Data Sheet

MITRE ATT&CK Module

LogRhythm
The Security Intelligence Company

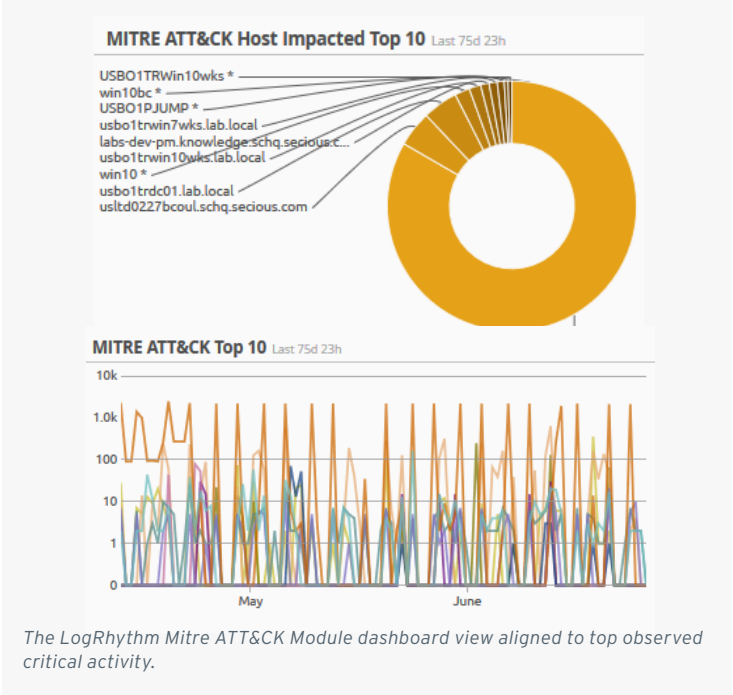
Throughout the years, the tactics and techniques of adversaries have evolved to avoid detection driving cybersecurity advancements in technology, knowledge, and program maturity. Today, security programs must continue to update their methodologies as fast as adversaries iterate to detect new threats and prevent damaging breaches.

MITRE ATT&CK™ is an open knowledge base of observed adversary tactics and techniques based on real-world observations. This framework enables broad sharing of adversarial behaviors across the attack lifecycle and provides a common taxonomy for threat analysis and research.

Amplify Your ATT&CK Strategy

ATT&CK delivers actionable intelligence based on known adversary behaviors modeled from specific threat observations. The LogRhythm MITRE ATT&CK Module applies this methodology to deliver immediate insight for security teams to respond effectively and address gaps in their security visibility, operations, and infrastructure.

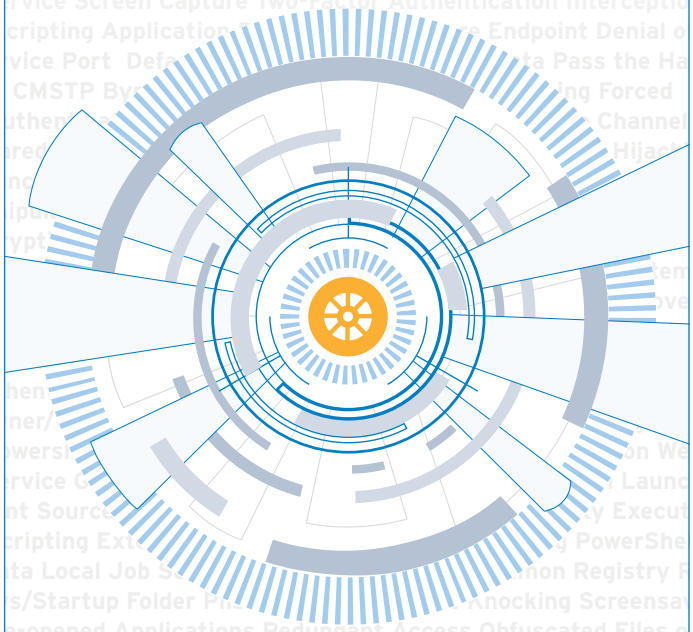
The LogRhythm MITRE ATT&CK Module provides prebuilt content mapped to ATT&CK within your LogRhythm NextGen SIEM Platform, including analytics, dashboard views, and threat hunting tools. This content enables you to detect adversaries and improve your security program as prescribed by the MITRE ATT&CK framework.



The LogRhythm Mitre ATT&CK Module dashboard view aligned to top observed critical activity.

BENEFITS

- ✓ **Amplify threat detection across your security stack**
- ✓ **Increase threat hunting accuracy and speed**
- ✓ **Assess security program coverage and gaps**
- ✓ **Reference corresponding ATT&CK IDs in alarms to quickly look up next steps**
- ✓ **Use LogRhythm's RespondX SOAR to streamline efficient response workflows**



KEY TERMS

ATT&CK: an acronym for Adversarial Tactics, Techniques, & Common Knowledge

Adversary: cyber threat actor

Tactics: adversarial goals

Techniques: methods to achieve a goal

Procedures: steps to execute a technique

High-Fidelity Visibility for Accurate Threat Detection

Detecting adversaries requires pervasive visibility across your security data and a proactive approach to efficiently identify suspicious behavior. With support for over 900 log source types, LogRhythm ensures collection of the right data to best optimize detection by the MITRE ATT&CK Module.

Complete coverage of ATT&CK techniques requires data from a wide set of technologies, including endpoint detection and response (EDR), antivirus/anti-malware, intrusion detection/prevention systems (IDS/IPS), and other products. The analytics in the LogRhythm MITRE ATT&CK Module expose events across all available sources to identify one or more system or application with the necessary data.

Go beyond just shutting down one instance of a threat. Tap into a referential system for how to best assess and harden your organization against future threats using the same exploits.

Expand the scope of your security strategy to keep up with changing security challenges and avoid the pitfalls of a single approach. Leverage ATT&CK with LogRhythm network and user analytics, compliance modules, and threat feeds to generate higher-value alarms that more accurately detect adversaries.

LogRhythm	Point Solutions
✓ LogRhythm analytics detect specific techniques mapped directly to the ATT&CK framework.	Most security-focused queries only observe set parameters, indicators, and types of behavior.
✓ LogRhythm's Machine Data Intelligence (MDI) Fabric's flexible data schema is source-type agnostic.	EDR vendors dependence on agent-based data collection limits support for all log source types.
✓ LogRhythm NetworkXDR and UserXDR solutions augment ATT&CK by adding enhanced network and user context around threats.	Other solutions do not have the choice to add network and user visibility for a higher-fidelity approach to your data.
✓ LogRhythm's free log generator tool, Echo, generates test data enabling Red Team / Blue Team activities for discovering gaps and testing the efficacy of your SOC.	Testing the efficacy of your security operations with point solutions increases overhead and provides reduced visibility, limiting your ability to identify gaps.
✓ LogRhythm's SOAR solution RespondX enables streamlined and automated ATT&CK workflows for security response across your IT environment.	EDR solutions and add-on SOAR products lack direct access to your full data set, creating inefficiencies in your threat investigation and response processes.

Learn more today. Visit www.logrhythm.com for more information.

©2019 LogRhythm Inc. | DS1279_2019