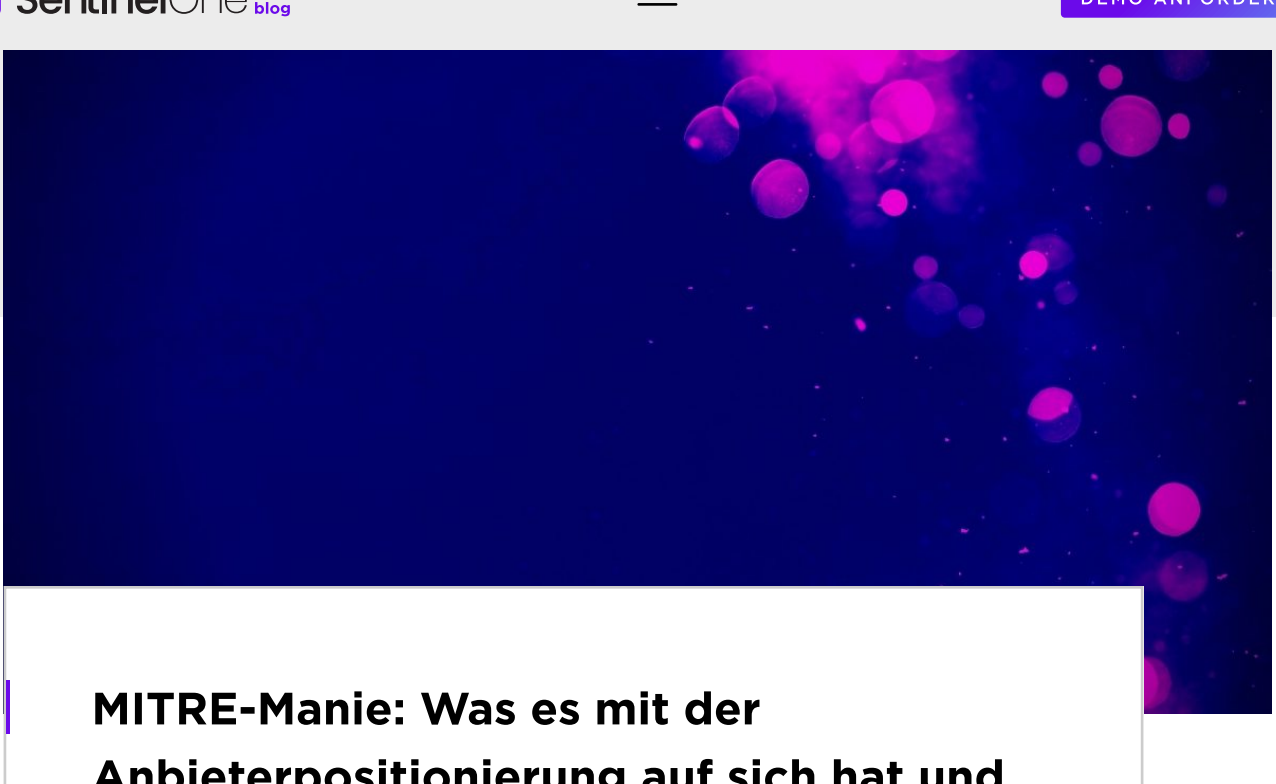
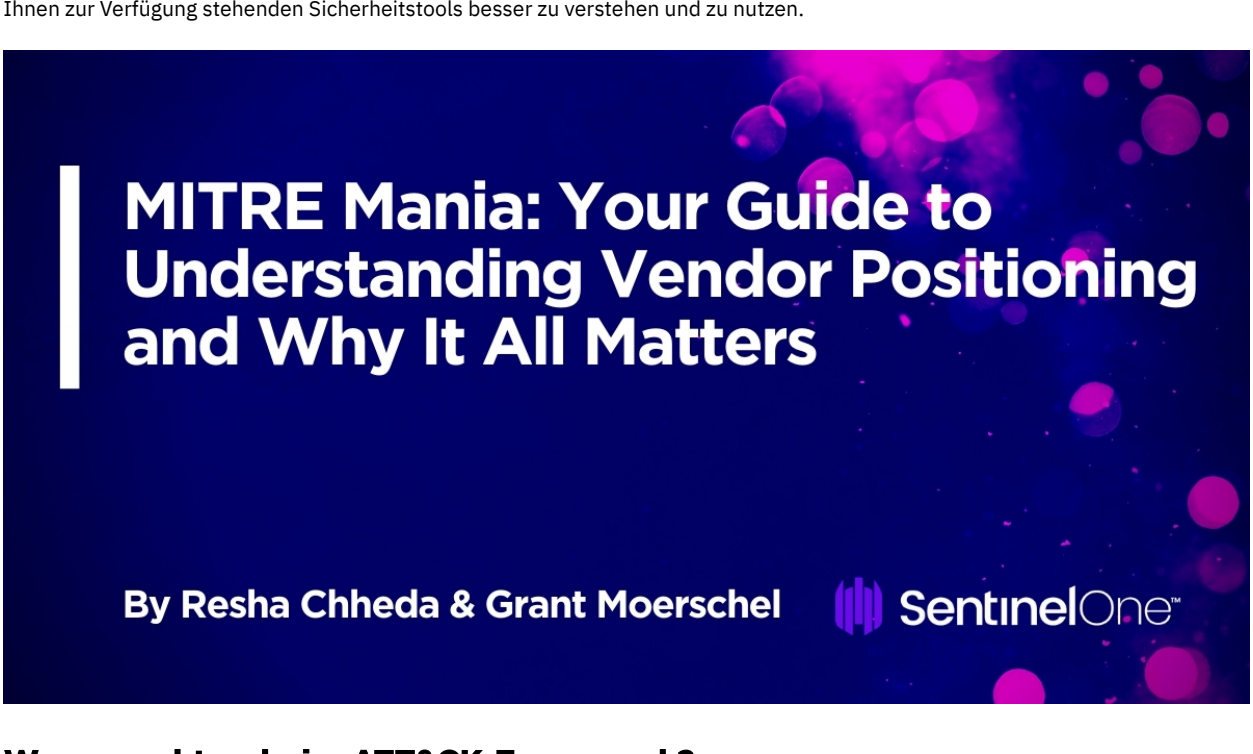


MITRE-Manie: Was es mit der Anbieterpositionierung auf sich hat und worum es eigentlich geht

April 15, 2021
by SentinelOne

Es ist wieder soweit: Die Testrunde der MITRE Engenuity ATT&CK Evaluations (im Folgenden ATT&CK-Bewertungen genannt) für das Jahr 2021 ist abgeschlossen und Technologen in aller Welt warten nun auf die Ergebnisse. Wir bei SentinelOne sind nach wie vor begeisterte Anhänger von MITRE Engenuity. Das Unternehmen entwickelt und erweitert eine gemeinsame Cybersicherheitssprache, mit der sich die Vorgehensweise von Angreifern beschreiben lässt. Sie profitieren von dieser mühevollen Kleinarbeit, denn in den ATT&CK-Bewertungen werden all die Kräfte der Menschen gebündelt, die an vorderster Front unermüdlich ihre Infrastruktur und Ressourcen vor skrupellosen Angreifern schützen, welche an Geld gelangen, Chaos stiften oder jemandes Lebenswerk stehlen wollen. Wenn Anbieter die ATT&CK-Bewertungen nutzen – oder besser: Wenn Anbieter die ATT&CK-Bewertungen *vollständig umsetzen*, haben ihre Produkte und Services das Potenzial, Abwehr- und Reaktionsmaßnahmen potenziell zu vereinfachen, zu beschleunigen und wirksamer zu machen.

Dieser Beitrag richtet sich an CISOs, SOC-Analysten und Architekten. Er erläutert die Meinung von SentinelOne zu den ATT&CK-Bewertungen 2021, die Bedeutung dieser Bewertungen für Ihr Unternehmen und wie Sie die Ergebnisse nutzen können, um die Ihnen zur Verfügung stehenden Sicherheitstools besser zu verstehen und zu nutzen.



Worum geht es beim ATT&CK-Framework?

Im Schach gibt es drei taktische Spielphasen: die Eröffnung, das Mittelspiel und das Endspiel. In jeder Spielphase wird das Spiel durch mehrere Züge von einer Phase zur nächsten vorangetrieben. Während sie mit verschiedenen Strategien auf das Schachmatt hinarbeiten, wenden Spieler je nach spielerischem Können unterschiedlich ausgereifte Techniken an.

In der realen Welt haben wir es mit Angreifern zu tun, die mit leicht unterschiedlichen Methoden Schach spielen. Sie alle nutzen Tools und entwickeln Vorgehensweisen und Ansätze, um ihre Ziele zu erreichen. Sie verknüpfen legitime und untypische Verhaltensweisen zu unterschiedlichen Angriffsmustern – und wissen alle ganz genau, was sie wollen.

Mithilfe der ATT&CK-Bewertungen können wir beschreiben, wie und warum sie etwas tun. Das MITRE ATT&CK-Framework ist *„eine gut gepflegte Wissensdatenbank und ein Modell für die Verhaltensweisen von Cyberangreifern. Es beinhaltet die verschiedenen Phasen eines Angriffslebenszyklus von Angreifern und die Plattformen, die sie bekanntlich ins Visier nehmen“*. Sein Zweck ist die Schaffung einer gemeinsamen Sprache, deren Bestandteile endlos kombiniert werden können, um die Vorgehensweise von Bedrohungsakteuren zu beschreiben.

Lassen Sie uns das näher erläutern. Der erste zentrale Begriff ist *Phasen*. Ein Angreifer geht in mehreren Phasen vor, um ein Ziel zu erreichen. Ein allgemeines Beispiel:

```
Erstzugang → Erkennung → Laterale Bewegung → Erfassung → Exfiltration
```

In diesem linearen Beispiel besteht die Strategie des Angreifers – sein Ziel – letztendlich darin, Ihre Daten zu exfiltrieren. Die Vorgehensweise des Angriffs lässt sich in 5 taktische Phasen unterteilen, wobei der erste Schritt der Erstzugang und der fünfte Schritt die Exfiltration darstellt. Das Framework MITRE Engenuity ATT&CK Evaluations besteht aktuell aus 14 Taktiken, wie Sie auf der X-Achse des Enterprise Navigator-Tools erkennen können (Hinweis: Klicken Sie auf „Create New Layer“ (Neue Ebene erstellen) und dann auf „Enterprise“ (Unternehmen)).

Der zweite zentrale Begriff aus dem obigen Zitat ist *Verhaltensweisen*. Kriminelle setzen bei jedem Schritt bestimmte Verhaltensweisen gegen Sie ein. Dabei handelt es sich um die Techniken, die sie in der jeweiligen taktischen Phase anwenden. Um zum Beispiel Erstzugang zu erlangen (Taktik Nr. 1 von oben), versendet der Angreifer eventuell eine Phishing-E-Mail mit einem Link zu einer kompromittierten Webseite, die eine ungepatchte Sicherheitslücke im Browser ausnutzt. Das ATT&CK-Framework umfasst momentan mehr als 200 Techniken (auf der Y-Achse des Navigator-Tools), die den 14 Taktiken zugeordnet sind.

Auf der nächsten Stufe sind die von Angreifern verwendeten *Prozeduren*. Als Prozeduren werden die genauen Mechanismen einer Technik bezeichnet.

Zum Erreichen des Endziels ist daher eine Anfangstaktik mit einer oder mehreren Techniken erforderlich, auf die eine weitere Taktik mit Techniken folgt, und so weiter. Das geht so lange, bis das Ziel des Angreifers erreicht ist. Durch die Einteilung in allgemeine Taktiken bis hin zu speziellen Prozeduren erhalten wir die TTPs – *Taktiken, Techniken, Prozeduren*.

Welche Bedeutung haben die Bewertungen vom MITRE Engenuity ATT&CK-Framework?

Die Emulationen der MITRE Engenuity ATT&CK-Bewertungen sind so aufgebaut, dass sie die bekannten TTPs eines Angreifers nachahmen. Sie werden unter kontrollierten Laborbedingungen ausgeführt, um die Wirksamkeit jedes teilnehmenden Anbieterprodukts zu bestimmen. MITRE Engenuity beschreibt das wie folgt:

„Die ATT&CK-Bewertungen setzen Angreifer-Emulationen ein. Die Tests laufen also ‚im Stil‘ eines Angreifers ab. Dadurch können wir Tests mit einer relevanten Teilmenge von ATT&CK-Techniken durchführen. Zur Erstellung unserer Emulationspläne nutzen wir öffentliche Berichte mit Bedrohungsdaten, ordnen sie ATT&CK zu und legen dann fest, wie wir die Verhaltensweisen replizieren.“

Es geht darum, einen vollständigen logischen Angriff zusammenzustellen, der alle Phasen eines umfassenden erfolgreichen Angriffs durchläuft – von der ersten Kompromittierung bis hin zu Persistenz, lateraler Bewegung, Datenexfiltration und so weiter.

Das ATT&CK-Framework bietet Verantwortlichen, Sicherheitsexperten und Anbietern einen gemeinsamen Wortschatz und unterstützt uns mit diesem Wissen in der Bemühung um eine bessere Cybersicherheit.

Daraus ergeben sich drei Vorteile:

1. Wir erhalten einen Einblick in die Strategie des Angreifers bezüglich der Kombination von Taktiken und Techniken.
2. Wir können die genaue Art einer Bedrohung klar kommunizieren und dank eines besseren Verständnisses schneller reagieren.
3. Wenn wir wissen, wer unsere typischen Angreifer sind und wie sie vorgehen, können wir proaktiv Abwehrmaßnahmen treffen, um uns besser gegen sie zu schützen.

MITRE Engenuity betont, dass es ein „Angreifer-Modell der mittleren Ebene“ und somit weder zu allgemein, noch zu spezifisch ist. Modelle der höheren Ebene wie die Lockheed Martin Cyber Kill Chain® veranschaulichen die Ziele von Angreifern – es bleibt jedoch unklar, wie diese Ziele konkret erreicht werden. Umgekehrt dazu definieren Exploit- und Malware-Datenbanken ganz gezielt konkrete IoC-Puzzlestücke (Indicators of Compromise, Kompromittierungsindikatoren) in einem riesigen Puzzle. Sie erklären jedoch nicht, wie Kriminelle sie einsetzen und geben üblicherweise auch nicht an, wer die Kriminellen sind. Das TTP-Modell von MITRE Engenuity stellt den goldenen Mittelweg dar. Hier werden Taktiken als schrittweise Zwischenziele dargestellt und mit den Techniken wird veranschaulicht, wie jede Taktik umgesetzt wird.

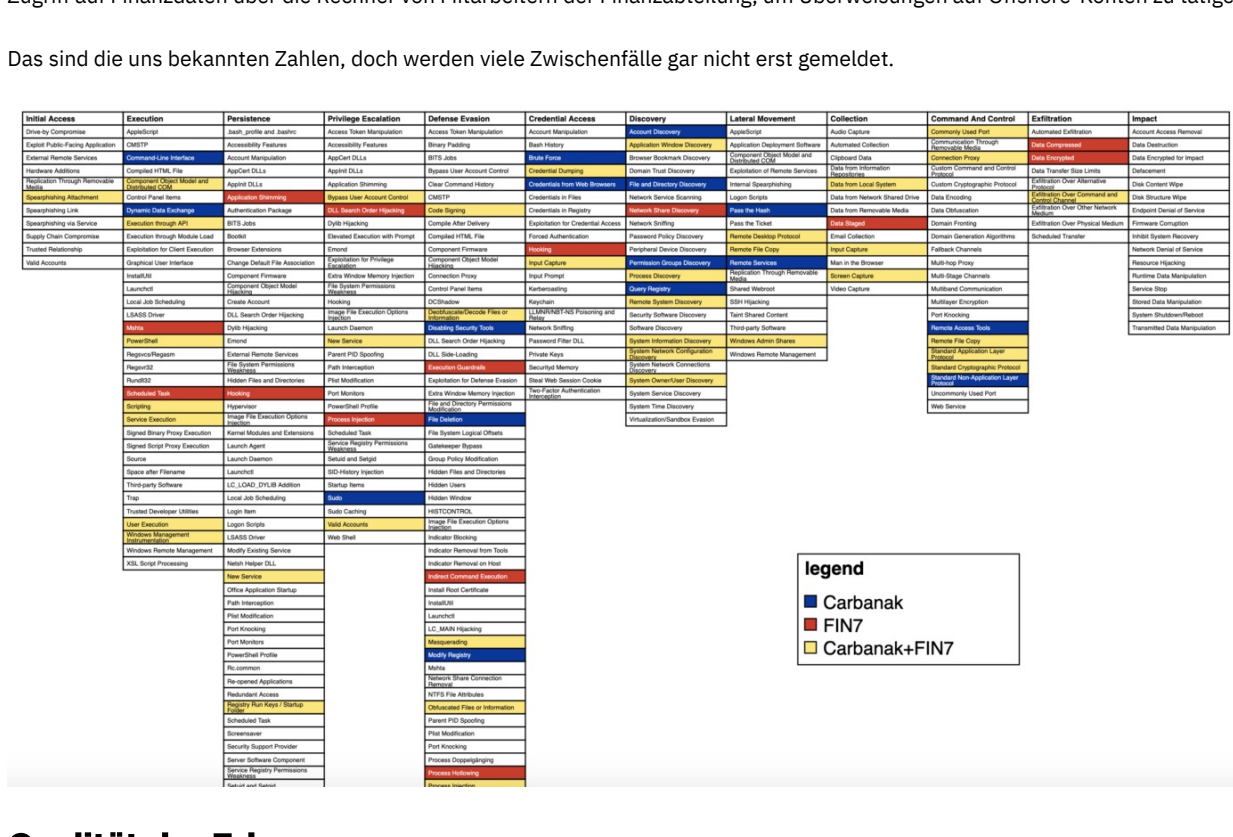
ATT&CK-Bewertungen 2021

Da MITRE Engenuity während der Bewertungen mit den Anbietern zusammenarbeitet, ist MITRE Engenuity quasi das „Red Team“. Der Anbieter, der für MITRE Engenuity Erkennung und Reaktion bereitstellt, ist dagegen das „Blue Team“. Zusammen bilden sie ein „Purple Team“, das bei den Echtzeit-Tests der Sicherheitskontrollen hilft, indem es die Art von Ansätzen emuliert, mit denen Eindringlinge wahrscheinlich in einem echten Angriff vorgehen würden. Die Emulationen basieren dabei auf den bekannten, tatsächlich beobachteten TTPs.

Während sich die ATT&CK-Bewertungen 2019 (das erste Testjahr) um APT3 (Gothic Panda) drehten und die ATT&CK-Bewertungen im Jahr 2020 auf die mit APT29 (Cozy Bear) verbundenen TTPs fokussiert waren, geht es in den diesjährigen Bewertungen um die Emulation der Bedrohungsgruppen Carbanak und FIN7.

Die Geschichte der weitreichenden Auswirkungen von Carbanak und FIN7 wurde umfassend dokumentiert. Carbanak wird der Diebstahl von insgesamt 900 Millionen US-Dollar von Banken und mehr als eintausend Privatkunden angelastet. FIN7 soll für den Diebstahl von mehr als 15 Millionen Datensätzen von Kundenkreditkarten aus der ganzen Welt verantwortlich sein. Das Hauptziel der böswilligen Aktivitäten ist der Diebstahl finanzieller Ressourcen von Unternehmen (z. B. Geldkarteninformationen) oder der Zugriff auf Finanzdaten über die Rechner von Mitarbeitern der Finanzabteilung, um Überweisungen auf Offshore-Konten zu tätigen.

Das sind die uns bekannten Zahlen, doch werden viele Zwischenfälle gar nicht erst gemeldet.



Qualität der Erkennung

ATT&CK bewertet nicht die Leistung von Anbietern, sondern konzentriert sich darauf, wie es im Verlauf der einzelnen Testschritte zu den Erkennungen kam. Seit mehreren Jahren betont SentinelOne genau das, was MITRE Engenuity im Bewertungsleitfaden anschaulich darstellt: Nicht jede Erkennung hat die gleiche Qualität. Eine „Telemetrie“-Erkennung beispielsweise enthält minimal verarbeitete Daten zu einem Angreiferverhalten. Am anderen Ende des Qualitätsspektrums dagegen ist eine „Technik“-Erkennung reich an Informationen und gibt Analysten auf einen Blick Orientierung. Konsistente, auf Techniken fokussierte Erkennungen sind ideal für Unternehmen, die mehr aus ihren Tools herausholen wollen.

> Die wichtigste Information aus diesem Blogartikel ist die Erkenntnis, dass Anbietertools idealerweise die Erstellung von Echtzeitkontext zu Angreiferbewegungen automatisieren und dies im Tool mit so wenigen Warnmeldungen wie möglich sichtbar machen sollten. Je mehr Techniken ein Tool automatisch erkennen und anschließend zu nur einer Zwischenfallwarnmeldung aggregieren kann, desto besser kann das Tool Sicherheitsfunktionen automatisieren. Dies ist entscheidend, um die mittlere Zeit bis zur Reaktion so gering wie möglich halten.

Mehr Informationen zu den Erkennungstypen:

- **„Tactic“ (Taktik) und „Techniques“ (Techniken):** Dies sind die hochwertigsten Erkennungen, die ein Tool liefern kann. *Taktiken* liefern Analysten Informationen zu Aktivitätsabsichten (Warum tun sie das? Was wollen sie damit erreichen?). *Techniken* liefern Analysten Informationen darüber, wie Aktionen ausgeführt wurden, oder helfen dabei, die tatsächlichen Ereignisse festzustellen.
- **„General“ (Unbestimmt) und „Telemetry“ (Telemetrie):** Diese Erkennungstypen liegen weiter unten auf der Qualitätsskala und sind von eher einfacher Natur. Allein betrachtet liefern *unbestimmte* und *Telemetrie*-Erkennungen Analysten weniger Kontext und gelten somit eher als Rohdaten. Hinweis: Wenn Anbieter eine *Technik* erhalten, bekommen sie oft ebenfalls eine *Telemetrie*. Erhalten Sie jedoch nur eine einfache *Telemetrie* (da das Tool nicht genug Datenpunkte korrelieren kann), wird diese nicht durch die aussagekräftigere *Technik* ergänzt.
- **„Configuration Change“ (Konfigurationsänderung) und „Delayed“ (Verzögert):** Dies sind Testmodifikatoren. *Konfigurationsänderung* signalisiert, dass ein Anbieter seine Konfiguration mitten im Test „optimiert“ hat. *Verzögert* bedeutet, dass eine Erkennung für die Testaufsicht aufgrund einer verzögerten Verarbeitung nicht sofort verfügbar war.

> Idealerweise verändern Anbieter ihre Produktkonfigurationen nicht mitten im Test. Alle Erkennungen sollten in Echtzeit und ohne Verzögerung verfügbar sein.

In den ATT&CK-Bewertungen 2021 wurden zwei bedeutende Weiterentwicklungen eingeführt: Tests in **Linux-Umgebungen** sowie die Überprüfung von **Schutzmaßnahmen**.

Die Endergebnisse werden am 20. April 2021 veröffentlicht. Bis dahin müssen wir abwarten. Möchte jemand eine Runde Schach spielen?

Wie finden sich CISOs am besten in den Anbieterpositionierungen zurecht, um die Ergebnisse zu interpretieren?

Für CISOs kann es eine echte Herausforderung sein, sich in den Anbieterpositionierungen zurechtzufinden. Hier sind einige Tipps:

- **Vorsicht bei zu vielen Fehlern, Verzögerungen und Konfigurationsänderungen**
  Anbieter, die zu viele Erkennungsfehler haben… mehr muss nicht gesagt werden. Anbieter, die viele Verzögerungen aufweisen, bekommen ihre Erkennungen üblicherweise durch Mittel außerhalb des normalen Workflows des Tools zuerkannt. Das bedeutet, dass Ihre Mitarbeiter auf die gleiche Weise verfahren müssen, um diese Ergebnisse zu erzielen. Anbieter mit vielen Konfigurationsänderungen hatten das Bedürfnis, ihre Erkennungsfunktionen mitten im Test zu modifizieren. Hier stellt sich die Frage, ob die Änderungen einem nachvollziehbaren Zweck geschuldet waren oder ob der Test dadurch manipuliert wurde.
- **Vorsicht bei einer hohen *Telemetrie*-Zahl und einer niedrigen *Techniken*-Zahl**
  Wenn Anbieter ihre hohen *Telemetrie*-Zahlen in den Vordergrund stellen, ohne auf viele *Techniken* verweisen zu können, kann das Tool Ereignisse nicht automatisch korrelieren. Das bedeutet, dass Ihre Mitarbeiter diese Korrelation manuell durchführen müssen oder dass es eventuell große Verzögerungen und Ungenauigkeiten beim Herstellen von Zusammenhängen gibt. Hier auftretende Verzögerungen führen zu Reaktionsverzögerungen, was wiederum das Risiko erhöht.
- **Vorsicht vor Anbietern, die ihr eigenes Bewertungssystem erfinden**
  Wir haben viele Anbieter gesehen, die ihre schlechten Ergebnisse mit Statistiken und Zahlen verschleiern, die sie gut aussehen lassen, in Wirklichkeit jedoch völliger Unsinn sind. Angaben wie „Kontext pro Warnmeldung“ und „100-prozentige Erkennung“ (obwohl es eindeutig fehlende Erkennungen gab) sind lächerlich. Lesen Sie das Kleingedruckte.

In Bezug auf Produktarchitekturen werden CISOs erkennen, dass diese produktorientierten Grundsätze mit den Zielen von MITRE Engenuity vereinbar sind:

- **Überblick und Abdeckung durch EDR sind Mindestanforderungen**
  Eine erstklassige EDR-Lösung kann Daten skalierbar sowie kostengünstig erfassen und korrelieren, indem sie das Potenzial der Cloud nutzt. Alle relevanten Datenelemente sollten erfasst werden – mit wenigen oder ohne Fehlerkennungen –, um dem SecOps-Team einen umfangreichen Überblick zu bieten. Die Erfassung aller Daten und Ereignisse ist das Fundament für EDR und sollte als Mindestanforderung und wichtige MITRE Engenuity-Metrik eingestuft werden.
- **Maschinell erstellter Kontext und automatische Korrelation sind unverzichtbar**
  Der Begriff Korrelation beschreibt den Aufbau von Beziehungen zwischen winzig kleinen Datenpunkten. Die Korrelation sollte möglichst von der Maschine in Maschinengeschwindigkeit durchgeführt werden, sodass Analysten keine Zeit mit der manuellen Verknüpfung von Daten verschwenden müssen. Zudem sollte die Korrelation bei Bedarf für einen längeren Zeitraum in ihrem ursprünglichen Kontext abrufbar sein.
- **Die Zusammenführung von Konsolen-Warnmeldungen ist äußerst wichtig**
  Mehr Signal, weniger Rauschen – eine Herausforderung für SOC- und IR-Teams, die mit Informationen überlastet werden. Das bereits überlastete SOC-Team sollte nicht zusätzlich mit Warnmeldungen zu jedem einzelnen Telemetrie-Element in einem Zwischenfall ermüdet werden. Sorgen Sie stattdessen dafür, dass die Lösung Datenpunkte automatisch in zusammengeführte Warnmeldungen gruppiert. Im besten Fall kann eine Lösung ähnliche Aktivitäten in zusammengefasste Warnmeldungen korrelieren, die Einblicke auf Kampagnenebene bieten. Dadurch reduziert sich der erforderliche manuelle Aufwand, die „Warnmeldungsmüdigkeit“ verringert sich und es sind deutlich weniger Kenntnisse erforderlich, um auf Warnmeldungen reagieren zu können. Diese Maßnahmen führen für das Security Operations Center (SOC) zu besseren Ergebnissen in Form von kürzeren Eindämmungszeiten und insgesamt verringerten Reaktionszeiten.

Wie sollten CISOs das ATT&CK-Framework in ihrem Unternehmen einsetzen?

Mit den folgenden bewährten Methoden können CISOs und Sicherheitsteams ihre Sicherheit stärken:

- **Entwickeln Sie eine Cybersicherheitsstrategie.** Entwickeln Sie mithilfe von ATT&CK eine Cybersicherheitsstrategie. Richten Sie Ihr Verteidigungssystem auf die Abwehr von Techniken ein, die bekanntlich gegen Unternehmen wie Ihres eingesetzt werden und statten Sie Ihr System mit Überwachungstechnologie aus, die Hinweise auf ATT&CK-Techniken in Ihrem Netzwerk erkennt.
- **Führen Sie Angreifer-Emulationspläne durch.** Erstellen Sie mithilfe von ATT&CK Angreifer-Emulationspläne, mit denen Sie die Leistung Ihres Red Teams verbessern können. Das Red Team kann eine konsequente und gut organisierte Methode für die Definition von Taktiken und Techniken bestimmter Bedrohungen entwickeln und umsetzen. Anschließend bewertet es die Umgebung, um festzustellen, ob die Abwehrmaßnahmen wie erwartet funktionieren.
- **Erkennen Sie Lücken im Verteidigungssystem.** Die ATT&CK-Matrices können Blue Teams dabei unterstützen, Bestandteile eines potenziellen oder laufenden Cyberangriffs besser zu verstehen. Dies ermöglicht ihnen, Lücken im Verteidigungssystem zu erkennen und Lösungen dafür zu implementieren. In ATT&CK-Dokumenten werden Behebungen und kompensierende Kontrollen für Techniken empfohlen, für die Sie tendenziell anfällig sind.
- **Integrieren Sie Bedrohungsdaten.** ATT&CK kann Ihre Bedrohungsdaten wirksam in Cybersicherheitsmaßnahmen integrieren. Wenn Sie Bedrohungen bestimmten Angreifertechniken zuordnen, können Sie Lücken aufdecken, Risiken bestimmen und planen, welche Behebungsmaßnahmen Sie anschließend implementieren sollten.

Fazit

MITRE Engenuity ATT&CK Evaluations treibt mit seinen herausragenden Leistungen die Entwicklung der Sicherheitsbranche weiter voran und bringt dringend benötigte Transparenz und unabhängige Tests in den EDR-Bereich. Als Führungskraft oder Sicherheitsexperte sollten Sie nicht *nur* auf die Zahlen schauen, sondern das große Ganze betrachten und Anbieter danach beurteilen, ob sie einen guten Überblick und hochwertige Erkennungen liefern und gleichzeitig Ihr Sicherheitsteam entlasten.

Für die nahe Zukunft freuen wir uns, Ihnen Details zur **Teilnahme von SentinelOne an den MITRE Engenuity ATT&CK Evaluations 2021** ankündigen zu können. Die Ergebnisse werden hier veröffentlicht, sobald sie verfügbar sind. Wenn Sie in der Zwischenzeit mehr darüber erfahren möchten, wie die SentinelOne Singularity-Plattform Ihr Unternehmen bei der Umsetzung dieser Ziele unterstützen kann, kontaktieren Sie uns oder fordern Sie eine kostenlose Demo an.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security