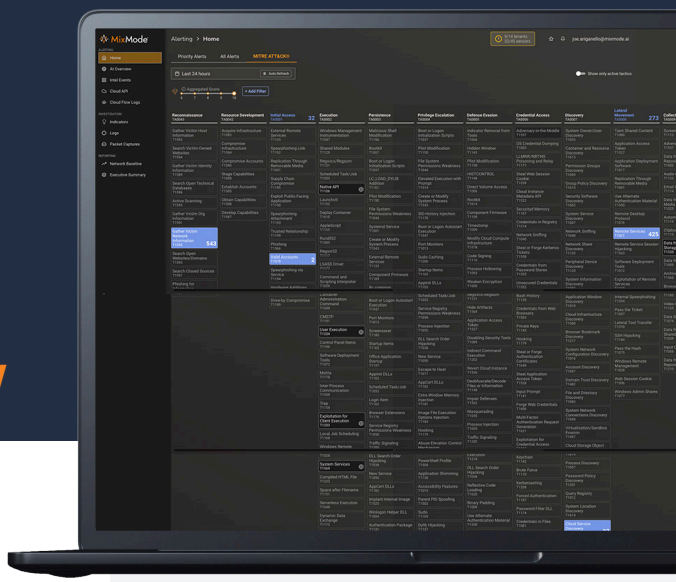
MixMode®

THE MIXMODE PLATFORM AND THE MITRE ATT&CK FRAMEWORK

ATT&CK Techniques Detected Overview



MITRE ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) catalogued by MITRE based on real-world observations. The framework serves as a model for understanding how attackers infiltrate systems and networks to achieve their objectives.

Mapping security tools and detections to MITRE ATT&CK has become vital for assessing visibility gaps and monitoring coverage of threats. With ATT&CK profiling, organizations gain an objective way to evaluate security solutions based on their ability to detect known adversary behaviors across the attack lifecycle.

The MixMode Platform fully integrates with The MITRE ATT&CK Framework, automatically mapping detections to techniques and tactics. This enables transparent ATT&CK coverage analysis, empowering customers to validate visibility into threats mapped by MITRE.

How it Works

The MixMode Platform is the only generative AI cybersecurity solution built on patented technology purpose-built to detect and respond to threats in real-time, at scale. MixMode's generative AI is uniquely born out of dynamical systems (a branch of applied mathematics) and self-learns an environment without rules or training data.

The MixMode Platform provides customers unparalleled visibility into exposure to attacker TTPs catalogued by MITRE, highlighting threats moving laterally and progressing through the kill chain, as well as surfacing advanced techniques that evade other defenses.

With The MixMode Platform, security teams gain an ATT&CK lens into potential blind spots, visibility gaps, and coverage strengths across their environments. This insight informs security strategies and solution decisions grounded in real-world adversary behavioral data rather than subjective opinions or biased vendor claims.

KEY BENEFITS

Identify blind spots:

Map detections to ATT&CK to highlight visibility gaps and expose areas that may lack coverage.

Context for alerts:

Gain instant context on adversary trade craft with alerts linked to ATT&CK techniques.

Frame investigations:

Enables analysts an attack framework to drive response actions with detections mapped to tactics/ techniques.

Improve threat hunting:

Leverage ATT&CK models to increase likelihood of finding evasive behaviors during hunting exercises.

Enable data-driven security:

Synthesize ATT&CK alignment to bring threat intelligence into operations and strategy.

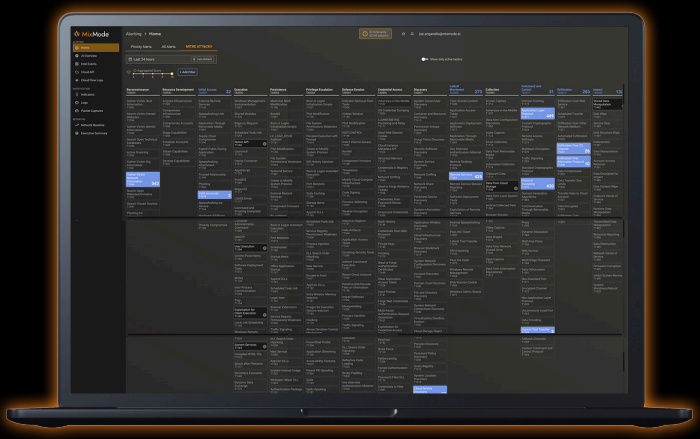
COMPLETE COVERAGE FOR MITRE ATT&CK ENTERPRISE MATRIX

MixMode provides thorough coverage for the MITRE ATT&CK™ Framework and has been proven to out perform competitive products in detecting MITRE ATT&CK™ TTPs. MITRE ATT&CK Framework detections can be further enhanced within The MixMode Platform through integration with your existing security stack (i.e. Endpoint, Firewall, Vulnerability Scanning etc.).

Reconnaissance: The adversary is trying to gather information they can use to plan future operations.
Resource Development: The adversary is trying to establish resources they can use to support operations.
Initial Access: The adversary is trying to get into your network.
Execution: The adversary is trying to run malicious code.
Persistence: The adversary is trying to maintain their foothold.
Privilege Escalation: The adversary is trying to gain higher-level permissions.
Defense Evasion: The adversary is trying to avoid being detected.
Credential Access: The adversary is trying to steal account names and passwords.
Discovery: The adversary is trying to figure out your environment.
Lateral Movement: The adversary is trying to move through your environment.
Collection: The adversary is trying to gather data of interest to their goal.
Command and Control: The adversary is trying to communicate with compromised systems to control them.
Exfiltration: The adversary is trying to steal data.
Impact: The adversary is trying to manipulate, interrupt, or destroy your systems and data.

No rules. No tuning. No maintenance. Any environment.

Cloud Native | On-Prem | Hybrid



MixMode is the leader in delivering generative AI cybersecurity solutions at scale. MixMode offers a patented, self-learning Platform designed to detect known and unknown threats in real-time across cloud, hybrid, or on-prem environments. Large enterprises with big data environments, including global entities in financial services, fortune 1K commercial enterprises, critical infrastructure, and government sectors, trust MixMode to protect their most critical assets. Backed by PSG and Entrada Ventures, the company is headquartered in Santa Barbara, CA. Learn more at www.mixmode.ai.