PICUS | Gurucul

SIEM

SOLUTION BRIEF

PICUS PLATFORM AND GURUCUL SIEM INTEGRATION

Integration Benefits

✔ Enhanced Threat Detection

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

✔ Proven CTEM Alignment

Transform Gurucul 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 Gurucul, enabling informed, data-driven decisions.

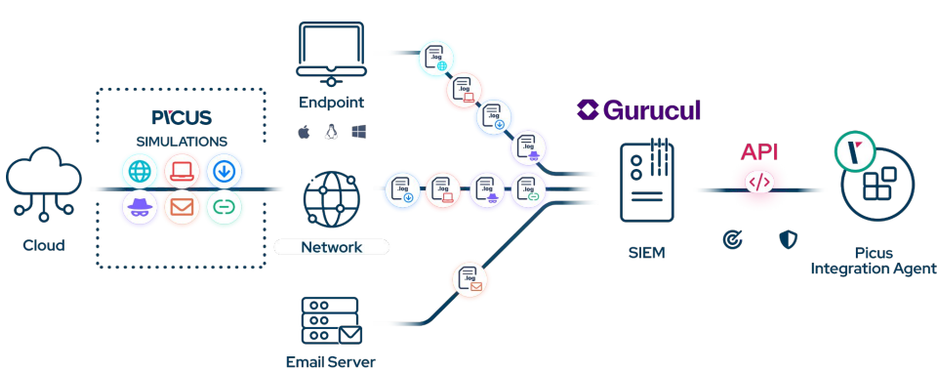
✔ Efficient Resource Allocation

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 Gurucul SIEM Integration

Security Information and Event Management (SIEM) and risk analytics platforms are central to modern Security Operations Centers (SOCs). Gurucul provides security teams with unified log ingestion, behavioral analytics, identity analytics, and risk-based threat detection, enabling efficient threat detection, investigation, and response across complex environments. Picus integrates with the Gurucul 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 ingestion, data integrity, and detection readiness within Gurucul. With its comprehensive Threat Library, covering MITRE ATT&CK techniques and thousands of attack scenarios, Picus assesses and enhances Gurucul'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 Gurucul 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 Gurucul.
3. Picus queries Gurucul 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 prove what attackers can exploit and what their defenses actually stop.

The Picus Platform brings Breach and Attack Simulation, Autonomous Pentesting, and Exposure Validation together to deliver that proof, then close real gaps with ready-to-deploy fixes and re-validate to confirm.

We help organizations operationalize Continuous Threat Exposure Management (CTEM) with validated evidence and faster remediation.

Experience Picus *in Action*

GET A DEMO

FALL 2026 Leader

4.8/5.0
#1
Solution Provider

4.8/5.0
Highest-rated Vendor

Gartner Peer Insights Customers' Choice 2026

Gartner, Voice of the Customer for Adversarial Exposure Validation, Peer Contributors, 27 August 2026

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 Gurucul SIEM Integration

Together, Picus and the Gurucul empower organizations to strengthen defenses and improve SOC efficiency. Seamless integration ensures validated log ingestion, complete telemetry, and reduced detection gaps, helping teams accelerate detection and response.

This integration removes the uncertainty often associated with security analytics platforms by addressing challenges such as incomplete log ingestion, inconsistent data normalization, and gaps in detection coverage. 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 Gurucul's behavioral analytics, identity analytics, and risk-based threat detection 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 Autonomous Exposure Validation Platform

The **Picus Platform** validates security controls, proves exploitability, and prioritizes the fixes that matter. **Breach and Attack Simulation** proves what your controls block and detect, **Autonomous Pentesting** executes real exploit chains to show what an attacker can reach, and **Exposure Validation** confirms whether an exposure is truly exploitable in your environment, even when no working exploit exists or the asset is too critical to execute one against.

Why is exposure validation important?

- CVSS scores show how bad a flaw could be, not whether it is exploitable in your environment.
- Most vulnerabilities are never exploitable once your controls are in place, so validation surfaces the few that carry real risk.
- Patch backlogs grow faster than teams can remediate, and validation shows what to fix first.
- Decisions to patch, mitigate, or accept a risk need evidence, not assumptions.