PICUS | THE COMPLETE SECURITY VALIDATION PLATFORM

DATASHEET

SECURITY CONTROL VALIDATION FOR DETECTION CONTROLS

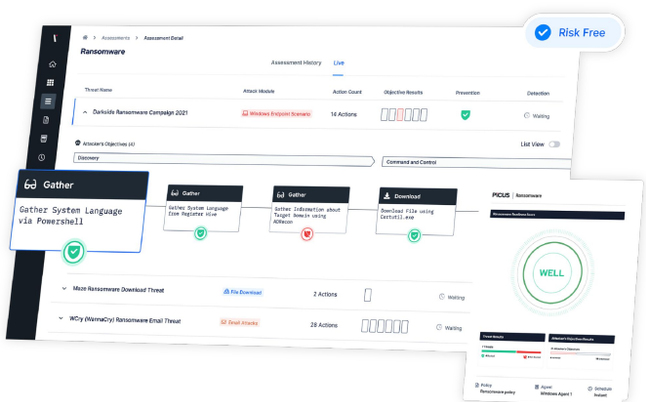
A strong and resilient defense against cyber threats not only demands a robust layer of prevention but proactive detection capabilities too. With **Picus Security Control Validation** (SCV) featuring integrated **Detection Analytics**, get the support you need to validate the performance of your organization's SIEM & EDR tools and ensure that they are optimized to identify and respond to the latest attacks.

ACCELERATE DETECTION AND RESPONSE BY MAXIMIZING THE EFFECTIVENESS OF YOUR SECURITY STACK

To minimize the risk of cyber-attacks causing damage and disruption, it's vital to detect and respond to them as early as possible.

By simulating over 3,800 real-world threats and supplying actionable insights to optimize your controls to identify them, Picus SCV helps you to be proactive and ensure your defenses are ready to disrupt malicious events more swiftly and reliably.

With its automated and continuous approach to security control validation, Picus SCV also alleviates the strain of keeping up with threats 24/7 - enabling you to focus on mitigating coverage and visibility gaps rather than discovering them.



Validate, measure and enhance the performance of your SIEM and EDR tools.

HOW PICUS SECURITY CONTROL VALIDATION WITH DETECTION ANALYTICS BOOSTS YOUR SECURITY OPERATIONS

Identifies visibility blindspots

Picus pinpoints attacks that are missed by your prevention and detection controls, enabling you to identify threats which could pose a serious risk if mitigating action is not taken.

Decreases attacker dwell time

So you can respond to threats earlier in the kill chain, Picus validates that the rulesets you use to optimize your controls are effective and generate prompt alerts.

Enables swiftlier threat mitigation

To reduce the time and effort required to tune your security controls, Picus supplies thousands of vendor-specific and SIGMA-based detection rules.

Operationalizes MITRE ATT&CK

Picus maps assessment results to the MITRE ATT&CK Framework, enabling you to visualize threat coverage and prioritize mitigation of gaps.

Facilitates threat hunting

By identifying attack techniques able to bypass your controls, Picus aids your hunt for threats that may have used similar methods and remain undetected.

Reduces false positives

Supplying correlation rules that are tested by our Labs team prior to release, Picus ensures that the detection content you use is effective and reliable.

ENHANCING THREAT DETECTION ACROSS NETWORKS AND ENDPOINTS

To ensure that your detection controls remain effective, it's vital to test and tune them regularly. With Picus Security Control Validation, obtain the real-time data and actionable insights required to achieve optimal protection at all times.

SUPPORTED TECHNOLOGIES:

Security Incident and Event Management (SIEM)

→ Log Validation

Without the right data it's impossible to identify threat activity in your networks.By simulating real-world threats and analyzing the security logs captured by your SIEM, Picus SCV enables you to:

- Determine if logs from relevant sources are being ingested (and in a timely fashion)
- Understand and prioritize new data sources required to address logging gaps
- Ensure that logs contain the requisite level of data granularity

→ Alert Validation

In order to detect threats early and reduce attacker dwell time, it's also vital to ensure that appropriate SIEM correlation rules are in place to alert on the latest adversary behaviors. With Picus SCV, quickly identify:

- Missing, redundant and obsolete rulesets
- Logged events that don't generate alerts
- Delays between security events and alert generation

SIEM PARTNERS Include

splunk> Microsoft Sentinel SIGMA

CyberRes ArcSight Elastic Security securonix

NETWITNESS An RSA Business LogRhythm CRYPTOSIM

IBM Security QRadar

Endpoint Detection and Response (EDR)

→ Telemetry, Alert and Detection Rule Validation

Detecting and responding to attacks early in the cyber kill chain also relies on rich telemetry from endpoints. To facilitate the detection of threats that target your organization's devices, Picus SCV integrates with leading EDR solutions to:

- Validate that the most relevant endpoint data is being captured and analyzed
- Identify missing, redundant and obsolete rulesets and watch lists
- Measure the time between security events and alert generation
- Highlight behaviors that are detected but not blocked by prevention controls
- Locate quality and performance issues that limit rule effectiveness

EDR PARTNERS Include

Microsoft Defender for Endpoint SentinelOne CROWDSTRIKE vmware Carbon Black

THE INSIGHTS YOU NEED TO SWIFTLY MITIGATE GAPS

Identifying threat coverage and visibility gaps is one thing but closing them requires additional technical skills and experience.

To reduce the time it takes to develop, implement and tune detection content, Picus SCV supplies thousands of prevention signatures and detection rules.*

This includes vendor-specific and SIGMA rules - all fully tested by the Picus Labs team to ensure that they are effective and can be implemented without a high risk of false positives.

* Mitigation insights for detection controls are currently available for attacks includ as part of The Picus Platform's Endpoint Attack Module only

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

© 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.