RAPID7

PRODUCT BRIEF

Putting MITRE ATT&CK® to Work In Your SOC

MITRE ENGENUITY ATT&CK® EVALUATIONS
Enterprise
WIZARD SPIDER & SANDWORM
PARTICIPANT
2022

Visualize detections coverage and accelerate detection and response

The MITRE ATT&CK framework provides common language and guidance for threat intelligence gathering, understanding and prioritizing detections coverage, as well as incident response planning.

The good news: the framework is thorough, detailed, and always growing. But that also means most SOCs, straining under heavy daily demands, could use help.

Key Security Operations Challenges Today

- **Demonstrating Coverage:** Difficult to visualize or measure that you have the right detections in place
- **Overwhelming Attack Surface:** Proliferation of the environment - and attackers' ways to disrupt it
- **Resource Shortage:** Challenged to keep up with emergent threats

InsightIDR — Rapid7's cloud-native SIEM and XDR — delivers highly efficient, accelerated detection and response. With InsightIDR's breadth, native detection capabilities, and curated library, teams can feel confident that they always have defense-in-depth across the attack surface.

Now, with MITRE ATT&CK framework infused into InsightIDR, customers can visualize their coverage across the framework, and more quickly leverage this valuable content in the moment.

Use Cases	InsightIDR with MITRE ATT&CK Mapping
Visualize Coverage Across MITRE ATT&CK Framework	• Visualize which techniques and sub-techniques you have detections mapped to with information on each threat actor's TTPs (Tactics, Techniques, and Procedures). • Drill down and see the specific detection rules that map to each area of the framework in your environment. • MITRE ATT&CK context and filters apply automatically against all of your data, helping you detect and respond to attacks early and giving you the alert fidelity you want, filled with the context you need.

Use Cases	InsightIDR with MITRE ATT&CK Mapping
Triage Alerts Faster	● Tune your detection rules based on the ATT&CK context and your unique security environment to reduce benign alerts and bring high-priority alerts to the forefront. ● Understand the context behind an alert by viewing information about the attacker's underlying techniques and sub techniques. ● Filter and sort your alerts and investigations based on the MITRE info to distill down to where it really matters when time is of the essence.
Accelerate Mean Time to Respond (MTTR)	● Quickly prioritize which investigations are most critical to tackle first. ● Determine how to respond to the attack with the mitigation recommendations provided by MITRE ATT&CK (alongside InsightIDR's recommendation context). ● Leverage the strategies provided to work internally and take proactive steps within the organization to prevent the next attack, staying one step ahead of attackers. ● Use the MITRE insights provided in the evidence panel to inform the decision-makers on the best way to proceed.

Teams are empowered to detect, investigate, and respond like experts

Rapid7's Threat Intelligence and Detections Engineering (TIDE) team leverages a unique combination of intelligence – including from Rapid7's own open source technologies – to curate a detections library that spans the entire attack surface. InsightIDR covers users, endpoints, the network, and the cloud. The highly manicured library is vetted in the field by the Rapid7's global Managed Detection and Response (MDR) SOC teams, ensuring high fidelity alerts and strong signal-to-noise.

The modern environment continues to sprawl, and so do attackers' tactics and techniques. InsightIDR can be gamechanger.