PICUS | THE COMPLETE SECURITY VALIDATION PLATFORM

DATASHEET

DETECTION RULE VALIDATION

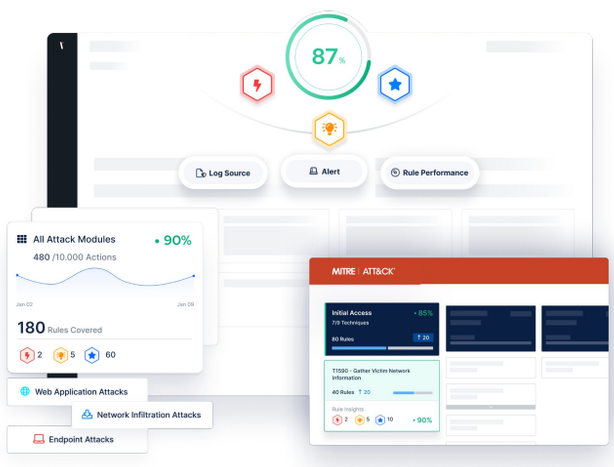
VALIDATE THE EFFECTIVENESS OF YOUR DETECTION RULES

SIEMs are fundamental to modern SOCs, helping security teams detect and respond to cyberattacks before they significantly impact an organization's business. In recent years, the volume of alerts, logs, and the number of new threats that security teams have to deal with has increased exponentially. This is because organizations are collecting more data than ever, and new and more sophisticated threats are constantly emerging. Due to time and resource constraints, SOC engineers struggle to keep on top of existing rules as well as develop and test new ones.

SIEM solutions that process security alerts in real-time and analyze data from multiple sources are considered critical to enterprise security. When asked what problems hinder organizations from maximizing the value of their SIEM systems, the most common answer was a lack of capable employees (41%)* and too many false positives (37%).*

With Detection Rule Validation, security teams can quickly identify issues related to the performance and hygiene of detection rules and obtain insights to help optimize threat detection and response capabilities.

* Cybersecurity Insights 2022 SIEM Report



PICUS DETECTION RULE VALIDATION

The **Picus Detection Rule Validation,** optimizes threat detection and response capabilities along with reducing the effort required to maintain and optimize the performance of detection rules.

HOW DETECTION RULE VALIDATION STRENGTHS YOUR RULEBASE

Maximize SOC Effectiveness

Maximize the SOC team's confidence that the right rules are in place and that alerts are triggered for critical security incidents.

Focus on What Matters Most

Highlight detection coverage based on real-world threats that matter to the organization and relieve SOC engineers from tedious tasks so that they can focus on what matters most.

Enable Proactive Rule Validation

Get insights about the threat coverage, accuracy and performance of detection rules and enable SOC teams to perform proactive rule validation.

Optimize Threat Detection and Response

Get an holistic visibility of threat detection and response capabilities and accelerate the operationalization of the MITRE ATT&CK Framework.

Reduce the Effort Required to Maintain and Optimize

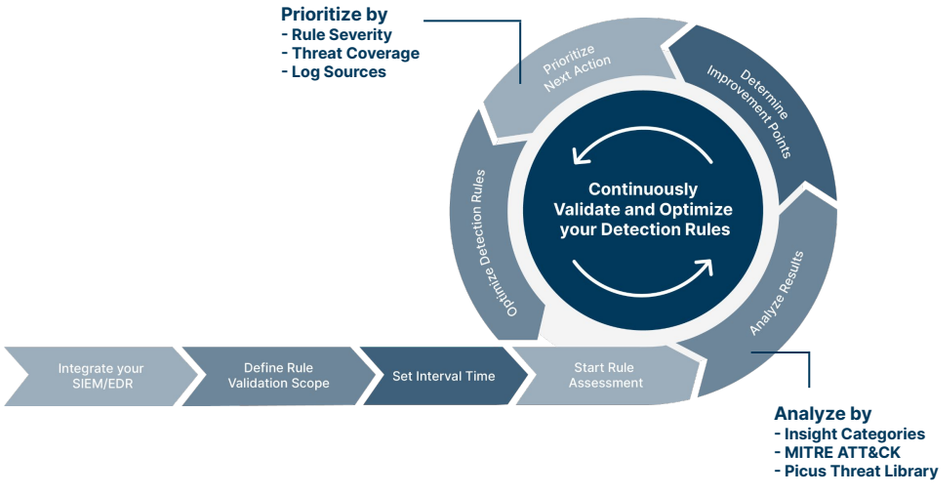
Reduce the detection engineering efforts for newly emerging threats from hours to a few minutes.

Validate the Effectiveness of Detection Rules

Validates the effectiveness of existing and new rules based on log coverage, alert frequency and performance metrics.

THE MOST SENSIBLE WAY
CONTINUOUS DETECTION RULE VALIDATION

SOC teams require a proactive alert validation process to identify redundant and obsolete rules and incomplete and ambiguous use cases. This process should also be able to add new high-quality detection rules proactively to address new tactics, techniques, and procedures utilized by adversaries. This is the most sensible way to lower the number of alerts and ensure that security analysts receive relevant alerts.



SUGGESTED BEST PRACTICES

✓ Determine an assessment scope and continuous assessment times with an API connection. After starting the first of the continuous assessments, the best practice is to examine the results of the assessment and prioritize the improvement insights in the rules according to the insight categories, improve the rules, see the improvements made in the next assessment and repeat the cycle.

✓ Develop new rule and analyze this new rule in the next automatic assessment. In this way, examine and evaluate the insights about the rule, and improve the rule if necessary. Thus, ensure that the new rule works better/performing from the first day and follow the improvement insights that may arise in the rule with continuous assessments.

DETECTION RULE VALIDATION SECURITY ALLIANCES

splunk> IBM Security QRadar Microsoft Sentinel

More partnerships are added regularly.

WHY DETECTION RULE VALIDATION?

- ✓ Awareness-raising and resolution-providing solution
- ✓ Not the problem maker, but the solution provider technology.
- ✓ Easy to deploy, use and manage.
- ✓ Executive dashboards and reports

KEY FEATURES

✓ Supplies **holistic visibility** of threat detection and response capabilities.

✓ Provides **insights** on the Fixing Items, Improvement Points, and Positive Points over detection rule baseline.

✓ **Continuously** detects improvement points in the rule baseline by the correlations of the insights given for the rule.

✓ **Prioritizes** rules that need improvement with filtering options on the assessment result.

✓ Reveals the effect of a **newly developed rule** on SIEM.

✓ Maps results to **MITRE ATT&CK** Framework.

✓ Measures the **threat coverage** of rules and analyze deficiencies with **an extensive Picus Threat Library** of 3,700+ threats consisting of 19K+ actions, **updated daily.**

It's time to automate the jobs you can't find time for!

LEARN MORE

Gartner peerinsights™

4.9 / 5*

*average score at time of press in January 2023

www.picussecurity.com

picussecurity