A Practical Guide to

ACTIONABLE ATTACK SURFACE MANAGEMENT

Sprocket Security | www.sprocketsecurity.com

TABLE OF CONTENTS

Casey Cammilleri
Chief Executive Officer
Sprocket Security

EXECUTIVE SUMMARY

Protecting an organization against cyberattacks is becoming more challenging these days as attack surfaces grow exponentially and attackers increase the sophistication of their tactics. Even one breach can *cost upwards of $4.88 million*[1] in monetary damages, and stolen customer data or company IP can result in priceless additional damages.

To stay ahead, security teams must shift from reactive response to proactive defense. But how do you protect assets you don't even know exist?

This is where *Attack Surface Management*[2] (ASM) comes in. ASM allows a security team to continuously discover, monitor, and assess all of their exposed assets—internal and external—and prioritize remediation based on real-world risk. ASM also forms the foundation of a strong Continuous Threat Exposure Management (CTEM) approach focused on reducing organizational exposure over time.

But ASM alone isn’t enough. To truly think and act like an attacker, you must integrate multiple facets into your ASM practices. This whitepaper examines how to leverage threat intelligence in your approach to ASM and validate data through Continuous Penetration Testing (CPT) to build a robust security posture that can prevent attacks before they begin.

#1

THE EXPANDING ATTACK SURFACE PROBLEM

As businesses grow, so do their IT environments, assets, services, networks, and more. But multiplying assets means increased opportunity for exploitation by malicious actors looking for unsecured areas of that attack surface. Attack surface expansion *is the top challenge impacting security practices*,[3] according to Gartner.

There are more factors contributing to expanding attack surfaces today beyond just expected organizational growth that regularly compounds assets, environments, and devices:

TESTING IN SHARED OR HOSTED INFRASTRUCTURE:

Today, a number of organizations use at least some cloud service or shared/hosted infrastructure, and they may have direct responsibility as an organization for the data secured within them. Yet they might not be able to authorize a security test against these resources. How can an organization effectively protect data if they cannot test for vulnerabilities in the same way an attacker will?

> *"From an attacker's perspective, public-facing cloud environments are an ever-shifting target that emphasizes the need for accurate targeting data."*
>
> **MICHAEL BELTON**
>
> Head of Service Delivery at Sprocket Security

DEPENDENCY COMPLEXITY:

Modern Single Page Applications (SPAs) can carry massive dependency trees due to frameworks like React, Vue, or Angular. Each update introduces potential vulnerabilities in nested libraries, and pentesters consistently discover outdated or unpatched modules hidden several layers deep.

GROWING SUPPLY CHAIN COMPLEXITY:

An organization's attack surface isn't just the assets that are unique to their organization, but extends to their supply chain as well. Gartner estimates that *nearly half of organizations have experienced attacks on their supply chain,*[3] three times the amount from 2021.

MICROSERVICES AND APIS:

Shifting to microservices can exponentially increase an application's footprint. Each service may have its own stack (Node.js, Python, Go), with configurations often left to individual teams. This fragmentation complicates ASM as new endpoints appear rapidly and are sometimes forgotten.

CLIENT-SIDE DATA EXPOSURE:

SPAs tend to offload significant logic and data into the client layer for seamless user experiences. However, there are often secrets or environment details in minified scripts or accessible source maps, which can be trivially reversed.

CI/CD MISCONFIGURATIONS:

Continuous Integration/Continuous Deployment (CI/CD) systems are a prime target because they often store the keys to production environments. Misconfigurations like storing credentials in plaintext environment variables or failing to scrub logs enable attackers to harvest secrets quickly.

TRADITIONAL SYSTEMS MANAGEMENT:

Beyond all of the sophistication and complexity happening at the application layer, it is important to remember fundamental system security concepts related to service isolation, least privilege and separation of privilege principles, secure network design, and much more. There is a big difference between a “vulnerability” and an “exploitable vulnerability.” Given the ever-shifting nature of a public-facing attack surface, a lack of focus on these aspects of system design can result in situations where exploitable vulnerabilities emerge.

> *“At Sprocket Security, we routinely identify systems that expose remote access services, database services, infrastructure services, and more.”*
>
> **NICK AURES**
>
> Senior Penetration Tester at Sprocket Security

As an organization grows, it’s only natural that their attack surface will grow too—but so do the opportunities for attackers to find entry points among the growing assets. Organizations need effective ways to manage and protect their attack surface.

#2

TURNING ASM VISIBILITY INTO ACTION

It's a challenge for any organization to maintain a continuously updated list of every asset, system, and device their organization touches—and it's even harder to do so in cloud and DevOps-heavy environments where new applications are constantly being deployed. Despite deploying ASM, many organizations still struggle to translate visibility into actionable security outcomes. In fact, fewer than *1% of companies today have visibility into 95% or more of their assets.*[4]

> *"ASM enables penetration testers to identify and remediate risks before attackers can exploit them. By continuously monitoring the external environment, we [testers] uncover and report critical vulnerabilities—often before organizations are even aware these assets are part of their infrastructure."*
>
> **JUAN PABLO GOMEZ P.**
> Senior Penetration Tester at Sprocket Security

To get the most value from ASM, teams must go beyond asset discovery and focus on how exposed systems evolve over time, where risks are emerging, and how changes in infrastructure map to potential attacker entry points.

The true strength of ASM lies in its ability to:

- *Surface unknown or forgotten assets that attackers can find before defenders do*
- *Track changes across your digital footprint to detect risk windows early*
- *Prioritize remediation by linking exposures to business-critical systems or known threats*

By leveraging ASM data as a live source of truth, security teams gain the ability to continuously track exposed assets, monitor changes across their digital footprint, and identify weak points in their external defenses. This is essential because attackers are constantly scanning the internet for vulnerabilities, often identifying and targeting assets before internal teams even know they exist. Any one of these assets—whether a forgotten subdomain, an exposed API, or a misconfigured cloud service—can become an entry point for exploitation.

ASM closes this gap by offering continuous discovery and assessment. But visibility alone isn't enough. The true power of ASM lies in how that visibility is translated into action. ASM data enables a range of high-value security outcomes—from prioritizing vulnerability remediation based on exposure, to guiding red team operations, supporting compliance audits, and powering a broader Continuous Threat Exposure Management (CTEM) strategy.

The key is context: ASM not only reveals what assets are out there, but how those assets behave, how they change over time, and whether those changes introduce new risk. For example, an asset that was secure last week might become vulnerable today due to a new deployment, configuration drift, or a newly disclosed exploit.

ASM is not just about building an asset inventory—it's about driving better security decisions:

- *Which vulnerabilities should be fixed first?*
- *Which exposures require continuous monitoring?*
- *Where should security resources be focused for maximum impact?*

When used effectively, ASM becomes a foundational layer of any proactive security program, helping organizations stay ahead of attackers by continuously aligning their defenses with the realities of their external risk surface.

OPERATIONALIZING ASM WITH CONTINUOUS PENETRATION TESTING

Visibility into your attack surfaces is a powerful starting point, but to truly reduce risk, that visibility must be validated. Continuous Penetration Testing (CPT) transforms ASM data from static discovery to active validation.

CPT is designed to perform ongoing monitoring, testing, and remediation of vulnerabilities that leave networks exposed to cyberattacks. Unlike traditional pentesting that offers a snapshot of one point in time, CPT delivers real-time information about how evolving threats could impact your organization.

By integrating ASM data into CPT workflows, security teams move past reactive fixes and begin to:

- ***Actively validate*** *which exposures are exploitable.*
- ***Cut through the noise*** *of alerts and surface real, impactful risks.*
- ***Maintain compliance*** *by testing frequently and continuously meeting audit requirements.*
- ***Focus remediation*** *efforts where they'll deliver the greatest impact.*

This operationalized approach creates a continuous feedback loop. ASM data feeds CPT, CPT generates real-world risk data, and human testers validate the findings. It's a cycle of discovery, validation, and response that bridges the gap between passive visibility and active defense, making ASM a true force multiplier for modern security teams. It's crucial to build a testing pipeline that combines automation with manual testing to achieve better, faster, and more accurate results.

#3

LAYING THE GROUNDWORK FOR CONTINUOUS THREAT EXPOSURE MANAGEMENT

To fully mature your security program, ASM must evolve into a core component of Continuous Threat Exposure Management (CTEM).

> *"CTEM is an emerging security management process that emphasizes continuous risk validation and remediation."*
>
> **MICHAEL BELTON**
>
> Head of Service Delivery at Sprocket Security

Unlike traditional threat management, which relies on periodic assessments, CTEM provides a framework through which security teams continuously monitor and manage potential vulnerabilities by focusing on real-time threat detection and response. According to Gartner, nearly half of organizations have experienced a supply chain attack—a threefold increase since 2021 and organizations that prioritize a CTEM approach to security will be *three times less likely to experience a breach.*[5]

This framework ensures that organizations don't merely react to incidents after they occur but continuously evaluate and strengthen their defenses to prevent attacks in the first place, significantly reducing the window of exposure to cyber threats. ASM is a critical first step to building a mature CTEM framework. Here's how it fits into the five stages of CTEM:

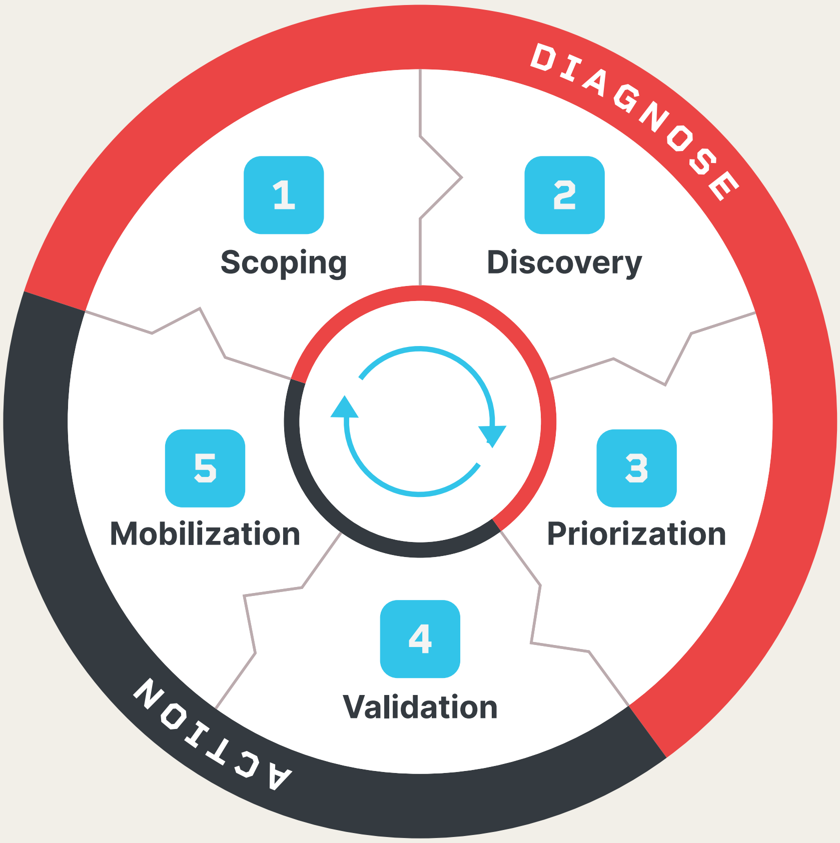
1. **SCOPING:** Start by defining the objectives and scope of threat management, including identifying risky or critical assets, as well as the resources and approach needed. ASM plays a key role in this stage of CTEM.

2. **DISCOVERY:** Using tools and techniques to identify networks, applications, and data, conduct a thorough inventory of digital assets and their exposure. ASM tools play a key role in this stage as well.

3 **PRIORIZATION:** Next, assess and rank the identified threats based on their impact, severity, and risk levels. This can help the security team better allocate resources to higher-priority efforts.

4 **VALIDATION:** By simulating real-world attacks, test the effectiveness of current security controls against the identified threats and pinpoint gaps for improvement.

5 **MOBILIZATION:** Finally, implement remediation actions like deploying patches and updates to mitigate the identified risks.



By implementing ASM as part of a robust CTEM approach, security teams aren't just adopting surface-level protection but are able to exact a full-scale threat management program that evolves with their attack surface.

#4

ENHANCING ASM & CPT WITH THREAT INTELLIGENCE

THE ROLE OF THREAT INTELLIGENCE IN ASM

Another way to stay one step ahead of attackers is by integrating threat intelligence into your ASM approach. Threat intelligence is the process of gathering, analyzing, and interpreting information about potential or existing cyber threats that could harm an organization. Threat intelligence helps security teams split theoretical or “coming soon” attacks versus what is being seen or actively exploited already, allowing for defenders to strategize in both the short term and long term.

Threat intelligence can be thought of as having two sides: the attacker’s side and the defender’s side. The attacker uses threat intelligence to understand things like what technology is commonly vulnerable and exploited, and how to identify more of those assets. The defender uses threat intelligence to understand what indicators of compromise look like. This can help proactively create defenses, or in less fortunate situations, prove a compromise has already occurred.

The attacker and defender likely can look at the same ASM data and use it to determine how to act accordingly. An attacker will know which items from their threat intelligence will apply to the ASM dataset, and it’s the same for the defender. It's either attack, or mitigate and defend.

THE ROLE OF THREAT INTELLIGENCE IN CPT

Once your attack surface is mapped, CPT focuses on actively probing that surface for real-world weaknesses. However, without threat intelligence, CPT risks becoming static. The same tests are repeated, regardless of what’s actually happening in the threat landscape.

Threat intelligence adds depth, relevance, and urgency to CPT. Instead of testing in a vacuum, security teams can align their efforts with current attacker behaviors, industry-specific threats, and high-priority vulnerabilities being exploited in the wild. This intelligence-driven approach transforms CPT into a dynamic, evolving test environment.

THE DIFFERENT TYPES OF CYBER THREAT INTELLIGENCE

Cyber Threat Intelligence (CTI) can be a powerful component of an information security program. In modern times, high-quality CTI sources are available as commercial and open-source offerings. In practice, there are three broad categories of CTI: **strategic, operational, and tactical.**

Strategic:

Strategic CTI provides a broad understanding of the current threat environment. As applied to information technologies, strategic CTI should inform decisions related to governance, resource allocation, operational prioritization, technical tooling, and more.

Strategic CTI Should Incorporate The Following Key Elements:

- *Threat actors, their motivations, and historical behaviors*
- *Technical trends that change the attack surface*
- *Industry-specific trends that might influence threats*
- *Geopolitical context that might influence threats*

Operational Benefits of Strategic CTI Include:

- *Threat prioritization and contextual analysis*
- *Indicator enrichment and proactive threat hunting*
- *Information sharing and collaboration*
- *Changes in monitoring priorities*

For maturing information security programs, strategic CTI can be a useful tool towards building a defense posture that rapidly adapts to a dynamic threat landscape.

Operational:

Operational CTI delivers timely, actionable insights into cyber threats to enable rapid and effective responses. It supports threat detection, incident response, and security tool optimization by providing specific data on indicators, attack methods, and vulnerabilities.

Operational CTI Should Incorporate The Following Key Elements:

- *Indicators of Compromise (IoCs) to inform threat detection*
- *Tactics, Techniques, and Procedures (TTPs) to understand methods*
- *Vulnerability and exploit intelligence to prioritize mitigation*
- *Incident and campaign context to assess active threats*

Benefits of Operational CTI Include:

- *Enhanced detection and alert triage*
- *Accelerated incident response*
- *Proactive threat hunting*
- *Dynamic tool optimization*

Operational CTI is a vital tool for building a defense posture that swiftly adapts to an evolving threat landscape through technical insights.

Tactical:

Tactical CTI provides immediate insights into cyber threats. With a focus on IoCs, adversary tooling, known vulnerabilities, and active attack patterns, it guides real-time threat detection, containment, and mitigation to produce a robust defense posture. Tactical CTI enables SOCs to respond swiftly and deploy targeted countermeasures.

Tactical CTI Should Incorporate The Following Key Elements:

- *Specific IoCs for rapid detection*
- *Adversary tools and techniques for targeted countermeasures*
- *System and network vulnerabilities for urgent patching*
- *Active attack patterns for prioritized response*

Operational Benefits of Tactical CTI Include:

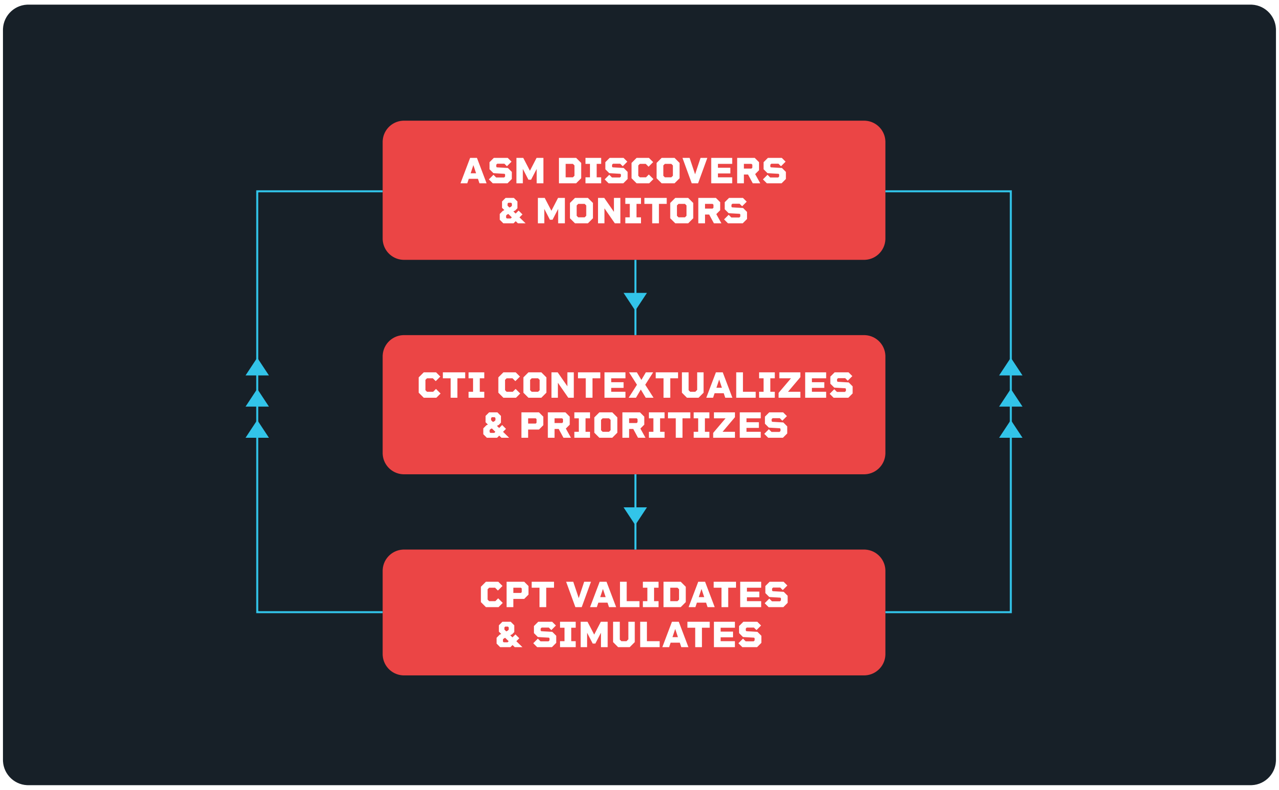
- *Real-time threat identification*
- *Swift incident containment*
- *Targeted mitigation actions*
- *Optimized security tool deployment*

Tactical CTI is vital because it provides timely, actionable insights into specific threats and attacker behaviors, enabling rapid detection, response, and mitigation of ongoing cyber incidents.

Tactical and operational CTI share elements like IoCs, TTPs, vulnerabilities, and attack patterns, but differ in application. For example, operational CTI uses IoCs for sustained monitoring and trend analysis, guiding near-term operations. Tactical CTI leverages IoCs for urgent, real-time detection and response to active threats. Other elements follow suit: TTPs inform preparation versus immediate countermeasures, vulnerabilities drive planned versus urgent patching, and patterns adjust monitoring versus response prioritization.

A robust operational structure to ingest, qualify, and use CTI ensures these elements support both proactive readiness and rapid reaction. The overall effect is to strengthen maturing security programs against dynamic threats.

THE FEEDBACK LOOP



ASM DISCOVERS & MONITORS

CTI CONTEXTUALIZES & PRIORITIZES

CPT VALIDATES & SIMULATES

#5

THREAT INTELLIGENCE IN ACTION

ASM USE CASES

In practice, keeping pace with the rapidly evolving threat landscape is challenging. Organizations face growing sophistication in threat actor capabilities that result in rapid exploitation of emerging threats. Combining ASM and CTI offers a fresh approach to cybersecurity, aligning real-time threat insights with comprehensive asset visibility. The following use cases illustrate how this integration empowers security teams to prioritize risks, enhance proactive defenses, and respond swiftly to emerging threats, delivering measurable value to maturing cybersecurity programs.

ENHANCING VULNERABILITY MANAGEMENT

When attack surface data and threat intelligence are combined, security teams can identify useful associations between the two. This formula can be further improved by incorporating vulnerability management data. Synthesizing attack surface, threat intelligence, and vulnerability management data is most easily accomplished in organizations with mature information security and risk management practices.

A core concept in vulnerability management involves the idea of a “vulnerability.” Clarifying further, there is a distinct difference between a “vulnerability” and an “exploitable vulnerability.” This distinction is important because it helps inform the overall level of effort required to implement an effective set of risk reduction controls. For example, an asset facing the public internet is vulnerable to the latest *NextJS*[6] exploit. However, for any given target, the deployed controls are effective at preventing exploitation of the vulnerability.

The vulnerability is present, but an adversary is unable to exploit it. In practice, this offers the benefit of time as the organization monitors the attack traffic and measures the potential impact of any attack. All of this is happening while operational teams set about eliminating the vulnerability across the affected assets.

By leveraging threat intelligence to provide insights into who is targeting an organization and how they might likely do it, an organization can better defend against emerging threats by:

- *Prioritizing remediation activities based on exploitability*
- *Creating context for vulnerabilities*
- *Enhancing threat detection and prevention*
- *Improving incident response*
- *Creating a more predictive vulnerability management approach*
- *Reducing false positives*
- *Providing continuous feedback for adaptive defense*

In this way, synthesizing threat intelligence, attack surface, and vulnerability management data supports prioritization for remediation activities as well as providing a way to identify active attack traffic and its effects.

INCREASING PENETRATION TESTING VALUE

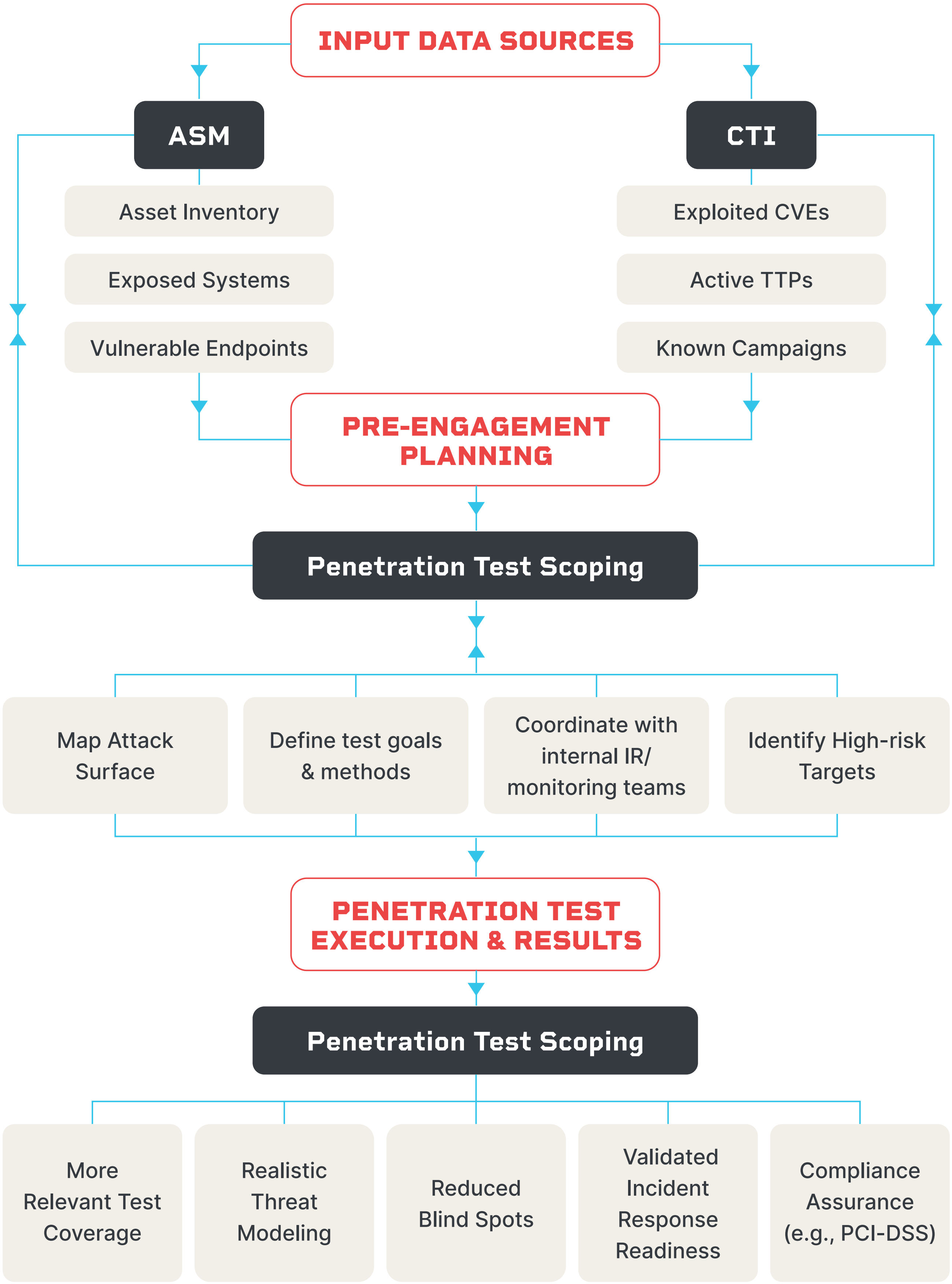
Combining CTI with ASM data steers penetration testing toward the most critical threats to an organization's systems. CTI identifies prevalent risks such as exploited vulnerabilities or active TTPs, while ASM pinpoints exposed assets. Using ASM and CTI data as part of a pre-engagement scoping process ensures testing activities target high-priority vulnerabilities and mimic real-world attacks.

To better understand this value, consider a retail organization that conducts an annual penetration test to ensure compliance with PCI-DSS and identify potential gaps in the overall defensive posture. The organization leverages ASM data to define an asset inventory that highlights vulnerabilities. CTI data reveals active campaigns targeting the affected asset or vulnerability. Penetration testers use these inputs to scope testing activities for the affected assets. Likewise, the penetration testers propose a testing plan to validate the vulnerability and potential post-exploitation activities. Through this process, internal teams focused on monitoring and incident response work with the penetration testers to validate and adjust their monitoring systems and response processes.

Now, by introducing CPT into this process, the organization moves beyond one-time validation. Instead of waiting for the next annual test, CPT enables ongoing, CTI-driven assessments throughout the year. As new vulnerabilities emerge or attackers shift tactics, CPT adapts.

By combining CTI, ASM, and CPT the penetration testers enhance the relevance, scope, and impact of the test to focus on real-world threats and critical assets. This helps the penetration testers build more accurate threat models to define the appropriate testing goals, tooling requirements, and potential outcomes.

PENETRATION TESTING PLAN



INPUT DATA SOURCES

ASM

- Asset Inventory
- Exposed Systems
- Vulnerable Endpoints

CTI

- Exploited CVEs
- Active TTPs
- Known Campaigns

PRE-ENGAGEMENT PLANNING

Penetration Test Scoping

- Map Attack Surface
- Define test goals & methods
- Coordinate with internal IR/ monitoring teams
- Identify High-risk Targets

PENETRATION TEST EXECUTION & RESULTS

Penetration Test Scoping

- More Relevant Test Coverage
- Realistic Threat Modeling
- Reduced Blind Spots
- Validated Incident Response Readiness
- Compliance Assurance (e.g., PCI-DSS)

CONCLUSION

Instead of rushing to exploit, hackers tend to spend most of their time doing reconnaissance on an organization so they can find the right place to exploit. But with a powerful dataset kept fresh inside an ASM platform, security teams gain visibility into what assets are exposed and where attackers are looking to target.

Threat intelligence provides you with a method for qualifying your ASM data by allowing you to understand what exposures are the most susceptible to threats based on tactics and targeting. Adding CPT to the mix takes this a step further by actively validating these risks in real time and revealing exploitable weaknesses.

The powerful synergy of ASM, CTI, and CPT can shape where resources should be spent to mount the most efficient and effective defense. Ultimately, the greatest value to integrating threat intelligence into ASM, and ultimately CPT, is having access to the same intelligence that attackers who are targeting your organization have access to already—and staying one step ahead of them.

Better security starts by assessing and integrating threat intelligence into the ASM processes to improve security and reduce exposure to attacks. Sprocket's no-cost ASM provides the visibility needed to effectively manage your attack surface. Discover all your exposed assets and prioritize them by risk so you can focus on what matters most and gain control of your security posture. Learn more about Sprocket today.

SOURCES

1 https://www.ibm.com/reports/data-breach

2 https://www.sprocketsecurity.com/solutions/attack-surface-management

3 Gartner, Identifies Top Security and Risk Management Trends for 2022, March 2022. © 2022 Gartner, Inc. Used with permission.

4 https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/gartner-innovation-insight-for-sttack-surface-management.pdf

5 Gartner, How to Manage Cybersecurity Threats, Not Episodes, August 2023, © 2023 Gartner, Inc. Used with permission.

6 https://www.sprocketsecurity.com/blog/a-vulnerability-hunters-view-of-next-js-cve-2025-29927-exploit-validation

LEARN ABOUT SPROCKET'S NO-COST ASM PLATFORM

Sprocket
Security