DATASHEET

NSFOCUS

# Continuous Threat Exposure Management (CTEM)

## OVERVIEW

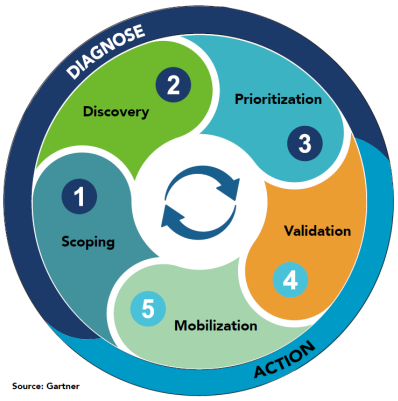
Continuous Threat Exposure Management (CTEM) is a continuous process that helps organizations scope, discover, prioritize, validate and mobilize resources to address cyber risks. It does this by:

- Adequately Scoping Risk Assessments
- Discovering digital assets that may be weaponized for exploitation
- Employing contextualized prioritization, refocusing on the most impactful issues.
- Validating the exploitability of prioritized exposures
- Surfacing a variety of fix options, increasing approvals for treatment recommendations.

Cybersecurity risk and resiliency are top of mind for both technical and business leaders. They need to find a common language to understand and communicate the impact of threats to business operations.

Without the appropriate synchronization of technologies and processes, it can be challenging to quantify cyber risk in relationship to business initiatives, ultimately right-sizing your efforts to the business' tolerance for risk. Proactive attack surface defense requires full spectrum CTEM, unifying risk assessment, and validation technologies for a comprehensive view of risk exposure.

**CONTINUOUS THREAT EXPOSURE MANAGEMENT**




Source: Gartner

Gartner identifies CTEM as a programmatic approach to continuously managing exposure risk, optimizing cyber programs, and improving cyber resilience.

If you're looking to improve your organization's cybersecurity posture, CTEM is a great place to start. It can help you reduce risk, optimize your cyber programs, and improve your cyber resilience.

**NSFOCUS Platform Drives Continuous Threat Exposure Management Programs**

| Step | | NSFOCUS Offering | CTEM Value |
|---|---|---|---|
| **Diagnose** | **Scoping**<br>**Discovery**<br>**Prioritization** | » Cyber Asset Attack Surface Management (CAASM)<br>» External Attack Surface Management (EASM)<br>» Remote Security Assessment System (RSAS)<br>» Digital Risk Protection Service (DRPS)<br>» WebSafe<br>» Source Code Review<br>» Vulnerability Assessment (VA)<br>» Configuration Verification<br>» Vulnerability Prioritization Technology (VPT)<br>» Threat Intelligence (TI) | » Identify your most valuable assets and data. By identifying the critical assets and data, organizations can prioritize their resources and focus their efforts on digital assets critical to business operations.<br>» Gather data from all of your systems and networks. By collecting data from a variety of sources, organizations can get a more complete view of their security posture and identify threats that may not be detected by individual security products.<br>» Identify the threats that pose the greatest risk to your organization. By prioritizing threats based on their likelihood and impact, organizations can make the most of their resources and focus their efforts on the threats that pose the greatest risk. |
| **Action** | **Validation**<br>**Mobilization** | » Breach and Attack Simulation (BAS)<br>» Penetration Testing as a Service (PTaaS)<br>» Red Teaming<br>» Incident Response (IR)<br>» Security Awareness Training | » Confirm that the threats you've identified are real and pose a risk to your organization. By validating threats, organizations can avoid wasting time and resources on threats that are not real or that do not pose a risk.<br>» Take action to mitigate the threats you've identified. By taking action to treat validated threats, organizations can reduce the likelihood of experiencing business disruptive cyber attacks. |

While traditional cybersecurity approaches focus on reacting to specific threats, this reactive approach often falls short in addressing the evolving threat landscape. Tactical measures may provide temporary relief, but they fail to address the underlying risk of future attacks. CTEM offers a more proactive and effective approach, prioritizing threats that pose the greatest risk to your organization's business objectives.

By embracing this proactive approach, you can proactively defend against and neutralize threats before they can cause irreversible damage to your organization's business objectives. Below are recommended steps to implement your CTEM.

### Step 1: Scope for cybersecurity exposure, first for external and SaaS threats

The first step in continuous threat exposure management is to scope your organization's attack surface, encompassing both external and SaaS threats. This attack surface extends beyond the traditional focus of vulnerability management programs and includes not just devices, apps, and applications but also fewer tangible elements like corporate social media accounts, online code repositories, and integrated supply chain systems. Organizations embarking on their first CTEM initiative can consider focusing on either the external attack surface, where a narrower scope aligns with a growing ecosystem of tools, or the SaaS security posture, which has gained increasing importance with the rise of remote work and the proliferation of critical business data hosted on SaaS platforms.

With NSFOCUS RSAS, you can effectively scope your organization's attack surface, identify potential vulnerabilities, and prioritize threats based on their impact on your business goals. Our comprehensive solution empowers you to take a proactive approach to cybersecurity and safeguard your organization from a wide range of threats.

**Click here for the datasheet:**

- Remote Security Assessment System

### Step 2: Develop a discovery process for assets and their risk profiles

While initial discovery efforts may focus on areas identified during the scoping phase, comprehensive CTEM programs should encompass the identification of both visible and hidden assets, vulnerabilities, misconfigurations, and other potential risks. Mistaking scoping for discovery is a common pitfall in CTEM program implementation. The sheer volume of discovered assets and vulnerabilities is not a measure of success. Instead, the true value lies in accurately scoping the attack surface based on business risk and potential impact.

NSFOCUS's EASM, DPRS, VA and WebSafe services can guide you through the entire CTEM process, from scoping to discovery, ensuring that your organization's attack surface is thoroughly assessed and that potential threats are prioritized based on their true risk to your business. Our comprehensive solution helps you avoid the pitfalls of traditional discovery approaches and achieve a truly effective CTEM program.

**Click here for the datasheets:**

- External Attack Surface Management
- Vulnerability Assessment
- Security Assessment Services
- WebSafe
- Digital Risk Protection Services

### Step 3: Prioritize the threats most likely to be exploited

Prioritization of identified security issues is crucial for effective CTEM implementation. Rather than attempting to address every single issue, organizations should consider factors such as urgency, security impact, availability of compensating controls, tolerance for residual attack surface, and the overall level of risk posed to the organization. The key lies in identifying high-value assets and focusing on a treatment plan that prioritizes these critical components.

Leveraging Vulnerability Prioritization Technology (VPT), NSFOCUS's EASM service provides advanced prioritization capabilities that help you identify and address the most critical security issues first. Our intelligent risk assessment engine considers a wide range of factors, including threat intelligence obtained by multi-source data correlation analysis, to ensure that your organization's resources are allocated effectively and that high-value assets are protected from potential threats.

**Click here for the datasheets:**

- External Attack Surface Management
- Threat Intelligence
- Vulnerability Assessment and Penetration Testing

### Step 4: Validate how attacks might work and how systems might react

Effective CTEM implementation goes beyond simply identifying vulnerabilities; it involves validating the exploitability of those vulnerabilities, analyzing potential attack pathways, and ensuring that response plans are robust and timely. Additionally, gaining consensus among stakeholders on remediation triggers is crucial for successful CTEM implementation. A study predicts that by 2026, organizations that prioritize security investments based on a continuous exposure management program will be three times less likely to experience a breach.

NSFOCUS's PTaaS, Red Teaming and BAS services go beyond traditional vulnerability management by providing comprehensive vulnerability validation, attack pathway analysis, and remediation prioritization capabilities. Our solution empowers you to make informed decisions about resource

allocation, ensuring that your organization's most critical assets are protected. By leveraging NSFOCUS services, you can significantly reduce your risk of breaches and safeguard your business from evolving threats.

**Click here for the datasheets:**

- Penetration Testing as a Service
- Red Teaming

### Step 5: Mobilize people and processes

While automated remediation can be beneficial for certain low-risk and non-disruptive issues, comprehensive CTEM implementation requires proactive communication and collaboration. Clearly communicate your CTEM plan to both the security team and business stakeholders, ensuring that everyone understands the objectives and their roles. The mobilization phase focuses on operationalizing CTEM findings by eliminating any roadblocks to approvals, implementation processes, or mitigation deployments. Documenting cross-team approval workflows is essential for streamlining the process and ensuring accountability.

NSFOCUS's incident response and security awareness training services facilitate seamless communication and collaboration among stakeholders, ensuring that CTEM findings are translated into actionable steps. Our solution provides comprehensive documentation capabilities, enabling you to clearly capture and share remediation plans, approval workflows, and mitigation strategies. With NSFOCUS's services, you can effectively mobilize your teams and achieve the desired outcomes from your CTEM program.

**Click here for the datasheets:**

- Incident Response
- Security Awareness Training