SIEM

SOLUTION BRIEF

THE PICUS COMPLETE SECURITY VALIDATION PLATFORM AND CROWDSTRIKE NEXT-GEN SIEM INTEGRATION

INTEGRATION BENEFITS

✔ **Real-Time Visibility**
Gain enhanced visibility into security events with continuous validation of log delivery, alerts, and analytical insights.

✔ **Expanded Detection Analytics**
In addition to alert validation, this integration supports Vendor-Based and OS-Based Analysis for a more granular understanding of threats.

✔ **Accelerated Threat Detection**
Enable faster correlation across multiple data sources and reduce time-to-detection with automated validation workflows.

✔ **Continuous Threat Readiness**
Picus simulations help measure the effectiveness of detection logic and keep pace with evolving threats using MITRE ATT&CK® mapped techniques.

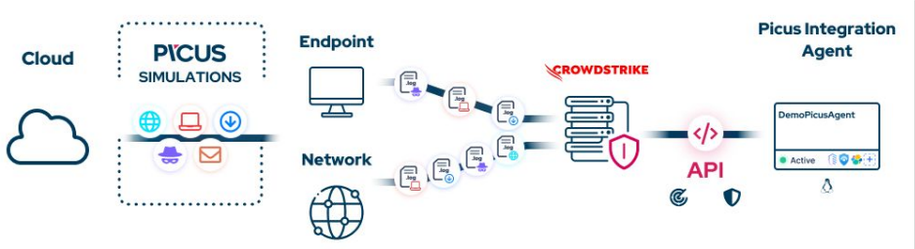
✔ **Reduced Operational Overhead**
Filter out false positives and improve alert fidelity to help security teams focus on meaningful actions.

STRENGTHENING CYBER RESILIENCE: THE PICUS X CROWDSTRIKE NG SIEM INTEGRATION

The integration between Picus Security and CrowdStrike's Next-Gen SIEM provides a modern, unified approach to strengthen detection analytics and bolster cyber resilience.

The Picus Platform integrates seamlessly with CrowdStrike Falcon®, enabling enriched analysis through Next-Gen SIEM capabilities. This integration supports real-time threat detection beyond alert validation, leveraging Vendor-Based and OS-Based Analysis to improve visibility and operational response.

With this integration, security teams can measure and validate detection coverage, correlate events from multiple data sources, and take proactive action to reduce risk.



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® Next-Gen SIEM.
3. Picus pulls the logs and alerts from CrowdStrike Falcon® Next-Gen 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

Picus Security, the leading security validation company, reveals true cyber risk by validating and prioritizing exposures across siloed findings.

Offering Adversarial Exposure Validation with Breach and Attack Simulation and Automated Penetration Testing, Picus enables teams to pinpoint critical gaps, deliver high-impact fixes, and stop more threats with less effort.

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.

© 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.

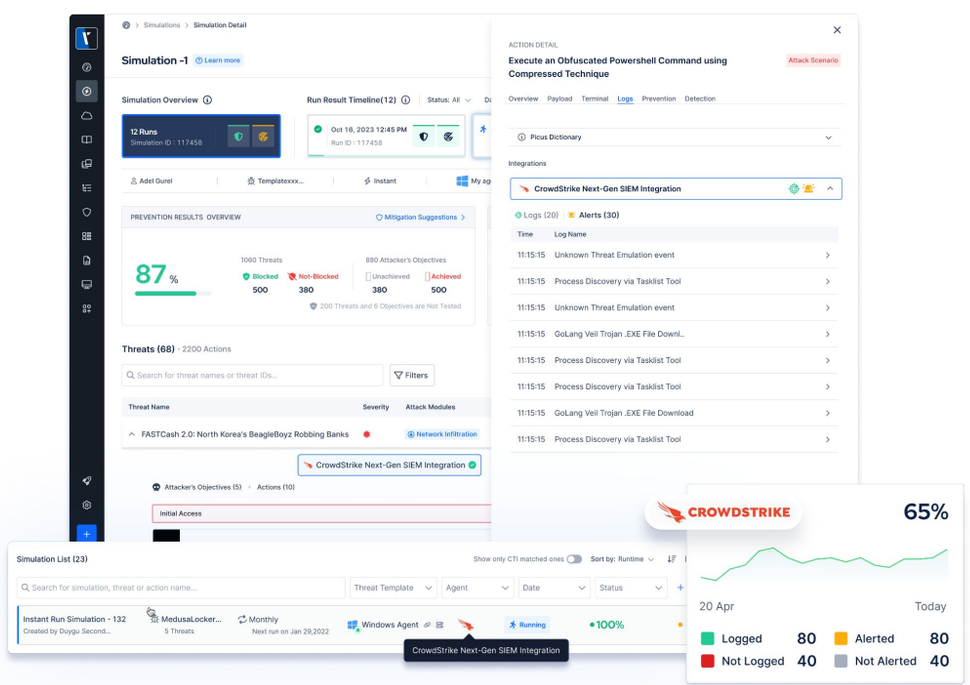
FORTIFYING ANALYTICS-DRIVEN THREAT DETECTION WITH PICUS X CROWDSTRIKE FALCON® CROWDSTRIKE NG SIEM INTEGRATION

The integration between the Picus Complete Security Validation Platform and CrowdStrike Next-Gen SIEM equips security teams with advanced capabilities to proactively assess, validate, and enhance their detection posture.

This integration leverages CrowdStrike's native event analytics, including vendor-based and OS-based analysis, to provide a richer, multi-dimensional view of security coverage. Picus simulates real-world attack scenarios aligned to MITRE ATT&CK®, then validates whether the underlying analytics of CrowdStrike NG SIEM, are correctly identifying and interpreting adversarial activity.

Through secure API-based data exchange, Picus collects relevant logs and alerts from CrowdStrike NG SIEM to observe how detection rules and analytics behave in response to simulated threats. This continuous validation loop enables security teams to verify alert accuracy and assess the depth and context of event correlation, helping ensure that detections are timely, reliable, and aligned with real-world attack scenarios.

As a result, security teams benefit from increased visibility, reduced noise, and accelerated mean-time-to-respond (MTTR). The integration fosters a more resilient detection architecture, where analytics are stress-tested against real-world threats, and actionable insights are delivered to continuously strengthen defenses.



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.