CUSTOMER TESTIMONIAL

Advancing Red Team–Driven Cyber Resilience for a Global Insurance Company

OBJECTIVES

A large U.S.-based insurance company with a mature cybersecurity program sought to better operationalize its advanced red team by turning episodic campaigns into reusable, enterprise-wide validation tightly linked to security operations.

SOLUTION

The organization deployed SCYTHE as the foundation of its red team and purple team program, with detection engineering embedded as a downstream operational capability.

Key components included:

- Continuous emulation of red team tradecraft to measure control effectiveness and exposure
- Automated regression testing of red team–derived detections with engineering feedback loops
- Flexible agentless deployment supporting EXE, DLL, and shellcode payloads with built-in evasion techniques

THE RESULTS

Red Team & Adversary Coverage
25+ adversary scenarios were continuously replayed across critical systems, uncovering high-risk attack paths impacting regulated data.

Detection & Control Improvement
Prioritized detection coverage improved by 25–40%, false negatives fell by 30–50%, and repeatable regression testing was established for red team–derived detections.

Regulatory & Leadership Impact
Defensible regulatory evidence improved executive reporting and increased confidence in controls protecting sensitive customer data.

AT A GLANCE

Challenges

- Limited programmatic Scale
- Complex, Regulated Attack Surface
- Bridging operations

Benefits

- 31% increase in coverage
- 25% increase in reusable test (red to blue)
- 50% reduction in false negatives

"We already had a strong red team, but their impact was episodic.

SCYTHE allowed us to scale red team tradecraft across the enterprise, align our blue teams around measurable outcomes, and turn adversary emulation into a continuous driver of cyber resilience and regulatory confidence."

Head of Red Team, Global Insurance Enterprise