



Crossing the IT/OT Divide:

Continuous Validation for IT and OT Systems with Picus Platform

Picus Security Validation Platform validates security control effectiveness across IT and OT layers by safely simulating real-world attack scenarios and providing actionable remediation aligned with industrial cybersecurity standards.

Problem:

Assumed Security, Unvalidated Risk

- **IT/OT segmentation** is often assumed secure but rarely validated under real-world conditions.
- Security tools in **industrial environments** lack regular testing, leaving gaps undetected.
- **Critical infrastructure** teams lack safe, scalable methods to assess their true exposure.

Solution:

Picus Security Validation Platform

- **Simulate APT-style attacks** across Purdue levels to test control effectiveness in hybrid networks
- **Identify and mitigate attack paths** bridging IT and OT systems.
- **Demonstrate cyber resilience** through safe, automated testing aligned with industry standards

Validate Security Controls

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

> **Mitigate Security Gaps 81% Faster** ¹

Be Prepared Against Threats

Simulate APTs, ransomware, and malware campaigns that target industrial systems to ensure readiness against attacks that pivot from IT to OT.

> **Prevent %200 more threats in 3 months** ²

Compliance with Proof

Generate audit-ready and evidence-backed reports aligned with industrial cybersecurity standards without manual validation.

> **Prove Compliance with Confidence & Evidence**

Core Capabilities

✓ Integrated BAS and Automated Pentesting

Combine Breach and Attack Simulation (BAS) with Automated Pentesting to assess both control effectiveness and exploitability.

✓ Risk Free

Picus runs non-destructive and production-safe attack simulations to ensure business continuity.

✓ Flexible Deployment

Simulate attacks to measure control effectiveness across on-prem, cloud, and hybrid environments.

✓ OT-Specific Threat Coverage

Leverage the Picus Threat Library with over 26,000 unique attack actions to validate defenses against threats targeting ICS and IT/OT environments.

✓ 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.


¹ Based on analysis of 10M exposures from Early Availability Program participants, ² The Blue Report 2024, Picus Security

Picus Security Validation Platform


Integrated approach to continuous validation




Security Control Validation (SCV):
Measure and optimize the effectiveness of security controls with Breach and Attack Simulation (BAS).




Attack Path Validation (APV):
Run automated penetration testing to eliminate high-risk attack paths.




Exposure Validation (EXV):
Distinguish between theoretical and truly exploitable exposures to prioritize remediation efforts based on real-world risk.



Detection Rule Validation (DRV):
Continuously assess SIEM rules to ensure high-fidelity alerts.



Cloud Security Validation (CSV):
Validate cloud configurations to identify exploitable misconfigurations, privilege risks, and cloud-native attack paths.



Attack Surface Validation (ASV):
Discover exposed assets across environments and gain context-aware visibility into the attack surface.

Validate Across IT/OT Layers

Picus Platform simulates real-world attacks across IT and OT layers without disrupting operations to validate control effectiveness from enterprise systems to industrial endpoints and ensure full-stack security coverage.

Attack Simulations in Levels 4 and 5:

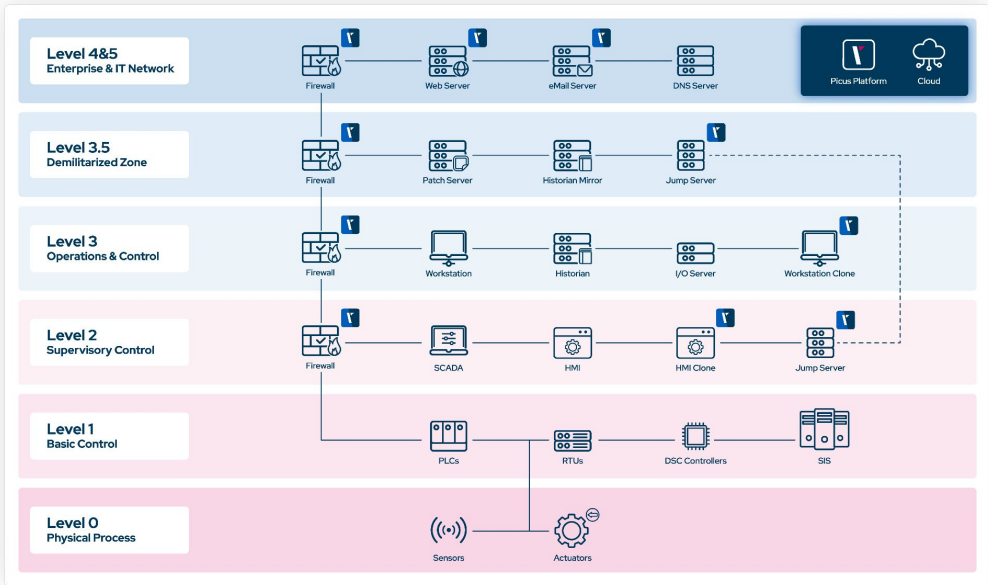
Picus performs network and host-level simulations to validate security controls at the IT/OT boundary:

- Validate host-level security controls
- Validate network and web application attacks
- Validate network-wide detection and logging across SIEM, EDR, and other security controls
- Simulate IT to OT attack campaigns

Attack Simulations Across Levels 3.5 to 2:

Picus performs network-level simulations to validate network segmentation and detection capabilities:

- Validate network and web application attacks
- Validate network-wide detection and logging across SIEM, EDR, and other security controls
- Simulate OT targeted attack campaigns
- Design and simulate custom attacks across layers



“

In the energy sector, downtime isn't an option. Picus enables us to safely test defenses from the office network to the control room, shows the gaps, and lets us patch them before they hit operations.

CISO, Top 100 Energy Company