PICUS

OPERATIONALIZING CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM) WITH PICUS

Executive Summary

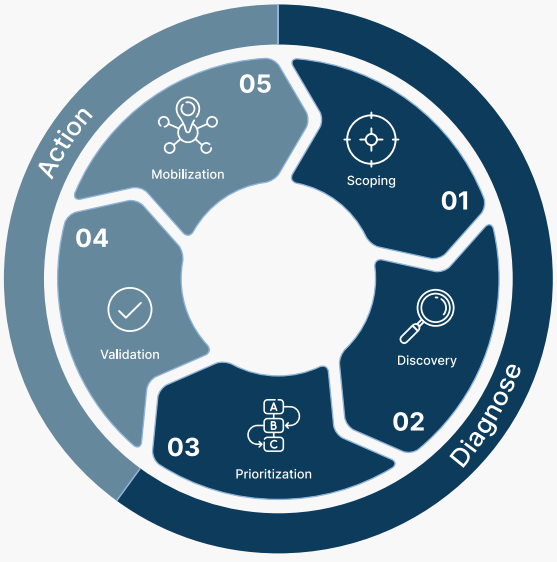
Continuous Threat Exposure Management (CTEM) is a more practical and systematic approach compared to traditional risk-based vulnerability management (RBVM) processes or preventative-only approaches. By running a CTEM program, organizations can continually assess the accessibility and vulnerability of their physical and digital assets, and prioritize remediation efforts based on standard processes for risk acceptance and operational viability.

Picus aligns with the CTEM process by providing tools to identify and analyze an organization's entire attack surface, simulate a variety of attack scenarios, and validate security controls through controlled attack simulations and adversary emulations. By operationalizing the CTEM process with Picus, organizations can proactively identify and mitigate cyber threats, improving their overall cyber resilience.

CTEM: A Recap

Continuous Threat Exposure Management (CTEM) is a program by Gartner that helps organizations achieve long-term cyber resilience. It is not a specific technology or tool, but rather a continuous process.

CTEM consists of five steps:



01 **Scoping:** Identify business objectives and potential high-critical impacts.

02 **Discovery:** Pinpoint vulnerabilities and weak points in infrastructure.

03 **Prioritization:** Determine which threats are most likely to be exploited based on potential impact and other factors.

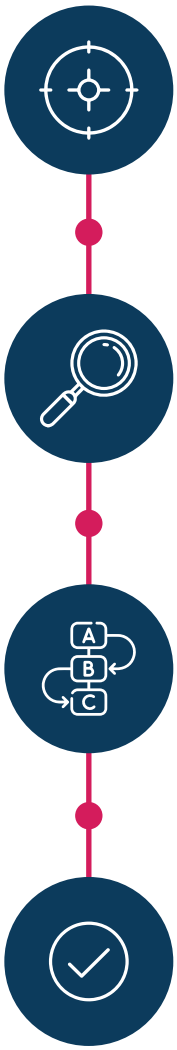
04 **Validation:** Conduct controlled simulations or adversary emulations in production environments.

05 **Mobilization:** Ensure CTEM findings are smoothly operationalized through defined communication standards and cross-team approval workflows.

These steps allow organizations to prioritize potential threats and corresponding remediation efforts based on their attack surface. This is a more practical and systematic approach compared to traditional risk-based vulnerability management (RBVM) processes or preventative-only approaches that may not be feasible.

By running a CTEM program, an organization can continuously assess the accessibility and vulnerability of their physical and digital assets. They can then prioritize remediation efforts based on standard processes for risk acceptance and operational viability.

How Picus Aligns with CTEM



Scoping

Picus can be used to identify and analyze an organization's entire attack surface, including external, internal, and cloud-based threats. This information can be used to define the scope of the CTEM initiative, ensuring that all relevant infrastructure segments are included in the process.

Discovery

With the ability to simulate a variety of attack scenarios, you can expose vulnerabilities and misconfigurations in the organization's security infrastructure, helping to identify areas for improvement. This information can be used to prioritize the most pressing threats and weak points and to develop remediation plans.

Prioritization

Organizations prioritize threats, weak points, and remediation efforts based on business criticality and the likelihood of exploitation. This allows security teams to focus their efforts on the most pressing issues and ensure that resources are used effectively.

Validation

To ensure that the organization's security controls are effective in preventing and detecting cyber attacks, it is important to validate them through controlled attack simulations and adversary emulations. Picus offers a range of automated and continuous technical assessments to validate the organization's cyber security posture and provide actionable insights for improvement. By operationalizing the CTEM process with Picus, organizations can proactively identify and mitigate cyber threats, improving their overall cyber resilience.

Operationalize CTEM with The Picus Platform REQUEST A DEMO

FROST & SULLIVAN LEADING VENDOR IN BAS MARKET 2020

2021 Cyber Security Awards WINNER BEST SECURITY PRODUCT OF THE YEAR

CYBERTECH100 2021 The World's Most Innovative CyberTech Companies for Financial Services

2021 Computing Security Awards WINNER Breach and Attack Simulation Solution of the Year

CYBER SECURITY EXCELLENCE AWARDS WINNER 2022