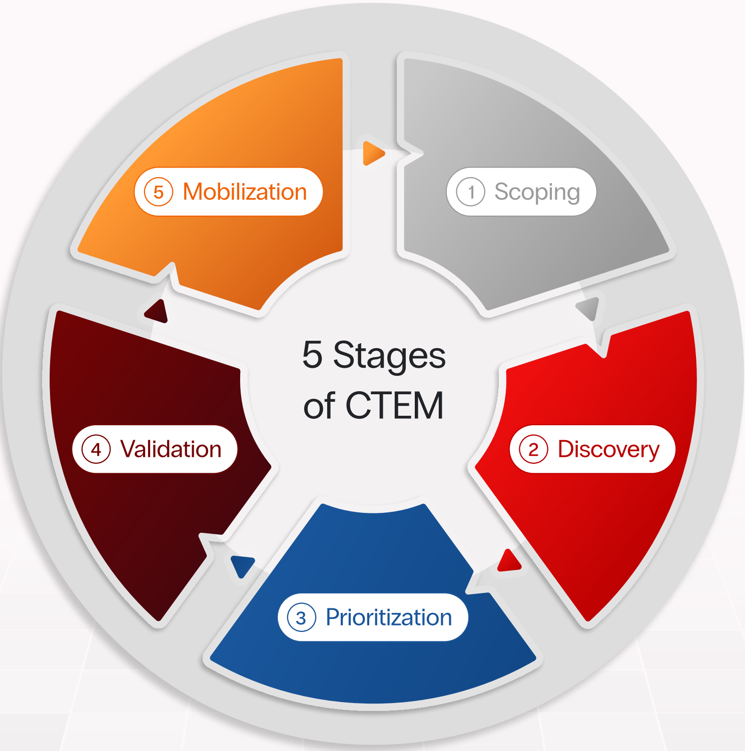
ZAFRAN

A Practical Guide for **Evolving from VM to CTEM**

Contents


5 Stages
of CTEM
1 Scoping
2 Discovery
3 Prioritization
4 Validation
5 Mobilization

Introduction

A PRACTICAL APPROACH TO IMPLEMENTING CTEM

Outdated processes have left vulnerability management (VM) teams drowning in alerts, fragmented tools, and lengthy, inefficient patch cycles. Traditional scanners label thousands of vulnerabilities as critical, but lack the context to determine what's actually exploitable. As a result, security teams waste cycles chasing ghosts.

Unsurprisingly, vulnerability exploitation is now the leading initial access vector in attacks. The need to improve how organizations understand and manage risk has never been more timely. This is the goal of Continuous Threat Exposure Management (CTEM). To make better decisions about how to manage risk, both reactively and proactively, we must first develop a clear, contextual picture of the risks we face. That understanding enables more informed decisions about how much risk we're willing to tolerate, and what actions are required to keep us within those bounds.

Unfortunately, organizations often struggle with this. While most know what they need to protect (e.g., sensitive data, business-critical applications, intellectual property), they are far less confident in assessing the likelihood that those assets will be threatened. Risk isn't just about impact; it's **likelihood × impact.**

That formula is fundamental to everything from cyber strategy to board-level risk governance.

Think of it like buying insurance. It's not enough to know what's valuable, you need to understand how likely it is to be lost. You wouldn't pay for expensive flood insurance if you lived in the desert. Similarly, organizations shouldn't overcommit resources to theoretical threats while ignoring high-risk systems simply because they have yet to be exploited.

This is where CTEM adds structure. It brings together fragmented tools, assessments, and findings into a repeatable, outcome-driven process that helps answer four core questions:

- What matters most?
- Where are we exposed?
- What could realistically happen?
- Are we taking action quickly and effectively?

CTEM isn't just a control layer. It's a decision-making framework, one that provides context, prioritization, and operational clarity.

Why a Practical Guide?

Many organizations are now adopting CTEM as a foundational cybersecurity strategy, to optimize the value of their existing investments. But CTEM isn't a product or one-time rollout; it's a **maturity journey**. Like training for a triathlon, you need to build proficiency across multiple disciplines before trying to compete at scale. You can't automate what you haven't operationalized.

This guide is designed to help teams:

- Take clear, practical first steps, regardless of maturity
- Apply CTEM principles to their existing vulnerability management processes
- Prioritize effectively using real-world context
- Iterate in cycles that strengthen exposure visibility and risk reduction over time

Introducing the Exposure Management Maturity Model

CTEM is a powerful concept and, like any strategic initiative, needs to be made actionable. One of the most common questions I hear from security leaders and practitioners alike is: “Where do we start?” That’s why a maturity model can be helpful, not as a theoretical framework, but as a practical tool to benchmark your current state and identify clear next steps.

The Exposure Management Maturity Model shown below is not intended to be definitive or prescriptive. It won’t give you a compliance score or a gold star. **Instead, it’s grounded in thousands of real-world conversations with security teams navigating the complex transition from traditional vulnerability management toward something more dynamic, contextual, and continuous.** It’s designed to help you diagnose where you are today, where you want to be, and how you can get there from here.

	STAGE 1: **Scanning Focus**	STAGE 2: **Basic Prioritization**	STAGE 3: **Risk-Based Vulnerability Management (RBVM)**	STAGE 4: **Continuous Threat Exposure Management (CTEM)**
Asset Discovery	Ad hoc, manually maintained asset inventory	Network-based discovery performed periodically	Regular discovery integrated with CMDB	Continuous asset discovery with attack surface visibility
Scanning & Detection	Infrequent, incomplete vulnerability scans	Regular vulnerability scanning in place	Vulnerability scanning at least weekly	Vulnerability scanning at least daily
Prioritization	No prioritization beyond scanner severity (CVSS)	Manual process for prioritization, includes basic threat intelligence	Beyond threat intel, to include internet exposure and asset/business context	Expanded to include runtime presence and compensating controls
Exposure Hunting	No exposure hunting capability	Critical vulnerability campaigns; limited threat actor understanding	Defined process for investigating critical vulnerabilities and threats	Continuously, proactively identifying and mitigating critical threats
Communication & Workflow	Manual spreadsheets and emails	Manual ticket assignment	Automated ticket assignment (via RBVM tool)	Automated ticketing + near real-time dashboards

Maturity Stages:

- ▶ Scanning Focus
- ▶ Basic Prioritization
- ▶ Risk-Based Vulnerability Management (RBVM)
- ▶ Continuous Threat Exposure Management (CTEM)

Functional Areas:

- ▶ Asset Discovery
- ▶ Scanning & Detection
- ▶ Prioritization
- ▶ Exposure Hunting
- ▶ Communication & Workflow

We’ll explore each of these in depth. The goal isn’t to chase perfection, it’s to help your team take confident steps forward, no matter where you’re starting.

Asset Discovery

	STAGE 1: Scanning Focus	STAGE 2: Basic Prioritization	STAGE 3: Risk-Based Vulnerability Management (RBVM)	STAGE 4: Continuous Threat Exposure Management (CTEM)
Asset Discovery	Ad hoc, manually maintained asset inventory	Network-based discovery performed periodically	Regular discovery integrated with CMDB	Continuous asset discovery with attack surface visibility
Scanning & Detection	Infrequent, incomplete vulnerability scans	Regular vulnerability scanning in place	Vulnerability scanning at least weekly	Vulnerability scanning at least daily
Prioritization	No prioritization beyond scanner severity (CVSS)	Manual process for prioritization, includes basic threat intelligence	Beyond threat intel, to include internet exposure and asset/business context	Expanded to include runtime presence and compensating controls
Exposure Hunting	No exposure hunting capability	Critical vulnerability campaigns; limited threat actor understanding	Defined process for investigating critical vulnerabilities and threats	Continuously, proactively identifying and mitigating critical threats
Communication & Workflow	Manual spreadsheets and emails	Manual ticket assignment	Automated ticket assignment (via RBVM tool)	Automated ticketing + near real-time dashboards

BUILDING THE FOUNDATION OF EXPOSURE MANAGEMENT

Every exposure management program, no matter how advanced, rests on a foundational truth: you cannot protect what you do not know exists. **Asset discovery** is the first step in the exposure management lifecycle, and the foundation upon which your CTEM practice relies. Without accurate and comprehensive visibility into your assets, all downstream processes (i.e., scanning & detection, prioritization, exposure hunting, and communication & workflow) will be significantly impacted.

Relying solely on static inventories or reports provided by other teams without validating them through independent discovery processes risks omitting entire classes of assets or capturing outdated information. **Discovery must be active, continuous, and independently verifiable.** This includes scanning to capture:

- Virtual environments (VMs, containers, cloud-native assets)
- Shadow IT and rogue systems not provisioned through formal IT channels
- Physical endpoints (laptops, servers, IoT devices)

Organizational networks are inherently dynamic. New assets are provisioned, decommissioned, moved, renamed, or re-IP'd on a regular basis. Subnets are added or removed. Cloud workloads spin up and down on demand. Dynamic network configurations, such as those managed through DHCP (Dynamic Host Configuration Protocol), further complicate the picture, as devices may change IPs regularly, making static tracking insufficient.

Discovering an asset is only part of the job. **Assigning ownership** is just as critical. Without clear accountability:

- Patching and hardening responsibilities are unclear
- Incident response workflows break down
- Vulnerability mitigation and remediation stalls

While asset inventories and defining ownership is often thought to be purely an IT responsibility, the effectiveness of cyber programs and processes rely on their accuracy. In the most effective environments Cybersecurity partners with IT to ensure processes are defined for:

- Assigning ownership within a defined SLA
- Maintaining an up-to-date asset-to-owner mapping
- Escalating unowned or orphaned assets to a defined authority (e.g., asset governance board or IT leadership)

Ownership data shouldn't live in isolation. It must be integrated into your exposure management capabilities so that alerts and tasks can be routed to the appropriate teams automatically.

A maturing Exposure Management program should move beyond reliance on manual inventories and static spreadsheets. Asset discovery is a continuous process, one that must evolve alongside your infrastructure and organizational complexity. Let's talk about how we can some steps for maturing our processes and capabilities:

Maturing Asset Discovery: From Ad Hoc to Continuous

STAGE 1 → STAGE 2: INTRODUCE SYSTEMATIC, NETWORK-BASED DISCOVERY

Start performing network discovery scans (e.g., NMAP) and compare its findings with presently available inventory sources, such as a CMDB. You might find that while there is no comprehensive inventory available, there are relevant data sources utilized by other teams within your organization which might help you to start putting the puzzle together.

In addition to preexisting inventories, many of the capabilities and tools we use today natively discover key data points related to assets and devices. Leverage capabilities like virtualization platforms, EDRs, and cloud providers to identify assets, devices and associated details.

Define the minimum necessary data points required to support your Exposure Management processes (e.g., Device Name, IP Address, Asset Owner etc.). Begin to correlate asset records with business units or functional owners.

HOT TIP

Don't worry if you don't have all the necessary asset data you need right away. Start small and build from there. Bringing visibility to missing data can help galvanize support across the organization.

STAGE 2 → STAGE 3:
EXPAND FREQUENCY, CONTEXT, AND EXPOSURE AWARENESS

Deploy network-based scanners that can perform discovery and map internal assets on a **scheduled basis**. These capabilities may be available or deployed already, but not fully functional. ITSM or vulnerability scanning tools often include network-based discovery capabilities.

Now that you have begun performing regular network discovery scans, develop a plan to gradually increase scan frequency and **automate synchronization** with inventory systems like your CMDB.

Leverage existing tools to identify likely owners based on login patterns or deployment metadata. Endpoint Detection and Response (EDR) tools are often a great place to identify users who login to an endpoint most frequently. Even if they aren't the rightful owner, they can usually help you find who is.

HOT TIP

Deduplication and normalization of assets and associated data can be an ongoing challenge. If you're performing discovery more frequently and your asset count continues to grow, but new assets are not being deployed you may have a problem!

STAGE 3 → STAGE 4:
NORMALIZE GOVERNANCE AND REAL-TIME VISIBILITY

Establish a **standardized data model** that captures all essential asset and device information, including relationships between systems. Ensure this model supports mapping applications to their underlying assets and includes the necessary attributes to identify and manage these assets across the network.

Broaden and deepen your asset discovery capabilities by consolidating data from active, passive, agent-based, and cloud-native sources into a **unified inventory**. This centralized view should provide comprehensive coverage across your environment.

Implement automated workflows for newly discovered assets to ensure that ownership, metadata, and context are promptly recorded and maintained. Formalize a review process where asset owners regularly validate the accuracy and completeness of asset data. Governance policies should clearly define not only asset ownership but also the ongoing responsibility for keeping asset records current.

HOT TIP

Most organizations already have teams dedicated to IT Asset Management, but their work is complex and often under-resourced. Engage these teams early to align on your data requirements and emphasize the critical role that continuous asset discovery plays in your program's success.

Treat them as strategic partners; collaborate to strengthen discovery efforts and look for opportunities where your tools or insights can help streamline their workflows. A strong partnership not only improves asset visibility but also builds shared accountability for maintaining accurate, up-to-date inventories.

Scanning & Detection

	STAGE 1: Scanning Focus	STAGE 2: Basic Prioritization	STAGE 3: Risk-Based Vulnerability Management (RBVM)	STAGE 4: Continuous Threat Exposure Management (CTEM)
Asset Discovery	Ad hoc, manually maintained asset inventory	Network-based discovery performed periodically	Regular discovery integrated with CMDB	Continuous asset discovery with attack surface visibility
Scanning & Detection	Infrequent, incomplete vulnerability scans	Regular vulnerability scanning in place	Vulnerability scanning at least weekly	Vulnerability scanning at least daily
Prioritization	No prioritization beyond scanner severity (CVSS)	Manual process for prioritization, includes basic threat intelligence	Beyond threat intel, to include internet exposure and asset/business context	Expanded to include runtime presence and compensating controls
Exposure Hunting	No exposure hunting capability	Critical vulnerability campaigns; limited threat actor understanding	Defined process for investigating critical vulnerabilities and threats	Continuously, proactively identifying and mitigating critical threats
Communication & Workflow	Manual spreadsheets and emails	Manual ticket assignment	Automated ticket assignment (via RBVM tool)	Automated ticketing + near real-time dashboards

IMPROVING FREQUENCY, COVERAGE, AND ACCURACY

Once assets have been discovered, the next step in the exposure management lifecycle is understanding how vulnerable they truly are. Vulnerability scanning is the lens through which we gain visibility into the security posture of our assets. But in today's fast-moving threat landscape where attackers weaponize new vulnerabilities within hours, slow, incomplete, or shallow scanning processes are no longer acceptable.

Scanning effectiveness is directly dependent on complete and accurate asset discovery. An organization that runs routine scans but fails to include all exposed or discoverable assets risks creating dangerous blind spots. This is like installing a security camera system and leaving one side of the building unmonitored.

This concept is referred to as **scanning breadth** - the extent to which all relevant assets (on-prem, cloud, remote, ephemeral) are included in the scanning scope.

As we work to mature our scanning and detection capabilities we should ensure that we have processes to identify assets which are not being scanned, not being scanned effectively, and/or not being scanned regularly. This can begin with basic reconciliation of asset inventories with scan results and can move to more automated processes with some CTEM capabilities now providing capabilities to quickly identify these control gaps.

Another key aspect of scanning and detection is referred to as **scanning depth**. This refers to the level of inspection performed as part of your scanning processes. Scanning an asset or device but not identifying all the vulnerabilities present can give a false sense of security. It's like taking your car to the mechanic and he doesn't even look under the hood!

There are **three primary means of vulnerability scanning** used in most organizations: Unauthenticated, Authenticated and Agent-Based. It is important to understand these scanning types so you can determine which is right for you, but also so you can understand the level of administration overhead required to perform these scans effectively.

Unauthenticated network scanning evaluates systems from the outside-in, without using any login credentials. This form of scanning can help identify exposed services, open ports, and vulnerabilities that are visible without authentication. It's valuable for performing external scans, but offers only limited visibility into vulnerabilities and the security posture of an asset.

Authenticated network scanning involves scanning systems over the network using valid credentials. This grants deeper insight into the host's configuration, installed software, missing patches, and privilege settings. It provides much more comprehensive results than unauthenticated scans, but requires secure handling of credentials and proper permissions for access.

Agent-based scanning involves deploying a lightweight software agent on each system being monitored. These agents run local scans and report findings back to a central system. Agents enable real-time or continuous scanning, work well in dynamic or remote environments (like cloud or remote endpoints), and reduce network load, but require installation, maintenance, and version control.

Mature organizations often use a combination of scanning techniques when evaluating the asset on their network. This is generally done to ensure all assets can be scanned (e.g., some devices are unable to be scanned via an agent) and to provide redundancy in case one method of scanning fails. Maturing scanning depth is not about the number of scans, but the quality of the scans performed. Organizations should have processes to evaluate the results of scans performed to ensure quality and accuracy, if only on a sample basis.

This evaluation of results speaks to the importance of aggregating, normalizing, and de-duplicating vulnerability data into a single source of truth. Within this data lake, the data are prepared for reasoning at scale, such as with AI and machine learning.

In addition to scanning breadth and depth, **scanning frequency** is a key part of maturing your scanning and detection processes. Threat actors now exploit vulnerabilities within days, if not hours, of disclosure. Performing quarterly or annual scans are no longer acceptable.

The exposure window is inversely proportional to the scanning frequency: increase the frequency to reduce the exposure window. As we work to mature our capabilities we should gradually increase the frequency of scans. Increasing scan frequency not only discovers new vulnerabilities and exposures, but also verifies that remediations have successfully completed (or failed). This lays the groundwork for effective prioritization.

Maturing Scanning & Detection: From Ad Hoc to Continuous and Actionable

STAGE 1 → STAGE 2: ESTABLISH A CADENCE AND CLOSE VISIBILITY GAPS

Set a minimum scanning frequency (e.g., monthly or bi-weekly). This cadence may be set based on different asset types or criticality, but should be defined and adhered to. Organizations which are subject to contractual and compliance requirements should understand if there are requirements for scanning frequency which must be adhered to before establishing a cadence.

Identify major scan coverage gaps. Use available inventories and/or network discovery results to identify which assets and devices are not being scanned or are not being scanned in accordance with the expected frequency.

Start tracking which assets are scanned, how often, and by what method. Create a process and timeline for onboarding new assets into scanning inventory and troubleshooting existing assets which are not being scanned successfully.

HOT TIP

Educate stakeholders on the importance of regular vulnerability scanning to not only the security of the device and network, but to the performance and availability of the system itself. Appropriately educated stakeholders will appreciate the increased visibility.

STAGE 2 → STAGE 3: EXPAND AUTHENTICATED SCANNING AND INTRODUCE AGENTS

Increase scan frequency to at least weekly.

Compare your asset inventory with current scan data to identify devices not being scanned with authenticated credentials or agents. Where tooling does not exist to automate this, use metrics like “vulnerability count per asset” to detect anomalies: assets with zero or unusually low vulnerabilities may not be scanned deeply.

Develop and execute a prioritized scanning coverage plan. Ensure all assets receive authenticated or agent-based scans (ideally both), prioritizing based on asset criticality, sensitivity, and exposure. Acknowledge and plan for edge cases like OT systems, legacy assets, or devices that cannot support agents, and fallback to authenticated scans or compensating controls.

Standardize onboarding processes for new scan methods. Establish clear workflows for deploying agents or enabling authenticated access across asset types. Coordinate with IT and application owners to reduce delays and ensure sustainable credential management practices.

HOT TIP

Combine agent-based and authenticated scanning to ensure persistent visibility with broad coverage.

STAGE 3 → STAGE 4: AUTOMATE AND ALIGN WITH REAL-TIME CHANGE

Increase scanning frequency to at least daily.

Automate scan initiation based on asset or infrastructure changes. Implement integrations with asset management tools, cloud platforms, and network monitoring to trigger scans automatically when new assets are provisioned, devices change network segments or IPs, and operating systems or installed packages are updated.

Integrate vulnerability scanning into CI/CD and IaC workflows. Scan images and infrastructure-as-code (IaC) templates before deployment. Use build-stage checks to block the promotion of images or code that contain known vulnerabilities or vulnerabilities of a certain risk level (i.e., Critical or High vulnerabilities).

Continuously validate scan frequency, breadth, and depth. Use dashboards and metrics to track KPIs like percentage of assets scanned within target SLAs, percentage of critical assets covered by authenticated or agent-based scans, scanning error rates, and scan latency.

HOT TIP

Treat every infrastructure change as a potential exposure event. By automating scan triggers and integrating with deployment pipelines, you turn vulnerability detection into a continuous, invisible safeguard, proactively catching risks before they reach production.

Prioritization

	STAGE 1: Scanning Focus	STAGE 2: Basic Prioritization	STAGE 3: Risk-Based Vulnerability Management (RBVM)	STAGE 4: Continuous Threat Exposure Management (CTEM)
Asset Discovery	Ad hoc, manually maintained asset inventory	Network-based discovery performed periodically	Regular discovery integrated with CMDB	Continuous asset discovery with attack surface visibility
Scanning & Detection	Infrequent, incomplete vulnerability scans	Regular vulnerability scanning in place	Vulnerability scanning at least weekly	Vulnerability scanning at least daily
Prioritization	No prioritization beyond scanner severity (CVSS)	Manual process for prioritization, includes basic threat intelligence	Beyond threat intel, to include internet exposure and asset/business context	Expanded to include runtime presence and compensating controls
Exposure Hunting	No exposure hunting capability	Critical vulnerability campaigns; limited threat actor understanding	Defined process for investigating critical vulnerabilities and threats	Continuously, proactively identifying and mitigating critical threats
Communication & Workflow	Manual spreadsheets and emails	Manual ticket assignment	Automated ticket assignment (via RBVM tool)	Automated ticketing + near real-time dashboards

FOCUSING REMEDIATION WHERE IT MATTERS MOST

The detection of vulnerabilities and exposures is just the beginning of a successful exposure management program. The real value lies in what happens next: assessing and prioritizing those findings to drive timely, risk-informed action. A program that generates thousands of vulnerability alerts but lacks the ability to prioritize effectively risks wasting time, overwhelming teams, and missing critical threats.

The challenge is that exposure risk is not universal, but highly specific to each organization's assets, environment, threat profile, and risk appetite. The same vulnerability may pose an urgent risk in one environment but be largely irrelevant in another. That's why **prioritization must be rooted in organizational context, not just CVSS scores or scanner output.**

As you mature your prioritization of vulnerabilities and exposures you should gradually add more context into your assessment. There is a long list of factors that can be added into your risk assessment, but you should be judicious in determining which factors to include and how those factors impact your prioritization. Adding additional factors into your assessment for which you do not have accurate or complete data could negatively impact your assessment of risk and also cause your stakeholders to lose trust in how you are determining what needs to be prioritized.

Prioritization must be rooted in organizational context, not just CVSS scores or scanner output.

Below are some common risk factors which may be included in your assessment to help you better prioritize vulnerabilities and exposures. This list is not exhaustive and your organization may not have quality data for each of these risk factors, at least not yet:

- **Threat intelligence.** Is this vulnerability actually being targeted or exploited by threat actors?
- **Business criticality.** Is this asset supporting business critical functions or processes?
- **Runtime presence.** Is the detected vulnerability found in code that is actually running?
- **Internet exposure.** Is this asset accessible from the internet, making vulnerability exploitation potentially easier?
- **Compensating controls.** Are there security defenses in place which reduce the likelihood of the vulnerability being exploited or the impact if exploited?

Organizations should work to continuously improve and mature their assessment by identifying and incorporating valuable data points which improve the accuracy thereof. It is equally important that timelines, frequently referred to as Service Level Agreements, or SLAs, be set to define when vulnerabilities of different risk levels must be remediated (e.g., Critical vulnerabilities must be remediated in 7 days, etc.). These SLAs should be defined in policy and regularly communicated to those stakeholders responsible for remediation.

SLAs must be set carefully to ensure they address applicable compliance and contractual requirements (i.e., PCI-DSS) that mandate remediation timelines, but also so they align to management's risk appetite. Management's risk appetite should account for the sophistication and speed of which threat actors are exploiting exposures, but also the likelihood that threat actors would target their organization and the impact if they are successful.

Maturing Prioritization: From Static Scoring to Contextual, Risk-Based Decisions

STAGE 1 → STAGE 2: MOVE BEYOND CVSS AND DEFINE SLAS

Begin using **basic threat intelligence** from available sources to highlight actively exploited vulnerabilities. Most commonly used vulnerability scanners now incorporate some level of threat intelligence into their platforms.

Establish clear SLAs based on **assessed risk** (e.g., critical = 7 days, high = 14). SLAs should be set in consideration of contractual and/or applicable compliance requirements (e.g., PCI DSS), as well as your organization's risk appetite.

Communicate the process for prioritizing vulnerabilities as well as the expected remediation timelines to organizational stakeholders . These guidelines should be regularly communicated, to manage expectations and ensure continued awareness for new stakeholders or those who have recently changed roles.

HOT TIP

Formalize SLAs in your InfoSec policy and require a security exception to be documented and approved for vulnerabilities not remediated in alignment with defined SLAs.

STAGE 2 → STAGE 3: FACTOR IN INTERNET EXPOSURE AND BUSINESS CRITICALITY

Understand whether an asset supports critical business functions. **Business criticality** can often be found when a robust asset tagging policy is deployed. By automatically cross-referencing business criticality with vulnerability scanning results, security teams can more readily prioritize those vulnerabilities which are vital for business continuity.

Identify all **internet-exposed assets**, a critical risk factor for both vulnerability prioritization and understanding your overall attack surface. This information, even if not fully accurate, should be heavily weighted in prioritizing mitigation and remediation efforts, and can usually be found by consulting asset management or network teams.

HOT TIP

Work with the risk professionals in your organization to define your assessment and prioritization methodology. Not only are they well versed in understanding and assessing risk, they can help make sure you get the appropriate organizational buy-in to make your prioritization capabilities successful.

STAGE 3 → STAGE 4: INCORPORATE RUNTIME SIGNALS AND DEFENSIVE POSTURE

Determine runtime presence of vulnerabilities. While only provided by select vendors and complex to assess otherwise, this capability provides a powerful indicator of exploitability, regardless of whether exploits are available to threat actors.

Evaluate the availability and configuration of compensating controls (security tools) as mitigating factors in your risk assessment. **Your existing security tools (e.g., EDR, IDS/IPS, WAF etc.) may significantly reduce the likelihood or potential impact of a vulnerability's exploitation.**

Determine the appropriate weighting of risk factors in your assessment, based on both the quality of each factor and its relevance to likelihood and impact. If advanced capabilities (e.g., CTEM, UVM, or RBVM) for ingesting and weighting these factors are unavailable, perform the calculations manually.

HOT TIP

Your risk assessment and prioritization process isn't "set it and forget it." Periodically revisit your prioritization logic to see if there are opportunities to take advantage of new data sources and telemetry. As tooling improves, so does your ability to make risk-based decisions with greater precision and confidence.

Your existing security tools (e.g., EDR, IDS/IPS, WAF etc.) may significantly reduce the likelihood or potential impact of a vulnerability's exploitation.

Exposure Hunting

	STAGE 1: **Scanning Focus**	STAGE 2: **Basic Prioritization**	STAGE 3: **Risk-Based Vulnerability Management (RBVM)**	STAGE 4: **Continuous Threat Exposure Management (CTEM)**
Asset Discovery	Ad hoc, manually maintained asset inventory	Network-based discovery performed periodically	Regular discovery integrated with CMDB	Continuous asset discovery with attack surface visibility
Scanning & Detection	Infrequent, incomplete vulnerability scans	Regular vulnerability scanning in place	Vulnerability scanning at least weekly	Vulnerability scanning at least daily
Prioritization	No prioritization beyond scanner severity (CVSS)	Manual process for prioritization, includes basic threat intelligence	Beyond threat intel, to include internet exposure and asset/business context	Expanded to include runtime presence and compensating controls
Exposure Hunting	No exposure hunting capability	Critical vulnerability campaigns; limited threat actor understanding	Defined process for investigating critical vulnerabilities and threats	Continuously, proactively identifying and mitigating critical threats
Communication & Workflow	Manual spreadsheets and emails	Manual ticket assignment	Automated ticket assignment (via RBVM tool)	Automated ticketing + near real-time dashboards

FROM REACTIVE FIXES TO PROACTIVE DISCOVERY

Scanning and prioritization help uncover known vulnerabilities, issues that your tools are specifically designed to detect. But what about the risks that fall outside those predefined rules? That's where exposure hunting comes in. It's a proactive, hypothesis-driven approach to identifying exposures that standard scanners and alerting systems may miss. Often, the clues are already present but scattered across tools and logs, and require intentional, targeted analysis to connect the dots.

Vulnerability and exposure management are often thought of as detective processes or controls. Scans are done to identify existing misconfiguration or vulnerabilities affecting software in your organization at which point actions are taken to address the deficiencies. Exposure hunting is considered to be a more preventive or proactive approach, as it seeks to not only understand current vulnerabilities and misconfigurations, but also to correlate that data with other contributing factors (e.g., absence of controls, increased threat actor activity, and other environmental weaknesses) to understand what actions or protections can be put in place to mitigate or reduce the exposure risk.

If you leave a door unlocked or a window open, you've introduced a vulnerability, something obvious that needs fixing. But imagine that in addition to that, there's been a string of burglaries nearby. You're on vacation and your spouse is posting updates about it on social media. Your alarm system is offline or broken. Your home is isolated. Individually, each of these might not seem urgent. But together, they create a perfect opportunity for exploitation.

Exposure hunting is about identifying and acting on that convergence of risk. It's the practice of correlating vulnerabilities, environmental weaknesses, control gaps, and threat intelligence to uncover exposures that demand preemptive action. Just as you might ask a neighbor to check on your house or call the police to increase patrols, exposure hunting enables you to mitigate or reduce risk before an incident occurs.

To mature your exposure management capabilities, you must go beyond enrichment and prioritization. While adding asset criticality and threat intelligence to scan results can improve prioritization, exposure hunting drives depth of understanding, ensuring you're not just responding to alerts, but actively hunting for hidden risks.

The US Army may be a powerful defense force, but exposure hunting is like bringing in the Marines: specialized, agile, and capable of going deeper to eliminate threats that standard processes miss.

As you mature your exposure hunting capabilities, it's important to remember that starting small is perfectly acceptable. **Begin by developing a structured process for conducting focused campaigns** that aim to identify, analyze, and respond to risks or contextual gaps that may have been missed by your existing scanning and prioritization workflows.

Over time, expand the scope of these efforts by incorporating additional data sources, especially those not currently factored into your assessments. **Broaden your hypotheses** to cover a wider range of asset types, software categories, and deployment environments. **Deepen your analysis** to include threat actor intelligence relevant to your industry, the techniques they commonly employ, and the defenses you have in place (or which may be lacking) to counter them. By layering in this depth of context, exposure hunting becomes a powerful force multiplier for reducing risk and shrinking your organization's exposure window.

For more specifics on exposure hunting, please review the Zafran series on Threat and Exposure Hunting.

Maturing Exposure Hunting:
From Ad Hoc Checks to Continuous, Hypothesis-Driven Discovery

STAGE 1 → STAGE 2: INTRODUCE STRUCTURED INVESTIGATIONS

Inventory the tools and data at your disposal to help you better understand and investigate asset details and telemetry, threat actors and their behaviors, and current vulnerabilities and exposures. Specifically, identify key data points that may not yet be incorporated into your prioritization capabilities, but would be useful for better understanding areas of exposure (i.e., if you don't incorporate internet exposure into prioritization, see if you are able to identify data points on internet-facing assets to inform your hunts).

Start by looking for the most basic items that would be missed by your vulnerability scans. Perhaps you are only scanning once a month, but you know a new vulnerability has been published, is being exploited and won't be identified for another week when you scan again. In this example you might use available data on deployed software and versions, threat intelligence, and asset data to identify and address potential exposures before they are captured by a vulnerability scan.

Communicate the results of your hunting activities to relevant stakeholders. Be sure to include the data and the analysis performed, the results of the hunt, and the actions taken as a result.

HOT TIP

Exposure hunting does not take the place of prioritization. Your exposure hunting capabilities often mature as your prioritization matures. Where prioritization is immature, exposure hunting can be a good way to demonstrate the value of improved prioritization.

STAGE 2 → STAGE 3: EXPAND CONTEXT AND OPERATIONALIZE HUNTING

Define a frequency, responsibilities, and high-level process for performing periodic hunting activities. When defining the process remember that every hunt starts with a hypothesis. Be sure to document and track the hypotheses, results of the hunt and actions taken afterwards, so you can learn and build upon previous insights.

Standardize basic, high-impact hunts into regular processes. If during your hunts you have regularly identified internet-exposed assets which have a large number of exploitable vulnerabilities impacting end-of-life (EOL) software, then perhaps it is time to incorporate this as a regularly performed part of your operations. This way you can make sure you are continuing to identify and address this known risk, but so you can also focus hunting activities on new areas of exposure.

Expand the complexity and scope of your hypotheses by incorporating data on your security defenses. Go beyond asking whether a certain threat scenario exists to understand what protections are in-place to mitigate that risk. Consider capabilities like firewalls, endpoint detection and response (EDR), web application firewalls and more.

HOT TIP

Identify and document blind spots where data is not available to evaluate a hypothesis. Key visibility gaps should be considered when evaluating new capabilities or defining crossfunctional requirements.

STAGE 3 → STAGE 4: SCALE WITH HYPOTHESIS-DRIVEN DISCOVERY AND CONTROL VALIDATION

Automate capabilities for performing exposure hunting. If you are able to improve the efficiency in which you perform hunting activities this will allow additional time and resources for more complex hunting activities.

Go beyond point-in-time exposure hunts to evaluate trends as part of your analysis. Understanding trends can help better inform your response as well as your ongoing defense strategy. For instance, if Linux servers are more likely to be internet-facing, have exploitable vulnerabilities in runtime, and be targeted by threat actors known to target your industry, perhaps it's time to consider additional safeguards for those systems.

Add mitigations to your exposure hunting strategy to quickly respond to identified areas of heightened risk. **Mitigations may not take the place of remediation, but are an effective means to quickly reduce exposure windows.**

HOT TIP

Review findings regularly with other relevant cybersecurity teams to validate assumptions, close visibility gaps, and strengthen shared understanding of exposure risk.

Communication & Workflow

	STAGE 1: **Scanning Focus**	STAGE 2: **Basic Prioritization**	STAGE 3: **Risk-Based Vulnerability Management (RBVM)**	STAGE 4: **Continuous Threat Exposure Management (CTEM)**
Asset Discovery	Ad hoc, manually maintained asset inventory	Network-based discovery performed periodically	Regular discovery integrated with CMDB	Continuous asset discovery with attack surface visibility
Scanning & Detection	Infrequent, incomplete vulnerability scans	Regular vulnerability scanning in place	Vulnerability scanning at least weekly	Vulnerability scanning at least daily
Prioritization	No prioritization beyond scanner severity (CVSS)	Manual process for prioritization, includes basic threat intelligence	Beyond threat intel, to include internet exposure and asset/business context	Expanded to include runtime presence and compensating controls
Exposure Hunting	No exposure hunting capability	Critical vulnerability campaigns; limited threat actor understanding	Defined process for investigating critical vulnerabilities and threats	Continuously, proactively identifying and mitigating critical threats
Communication & Workflow	Manual spreadsheets and emails	Manual ticket assignment	Automated ticket assignment (via RBVM tool)	Automated ticketing + near real-time dashboards

TURNING INSIGHTS INTO ACTIONS

Similar to interpersonal relationships, solid communication is critical to the success of vulnerability and exposure management programs. It's also one of the biggest challenges. While cybersecurity teams are responsible for discovering and prioritizing vulnerabilities, the actual remediation work typically falls to others: IT operations, application owners, business units, and infrastructure teams. Bridging that divide requires communication that is clear, timely, and actionable.

In many organizations, this “last mile” of the process, communicating exposures to the right people and driving remediation, is the most time-consuming and manual part of the program. That’s why improving communication and workflow maturity is so critical. The more efficiently teams can assign, route, and resolve issues, the more time they can spend on higher-value activities like exposure hunting, proactive defense, and strategic planning.

It’s important to separate effectiveness from maturity. Although a vulnerability workflow managed through spreadsheets and email can still be effective, it's rarely sustainable or scalable. As organizations mature, automation becomes a force multiplier. By embedding business logic into workflows, integrating with ITSM platforms, and reducing manual intervention, you improve both efficiency and reliability, ultimately accelerating time-to-remediation and shrinking the exposure window.

Before you can automate, though, you need to **get the fundamentals right.** That starts with governance. Have you formally documented who is responsible for addressing vulnerabilities across different asset types? Are SLAs clearly defined, communicated, and enforced? Do stakeholders understand the timelines and expectations? Without clear policies, even the best workflows will struggle to compel action.

Ownership data is equally critical. If your policies say server owners are responsible for remediation, but your asset inventory lacks up-to-date ownership mappings, even an automated ticketing system won't know where to send the alert. Centralized and reliable ownership attribution is the backbone of scalable communication, and the key to enabling automated delivery of vulnerability and exposures in a timely manner.

Even if communication and workflow may not be the most glamorous part of an exposure management program, they are among the most essential. This is where strategy becomes execution. With deliberate steps and foundational improvements, even highly manual environments can make fast progress toward automation and maturity.

Maturing Communication & Workflow:
From Reactive Email Chains to Continuous, SLA-Driven Coordination

STAGE 1 → STAGE 2: ESTABLISH OWNERSHIP AND TIMELY NOTIFICATION CHANNELS

Define responsibilities and timelines (SLAs) for remediation of vulnerabilities within your organization's Cybersecurity Policy. Be sure these policies are approved by leadership and communicated to stakeholders on a regular basis.

Identify the source of truth for asset data and ownership information (i.e., CMDB). Work with the individuals responsible for maintaining this information to understand how and how often this data is updated.

Determine a means of stakeholder communication and ticketing as well as frequency for delivery. It is often good to use ticketing systems already in place for IT Operations, as these will be most familiar to your stakeholders. Work with your stakeholders to define the required data necessary to enable remediation via tickets such as asset name and IP, the vulnerability, remediation guidance, and expected resolution timelines.

HOT TIP

Don't let a lack of asset ownership data keep you from improving your communication processes. Work with IT to improve processes for asset attribution. Start reporting to leadership the vulnerabilities on assets without defined owners. Work with leadership to employ strategies which may help you improve the accuracy and completeness over time such as requiring security exceptions for vulnerabilities on assets without owners or decommissioning of assets with aged vulnerabilities that continue to go unremediated.

STAGE 2 → STAGE 3: AUTOMATE TICKET ROUTING AND STANDARDIZE WORKFLOWS

Automate the assignment and delivery of tickets to those responsible for remediation. This will also require supporting processes to regularly review vulnerabilities which are not assigned due to absence of ownership information or other errors. Note that this may require additional tooling such as an RBVM, UVM, or CTEM solution if not already available.

Establish escalation processes for tickets which are not addressed in a timely manner. Based on your organization escalations may be most effective if progressive. For example, vulnerabilities not remediated within 5 days of SLA are communicated to the owner's manager; and vulnerabilities which miss SLA are then communicated to manager's manager, and so on.

Define and implement a process for documenting security exceptions for vulnerabilities and exposures which will not be able to be remediated in alignment with established SLAs. This process should require the owner or their leadership to accept the risk of not resolving the vulnerability within defined timelines.

HOT TIP

A well-defined security exception and risk acceptance process can really help drive timely remediation and compliance with SLAs. Asset owners will generally work harder to find ways to meet timelines rather than having to spend time working through an exception process or having to accept the risk formally.

STAGE 3 → STAGE 4: OPERATIONALIZE END-TO-END EXPOSURE RESPONSE

Configure dashboards for each team, business unit, or segment showing active tickets, SLAs, and aging vulnerabilities, refreshed at least daily. This centralized view will improve the experience and can enable teams to more effectively work through remediation queues especially when responsible for a large number of assets or assets which are relatively short-lived like cloud workloads.

Embed communication into change and deployment workflows. Ensure vulnerabilities are communicated as part of CI/CD pipelines and DevOps workflows to identify issues in pre-production. Change management processes should also include steps to ensure vulnerabilities introduced by changes are identified, communicated and tracked.

Implement mitigation workflows for exposures and vulnerabilities. These may be owned by cyber teams other than the ones managing vulnerabilities and exposures.

HOT TIP

Build dashboards that speak both security and business. Don't just display technical data, translate it into business impact (e.g., "Top 10 unpatched vulnerabilities affecting revenue-generating systems") to drive urgency and executive engagement.

Conclusion

Continuous Threat Exposure Management (CTEM) is a strategic shift in how organizations understand and act on risk. It moves us beyond compliance checklists and siloed tooling into a dynamic, integrated discipline grounded in context, collaboration, and continuous improvement.

This guide was designed not to offer a silver bullet, but a practical blueprint. Whether you're just beginning or are already on your CTEM journey, the path to maturity is built on incremental progress. While this guide won't include every step or action necessary to build and mature your program, it will give you insight into the key actions organizations are taking to mature from traditional vulnerability management to more mature practices like CTEM.

The most effective organizations treat CTEM as a core operational function, not an overlay. They partner across IT and security domains, build shared accountability, and invest in the workflows that turn insights into outcomes. They ask not just "Where are we exposed?", but "Are we acting fast enough, with the right context, in the right places?"

If you've made it this far in the guide, you're already on that path. Keep moving forward, stage by stage, decision by decision. Because in a world where exposure is constant, maturity is momentum.