scythe.io

SCYTHE | PLATFORM OVERVIEW 2026

SCYTHE PLATFORM

Adversarial Exposure Validation: Continuous Validation of Defenses Against Real-World Threats

SUMMARY

SCYTHE delivers an AI-enabled Adversarial Emulation & Validation (AEV) platform that empowers teams to proactively assess, test, and strengthen defenses. Through automated, realistic tests and seamless integrations (e.g., EDR, SIEM, ITSM), SCYTHE enables teams to identify exposures and validate controls across IT and OT/ICS environments.

SOLUTION

Designed to satisfy the broadest organizational deployment needs, the SCYTHE platform supports SaaS, on-premises, and air-gapped deployments, with or without agents, providing foundational detection assurance.

Key capabilities included:

- AI-driven dynamic generation of realistic adversary tests
- Continuous agent-based and agentless testing of security controls
- Seamless, bi-directional integrations, easily customized
- Automated validation of alerts, detections, response actions, and security posture over time

THE BENEFITS

Discover & Prioritize Exposures

Validation coverage increases 2–3×, revealing hidden attack paths and prioritizing material risk.

Validate Detection Effectiveness

Detection success improves 25–40% while false negatives drop 30–50% through validation against real adversary behavior.

Mobilize Response & Operations

Automated validation reduces manual effort 40%+, accelerates re-testing to days, and scales without new headcount.

Measure & Improve Continuously

Repeatable AEV testing drives closed-loop team feedback and sustained improvements in MTTD/MTTR and detection quality.

AT A GLANCE

Key Capabilities

- AI-enabled Test Generation
- Adversary Emulation
- Security Control Validation
- Seamless Tool Integrations
- IT, Cloud, and OT/ICS Support

Outcomes

- Prioritized risk reduction
- Improved MTTD/MTTR
- Increased coverage without increased resourcing

INDUSTRIES

Banking

Insurance

Financial

Manufactering

Utilities

Oil & Gas

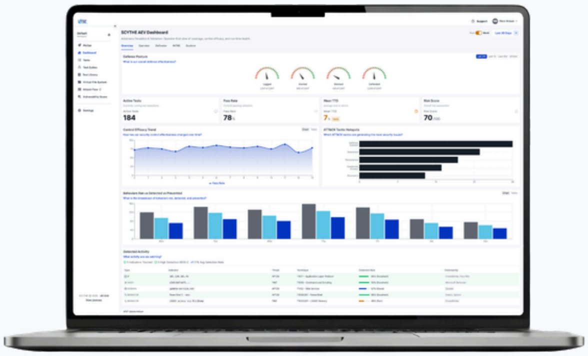
Retail

Healthcare

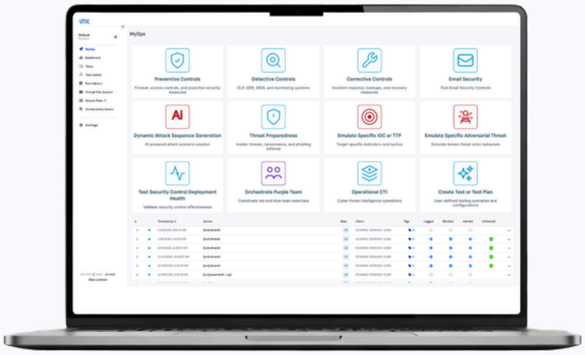
SCYTHE | PLATFORM OVERVIEW

scythe.io

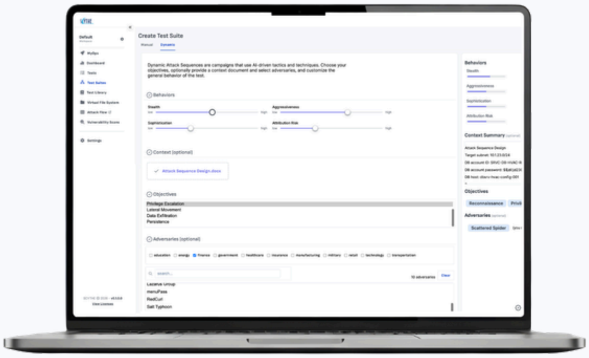
2026



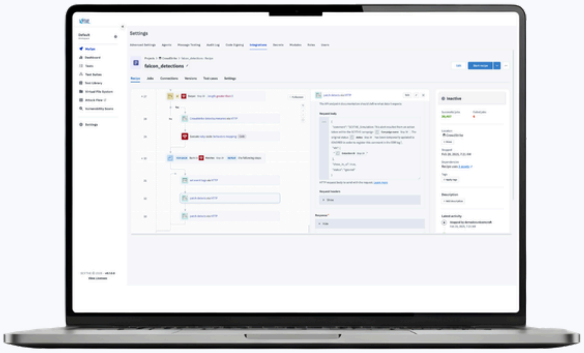
SCYTHE provides comprehensive dashboards and reporting with real-time visibility into adversarial exposure and control effectiveness. Executive metrics, Operator and Defender views, a MITRE ATT&CK coverage heat map, and custom dashboards support detection engineering, response validation, and CTEM-driven decisions.


MyOps
Preventive Controls
Firewall, access controls, and proactive security measures
Detective Controls
DLP, EDR, SIEM, and monitoring systems
Corrective Controls
Incident response, backups, and recovery measures
Email Security
Test Email Security Controls
Dynamic Attack Sequence Generation
AI-powered attack scenario creation
Threat Preparedness
Insider threats, ransomware, and phishing defense
Emulate Specific IOC or TTP
Target specific indicators and tactics
Emulate Specific Adversarial Threat
Simulate known threat actor behaviors
Test Security Control Deployment Health
Validate security control effectiveness
Orchestrate Purple Team
Coordinate red and blue team exercises
Operational CTI
Cyber threat intelligence operations
Create Test or Test Plan
User-defined testing scenarios and configurations

SCYTHE MyOps is a centralized operations panel for executing and managing adversarial testing workflows. It enables teams to launch AI-driven attack sequences, test security controls, and orchestrate purple team operations through a single, CTEM-aligned interface.



SCYTHE's AI-powered Dynamic Test Generator enables teams to quickly create realistic adversary campaigns tailored to their environment and objectives. AI-driven attack sequences, adjustable behaviors, and contextual inputs allow continuous testing of real-world attack paths without manual scripting.



SCYTHE's integration fabric enables powerful, bi-directional data correlation and workflow automation across EDR, SIEM, SOAR, and security tooling. With tailorable integrations and logic-driven workflows, teams can synchronize detections, enrich alerts, validate response actions, and adapt data flows to their operational needs, turning adversary emulation results into actionable, closed-loop security outcomes.

Learn more at scythe.io

SCYTHE Inc.

390 NE 191st St.
STE 8442
Miami, FL 33179

About SCYTHE

SCYTHE is a leading Adversarial Emulation & Validation (AEV) platform that helps organizations continuously test and strengthen security defenses against real-world threats using AI-powered adversary emulation.

For information, email sales@scythe.io.