

Securing the Credit Union System: Continuous Validation for Member-Owned Institutions with the Picus Platform

Your members trust you to keep their money safe and their services running. The Picus Platform proves which attacks would actually succeed and which your defenses stop, then helps you fix the gaps, so your lean team strengthens your security posture and answers every examiner question with evidence.

Problem:

Lean Team. Hundreds of Findings. Attacks at AI Speed.

Credit union security teams are lean by design, yet they face the same threats as the largest banks.

- Scanners generate hundreds of findings, but they cannot say which ones an attacker could actually exploit in your environment.
- Core processors and CUSOs are vetted through questionnaires and SOC reports, never against a real attack.
- Core banking systems and member data platforms are too critical to test live, so their real risk stays unknown.

Solution:

Picus Autonomous Exposure Validation Platform

Know which attacks would succeed against your credit union, and prove which ones your defenses stop.

- Continuously simulate ransomware, credential theft, and the latest CISA-flagged techniques, safely in production.
- Prove exploitability for every exposure and asset, including restricted systems like core banking systems.
- Cut the backlog to what is truly exploitable, and resolve each finding as patch, mitigate, monitor, or accept, with evidence attached for boards and examiners.

Validate Security Controls

Continuously test the prevention and detection stack you already own, across endpoint, email, network, cloud, and identity, and close every gap with ready-to-deploy rules.

Be Prepared Against Threats

Simulate the ransomware and malware campaigns targeting credit unions, and validate whether the techniques behind real sector incidents are blocked and detected.

Compliance and Resilience with Proof

Generate audit-ready, evidence-based reports aligned with NCUA Part 748 and ISE, GLBA Safeguards, NIST CSF 2.0, and the CRI Profile effortlessly.

 **2x Security Control Effectiveness in 90 Days³**

 **Up to 86% Smaller Vulnerability Backlog⁴**

 **Prove Examination Readiness with Evidence**

¹ Verizon 2026 DBIR, ² CrowdStrike 2026 GTR, ^{3 & 4} Picus customer data, aggregated across production deployments

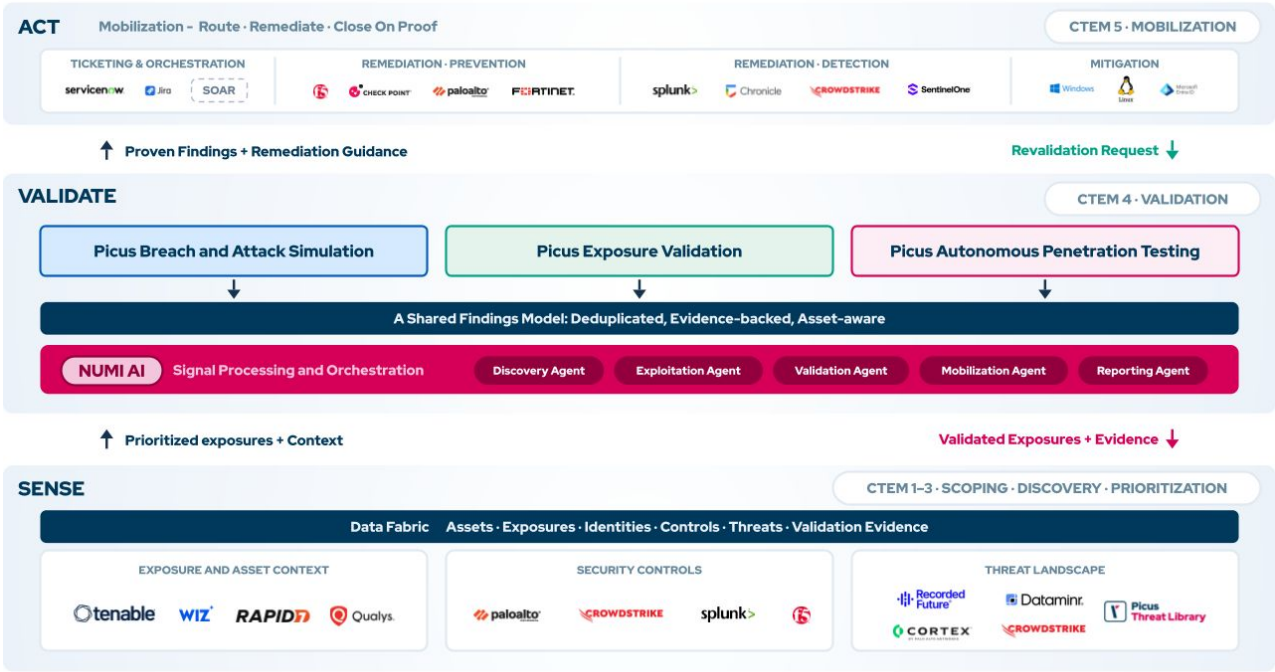
Core Capabilities

- ✓ **Integrated BAS and Autonomous Pentesting**
Combine Breach and Attack Simulation with Autonomous Penetration Testing to continuously assess both control effectiveness and exploitability.
- ✓ **Proof Where Live Testing Cannot Reach**
Get a per-asset exploitability verdict for every exposure and asset, including restricted ones and CVEs with no working exploit, on the day of disclosure.
- ✓ **Risk Free & Flexible Deployment**
Non-destructive, production-safe simulations run across on-prem, cloud, and hybrid estates, agentless where needed, with no maintenance windows.

- ✓ **Industry-Specific Threat Coverage**
Run a continuously updated financial services threat template from Picus Labs, ready to test the campaigns targeting credit unions and their providers as they emerge.
- ✓ **Actionable Mitigation Guidance**
Receive 80,000+ vendor-specific prevention signatures and detection rules to close gaps quickly.
- ✓ **Rapid Emerging Threat Coverage**
Picus adds simulations for the latest CISA alerts and emerging threats within a 24-hour SLA, so evidence is machine produced rather than person dependent.

Picus Platform - AI-powered Autonomous Validation

The **Picus Platform** continuously validates exposure across all layers, including network, endpoint, email, cloud, and identity. Powered by **Numi AI**, the platform delivers continuous security testing, automated penetration testing, attack-path validation, intelligent risk prioritization, and automated remediation guidance against real-world threats targeting member-owned financial institutions. Attack Surfaces. Exposures. Security Controls. All Validated.



picussecurity.com

Experience Picus *in Action*

GET A DEMO

