PICUS

SECURITY VALIDATION WITH MITRE ATT&CK®

From ATT&CK to Action:
Operationalize MITRE ATT&CK® with The Picus Platform

Bringing ATT&CK Techniques to Life with Real-world Validation

The MITRE ATT&CK® matrix provides a well-structured framework for understanding adversary behaviors. However, to utilize it effectively, security teams need to analyze examples and procedures for each technique to develop a safe way to validate them.

The Picus Platform brings the ATT&CK guidelines to life by simulating real-world attack techniques, identifying your detection and prevention gaps, and delivering valuable insights you can use right away. With Picus, security teams can move beyond theory and guesswork to actively assess and improve their defense and organizational resilience against ever-evolving cyber threats.

How to Operationalize MITRE ATT&CK® with Picus

Picus simulates real-world cyberattacks that are mapped to the MITRE ATT&CK® framework. This helps organizations quickly move beyond theoretical threat modeling and actively validate their defenses against the actual tactics, techniques, and procedures (TTPs) that modern adversaries are using. Picus gives organizations deep visibility into their MITRE ATT&CK® coverage, allowing them to identify their gaps and measure their prevention and detection effectiveness, making sure they're ready for real-world threats.

By simulating a wide range of TTPs, Picus provides security teams with a granular and data-driven analysis of their security posture, featuring:

- TTP-based adversary emulation and attack simulation
- ATT&CK coverage of prevention and detection capabilities
- An interactive and customized MITRE ATT&CK® heat map
- AI-powered detection rule mapping to the ATT&CK framework

Instead of relying on assumptions or reactive responses, security teams can proactively test their defenses against a wide range of modern attacks. The Picus Platform can simulate all the tactics in the MITRE ATT&CK® Matrix, including:

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Picus also provides severity levels for each simulated technique or subtechnique and highlights which MITRE ATT&CK® techniques security teams should focus on.

Product Highlights:

✔ **Simulate MITRE ATT&CK® Techniques**
With our extensive threat library, Picus enables security teams to simulate MITRE ATT&CK techniques in just a few clicks.

✔ **Assess ATT&CK Coverage**
By continuously running attack simulations, Picus provides a clear and comprehensive view of MITRE ATT&CK coverage.

✔ **Unified MITRE ATT&CK® heat map**
Our customized heat map feature lets your teams visualize your ATT&CK coverage to demonstrate both the prevention and detection efficacy of your security controls.

✔ **AI-powered Detection Rule Mapping**
Effortlessly map your whole detection content to MITRE ATT&CK® techniques using our AI-driven analysis to accurately assess your detection coverage against ATT&CK.

✔ **Create custom threats with ATT&CK**
Modify existing threats or design entirely new ones by combining multiple ATT&CK techniques and procedures to create custom red teaming scenarios.

✔ **Real-world attacks, without the risk**
Picus prioritizes operational stability and business continuity, bringing peace of mind without risking unintended disruptions.

Why The Picus Platform?

Picus Labs has conducted extensive research based on the MITRE ATT&CK framework to ensure that security teams can test their defenses against the most relevant and most up-to-date adversary techniques. Our research powers the development of The Picus Threat Library, where threats are mapped to specific ATT&CK techniques. By leveraging this intelligence, organizations can validate their security controls against the exact methods used by real attackers, letting them proactively assess and enhance their real-world detection and prevention capabilities.

Picus also goes beyond attack simulation by helping security teams improve their ability to detect threats in their actual environments. For each threat, The Picus Mitigation Library provides corresponding actionable mitigation recommendations, ensuring that your security teams take immediate action to close your gaps.

Industry-leading Attack Simulations
Test your security controls against real-world adversary behaviors, ensuring that your defenses align with the latest attack trends.

Research-driven Threat Intelligence
Prioritize your defense efforts based on actual attack prevalence and recent threats rather than guessing at hypothetical risks.

Comprehensive ATT&CK Coverage
Get a clear and comprehensive view of your MITRE ATT&CK coverage and see how you stand against each MITRE ATT&CK technique.

Ready to Use ATT&CK-based Mitigation
Remediate identified security gaps right away using actual mitigation recommendations for both prevention and detection.

Picus Platform Products and Modules

	Picus Attack Surface Validation (ASV)	Picus Security Control Validation (SCV)						Picus Attack Path Validation (APV)	Picus Cloud Security Validation (CSV)
	Attack Surface Validation	Endpoint Attacks	Network Infiltration Attacks: Vulnerability Exploitation	Network Infiltration Attacks: Malware Download	Web Application Attacks	E-mail Infiltration Attacks (Phishing Attachment/Link)	Data Exfiltration Attacks	URL Filtering	Attack Path Validation	Cloud Security Validation
Reconnaissance	✔									
Resource Development	✔									
Initial Access		✔	✔	✔	✔	✔				
Execution		✔			✔				✔	✔
Persistence		✔			✔				✔	✔
Privilege Escalation		✔			✔				✔	✔
Defense Evasion		✔			✔				✔	✔
Credential Access		✔			✔				✔	✔
Discovery	✔	✔			✔				✔	✔
Lateral Movement		✔							✔	✔
Collection		✔			✔				✔	
Command and Control		✔						✔	✔	
Exfiltration		✔					✔	✔	✔	
Impact		✔			✔					✔