

Threat-Based Attack Simulations Using MITRE ATT&CK

Validato helps you efficiently test cyber threats and MITRE ATT&CK Techniques to identify and mitigate security risks.



Testing Evolving Cyber Threats

In today's ever-evolving cyber threat landscape, organisations of all sizes need a robust preventative cyber defence strategy. Testing MITRE ATT&CK Techniques is an essential part of this strategy.

Why Choose Validato



Identify Security Gaps

Simulate real-world attacker tactics to pinpoint areas where your security controls are weakest.



Assess Security Control Effectiveness

Evaluate how well your controls perform against the latest attack techniques.



Improve Security Controls

Continuously test and refine your defences to stay ahead of evolving threats.



Reduce Cyber Risk

Proactively address vulnerabilities before they can be exploited.

About Validato

Validato is a cybersecurity platform that simplifies cyber threat testing and MITRE ATT&CK Technique evaluation.

With Validato You Can

- ✓ **Leverage Pre-Built Attack Simulations**
Access a library of 100s attack scenarios based on known cyber threat scenarios.
- ✓ **Test Safely In Production**
Conduct testing without disrupting your live environment.
- ✓ **Access Guided Remediation Advice**
Harden vulnerable areas of your environment with step-by-step configuration and remediation instructions.



+44 (0) 124 237 4181

justask@validato.io

<https://validato.io/>

46% Protection 93% Detection

Scenario

Description
The most commonly used MITRE ATT&CK Techniques used by adversaries as observed by MITRE Engenuity

MITRE Tactics
Defense Evasion, Credential Access, Execution, Persistence, Privilege Escalation, Command and Control

Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Valid Accounts	Windows Management Instrumentation	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Direct Volume Access	OS Credential Dumping	System Service Discovery	Remote Services	Data from Drive
Replication Through Removable Media	Scheduled Task/Job	Scheduled Task/Job	Scheduled Task/Job	Rootkit	LSASS Memory	Application Window Discovery	Software Deployment Tools	Data from Drive
External Remote Services	At	At	At	Obfuscated Files or Information	Security Account Manager	Query Registry	Taint Shared Content	Data from Drive
Drive-by Compromise	Scheduled Task	Scheduled Task	Scheduled Task	Binary Padding	NTDS	System Network Configuration Discovery	Replication Through Removable Media	Input Capture
Exploit Public-Facing Application	Command and Scripting Interpreter	Valid Accounts	Process Injection	Software Packing	LSA Secrets	Remote System Discovery	Exploitation of Remote Services	Data Stages
Supply Chain Compromise	PowerShell	Account Manipulation	Dynamic-link Library Injection	Steganography	Cached Domain Credentials	System Owner/User Discovery	Internal Spearphishing	Screen Capture
Trusted Relationship	Windows Command Shell	External Remote Services	Portable Executable Injection	Compile After Delivery	DCSync	System Owner/User Discovery	Use Alternate Authentication Material	Email Collection
Hardware Additions	Visual Basic	Create Account	Thread Execution Hijacking	Indicator Removal from Tools	Network Sniffing	Network Service Discovery	Remote Service Session Hijacking	Clipboard Data
Phishing	Python	Office Application Startup	Asynchronous Procedure Call	HTML Smuggling	Input Capture	System Network Connections Discovery	Lateral Tool Transfer	Automated Malware Downloads
Content Injection	JavaScript	Browser Extensions	Thread Local Storage	Dynamic API Resolution	Brute Force	Process Discovery		Audio Capture
			Extra Window Memory	Embedded Payloads	Multi-Factor Authentication	Permission Groups		Video Capture

Empower Your Preventative Cyber Defence Team




Prioritise Security Investments

Focus resources on the areas most vulnerable to attacks.



Develop Threat-informed Defence

Base security decisions on real-world attacker behaviour.




Continuously test and monitor your internal cyber risk posture

Test cyber resilience against known threat scenarios.



Understand your resilience to key cyber threats

Understand where security gaps may be in your environment



Last scenario run: 1/16/2024 16:11

Run scenario

Scenarios are based on MITRE ATT&CK techniques.

Recommended scenarios

Based on current threats

Top MITRE ATT&CK Techniques

Recommended 21 | 233 2 hours 11 minutes

The most used techniques by attackers from MITRE ATT&ck version 10.1 statistics

Category: Host-based
Scenario type: MITRE - Malware, MITRE - Adversary group, Validato
MITRE tactics: Execution, Persistence, Privilege escalation, Defense evasion...

LockBit Ransomware

Recommended 31 | 365 1 hour 5 minutes

LockBit 2.0 is ransomware as a service (RaaS) that first emerged in June 2021 as an upgrade to its predecessor LockBit (aka ABCD Ransomware), which was first observed in September 2019.

Since its inception, the LockBit 2.0 RaaS attracted affiliates via recruitment campaigns in underground forums, and thus became particularly prolific during the third quarter of calendar year 2021. The LockBit 2.0 operators...

Category: Host-based, Lateral movement
Scenario type: MITRE - Malware, Validato
MITRE tactics: Collection, Execution, Credential access, Persistence, Initial ...

Top 25 Validato Techniques

Recommended 23 | 243 1 hour 46 minutes

The Validato top MITRE Techniques scenario represents the results of Validato's own research into the most prevalent and exploited MITRE ATT&CK TTPs. This scenario includes guided remediation information and advice aimed to harden defences against exploitation of the techniques covered in this scenario. Run this scenario first if you are looking for a logical way to start using Validato.

Category: Host-based
Scenario type: Validato
MITRE tactics: Execution, Persistence, Privilege escalation, Defense evasion...

Take Control Of Your Cyber Security

Book a demo today and see how Validato can help you test cyber threats, harden your security controls, and reduce your risk of cyber attacks.



+44 (0) 124 237 4181

justask@validato.io

https://validato.io/