INTRODUCING

SCYTHE 5.1

Your Team's Biggest Upgrade Yet.

SCYTHE 5.1 is a major step forward in how security teams build, run, and measure adversary emulation. From AI that designs your test campaigns to a new generation of threat preparedness scoring, this release is built to help you do in minutes what used to take days — and prove your security posture with data.

90%+
Faster Test Design
AI-powered campaign generation

5–10×
Faster Campaign Load
Bulk endpoint architecture

3
New Risk Scores
Ransomware · Phishing · Insider

> ***"SCYTHE 5.1 fundamentally changes how fast security teams can operate — from building campaigns to understanding risk, everything is faster, smarter, and more measurable."***

AI-Powered Test Generation

Stop spending days building test campaigns by hand. SCYTHE 5.1 introduces AI-driven campaign generation — just describe your threat scenario in plain language and SCYTHE builds it for you.

Natural-Language Campaign Building

Tell SCYTHE what you want to emulate — a ransomware intrusion, a phishing-led credential harvest, a lateral movement scenario — and the AI constructs a full adversary campaign aligned to relevant TTPs. No manual configuration required.

Intelligent Test Sequencing

The AI layer doesn't just generate tests — it groups and sequences them in a realistic order that mirrors how actual adversaries operate, giving you higher-fidelity results and more meaningful detection data.

The result: security teams that previously spent hours or days designing a single campaign can now go from idea to execution in minutes — a 90%+ reduction in test design time that frees your team to focus on what matters most: analyzing results and improving defenses.

> ***"90%+ reduction in test design time — from days to minutes."***

A Faster, Smarter Platform Experience

Every part of the SCYTHE interface has been refined for speed and clarity. Whether you're launching a campaign, monitoring a live test, or reviewing the dashboard, 5.1 gets you there faster.

- **Instant startup.** The platform now loads critical services first and defers the rest — you're in and working immediately.
- **5–10× faster campaign loading.** Large campaigns with 50+ devices that previously took minutes to load now open in seconds.
- **Real-time test monitoring.** Device check-ins appear live as tests run — no more refreshing to see what's happening.
- **Remote shell access.** Launch a live shell directly from test execution for immediate, hands-on investigation.
- **Customizable views.** Show or hide event columns in the tests table to focus your view on what matters to your workflow.

- **SIEM correlation built in.** A new SIEM view in the test execution dashboard connects SCYTHE events to your external security data in real time.

Email Security & Phishing Simulation

Email remains the #1 initial access vector for adversaries. SCYTHE 5.1 introduces a complete phishing simulation platform so you can test your organization's defenses against the threats that matter most.

End-to-End Phishing Campaigns

Build realistic phishing lures with a full email template builder — configure sender identity, links, and attachments. Deliver simulated payloads through integrated SMTP to test detection and response from inbox to endpoint.

Reusable Scenario Library

Create and save phishing templates for recurring use across campaigns. Run the same scenario against different teams, environments, or timeframes to track improvement over time.

Realistic Delivery Simulation

Simulated payloads are delivered in OS-aware encrypted packaging designed to test your email security gateway's detection capabilities — not bypass them. Know whether your controls are actually working.

Threat Preparedness Scores

For the first time, SCYTHE gives your team quantified, at-a-glance scores across the three threat categories that boards and CISOs ask about most.

- **Ransomware Readiness.** How well do your controls hold up against ransomware-aligned attack patterns? SCYTHE now scores it continuously.
- **Phishing Resilience.** Beyond awareness training — a measurable score that reflects how effectively your organization detects and stops email-based attacks.
- **Insider Threat Posture.** A visibility score that tracks whether your detection capabilities cover behaviors associated with malicious or negligent insiders.

These scores update continuously as you run emulations — giving your team a living view of preparedness, not a point-in-time snapshot. Every test you run feeds the score, and every score improvement is evidence of progress you can report upward.

Rebuilt Reporting & Dashboards

Reporting in SCYTHE 5.1 has been rebuilt from the ground up — faster, richer, and designed to connect your emulation results to the metrics that matter for both your security team and your leadership.

- **MITRE ATT&CK report, exportable as PDF.** Generate a board-ready MITRE ATT&CK coverage report directly from the platform with a single click.
- **Live data, no stale caches.** Every reportlet reflects real-time database state — what you see is what's actually happening.
- **Priority-first dashboard loading.** The most important information loads first. Your dashboard is ready to use in seconds, not after a full page load.
- **Assessment-driven scoring.** Test event assessments feed directly into scoring and compliance tracking for a continuous, evidence-based picture of your defenses.

Stronger Security & Simpler Administration

SCYTHE 5.1 sets a new baseline for platform security and compliance — so the tool you use to test others' defenses is itself hardened to enterprise standards.

SSO Made Easy

- A new guided SSO setup wizard walks administrators through configuration step by step — no more manual SAML editing.

- Import and export SAML configurations as XML for easy migration between environments.
- Full support for SAML and OIDC providers.

Authentication Everywhere

- Every route in the SCYTHE platform now requires a valid authenticated session — eliminating an entire class of potential unauthorized access.
- Workspace-level access controls enforced at login: users without an assigned role are denied, not defaulted in.
- Session integrity enforced after EULA acceptance, including re-authentication after device sleep.

Compliance-Ready by Default

- Third-party analytics and feature flag services (Pendo, Split.io) have been fully removed — reducing your data exposure surface for compliance-sensitive deployments.
- A critical server-side vulnerability has been patched and security dependencies updated across the platform.
- AI credentials and email server passwords are no longer exposed in logs or plain storage.

Help When You Need It — Right Inside the Platform

SCYTHE 5.1 embeds our knowledge base directly in the platform. Get answers to your questions without switching context — support articles surface exactly where and when you need them.

Ready to experience SCYTHE 5.1?

Contact your customer success manager or reach us at **info@scythe.io** to schedule your upgrade.

scythe.io