PICUS

High Performance Breach & Attack Simulation

Reduce risk by validating detection and prevention effectiveness

Organizations struggle to understand which cybersecurity threats will have the most impact on their business operations. Security teams need the ability to fine-tune both detection and prevention by validating the effectiveness of their controls. By validating, teams can easily identify and shut down the most business-critical cyber threats, improving their overall security posture.

What Security Control Validation Does

Picus Security Control Validation (SCV) is a Breach and Attack Simulation (BAS) product that:

- **Identifies gaps in your security posture** through on-demand testing of your existing security infrastructure and controls

- **Validates the efficacy of your controls** through simulated attacks

- **Provides vendor-specific mitigation and actionable remediation recommendations** that are highly focused, saving remediation time

- **Gives industry and geographical context**, improving alert relevance and decreasing alert noise

- **Tracks security posture changes over time with scheduled or on-demand testing** of infrastructure changes, network issues, and configuration drift, enabling a consistent security posture

- **Tests security controls** against thousands of real-world threats, including malware, ransomware, vulnerability exploits, APTs, and more with the Picus Threat Library

- **Integrates with top SIEMs and EDRs,** targeting whether alerts and vulnerabilities are detected and logged

- **Maps simulation results against The MITRE ATT&CK® Framework**, to quickly identify gaps and prioritize threat mitigations that pose the greatest risk to your organization

Product Highlights:

✔ **Save time and focus on what matters**
Prioritize high-risk vulnerabilities and misconfigurations while demoting low-risk gaps

✔ **Identify context-based gaps and get actionable mitigation recommendations**
Simulate real-world cyber threats

✔ **Optimize SecOps**
Let your SecOps teams work on what matters

✔ **Maximize your security stack's effectiveness**
Measure the efficacy and scalability of your existing cybersecurity investments

✔ **See if your security profile is improving over time**
Continuous, repeatable, and on-demand testing and validation for your security controls and ops

MITRE ATT&CK® Mapping

Visualize the threat coverage provided by your security controls against the MITRE ATT&CK® framework to build a more resilient security posture.

Picus maps to the framework providing up-to-date data on Privileged Access, Persistence, Execution, Initial Access and more.
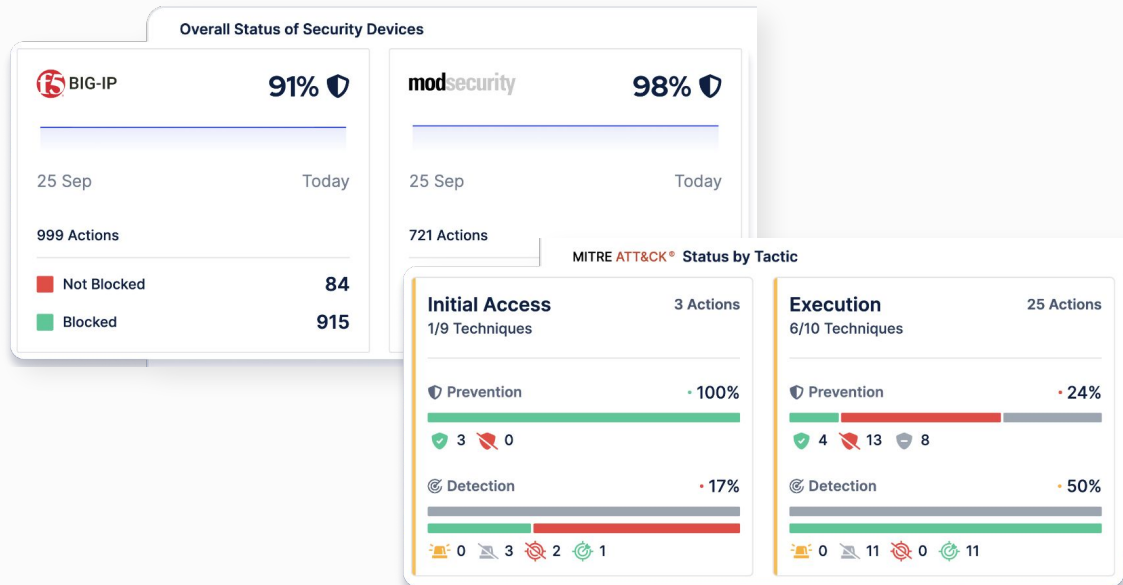
Why Picus SCV

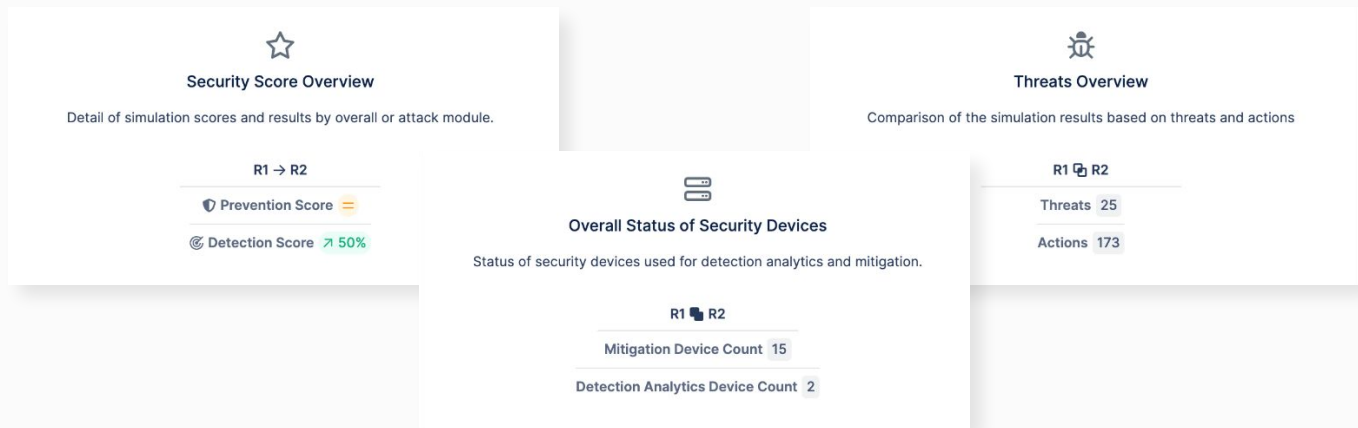### Superior Security Control Validation

A constantly evolving threat landscape requires on-demand control validation so that you know if, and how, your cyber risk profile is changing. You need to be able to take immediate steps to mitigate threats by remediation or validation of compensating controls. With Picus Security Control Validation you get:

- BAS technology that emulates and simulates over 100+ lateral movement techniques

- Vendor-specific and category mitigation insights that save remediation time

- Reporting that easily tracks infrastructure drift and configuration changes

- An extensive threat library with daily updates and mapped findings; currently over 25,000 TTPs and 5,700 threats

- Simulation templates which offer the flexibility to easily introduce new threats, or customize scenarios for specific compliance or industry requirements.

- Prevention and detection tool validation available on a continuous, scheduled, or on-demand basis

- All simulation results automatically mapped to MITRE ATT&CK® framework

- An industry-leading tool that's as powerful as it's easy to deploy, use, and manage
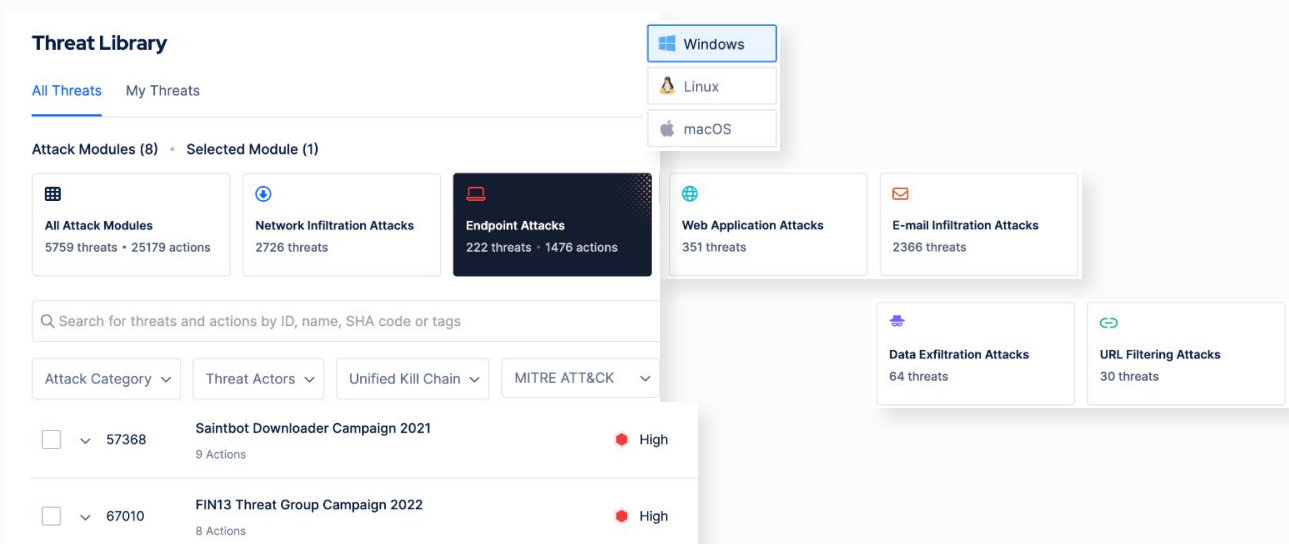
Test the Effectiveness of Security Controls Over Time

By running comparisons over time of your security score, status of security devices, and threats, organizations are able to track critical changes affecting security posture.

Security Score Overview
Detail of simulation scores and results by overall or attack module.

R1 → R2

🛡 Prevention Score =

☯ Detection Score ↗ 50%

Overall Status of Security Devices
Status of security devices used for detection analytics and mitigation.

R1 🔁 R2

Mitigation Device Count 15

Detection Analytics Device Count 2

Threats Overview
Comparison of the simulation results based on threats and actions

R1 🔁 R2

Threats 25

Actions 173

Picus Premium Threat Library

Test your security controls against thousands of real-world threats, including malware, ransomware, vulnerability exploits, APTs, and more.

Threat Library

All Threats   My Threats

⊞ Windows
△ Linux
 macOS

Attack Modules (8) · Selected Module (1)

| ⊞ All Attack Modules 5759 threats · 25179 actions | ⊕ Network Infiltration Attacks 2726 threats | 🖥 Endpoint Attacks 222 threats · 1476 actions | 🌐 Web Application Attacks 351 threats | ✉ E-mail Infiltration Attacks 2366 threats |

Data Exfiltration Attacks
64 threats

URL Filtering Attacks
30 threats

🔍 Search for threats and actions by ID, name, SHA code or tags

Attack Category ∨   Threat Actors ∨   Unified Kill Chain ∨   MITRE ATT&CK ∨

☐ ∨ 57368   Saintbot Downloader Campaign 2021
9 Actions   🔴 High

☐ ∨ 67010   FIN13 Threat Group Campaign 2022
8 Actions   🔴 High

Level Up Your Detection and Validation Capabilities

SCV helps propel you past the limits of vulnerability scanning, pen testing and red teaming. While these are critical components of a holistic cybersecurity program, they are insufficient on their own due to the following limitations:

- **Vulnerability scanning:**
  - Lacks the context to prioritize vulnerabilities based on risk scoring.
  - Lengthy remediation time with approximately 25 days to publish exploits and 60 days to remediate.
  - CVSS and EPSS scoring does not consider intelligence from other toolsets, context from critical business units, or exploitability.

- **Penetration Testing:**
  - Moment-in-time assessments which are not relevant 90 days after assessment.
  - Narrow in scope, leaving a large portion of the security ecosystem untested.
  - Dependent on the expertise of the team or consultant conducting the testing.

- **Red Teaming**
  - Objectives are limited by the scope of the project, Red Teams test only specific network segments or endpoints
  - Red Team tests are expensive and are not conducted that often. The results provide a snapshot of your cybersecurity just for a specific point in time
  - Inconsistencies in ethical hacker techniques can make results difficult to compare

How We Solve the Problem

Unmatched Breach and Attack Simulation

Picus SCV has the added benefit of our proven threat simulations and premium threat library, powered by award-winning Breach and Attack Simulation (BAS) technology, the cornerstone of the Picus Security Validation Platform. SCV measures and strengthens your cyber resilience by continuously testing the effectiveness of your security controls. SCV simulates the full attack cycle including insider threats, lateral movement, and data exfiltration with:

- **Superior Content**
  Picus provides the building blocks to create and execute simulations tailored to your business using our extensive, daily-updated threat library, threat templates, threat intelligence, and threat builder feature.

- **Actionable Learnings / Insights to Mitigations**
  Easily take the next steps through vendor-specific mitigations, MITRE ATT&CK® mappings, and customizable reports.

- **Continuous Breach and Attack Simulations**
  Validate controls, discover gaps and take proactive measures through templates in a way that fits your team.

Comprehensive Integrations

Network Security	SIEM	EDR	XDR
CISCO	splunk>	Microsoft Defender for Endpoint	TREND MICRO
citrix	Microsoft Sentinel	CROWDSTRIKE	SentinelOne
paloalto NETWORKS	IBM Security QRadar	vmware Carbon Black	CORTEX XSOAR BY PALO ALTO NETWORKS

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

SCV Features:

✔ Operationalize the MITRE ATT&CK® framework providing threat coverage visualization to quickly identify gaps and prioritize high-risk threat mitigations

✔ Validate technologies focusing on Continuous Threat Exposure Management (CTEM)

✔ Customize threats and attack scenarios

✔ Compare security scores across geographies, industries, and against other members of our extensive global user community

✔ Supports cross-platform operating systems - Windows, MacOS, and Linux

Gartner Peer Insights Customers' Choice 2024

Highest Rated Vendor
4.8/5
★★★★⯪