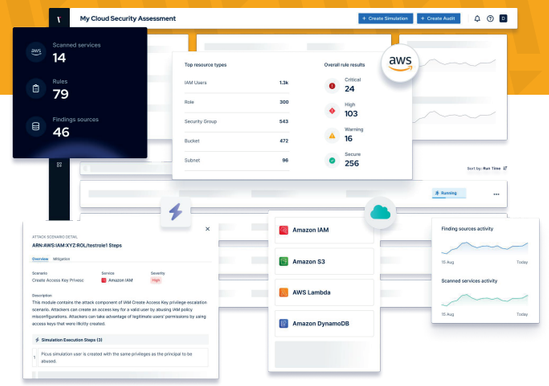
CLOUD SECURITY VALIDATION

Picus Cloud Security Validation (CSV) helps security teams alleviate cloud security posture management by identifying common misconfigurations that put assets at risk and by simulating real-world attacks to assess the effectiveness of controls and gauge the impact of breaches.



PICUS CLOUD SECURITY VALIDATION FOR AWS HELPS YOU TO QUICKLY IDENTIFY AND ADDRESS EXPOSURES PROACTIVELY BY

Auditing essential AWS services

Scanning fourteen core AWS services, Picus CSV identifies critical misconfigurations such as excessive privileges, exposed S3 buckets, unused resources, cryptographic failures, and more.

Simulating attacks in your environment

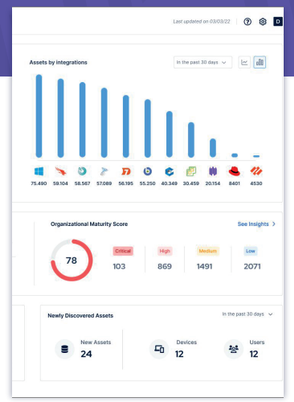
To validate the impact of any privilege escalation scenarios identified, Picus CSV provides the option to simulate attacks in your AWS environment. All actions are executed using newly created users and rolled back upon assessment completion.

Discovering privilege escalation scenarios

In the event attackers are able to access your AWS environment, they will likely attempt to access critical systems by escalating privileges. To identify overly permissive IAM policies, Picus CSV gathers AWS resources and simulates attacks in a Local Policy Simulator.

ATTACK SURFACE VALIDATION

Picus Attack Surface Validation (ASV) enhances visibility of users, hosts, systems and applications inside your network to help you improve security awareness and prioritize risks.



BY AGGREGATING ASSET DATA FROM MULTIPLE SOURCES AND PRESENTING IT FOR ANALYSIS VIA A SINGLE PANE OF GLASS, PICUS ASV PROVIDES THE INSIGHTS AND RICH CONTEXT YOU NEED TO

- **Obtain a more complete view of your asset inventory**
- **Identify policy gaps and misconfigurations**
- **Detect non-compliant devices with insufficient security coverage**
- **Prioritize vulnerability management based on asset importance**
- **Accelerate the analysis of security alerts**

CONTACT US FOR MORE INFORMATION ABOUT THE SOLUTIONS:

picus@bakotech.com || picussecurity.bakotech.com

PICUS | bako tech®

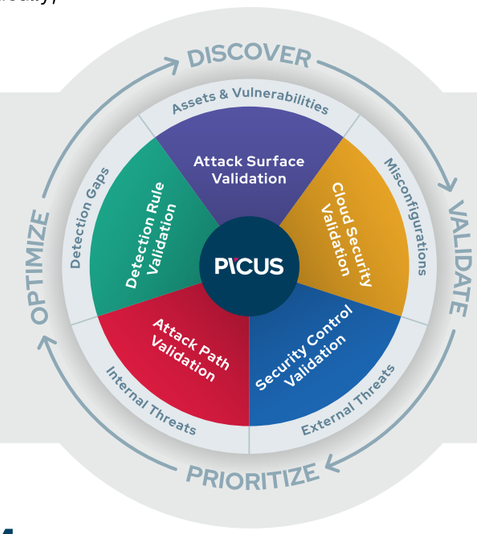
PICUS COMPLETE SECURITY VALIDATION PLATFORM

THE PICUS COMPLETE SECURITY CONTROL VALIDATION PLATFORM

is a Breach and Attack Simulation (BAS) solution that automatically, continuously and consistently validates, measures, and helps enhance cyber resilience 24/7.

MAIN FUNCTIONS:

- Measure and optimize the protection provided by existing security controls
- Discover and eliminate attack paths to critical systems and users
- Optimize detection and response capabilities to eliminate attacks sooner



HOW THE PICUS PLATFORM STRENGTHENS YOUR SECURITY POSTURE

Supplies a holistic and continuous view

Understand at any moment your organization's readiness to defend against the latest threats by validating security effectiveness in key areas.

Accelerates mitigation of security gaps

Get the insights you need to not only proactively identify security gaps but also address them before they are exploited by adversaries.

Automates manual validation processes

Address security risks earlier by automating manual assessment processes and by empowering your team to focus on remediation rather than discovery.

Evidences threat readiness and ROI

Obtain the metrics and insights you need to make data-driven decisions, be threat-centric, and demonstrate assurance and value to business leaders and auditors.

The Picus Complete Security Validation Platform provides the capability you need to assess your organization's security posture automatically, continuously and consistently.

Integrating three individually licensable products — Security Control Validation, Attack Path Validation, and Detection Rule Validation — enables you to proactively discover unknown risks, validate the effectiveness of controls and processes, prioritize gaps and optimize your defense, 24/7.

SECURITY CONTROL VALIDATION

Simulate real-world cyber threats to identify prevention and detection gaps and obtain actionable mitigation recommendations to address them swiftly and effectively.

HOW SECURITY CONTROL VALIDATION IMPROVES YOUR SECURITY POSTURE

Tests security controls continuously, 24/7

Picus identifies threat prevention and detection weaknesses by assessing the effectiveness of your security tools via continuously scheduled simulations.

Validates preparedness against the latest threats

With a rich threat library, updated daily by offensive security experts, Picus tests your defense against current and emerging attack techniques.

Optimizes prevention and detection capabilities

To achieve optimal protection from your security tools, Picus supplies easy-to-apply prevention signatures and 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.

Evidences the value of investments

Supplying real-time metrics, including an overall security score for your organization, Picus helps you to measure performance and prove value.

Improves SOC efficiency and effectiveness

Picus automates manual assessment and engineering processes to reduce fatigue and help your security teams work together more collaboratively.

ATTACK PATH VALIDATION

Picus Attack Path Validation (APV) enables security teams to automatically discover and visualize the steps an evasive attacker with initial access to an on-premises network could take to compromise critical systems and users. Simulating real-world adversary actions, this tool uncovers attack paths that pose the greatest risk and provides insights to remediate them.

Powered by Picus' Intelligent Adversary Decision Engine, this easy-to-use tool simulates real-world adversary actions to identify the shortest attack paths and validate that they pose a genuine risk.

HOW ATTACK PATH VALIDATION STRENGTHS YOUR INTERNAL NETWORK SECURITY

Reveals and validates paths to critical assets

Picus APV identifies the shortest route attackers could take to compromise your Active Directory and simulates real-world adversary actions to validate that they are actual paths that can be exploited not ones that exist theoretically.

Supplies a holistic view of your internal attack surface

Unlike manual red teaming exercises, which are conducted from a single initial access point, Picus APV provides a broader perspective by enabling you to run simulations from multiple areas of your network and obtain results in minutes, not weeks.

Helps prioritize vulnerabilities and misconfigurations

Identify entities on your network where multiple attack paths converge and prioritize mitigating vulnerabilities and misconfigurations at these choke points to ensure you achieve the best security impact.

Hardens Active Directory security

Mitigate weaknesses that could enable an attacker to obtain Domain Admin privileges and gain control of all users, systems and data in your environment.

Automates manual red teaming

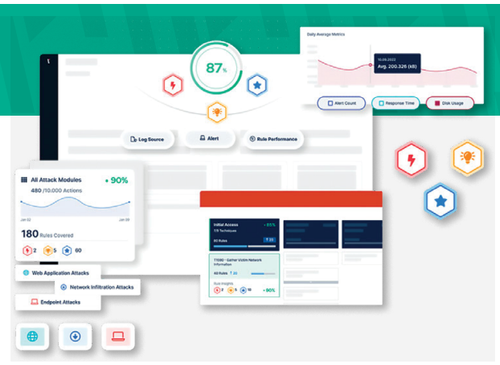
Save time and money by automating offensive security testing and ensure that when you do commission manual engagements, they deliver better outcomes and value.

Test security control effectiveness

Use Picus AP to gauge whether your organization's endpoint security is configured to detect and prevent lateral movement and other evasive techniques used by adversaries.

DETECTION RULE VALIDATION

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 the 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 SIEM and EDR detection rules and enable SOC teams to perform proactive rule validation.

Optimize threat detection and response

Get a 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