SIEM

SOLUTION BRIEF

THE PICUS COMPLETE SECURITY VALIDATION PLATFORM AND CROWDSTRIKE FALCON® LOGSCALE™ SIEM INTEGRATION

INTEGRATION BENEFITS

✔ **Enhanced Threat Detection**
The integration amplifies SIEM capabilities by validating security logs against MITRE ATT&CK tactics and adversary kill chains, enabling immediate and accurate threat detection.

✔ **Streamlined Incident Response**
Validated alerts help security teams respond swiftly to threats, reducing false positives and minimizing attacker dwell time.

✔ **Improved Cyber Resilience**
Continuous threat assessments and real-time mitigation recommendations ensure your defenses remain adaptive and robust against evolving threats.

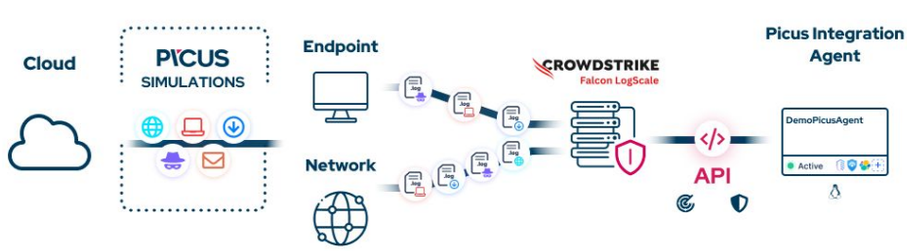
✔ **Comprehensive Security Posture**
Gain holistic visibility into your security posture by validating logs and alerts, enabling informed, data-driven decisions.

✔ **Efficient Resource Allocation**
By reducing noise and identifying genuine risks, teams can focus on impactful security operations, optimizing resource allocation.

Empowering Cyber Resilience: The Picus x CrowdStrike Falcon® LogScale™ Integration

As the threat landscape evolves rapidly, organizations must ensure that their cybersecurity defenses are not only efficient but resilient to emerging threats. Picus Security has partnered with CrowdStrike Falcon® LogScale™ to provide organizations with an integrated approach to cybersecurity, enabling them to identify and mitigate security gaps proactively while optimizing their security operations for superior resilience.

By simulating real-world cyber threats, the Picus Platform validates log delivery and alert accuracy of the CrowdStrike Falcon® LogScale™ SIEM. Picus' Threat Library, featuring a comprehensive range of MITRE ATT&CK techniques and thousands of attack scenarios, complements CrowdStrike Falcon® LogScale™ by enhancing threat detection and response capabilities. This integration ensures consistent data flow and enables teams to act swiftly by leveraging both SIGMA detection rules and direct LogScale queries provided by Picus.



HOW IT WORKS

1. Picus simulates attacks in a safe environment to test security controls.
2. The logs generated by security solutions are forwarded to CrowdStrike Falcon® LogScale™ SIEM.
3. Picus pulls the logs and alerts from CrowdStrike Falcon® LogScale™ SIEM by using API queries and then validates the logs.
4. The results are displayed on the dashboard, allowing security teams to take action and improve their 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 Complete Security Validation Platform simulates real-world threats to automatically measure the effectiveness of security controls, identify high-risk attack paths to critical assets, and optimize threat prevention and detection capabilities.

As the pioneer of Breach and Attack Simulation, our people and technology empower customers worldwide to be threat-centric and proactive.

Experience Picus *in Action*

GET A DEMO

Gartner Peer Insights Customers' Choice 2024

Highest Rated Vendor

4.8/5

Gartner, Voice of the Customer for Breach and Attack Simulation Tools, Peer Contributors, 30 January 2024

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.

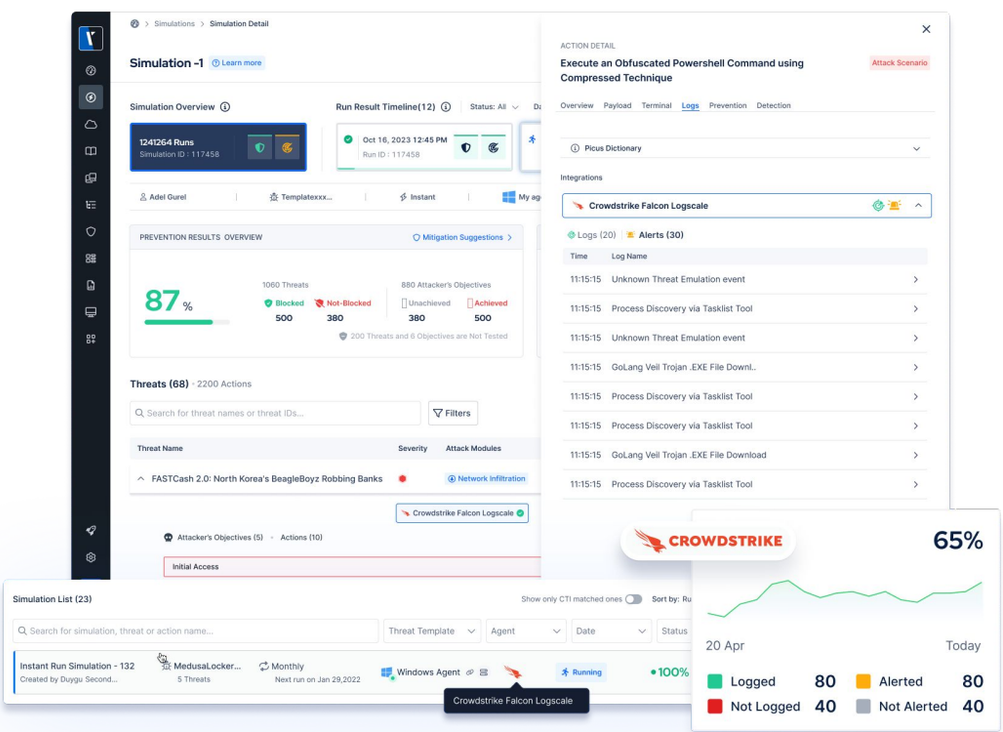
© 2024 Picus Security. All Rights Reserved.

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 CrowdStrike Falcon® LogScale™ Integration

The integration empowers organizations with the capability to fortify their defenses and enhance security operations. By leveraging seamless API connections, Picus conducts targeted attack simulations and enriches CrowdStrike Falcon® LogScale™ SIEM with validated security logs. This provides a deeper, more accurate understanding of an organization's security posture.

Security teams benefit from real-time alerts and reduced false positives, enabling quicker, more effective responses to real threats. Together, Picus Security and CrowdStrike Falcon® LogScale™ establish a resilient and adaptable cybersecurity ecosystem, empowering teams with actionable insights to develop robust defense strategies.



PICUS PLATFORM

The Picus Complete Security Validation Platform simulates cyber threats to continuously 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.
- Pen testing is vulnerability-focused and quickly out of date.
- Boards, auditors & insurers want evidence of security effectiveness.