# PICUS

## SECURITY CONTROL VALIDATION & MITIGATION

#### Threat-centric, pervasive, flexible end-to-end security validation

Today's security leaders face a herculean task: maintaining a hard baseline against ever evolving cyber threats, while balancing requirements and investment. Modern cyber security stacks are often complex, but hardly gap-free. While security analysts try to weather a storm of threat intelligence coming from multiple sources, skills and resources are required to turn huge amounts of data into concrete tactics to validate security effectiveness. The foundation of readiness is frequent testing and validation. With all these tools and responsibilities, how often do you ask yourself "am I secure?"

Picus Security Control Validation and Mitigation is a threat centric, flexible platform that allows to measure security effectiveness and quickly assess controls, automatically and consistently identify gaps, and instantly apply selected mitigation advice for the purpose of security validation, hardening and mitigation. The platform is powered by an extensive Threat Library curated by Picus Labs, and a broad set of mitigation advice coming from the Picus Technology Alliance Network.





### THREAT EMULATION BASED ON THE MOST EXTENSIVE THREAT LIBRARY

By undertaking global threat watch, imminent threat analysis and commonality evaluation processes, Picus Labs maintains a proprietary Threat Library around the clock and provides thousands of curated, indicative realworld threat samples and scenarios. All content is tied to MITRE ATT&CK with over 90% coverage.



#### FAST DEPLOYMENT, EASY MANAGEMENT

The Picus Platform engine assesses the readiness level of network, web application, endpoint and email security controls in production networks, either while operating 24×7 or on-demand when required. Picus is categorically safe, technology agnostic, requires limited deployment effort and fully automated.

#### HIGHLIGHTS

#### Maximise ROI

Utilise your security investments at their maximum. Manage your security estate effectively.

#### Automated and consistent validation

Streamline the validation process through automatic, continuous and pervasive security testing.

### • Elevate the quality of the visibility insight

Monitor your security posture through consistent and continuous validation.

#### Speed up mitigation and change management

Automate and speed up security policy and signature management.

#### • Empower your teams with threatcentric validation

Leverage on the Picus Threat Library and benefit from constant vigilance and awareness of the global threat landscape for timely and precise operations.



#### VENDOR-SPECIFIC MITIGATION FOR PRECISION AND SPEED

Picus Mitigation Library carries technology-specific security policy insights. Laser-focused mitigation advice from our Technology Alliance Ecosystem can be applied to alliance vendors for rapid remediation. Solutions include next-generation firewall, network intrusion prevention systems, and web application firewalls. The Picus Security Control Validation and Mitigation solution consists of Picus Threat Library, Threat Emulation Module, and Mitigation Library. While the Threat Emulation Module continually collects adversarial content from the Threat Library and runs assessments, the Mitigation Library reveals available signatures and policies developed by the vendors to address the identified security control gaps.

#### **PICUS THREAT LIBRARY**

Picus Threat Library contains thousands of daily-updated malware, vulnerability exploits, web application attack samples, and atomic adversarial techniques selected via commonality evaluation of global threat watch data. Hundreds of nation-state and vertical driven attack scenarios are included. Content is mapped to the frameworks of MITRE ATT&CK, Cyber Kill Chain, and OWASP and presented in relation to targeted applications, targeted operating systems, severity level as well as Common Vulnerabilities and Exposures/Common Weakness Enumeration (CVE/CWE) references. Through the Threat Library, users find samples of the most recent adversarial techniques at their fingertips, allowing them to stay ahead of newest threats, saving the hassle of setting up and maintaining an in-house repository. SOC analysts, threat hunters and incident responders, security operations teams, red team and pen-testers can utilize this granular content for various testing scenarios.

PICUS III								Salahin Pena Vi	1	
Harma	Total Threat Count	Threat Categories					Vectors			
Rttack Simulation 👻	9129 C Laster 7 100/00 400	۰	0	8	8		285	40		
Threat Summary	Last 7 Days	Maficious Code	Web Application Attecks	Vulnerability Exploitation	Attack Scenario	Data Exfitzation	Network	Endpoint	Enal	
Treat Library Mitpation	+9	6321 -•	1369	657	563	219	8566	6835	3089	
Detection v										
	APT Scenarios 46	Malicious Code	6321 +9	Vulnerability Exploitation 657						
	APTI APT Scenario (3) A	PT20 (2) Tark APT So	maria (2)	Categories	Court.	Categories		Count		
	Tick APT Scenario (2) Tr	*	~	APT Drive 1323		Code Execution 472				
	-			Traian 626		Memory Corruption 41				
	PickAxe APT Campaign (1)	DARIO HYDRUS APT Scill	erio 1	Banking Malware 437		Fully Confey 35				
	Patchwork APT Scenario (1	Silence (1) RTM A	PT Scenario 1	RAT	425	Information Disclosure 17				
Reports										
t Settings	Kill Chain Phase Delvery	Comprom	ine .		MITRE ATT&CK	fectiviques 12 Testics	203 Techniques +:	2		
© 2018 Pous Browly Balance						Privilege Escalation Defense I 23 Techniques +1 56 Techniq				
0.31.01.2021	-									

#### **PICUS MITIGATION LIBRARY**

While Picus Labs' Red Team adds new adversarial content to the Threat Library, the Blue Team examines the solution inventory of Picus' technology partners to enrich each threat and technique sample with mitigation alternatives. New threats and associated mitigation alternatives are added daily.

Picus Mitigation Library provides vendor-specific policy insights for the following categories: network security controls, next-generation firewall, network intrusion prevention systems, web application firewalls, Endpoint Detection & Response (EDR) solutions, SIEM platforms.



#### **PICUS THREAT EMULATION MODULE**

Picus Threat Emulation Module is the pivotal piece of the Picus Platform, bridging your defensive capabilities with the largest adversarial library available and with the Mitigation Library for eliminating risks quickly.

The Threat Emulation Module assesses the "readiness level" of network, web application, endpoint, and email security controls in production networks, either while operating 24×7 or on-demand for red team practices. The emulation module can be configured over multiple attack vectors simultaneously and can process thousands of adversarial scenarios from the Picus Threat Library across your whole defensive estate, cloud based or on-premise, in a matter of hours.

Picus assessments are categorically safe, technology agnostic, and require limited deployment effort. Emulated attacks are run between agent peers. Each Picus peer has the capability of taking the attacker or victim side of the emulation based on the scenario, significantly simplifying the deployment requirements. The validation output collected by Picus is presented in real time and in retrospect, distilled as security scoring and threat-based checks (blocked vs unblocked threats) and drives prevention advice and mitigation actions.

Picus Threat Emulation Module has an easy to use and functional user interface.



#### **KEY USABILITY FEATURES**

- Executive level reporting.
- Advanced notification features on sudden success rate drop situations.
- Easy navigation among different attacks vectors.
- Advanced historical and vector-based comparisons.
- Enriched threat or technique information visibility containing CVE, CWE, OWASP, cyber-kill chain, MITRE ATT&CK references, hash information, targeted operating systems, targeted applications and others.

						Vecto							
						vecto	ors						
	•••					All (3)	%49	an Netwo	rk (1)	티	indpoint (1)		🛎 Email (1)
	Overview Analysis of ATTRCK Framework ×					0.0	- d F	Internal P			N. Dever	10	
						Cloud-Em → Internal-E ● LA				LAN-Peer → Win10			
	LAN-Peer - Winto					Security Score Blocked Not Blocked Secu					curity Score Blocked Not Blocked		
	Hiller Access	Departies	Persistance	Privilege	Defense Everen	52		1.6k	1.5k		2%	5.6k	1.2k
	T1078 T1028		T1004	T1013	T1006	Analysis > Analysis >							
	Valid Accounts	Windows Bornete	Winlogan Helper DLL	Port Monitors	File System Logical Offsets	Dumping	Service Discovery	Deployment Software	Local System	Compressed	Obfuscation	Destruction	
Comparison  Vector Comparison Vector 1			T1013 Port Monitors	T1015 Accessibility Features	T1009 Binary Padding	T1040 Network Sniffing	T1010 Application Window	T1021 Remote Services	T1025 Data from Removable	T1011 Exfittation Over Other Notwork	T1008 Fellback Channels	T1486 Data Encrypted for impact	
		T1015 Accessibility Features	T1034 Path Interception	T1014 Rootkit	T1066 Input Cepture	Discovery T1012	T1028 Windows	Media T1039	Medium T1020	T1024 Custom Cryptographic	T1488 Disk		
Select a vector to compare	re	~	T1019	T1038	T1027	Capture T1068	Guery Registry	Nindows Remote Management	Data from Network	Automated Exfittration	Protocol	Content Wipe	
Vector 2			System Firmware	OLL Search Order Hijacking	Obfuscated Files or Information	Exploitation for Privilege Excelation	T1016 System	T1037 Logan	Shared Drive	T1022 Data	T1026 Multiband Communication	T1489	
Select a vector to compar	re .	Ŭ.	T1023 Shortcut Modification	T1044	T1036	T1081	Natwork Configuration Discovery T1018 Remote System Discovery Discovery	Scripts	Th056 End Input Capture T10 Sch Th074 Tha Staged T10 T1113 Tha	Encrypted	T1032	Stop T1490	
	Compa					T1091 Replication Through Removable				T1029 Scheduled Thatsfer	Standard Cryptographic Protocol		
		T1061	Modify Existing Service	T1050 New						T1030 Data	T1043 Commonly Used Port		
		Graphical User	face Path Interception	Service						Data Transfer Size Limita		Defacement	
		Interface		TI So ••									
		1.004											Be to Attack Simulati
						3804 4		e	748 BLOCKED	3 🕈 3827		9 132 NOT BLO	
				s 100	lecurity Score Chan	0×							Last 1 M
				50		_	_						
					Jun								'n

#### **USE CASES**



#### FOR SECURITY LEADERS

- Build cross-departmental defense capabilities through clear-cut cyber-attack readiness visibility.
- Manage cyber-security function based on attack readiness based metrics and KPIs.
- Help answer questions on the readiness status about the threats covered publicly.
- Support budget discussion with evidence on limitations and explain cybersecurity risk in the business context.
- Demonstrate the value delivered by cybersecurity operations against a stream of adversarial activities.
- Empower cyber-security teams by giving them the toolset for uncovering new configuration requirements against the changing adversarial landscape instantly.
- Reveal systemic shortcomings such as poor service quality, network flaws, new employee onboarding shortcomings, aged technologies, and others.

# O FOR SOC MANAGERS

- Gain granular and technology-related visibility on security control gaps.
- Empower threat hunters and incident responders by providing real threat samples and specific validation capacity.



- Build, sustain, and harden the security baseline across the security controls such as next-generation firewall, intrusion prevention systems, web application firewalls, email gateways, and endpoint controls.
- Respond to emerging threats quicker and speed up change management during mitigation operations.
- Run quicker and easier proof of concept processes.



- Automate the test process using the readily available threat samples and attacker and victim attributes.
- Apply larger number of test scenarios in a given time frame.
- Gain flexibility in delivering continuous and on-demand assessments.

#### REQUIREMENTS

#### **Picus Manager**

VMware ESX/i 5.1 or later. Hyper-V Server 2008 and later. Physical Servers: Any hardware supporting CentOS 7 x64 (minimal installation).

#### **Picus Network and Email Peer**

VMware ESX/i 5.1 or later. Hyper-V Server 2008 and later. Physical Servers: Any hardware supporting CentOS 7 x64 (minimal installation).

#### **Picus Endpoint Peer**

Supports Windows 7 SP1, Windows 8.1, Windows 10, Windows Server 2012 R2 and Windows Server 2016 with .NET Framework 4.5.2 or above.



#### **DEPLOYMENT COMPONENTS**

**Picus Manager** – provides an easy-to-use web user interface from which Picus assessments and reports are managed.

**Picus Network and Email Peer** – A vector defines the network path followed by an attack. Any vector terminates in two peers (an attacker and a victim). A network peer can be selected either as a victim or attacker peer.

**Picus Endpoint Peer** – Simulation peer to test endpoint security. It can only be configured as a victim peer.

**Picus Integration Peer** – provides integration with security solutions/systems in the customer environment for Picus Security modules.

#### **DEPLOYMENT OPTIONS**

**Picus Manager** - Available as HyperV and VMware virtual images or also available on physical/virtual servers which support CentOS 7 x64.

**Picus Network and Email Peer** – Available as HyperV and VMware virtual images. It is also possible to install Picus Peers on physical servers and PCs which support CentOS 7 x64.

**Picus Endpoint Peer** – Runs on Microsoft Windows. Picus does not distribute any Endpoint Peer image. It is expected that Endpoint Peer is to be installed on an instance of the organization's Windows golden image.

**Picus Integration Peer** – Available as HyperV and VMware virtual images. It is also possible to install Picus Peers to physical servers and PCs which support CentOS 7 x64.

### PICUS

#### 302.001.V2 EN

**About Picus** 

Picus Security is a breach and attack simulation (BAS) vendor. BAS was categorized as a new security assessment domain in 2018 by Gartner, and Picus has been named as a Cool Vendor in 2019. Picus is an intelligence-driven security validation platform that simplifies security operations and optimizes defenses. The platform safely emulates cyber threats and provides mitigation guidance - allowing organizations to improve visibility and security investment utilization.