Solution Overview

ATLAS

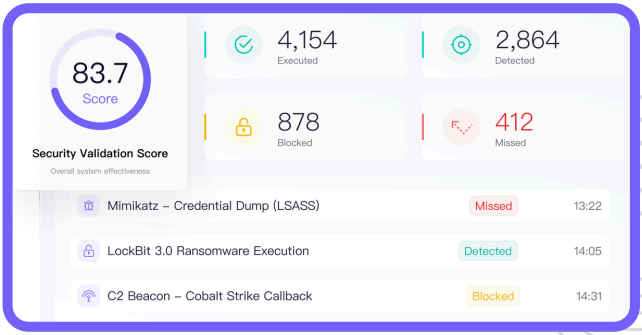
AI-Powered Security Validation Platform

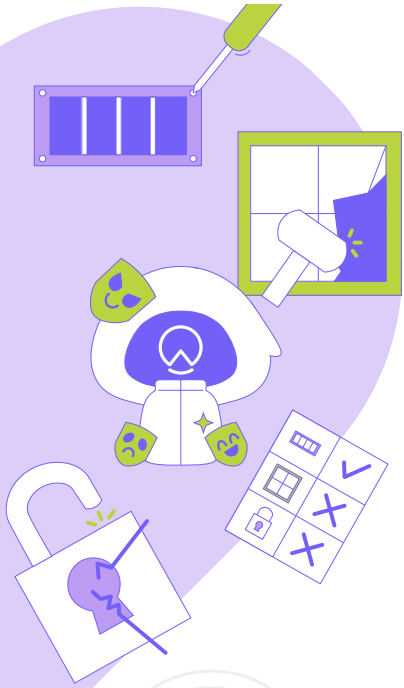
Continuously Validate, Continuously Secure.

Security controls are only as good as their last validation. Turn security assumptions into measurable proof of what works, what does not, and where to act.

Most security programs are built on assumptions. Traditional assessments produce point-in-time snapshots that go stale within days or weeks, leaving gaps invisible until a breach makes them undeniable. The threat landscape does not pause between assessments, and neither do the adversaries exploiting it.

Security teams are increasingly structuring their programs around Continuous Threat Exposure Management (CTEM), a framework designed to continuously identify, validate, and remediate cyber risk. The Validation phase is where that strategy succeeds or fails: it confirms which exposures are exploitable, whether security controls work, and where remediation efforts should be prioritized.





ATLAS operationalize the CTEM Validation phase. Powered by Digital Mind's adversarial intelligence and mapped to the MITRE ATT&CK framework, it continuously validates security controls and response processes against real-world adversary techniques, safely executing even destructive payloads in isolated environments with full rollback to produce measurable evidence of defensive effectiveness rather than assumptions. With TARA AI, ATLAS continuously selects validation scenarios, converts the latest threat intelligence into executable validation rules, and orchestrates validation activities autonomously.

AI CAPABILITIES IN ATLAS

- **TARA AI:** The Autonomous CTEM Agent behind ATLAS. Security teams interact through natural language to define validation objectives and review results, while TARA AI continuously selects validation scenarios, converts threat intelligence into executable rules, and orchestrates validation activities autonomously.
- **Detection Evasion:** Uses AI to continuously generate adversary variants that mirror real-world attacker behavior, adapting techniques to bypass security controls so defenses are validated against evolving threats rather than static signatures.
- **Digital Mind:** The proprietary AI foundation powering ATLAS. Continuously collects, correlates, and operationalizes real-world adversary intelligence, ensuring every validation scenario reflects the latest threat landscape.

Product Highlights

Real-World Threat Simulation
Continuously updated validation scenarios drawn from real-world adversary techniques ensure every validation reflects the threat landscape.

Intelligent Playbook
Simulate multi-stage attack campaigns across production environments. When a technique is blocked, ATLAS automatically selects alternative attack variants to continue validation.

Production-Safe Simulation
Validation agents deploy on dedicated virtual machines with no installation on production systems or privileged credentials, allowing validation without disrupting business operations.

Actionable Remediation Output
Every validation generates Sigma and Suricata rules that accelerate detection engineering and help security teams remediate findings faster.

Autonomous Validation
TARA AI selects validation scenarios, converts threat intelligence into executable rules, and orchestrates validation autonomously while teams approve key decisions.

Destructive Testing
Safely execute destructive payloads, including ransomware, in isolated environments with full rollback to validate whether security controls stop real attacks.

Continuous Validation Workflow

1

SIMULATE

Safely simulate real-world adversary techniques across production environments using continuously updated threat intelligence.

2

VALIDATE

Measure how security controls, detections, and response processes perform against every stage of the simulated attack.

3

IDENTIFY

Identify exploitable security gaps, control failures, and detection blind spots with measurable evidence to prioritize remediation.

4

IMPROVE

Generate actionable remediation guidance to strengthen defensive effectiveness and improve future validation outcomes.

> **ATLAS** *transformed our security validation from reactive to proactive. We now have continuous visibility into our security posture and can address vulnerabilities before they become breaches.*
>
> —— **Chief Information Security Officer, Leading Asian Bank**

www.digidations.com
info@digidations.com

digiDations is an AI Native cybersecurity company helping organizations move from hoping their defenses will hold to knowing they will through Autonomous Cyber Defense.