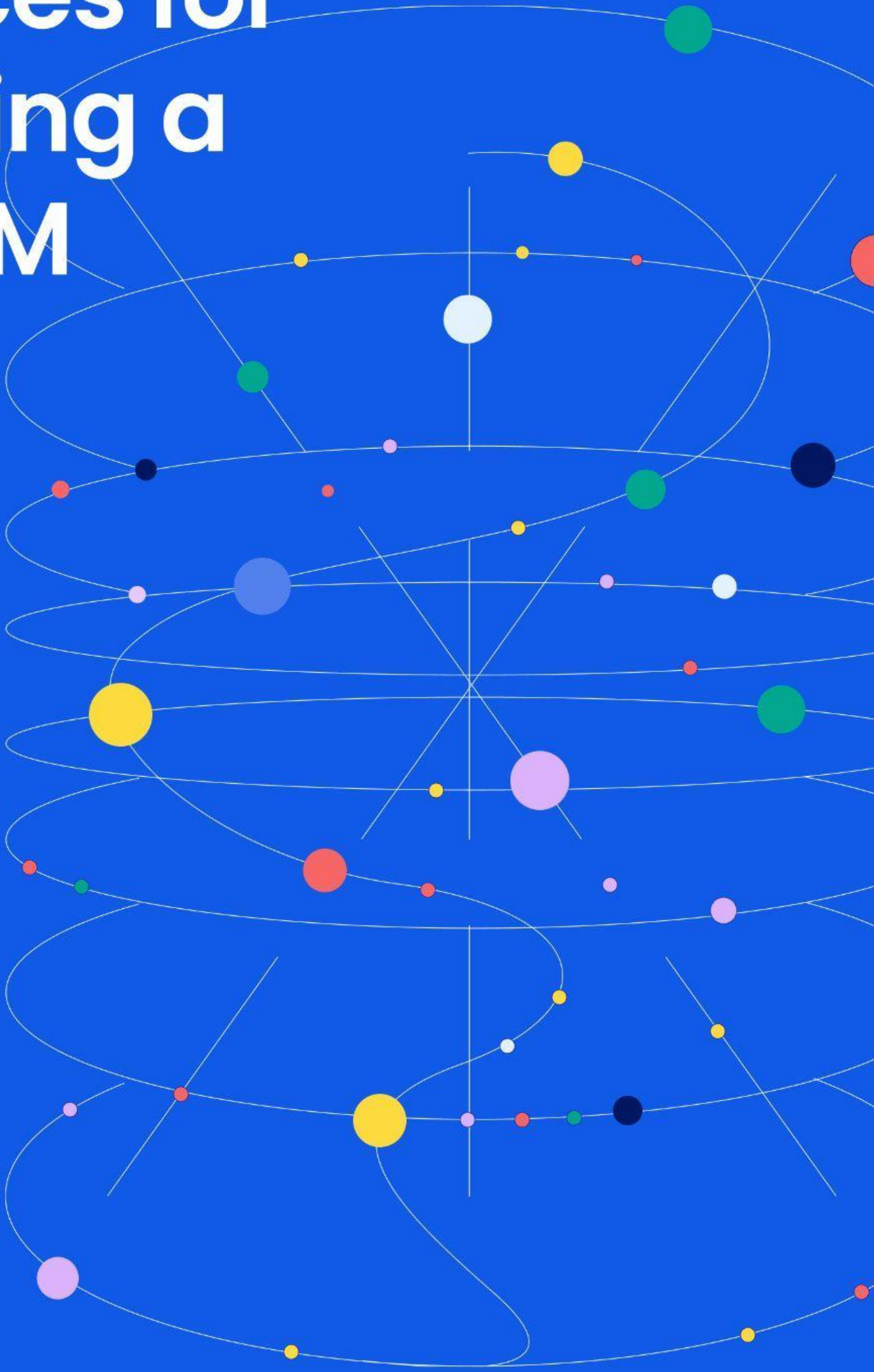
Best Practices for Implementing a Robust CTEM Program

A TONIC BROCHURE



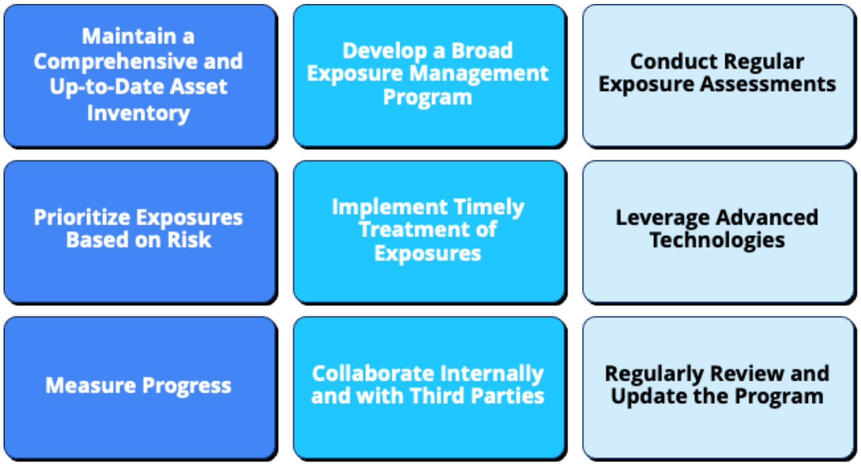
Tonic

www.tonicsecurity.com

Introduction

As modern organizations face an ever-expanding threat landscape, a fragmented or reactive approach to cyber risk is no longer viable. Continuous Threat Exposure Management (CTEM) offers a structured, ongoing, and proactive approach to managing digital risk. CTEM focuses not only on identifying vulnerabilities but on aligning threat exposure efforts with business priorities to enhance resilience and reduce the likelihood of successful attacks.

Here we outline the nine best practices for implementing a robust CTEM program, providing practical guidance, recommended technologies, and actionable metrics to mature your organization's exposure management capabilities.



Maintain a Comprehensive and Up-to-Date Asset Inventory

Develop a Broad Exposure Management Program

Conduct Regular Exposure Assessments

Prioritize Exposures Based on Risk

Implement Timely Treatment of Exposures

Leverage Advanced Technologies

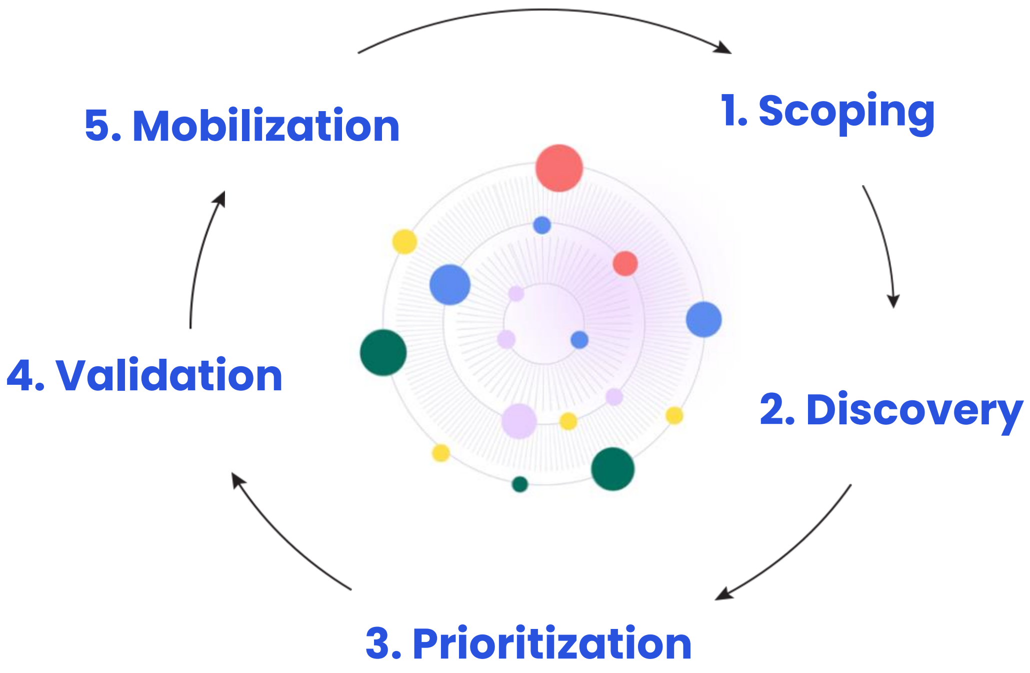
Measure Progress

Collaborate Internally and with Third Parties

Regularly Review and Update the Program

These best practices are traced to the 5 stages of CTEM:

1. **Scoping:** Define what to assess by identifying the environments, assets, and business processes that matter most.
2. **Discovery:** Continuously uncover assets, exposures, vulnerabilities, misconfigurations, and attack paths across the scoped environment.
3. **Prioritization:** Assess and rank exposures based on business context, exploitability, and potential impact.
4. **Validation:** Simulate or test if prioritized exposures are exploitable and whether defenses are working effectively.
5. **Mobilization:** Coordinate and drive timely remediation, mitigation or risk approval actions across teams.



1. Maintain a Comprehensive and Up-to-Date Asset Inventory

An effective CTEM program starts with visibility. You cannot protect what you cannot see. Maintaining a comprehensive asset inventory ensures you know exactly what exists across your digital environment.

CTEM phase: Discovery.

Best Practices:

- **Automate Discovery and Inventory:** Use tools to continuously identify and monitor digital assets, including endpoints, applications, and cloud resources. Monitor both commissioned and decommissioned assets.
- **Update Regularly:** Ensure inventory reflects additions, removals, and changes in assets.
- **Include Critical Details:** Capture asset type, location, owner, purpose, and associated risks.
- **Classify Assets:** Identify which assets are critical to the organization's operations and hold sensitive information and use consistent labels.
- **Identify Unmanaged Assets:** Ensure the inventory includes often overlooked assets, such as SaaS, BYOD, serverless, containers, and microservices.

- **Define Asset Ownership:** Assign ownership for accountability, remediation, and lifecycle management.

2. Develop a Broad Exposure Management Program

CTEM should be a cross-functional, policy-driven program that integrates with business and IT processes.

CTEM phase: Scoping.

Best Practices:

- **Establish Clear Policies and Procedures:** Define the scope, roles, and responsibilities for exposure management within the organization. This includes setting up a structured framework to identify, assess, and remediate exposures.
- **Centralize Management:** Ensure a uniform – centralized and standardized - view and management of exposures from a people, process and technology perspective, across all sources, business units, teams, etc.

3. Conduct Regular Exposure Assessments

Regular exposure assessments ensure that vulnerabilities and misconfigurations are discovered before adversaries exploit them.

CTEM phase: Discovery, Validation.

Best Practices:

- **Conduct Regular Scans:** Use scanning tools to maintain an up-to-date view of exposures, at a frequency derived from the organization's risk tolerance, compliance mandates, and type of assets.
- **Validate Manually:** Complement automated processes with human oversight to verify findings and uncover complex exposures that automated tools might miss.

4. Prioritize Exposures Based on Risk

Not all exposures carry equal weight. Prioritization is key to optimizing resource allocation and mitigating the highest risks first.

CTEM phase: Prioritization.

Best Practices:

- **Adopt a Risk-Based Approach:** Evaluate exposures based on their potential impact and exploitability, focusing on those that pose the highest risk to critical assets.
- **Find the Root Cause:** Go beyond symptoms to address systemic issues. Uncover fundamental causes and interconnected components and implement comprehensive measures to prevent exposures from recurring.
- **Utilize Threat Intelligence:** Incorporate real-time threat intelligence to understand the current threat landscape and adjust prioritization accordingly.
- **Use Contextual Risk Indicators:** Apply frameworks like Tonic's Contextualized Risk Indicator to assess severity, criticality, sensitivity, reachability, exploitability, and resilience.

5. Implement Timely Treatment of Exposures

Prompt action reduces the attack window and limits potential damage.

CTEM phase: Mobilization, Validation.

Best Practices:

- **Automate Remediation:** Employ orchestration tools for fast, policy-aligned remediation.
- **Validate the Fix:** Conduct follow-up assessments to verify effectiveness. Continuous monitoring ensures that exposures have been successfully addressed, and identifies new issues that may arise.
- **Test in Safe Environments:** Simulate and test remediation measures before applying to production.
- **Track Exceptions:** Document risk acceptance and compensating controls, while ensuring all temporary controls have expiration and review dates.

6. Leverage Advanced Technologies

A successful CTEM program integrates tools across various domains of security.

CTEM phase: Scoping, Discovery.

Recommended Technologies:

- Unified Vulnerability Management (UVM) / Exposure Assessment Platforms (EAP)
- Cyber Asset Attack Surface Management (CAASM)
- External Attack Surface Management (EASM)
- Cloud Security Posture Management (CSPM)
- Application Security Posture Management (ASPM)
- Endpoint Detection and Response (EDR)

7. Measure Progress

Tracking progress with meaningful metrics helps optimize performance and communicate with stakeholders.

Recommneded Metrics:

- **Mean Time to Remediate (MTTR)** – Time from vulnerability identification to resolution.
- **Open vs. Closed Findings** – Number of unresolved vs. resolved findings over time.
- **SLA Compliance** – Percentage of findings fixed within defined SLA limits.
- **New Findings by Discovery Date** – Number of newly discovered findings each day.
- **Average Vulnerability Age** – Time between public disclosure and remediation.
- **Patch Compliance Rate** – Percentage of systems with up-to-date security patches.
- **Recurrence Rate** – Percentage of findings that reappear after being marked as resolved.
- **Scan Coverage** – Percentage of assets that have undergone vulnerability scanning.
- **Scan Frequency** – Average time between vulnerability assessments.
- **Mean Time to Detect (MTTD)** – Time from public disclosure to detection in your environment.

Best Practices:

- **Enable Regular Reporting:** Provide dashboards and periodic reports to CISOs, IT leaders, and the board.
- **Make Metrics Actionable:** Tie KPIs to business decisions and continuous improvement efforts.

Additional guidance:

- A popular type of metric is the **Key Performance Indicator (KPI)** - a measurable value or target that indicates how effectively an organization or individual is achieving key business objectives. KPIs are used to evaluate the success of an organization, department, project, or individual in meeting performance targets. KPIs are typically quantitative and are chosen based on their relevance to the critical success factors of the organization.

- By looking at several key indicators, businesses can identify successes, as well as what is not working. Analyzing KPIs on a regular basis provides a solid overview of how well a business is performing, and enables informed decision making on operaitons and strategy.
- Good KPIs (and metrics in general) are **SMART**:
  - **Specific:** Based on a clearly understood goal; clear and concise.
  - **Measurable:** Can be measured; quantifiable; objective.
  - **Attainable:** Realistic; based on achievable goals and values.
  - **Relevant:** Directly related to a specific activity or goal; relevant to improving outcomes
  - **Timely:** Grounded in a specific time frame.
- Additional characteristics of good KPIs:
  - **Accurate:** Not exact science; a reasonable degree of accuracy is generally adequate.
  - **Cost-effective**: The measurements should not be too expensive to acquire or maintain.
  - **Repeatable**: The ability to measure the KPI must be able to be acquired reliably over time.
  - **Predictive**: The KPI should be indicative of outcomes.
  - **Actionable:** It should be clear to the "customer" of the KPI what action must be taken.

8. Collaborate Internally and with Third Parties

Exposure management is a shared responsibility. Success depends on alignment across departments and the supply chain.

Best Practices:

- **Assign Ownership:** Clarify accountability across IT, security, DevOps, and infrastructure teams.
- **Engage the Business:** Regularly brief business unit stakeholders and escalate blockers.
- **Enable Cross-Functional Collaboration:** Use workflow platforms to integrate efforts across teams.
- **Evaluate Vendor Risk:** Ensure third-party providers meet your exposure management standards.

9. Regularly Review and Update the Program

CTEM must evolve to stay relevant as threats, technologies, and business priorities change.

Best Practices:

- **Continuous Improvement:** Use retrospectives and lessons learned to iterate on your program.
- **Perform Audit and Compliance Checks:** Ensure alignment with internal policies and industry regulations.

Final Thoughts

Building an effective CTEM program isn't a one-time initiative. It's a continuous cycle of discovery, assessment, prioritization, treatment, and measurement. By adopting these best practices, organizations can reduce their attack surface, mitigate risk faster, and align cybersecurity efforts with business outcomes.

Investing in the right technologies, processes, and people will allow your organization to move from reactive patching to strategic exposure management. In today's dynamic threat landscape, this is not just a technical imperative - it's a business necessity.