and **third-party assets.**

SOCRadar's EASM service proactively **tracks down external vulnerabilities** across the **accessible internet** and **the dark web.** This service equips your organization with crucial information about potential exposures, **safeguarding sensitive data** by diligently scanning and monitoring your external digital assets. It also detects the **digital footprint** of companies using only the main domain address information and can automatically extract the asset inventory by classifying it. By monitoring the assets that make up the attack surface, it enables us to follow the attacker and **prevent possible attacks.**



What sets SOCRadar's EASM service **apart** from the competition is our unique approach to **asset detection** and **discovery.** While other EASM providers typically request a list of digital assets from their clients, **SOCRadar only requires the domain name.** Emulating **a hacker's mindset,** our service starts with the domain name and delves into the web to **uncover digital assets,** just as a **potential intruder** would. This method allows us to detect even those assets that the organization itself may not be aware of. Our philosophy is simple: Hackers don't ask for a list of your assets, they find them. And so do we, helping you **stay one step ahead in the cybersecurity landscape.** EASM, **one of the three services provided by SOCRadar's XTI,** helps customers **gain broader visibility** and **context** regarding the severity of unknown internet-facing digital assets in an automated manner. The module provides security teams with direct visibility into all **internet-facing technological assets** in use and assets attributed to **IP, DNS, domain** and **infrastructure** through advanced **internet-wide monitoring algorithms.**

TRACKS DOWN EXTERNAL VULNERABILITIES ACROSS THE ACCESSIBLE INTERNET AND THE DARK WEB

SOCRadar's EASM also has the skill of detecting and managing **shadow IT activities** which refers to usage of technology systems, software, or services without the explicit **approval of IT teams.** Employees or departments who independently purchase and deploy technological solutions to address their own needs, **bypass conventional IT standards** and **security measures,** violate the principles of IT procedures and can **cause external attacks.**

Leveraging automation, SOCRadar not only meticulously maps out the external attack surface, but also **proactively sends warning alerts** to customers and users about assets at risk. Through our innovative EASM module and sophisticated monitoring algorithms, organizations acquire an **unprecedented level of visibility** and context for their current and future attack surfaces, eliminating the need to manually inventory digital assets. This level of automation streamlines the process, allowing organizations to focus more on **strategic security initiatives.** It further ensures continuous vigilance, with **real-time alerts** enabling swift response.