SECURITY CONTROL VALIDATION

Prevention and Detection Controls

Reduce risk by validating detection and prevention effectiveness

A powerful defense against cyber threats not only demands a layer of prevention but also detection capabilities. In addition to validating the effectiveness of your organization's preventative security stack, companies need to validate the performance of SIEM and EDR tools to ensure they are implemented properly to identify and mitigate attacks.

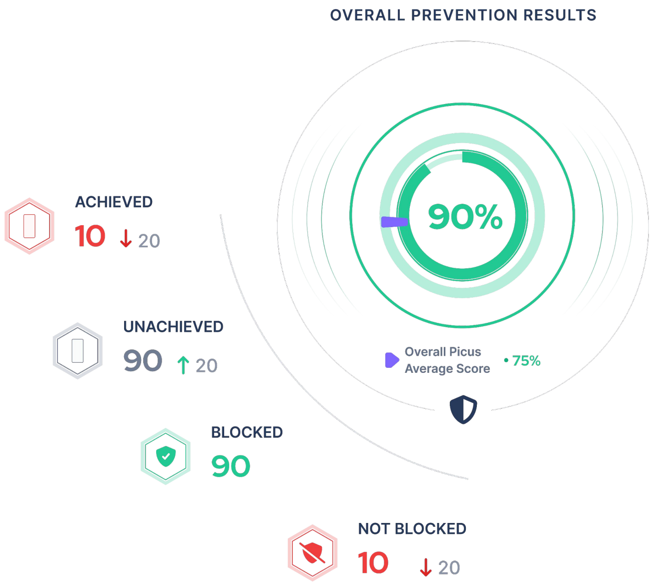
While preventive controls aim to stop security incidents from happening in the first place, detective controls are designed to identify potential breaches after they occur. Security Control Validation (SCV) offers both protection and detection control validation capabilities that are critical to ensure security posture.

What Prevention and Detection Control Validation Does

Prevention Control Validation

Validates the effectiveness of prevention defenses including:

- Network Security, IPS, NGFW
- Secure Web Gateways (SWG)
- Antimalware / antivirus
- Data Loss Prevention
- Endpoint Protection (EPP)
- Email and Network Sandboxes
- Web Application Firewalls
- Secure Email Gateways
- URL Isolation



Detection Control Validation

Validates the effectiveness of detection defenses including:

SIEM

Collect and analyze security logs from various sources to identify anomalies, threats, and incidents

Tested capabilities of detection controls include:

- Log Collection
- Correlation Rules
- Custom Rule Creation
- Alerting
- Behavioral and Signature-Based Detection

EDR

Analyze endpoint activities to detect and respond to threats:

- Laptops
- Desktop
- Servers

How SCV Optimizes Threat Prevention and Detection

Picus SCV Optimizes Threat Prevention by:

- Identifying attacks that weren’t prevented by controls, enabling security gap mitigation
- Validating that assets are covered by preventive controls, as your IT infrastructure expands
- Boosting prevention capability effectiveness, benchmarked continuously, SCV provides individual and collective performance metrics for each of your controls
- Delivering vendor-specific prevention signatures and generic mitigation suggestions
- Mapping validation results to the MITRE ATT&CK® framework, enabling you to visualize threat coverage and prioritize gap mitigation

Product Highlights

- Maps validation results to the MITRE ATT&CK® framework, enabling you to visualize threat coverage and prioritize gap mitigation
- Identifies gaps in your security posture through on-demand testing of your security infrastructure and controls
- Tracks security posture changes over time, enabling organizations to maintain appropriate controls.

Picus SCV Optimizes Threat Detection by:

- Enabling quick response to threats earlier in the kill chain and validating rulesets to so that controls are effective, generating immediate alerts
- Reducing the time and effort required to tune your security controls, Picus provides thousands of vendor-specific and SIGMA-based detection rules
- Identifying attack techniques able to bypass controls, Picus aids your hunt for threats that may have used similar methods and remain undetected
- Leveraging correlation rules tested by our lab team prior to release, Picus ensures that detection content is effective and reliable.

Product Highlights

- Integrates with top SIEMs and EDRs, targeting whether threats, malicious activities and anomalous behaviors are logged, correlated, detected, alerted and responded to.
- Vendor-specific and category mitigation insights that save remediation time
- Log validations to ensure that SIEM and EDR solutions are collecting and processing the necessary logs to accurately detect threats.
- Alert validations to ensure that security alerts generated by SIEM and EDR systems are accurate and relevant.

Comprehensive Integrations

SIEM

splunk>

Microsoft Sentinel

IBM Security QRadar

EDR

CROWDSTRIKE

vmware Carbon Black

Microsoft Defender for Endpoint

To see our latest integrations visit picussecurity.com/integrations.

How SCV Threat Prevention and Detection Works

Threat Prevention

To ensure that prevention control are effective at blocking the latest threats, the Picus Threat Library, with over 5,800 threats and 25,000 TTPs, is updated daily by a team of experts. New threats are added within 24 hours of disclosure and are mapped to MITRE ATT&CK, OWASP, CVE, and CWE references, as well as target applications and operating systems.

Picus SCV, with its leading breach and attack simulation (BAS) technology, simulates the following attacks:

- **Malware and Ransomware:** Determine the readiness of your organization's controls to prevent the latest malware and ransomware attacks
- **Email:** Validate the effectiveness of your controls to block malicious links and attachments
- **Endpoint**: Validate that attacks from threat groups, including APTs, are prevented by endpoint security controls
- **Vulnerability Exploitation**: Understand how effective your security controls are at blocking local and remote code exploitation
- **Web Application :** Gauge if your defenses are capable of blocking code injection, denial of service, and brute force attacks
- **Data Exfiltration:** Assess whether your defenses can prevent the exfiltration of sensitive personal and financial information over HTTP/S
- **Cloud Attacks:** Proactively identify and address security threats specific to your cloud infrastructure by performing cloud attack simulations

Threat Detection

Identifying threat activity, including potential breaches quickly, is critical to response times and overall organizational resilience. Through SIEM and EDR integrations, Picus validates controls for your network and endpoints.

SIEM

- **Log Validation**: Picus identifies threat activity in your networks by simulating threats and analyzing security logs captured by your SIEM. With Picus, you can:
    - Determine if logs 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 vital to ensure that SIEM correlation rules are in place to alert on the latest adversary behaviors. With Picus SCV, you can quickly identify:
    - Missing, redundant and obsolete rulesets
    - Logged events that don't generate alerts
    - Delays between security events and alert generation

EDR

- **Telemetry, Alert and Detection Rule Validation:** Detecting and responding to attacks early in the cyber kill chain relies on rich telemetry from endpoints. To detect threats that target your organization's devices, Picus integrates with leading solutions.

Gartner
Peer Insights
Customers' Choice 2024 ™

Highest Rated Vendor

4.8/5

★★★★★

Gartner, Voice of the Customer for Breach and Attack Simulation Tools, Peer Contributors, 30 January 2024

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.