Picus Security and Microsoft Defender for Endpoint EDR Solution Brief

Picus Security Cyber Defense Validation Platform Maximizes Microsoft Defender for Endpoint's Potential

Introduction

As the sophistication of attacks increase and endpoint segments generate large volumes of data, it gets more difficult to attain uninterrupted visibility on malicious activities. Endpoint Detection and Response (EDR) technologies play an important role in analyzing the large volume of endpoint telemetry and pinpointing malicious activities. On the other hand, EDRs also need diligent surveillance and to be kept adapted to the changing adversarial and environmental changes.

To assist Microsoft Defender users, the Picus platform challenges and consequently applies advanced detection analytics queries on Microsoft Defender EDR to reveal unactivated log sources, missing telemetry, and missing detections. The validation provided by the Picus platform helps identify if EDR logging policies are set correctly and detection rules have the right scale and quality so that attacks are detected while false positives are minimized.

Products

- Microsoft Defender for Endpoint
- Picus Security Cyber Defense Validation Platform

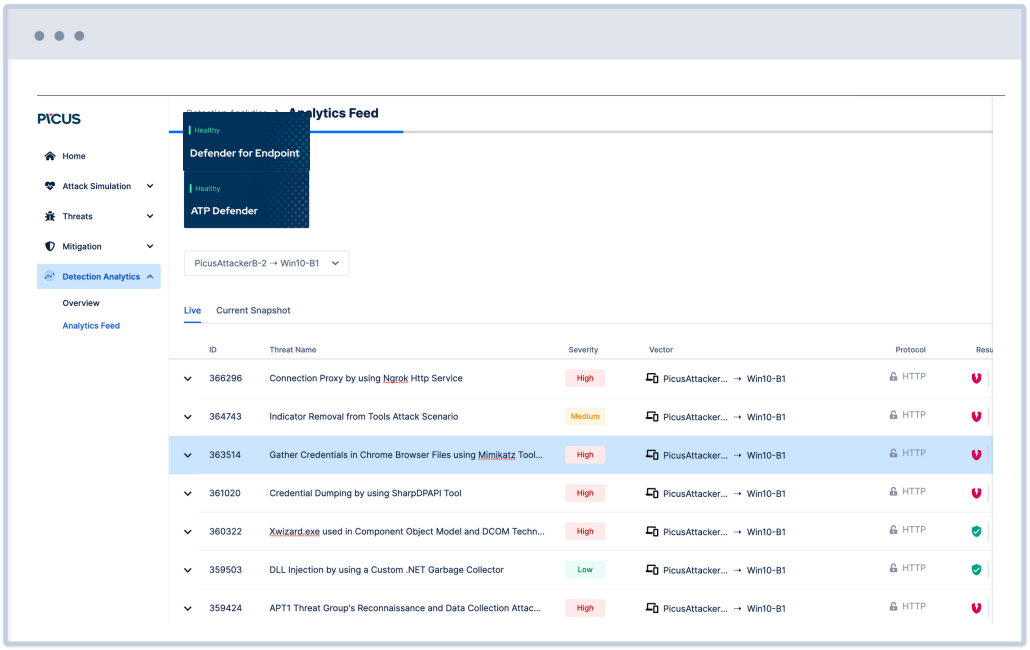
The integration between Picus Cyber Defense Validation Platform, based on an innovative Breach and Attack Simulation technology, and Microsoft Defender for Endpoint EDR proactively reveals undetected attack techniques and guides security practitioners to take the required corrective actions.

Picus Detection Analytics Solution Overview

The Picus Platform challenges the entire security control estate in customer networks continually or on-demand by executing thousands of real adversarial scenarios. Results of these controlled tests are stored in the Picus Manager. Picus Detection Analytics is an automated module that queries endpoint processes and security activities collected in EDR platforms and compares the findings with the emulation results stored in the Picus Manager. This comparison reveals security gaps in different forms and depth SOC technologies may have.

The Picus Platform operationalizes the most extensive adversarial context, covering more than 90% of the MITRE ATT&CK techniques and the largest number of malware, vulnerability exploits, and web application attack samples, thanks to the Picus Threat Library.

Picus Detection Analytics module narrows down its log and detection validation findings utilizing a proprietary content called Picus Keyword dictionary. This precision on validation findings shortens alert triage in the range of 30 to 90%.

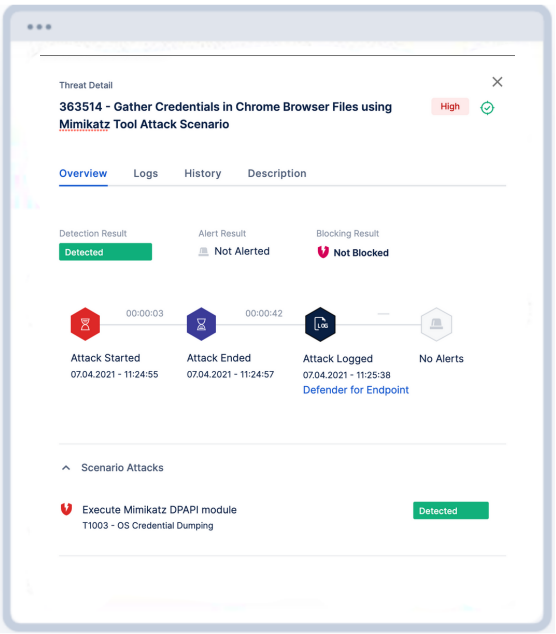


Benefits of Picus Cyber-Defense Validation Platform & Microsoft Defender for Endpoint EDR Integration

The technology integration between Picus Security and Microsoft Defender for Endpoint aims at providing:

- insights on not overlooked and new log and telemetry sources,
- proactive detection coverage visibility to reveal security gaps,
- guidance on which existing rules should be activated,
- guidance on developing new rules
- rich and validated threat content to facilitate threat hunting activities.

This innovative approach helps users make the most out of their advanced Microsoft Defender for Endpoint EDR investments and preemptively mitigate cyber risk.



About Picus Security Inc.
Picus is a simple, pervasive, continuous security validation in a box. The Picus Platform is designed to continuously and instantly measure the effectiveness of security defenses by using emerging threat samples in production environments. Picus requires minimum deployment effort and is fully automated to deliver effortless threat-centric assessments and actionable, technology-specific insights. With Picus, it is possible to leverage advanced technologies to fully utilize their potential, maximize their effectiveness, and keep a hard security baseline free of hidden gaps.
For more information go to picussecurity.com