opentext™

MITRE ATT&CK® framework and Managed XDR

Finding the real cyber attacks in the noise

opentext™

Contents

Challenges of managing XDR

When expanding their security field of vision to spot subtle attacks, organizations typically get buried in overwhelming amounts of data, distracting from the real problems.

Cyber attack surface has increased immensely with digital transformation and hybrid cloud adoption. Many Managed Security Services are only alert services, where 75 percent of businesses waste as much time on false positive alerts as they spend on legitimate attacks.[1] Everyone could benefit from an approach that ensures threat-informed detections cut through the noise to know what is actually on their network, endpoints, the cloud and beyond.

Mounting a great defence is about more than simply being vigilant; it is also about understanding what a serious threat is so the organization can optimize resources to counteract the offender's actions. Many organizations are facing shortfalls for skilled cybersecurity specialists[2] and an inability to respond fast enough to potential threats to mitigate risks.

Add to that defensive shortage the fact that bad actors are becoming ever more sophisticated and adept at breaching enterprise defences unnoticed. Increasingly, cyber attackers are playing a long game—embedding malicious software inside enterprise systems, building persistence and waiting for the opportune time to strike.

Rooting out what these bad actors have hidden can be both daunting and prohibitively time consuming. To be effective in shutting down potential trouble, it is essential to both recognize what is an actual threat and rapidly detect every real attack tactic.

1 SRS Networks, 75% of Businesses Waste Just As Much Time on False Positive Security Threats, Study Finds. (2021)

2 (ISC)², 2022 Cybersecurity Workforce Study. (October 2022)

opentext™

Introduction to MITRE

Spun out from the Massachusetts Institute of Technology in 1958, MITRE has undertaken to create a comprehensive list of known cyber attack tactics and techniques. Open to government, education and commercial organizations, the MITRE ATT&CK® framework is intended to create a standard taxonomy to improve communications regarding cyber attackers.

The first-ever independent MITRE Engenuity ATT&CK Evaluations for Managed Services[3] showed just how difficult it is to achieve and maintain that type of defensive posture. Sixteen leading cybersecurity providers opted to showcase their ability to identify and analyze a threat and describe adversary behavior, but only OpenText was able to minimize false positive noise to zero while identifying every attack vector that was deployed.[4]

With its Managed Extended Detection and Response (MxDR) solution, OpenText was the fastest in a field including some of the sector's top vendors,[5] identifying the threat actor and detecting every attack tactic within seven minutes while defending successfully against a simulated OilRig attack.

In a world where malicious actors continue to develop new attack vectors while organizations of all sizes attempt to keep up with the demand for skilled cybersecurity resources, an effective defense aligned with MITRE ATT&CK is something no one can afford to disregard.

On the ATT&CK

For those who are new to the MITRE ATT&CK concept, or who need a short refresher, these are the basics:

- MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
- The index continues to evolve with the threat landscape and has become a trusted knowledge base for the industry to understand attacker models, methodologies and mitigation.
- The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies.
- ATT&CK can be used in several ways to help security operations, threat intelligence and security architecture.
- ATT&CK is updated twice a year, using publicly available threat intelligence and incident reporting. The current version is #12.

As a knowledge base of commonly used techniques and tactics, MITRE ATT&CK is employed by organizations around the world to effectively identify the distinct stages of a cyber attack. Because most attacks use some aspect of the ATT&CK matrix over time, the framework provides effective enterprise detection and response techniques to actively recognize the various stages.

3 MITRE Engenuity ATT&CK Evaluations, OilRig Managed Services Evaluation 2022.

4 OpenText, OpenText is a leader in Detection and Response. (Nov. 9, 2022)

5 Participants in the evaluation included: Atos, Bitdefender, BlackBerry, BlueVoyant, Critical Start, CrowdStrike, Microsoft®, NVISO, OpenText, Palo Alto Networks, Rapid7, Red Canary, SentinelOne, Sophos, Trend Micro and WithSecure.

The winning formula

To score the highest results in MITRE Engenuity ATT&CK Evaluations—including eliminating false positives and scoring a 100 percent detection rate[6]—OpenText applied its advanced behavioral approach to threat detection.

Some key use cases for the MITRE ATT&CK framework include:

- Detection and Analytics
- Adversary Emulation and Red Teaming
- Threat Intelligence Assessments
- Engineering

As threat actors continue to gain sophistication, sharing tools and tactics, it grows increasingly important to have the tools to both protect and surveil organizations' entire system—network, endpoints, cloud and everything else. OpenText MxDR is a fully remote, cloud-based virtual security operations center that provides rapid detection, response and remediation of cyber threats.

Using behavioral analytics aligned to the MITRE ATT&CK framework, along with proprietary threat research, OpenText MxDR provides continuous threat monitoring in real time. It provides early detection in the cyber kill chain, digital forensic investigations, advanced threat hunting by a team of skilled specialists, along with incident response and remediation.

Through better vision and better response—OpenText MxDR empowers organizations to combat increasingly sophisticated threats while controlling ever-mounting costs.

About OpenText Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention to detection and response, to recovery, investigation and compliance, this unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio.

Powered by actionable insights from realtime contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

6 MITRE Engenuity ATT&CK Evaluations, OilRig Managed Services Evaluation 2022.

opentext.com/contact