A Guide

to Automating Threat Detection with

MITRE | ATT&CK™

Framework

mistnet

Enterprise security. Demystified.

Table of Contents

What is MITRE ATT&CK framework? 1

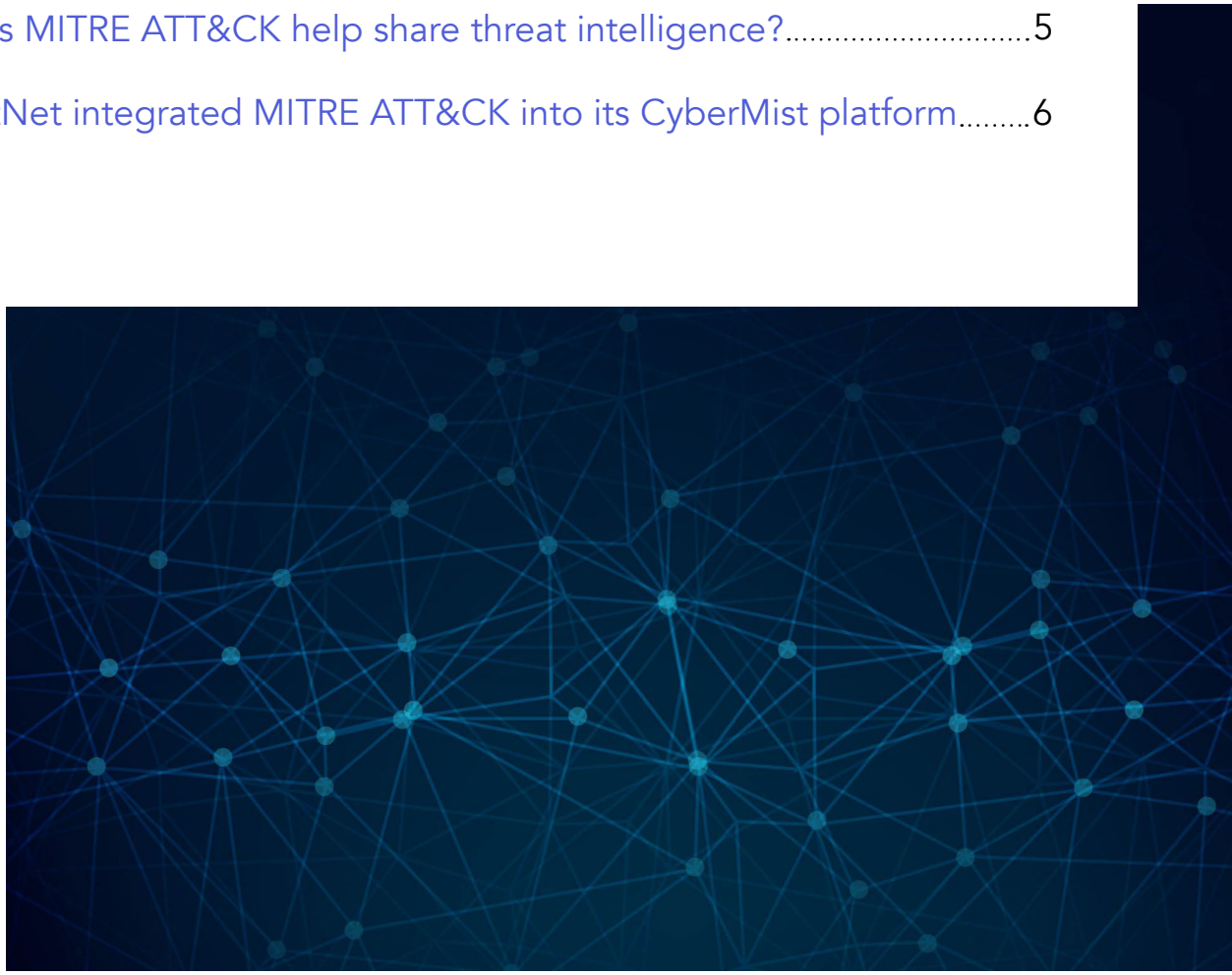
Why is MITRE ATT&CK valuable? 2

Using MITRE ATT&CK to map defenses and identify gaps 3

Using MITRE ATT&CK with cyber intelligence 4

How does MITRE ATT&CK help share threat intelligence? 5

Why MistNet integrated MITRE ATT&CK into its CyberMist platform 6



What is MITRE ATT&CK?

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on events that have happened in the real-world. It provides a complex framework of more than **200 techniques** that adversaries have used during an attack. These include specific and general techniques, as well as concepts and background information on well-known adversary groups and their campaigns.

The acronym ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge. Tactics represent the "why" of an ATT&CK technique. The tactic is the adversary's tactical objective for performing an action. Tactics offer contextual categories for individual techniques and cover standard, higher-level notations for activities adversaries carry out during an operation such as persist, discover information, move laterally, execute files, and exfiltrate data.

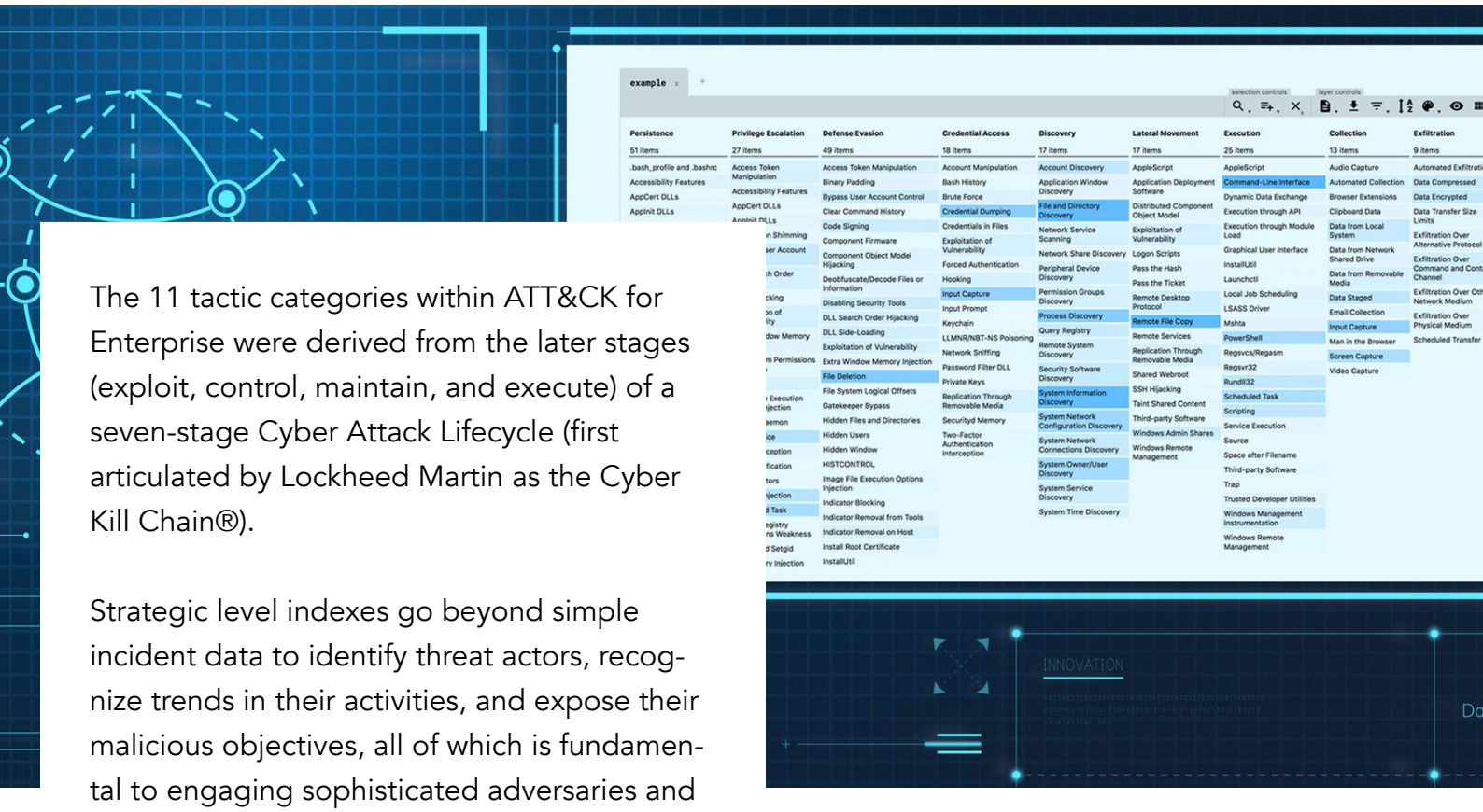
Techniques represent "how" an adversary achieves a tactical objective by performing an action. For example, an adversary may dump credentials to gain access to useful credentials within a network that can be used later for lateral movement. Techniques may also represent "what" an adversary gains by performing an action. This is a useful distinction for the 'discover' tactic since the techniques highlight what type of information an adversary going after based on a particular action.

Why is MITRE ATT&CK valuable?

Many organizations can benefit from using the MITRE ATT&CK framework. The framework provides a matrix view of all the techniques so that security analysts can see what techniques an adversary might apply to infiltrate their organization and get answers to questions like: Who is this adversary? What techniques and tactics are they using? What mitigations can I apply?

Security analysts can use the data from the framework as a detailed source of reference to manually enrich their analysis of events and alerts, inform their investigations and determine the best actions to take depending on relevance and sightings within their environment.

ATT&CK for Enterprise focuses on TTPs adversaries use to make decisions, expand access, and execute their objectives at a high enough level, widely across platforms with enough details to be technically useful.



The 11 tactic categories within ATT&CK for Enterprise were derived from the later stages (exploit, control, maintain, and execute) of a seven-stage Cyber Attack Lifecycle (first articulated by Lockheed Martin as the Cyber Kill Chain®).

Strategic level indexes go beyond simple incident data to identify threat actors, recognize trends in their activities, and expose their malicious objectives, all of which is fundamental to engaging sophisticated adversaries and building effective plans to defend one's organization, operations, and strategic objectives.

Using MITRE ATT&CK to map defenses and identify gaps

There are a number of ways an organization can use MITRE ATT&CK to map defenses and identify gaps. Here are the common use cases:

Adversary Emulation – ATT&CK can create adversary emulation scenarios to test and verify defenses against common adversary techniques.

Red Teaming – ATT&CK is used to design red team plans and organize operations to avoid certain defensive measures that may be in place within a network.

Behavioral Analytics Development – ATT&CK enables IT to construct and test behavioral analytics to detect adversarial behavior within an environment.

Defensive Gap Assessment – ATT&CK can help you run common behavior-focused adversary models to assess tools, monitoring, and mitigations of existing defenses within an organization's enterprise.

SOC Maturity Assessment – ATT&CK is employed as one measurement to determine how effective a SOC is at detecting, analyzing, and responding to intrusions.

Cyber Threat Intelligence Enrichment – ATT&CK helps you understand and document adversary group profiles from a behavioral perspective that is agnostic of the tools the group may use.

Using MITRE ATT&CK with cyber intelligence

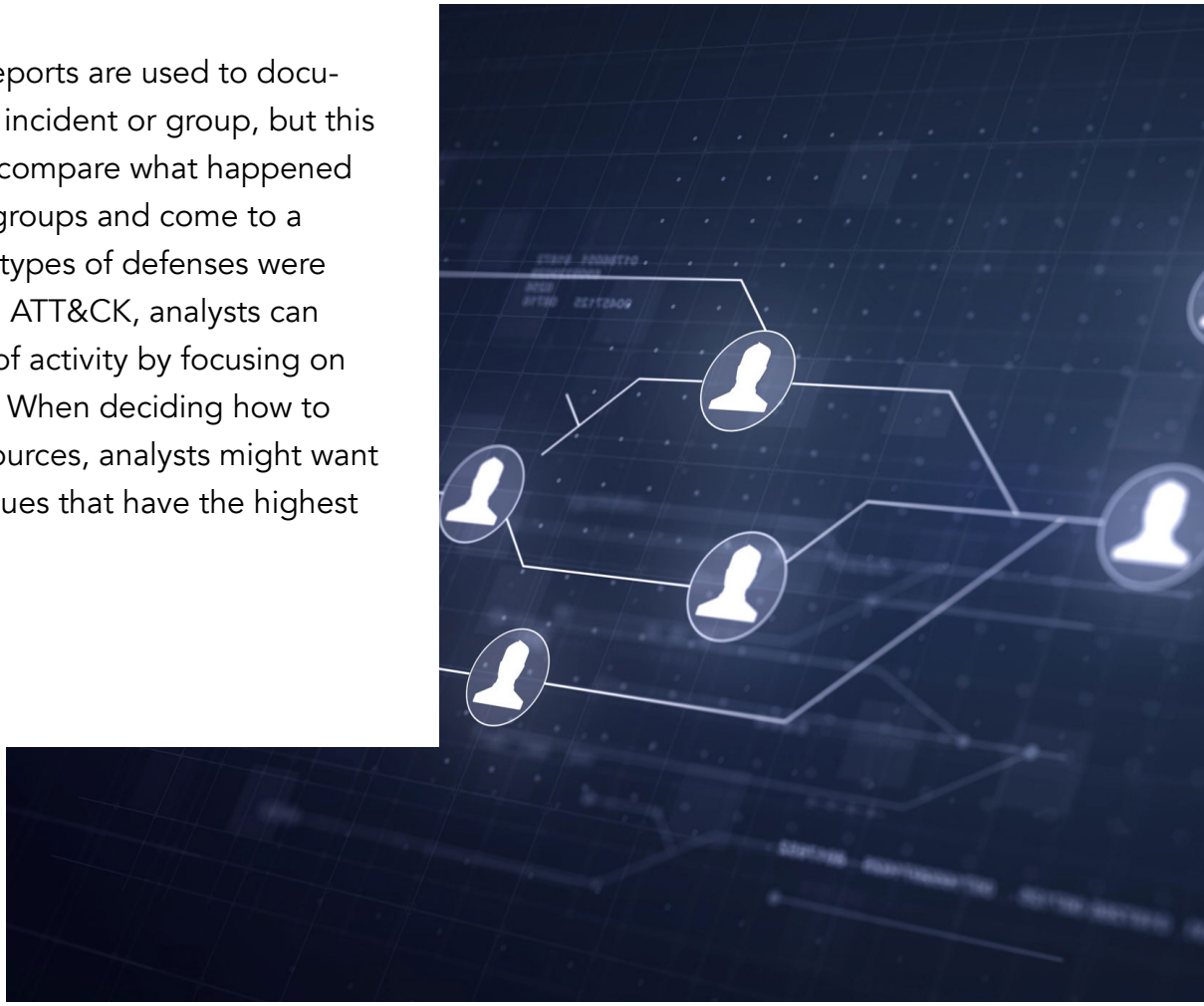
The value of cyber threat intelligence (CTI) is knowing what your adversaries do and applying that information to improve decision-making. For smaller organizations that want to start using the ATT&CK framework for threat intelligence, they can begin by taking a single threat group and examining their behaviors as structured in the framework. You might choose a threat group from those mapped out on the MITRE website based on who they've previously targeted.

Analysts and defenders can structure intelligence about adversary behavior and defenders can structure information about what behavior they can detect and mitigate. By overlaying information from two or more groups, you can create a threat-based awareness of what gaps exist that analysts know adversaries are exploiting.

How does MITRE ATT&CK help share threat intelligence?

Another important aspect of the ATT&CK framework is how it integrates CTI with the cyber security community. Unlike previous ways of digesting CTI that were used primarily for indicators, ATT&CK documents adversary group behavior profiles, such as APT29, based on publicly available reporting to show which groups use what techniques.

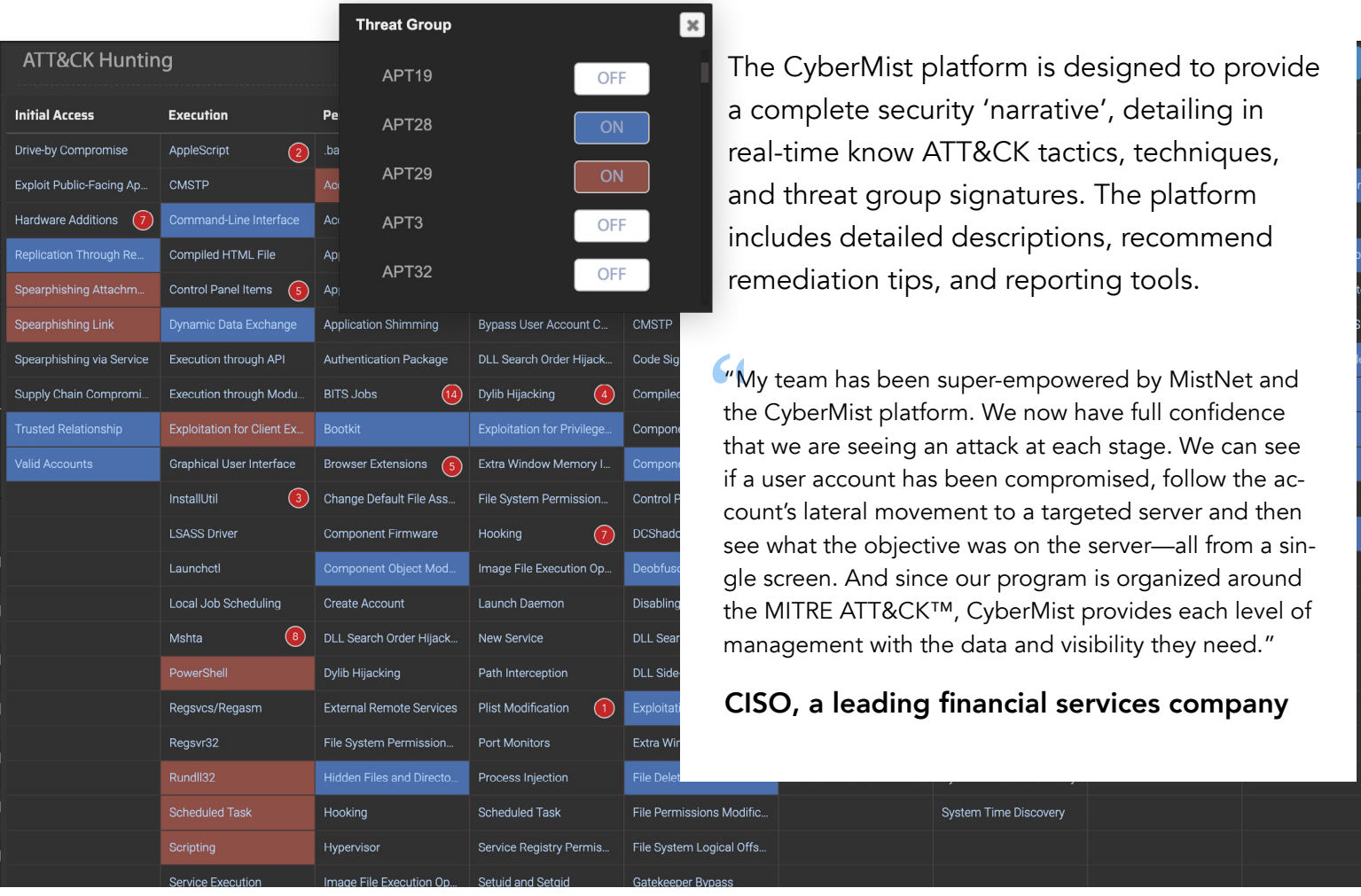
Usually, individual reports are used to document one particular incident or group, but this makes it difficult to compare what happened across incidents or groups and come to a conclusion on what types of defenses were most effective. With ATT&CK, analysts can look across groups of activity by focusing on the technique itself. When deciding how to focus defensive resources, analysts might want to start with techniques that have the highest group usage.



Why MistNet integrated MITRE ATT&CK into its CyberMist platform

IT teams are struggling to find security gaps, but due to lack of visibility, they don't know where those gaps are. In fact, according to new research, 20% of IT managers surveyed are unaware of how their most significant cyberattack entered their organizations. Also concerning, 17% don't know how long the threat was in the environment before it was detected.

To help with this, we've integrated the MITRE ATT&CK framework directly into our CyberMist threat detection platform, enabling automated detection and AI-assisted hunting mapped in real-time to the enterprise matrix. This allows IT security personnel to pinpoint suspicious activity identifying known tactics and threat groups in real time and reacting instantly to intrusions.



CyberMist integrated Mitre ATT&CK framework engine reveals tactics and threat groups in real time

The CyberMist platform is designed to provide a complete security 'narrative', detailing in real-time know ATT&CK tactics, techniques, and threat group signatures. The platform includes detailed descriptions, recommend remediation tips, and reporting tools.

> "My team has been super-empowered by MistNet and the CyberMist platform. We now have full confidence that we are seeing an attack at each stage. We can see if a user account has been compromised, follow the account's lateral movement to a targeted server and then see what the objective was on the server—all from a single screen. And since our program is organized around the MITRE ATT&CK™, CyberMist provides each level of management with the data and visibility they need."
>
> **CISO, a leading financial services company**

Learn more about real-time and historical visualization tools and how you can use CyberMist's AI-integrated Mitre ATT&CK™ framework tools to hunt for threats, run compliance checks, and measure overall SOC efficacy and maturity.

Turn Your **SOC Team** into a **SWAT Team**

CyberMist from MistNet

Schedule your free
MITRE ATT&CK assessment today »

About Us

MistNet was founded in 2016 with the simple mission of making the connected world a safer place. We focus our energies on securing large-scale complex enterprise environments.

We have developed disruptive technology using distributed AI and mist computing technology dramatically improving threat detection at scale and significantly reducing false positives. Our service is deployed in Fortune 1000 customers worldwide. We are backed by top-tier VCs with global headquarters in Mountain View, California.

Contact

info@mistnet.ai
(650) 665-9117

655 Castro Street, #3
Mountain View, CA 94041