PICUS THE COMPLETE SECURITY VALIDATION PLATFORM

DATASHEET

ATTACK PATH VALIDATION

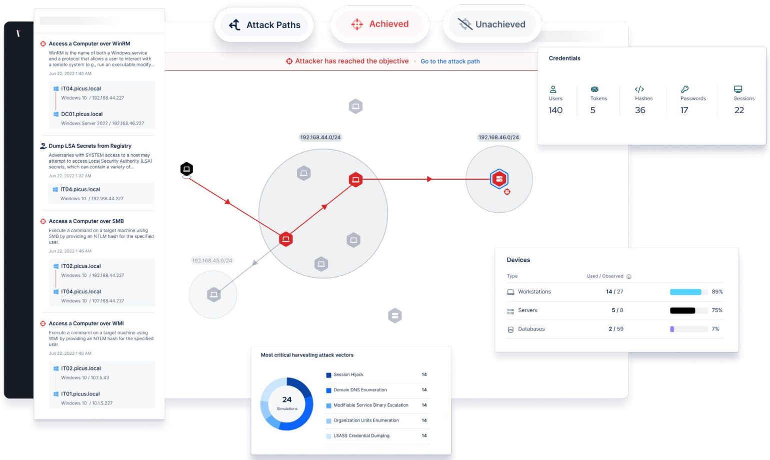
STOP ADVERSARIES IN THEIR TRACKS BY ELIMINATING ROUTES TO CRITICAL USERS AND ASSETS

With cyber security breaches now an operational reality, it's essential to plan for the worst. Key to an assumed breach mindset is understanding how, having achieved initial access to your network, sophisticated adversaries could accomplish their objectives by exploiting previously undiscovered vulnerabilities and misconfigurations.

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.

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.

Discover the shortest paths to your Windows Active Directory



Access a Computer over WinRM

WinRM is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable,modify...

Jun 22, 2022 1:46 AM

IT04.picus.local
Windows 10 / 192.168.44.227

DC01.picus.local
Windows Server 2022 / 192.168.46.227

Dump LSA Secrets from Registry

Adversaries with SYSTEM access to a host may attempt to access Local Security Authority (LSA) secrets, which can contain a variety of...

Jun 22, 2022 1:32 AM

IT04.picus.local
Windows 10 / 192.168.44.227

Access a Computer over SMB

Execute a command on a target machine using SMB by providing an NTLM hash for the specified user.

Jun 22, 2022 1:46 AM

IT02.picus.local
Windows 10 / 192.168.44.227

IT04.picus.local
Windows 10 / 192.168.44.227

Access a Computer over WMI

Execute a command on a target machine using WMI by providing an NTLM hash for the specified user.

Jun 22, 2022 1:46 AM

IT02.picus.local
Windows 10 / 10.1.5.43

IT01.picus.local
Windows 10 / 10.1.5.227

Attacker has reached the objective • Go to the attack path

Credentials

Users	Tokens	Hashes	Passwords	Sessions
140	5	36	17	22

Devices

Type	Used / Observed	
Workstations	14 / 27	89%
Servers	5 / 8	75%
Databases	2 / 59	7%

Most critical harvesting attack vectors

24 Simulations

Session Hijack	14
Domain DNS Enumeration	14
Modifiable Service Binary Escalation	14
Organization Units Enumeration	14
LSASS Credential Dumping	14

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 AD 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.

WHAT IS AN ATTACK PATH?

An attack path is a visualization of a route an attacker, that has breached an organization's network, could take to achieve an objective. Most organizations have thousands of potential attack paths which continue to grow and, if left unmanaged, could make it easy for cybercriminals to compromise critical assets.

Common exposures that attackers can exploit once inside a network include misconfigurations, excessive user privileges, weak passwords, inadequate access controls and network segmentation, and unpatched vulnerabilities.

HOW DOES PICUS HELP MANAGE ATTACK PATHS?

Picus Attack Path Validation strengthens internal network security by discovering and helping to disrupt the paths that, left unseen and unmanaged, could enable attackers to compromise a Windows Domain Administrator.

Unlike other solutions, Picus APV doesn't overwhelm security teams by revealing thousands of theoretical paths that are challenging to prioritize. Instead, it simulates the actions of an internal attacker to discover the shortest path and to validate that it poses a genuine risk.

Active Directory Security is a critical issue for security teams since compromising a domain admin account could enable attackers to access an organization's systems and data, impersonate users and achieve deep persistence.

PICUS' INTELLIGENT ADVERSARY DECISION ENGINE

Central to Picus APV is the product's **Intelligent Adversary Decision Engine**. By conducting discovery and enumeration in your environment, it determines how to complete an objective in the most efficient and evasive way possible.

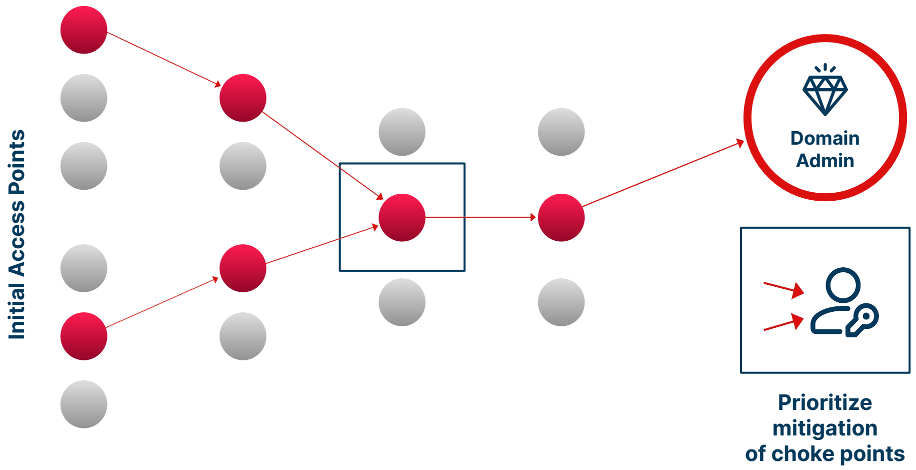
Real-world actions that can be simulated by Picus APV include:

- ✓ **Credential harvesting**
- ✓ **Password cracking**
- ✓ **Data Gathering**
- ✓ **Lateral movement**
- ✓ **Pivoting**
- ✓ **Privilege escalation**
- ✓ **Masquerading**
- ✓ **Relay**
- ✓ **Vulnerability exploitation**
- ✓ **Kerberoasting**

FOCUS REMEDIATION IN THE RIGHT AREAS

To provide a more holistic view than manual red team exercises, Picus APV makes it quick and easy to conduct assessments from multiple initial access points.

Compare the results of assessments to identify 'choke points' - the entities where multiple paths converge - and prioritize mitigating vulnerabilities and misconfigurations at these points to maximize security impact.



KEY FEATURES

✓ **Automated attack path mapping**
Visualize high-risk attack paths and take swift action to remediate them.

✓ **Intelligent Adversary Decision Engine**
Get a realistic view by testing your security against evasive adversary actions.

✓ **A library of real-life attack actions**
Discover and validate paths using the latest attack techniques curated by Picus Labs.

✓ **Customizable assessment options** Tailor simulations to your requirements by defining the scope and actions that can be leveraged.

✓ **Fully agentless deployment**
Run PowerShell script or an executable file on an Initial Access Point to start a simulation.

Gartner peerinsights™
4.9 / 5*

*average score at time of press in January 2023

www.picussecurity.com

picussecurity