

SOLUTION BRIEF

PICUS PLATFORM AND RECORDED FUTURE INTEGRATION

Integration Benefits

✓ Threat Informed Defense

Use validated threat intelligence to proactively guide attack simulations, ensuring defenses are aligned with the most likely and damaging threats, enhancing overall resilience.

✓ Informed Risk Management

Prioritize attack simulations based on intelligence, empowering security teams to make more informed decisions about their cybersecurity posture.

✓ Region-Specific Threats

Incorporate region-specific threat intelligence to ensure that attack simulations target the most relevant and geographically specific threats, enhancing regional security posture.

✓ Industry-Focused Threats

Align attack simulations with industry-specific threat intelligence, enabling organizations to focus on the most relevant risks affecting their sector.

✓ Efficient Resource Allocation

Leverage threat intelligence to prioritize attack simulations based on real-world risks, ensuring security teams focus their resources on the most critical threats and vulnerabilities, optimizing both time and effort.

Empowering Attack Validation with Intelligence: The Picus x Recorded Future CTI Integration

In the rapidly evolving world of cybersecurity, organizations are constantly challenged with staying ahead of emerging threats while ensuring that their defenses are continually validated. The Picus and Recorded Future integration enables security teams to automate and operationalize the use of threat intelligence, enhancing proactive defense capabilities.

This integration enables the seamless mapping of Recorded Future's threat intelligence with Picus' extensive Threat Library, allowing teams to focus on the most pertinent threats. By automating the alignment of threat intelligence data with attack simulations, the integration drives more accurate decision-making, prioritization, and risk mitigation, helping organizations stay ahead of attackers.



How Picus x Recorded Future CTI Integration Works

- 1. Integration of Threat Intelligence**
Picus syncs Recorded Future's latest threat intelligence and ensures simulations reflect current and relevant risks.
- 2. Threat Informed Validation**
Picus provides CTI-mapped threats, assessing blocked and unblocked actions to gauge the impact of potential threats.
- 3. Dynamic Threat Templates**
Picus' Threat Library provides dynamic templates based on Recorded Future's intelligence, tailored by sector, threat actor, or specific threat.
- 4. Customizable Threat Scenarios**
Create tailored templates to address organization-specific needs, using intelligence-driven insights to quickly adapt to emerging threats and refine defense strategies.

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.

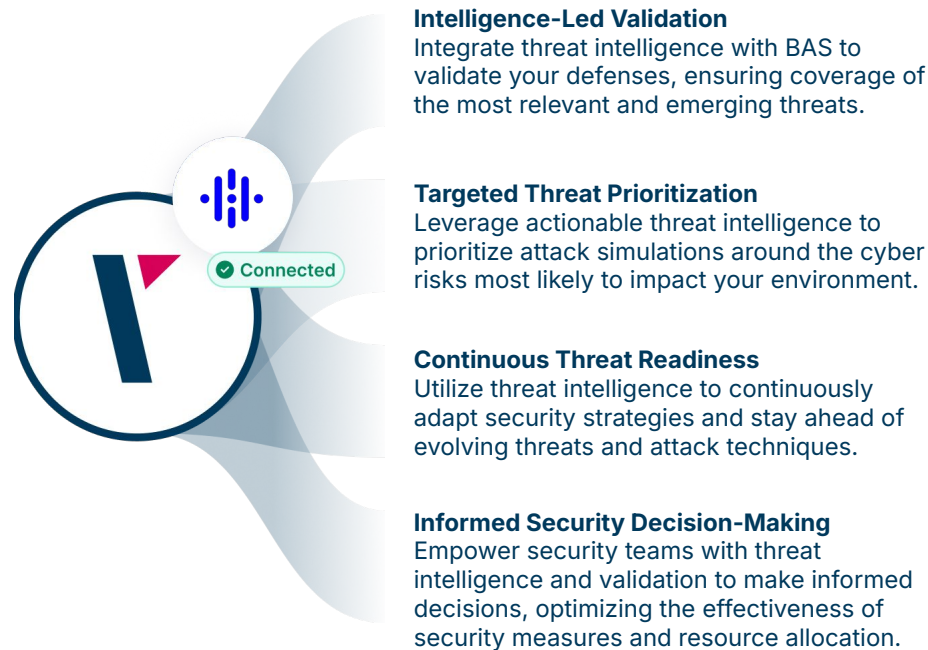
All other product names, logos, and brands are property of their respective owners in the United States and/or other countries.

Strengthening Cybersecurity Defenses With Picus x Recorded Future CTI Integration

Together, Picus and Recorded Future empower organizations to leverage threat intelligence to stay ahead of emerging risks. By integrating Recorded Future's latest threat intelligence, Picus Platform ensures that attack simulations are not only relevant but strategically prioritized.

This integration helps security teams focus on the most critical threats by prioritizing attack vectors and adversary scenarios based on actionable intelligence. This targeted approach enables organizations to make informed decisions, optimize security efforts, and strengthen their resilience in the face of evolving threats.

By combining Picus Breach and Attack Simulation with Recorded Future's threat intelligence, organizations build a dynamic and resilient ecosystem, supported by actionable insights that drive robust defense strategies.



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.