

SOLUTION BRIEF

# PICUS PLATFORM AND DEVO SIEM INTEGRATION

## Integration Benefits

### ✓ Enhanced Threat Detection

Validate Devo SIEM detections against MITRE ATT&CK tactics and adversary kill chains, ensuring accurate and consistent detection of real threats.

### ✓ Proven CTEM Alignment

Transform Devo SIEM telemetry into validated evidence of exploitable risks, enabling clearer prioritization within the CTEM cycle.

### ✓ Streamlined Incident Response

Validated alerts reduce false positives, empowering SOC teams to respond swiftly and minimize attacker dwell time.

### ✓ Improved Cyber Resilience

Continuous assessments and real-time recommendations help defenses stay robust and adaptive to new threats.

### ✓ Holistic Security Posture

Gain a comprehensive view of your defenses by validating logs and alerts across Devo, enabling informed, data-driven decisions.

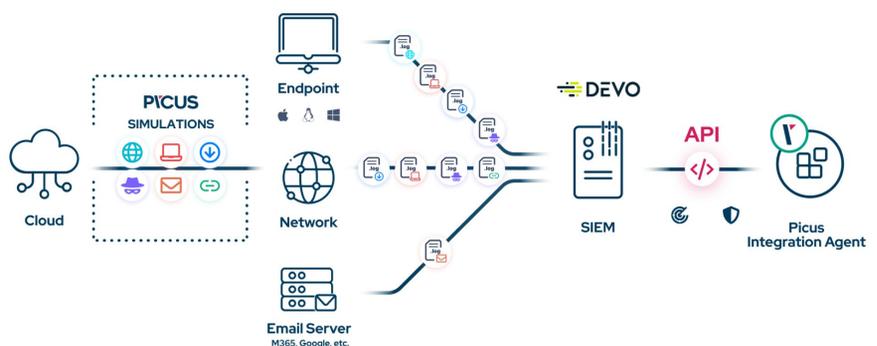
### ✓ Efficient Resource Allocation

Filter out unnecessary alerts, focus on genuine risks, and enable SOC teams to address what truly matters by reducing workload and building confidence.

## Enhancing Threat Detection with Attack Simulations: The Picus x Devo SIEM Integration

Security Information and Event Management (SIEM) platforms are central to modern Security Operations Centers (SOCs). Devo SIEM provides security teams with high-performance, real-time log management, advanced analytics, and scalable detection capabilities across complex environments. Picus integrates with Devo SIEM to provide SOC teams with a unified approach to cybersecurity, enabling them to proactively identify and close security gaps while optimizing detection and response.

By simulating real-world adversarial techniques, the Picus Platform validates log delivery and detection accuracy within Devo SIEM. With its comprehensive Threat Library, covering MITRE ATT&CK techniques and thousands of attack scenarios, Picus assesses and enhances Devo's detection and response capabilities by validating telemetry from diverse sources and enabling teams to act faster with Picus-provided, ready-to-use SIGMA rules.



## How Picus x Devo SIEM Integration Works

1. Picus safely simulates real-world attack techniques across the environment to test security controls.
2. Security logs generated by endpoints, network, and cloud sources are ingested into Devo SIEM.
3. Picus queries Devo via APIs, validates logs and alerts, and correlates them with simulated attack activity.
4. The validated results are displayed on the Picus dashboard, enabling SOC teams to close detection gaps and enhance security posture.

## ABOUT PICUS

At Picus Security, our priority is making it easy for security teams to continuously validate and enhance organizations' cyber resilience.

Our Security Validation Platform simulates real-world threats to measure control effectiveness, confirm exploitable exposures, and identify high-risk attack paths to critical assets.

As the pioneer of Breach and Attack Simulation, we help organizations operationalize Continuous Threat Exposure Management (CTEM) with validated evidence, clear prioritization, and faster remediation.

Experience Picus  
*in Action*

GET A DEMO



4.9/5.0  
#1  
Solution Provider

4.8/5.0  
Highest-rated  
Vendor



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

GARTNER is a registered trademark and service mark, and the GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge and PEER INSIGHTS are trademarks and service marks, of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

© Picus Security. All Rights Reserved.

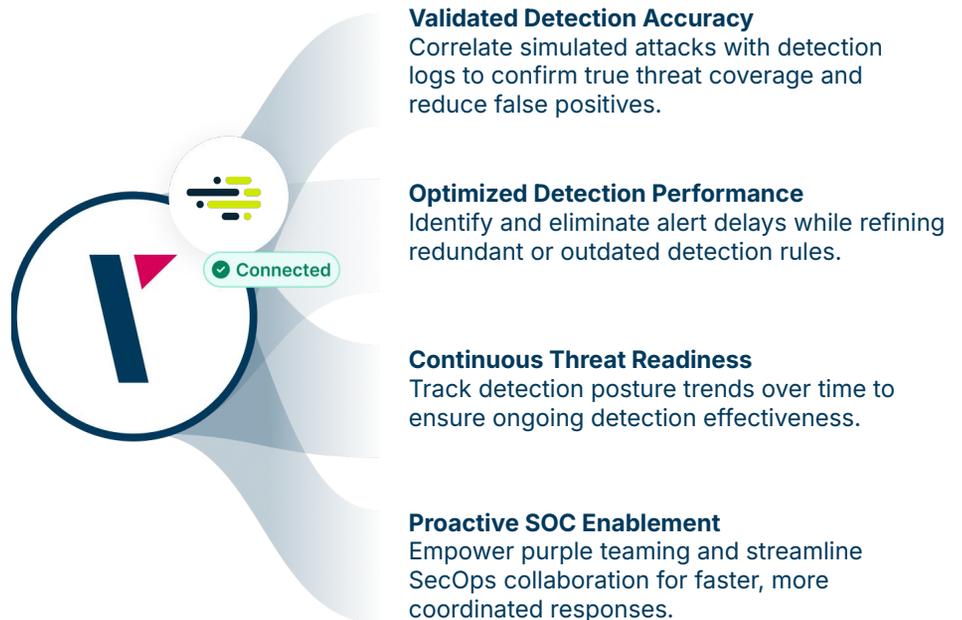
All other product names, logos, and brands are property of their respective owners in the United States and/or other countries.

## Strengthening Cybersecurity Defenses With Picus x Devo SIEM Integration

Together, Picus and Devo empower organizations to strengthen defenses and improve SOC efficiency. Seamless integration ensures validated log delivery, accurate alerts, and reduced false positives, helping teams accelerate detection and response.

This integration removes the uncertainty often associated with high-volume, real-time data environments by addressing challenges such as inconsistent log ingestion, untested detection logic, and alert fatigue. With validated alerts and clear visibility into detection gaps, security teams gain confidence that they can detect and respond to real threats before attackers can progress across their environment.

By combining Picus Breach and Attack Simulation with Devo's real-time analytics and high-performance querying capabilities, organizations gain an adaptable and resilient security ecosystem with the clarity needed to strengthen detection strategies and improve overall security posture.



## Picus Security Validation Platform

Picus Security Validation Platform simulates cyber threats to consistently validate, measure and enhance organizations' cyber resilience. It facilitates a more proactive and threat-centric approach to security by automatically evaluating the effectiveness of security controls, identifying high-risk attack paths, and helping to optimize threat prevention and detection capabilities.

### Why is security validation important?

- Controls don't perform out-of-the-box and must be customized.
- New threats mean that security tools can lose their effectiveness.
- Infrastructure drift creates weaknesses that can go unaddressed.
- Pentesting is vulnerability-focused and quickly out of date.
- Boards, auditors & insurers want evidence of security effectiveness.