EDR

SOLUTION BRIEF

THE PICUS COMPLETE SECURITY VALIDATION PLATFORM AND CROWDSTRIKE FALCON INSIGHT EDR INTEGRATION

MAXIMIZE THE VALUE OF CROWDSTRIKE TO ENHANCE YOUR THREAT DETECTION AND RESPONSE CAPABILITIES

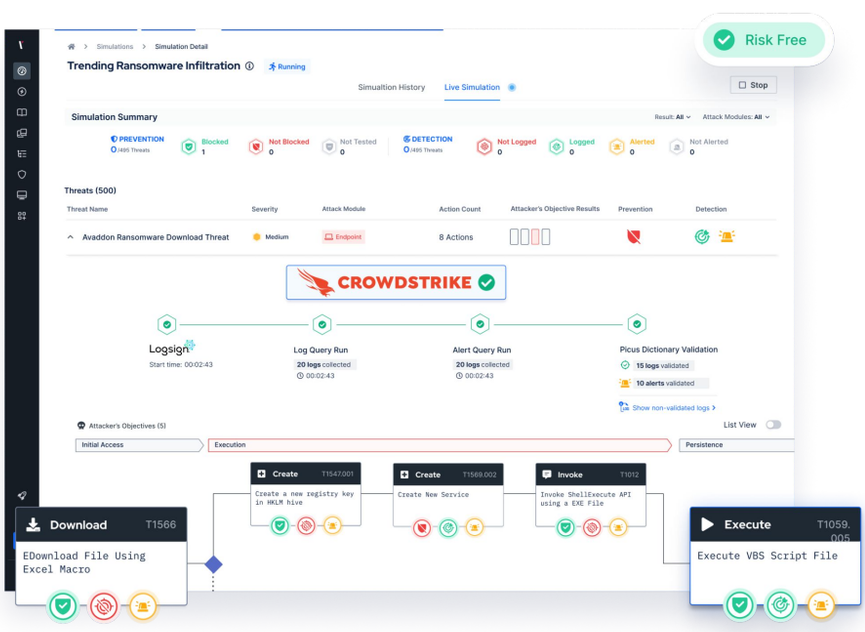
THE CHALLENGE

Endpoint Detection and Response (EDR) technologies have been a game-changer. Going beyond simple and fast-changing attack indicators, cyber security professionals can now build long-lasting detection policies against attack behaviors a.k.a. TTPs (techniques, tactics and procedures) utilizing rich endpoint telemetry. While the adoption of EDR has been relatively fast, the increasing sophistication of cyber-attacks and operational load create challenges in ensuring security tools remain effective at preventing, detecting, and responding to the latest threats.

Picus Security, the pioneer of Breach and Attack Simulation, and CrowdStrike have joined forces to make is easier for CrowdStrike EDR users to proactively update their security policies, achieve the best detection coverage, and increase ROI. The Picus Platform simulates real-world cyber threats and uses advanced detection analytics to reveal unactivated and missing telemetry sources, and missing detections. The validation provided by The Picus Platform helps identify if EDR logging policies are set correctly and that detection rules have the right scale and quality so that attacks are detected.

PICUS & CROWDSTRIKE INTEGRATION

Based on a seamless API-based integration, The Picus Complete Security Control Validation Platform becomes Crowdstrike Falcon EPP & EDR users' de-facto validation tool. The integration reveals policy update requirements about data generation settings and detection rules (custom IOAs) on Falcon Insight. Thanks to The Picus Platform's continuous attack simulation and analysis features, the integration provides trend analysis on security posture, historical and segment-based comparisons, MITRE ATT&CK Enterprise mapping and more. The integration also reveals delays on alerting and helps security analysts pinpoint issues such as storage availability, licensing issues, network outages, and application conflicts.



The integration of Picus and CrowdStrike EDR offers several benefits:

✔ Proactively identify detection gaps to enhance security before real attacks occur.

✔ Establish and maintain an effective detection baseline.

✔ Reduce false positives, minimize alert noise, and accelerate the time to detect threats.

✔ Generate actionable metrics by mapping advanced attack scenario emulations to the MITRE ATT&CK Framework.

✔ Facilitate agile threat hunting capabilities.

✔ Save time through advanced usability, filtering, and reporting features.

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.

Test Your Defenses Against the Latest Threats

START FREE TRIAL

Gartner peerinsights™

4.9 / 5*

*average score at time of press in January 2023

www.picussecurity.com

picussecurity

USE CASES

1. Improve Attack Readiness Visibility

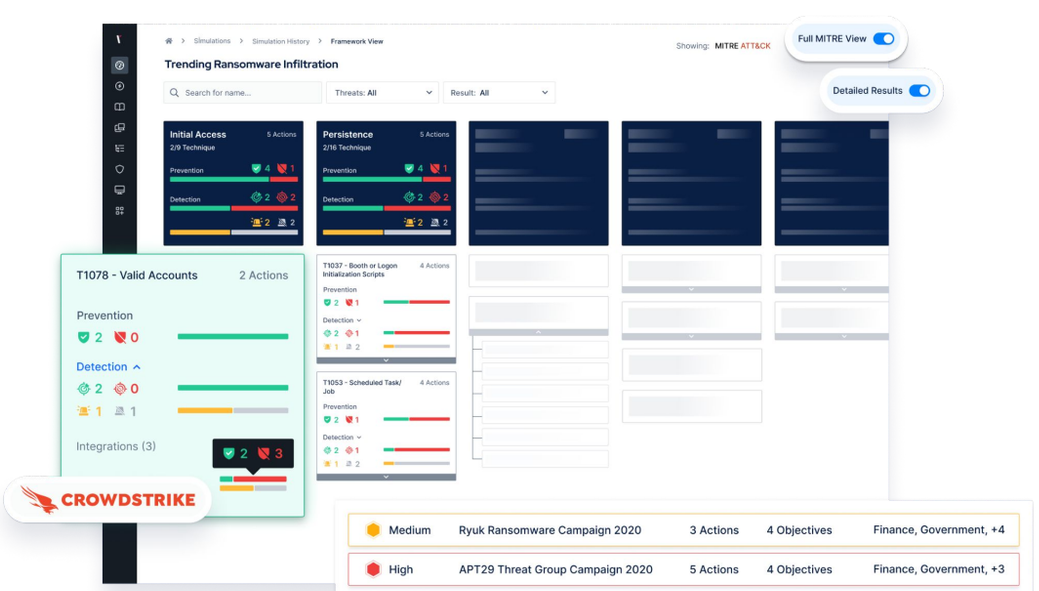
The evolving threat landscape means that the question "are we ready" often unsettles cyber security professionals. Challenges around identifying the most relevant adversarial activities, business continuity, finding reliable test tools and crafting threat samples makes it difficult to establish if defenses are ready against new potential attacks.

Offering the most extensive curated threat library in its field, The Picus Platform continuously challenges Falcon Insight with over 11,000 threat samples and custom-built scenarios. It effortlessly identifies detection gaps and answers questions on readiness for Falcon users with an intuitive UI. Rich reporting features of The Picus Platform enable security teams to demonstrate the value of Crowdstrike.

2. Achieve Better Detection Rates and Faster Response Times by Adding Purple Teaming Capabilities

As internal and external cyber-risks constantly change, organizations may find it difficult to provide the most relevant risk context to its defense teams. Scarcity of human resources, time and tools each play an important role for the absence of this invaluable context.

The integration between Picus and Crowdstrike ties internal and external risk factors together, aligns offensive and defense teams, enables proactive Secops and SOC practices, and establishes a purple teaming capability. The Picus Platform offers not only an innovative Breach and Attack Simulation technology, but also a set of rich automation features and mitigation insights, whether it is in the form of telemetry enhancement or a new Crowdstrike IOA rule. This combination of rich feature set and content help security practitioners lower alert fatigue by eliminating low quality alerts and false positives, and improve MTTD (mean time to detect) and MTTR (mean time to response) metrics.



3. Operationalize MITRE ATT&CK Matrix to Achieve Metrics-Driven Operations

MITRE ATT&CK Matrix for Enterprise has become the de facto knowledge base to understand adversarial behaviors and how criminal actors chain them together to launch sophisticated attacks. While this extensive knowledge base is invaluable as an entity, making effective use of it requires organizations to build a live link between a massive number of security events and MITRE ATT&CK.

By mapping gaps and coverage findings for both security events and detections to MITRE ATT&CK, The Picus Picus elevates this knowledge base to a measurement baseline and helps Falcon Insight customers to run their operations with relevant and impactful success metrics.