PRAETORIAN

eBook

Continuous Threat Exposure Management

A Modern Blueprint for
Risk Prioritization and Reduction

Get Started ›

Inside this eBook

1308

cyber-attacks per organization per week

Introduction

Modern enterprises face a swam of interlocking security problems.

Attack surfaces sprawl over thousands of assets, dozens of subsidiary organizations, and multiple geolocations. Network perimeters consist of on-premise data centers, cloud environments, edge devices, SaaS providers, and other sources. Agile development deploys new code to applications daily, or even hourly. Organizations today are in constant flux, and keeping track of them becomes a full time job for an entire team.

> **“Too many alerts, too few resources, and not enough communication”**

But most security officers do not have enough staff to dedicate an entire team to asset inventory. In fact, they rarely have enough staff to dedicate an entire team to anything at all. Security teams drown in floods of noisy alerts from automated vulnerability scanners and seldom have time or budget left over for strategic improvements.

When teams do take on a strategic initiative, its importance seems lost on the wider organization. Non-technical stakeholders appear to slow or even halt the rollout of much-needed improvements. Security personnel’s advice all-too-frequently falls on deaf ears, and they frequently do not feel listened to outside their teams.

Meanwhile, the average number of cyber attacks per organization reached 1,308 per week[1] in the first quarter of 2024. Attackers are on the move as security teams feel stuck in a quagmire of ticketing systems, back-and-forth meetings, and endless alerts.

Too many alerts, too few resources, and not enough communication.

These problems all share a common root: viewing security as a task rather than a process. This approach is like trying to complete an entire year’s worth of garden weeding all at once. The result is predictably backbreaking, frustrating, and ineffective. But there is a way for organizations to root out the weeds in their digital landscape. It only requires a shift in thinking.

1 https://blog.checkpoint.com/research/shifting-attack-landscapes-and-sectors-in-q1-2024-with-a-28-increase-in-cyber-attacks-globally/

The Shortcomings of Modern Security Programs

The tools we use to interact with the world shape our perception, and security is no exception. The task-vs-process misconception stems from how existing tools and services work. Tools are purchased, run, and reviewed. Security services are scheduled, conducted, and reported. There is a discrete nature to these workflows with set start and end times, and it is only natural that one's worldview will match. Unfortunately, this workflow sustains a perception unsuited to modern digital environments.

The Shortcomings of Vulnerability Scanners

Historically, a vulnerability scanner looks something like this:

The operator launches the scanner and inputs the assets they wish to scan. They then wait several hours or days for it to complete. As the results come in, the operator spends days or weeks painstakingly reviewing them for true positives.

With their list of true positives, the operator begins the frustrating process of remediation. For each vulnerability, the operator must determine which stakeholder owns the impacted asset(s), prepare clear remediation instructions, convince the stakeholder to implement their advice, and follow up to retest the asset(s). When the operator has addressed each issue, they return to their scanner to begin again.

Modern vulnerability scanners have slightly improved this process but generally by completing the above steps faster. The fundamentals remain the same: scan, triage, patch, repeat.

This process generates a daily tidal wave of alerts to review. The overwhelming majority of these alerts are pure noise, and a typical SOC analyst loses one-third of their workday [2] processing false positives. This is a mind-boggling time cost for teams that are already overstretched and undersupplied. As a result, the team has little time left over for strategic initiatives, and the organization's security posture stagnates or even declines over time.

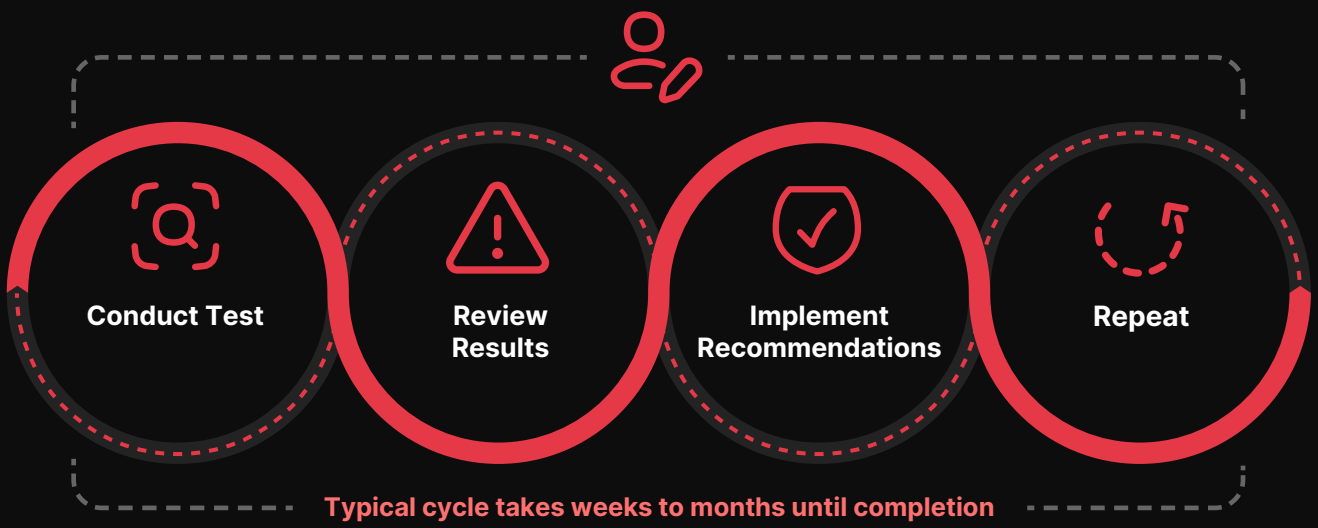
A typical SOC analyst will spend one-third of their work day processing false positives

Furthermore, vulnerability scanners are generally built with security experts in mind. Their results are highly technical and lack appropriate business context to be understood by non-security personnel. As attack paths become increasingly complicated, it becomes increasingly difficult to communicate the severity of identified risks to non-technical coworkers, executives, and board members.

Vulnerability scanners are supposed to make it easier for an organization to uncover meaningful threats to its security. Unfortunately, security teams often find that scanners add, rather than remove, work to their already busy schedules.

The Shortcomings of Security Assessments

Risk assessments (including penetration testing, red teaming, code review, and threat modeling) follow a similar, albeit slower, workflow to vulnerability scanners:



2 https://www.ibm.com/downloads/cas/5AEDAOJN#page=6

A security lead appoints an internal team or hires a third party to conduct a test. The team spends several days, weeks, or months completing the test and reporting their findings. The team then debriefs the organization on their results and gives a set of recommendations for the organization to follow.

> **“Organizations conduct most security assessments anually... But organizations change daily.”**

Unfortunately, what happens next is less clear. The testers' recommendations are typically high-level and ignorant to the specific needs and circumstances of the organization. Because of this, the security team must convince their lay stakeholders to implement security recommendations that may not clearly tie back to business objectives. And when the security team heroically finishes their crusade, it's time to plan the next assessment.

Manual security assessments cover objectives that are too complicated to fully automate. However, the underlying workflow resembles a vulnerability scanner's: test, review, fix, repeat. Unsurprisingly, security assessments suffer from similar shortcomings.

Even with automated help, modern attack surfaces are too complicated to fully comprehend at once. Manual testers spend increasingly longer times mapping out the terrain before they can even begin testing. This increases the cost of manual tests, both due to increased time requirements and specialized expertise for new technologies.

Even without cost increases, security budgets do not have room for additional testing. A typical enterprise spends only 12% of its IT budget on security [3], and 61% of mid-sized businesses have no cybersecurity staff whatsoever [4]. Organizations conduct most security assessments annually, with particularly well-funded or high-priority projects receiving quarterly or monthly testing. But organizations change daily. Between tests, security teams' visibility into their security posture decays significantly.

And when the test concludes, teams struggle to act on the test's recommendations. Third-party vendors generally do not understand business context necessary to issue practical, holistic recommendations. Instead, this calculus is left to the security team, who must present the findings in a compelling manner to stakeholders with varying interests across the organization.

Security assessments should reveal significant risks in an organization. But if the organization cannot resolve them, the assessment accomplishes little other than meeting a handful of compliance requirements.

3 https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/
4 https://www.helpnetsecurity.com/2024/01/02/cybersecurity-skills-gap-statistics/

The Shift to a Continuous Approach

Recall the problem statement introduced at the start of this eBook: attack surfaces are growing in size and complexity, security programs are understaffed and underfunded, and security experts do not feel listened to outside their teams.

The core of these problems is a mismatch between the source of cyber risks and the tools and processes used to detect them. Modern attack surfaces are now moving targets, but detection capabilities have not caught up. To discover risks in a continuously shifting environment, organizations need a security testing methodology that changes in kind.

Continuous Threat Exposure Management (CTEM)

One such framework is Continuous Threat Exposure Management (CTEM), which rethinks several core aspects of traditional security testing. CTEM shifts away from point-in-time assessments and toward continuous testing. It is fundamentally rooted in people, processes, and technology.

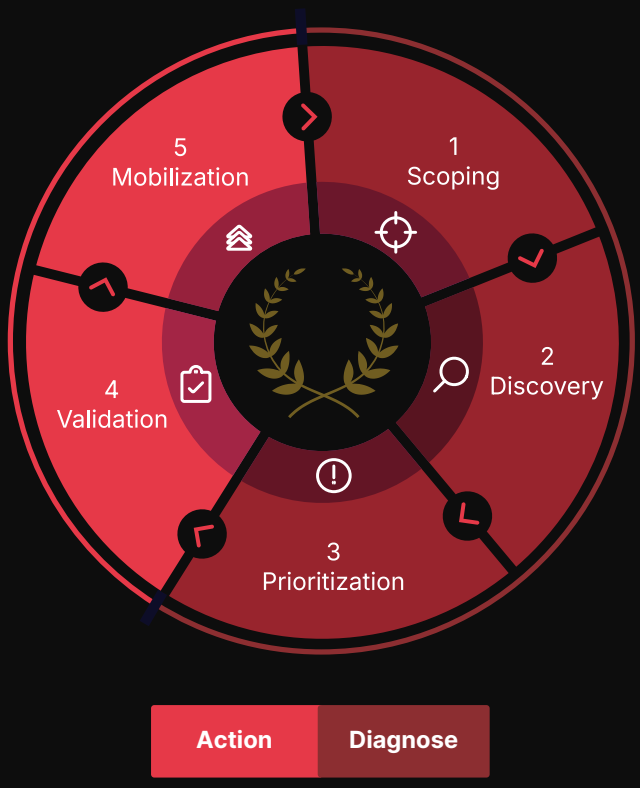
CTEM is not about buying more security tools, which already clog[5] security budgets and workspaces. Instead, CTEM builds processes around existing tools to improve their efficiency. Organizations quickly realize which tools are critical to security posture, allowing them to consolidate or eliminate everything else.

Additionally, CTEM engages the entire organization. Although security teams continue to lead security testing, they collaborate with stakeholders across the organization while designing their testing program. By achieving early buy-in on what testing is necessary and what constitutes a risk, security personnel can easily associate later requests, projects, and initiatives with core business objectives to easily communicate their importance to non-technical stakeholders.

5 https://www.infosecurity-magazine.com/news/organizations-76-security-tools/

6 https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes

The CTEM Cycle



Gartner proposed a five-step cycle[6] to implement CTEM: Scoping, Discovery, Prioritization, Validation, and Mobilization. While organizations do not need to follow this framework verbatim, it is a useful starting description of a continuous program.

The cycle above is not a sequential set of steps. Rather, each phase operates modularly, continuously receiving inputs from the previous phase and producing outputs for the next.

Five Phases of a Continuous Approach

Scoping

The Scoping phase determines what the testing program is responsible for. This phase inputs broad security objectives and outputs two deliverables: a list of in-scope assets and a set of test cases.

Security teams collaborate with stakeholders across the organization to identify assets that are critical to its success. For each asset, the security team then determines what risks threaten the asset and selects test cases to evaluate each perceived risk. Teams do not need to build tailored test cases for every individual system and can instead focus on broader categories of assets, such as public-facing web servers, internal workstations, and source code repositories. Test cases can be equally broad, such as checking sensitive ports, scanning for known CVEs, and spraying weak passwords.

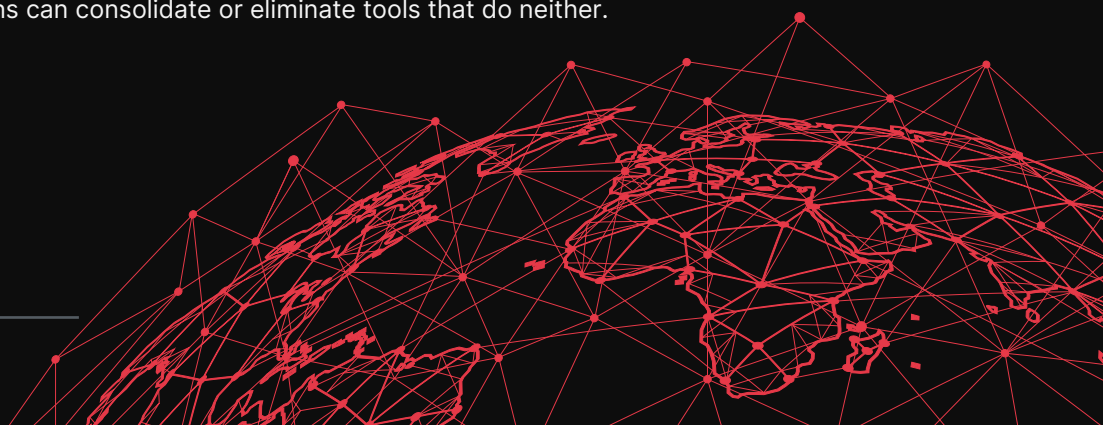
When selecting assets and test cases, organizations must consider resource constraints. Organizations will see better initial results starting with a smaller set of high-priority items than attempting to cover too much. As the program matures, the scope will naturally expand to encompass lower-priority items.

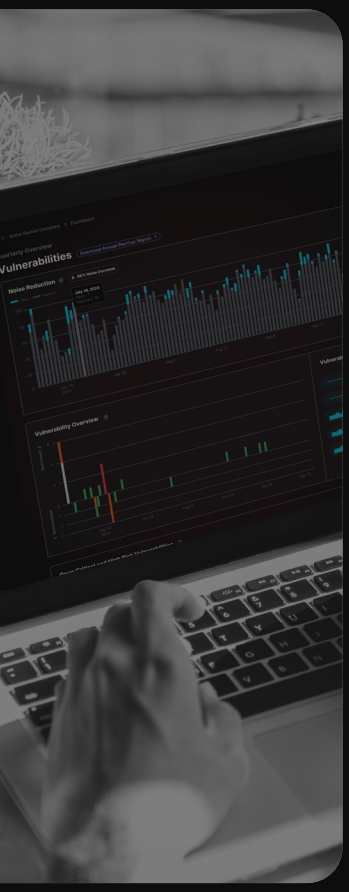
The assets and test cases from the Scoping phase become the input for the Discovery phase.

Discovery

The Discovery phase maps assets to live systems and detects risks in those systems. This phase generates an unprocessed set of risk alerts.

Discovery relies on security tools more than the other phases, but organizations can use Discovery as an opportunity to reduce tool spend. When building a CTEM program, organizations should evaluate their tools on whether they help probe a scoped asset or execute a selected test case. Organizations can consolidate or eliminate tools that do neither.





After assembling their toolkit, organizations can begin discovering assets. Organizations should begin with their perimeter, or part of their perimeter if the whole is too large. As the program matures, organizations should connect their asset detection to additional environments, such as cloud providers, source code managers, SaaS platforms, and other attack surfaces. Depending on its size, organizations may find an Attack Surface Management (ASM) solution useful, which can replace a suite of historical scanners and inventory systems.

With an inventory of live systems, the organization executes the associated test cases to detect risks. Organizations can use traditional vulnerability scanners here, but continuous detection systems are increasingly available that replace multiple existing scanners and fit neatly into a CTEM framework. Whatever technology is chosen, it must run continuously (at least daily) to detect new changes in the organization.

- ✓ **Discover live systems from scoped assets**
- ✓ **Detect risks in all discovered systems**

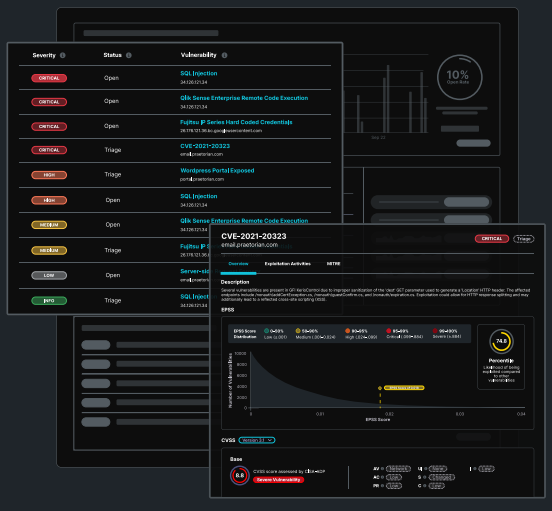
Manual assessments also have a place in Discovery and are particularly well-suited for higher-risk assets or complicated test cases. But manual testing must be informed by Scoping and directed at priority items to justify its slower time and higher cost.

Discovery generates a steady stream of alerts to process. This is generally all that traditional security programs accomplish. But it's what happens next that is crucial.

Prioritization

The Prioritization phase inputs a list of risk alerts and orders them by decreasing severity to the business. Prioritization is a preprocessing step that increases efficiency in later phases.

Organizations must create a repeatable schema to classify vulnerability severities. The schema must consider core business objectives so the metric is clear to lay stakeholders. It is not enough to rely solely on raw CVSS scores -- the schema must also incorporate contextual factors, such as the impacted asset's business function, number of instances, and likelihood of



exploitation. The prioritization scheme doesn't have to be perfect, but it must roughly approximate the severity a potential issue would have if realized.

To scale with the organization, the schema's metric must be computer-friendly and cannot rely on human evaluation. To quantify business context of assets, organizations can leverage tagging capabilities of modern ASMs and Vulnerability Managers (VMs).

- ✓ **Numerical risk rating (e.g., CVSS)**
- ✓ **Number of instances**
- ✓ **Context of impacted assets**
- ✓ **Exploitability (e.g., EPSS)**

It is critical to include stakeholders across the organization when developing the prioritization schema. The schema serves as the common agreement between all parties for when security alerts matter and grease the wheels of subsequent interactions with non-technical stakeholders.

After prioritizing their alerts, the security team has a clearer understanding of how to allocate time during vulnerability triage.

Validation

In the Validation phase, analysts work through a queue of alerts prioritized by the previous phase and generate a set of true positives to act on.

Validation determines which risks are exploitable, what the business impact of an exploitation is, and what mitigating controls are in place. While this phase is still largely a manual process, organizations can look to automated triage solutions to handle the lowest hanging fruit in the queue (obvious false or true positives).

1. Confirm if attackers can actually exploit the vulnerability
2. Determine what assets are at risk by exploiting the vulnerability
3. Investigate what compensating defensive controls exist and how they respond to a compromise

After confirming an issue, the team may manually adjust the severity rating to reflect what they learned. The final rating will use the prioritization schema designed in the previous phase and thus clearly reflect the risk's business impact. This is a critical preparation step before notifying stakeholders elsewhere in the organization.

Now comes the most important part of a security program: addressing the true positives.

Mobilization

Mobilization is the organization's standard procedure to handle confirmed risks. This consists of both immediately addressing the risk and improving higher-level security posture.

In any security program, the security team must identify the stakeholders who are responsible for the associated asset, explain the severity and details of the risk, advise remediation instructions, and agree on a timeline. This is why securing buy-in during the Scoping and Prioritization phases is so critical. By now, the security team should be able to simply point to statements the stakeholder (or their manager) has already agreed to.

Improving higher-level security posture is a more abstract challenge. The security team should collect data on all confirmed vulnerabilities and perform regular reviews over the dataset to identify trends that inform security resource allocation. Example trends include increased frequency of a vulnerability class, continued recurrence of a specific type of risk, or decreased risks in a particular environment.

After addressing the risks, the team should leverage their database to reflect on what the next security priorities are. These priorities form the new goals for Scoping, which completes the cycle.

- ✓ **Identifying relevant stakeholders of affected assets.**
- ✓ **Agreeing on SLAs for remediation, based on risk rating.**
- ✓ **Determining follow-up process to ensure remediations are completed.**
- ✓ **Monitoring remediated assets to ensure regressions do not occur.**
- ✓ **Documenting all mobilization procedures in an easily accessible location.**

Conclusion

A patient gardener does not weed their entire garden annually or quarterly. Instead, they focus attention on one section at a time, starting with the most important parts of the garden and working their way to the peripheries until it is feasible to service the entire garden daily.

In a similar way, CTEM enables organizations to identify the most pressing security needs of the business and direct resources until they improve. As the program matures, the organization broadens the scope of testing until it can handle the entire business.

This process simplifies attack surfaces through a combination of improved technologies and workflows. It addresses budget and staff shortages by focusing resources on the most critical areas of the business. And it improves actionability by broadening the responsibility of security programs across the entire organization.

Organizations can build their own CTEM programs entirely in-house, or they may look to a trusted third-party vendor to provide the expertise, technology, or staffing necessary to achieve continuous security. Praetorian is one such vendor, providing CTEM via our Praetorian Guard platform.

How Praetorian Guard is Different

Praetorian's platform is designed to embody the principles of CTEM, by combining people, process, and technology. Praetorian Guard incorporates attack surface management, vulnerability management, attack path mapping, breach and attack simulation, continuous penetration testing/red teaming, and exploit/threat intelligence into a single solution. These components, wrapped in a managed service, work in complete unison to provide unparalleled security coverage.

Contact Praetorian **Start Free Trial**