SECURITY TAKE AWAY

powered by S@ND

# MITRE ATT&CK Matrix.
# Bedrohungsbasierte Abwehrstrategie - Was steckt dahinter?


Unser heutiges Thema: Wie kann die MITRE Matrix die IT-Security Ihres Unternehmens verbessern?

Erfahren Sie mehr über die hilfreichen Tools von "ATT&CK" und die neue „D3FEND" Variante, die das Mapping von Erkennungen noch einfacher macht.

Gleichzeitig werfen wir dabei einen Blick auf die IT-Abdeckung Ihres Unternehmens und wie Sie diese im Navigator-Tool festhalten können.

## MITRE - DIE ORGANISATION

MITRE

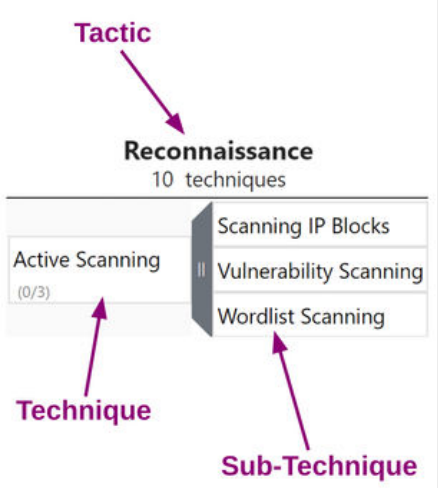
Das Wort MITRE hört man immer wieder im IT-Security Kontext. Wir wollen heute erklären, was sich hinter dem Begriff verbirgt und welchen Kontakt wir zu MITRE haben.

Auch wenn man MITRE oft mit Security in Verbindung bringt, so handelt es ich in erster Linie um ein nicht gewinnorientiertes Forschungsinstitut aus den USA. Der Name sieht zwar nach einer Abkürzung aus, hat aber tatsächlich keine Bedeutung. Ein Vorstandsmitglied entschied sich für diesen Namen, da er sich für ihn evokativ anhörte und keine Assoziation zu irgendwelchen Themen hat.
Außerhalb von der IT-Security ist die Organisation in den USA in unterschiedlichsten Bereichen vertreten und arbeitet unter anderem viel mit dem Militär zusammen.
In diesem NetDescribe TAKE AWAY geht es um die ATT&CK Matrix von MITRE, die wir genauer unter die Lupe nahmen.

## DIE MATRIX - WIE IST SIE AUFGEBAUT?

Die MITRE ATT&CK (**A**dversarial **T**actics, **T**echnique **and** **C**ommon **K**nowledge) Matrix beschreibt eine grafische Darstellung eines Security Frameworks zum besseren Verständnis und zur Kategorisierung von unterschiedlichen Vektoren, die von Angreifern bei einer Cyber-Attacke ausgenutzt werden.

Das Att&CK Framework hat sich weltweit etabliert. Viele Unternehmen und Organisationen nutzen es als Werkzeug, um existierende Angriffsmodelle besser zu verstehen, IT-Security-Risiken zu minimieren und als Standard zur Messung der bereits bestehenden IT-Security Abdeckung. Gleichzeitig dient das Framework als Wissenssammlung, deren Einträge häufig von Herstellern als Referenz genannt werden, so dass sich die Matrix immer mehr in die Richtung eines "Security Wiki" entwickelt.




Quelle: https://www.mitre.org/

Bei den Angriffsvektoren unterscheidet MITRE zwischen **tactics** und **techniques** zur Darstellung der Angriffswege.
Tactics beschreiben die Phase, in der sich ein Angreifer befindet, wie z. B. die Aufklärungsphase.
Darin befinden sich sogenannte techniques. Im abgebildeten Fall wäre unter anderem ein Portscan die Art des Angriffs. Fortführend gibt es sogenannte Sub-techniques die in ihrer Kategorie die Angriffe noch spezifischer beschreiben.

Darüber hinaus dokumentiert MITRE auch reale Cyberangriffe, die bestimmte TTPs verwendet haben und beschreibt, wie diese erkannt werden können. Ein passendes Beispiel hierfür ist WannaCry.

## DIE MATRIX - WIE KÖNNEN WIR SIE VERWENDEN?

Wie oben angesprochen, kann man mit der Matrix die IT-Security Abdeckung eines Unternehmens sehr gut festhalten. Hierfür gibt es von MITRE das Navigator Tool.
Der ATT&CK-Navigator ist ein webbasiertes Tool zur Kommentierung und Erkundung von ATT&CK-Matrizen. Es kann zur Visualisierung der Defensivabdeckung, der Planung und Priorisierung von Korrelationssuchen und vielem mehr verwendet werden.

Für **Splunk** Nutzer besteht außerdem die Möglichkeit, die Splunk die MITRE App zu verwenden, um Alarme mit den dort bestehenden Techniques zu mappen. MITRE dokumentiert alle Einträge mit einzigartigen Kennungen, so ist das Beispiel des aktiven Scannens in MITRE unter dem Code T1595 zu finden. Diese Codes erweisen sich immer wieder hilfreich bei der Recherche von bereits bestehenden Splunk Suchaufträgen oder auch Artikeln.

Aktuell arbeitet MITRE auch an einer "D3FEND" Variante der Matrix, um das Mappen von Erkennungen noch einfacher zu machen. Diese befindet sich noch in der Beta Phase, ist aber bereits einen Blick wert.

Das war unser TAKE AWAY - wie immer mit wichtigen Infos in Kürze erklärt.
Unsere Empfehlung: Bei ATT&CK sowie auch bei D3FEND einfach mal reinklicken und schauen, was sich spannend anhört! Denn selber erkunden macht immer noch am meisten Spaß ;)

**Sie wollen mehr zum Thema IT Security wissen? Kontaktieren Sie uns.**

**Und im nächsten TakeAway erfahren Sie mehr zu SMishing. Seien Sie gespannt!**

NETDESCRIBE
Member of xantaro group

CALL FOR APPOINTMENT

089 215 48 68 0

info@netdescribe.com

S@ND
MANAGED SECURITY SERVICES @NETDESCRIBE
Wir gehen auf Ihre individuellen Wünsche und Anforderungen ein. Unsere Services sind das Tuning für Ihre IT-Security und nicht die Serienausstattung.