PICUS | Cribl

SIEM

SOLUTION BRIEF

PICUS PLATFORM AND CRIBL LAKE SIEM INTEGRATION

Integration Benefits

✔ Enhanced Threat Detection
Validate Cribl Lake SIEM detections against MITRE ATT&CK tactics and adversary kill chains, ensuring accurate and consistent detection of real threats.

✔ Proven CTEM Alignment
Transform Cribl Lake 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.

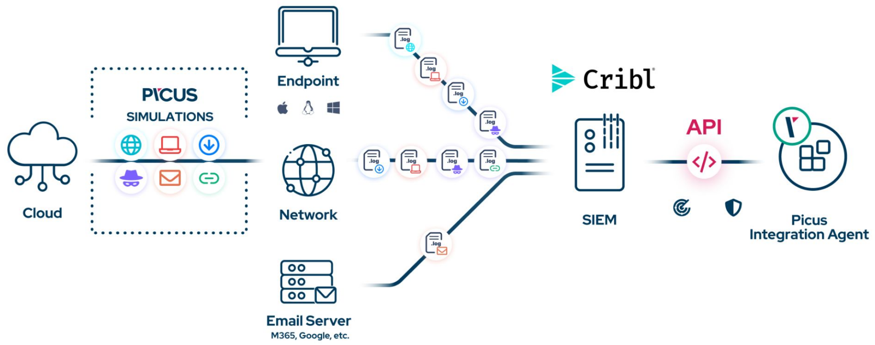
✔ Holistic Security Posture
Gain a comprehensive view of your defenses by validating logs and alerts across Cribl Lake, enabling informed, data-driven decisions.

✔ 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 Cribl Lake SIEM Integration

Security Information and Event Management (SIEM) and data lake platforms are central to modern Security Operations Centers (SOCs). Cribl Lake provides security teams with flexible, scalable log collection, processing, and storage capabilities, enabling efficient telemetry management across complex environments. Picus integrates with Cribl Lake 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, data integrity, and detection readiness within Cribl Lake. With its comprehensive Threat Library, covering MITRE ATT&CK techniques and thousands of attack scenarios, Picus assesses and enhances Cribl Lake'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 Cribl Lake 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, processed, and stored in Cribl Lake.
3. Picus queries Cribl Lake 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

WINTER 2026 Leader

4.9/5.0

#1 Solution Provider

4.8/5.0

Highest-rated Vendor

Gartner Peer Insights Customers' Choice 2025

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.

Strengthening Cybersecurity Defenses With Picus x Cribl Lake SIEM Integration

Together, Picus and Cribl Lake empower organizations to strengthen defenses and improve SOC efficiency. Seamless integration ensures validated log delivery, complete telemetry, and reduced data gaps, helping teams accelerate detection and response.

This integration removes the uncertainty often associated with distributed data pipelines by addressing challenges such as incomplete log ingestion, inconsistent data normalization, and gaps in telemetry visibility. With validated data and clear visibility into coverage gaps, security teams gain confidence that their detection stack operates on reliable, high-quality inputs and can identify real threats before attackers can progress across their environment.

By combining Picus Breach and Attack Simulation with Cribl Lake's flexible data routing, processing, and storage capabilities, organizations gain an adaptable and resilient security ecosystem with the clarity needed to strengthen detection strategies and improve overall security posture.

Validated Detection Accuracy
Correlate simulated attacks with detection logs to confirm true threat coverage and reduce false positives.

Optimized Detection Performance
Identify and eliminate alert delays while refining redundant or outdated detection rules.

Continuous Threat Readiness
Track detection posture trends over time to ensure ongoing detection effectiveness.

Proactive SOC Enablement
Empower purple teaming and streamline SecOps collaboration for faster, more coordinated responses.

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.