A SOC Guide to Attack Surface Management

Introduction

Teams inside security operation centers (SOCs) have a lot on their plate. Threats are multiplying and evolving, their organization's digital infrastructure is sprawling and complex, many assets are outdated or configured improperly, and employees accidentally create shadow IT. The issues are endless. To effectively handle challenges like these, one proactive tactic SOCs have implemented is attack surface management (ASM).

There's a simple way to explain this approach: find and correct vulnerabilities and exposures before adversaries find them. The fewer the risks, the fewer the attacks a SOC has to mitigate. Finding these risks—fully and quickly—is challenging in itself. However, ASM makes it happen.

What Is an Attack Surface?

Essentially, this is all the organization's public-facing assets that can be found on the internet by adversaries. Attackers can scan the entire internet for vulnerable systems in minutes, and they're constantly looking for a way into your network. Any internet-accessible asset could have an exposure that gives attackers a chance to get in. This includes IP addresses, domains, certificates, clouds, systems, services, data, devices, IoT and more.

Adding to the challenge, an attack surface is like shifting sand. It's constantly changing and hard to track. Employees are working remotely more than ever; software and data are shifting to multiple clouds; and assets are inherited through mergers and acquisitions (M&A). Supply chain partners improperly secured are accessing your network, while employees are using unauthorized software, devices and clouds. Then there's the task of knowing who's responsible for these assets and the remediation of any risks found on them.

What Is Attack Surface Management?

ASM performs several critical functions to give a SOC the visibility needed to ensure security across an organization. It provides a complete, up-to-date inventory of all assets—both known and unknown. It continuously finds potential vulnerabilities, and it offers risk prioritization. In the case of Cortex® Xpanse™, it also integrates with tools like Cortex XSOAR for the automated handling of alerts. This includes routing alerts to the responsible stakeholder or initiating remediation efforts.

Tracking Down the Unknown

There are many assets a SOC simply doesn't know exist. How can you protect what you don't know is there? In 2021, MIT Technology Review Insights found that 50% of organizations surveyed had experienced a cyberattack on an unknown or unmanaged asset, while another 19% expected an attack.[1] Adversaries will attack vulnerabilities, whether you know about them or not. In fact, unknown assets are more likely to have exposures that are not remediated for a long time, so there's a better chance they will be attacked.

Unfortunately, traditional vulnerability methods are outdated and simply not up to the task. What a scanner looks for can vary by product and may not catch all risks. Even more dangerous, scanners are only as good as the inventory of known assets an organization uses. They don't search and discover unknown assets, so they can't even scan them.

Teams should be looking from the outside in—the viewpoint of an adversary. Xpanse scans the entirety of IPv4 space for all assets (known and unknown) connected to an organization's network. In fact, Xpanse customers discover 35% more assets than they were previously tracking. As we all know, it only takes one rogue asset to make life difficult.

1. "A game changer in IT security", MIT Technology Review Insights, September 8, 2021, https://www.technologyreview.com/2021/09/08/1034262/a-game-changer-in-it-security/.

No Time to Dwell

A troubling thought to many SOC teams is that adversaries may be lurking within their digital ecosystem right now, and they don't even know it. Attackers continue to evolve their tactics to remain stealthy. The time they spend in your system before detection is dwell time. You want to ideally reduce dwell time to zero.

Additionally, security teams often focus on mean time to detect (MTTD) or mean time to respond (MTTR), but these metrics assume comprehensive asset inventories. If you have unknown assets with unknown risks, MTTD and MTTR are irrelevant. The focus should be on mean time to inventory (MTTI) first and foremost because MTTD and MTTR can't be reduced effectively without a single source of truth for internet-connected assets at the base of security operations.

Finding all your unknown assets is the first step. But then you have to keep your asset inventory up to date 24/7. Again, traditional methods have failed. Many times, asset inventories are updated only quarterly or, even worse, only during annual red team exercises or penetration testing.

Xpanse is automated to continuously scan your attack surface. You see what adversaries see as changes occur, lowering an organization's MTTI. This focus on the speed at which vulnerabilities are found helps prevent breaches altogether.

Outsprint Adversaries

A complete and up-to-date asset inventory is crucial for another reason: adversaries are constantly hunting for a way in. They have it automated, and they do it fast. They scan the entire internet for vulnerable systems in less than an hour.

Attackers also take advantage of announcements of Common Vulnerabilities and Exposures (CVEs). Once a CVE is announced, malicious actors normally search for that vulnerability in under an hour or even sooner if the issue is critical. On March 2, 2021, Microsoft announced vulnerabilities in Microsoft Exchange Server and Outlook Web Access (OWA). Threat actors started scanning for these vulnerabilities within five minutes, according to Xpanse research.

Efficient Remediation

Remediation used to be a highly manual process. It included determining who owned the asset, whether they could remediate the issue, and how remediation affected business.

With Cortex Xpanse, organizations are given a comprehensive, up-to-date inventory of all internet-connected assets—known and unknown. This inventory data is enriched with information on who owns the asset, potential exposures, risk prioritization, and why it was prioritized.

When integrated with tools like Cortex XSOAR, it allows for the automated handling of alerts. For example, you can automatically attribute a previously unknown asset and route the alert to the relevant stakeholders for remediation.

Learn more about how Cortex Xpanse works seamlessly with Cortex XSOAR here.

Summary

Attack surfaces are continually expanding and becoming more complex, requiring strong attack surface management. SOC teams need a comprehensive, up-to-date asset inventory 24/7. They need an efficient way to locate and prioritize vulnerabilities, and they need automated alerts. Only then can they take on the fiercest adversaries while focusing team resources on the most critical needs.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com