ArcSight Intelligence and MITRE ATT&CK

Micro Focus ArcSight Intelligence covers 75% of ATT&CK tactics and techniques.

MITRE's ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a living knowledge base of threat tactics and techniques observed in real-world attacks on enterprise networks, and it plays a pivotal role in ArcSight Intelligence's behavioral analytics.

Detect the Unknowns with ArcSight Intelligence and ATT&CK

With detailed information on data sources, mitigation, examples, and detection for many tactics and techniques, ATT&CK is a one-stop-shop for security researchers, practitioners, or vendors to better understand how to effectively protect organizations from real attacks. Today, ArcSight Intelligence covers 75% of the ATT&CK framework that has been seen in the wild, and our coverage will continue to grow.

ArcSight Intelligence leverages more than 450 machine learning models to baseline the behavior of every user and entity within an organization and evaluate deviations from those baselines as potentially risky behaviors. Our machine learning models are carefully mapped to ATT&CK's 219 techniques to better understand:

- Which attack techniques our customers face most often
- Where ArcSight Intelligence provides coverage most effectively
- How we can leverage our anomaly models to protect businesses against real threats.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-Stage Channels
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Hop Proxy
	Launchctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	Image File Execution Options Injection	DLL Side-Loading	Keychain	Security Software Discovery	Exploitation of Remote Services	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or	LLMNR/NBT-NS Poisoning	System Information	Taint Shared Content			Port Knocking

Figure 1. Heatmap

ArcSight Intelligence's behavioral analytics covers 75% of the techniques in MITRE's ATT&CK framework*, providing effective coverage against a range of threats that can facilitate exfiltration of high-value information, fraud, and more.

** The heatmap above does not represent the full MITRE ATT&CK framework. Visit* **mitre.microfocus.com** *for more information.*