DATASHEET

NSFOCUS

CTEM

Continuous Threat Exposure Management

OVERVIEW

CTEM is a continuous process that helps organizations identify, assess, and mitigate cyber threats. It does this by:

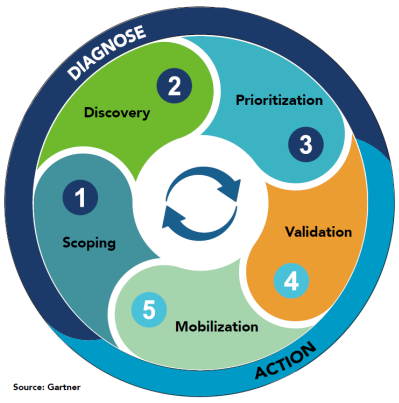
- Scanning for vulnerabilities and exposures
- Prioritizing risks
- Implementing remediation actions
- Measuring the effectiveness of those actions

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 and business operation changes.

It's difficult to define the security risk related to business initiatives while achieving a balance between over-protection and negatively impacting a company's risk tolerance levels.

Proactive security defense requires both security validation and threat exposure management. This creates a consistent, actionable security posture remediation and improvement plan that connects to business risks and initiatives.

CONTINUOUS THREAT EXPOSURE MANAGEMENT



Gartner identifies continuous threat exposure management (CTEM) as a programmatic approach to managing exposure risk, optimizing cyber programs, and improving cyber resilience.

CTEM is not a one-time solution. It's an ongoing process that helps organizations stay ahead of the latest threats.

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** **Discovery** **Prioritization**	» Cyber Asset Attack Surface Management (CAASM) » External Attack Surface Management (EASM) » Exposure Management (EM) » Remote Security Assessment System (RSAS) » Digital Risk Protection Service (DRPS) » WebSafe » Source Code Review » Vulnerability Assessment (VA) » Configuration Verification » Vulnerability Prioritization Technology (VPT)	» Identify your most valuable assets and data. By identifying the critical assets and data, organizations can prioritize their resources and focus their efforts on the areas that are most at risk. » 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. » 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** **Mobilization**	» Breach and Attack Simulation (BAS) » Exposure Management (EM) » Penetration Testing as a Service (PTaaS) » Red Teaming » Incident Response (IR) » Consulting Service » 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. » Take action to mitigate the threats you've identified. By taking action to mitigate validated threats, organizations can reduce their risk of being attacked.

EASM

NSFOCUS EASM is an external attack surface management (EASM) solution that continuously discovers and maps your internet-exposed assets, finds potential risks, and sends alert email when high risk vulnerability is detected. It also provides emergency vulnerability announcement, prioritization and remediation, and vulnerability analysis.

- Gain visibility of your internet-exposed assets and potential risks.
- Receive timely notification of critical and emergent vulnerabilities.
- Prioritize risks and vulnerabilities and create remediation plan.
- Find misconfigured assets, network architecture flaws, data exposures, authentication and encryption weaknesses, or other risks including CVEs.
- Perform advanced penetration testing on customer assets.

Click here for the datasheet: EASM datasheet

PTaaS

NSFOCUS PTaaS is a cloud-based PTaaS solution that helps organizations improve their security posture by providing a comprehensive set of features that are essential for CTEM.

- Vulnerability scanning: PTaaS can scan for vulnerabilities in an organization's assets, including web applications, APIs, and infrastructure.
- Penetration testing: PTaaS can simulate real-world attacks on an organization's assets to identify and exploit vulnerabilities.
- Incident response: PTaaS can be used to investigate and respond to security incidents.
- Compliance reporting: PTaaS can generate reports that demonstrate an organization's compliance with security standards.

Click here for the datasheet: PTaaS datasheet

RSAS

NSFOCUS RSAS is a security assessment tool that helps organizations manage risks, meet regulatory compliance, and ensure secure configurations. RSAS can help organizations mitigate vulnerabilities and prevent potential disasters. RSAS can be used as part of a CTEM program to help organizations continuously scan for vulnerabilities, prioritize risks, and implement remediation plans.

- Risk identification and prioritization: RSAS can help organizations identify and prioritize risks by using a variety of methods, such as vulnerability scanning, penetration testing, and threat intelligence. This can help organizations focus their security efforts on the most critical risks.
- Vulnerability assessment: RSAS can help organizations assess their vulnerabilities by scanning for known vulnerabilities and identifying potential attack vectors. This can help organizations identify and fix vulnerabilities before they can be exploited by attackers.
- Real-world attack simulation: RSAS can help organizations simulate real-world attacks to test their defenses and identify weaknesses. This can help organizations improve their security posture by identifying and fixing gaps in their defenses.
- Compliance reporting: RSAS can generate reports that demonstrate an organization's compliance with security standards. This can help organizations demonstrate to regulators and auditors that they are taking security seriously.

Click here for the datasheet: RSAS datasheet