FEATURE BRIEF

MITRE ATT&CK® alert mapping

OVERVIEW

What is the feature?

As security events arise, the Lacework platform maps each event to MITRE ATT&CK framework tactics and techniques. Security teams can then filter all security events by these tags to focus on specific attacker techniques.

This feature further enhances the platform's context-rich alerts. Each alert provides security event details in a comprehensive event card that displays the who, what, why, where, and when of each event. The information includes the user name associated with the event, machine details, process-related information, any related alerts, and more. Alert cards also include visualizations that provide rich context for fast remediation.

What is the MITRE ATT&CK framework?

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a comprehensive knowledge base of the tactics and techniques used by cyber adversaries when targeting and compromising organizations. The framework provides a detailed and continuously updated breakdown of the various methods attackers use throughout the lifecycle of their campaigns.

The importance of the MITRE ATT&CK framework lies in its ability to provide defenders with a holistic understanding of the cyber threat landscape. By being aware of the tactics and techniques used by adversaries, organizations can better design and implement defensive measures, conduct thorough threat hunting, and enhance incident response efforts. The framework also fosters collaboration within the cybersecurity community, as it provides a common language and reference point for discussing and analyzing cyber threats.

Lacework benefits

- **More context for threat investigation**
  Speed investigation and response with actionable context when prevention fails
- **Better collaboration with other teams**
  Share information on alerts using a common industry-recognized standard
- **Faster visibility into known tactics**
  MITRE + Lacework anomaly detection can detect and tag threats in near real-time

What MITRE tactics and techniques can be mapped within Lacework?

The platform can currently detect 14 different adversary tactics with their associated techniques. Those tactics are listed below. For a full view of attacker techniques aligned with these tactics, see this matrix on the MITRE ATT&CK website.

ID	Name	Description
TA0001	Initial Access	The adversary is trying to get into your network. *9 total techniques*
TA0002	Execution	The adversary is trying to run malicious code. *14 total techniques*
TA0003	Persistence	The adversary is trying to maintain their foothold. *19 total techniques*
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions. *13 total techniques*
TA0005	Defense Evasion	The adversary is trying to avoid being detected. *42 total techniques*
TA0006	Credential Access	The adversary is trying to steal account names and passwords. *17 total techniques*
TA0007	Discovery	The adversary is trying to figure out your environment. *31 total techniques*
TA0008	Lateral Movement	The adversary is trying to move through your environment. *9 total techniques*
TA0009	Collection	The adversary is trying to gather data of interest to their goal. *17 total techniques*
TA0010	Exfiltration	The adversary is trying to steal data. *9 total techniques*
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them. *16 total techniques*
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data. *13 total techniques*
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations. *8 total techniques*
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations. *10 total techniques*

Why is the feature important?

By combining MITRE ATT&CK techniques with Lacework anomaly detection, customers can detect and identify attacker techniques earlier in the attack lifecycle. Then, customers can leverage Lacework integrations to quickly triage these alerts to the appropriate teams. This results in faster investigations and more efficient remediation efforts, all while speaking in the common language of the MITRE ATT&CK framework.

DEPLOYMENT

How is the feature implemented?

MITRE ATT&CK tagging is an automated feature and requires no additional lift from users. Once tags are assigned, Lacework users can filter by MITRE ATT&CK technique or tactic, along with existing alert filters like alert severity, alert category, and more.

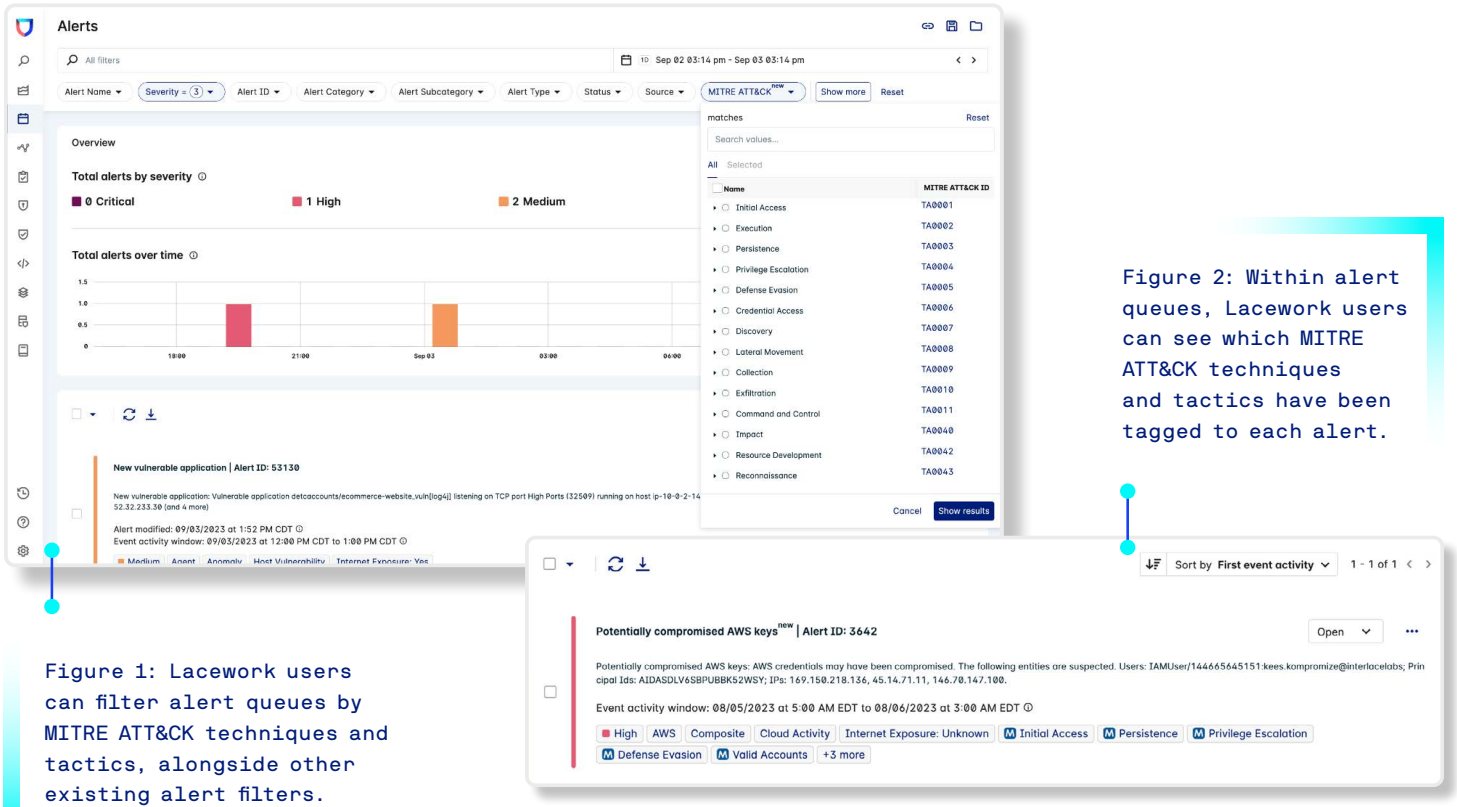

Figure 2: Within alert queues, Lacework users can see which MITRE ATT&CK techniques and tactics have been tagged to each alert.

Figure 1: Lacework users can filter alert queues by MITRE ATT&CK techniques and tactics, alongside other existing alert filters.

See it in action.

Book a live demo

See more ways to detect threats