# Build a Robust Security Practice based on the MITRE ATT&CK® Framework

## The MITRE ATT&CK Framework

The MITRE ATT&CK knowledge base was developed to help security professionals make sense of the near-infinite variety of tactics and techniques attackers use to infiltrate networks, steal data, extort payments, or otherwise do harm to legitimate businesses and their reputations. This "globally accessible knowledge base of adversary tactics and techniques based on real-world observations" has become popular as it meets a very real need: it provides a list of methods by which enterprise IT environments can be compromised, and the information is detailed and highly specific. If you can defend against every technique that's mentioned in the framework, the common wisdom goes, your environment will be fundamentally secure.

MITRE ATT&CK™

## MITRE ATT&CK: Strengths and Limitations

The MITRE ATT&CK knowledge base enables security professionals to move beyond identifying the simplest—and easiest to modify—indicators of malicious activity, such as file signatures associated with known malware or IP addresses linked to phishing attempts, to instead train their attention upon adversaries' behaviors.

Because it's grounded in real-world observations, it's applicable to real IT environments: any of the attack scenarios described in the ATT&CK framework can be emulated by red teams or in penetration tests. And because it's behavior-focused, the framework can help security analysts understand the "how" and "why" of particular malicious activities.

However, with more than 500 activities described among the adversarial techniques, the framework is large and complex. It would be extremely challenging for any organization to defend against all of them, all the time.


## Mapping sensor grid detection capabilities against attacker tactics and behaviors

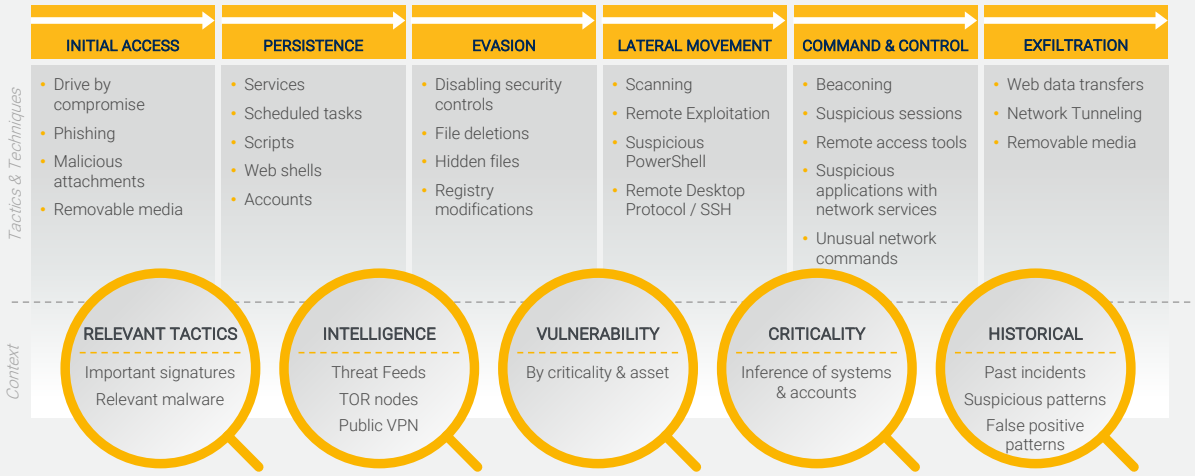
Security teams can employ the ATT&CK framework as a way to map their sensor grid's detection capabilities against real-world attackers' tactics, techniques, and procedures.

For example, the coverage offered by an individual network intrusion detection system (NIDS) can be compared with the full catalog of attack techniques in the framework to evaluate how well it can actually monitor—and thus enable protection of the environment. Security sensors are like the eyes and ears of a security operations team: the higher the quality, and the greater the quantity of the information they report, the better malicious activity can be detected.

## Designing a sensor grid according to the MITRE ATT&CK Framework

Sensor diversity and overlapping coverage is best. It might seem obvious, but if you were to compare the volume and quality of the sensor data you'd get from implementing tools from all the various NIDS, endpoint protection platforms (EPPs), endpoint detection and response (EDR) systems, URL filtering tools, and other security sensors, you will find that all of them, used together, will provide tremendously deeper coverage across the entire taxonomy of attacks than any single data source.

Because any individual vendor's solution has the potential to miss particular attack techniques, this really is a case where "the more, the merrier" is true. What types of traffic are you monitoring? Does your sensor grid include east-west network coverage? The depth and breadth of information you are gathering is of critical importance here. Including solutions from multiple vendors can help ensure you against security flaws or poor signature-writing on one vendor's part.




## Turn up the volume, tune up the sensors

Whenever you tune down your network sensors, you are excluding potentially valuable and illuminating information from consideration. No matter how carefully you construct rules and policies, you still inherently increase the risk that an attacker will evade detection with every alert you dismiss without analysis or consideration.

Unless it's being managed and monitored, you're not deriving real value from your security sensor data.

Information that's collected only to be stored within a data lake or security information and event management (SIEM) software without subject to monitoring or analysis will never help you detect attacks that are in progress. Though the argument is often made that this log data can be useful after the fact for forensic purposes, making post-breach investigations easier isn't the same as reducing your organization's real risks.

## The Respond Analyst: the most critical tool for deepening sensor grid coverage

Designing a security sensor grid that can monitor for more of the techniques and procedures in the ATT&CK framework also demands that your SecOps team maintain the capability to monitor these sensors—thoroughly, with care, and continuously. Implementing an automated software solution, such as the Respond Analyst, enables you to make deeply analytical decisions about what's likely to be worthy of further investigation.

With the latest generation of automated security monitoring technologies, including decision automation, the Respond Analyst is able to bring together a broad array of information from multiple security sensor sources within a single, integrated solution. The intelligent decision engine can correlate data across the various sources for enhanced effectiveness; the more multi-source corroboration that can be achieved, the more accurate and comprehensive your monitoring will be.

## Why use the Respond Analyst?

### Open

Choose best-of-breed controls to modernize your sensor grid. Works with **over 65 vendor offerings** across important categories such as EDR, IPS, Web Filtering, EPP, Vulnerability Scanning, Authentication and more.

### Intelligent

Connects the SOC's disparate evidence using probabilistic mathematics and **Integrated Reasoning** to determine the likelihood that events are malicious and important enough to escalate.

### Simple

**Deploys in hours** and constantly learns without tuning, coding or content writing. Cloud-native, so you don't have to manage infrastructure.

## How the Respond Analyst uses the MITRE ATT&CK Framework to stop attacks

| TACTICS | RESPOND'S APPROACH |
|---|---|
| **Initial Access** | |
| Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. | The Respond Analyst analyzes events from a variety of technologies, including Network IDS/IPS (NIDPS), Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) to identify exploitation and determine if a systems or accounts were compromised as a result. |

| TACTICS | RESPOND'S APPROACH |
| --- | --- |
| **Execution** | |
| Execution consists of techniques that result in adversary-controlled code running on a local or remote system. | The Respond Analyst determines if files were written to disk or processes were able to execute leveraging EPP and EDR technologies to determine if the execution phase has been reached during an incident. |
| **Persistence** | |
| Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. | The Respond Analyst determines persistence by analyzing the behavior of systems and accounts to identify malicious processes that run consistently or periodically and accounts that have been compromised to gain continued access to the organization. |
| **Privilege Escalation** | |
| Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. | The Respond Analyst determines Privilege Escalation by analyzing suspicious process behavior attempting to increase account permissions or gain access to a higher-level account via Endpoint Detection and Response solutions. |
| **Defense Evasion** | |
| Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. | The Respond Analyst determines Defensive Evasion by analyzing suspicious process behavior of systems and accounts via Endpoint Detection and Response solutions. |
| **Credential Access** | |
| Credential Access consists of techniques for stealing credentials like account names and passwords. | The Respond Analyst analyzes events from a variety of technologies, including Network IDS/IPS (NIDPS), Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) to identify when credentials are accessed in a suspicious ways with native tools or malicious software indicative of an attacker attempting to gain further persistence and access. |
| **Discovery** | |
| Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. | The Respond Analyst analyzes events from Network IDS/IPS (NIDPS) and Endpoint Detection and Response (EDR) to identify discovery / reconissance activities such as system and domain account informaiton collection conducted by an attacker that are often observed after initially compromising an organization. These activities are traditionally dificult to differentiate from normal user and administrator activity. |

| TACTICS | RESPOND'S APPROACH |
|---|---|
| **Lateral Movement** | |
| Lateral Movement consists of techniques that adversaries use to enter, pivot, and control remote systems on a network. | The Respond Analyst analyzes events from Network IDS/IPS (NIDPS) and Endpoint Detection and Response (EDR) to identify lateral movement activities such as remote exploitation or credential dumping that are often observed after initially compromising an organization. These activities are traditionally difficult to differentiate from normal user and administrator activity. |
| **Collection** | |
| Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. | The Respond Analyst determines Collection by analyzing suspicious process behavior intending to steal system credentials via Endpoint Detection and Response solutions. |
| **Command and Control** | |
| Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. | The Respond Analyst analyzes events from Network IDS/IPS and Web Filtering logs to identify command and control, understand the beaconing pattern, and evaluate attributes of the external adversary. In addition, the Respond Analyst analyzes events from EPP and EDR solutions to understand the malware and process enabling command and control. |
| **Exfiltration** | |
| Exfiltration consists of techniques that adversaries may use to steal data from your network. | The Respond Analyst analyzes events from EDR solutions to identify suspicious behaviors like data compression prior to adversaries exfiltrating data. |
| **Impact** | |
| Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. | The Respond Analyst specifically identifies Ransomware by evaluating the malware and process information within endpoint protection and endpoint detection alerts. |

## Summary

With the latest generation of automated security monitoring technologies, you're able to bring together a broad array of information from multiple security sensor sources within a single, integrated view. Integrated reasoning included with the Respond Analyst, correlates data across the various sources for enhanced effectiveness; the more multi-source corroboration that can be achieved, the more accurate and comprehensive your monitoring will be.

Given the MITRE ATT&CK framework's complexity, it's near-impossible for human security analysts working without the assistance of security automation software to achieve real coverage of even a small fraction of the attack methods it catalogs. With decision automation onboard your team, however, it's possible to perform at an entirely new level.