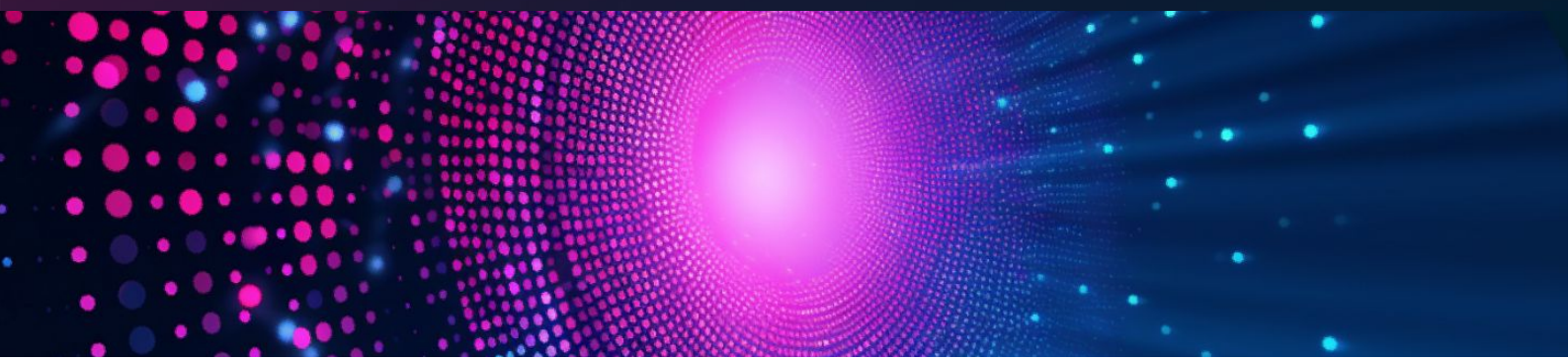
PICUS

# Checklist for Exposure Validation Solutions in CTEM



Exposure Validation technologies play a critical role in a Continuous Threat Exposure Management (CTEM) program by ensuring that vulnerabilities and security gaps are not only identified but actively tested for potential exploitation. As organizations adopt CTEM to maintain a proactive security posture, Exposure Validation has become the cornerstone of the strategy, allowing security teams to prioritize remediation efforts based on verified risks.

However, not all exposure validation solutions are the right fit for a CTEM program. Selecting the right tool requires careful consideration of various factors to ensure it supports continuous and dynamic threat management.

To this end, Picus has prepared this checklist for organizations looking to elevate their CTEM program to the next level. Addressing the questions below can help security teams channel their resources toward the most impactful and validated threats, establishing an efficient and effective CTEM program.

#1

# Scoping

The Scoping step of CTEM is the initial step in which security teams identify the infrastructure segments to be included in the program. During this step, security teams define the assets, networks, applications, and systems that will be assessed for potential vulnerabilities and exposures.

- [ ] **Does the solution cover on-premises, cloud, and hybrid environments?**

  Exposure Validation solutions should assess risks in on-premises, cloud, and hybrid environments. Comprehensive coverage helps ensure the CTEM program fully evaluates all environments to provide a holistic view of potential exposures.

- [ ] **Does the solution integrate with vulnerability management (VM) or cyber threat intelligence (CTI)?**

  A robust Exposure Validation solution should be able to integrate with VM and CTI tools. Integration allows more control over the CTEM scope, making exposure management more effective than isolated tools by streamlining insights across platforms.

- [ ] **Does the solution offer attack scenarios for effective scoping?**

  Every organization has unique risks. Exposure Validation solutions should provide attack scenarios that align with specific threat landscapes, helping security teams prioritize critical vulnerabilities for more effective CTEM scoping.

- [ ] **Can the solution validate exposures across all asset types?**

  The solution should assess exposures in all assets, including hardware, digital, and virtualized systems. By providing asset-specific insights, exposure validation solutions help security teams understand the potential impact and prioritize remediation strategies.

#2

# Discovery

In the Discovery step of a CTEM program, security teams meticulously identify all assets, including the hidden ones, and evaluate their risk profiles based on the scope. The Discovery step provides a comprehensive view of the organization's attack surface, laying the foundation for an effective CTEM process.

- [ ] **Does the solution provide asset discovery for on-premises, cloud, and hybrid networks?**

  An effective Exposure Validation solution should perform comprehensive asset discovery across all environments, directly or through integration with attack surface management platforms. This ensures full visibility into all assets, including servers, endpoints, containers, IoT devices, and shadow IT, for a complete attack surface overview.

- [ ] **Does the solution integrate with Vulnerability Assessment and Management tools?**

  Exposure Validation solutions should integrate seamlessly with vulnerability assessment tools. This integration allows automated import of findings, coordination in remediation, and real-time visibility into risk by synchronizing updates between the tools and solution.

- [ ] **Does the solution support automated attack path mapping and analysis?**

  Automated attack path mapping illustrates potential lateral movement routes to critical assets. This includes visualizing chokepoints and escalation paths and helping the security team pinpoint where to prioritize mitigation for optimal risk reduction.

- [ ] **Can the solution identify misconfigurations and security weaknesses beyond CVEs?**

  Exposure Validation should uncover misconfigurations and weaknesses like weak passwords, unpatched software, and misconfigured firewall rules. These insights are essential to address security risks that are not tied to specific CVEs but are still vulnerable to exploitation.

#3

# Prioritization

In the Prioritization step of a CTEM program, security teams prioritize exposures identified in the Discovery step by considering the business criticality of assets, the likelihood of exploitation of discovered weak points, and the availability of compensating security controls.

- [ ] **Can the solution adjust prioritization based on real-time threats?**

  An effective Exposure Validation solution should integrate real-time threat intelligence, dynamically prioritizing vulnerabilities based on active threats and exploits. This includes recalibrating priorities if a vulnerability is actively targeted. Threat advisories, exploit data, and attack campaigns are crucial for timely exposure prioritization.

- [ ] **Does the solution identify attack paths and prioritize chokepoints?**

  Exposure Validation solutions should identify attack paths and chokepoints where attackers could exploit vulnerabilities for lateral movement. Prioritizing these vulnerabilities aids in disrupting attack paths effectively by focusing on critical points for mitigation.

- [ ] **Does the solution support exposure prioritization based on adversary TTPs?**

  Mapping exposures to known adversary Tactics, Techniques, and Procedures (TTPs) helps align prioritization with real-world attack methods. Exposure Validation solutions should enable security teams to focus on vulnerabilities that fit typical attack chains, enhancing mitigation of likely exploitation paths.

- [ ] **Can the solution provide prioritization based on the likelihood of exploitation and ease of attack?**

  Exposure Validation solutions should consider factors like ease of exploitation, available exploit code, and common attack vectors. Vulnerabilities more likely to be exploited should be automatically prioritized, helping security teams focus on the most actionable risks.

#4

# Validation

In the Validation step In CTEM, security teams verify the security posture of their organizations against the prioritized exposures. The use of offensive security methods such as controlled attack simulation and adversary emulations has become the industry standard for the Validation step.

- [ ] **Does the solution offer adversarial exposure validation technologies like BAS, Automated Pentesting, and Autonomous Red Teaming?**

  An effective Exposure Validation solution should include automated testing such as Breach and Attack Simulations, Automated Penetration Tests, and Autonomous Red Teaming. These capabilities confirm if exposures are exploitable, enabling security teams to prioritize real threats based on validated risks.

- [ ] **Can the solution simulate real-world attack scenarios for validation?**

  Exposure Validation solutions should simulate real-world attacks to validate exposures and test security controls. This ensures identified exposures are exploitable by adversaries and provides insights on the impact of successful exploits to improve remediation prioritization.

- [ ] **Does the solution support adding and simulating custom threats and exploits?**

  Exposure Validation solutions should enable security teams to add custom threats for simulation, allowing them to assess resilience against unique attack methods. This enhances the proactive identification of weaknesses and enables tailored remediation for both common and organization-specific threats.

- [ ] **Does the solution provide detailed reports on validated exposures and remediation?**

  Exposure Validation solutions should deliver reports detailing exposure exploitability, impact, and remediation effectiveness. These should include metrics on validation tests, successful exploits, and overall risk reduction, providing clear insights into the remediation's impact.

#5

# Mobilization

In the Mobilization step of a CTEM program, security teams focus on their remediation and mitigation strategies based on the prioritized and validated exposures identified in previous steps. This phase involves assigning responsibilities, setting timelines, and coordinating efforts across different departments to ensure swift and efficient resolution of security gaps.

- [ ] **Does the solution provide actionable and easy-to-apply remediation suggestions?**

  Exposure Validation solutions should offer remediation recommendations with step-by-step guidance, vendor-specific signatures, detection rules, and best practices. These resources support effective, practical implementation of remediation efforts tailored to validated exposures.

- [ ] **Does the solution support the automation of remediation workflows?**

  Exposure Validation solutions should provide automation in remediation workflows, including task assignments, notifications, and tracking. Integration with ticketing and collaboration tools streamlines the response process, ensuring exposures are addressed swiftly and efficiently.

- [ ] **Can the solution validate remediation effectiveness after implementation?**

  Exposure Validation solutions should offer features to validate the effectiveness of remediation efforts once they have been implemented. This includes re-validating exposures to confirm that they have been adequately addressed and that the security posture has improved as a result of remediation actions.

- [ ] **Can the tool provide metrics and reporting on mobilization efforts?**

  Exposure Validation solutions should offer metrics and reporting capabilities to evaluate the effectiveness of mobilization efforts. Comprehensive reports enable management to assess remediation effectiveness, evaluate mobilization success, and inform future strategies.

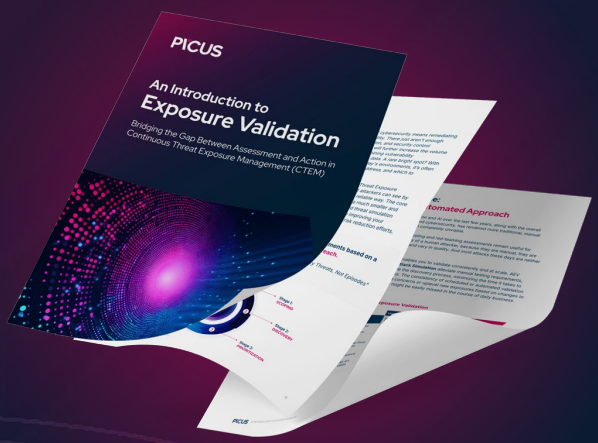
# About PICUS

Since pioneering Breach and Attack Simulation (BAS) technology in 2013, Picus Security has been at the forefront of helping organizations continuously assess and improve their cybersecurity posture. Picus Security Validation Platform delivers unmatched, actionable insights into your exposures, equipping you with the proactive awareness needed to stay ahead of evolving threats.

Picus Platform goes beyond reactive assessments, enabling you to validate and address exposures before they impact your operations. By simulating real-world attack scenarios and conducting automated penetration tests, security teams gain the accuracy and visibility needed to optimize defenses and protect critical assets.

Trusted by enterprises worldwide, Picus is committed to making exposure validation an integral part of every organization's defense strategy.

Begin your journey toward greater resilience and risk clarity at **picussecurity.com**




## Learn More About
## Exposure Validation

**DOWNLOAD THE eBOOK**

FROST & SULLIVAN
FROST RADAR™ LEADER
Global Breach and Attack Simulation
2022

CYBER SECURITY EXCELLENCE AWARDS
★ WINNER ★
2023

GLOBAL INFOSEC AWARDS
WINNERS
CYBER DEFENSE MAGAZINE
2024

Gartner
Peer Insights
Customers' Choice 2024

4.8/5.0
**Highest-rated vendor***
Breach and Attack Simulation

*Gartner, Voice of the Customer for Breach and Attack Simulation Tools, Peer Contributors, 30 January 2024