10 Wege, das **MITRE ATT&CK-Framework in die Praxis umzusetzen**

Ein Leitfaden zur Erstellung einer analysegestützten IT-Bedrohungsabwehr

splunk> turn data into doing™

10 Wege, das MITRE ATT&CK-Framework **in die Praxis umzusetzen**

Das MITRE ATT&CK-Framework gibt es schon seit Jahren. Aber erst jetzt erleben wir, dass Unternehmen es in stärkerem Maß einsetzen. Grund dafür ist, dass sie erkennen, wie wichtig ein starkes IT-Sicherheitsteam ist. Zusätzlich werden mehr Mittel zur Erhöhung der Qualität von Informationssicherheits-Programmen zur Verfügung gestellt.

Unternehmen investieren in mehr als reine Präventionstechnologien. Während sie sich von einem herstellerorientierten Ansatz zu einem analysegesteuerten Sicherheitsansatz weiterentwickeln, bauen Sie gleichzeitig Früherkennungs- und Incident-Response-Kapazitäten auf.

Sowohl für IT-Sicherheitsexperten als auch für Unternehmen, die versuchen, ihre Sicherheitsprogramme zu verbessern, ist es wichtig, zu verstehen, welche Taktiken und spezifischen Techniken unterschiedliche Bedrohungsgruppen bei Cyberangriffen nutzen.

> **„In einer Digitalisierten Welt sind Daten die Grundlage für IT-Sicherheitsteams, um strategisch Cyberangriffe zu Erkennen und darauf zu Reagieren. Damit werden Unternehmen, Kunden und Mitarbeiter vor Cyberbedrohungen geschützt.“**
>
> – Matthias Maier, CISSP & CEH, Sicherheitsexperte, Splunk

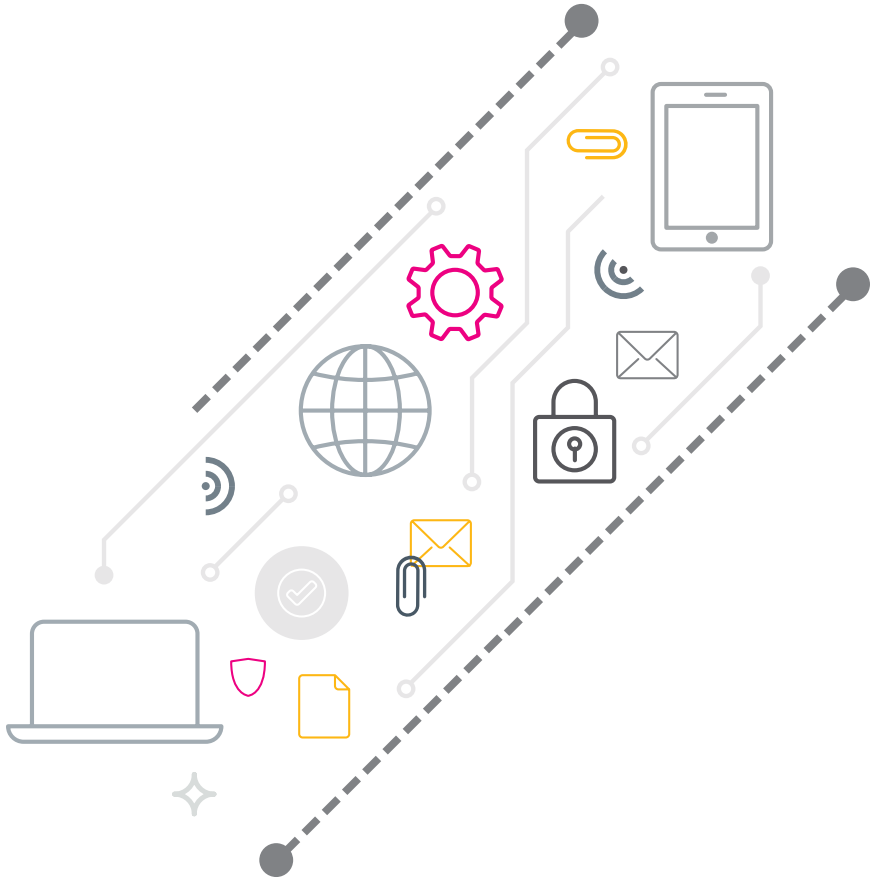
Diese Vorgehensweise unterstützt Unternehmen dabei, Cyber-Risiken besser zu managen und hilft zu planen, welche Daten sie zur Untersuchung eines Sicherheitsvorfalls benötigen. Außerdem können damit Früherkennungsindikatoren eingerichtet werden, bei denen herkömmliche präventionsbasierte Technologien versagen würden oder für die die jeweilige Unternehmenspolitik zu restriktiv wäre.

Das MITRE ATT&CK-Framework ist nicht nur für Sicherheitsexperten relevant. Es gibt diverse Möglichkeiten, es zu verwenden, um Transparenz zu erhöhen und die Effektivität der Sicherheitsbemühungen eines Unternehmens deutlich zu machen – die Größe des Sicherheitsteams spielt dabei nicht einmal die entscheidende Rolle. Suchen Sie ein Beispiel, wie das MITRE ATT&CK-Framework aussieht? Dann schauen Sie sich diesen Blog an.

Lernen Sie, wie unterschiedliche Teams **vom MITRE ATT&CK-Framework profitieren**

In diesem E-Book untersuchen wir, wie das MITRE ATT&CK-Framework verschiedene Teile des Unternehmens bei unterschiedlichen Aktivitäten unterstützt. Hierzu gehören:

1. Entwicklung einer „prevent, detect, respond & improve“-Strategie durch den Head of Security Operations
2. Schnelle Reaktion mittels Analysen durch Security Content Developer/das Blue Team
3. Validierung der Gefahrenabdeckung durch SIEM-Architekten
4. Rechtfertigung von Datenanforderungen des SOC-Ingenieurs gegenüber den IT-Ops-Teams
5. Dokumentieren und Treffen von Risikoentscheidungen auf Grundlage von Log- und Komponentenabdeckung durch den IT-Sicherheitsmanager
6. Begründung und Differenzierung von Investitionen auf Basis der Asset-Kritikalität sowie die Entwicklung einer entsprechenden Roadmap durch CISOs (Chief Information Security Officer)
7. Entwicklung eines risikobasierten Benachrichtigungsmodells (Risk-Based Alerting, RBA) durch SOC-Analysten
8. Qualitätssicherung des Data-Onboardings und Festlegung des Abdeckungsbedarfs durch SIEM-Admins
9. Dokumentation und Kommunikation der unternommenen Verbesserungsmaßnahmen durch Penetration Tester/Red Teams
10. Ermöglichen Sie Einkaufsabteilung und IT-Leitern, sowohl taktische Basislinien für die IT-Sicherheit als auch den Bedarf an Incident Response und Monitoring festzulegen.



1

Ermöglichen Sie dem Leiter Ihres Security Operations-Teams, eine Strategie zu entwickeln, die auf Prävention, Erkennung, Reaktion und Verbesserung basiert.

Mit den im MITRE ATT&CK-Framework dokumentierten Techniken können Unternehmen, eine Roadmap erstellen, die über reine Prävention hinausgeht und sich auf das Erkennen und Abwehren von Gefahren sowie die Verbesserung von Security-Prozessen konzentrieren.

Das SIEMENS EAGLE Datacenter-Sicherheitsteam verfolgt genau diesen Ansatz und hat damit einen Prozess zur Qualitätssicherung und kontinuierlichen Verbesserung aufgebaut. Die oberste Priorität des Teams ist es, jede mögliche Bedrohung zu verhindern. Wenn das Team etwas nicht verhindern kann, will es die Bedrohung frühzeitig erkennen und darüber benachrichtigt werden. Dann reagiert das Team: Es führt eine Untersuchung durch, informiert sich über den Fall und passt entweder die Erkennung an oder konfiguriert nach Möglichkeit eine Präventionsmaßnahme zur Verbesserung.

Ein ähnliches Konzept ist im NIST Cybersecurity Framework dokumentiert, das auf den Grundbausteinen “Erkennen des Risikos (Identify), Schützen (Protect), Ermitteln (Detect), Reagieren (Respond) und Wiederherstellen (Recover)” beruht.

„Wir möchten so viel wie möglich im Vorfeld mit Prävention abfangen, damit wir uns nicht täglich damit befassen müssen. Wenn es im Vorfeld nicht möglich ist, möchten wir Bedrohungen adäquat erkennen und in angemessener Weise reagieren. Das Wissen, das wir aus dem Tagesgeschäft gewinnen, fließt in die Verbesserungen ein, sodass wir die Situation morgen unter Kontrolle haben.”

– Oliver Kollenberg, EAGLE DataCenter, Siemens AG

Allgemeine Darstellung der Kernfunktionen des NIST CyberSecurity-Frameworks zurStrukturierung grundlegender Cybersicherheitsaktivitäten.

Die Grundlage beider Beispiele bildet ein Sicherheitsteam mit einer Verteidigungsmentalität, die auf Bedrohungsinformationen basiert sowie die Verfügbarkeit der richtigen Daten, anhand derer das Team Fragen formulieren kann, was in der Umgebung passiert.

2

Ermöglichen Sie Security Content Developern/dem Blue Team, mittels Analysen schnell zu reagieren.

Das MITRE ATT&CK-Framework ermöglicht es Blue Teams und Security Content Developern, neue Cyberangriffe, die öffentlich bekannt geworden sind, schnell den jeweils verwendeten Techniken zuzuordnen. Darüber hinaus können mithilfe des Frameworks Datenbedürfnisse identifiziert und Analysen erstellt werden. Dies ermöglicht eine Gefahrenerkennung in den verschiedenen Phasen der von Angreifern verwendeten Taktiken.

„Fokussieren Sie sich auf die Erkennung der Vorgehensweise, nicht des Angriffs. Wahrscheinlich sind Sie mit der Kill Chain oder dem MITRE ATT&CK-Framework vertraut. Wenn Sie nur versuchen, den eigentlichen Angriff zu entdecken, haben Sie wahrscheinlich nicht immer Glück. Wenn Sie Analysen in der Delivery-, Exploitation- und in der C2-Phase durchführen, können Sie die Vorgehensweise erkennen“.

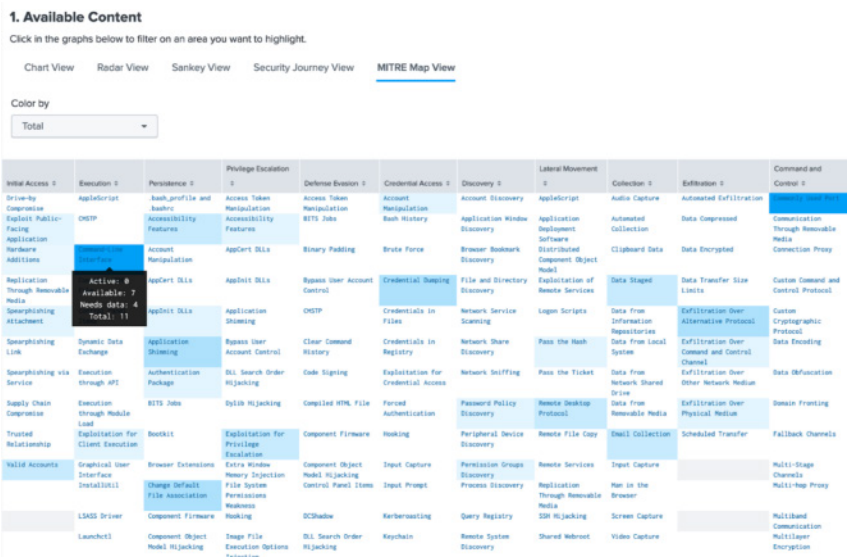
“Unser schnellster Turnaround für die Entwicklung eines neuen Erkennungsverfahrens für Angriffe betrug zwei Stunden, nachdem wir von einem neuen Verhalten erfahren hatten. Sich an den Anbieter zu wenden, ihm zu erklären, dass eine neue Angriffsart vorkommt und ihn zu bitten, sein Produkt entsprechend upzudaten ist keine Option, denn darauf können Sie dann 3 Monate warten.”

–Jonathan Pagett, Head of Security Defense Center, Bank of England

3

Ermöglichen Sie SIEM-Architekten, die Gefahrenabdeckung zu validieren und den jeweiligen Umsetzungsgrad zu messen.

Für SIEM-Architekten ist es schwer die Frage zu beantworten, wie viel und was tatsächlich von ihrem SIEM abgedeckt wird, insbesondere wenn die Abdeckung durch mehr als die Systeme oder Systemkomponenten definiert werden muss, die Logdaten liefern. Es muss definiert werden, ob die richtigen Systemaktivitäten zu einem protokollierten Event führen. Und es muss festgestellt werden, ob die SIEM Regeln und Analysen nach den richtigen Dingen suchen. Daher eignet sich das MITRE ATT&CK-Framework ideal als Übersicht zur SIEM-Abdeckung für SIEM-Architekten.



Tabellarische Auflistung aller Taktiken und Techniken in ATT&CK unter Hervorhebung der in Splunk verfügbaren Analysen. Sie können Inhalte mit den Status “Aktiv” (Active), “Verfügbar, aber nicht aktiv” (Available) oder “Daten erforderlich” (Needs data) hervorheben. Je dunkler die Farbe, desto mehr Inhalte sind vorhanden. Quelle: Analytics Advisor in der Splunk Security Essentials-App (Version 2.4)

4

Ermöglichen Sie SOC-Ingenieuren, Datenanforderungen gegenüber IT Operations-Teams zu rechtfertigen.

In der Regel ist der SOC-Ingenieur nicht für den operativen Betrieb der zu schützenden Systeme oder Anwendungen verantwortlich. Es kann eine unangenehme Aufgabe sein, dafür zu sorgen, dass das SOC-Team über die erforderliche Transparenz verfügt. Insbesondere zu kommunizieren, dass die richtigen Arten von Aktionen geprüft und gespeichert werden, kann vom IT Operations Team Zeit für die Überprüfung der Protokollierungsebenen und Konfigurationen erfordern.

Das MITRE ATT&CK-Framework ermöglicht es SOC-Ingenieuren, zu dokumentieren und zu kommunizieren, warum sie Events aus bestimmten Aktivitäten benötigen, z. B. wenn scheduled tasks auf einem Windows-Computer erstellt werden oder PowerShell verwendet wird. Darüber hinaus ermöglicht es IT Operations-Teams zu entscheiden, auf welche Weise Daten erfasst werden sollen, je nach der für die Architektur am besten geeigneten Technologie – z. B. durch das native Sammeln von Endpunktaktivitäten mit einer Sysmon-Konfiguration von SwiftOnSecurity oder durch eine bereitgestellte Lösung zum Schutz von Endpunkten.

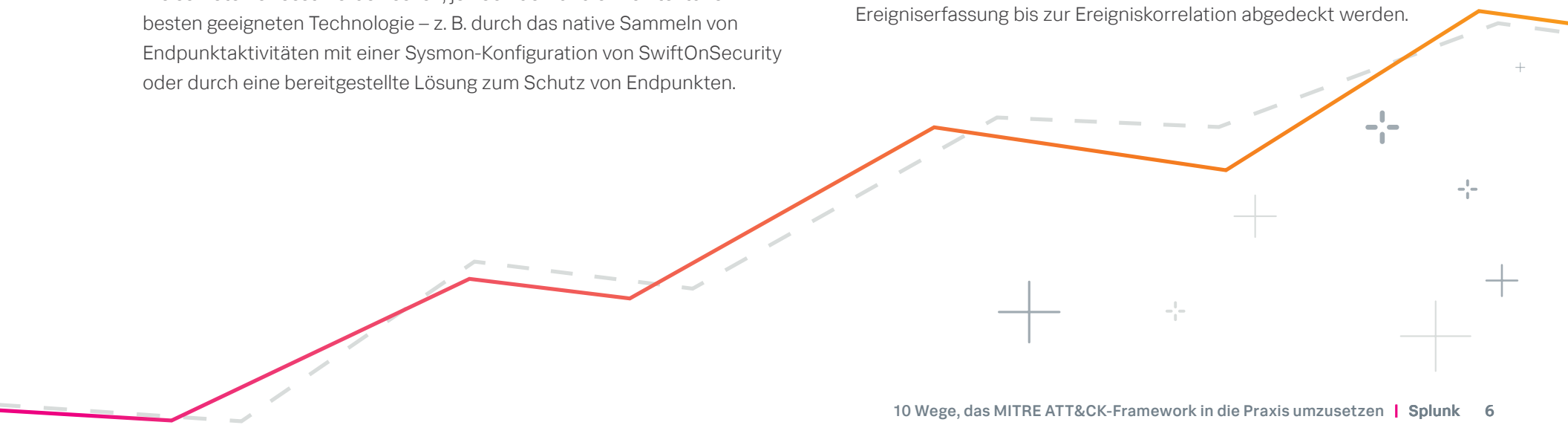
5

Ermöglichen Sie IT-Sicherheits-managern, Risikoentscheidungen zur Abdeckung von Logs und Komponenten zu treffen und zu dokumentieren.

Das MITRE ATT&CK-Framework ermöglicht es IT-Sicherheitsmanagern, Überwachungs- und Logging-Richtlinien innerhalb der Sicherheitskontrollen einer Organisation genauer zu spezifizieren. Dadurch kann beispielsweise ein SOC-Ingenieur das festgelegte und akzeptable Risikoniveau einer Organisation besser verstehen.

So definiert beispielsweise die ISO/IEC 27002 in den Richtlinien des Abschnitts Event Logging, dass Event Logs bei Relevanz unter anderem Systemaktivitäten enthalten sollen.

Das MITRE ATT&CK-Framework gibt einem IT-Sicherheitsmanager die Möglichkeit, eine Kontrolle beispielsweise in folgender Weise zu definieren: [10 %] der Techniken in jeder Taktik müssen von der Ereigniserfassung bis zur Ereigniskorrelation abgedeckt werden.



6

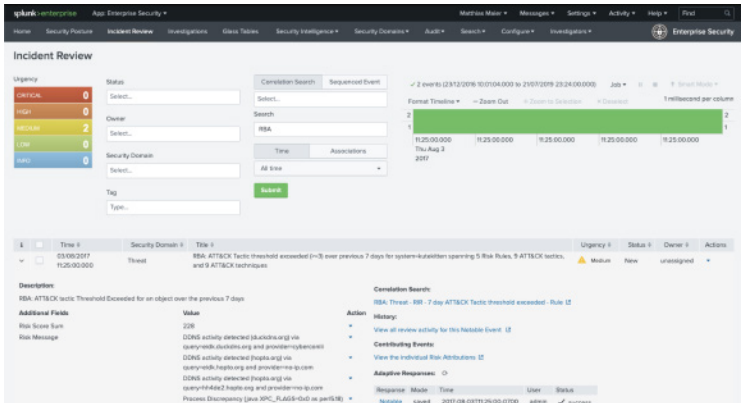
Ermöglichen Sie CISOs, den Sicherheitsstatus zu verbessern, das Monitoring auszubauen und neue Investitionen zu rechtfertigen.

Anstatt eine einheitliche Sicherheitsrichtlinie für sämtliche Fälle zu haben, ermöglicht das ATT&CK-Framework CISOs einen Sicherheitsstatus aufzubauen, der auf den individuellen Bedürfnissen und dem Risikoprofil des jeweiligen Unternehmens basiert. Durch Rückverfolgung spezifischer Risiken, tatsächlich erfolgter Angriffe, Bedrohungsgruppen und dokumentierter APT-Bedrohungsberichte, kann das Sicherheitsmanagement Lücken in seiner Strategie identifizieren und eine Roadmap zur Stärkung der Unternehmenssicherheit erstellen. Dies kann beispielsweise mehr Mitarbeiter, höhere Transparenz oder neue Sicherheitstools bedeuten. Das ATT&CK-Framework ermöglicht CISOs, Sicherheitsmaßnahmen basierend auf Abstraktionsebene, Anwendungskritikalität oder Protokollstufen zu fokussieren. Beispielsweise können die Schwachstellen essenzieller Assets durch eine bestimmte Reihe von MITRE-Techniken abgedeckt sein, während andere Techniken weniger relevant für die Unternehmensbedürfnisse sind – ein CISO gestaltet ein SOC unter Umständen so, dass mehr Ressourcen in Techniken investiert werden, die wichtigere Assets schützen, sodass sichergestellt wird, dass die richtigen Daten häufiger gesammelt und im Fall eines größeren Sicherheitsvorfalls zentral verfügbar gemacht werden.

7

Ermöglichen Sie SOC Analysten, ein risikobasiertes Benachrichtigungsmodell (RBA) zu entwickeln.

Während SIEM Content Developer Erkennungsmechanismen für MITRE ATT&CK-Techniken erstellen und bereitstellen, können SOC-Analysten von der Menge der generierten Benachrichtigungen überlastet sein. Um zu einer Priorisierung von MITRE ATT&CK-Techniken zu gelangen, können Benachrichtigungen konvertiert und als Signale betrachtet werden. Signale wiederum schreiben einer Ressource einen Risikowert zu. Basierend auf der Art der Technik und dem beobachteten Verhalten kann der Risikowert höher sein, oder es kann ausgehend von der involvierten Ressource oder dem involvierten Benutzer ein Multiplikator für die Berechnung hinzugefügt werden. Dies ermöglicht eine Abstraktionsebene für SOC-Analysten, die dabei hilft, dass sie nicht in der Flut der Benachrichtigungen untergehen. So können sie sich stattdessen auf die Ressourcen oder Benutzer mit der höchsten Risikoeinstufung konzentrieren.



Benachrichtigungstitel: RBA: ATT&CK-Schwellenwert für Taktik hat (>=3) über die letzten 7 Tage für System=kutekitten überschritten und 5 Risikoregeln, 9 ATT&CK-Taktiken und 9 ATT&CK-Techniken abgedeckt Risk Score Summe: 228; Quelle: Splunk Enterprise Security

8

Ermöglichen Sie SIEM-Admins, die Data-Onboarding-Qualität sicherzustellen und den Abdeckungsbedarf festzulegen.

Die Arbeit des SIEM-Administrators wird erleichtert, wenn sowohl das Security Operations Team als auch das Unternehmen als Ganzes identifizieren können, welche Daten, Protokolle und Ereignisse sie für die Bekämpfung von Bedrohungen, das Sicherheits-Monitoring oder die Untersuchung von Incidents benötigen. Mithilfe des MITRE ATT&CK Frameworks kann der SIEM-Administrator die Daten während des Onboarding-Prozesses überprüfen und so sicherstellen, dass die Anforderungen des SOC erfüllt werden oder ggf. über zusätzlich erforderliche Werkzeuge entscheiden. Die Simulation von Bedrohungsaktivitäten und Anomalien ist ein zusätzlicher Mechanismus zur Sicherstellung der Datenqualität und -abdeckung.

> **„Simulieren Sie Angreifer und generieren Sie Daten, um zu überprüfen, ob Ihre Erkennungsmechanismen End-to-End funktionieren.“**
>
> – Dave Herrald, Staff Security Strategist, Splunk

9

Ermöglichen Sie Penetration Testern und Red Teams, Verbesserungsmaßnahmen zu dokumentieren und zu kommunizieren.

Penetration Tester und Red Teams haben die Aufgabe, Schwachstellen in einem Informationsnetzwerk zu finden. Die meisten dieser Teams fragen dann zu allererst danach, wo sich Schwachstellen befinden. Aber eine ebenso wichtige Frage - die häufig gar nicht gestellt wird - bezieht sich auf die Aktivitäten, die zu der Attacke führten, aber durch das SOC nicht aufgedeckt wurden. Lange Rede, kurzer Sinn: egal ob Sie mit einem Penetration Testing-Team eines Drittanbieters oder mit Ihrem internen SOC arbeiten, das MITRE ATT&CK-Framework ist eine hervorragende Möglichkeit zur Standardisierung der Kommunikation. Sobald alle mit demselben Framework arbeiten, ist es einfacher und effektiver, die bei der Überprüfung verwendeten Taktiken und Techniken zu untersuchen und die Schwachstellen im Sicherheitssystem zu bestimmen.

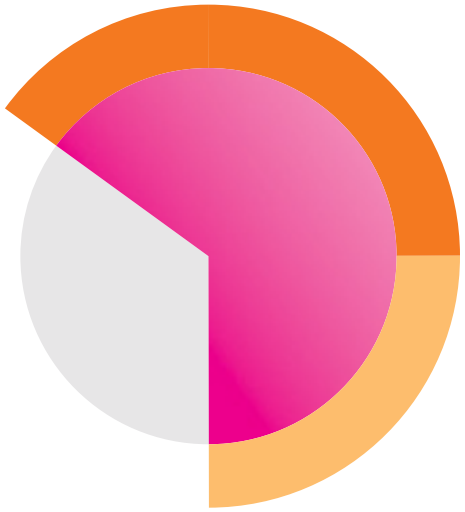
10

Ermöglichen Sie Einkaufsabteilung und IT-Leitern, sowohl taktische Basislinien für die IT-Sicherheit als auch den Bedarf an Incident Response und Monitoring festzulegen.

Der Einkauf von Tools und Services von Drittanbietern gehört heute für IT-Leiter und Führungskräfte zum Tagesgeschäft. Für diese Anbieter ist es von größter Wichtigkeit sicherzustellen, dass ihre Produkte sicher sind und Compliance-Anforderungen entsprechen. Sie werden darüber hinaus regelmäßig durch ihre Kunden und Aufsichtsbehörden auditiert, um zu gewährleisten, dass ihre Leistungen sicher sind. Das MITRE ATT&CK-Framework ist eine gute Möglichkeit, Anforderungen detaillierter zu definieren und sogar noch über IT-Governance-Frameworks, wie z. B. ISO27001- oder NIST-800-53-Zertifizierungen, hinauszugehen. Insbesondere in einem Modell der gemeinsamen Verantwortung (Shared Responsibility Model), bei dem die Zuständigkeit für bestimmte Teile des Services beim Informationssicherheitsteam eines Unternehmens verbleibt, ist es von entscheidender Bedeutung, dass der Serviceanbieter die automatisierte Erfassung von Audit-Trails ermöglicht und sicherstellt, dass in diesen Audit-Trails die richtigen Event-Daten erfasst werden. Der Schlüssel zum Erfolg ist hier die Definition der „richtigen Event-Daten“ auf einer Abstraktionsschicht, unabhängig von Anbieterarchitektur, Bedrohungsentwicklung oder neuen Betriebssystemen mit neuen Funktionen, die Angreifer nutzen könnten.

„In einer digitalisierten Welt sind Daten die Grundlage für IT-Sicherheitsteams, um strategisch Cyberangriffe zu erkennen und darauf zu reagieren. Damit werden Unternehmen, Kunden und Mitarbeiter vor Cyberbedrohungen geschützt.“

– Matthias Maier, CISSP & CEH, Sicherheitsexperte, Splunk



Erste Schritte.

Haben Sie die richtigen Daten? Stellen Sie die richtigen Fragen?

Finden Sie heraus, was mit Splunk und der Kraft der Search Processing Language (SPL) möglich ist. Testen Sie die Splunk Security Essentials App auf Splunkbase.

20-47401-10-Ways-to-Take-Your-MITRE-ATT_CK-From-Plan-to-Action-DE-103-11x8.5-EB

splunk> turn data into doing™