Powering Secure and Agile Networks

EventTracker SIEM and MITRE ATT&CK Framework

Use real-world adversary techniques to better detect cybersecurity threats

Overview

With cyber criminals spending an average of 206 days in an organization's environment, cyber threats require rapid detection and elimination to reduce costly damage. Threat groups and nation-state attackers often use distinct tactics and techniques that signify attempted compromise. These unique adversary tactics and techniques are compiled in a repository called the MITRE ATT&CK® knowledge base, but implementing it on your own can be complex and time consuming.

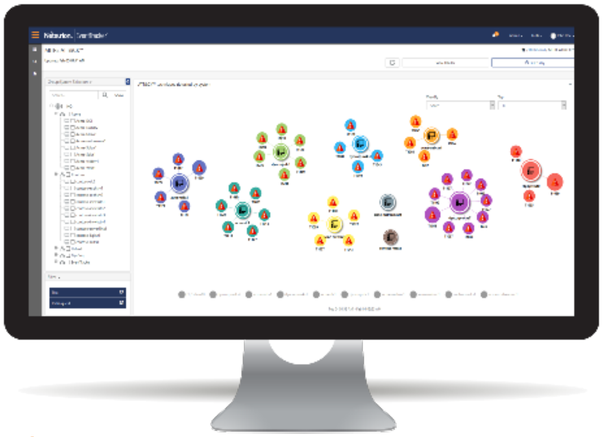
Netsurion integrates this database of known adversary techniques into the EventTracker Security Information and Event Management (SIEM) platform to accelerate threat detection and incident response. ATT&CK enables organizations of all sizes to fortify their defenses and stop similar attack techniques in the future.

What is ATT&CK and How it Helps

Developed by MITRE, the ATT&CK framework is based on real-world observations. The framework's descriptions of tactics, techniques, and procedures (TTPs) enable security defenders to identify relationships between individual observations and known threat actors.

Mapping the MITRE ATT&CK knowledge base with the EventTracker solution improves threat hunting and comprehensive discovery of ongoing attacks. This threat intelligence is available in the EventTracker console for better visibility and threat enrichment.

Our co-managed SIEM solution with its 24/7/365 security operations center (SOC) monitoring enables you to prioritize your most concerning alarms, detect hidden threats, and identify advanced risks that could lead to a data breach.



Benefits

- Creates a common language for describing attack patterns which simplifies information sharing
- Provides better detection and investigation advantages in the first critical moments of an incident
- Integrates with EventTracker SIEM to block adversary actions
- Updates adversary knowledge over time as the threat landscape evolves
- Improves rapid cybersecurity decision making

How it Works

Step 1: Correlates your EventTracker log data with the MITRE ATT&CK knowledge base.

Step 2: Provides the ATT&CK dashboard within the EventTracker console with detected adversary techniques.

Step 3: Continues to monitor for ATT&CK techniques within your organization for further investigation.

Step 4: Enables defenders to prioritize investigations and respond to threats more quickly and with better accuracy.

Netsurion Earned SC Media's Top Five-Star Rating for SIEM, EDR, and SOC-as-a-Service in 2019.

©2020 Netsurion, LLC

Features

Risk Management

- Prioritize threats earlier in the cybersecurity lifecycle
- Tailor threat response to industry threats and actual security gaps
- Protect your organization from future threats that use known exploits

Detection and Dashboards

- Identify patterns and TTPs quickly to pinpoint suspicious behavior
- Provide drill down capabilities such as the EventTracker ATT&CK Techniques Detected by System; EventTracker ATT&CK Timeline; and ATT&CK Navigator™
- Offer multi-tenant capabilities for MSPs and very large enterprises

Real-Time Alerting

- Enrich threat intelligence context with actual techniques used by hackers
- Detect anomalous behavior with machine learning, threat intelligence, the ATT&CK knowledge base, and EventTracker's 24/7 SOC analysts

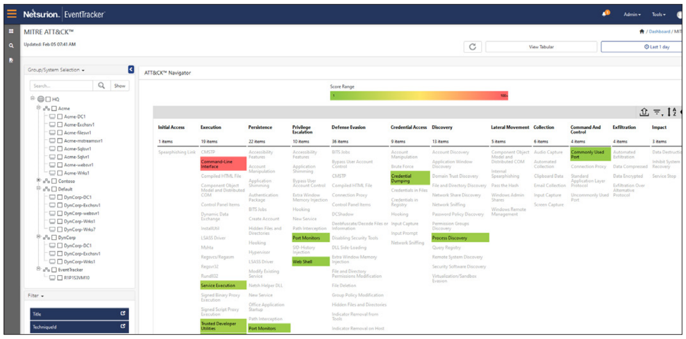
Simplicity and Ease of Use

- Incorporated into EventTracker SIEM's one-stop-shop console
- Pivot to MITRE's ATT&CK website for more in-depth insights on adversaries, techniques, and remediation steps
- Provide techniques and adversary behavior against popular platforms such as Microsoft Office 365, Microsoft Azure Advanced Threat Protection (ATP), and Amazon Web Services (AWS)

Technical Specifications

- EventTracker 9.3 or higher

The integration of the MITRE ATT&CK framework into EventTracker SIEM provides insights for a range of users in your organization. IT and security analysts with practitioner responsibilities benefit from the hands-on visibility in the EventTracker console. The threat intelligence enrichment based on actual adversary techniques helps further detection and prioritize which exploits to investigate.



Updated: Feb 05 07:41 AM

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
1 items	19 items	22 items	10 items	36 items	9 items	13 items	5 items	6 items	4 items	4 items	3 items
Spearphishing Link	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Account Manipulation	Account Discovery	Component Object Model and Distributed COM	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destructio
	Command-Line Interface	Account Manipulation	Application Shimming	Bypass User Account Control	Brute Force	Application Window Discovery	Internal Spearphishing	Automated Collection	Connection Proxy	Data Compressed	Inhibit System Recovery
	Compiled HTML File	Application Shimming	Bypass User Account Control	CMSTP	Credential Dumping	Domain Trust Discovery	Pass the Hash	Clipboard Data	Standard Application Layer Protocol	Data Encrypted	Service Stop
	Component Object Model and Distributed COM	Authentication Package	Extra Window Memory Injection	Compiled HTML File	Credentials in Files	File and Directory Discovery	Windows Admin Shares	Email Collection	Uncommonly Used Port	Exfiltration Over Alternative Protocol	
	Control Panel Items	BITS Jobs	Hooking	Connection Proxy	Credentials in Registry	Network Share Discovery	Windows Remote Management	Input Capture			
	Dynamic Data Exchange	Create Account	New Service	Control Panel Items	Hooking	Network Sniffing		Screen Capture			
	InstallUtil	Hidden Files and Directories	Path Interception	DCShadow	Input Capture	Password Policy Discovery					
	LSASS Driver	Hooking	Port Monitors	Deobfuscate/Decode Files or Information	Input Prompt	Permission Groups Discovery					
	Mshta	Hypervisor	SID-History Injection	Disabling Security Tools	Network Sniffing	Process Discovery					
	Regsvcs/Regasm	LSASS Driver	Web Shell	DLL Side-Loading		Query Registry					
	Regsvr32	Modify Existing Service		Extra Window Memory Injection		Remote System Discovery					
	Rundll32	Netsh Helper DLL		File and Directory Permissions Modification		Security Software Discovery					
	Service Execution	New Service		File Deletion		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Execution	Office Application Startup		Group Policy Modification							
	Signed Script Proxy Execution	Path Interception		Hidden Files and Directories							
	Trusted Developer Utilities	Port Monitors		Indicator Removal from Tools							
				Indicator Removal on Host							

Organizational executives can utilize ATT&CK to understand adversaries in your industry better and to identify gaps in protection and security maturity. Your entire company benefits from the intuitive dashboard and single-pane-of-glass visibility that save time in operational security and increases effectiveness in early threat detection.

MITRE ATT&CK Overview

The MITRE Company is a not-for-profit organization that provides practical solutions to make the world a safer place. It operates federally-funded research and development centers across the United States.

The MITRE ATT&CK framework covers over 90 threat actors and almost 300 of their distinctive threat techniques. ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) is continuously updated, providing you with more effective defense, detection, and remediation.

Businesses, government agencies, global partners, and vendors widely adopt ATT&CK as a methodology to inform defenses and share threat intelligence.

Learn more here: **www.attack.mitre.org.**

Netsurion Earned SC Media's Top Five-Star Rating for SIEM, EDR, and SOC-as-a-Service in 2019.

Netsurion™
Powering Secure and Agile Networks

©2020 Netsurion, LLC