Picus Security and Microsoft Azure Sentinel SIEM Solution Brief

Building Proactive Log and Detection Capabilities with Threat-Centric Validation in SOCs

Introduction

It is vital that cyber defense teams know whether they are ready for new threats before attacks occur or in the early stages of an attack campaign. Given the amount of work that cyber defense teams are under, the speed and complexity of cyber threats, and the increasing number of alerts and incidents overwhelm security teams and make it difficult to measure readiness to attacks. Moreover, concerns about business continuity and false positives delay the processes of developing the right policies and content to close security gaps.

Picus Security's Detection Analytics solution helps cybersecurity organizations address these challenges by integrating threat-based validation into SOC processes. Picus Cyber Defense Validation Platform emulates malicious techniques, finds the gaps, and measures risks associated with log collection and detection rule base. Picus' mitigation library provides ready to apply mitigation guidance and content so that security professionals can quickly take actions to close the identified gaps.

Products

- Microsoft Azure Sentinel SIEM
- Picus Security Cyber Defense Validation Platform

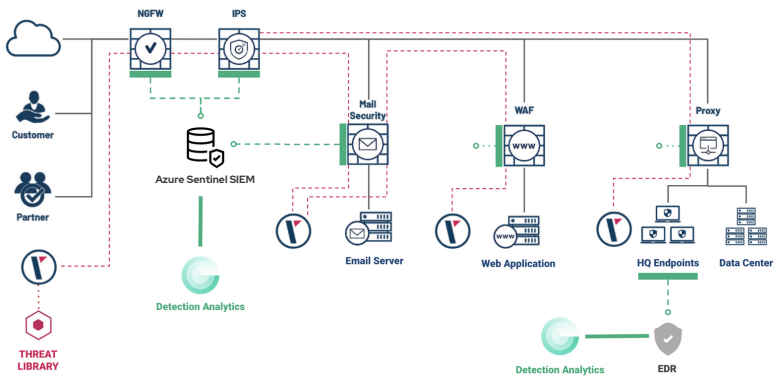
The integration between Picus Cyber Defense Validation Platform, based on an innovative Breach and Attack Simulation technology, and Microsoft Azure Sentinel SIEM helps customers build robust defenses and quicker detection processes. The Picus platform reveals log and alerting gaps, and provides detection content to help quickly close these gaps.

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 Picus Manager. Picus Detection Analytics is an automated module that queries security events collected in SIEM platforms to analyze the detection and prevention actions taken across the security control estate and compare the findings with the emulation results stored in Picus Manager. Picus Detection Analytics module minimizes false positives in detecting logs and alerting gaps by running an internal validation process based on an advanced detection content library called Picus Keyword Dictionary. The Keyword Dictionary contains a proprietary content of compromise indicators that the Picus Labs teams continually update and maintain.

Advanced capabilities of the Detection Analytics:

- identify log generation and collection problems,
- reveals threats that security controls have not detected,
- discover gaps and quality shortcomings about detection/correlation rule set,
- provides a verified Sigma-based detection rule set.

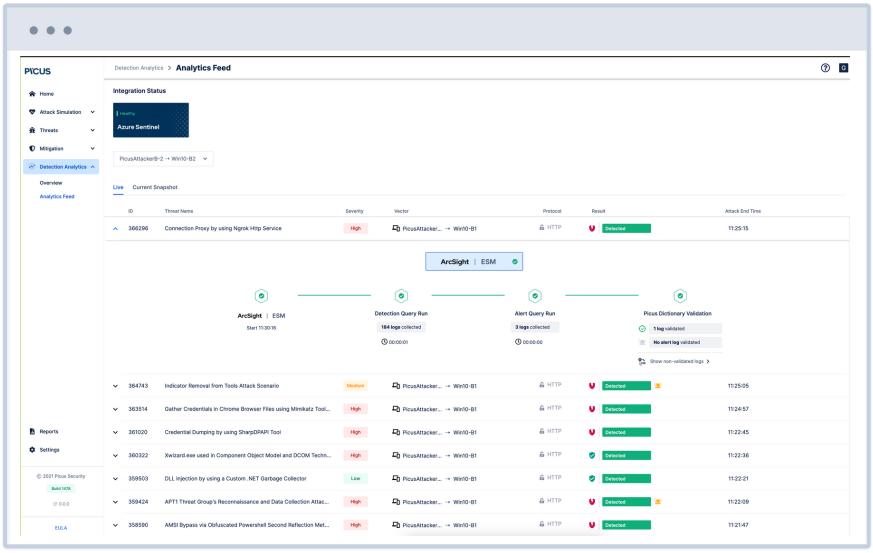


Picus Cyber-Defense Validation Platform & Microsoft Azure Sentinel SIEM

Working as part of the Picus Cyber-Defense Validation Platform, Picus Detection Analytics further enhances Microsoft Azure Sentinel's advanced features and increases its utilization, thereby increasing return on investment. Providing flexible 24x7 or on-demand modus operandi, Picus Detection Analytics validates log delivery status and alert status using its rich Threat Library. Picus Threat Library covers more than 90% of the MITRE ATT&CK techniques and a large number of malware, vulnerability exploits, web application attacks, and data exfiltration attack samples.

Based on emulated attack samples, Picus provides insights specific to Microsoft Azure Sentinel. As a result, it provides the SOC teams the ability to;

- validate the logging capability against a specific attack technique when needed,
- demand network teams to investigate and fix the delays in log delivery,
- help incident responders prioritize correctly,
- shorten mean time to detect and respond by improving log and alerting efficacy,
- use ready-to-apply and verified detection rules,
- proactively measure if processes are aligned, teams are empowered, and technology infrastructure is utilized effectively,
- provide threat hunters insight needed to build and execute scenarios.



Picus Provides an Extensive Sigma-Based Detection Content Library

Developing detection rules is a crucial SOC function. In most cases, all security analysts can understand detection rules fully or to a certain extent, but only expert security analysts, detection engineers, can write them. Detection rules are similar to software code, and developing them requires extensive technical knowledge and experience. Detection rules, similar to software, have their own life cycles. Based on field interviews and observations, the Picus Customer Success team found out that it takes seven hours on average to write a single, sophisticated detection rule. This duration is longer if the detection rule aims to address complicated advanced threats.

Due to the dependency mentioned above and the difficulty of continually writing and adding new rules, companies either work with a limited or a large but generic ruleset and are exposed to alerting gaps, alerting noise, and increased cyber-risk.

To address this challenge, Picus Labs develops Sigma-based rules. As of May 2021, there are 509 sigma rules that help successfully detect 788 malicious actions hidden in 494 threats.

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