CTI

SOLUTION BRIEF

PICUS SECURITY CONTROL VALIDATION AND CROWDSTRIKE FALCON INTELLIGENCE INTEGRATION

JOINT SOLUTION BENEFITS

✔ **Prioritized Threat Response**
By aligning simulation priorities with the latest threat intelligence, organizations can focus their defensive strategies on the most immediate and relevant threats, ensuring a more efficient and effective response.

✔ **Threat Relevance Alignment**
Stay ahead of the curve by continuously aligning your attack simulations with the most recent threat intelligence. This ensures that your cybersecurity efforts are always targeting the most pertinent threats.

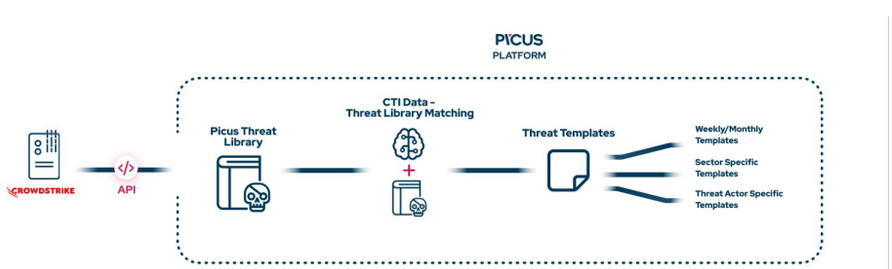
✔ **Informed Risk Management**
The prioritization of attack simulations based on latest threat intelligence enables to make more informed decisions about your cybersecurity posture and resource allocation.

✔ **Enhanced Preparedness**
Regularly testing defenses against prioritized, real-world attack scenarios ensures that organizations are not just prepared for any threat, but specifically for the most likely and damaging ones.

EMPOWERING SECURITY INTELLIGENCE: THE PICUS AND CROWDSTRIKE FALCON INTELLIGENCE INTEGRATION

In the dynamic landscape of cybersecurity, organizations encounter pressing challenges in responding to threats effectively and making informed security decisions. The Picus and CrowdStrike Falcon Intelligence Integration stands as a robust solution, aiming to redefine how security teams leverage threat intelligence. Recognizing the prevalent issues of lack of actionability, assurance, and prioritization, this integration strategically addresses these hurdles. Addressing the disconnect between threat intelligence and security controls, the integration automates the alignment of threat intel feeds with actions in the Picus Threat Library. This streamlines responses to emerging threats, providing a direct link between intelligence and action.

By addressing the challenges associated with threat intelligence and seamlessly integrating it into security processes, organizations can make prioritization with more informed decisions, strengthen their security posture, and effectively mitigate risks in an ever-changing threat landscape.



HOW IT WORKS

1. The integration aims to prioritize the validation of threats by leveraging the most current intelligence data. This is achieved by matching the intelligence data associated with potential threats in the CrowdStrike environment with the threat intelligence data stored in the Picus Threat Library.

2. Users can then access the Intelligence Page and see the metrics related to CTI-mapped threats and associated actions. The page provides visibility into both blocked and not-blocked actions, enabling security teams to assess the impact and severity of potential threats.

3. The Picus Threat Library offers advanced filtering features, allowing users to refine their threat analysis based on various parameters such as sector, malware family, threat actor, and release date. This enables security analysts to focus on threats relevant to their organization's specific environment and concerns.

4. Furthermore, the Dynamic Threat Templates are created to effectively use threats that match CTI data. These dynamic templates include weekly and monthly CTI mapped threats, templates specific to sectors and threat actors. By leveraging these templates, security teams can quickly and efficiently respond to emerging threats based on the latest intelligence data.

ABOUT PICUS

At Picus Security, our priority is making it easy for security teams to continuously validate and enhance organizations' cyber resilience.

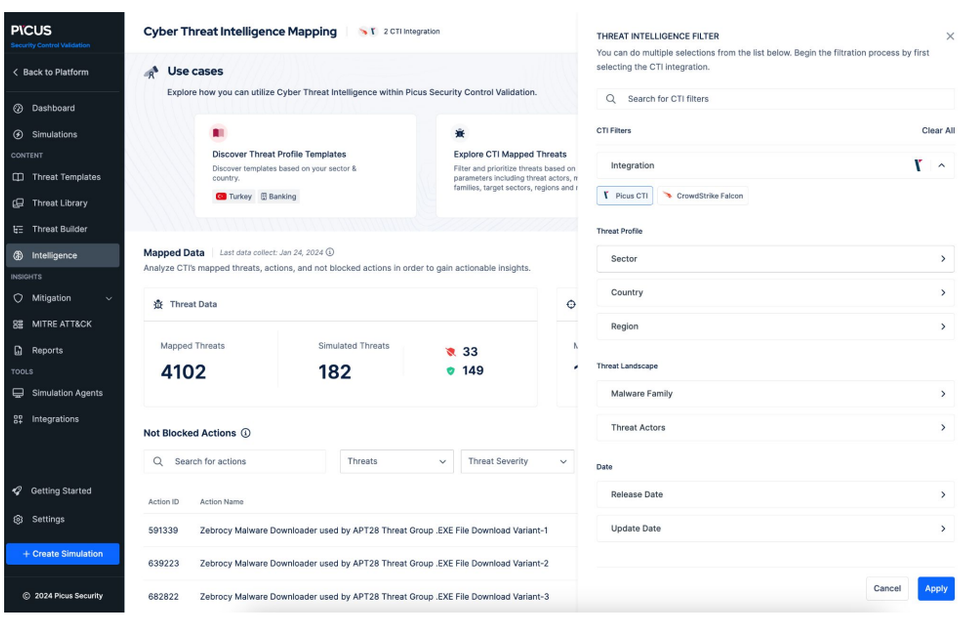
Our Security Validation Platform simulates real-world threats to automatically measure the effectiveness of security controls, identify high-risk attack paths to critical assets, and optimize threat prevention and detection capabilities.

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

INTEGRATION OVERVIEW

The integration between Picus Security Validation and CrowdStrike Falcon Intelligence signifies a groundbreaking evolution in cybersecurity practices, revolutionizing how organizations approach threat readiness. This integration strategically prioritizes attack simulations by leveraging the latest threat intelligence from CrowdStrike Falcon Intelligence. This ensures that an organization's cybersecurity efforts are not only targeted but also efficiently operationalized.

When the threat vectors identified by CrowdStrike align with those in our extensive Picus Threat Library, the Picus platform goes beyond merely highlighting these threats; it actively guides clients in prioritizing these specific attack vectors. This prioritization approach is both strategic and actionable, offering clear guidance on addressing the most critical threats first. This empowerment equips organizations with the insights needed to make informed decisions, directing their efforts where they are most impactful and maintaining a proactive stance in cybersecurity defenses.



THE PICUS 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.
- Pen testing is vulnerability-focused and quickly out of date.
- Boards, auditors & insurers want evidence of security effectiveness.

Experience Picus in Action

GET A DEMO

Gartner peerinsights™

4.9 / 5*

*average score at time of press in January 2023

www.picussecurity.com

picussecurity

© 2023 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.