

DATASHEET







SECURITY CONTROL VALIDATION ATTACK MODULES OVERVIEW

By choosing **Picus Security Control Validation**, get the functionality you need to validate your organization's security controls against the latest threats.

Individually licensable attack modules integrate together seamlessly to provide the end-to-end capability required to simulate threats, validate effectiveness, and mitigate gaps - safely, simply and continuously.

COMPREHENSIVELY ASSESS YOUR DEFENSES BY SIMULATING THREATS ACROSS THE CYBER ATTACK LIFECYCLE

With Picus SCV, test your security controls against an ever-expanding library of **3,800+ threats** and **19,000+ actions***

ATTACK PHASES	ATTACK MODULES	Choose this module to...	Example attacks and techniques simulated
INFILTRATION	 Network Infiltration	validate that malware and ransomware downloaded via client-side attacks is prevented/detected by network and/or endpoint security controls.	- Malicious Code Execution - Untrusted Macro Execution
	 Email	validate that malicious email attachments and links are prevented/detected by email security controls.	- Remote Code Execution (RCE) - Information Leak
	 Web Application	validate that malicious web app requests are prevented/detected by network and/or detection controls.	- SQL Injection - Cross-site Scripting (XSS) - RCE - Deserialization
EXPLOITATION	 Endpoint	validate that scenario attacks from threat groups are prevented and/or detected by endpoint security controls.	- Privilege Escalation - Persistence (XSS) - Local Code Execution
	 Cloud	validate that cloud specific threats to identify potential risks, ensuring a secure cloud environment	- Open Public Access Bucket - The Meta Data - AWS EC2 User Data Modification
EXFILTRATION	 Data Exfiltration	validate that exfiltration of data (such as personal and financial information) is prevented/detected by network and/or	- Over HTTP - Over HTTPS - Over TCP

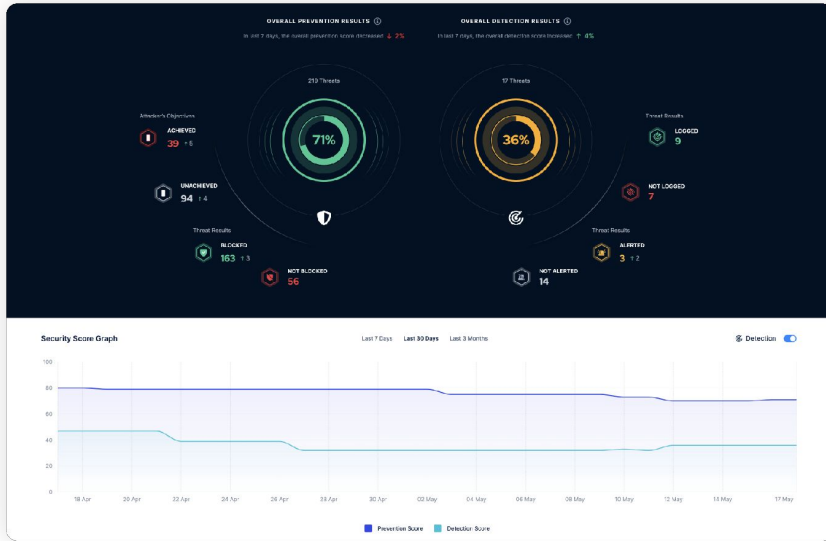
*Each threat consists of one or multiple actions. An action corresponds to a specific procedure required for a threat to achieve an objective.

COMPLETE SECURITY VALIDATION VIA A SINGLE UNIFIED PLATFORM

Whatever your security control validation needs, Picus Security Control Validation provides the functionality and flexibility you require.

Individually licensable attack modules enable you to create a custom solution aligned to the types of threats you want to simulate and the controls you have in place.

Picus SCV intuitive user interface and single pane of glass view makes it easy to schedule simulations, view assessment results, and obtain recommendations to mitigate prevention and detection gaps.



Schedule assessments and view results via a single pane of glass

TAILORED TO YOUR VALIDATION NEEDS^

Choose Picus Security Control Validation Attack Modules you require based on the security controls they support.

Attack Modules	Prevention Validation	Controls / Cloud Provider Supported	Detection Validation	Controls Supported
Network Infiltration	✓	NGFW, IPS, SWG, NS	✓	SIEM, NIDS
Email	✓	NGFW, SEG, ES, ESR, URL	Please inquire	SIEM, NIDS
Web Application	✓	NGFW, IPS, WAF, NS	✓	SIEM, NIDS
Endpoint	✓	AV, EPP, HIPS	✓	SIEM, NIDS, EDR
Data Exfiltration	✓	DLP	Please inquire	SIEM
Cloud	✓	AWS	Please inquire	AWS

KEY

- Firewalls and Next-Gen Firewalls (NGFW)
- Web Application firewalls (WAF)
- Intrusion Prevention Systems (IPS)
- Data Loss Prevention (DLP)
- Secure Web Gateways (SWG)
- Secure Email Gateway (SEG)
- Endpoint Protection Platforms (EPP)
- Antivirus (AV)
- Email Sandbox (ES)
- Network Sandbox (NS)
- Email Server (ESR)
- URL Isolation (URL)
- Endpoint Detection and Response (EDR)
- Network intrusion Detection System (NIDS)
- Host-based Intrusion Prevention System (HIPS)
- Security Incident and Event Management (SIEM)

Notes

- Attack modules for prevention and detection are licensed separately.
- Attack modules for prevention controls include generic mitigation insights as standard. Vendor-specific mitigation recommendations require an additional license per technology.
- Vendor-specific mitigation insights for detection controls are available for attacks included as part of Picus SCV's Endpoint Attack Module.



Latest Threat Library Updates Included

To keep your security controls optimized, all Picus Attack modules include access to the latest threats as soon as they are added to the Picus Threat Library*

*Threats available to simulate are dependent upon the Picus Attack Modules licensed.

Test Your Defenses Against the Latest Threats



START FREE TRIAL



4.9 / 5*

*average score at time of press in January 2023

www.picussecurity.com

