Securing the Oil and Gas Infrastructure: Continuous Validation for Critical Operations with Picus Platform

Picus Platform validates security posture across oil and gas infrastructure by safely simulating real world attack scenarios and providing actionable remediation aligned with industrial cybersecurity standards and regulatory requirements.

Problem:

Unvalidated Exposures and Cyber Risks

Oil and gas organizations face growing cyber risk across interconnected IT/OT environments.

- **IT and OT boundaries** across networks are often assumed secure but rarely validated under real world conditions.
- **Security controls protecting industrial systems** are difficult to test safely, leaving security gaps undiscovered.
- Operators face increasing pressure to demonstrate **cyber resilience and compliance** with industry standards.

Solution:

Picus Security Validation Platform

Picus enables teams to validate defenses across networks without disrupting operations.

- Simulate **ransomware, ICS malware, and adversary techniques** to test real world security effectiveness.
- Identify and mitigate **attack paths between corporate IT and critical OT networks**.
- Demonstrate **cyber resilience and compliance readiness** through safe, automated security validation.

Validate Security Controls

Continuously assess security effectiveness across IT and OT layers, and fine-tune controls such as firewalls, IPS/IDS, and network segmentation.

Be Prepared Against Threats

Simulate APTs, ransomware, and malware campaigns that target oil and gas companies to ensure readiness against attacks that pivot from IT to OT.

Compliance and Resilience with Proof

Generate audit-ready, evidence-based reports aligned with IEC 62443, API 1164, NIST CSF, and TSA pipeline directives effortlessly.

Mitigate Security Gaps 81% Faster[1]

Prevent %200 more threats in 3 months[2]

Prove Compliance with Confidence & Evidence

[1] *Based on analysis of 10M exposures from Early Availability Program participants,* [2] *The Blue Report 2025, Picus Security*

Core Capabilities

✔ **Integrated BAS and Automated Pentesting**
Combine Breach and Attack Simulation with Automated Pentesting to continuously assess both control effectiveness and exploitability.

✔ **Risk Free**
Picus runs non-destructive and production-safe attack simulations to ensure operational stability and business continuity, eliminating the risk of unintended disruptions.

✔ **Flexible Deployment**
Safely simulate real-world attacks to measure the effectiveness of controls across on-prem, cloud, and hybrid environments.

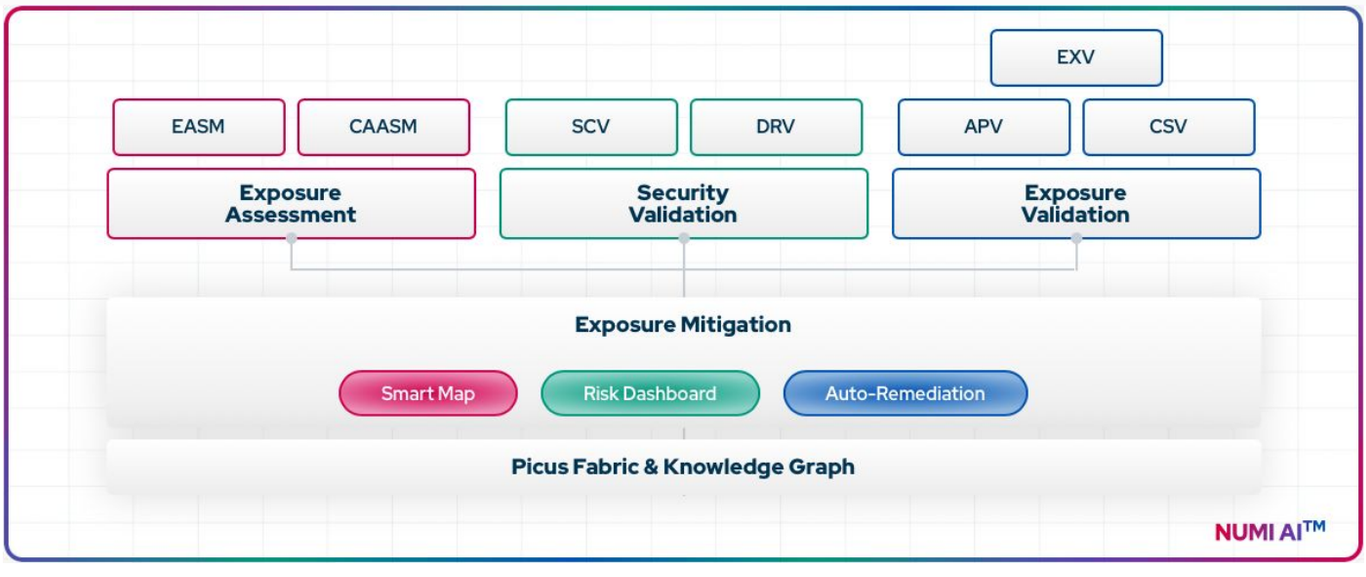
✔ **Industry-Specific Threat Coverage**
Leverage the Picus Threat Library featuring over 30,000 unique adversary actions to validate defenses against the threats commonly targeting oil and gas companies.

✔ **Actionable Mitigation Guidance**
Receive 80,000+ vendor-specific prevention signatures and detection rules to close gaps quickly.

✔ **Rapid Emerging Threat Coverage**
Picus adds attack simulations for the latest CISA alerts and emerging threats within a 24-hour SLA, ensuring your defenses are continuously validated against the most current adversary tactics.

Picus Platform - AI-powered Autonomous Validation

The **Picus Platform** continuously validates exposure across IT, OT, cloud, and hybrid environments. Powered by **NUMI AI**, the platform delivers continuous security testing, attack-path validation, intelligent risk prioritization, and automated remediation guidance against real-world threats targeting critical operations.



picussecurity.com

Experience Picus *in Action*

GET A DEMO

SPRING 2026 Leader

4.9/5.0

#1 Solution Provider*
Breach and Attack Simulation

*G2, Breach and Attack Simulation (BAS) Solutions, April Grid Report, 1 April 2026

Gartner Peer Insights Customers' Choice 2025

4.8/5.0

Highest-rated vendor*
Adversarial Exposure Validation

*Gartner, Voice of the Customer for Adversarial Exposure Validation, Peer Contributors, 30 October 2025

© Picus Security. All Rights Reserved.
All other product names, logos, and brands are property of their respective owners in the United States and/or other countries.