



# Leveraging SCYTHE for Continuous Threat Exposure Management (CTEM)

**Author**

Marc Brown  
VP - Product & Sales - SCYTHE

*A Guide to Strengthening Enterprise Cyber  
Defences with Adversarial Emulation &  
Validation (AEV)*

# Introduction



With its ability to emulate real-world attacks and integrate with existing tools, SCYTHER aligns seamlessly with CTEM, transforming reactive defenses into proactive resilience.

## **The Escalating Cyber Threat Landscape**

Cyberattacks have evolved from opportunistic exploits to highly targeted campaigns leveraging advanced persistent threats (APTs), zero-day vulnerabilities, and supply chain weaknesses. In 2024 alone, ransomware payments exceeded \$1 billion globally, with dwell times averaging 60 or more days<sup>1</sup>—ample time for attackers to escalate privileges and exfiltrate data.

## **Gartner's CTEM Framework: A Proactive Shift**

Gartner's Continuous Threat Exposure Management (CTEM) framework redefines cybersecurity by emphasizing ongoing visibility, prioritization, and validation of risks. Its five phases—Scoping, Discovery, Prioritization, Validation, and Mobilization—enable organizations to systematically reduce exposure in real time, bridging the gap between static audits and dynamic threats.

## **SCYTHER: Adversarial Emulation & Validation as a Game Changer**

SCYTHER is a Breach and Attack Simulation (BAS+) or Adversarial Emulation and Validation (AEV) platform that empowers enterprises to emulate adversary TTPs and validate security controls automatically and continuously. With its ability to emulate real-world attacks and integrate with existing tools, SCYTHER aligns seamlessly with CTEM, transforming reactive defenses into proactive resilience.

# Challenges of Cybersecurity Without Continuous Validation

## Complexity of Modern IT Environments

Today's enterprises manage hybrid ecosystems—on-premises servers, multi-cloud deployments, OT/ICS systems, and remote endpoints. This complexity obscures visibility, with 45% of CISOs reporting incomplete asset inventories (SANS Institute, 2024).

## Configuration Drift and Fluid Asset Management

Configuration drift—where systems diverge from secure baselines—occurs in 70% of organizations annually due to updates or human error (Verizon DBIR). Fluid assets, such as ephemeral cloud instances or BYOD devices, further complicate tracking, leaving vulnerabilities unaddressed.

## Overlooked IT Exceptions and Blind Spots

Temporary exceptions for legacy systems or critical apps often become permanent, while shadow IT introduces unmanaged risks. For example, 30% of breaches exploit misconfigured cloud assets (IBM Security).

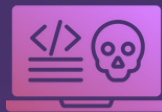
## The High Stakes of Inaction

Without continuous validation:



### Silent Failures

62% of organizations discover control failures only post-breach (Ponemon Institute).



### Prolonged Exposure

Unvalidated defenses extend attacker dwell time, increasing damage by 40% (FireEye).



### Regulatory Fines

Non-compliance with frameworks like PCI DSS or NIST 800-53 escalates penalties.

# The Business Case: Costs, ROI, and Statistics

- **The Financial and Operational Toll of Gaps in Validation**
  - Breach Costs: The average cost of a breach in 2024 was **\$4.45 million**, with critical infrastructure sectors hitting **\$4.82 million** (IBM).
  - Ransomware Impact: Recovery costs average **\$1.85 million**, with **19%** of victims paying ransoms exceeding **\$500,000** (Sophos).
  - Reputation Loss: **34%** of breached companies lose over **20% of customers** (Cisco).
- **ROI and Savings Through CTEM and SCYTHE**
  - Risk Reduction: Gartner forecasts a **66%** breach reduction for CTEM adopters by 2026.
  - Tool Optimization: SCYTHE cuts redundant security spending by **25%**, **saving \$500,000** annually for mid-sized firms.
  - Efficiency Gains: Automated validation reduces MTTD/MTTR by **50%**, per NIST studies.
- **Compelling Business Statistics**
  - Priority: **91%** of executives prioritize continuous security testing (Deloitte, 2024).
  - Incident Reduction: Companies with validated controls report **45%** fewer incidents (Forrester).
  - Savings: CTEM adoption could save **\$1.5 trillion** in global breach costs by 2030 (Gartner).

## SCYTHE and the CTEM Framework: A Strategic Alignment

### SCYTHE's Core Capabilities

SCYTHE combines adversarial emulation with automated validation:

01

#### Threat Emulation:

Emulates TTPs, IOCs, and Threats from APT groups like APT29 or ransomware strains like Conti.

02

#### Flexible Deployment:

Supports agent-based and agentless testing across IT, OT, and cloud.

03

#### Tool Integration:

Syncs with your security stack, like DLP (e.g., Proofpoint), EDR (e.g., CrowdStrike), SIEM (e.g., Splunk), SOAR (e.g., Palo Alto), and ticketing (e.g., ServiceNow) platforms.

04

#### Custom Campaigns:

Allows tailored attack scenarios for specific industries, threats, security products, or policies.

# Deep Dive: Phase 4 – Validation with Automated Continuous Security Control Testing

Validation is the linchpin of CTEM—it's where assumptions about security controls are tested against real-world attack scenarios. Without it, organizations operate on blind faith, assuming tools like EDR, DLP, or firewalls perform as advertised. In reality, 50% of security tools fail to detect advanced threats due to misconfiguration, outdated rules, or vendor overpromises (SANS Institute). Manual testing—such as annual pen tests—cannot keep pace with daily changes in assets, configurations, and threats, leaving gaps that attackers exploit.

Manual validation is slow, inconsistent, resource-intensive, often covering only 10-15% of an attack surface per cycle (Gartner). Automated continuous security control validation addresses this by:

- ▶ **Real-Time Feedback:** Detects control failures as they occur, not months later.
- ▶ **Scalability:** Tests thousands of endpoints, cloud instances, and OT devices simultaneously.
- ▶ **Consistency:** Eliminates human error and ensures repeatable, standardized testing.
- ▶ **Threat Relevance:** Adapts to emerging TTPs from frameworks like MITRE ATT&CK or real-time threat intelligence.

Without automation and continuity, organizations risk:

- **False Positives/Negatives:** Unvalidated SIEM rules generate noise, obscuring real alerts (e.g., 70% of SOC alerts are ignored, per ESG).
- **Undetected Gaps:** A single untested endpoint can become a pivot point—60% of breaches start here (Verizon DBIR).

## SCYTHE transforms validation into a proactive, automated process:

### Adversarial Emulation:

- Emulates multi-stage attacks, such as privilege escalation (T1078) or data exfiltration (T1041).
- Example: SCYTHE mimics a ransomware attack by encrypting test files, testing EDR blocking and backup restoration in real time.

### Control Testing:

- Validates specific tools: Does your DLP block sensitive file transfers? Does your SIEM correlate lateral movement logs?
- Example: SCYTHE tests an EDR's ability to stop a PowerShell-based attack (T1059.001), revealing if it's misconfigured or bypassed.

### Continuous Operation:

- Runs scheduled or on-demand campaigns, ensuring controls remain effective as environments evolve.
- Example: Daily tests detect if a new adversarial technique can bypass deployed EDR rules, inadvertently exposing a critical server.

### Metrics and Reporting:

- Provides pass/fail results, detection rates, and remediation steps.
- Example: A dashboard shows a 75% success rate against ransomware TTPs, prompting DLP tuning.

## Real-World Impact



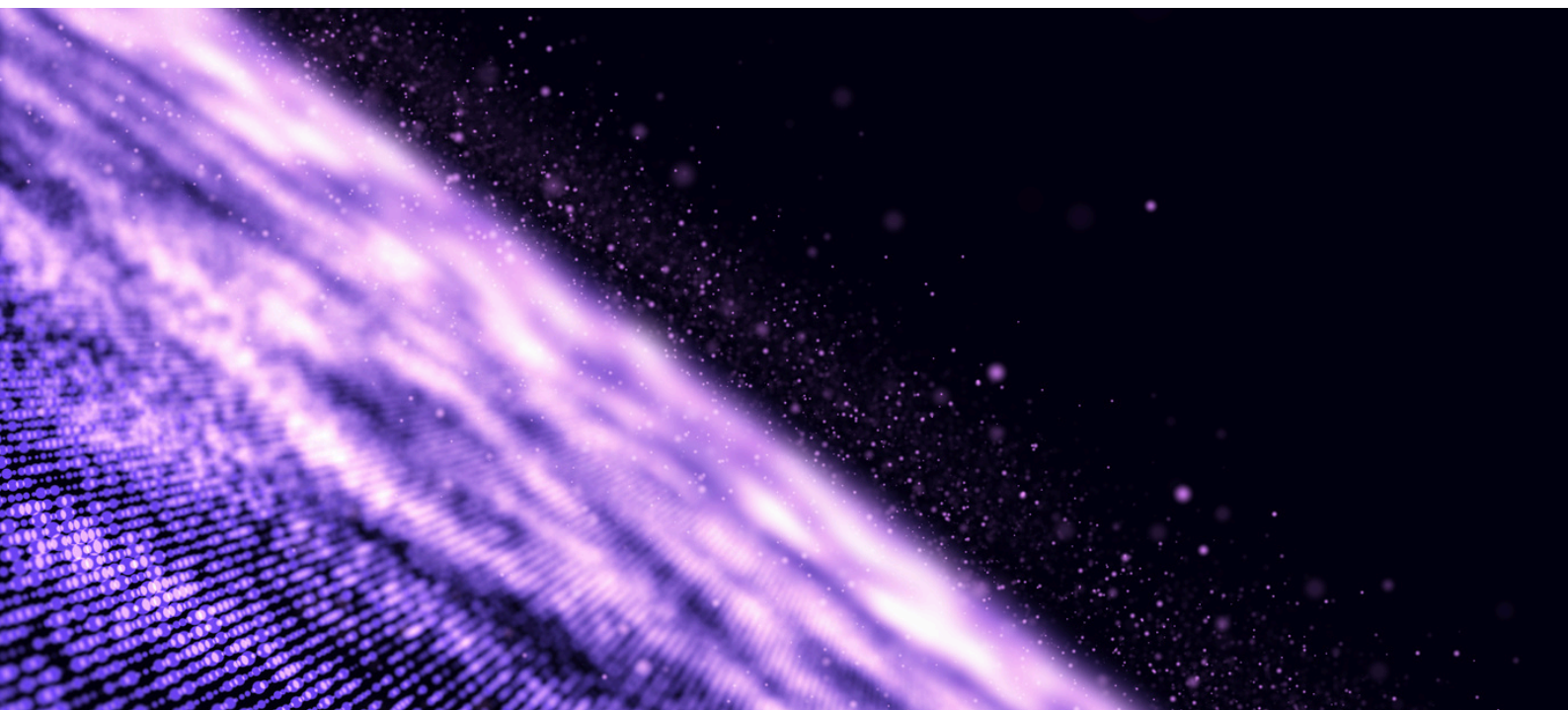
### Case Study

A financial firm used SCYTHE to validate its EDR against APT28 TTPs. It discovered 30% of endpoints lacked proper agent installation, a gap missed by static audits. Post-remediation, detection rates rose from 60% to 98%.



### Criticality Proof:

During a 2024 ransomware surge, a SCYTHE-equipped manufacturer validated its EDR daily, thwarting an attack that crippled peers relying on quarterly tests.



# Implementation Guidance: Deploying SCYTHE for CTEM – Phase 4: Validation

Validation is the linchpin of Gartner’s Continuous Threat Exposure Management (CTEM) framework, turning security assumptions into actionable evidence. SCYTHE’s Adversarial Emulation and Validation (AEV) capabilities make it indispensable in this phase, delivering continuous, automated testing to ensure controls withstand real-world threats. Here’s how SCYTHE provides visibility into key areas of your security posture.

**Simulate and Validate:** SCYTHE emulates industry-relevant attacks—such as phishing, lateral movement (e.g., PowerShell exploitation), or ransomware encryption—testing your defenses 24/7 and revealing gaps as they emerge.

## 1. Overall Cyber Hygiene and Exposure Visibility:

SCYTHE assesses cyber hygiene by simulating attacks and generating probability scores (e.g., 0-100) that reflect your ability to thwart specific cyber threats. For instance, a phishing campaign might yield an 85% success rate in blocking malicious emails, while a ransomware test could show a 90% probability of containment. These scores, derived from real-time emulation data, highlight exposures like unpatched systems, weak configurations, or user vulnerabilities, enabling targeted hygiene improvements.



### How to Use:

Run recurring campaigns (e.g., weekly phishing tests) and review SCYTHE’s dashboard for aggregated scores, pinpointing areas like outdated endpoints or lax email filters needing attention.



## 2. Endpoint Security Tooling Onboarding:

SCYTHE validates the installation, configuration, and operation of endpoint security tools (e.g., EDR like CrowdStrike or SentinelOne). It simulates endpoint attacks—such as malware execution or privilege escalation—to confirm agents are deployed correctly, configured to detect threats, and operational across all devices. For example, SCYTHE can reveal if 20% of endpoints lack an EDR agent or if policies fail to block a malicious process.



### How to Use:

Deploy a test campaign targeting endpoints, then analyze SCYTHE's logs to verify agent presence (e.g., installation success on 95% of devices) and operational status (e.g., 98% detection rate). Adjust onboarding processes based on gaps identified.

## 3. Testing Security Tool Performance and Control Validation:

SCYTHE tests the performance of deployed security tools—EDR, DLP, SIEM, firewalls—by emulating attacks and validating control efficacy. It identifies gaps (e.g., a SIEM missing lateral movement alerts) and suggests remediation, such as generating SIGMA rules for improved detection. For instance, a DLP test might show only 80% of sensitive data transfers are blocked, prompting policy tweaks.



### How to Use:

Launch a multi-stage attack (e.g., phishing to exfiltration) and review SCYTHE's reports for tool-specific metrics—detection rates, false negatives, and latency. Export SIGMA-compatible rules from SCYTHE to enhance SIEM or EDR coverage, closing identified gaps.

#### 4. TTP Coverage Analysis:

SCYTHE maps its emulations to MITRE ATT&CK, providing visibility into TTP coverage across your defenses. It tests tactics like T1566.001 (Phishing: Spearphishing Link), T1078 (Valid Accounts), or T1486 (Data Encrypted for Impact), revealing which TTPs your tools detect or miss. For example, a campaign might show 90% coverage for initial access but only 60% for persistence, guiding control enhancements.



##### How to Use:

Configure SCYTHE to run a comprehensive ATT&CK-aligned campaign, then analyze the coverage report to identify weak spots (e.g., low detection of T1059.001 – PowerShell). Prioritize mitigation based on adversary relevance to your industry.

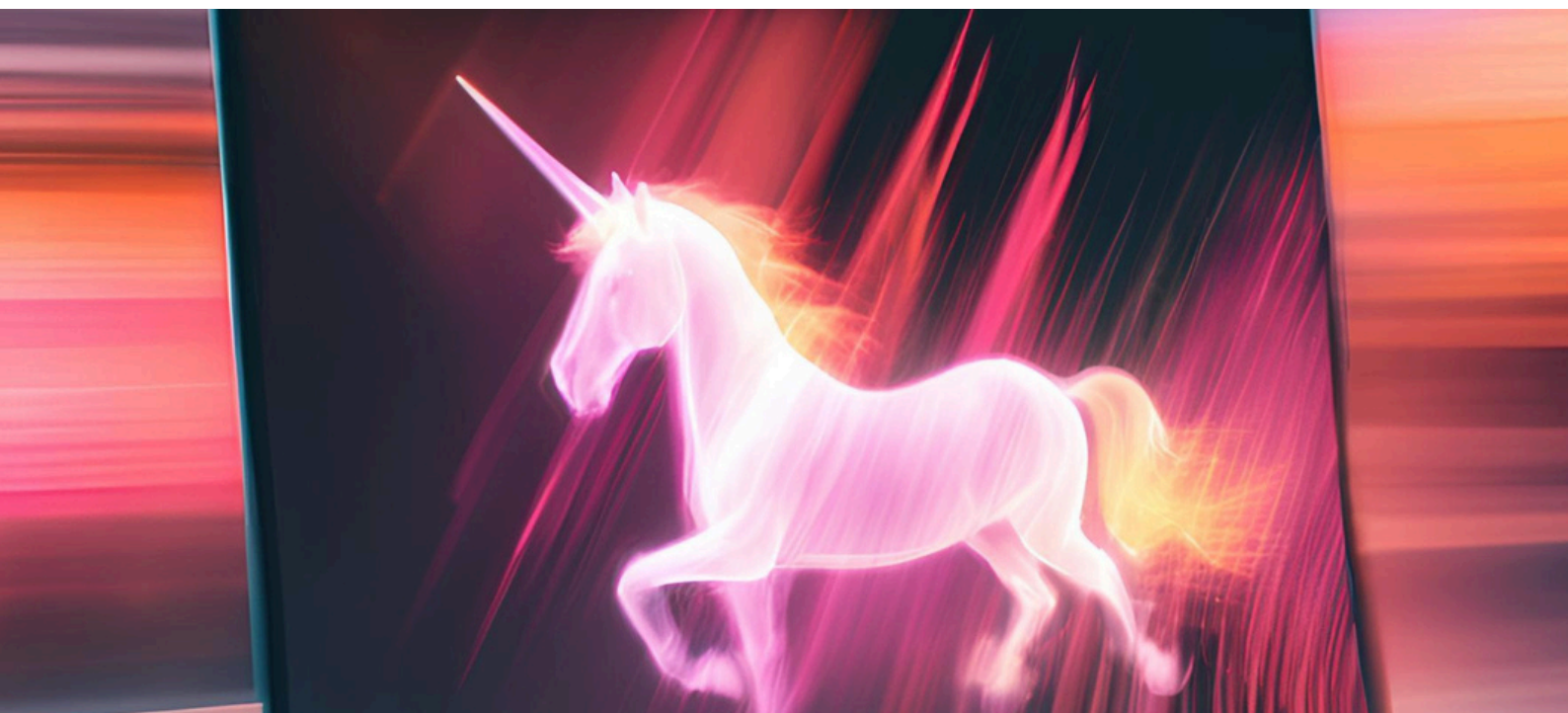
#### 5. Common Policy Audits:

SCYTHE audits compliance with common security policies—such as password strength, access controls, or patch management—by simulating policy violations. For instance, it can test if weak credentials (e.g., 'Password123') allow account compromise or if unpatched systems permit exploitation, flagging deviations from standards like NIST 800-53 or CIS Controls.



##### How to Use:

Set up a policy-focused campaign (e.g., brute-force login attempts) and review SCYTHE's results for policy failures (e.g., 30% of accounts vulnerable). Use findings to enforce stricter configurations or update compliance documentation.



## Actionable Outcomes

SCYTHE's continuous AEV delivers detailed metrics—detection rates, failure points, and remediation steps—via its dashboard and integrations (e.g., Splunk). This empowers SOC and IT teams to act swiftly, ensuring Validation isn't a one-time check but a dynamic shield against evolving threats. In this critical phase, SCYTHE's active role transforms visibility into resilience.

Continuous validation with SCYTHE and CTEM is not optional—it's a survival imperative in a threat landscape where attackers strike daily.



## About SCYTHE

SCYTHE is a leader in adversarial emulation and continuous security validation, empowering organizations to proactively identify exposures, validate security controls, and measure risk against real-world threats. Trusted by top enterprises and government agencies, SCYTHE enables security teams to automate threat testing, enhance cyber resilience, and maximize security investments.

[Book demo](#)

