PICUS

ATTACK PATH VALIDATION

Better Together:
Automated Penetration Testing and Attack Path Mapping

Fix What Matters

With today's assumed breach mindset, security teams are looking to understand how sophisticated adversaries could accomplish their objectives by exploiting undiscovered vulnerabilities and misconfigurations once they are inside the network.

Automated penetration testing is an effective tool to identify exploitable exposures, but not all exposures carry the same level of risk to your organization. In order to save time and focus on what really matters, security teams must determine which vulnerabilities exposed through automated penetration testing are exploitable, and shortlist the attack paths that pose the most risk.

What Attack Path Validation Does

Picus combines automated penetration testing with attack path mapping capabilities to deliver Picus **Attack Path Validation (APV)**. APV provides the ability to use automated penetration testing across the network to uncover vulnerabilities and misconfigurations. Additionally, attack path mapping is used to discover, visualize and prioritize the most critical steps of an evasive adversary. APV can uncover exposures that lead to domain admin compromise, disruptive ransomware attacks, and more.
The pairing of automated penetration testing and attack path mapping capabilities enables customers to easily discover and mitigate:

- Exploitation of vulnerabilities
- Exposures leading lateral movement
- Privilege escalation
- Exfiltration of data
- Ransomware threats

Central to APV is the Picus Intelligent Adversary Decision Engine. Based on the results of network discovery and enumeration, it determines which attack paths attackers are likely to take to achieve their objectives, such as ransomware attacks or obtaining admin privileges.

Adversary actions simulated by APV include:

- Asset and Service Discovery
- Vulnerability Assessment
- Credential Harvesting & Brute Forcing
- Privilege Escalation
- Password Cracking
- Data Exfiltration
- Lateral Movement
- Kerberoasting

In order to prioritize remediation, Picus APV identifies where multiple attack paths converge and prioritizes mitigating exposures at these high-traffic choke points to maximize impact.

Product Highlights:

✓ **Identifies high-impact exposures**
With a unique combination of asset discovery, attack path mapping and automated penetration testing capabilities, customers save time and gain accuracy

✓ **Emulates Active Directory exploitations**
Mimics attackers exploiting Active Directory to gain control of users, systems and data

✓ **Timely vulnerability assessments**
Enables penetration tests to be scheduled and initiated from any point within the network resulting in directed and timely vulnerability assessments

✓ **Reduces ransomware attack risk**
Determines which files an attacker can locate and exfiltrate

✓ **Maps lateral movement paths**
Attackers spend 80% of their time on lateral movement to exfiltrate data

✓ **Reveals credential and data loss risks**
Attempts domain admin account takeovers by leveraging exposures leading credential and data loss

✓ **Risk free**
Picus prioritizes operational stability, minimizing the risk of unintended disruptions

Why Picus APV

The combination of attack path mapping and automated penetration testing saves security teams time, pinpoints what is exploitable, and prioritizes what needs to be fixed. Large enterprise organizations report that they often spend considerable bandwidth researching vulnerabilities that don't matter.

With Picus APV, customers can:

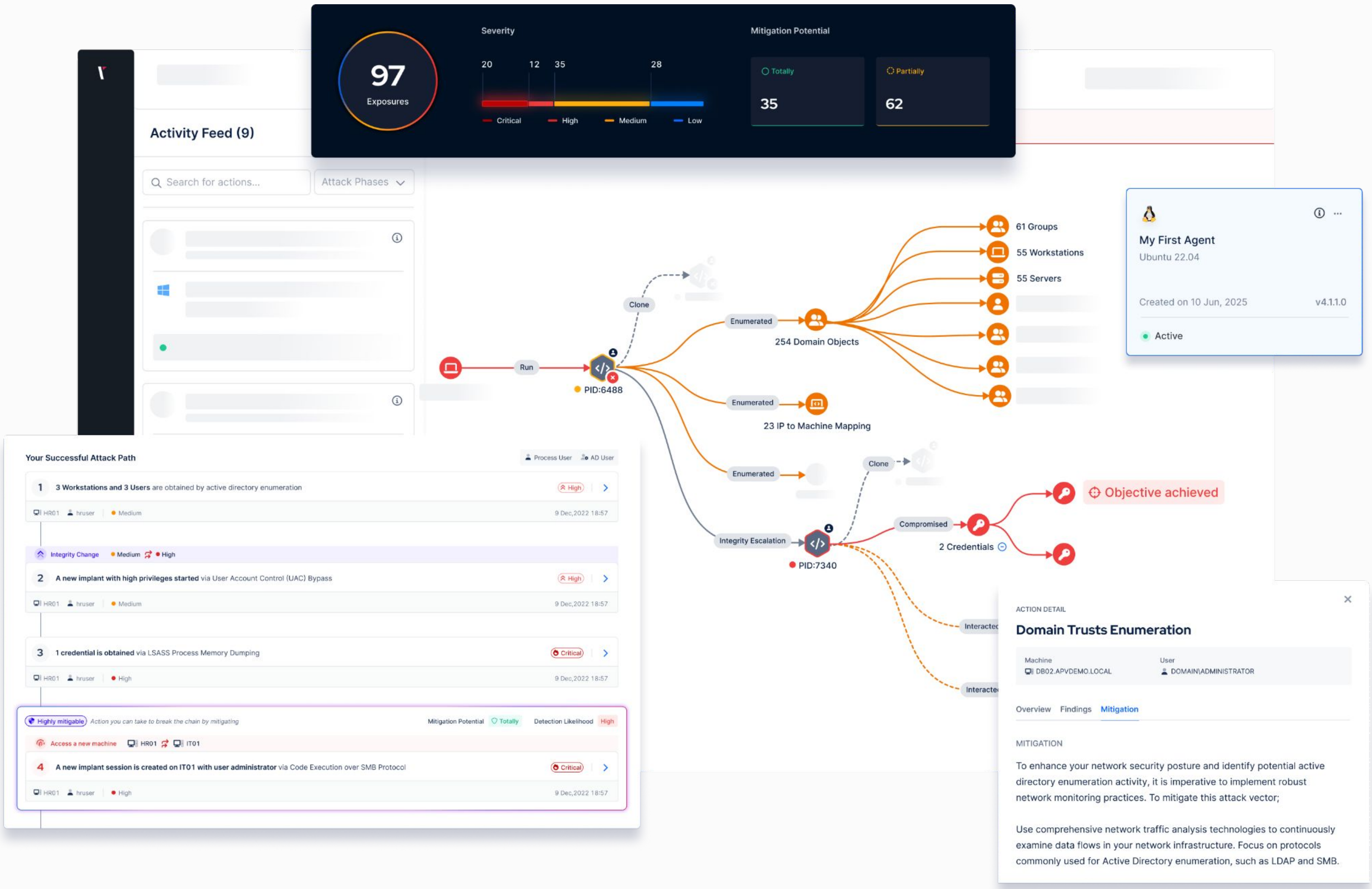
Uncover Exploitable Vulnerabilities
Gain complete visibility with asset discovery and identify exposures that traditional vulnerability assessment tools cannot provide

Prioritize Exposures
Benefit from context-aware prioritization of exposures based on user environments and attack paths together

Map Critical Attack Paths
Create prioritized exposure paths, highlighting the critical validated weaknesses that require immediate attention

Reduce Risk of Ransomware Attacks
Determine which files an attacker can locate and exfiltrate

Attack Path Validation with Asset Discovery and Credential Access



Your Successful Attack Path

Process User | AD User

1 **3 Workstations and 3 Users** are obtained by active directory enumeration — High
HR01 | hruser | Medium — 9 Dec,2022 18:57

Integrity Change | Medium | High

2 **A new implant with high privileges started** via User Account Control (UAC) Bypass — High
HR01 | hruser | Medium — 9 Dec,2022 18:57

3 **1 credential is obtained** via LSASS Process Memory Dumping — Critical
HR01 | hruser | High — 9 Dec,2022 18:57

Highly mitigable — *Action you can take to break the chain by mitigating* — Mitigation Potential: Totally — Detection Likelihood: High

Access a new machine | HR01 | IT01

4 **A new implant session is created on IT01 with user administrator** via Code Execution over SMB Protocol — Critical
HR01 | hruser | High — 9 Dec,2022 18:57

ACTION DETAIL

Domain Trusts Enumeration

Machine: DB02.APVDEMO.LOCAL
User: DOMAIN\ADMINISTRATOR

Overview | Findings | Mitigation

MITIGATION

To enhance your network security posture and identify potential active directory enumeration activity, it is imperative to implement robust network monitoring practices. To mitigate this attack vector;

Use comprehensive network traffic analysis technologies to continuously examine data flows in your network infrastructure. Focus on protocols commonly used for Active Directory enumeration, such as LDAP and SMB.

How We Solve the Problem

To provide a comprehensive approach, Picus Security Validation Platform offers an automated pentesting solution that also highlights attack paths that could enable attackers to achieve their objectives. Customers can now do network-wide automated pentesting and targeted attack path mapping which allows them to see and mitigate the high-risk exposures.

Picus provides mitigation recommendations and enables customers to find and focus on highest potential impact attack paths and determine which security controls need to be mitigated to close security gaps. Simple scheduling and the ability to run assessments in parallel provides a consistent approach. This allows teams to test continuously and keep up with their environment. Once configured and enabled, APV can run on auto-pilot and automatically initiate and execute simulations without requiring approvals for each exploit attempt.

Maps lateral movement paths

Identifies high-impact exposures

Discovers privilege escalation

Key Features

- **Identifies the shortest routes attackers could take:** Identifies the shortest exploitable routes for attackers to obtain domain admin privileges and encrypt sensitive data, leading to ransomware attacks
- **Picus Intelligent Adversary Decision Engine:** AI-powered engine that dynamically executes attack techniques based on the calculated value and impact of each attack path.
- **Automated asset and service discovery:** Automatically identifies and inventories assets and services to give full visibility into your attack surface.
- **Vulnerability assessment:** Scans for known vulnerabilities and misconfigurations and surfaces where they enable real attack paths.
- **Credential brute-forcing:** Tests credential-based attack vectors to expose weak authentication in Active Directory and remote access services like SSH, FTP, Telnet, and VNC.
- **Provides mitigation recommendations:** Suggests mitigations to address vulnerabilities and misconfigurations at 'choke points' to ensure you achieve the best security impact.
- **Leverages the Picus Threat Library**: Discovers attack paths by using the latest attack techniques, all mapped to the Unified Kill Chains.
- **Discovers Ransomware Risk:** Emulates ransomware behavior by determining which files an attacker can locate and exfiltrate.
- **Designed to run autonomously**: Users can schedule or initiate emulations on-demand, not requiring user intervention.
- **Agent-based and agentless deployment:** Flexible deployment modes allow agentless and agent-based assessments.

> **Picus Attack Path Validation** has been instrumental in elevating our proactive defense capabilities, particularly through its automated penetration testing features."

Andrea Licciardi
Sr. Cybersecurity Manager
MAIRE

Gartner, Voice of the Customer for Breach and Attack Simulation Tools, Peer Contributors, 30 January 2024

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.