Das SecOps-Handbuch zu TDIR

splunk>
a CISCO company

Es gibt wieder viel Wirbel um die jüngsten Cyberbedrohungen – kampferprobte Sicherheitsanalysten wissen das nur zu gut. Mutierte Malware erreicht neue Höchststände, KI eröffnet neue Angriffsvektoren, und kriminelle Banden werden immer einfallsreicher. (Und ihre Namen auch – oder was hätten Sie sich unter „Peach Sandstorm“ vorgestellt?) Klar ist: Security-Analysten haben es nicht leicht. Und glauben Sie uns – wir wissen das.

Von Jahr zu Jahr wird es schwieriger, mit den Anforderungen der Cybersicherheit Schritt zu halten. Gleichzeitig drohen Security-Teams in der Datenflut zu versinken und verlieren viel Zeit mit Log-Analysen in diversen Einzeltools – nur um zur rechten Zeit die richtigen Daten finden und schützen zu können. Laut unserem Lagebericht Security berichten 51 % der Befragten, dass sich ihre Tools schlecht integrieren lassen, und 46 % verbringen mehr Zeit mit Tool-Wartung als mit Verteidigung.

Mehr ~~Geld~~ Security-Tools, mehr Probleme

Der aktuelle ESG-Report zum SOC-Markt zeigt: Unternehmen betreiben eine Art Bäumchen-wechsel-dich-Security. Analysten springen von Tool zu Tool und wühlen sich durch Unmengen von Logs. Das kostet Zeit und erschwert es, rechtzeitig zu relevanten Erkenntnissen zu kommen.

Gartner zufolge wird sich das Datenvolumen, das Unternehmen on premises, am Edge und in Public Clouds erfassen, bis 2028 verdreifachen. Es müssen also noch mehr Daten überwacht und geschützt werden..

Deshalb brauchen Analysten eine einheitliche Sicht auf ihre Umgebung und Daten. Nur so lassen sich Events effektiv filtern, korrelieren und kontextualisieren – und irrelevante Warnmeldungen reduzieren. So bleibt SecOps mehr Zeit fürs Wesentliche.

Einfachheit ist der Schlüssel zur Security-Modernisierung

Aus all diesen Gründen überdenken viele Teams aktuell ihren Datenmanagement-Ansatz. Ziel ist ein SOC, das die Grenzen zwischen Erkennung, Untersuchung und Reaktion aufhebt. Wenn Systeme verschlankt, Tools integriert und Workflows durchgängig abgestimmt sind, wird Security-Arbeit deutlich effizienter – mit weniger Routineaufwand. Klingt gut doch, oder?

Die Devise lautet: TDIR

TDIR (Threat Detection, Investigation and Response) ist ein gemeinsamer Satz von Abläufen, mit dem die Security-Fachleute alles handlich beisammen haben, inklusive Workflows, Security-Tools und Daten.

Im Prinzip ist TDIR ein Plattform-Ansatz, der Bedrohungserkennung, Untersuchungen und automatische Reaktionen vereint. TDIR bedeutet freilich nicht, dass die Sicherheitsteams nichts mehr zu tun hätten – es ist ein wiederkehrender Prozess mit drei Kernphasen:

- **Bedrohungserkennung:** Ihr Sicherheitsteam entdeckt ungewöhnliches Verhalten im Netzwerk, z. B. dass jemand auf große Mengen sensibler Daten zugreift. Dies löst eine Warnmeldung wegen Verdacht auf Insider-Bedrohung bzw. Datenexfiltration aus.
- **Untersuchung:** Analysten untersuchen das Event und sehen sich die jüngsten Aktivitäten des Users an, die Netzwerk-Logs und weitere Datenquellen. Vielleicht ergibt sich, dass der Account durch einen Phishing-Angriff kompromittiert ist und das ungewöhnliche Verhalten zu einem laufenden Angriff gehört. Weil sensible Daten betroffen sind, stuft das Team den Incident als hohes Risiko ein.
- **Reaktion:** Das Sicherheitsteam handelt sofort, isoliert das kompromittierte Konto, ändert die Passwörter und blockiert die IP-Adresse der Angreifer. Außerdem schließt sich das Team mit der IT kurz, damit alle bekannten Schwachstellen rasch geschlossen werden.

Der Kern einer TDIR-Plattform ist eine moderne SIEM-Lösung (Security Information and Event Management), mit der Sie Folgendes erreichen:

- **Umfassende Übersicht schaffen.**
  Sie aggregieren die Logs der einzelnen Geräte, Endpunkte und Anwendungen, sodass Sie einen zentralen Überblick über Ihre Sicherheitslage bekommen.
- **Bedrohungserkennung optimieren.**
  Sie analysieren den Netzwerkverkehr und das Verhalten der Endpunkte, sodass Sie Anomalien erkennen können, die unter Umständen auf eine Sicherheitsverletzung hindeuten.
- **Untersuchungen und Threat Hunting beschleunigen.**
  Sie fokussieren auf Anzeichen von Schadaktivitäten und können so neuen und aufkommenden Bedrohungen zuvorkommen.
- **Reaktionen orchestrieren und automatisieren.**
  Wiederkehrende Aufgaben automatisieren Sie, damit Sie sich auf eingehende Analysen und Aufgaben mit hoher Priorität konzentrieren können.

Die einzelnen Phasen gehen ineinander über: Die Untersuchung baut auf den Daten der ersten Erkennung auf, die Reaktion stützt sich auf die in der vorherigen Phase gewonnenen Erkenntnisse.

TDIR hilft gegen eine ganze Reihe von SOC-Ärgernissen

- Manuelle Untersuchungen
- Digitale Komplexität
- Mangelnde Transparenz
- Unzureichender Kontext
- Fachkräftemangel

Das SOC der Zukunft

Eine Plattform, die den TDIR-Prozess vereinheitlicht, ist von entscheidender Bedeutung, wenn es darum geht, ein SOC aufzubauen, das sich angesichts neuer Bedrohungen als resilient erweist. Dem Cisco Cybersecurity Readiness Index zufolge gehen fast 75 % der Unternehmen davon aus, dass sie in den nächsten beiden Jahren von einem Cyber-Incident betroffen sein werden. 84 % der leitenden Führungskräfte zählen Effektivität und Effizienz zu den fünf wichtigsten Prioritäten. Vor diesem Hintergrund machen sich die Unternehmen an die SecOps-Modernisierung. Konkret geht es darum, wie sie in der digitalen Transformation mit Datenvolumen und Komplexität zurande kommen.

Das Geheimnis erfolgreicher Security-Modernisierung liegt in der Einfachheit. Im Wesentlichen beseitigt das SOC der Zukunft die Barrieren zwischen Erkennung, Untersuchung und Reaktion. Durch die Integration der zuvor getrennten Tools und durch die die Koordinierung der Workflows ist weniger lästige Handarbeit erforderlich, was die Arbeit der Analysten erheblich erleichtert.

Was Sie im SOC der Zukunft erreichen

- Große Datenmengen managen und schützen, unter Wahrung von Compliance und Governance.
- Risiken und Schwachstellen minimieren, durch konkrete Maßnahmen wie Security-Audits, Patches und strenge Zugangskontrollen.
- Security Operations mit KI und maschinellem Lernen schärfen, beschleunigen und treffsicherer machen – für optimale Erkennungen, Analysen und Reaktionen auf Bedrohungen.
- Bedrohungen erkennen und mit fortschrittlichen Technologien wie Verhaltensanalysen und integrierter Threat Intelligence auch komplexe oder noch unbekannte Bedrohungen identifizieren.
- Wiederkehrende Sicherheitsaufgaben automatisieren (z. B. Priorisierungen, Warnmeldungen, Patching) – das steigert die Effizienz, minimiert menschliches Versagen und verschafft den Analysten Luft für wichtigere Aufgaben.

Tools, die zusammenwirken, gehören zusammen

Sehen wir uns an, wie sich eine einheitliche TDIR-Lösung zu anderen Tools auf dem Markt verhält.

SIEM + TDIR

Die SIEM-Technologie ist die Grundlage einer einheitlichen TDIR-Lösung, weil Unternehmen damit überschauen, wie die Daten aus unterschiedlichen Systemen und Domänen zusammenspielen. Durch die Integration verschiedener Tools und Ansichten in ein Gesamtsystem ist eine SIEM-Lösung ein Cybersecurity-Ansatz, der viel proaktiver (und ganzheitlicher) ist, vor allem in Kombination mit Machine-Learning-Funktionen. Ein SIEM hilft den SecOps-Teams u. a. bei diesen Aufgaben:

- Entscheidende Erkenntnisse zutage fördern.
- Incidents priorisieren, auf der Basis integrierter Bedrohungsinformationen.
- Flexible Untersuchungen durchführen – für effektives Threat Hunting.

Ein SIEM ist ideal für kontinuierliches Monitoring, Echtzeit-Erkennungen, Untersuchungen und automatisierte Reaktionen. Ein SIEM kann den Sicherheitsteams helfen, das Chaos der Warnmeldungen in relevante, umsetzbare Informationen zu verwandeln, sodass sie sich auf das konzentrieren können, worauf es wirklich ankommt.

XDR/EDR/NDR + TDIR

Auch andere Tools können neben TDIR hilfreich sein, etwa Extended Detection and Response (XDR), Endpoint Detection and Response (EDR) oder Network Detection and Response (NDR). Solche Tools können TDIR bis zu einem gewissen Grad unterstützen, ihr jeweiliger Einsatzbereich ist allerdings begrenzt und jenseits ihres Spezialgebiets richten sie nichts oder nur wenig aus.

Es ist nicht leicht, die gesamte Bandbreite einer Bedrohung zu erfassen, vom Netzwerk über Server und Clouds bis zu anderen Umgebungen. Daher können XDR-, EDR- und NDR-Tools die Daten der Endpunkte nicht mit den Aktivitäten aus der Infrastruktur insgesamt korrelieren. Netzwerkverkehr, Cloud-Interaktionen oder Anwendungsverhalten bleiben dann außer Betracht.

Die mangelnde Sichtbarkeit erschwert auch die Erkennung von Advanced Persistent Threats, die erweiterte forensische Untersuchungen über lange Zeiträume hinweg erfordern. TDIR-Plattformen mit ihrem größeren Untersuchungsumfang und der Analyse historischer Daten sind daher besser in der Lage, solche APTs aufzuspüren und im Zeitverlauf selbst die geringsten Anzeichen einer Kompromittierung zu erkennen.

KI + TDIR

Die Wahrnehmung von KI ändert sich schnell. Der CISO-Report (mit dem wir jährlich untersuchen, wie CISOs mit den jeweils aktuellen Bedrohungen umgehen) hält in der Ausgabe 2023 fest, dass von den Befragten aus Westeuropa nur 17 % glaubten, dass KI ihnen einen gewissen Vorteil gegenüber Cyberkriminellen verschaffen werde. Im Lagebericht Security zeigten sich bereits 43 % derart zuversichtlich.

Künstliche Intelligenz macht sich daran, das SOC zu revolutionieren. Dies gilt insbesondere für Bereiche wie die Automatisierung von Threat Hunting und Bedrohungserkennung. Die klassische Erkennung hält sich an Signaturen und Korrelationsregeln, die konkrete Angriffsbedingungen in den Blick fassen – das funktioniert aber nicht mehr, wenn sich die Bedingungen ändern.

Mit KI-Unterstützung können die Sicherheitsteams Angriffe erkennen, die sie mit den üblichen Korrelationssuchen übersehen hätten. Sie können besser beurteilen, was als anormales Verhalten gelten soll, und leichter Aktivitäten identifizieren, die auf ein Hochrisiko-Event hindeuten könnten.

Ohne Splunk hätten wir kein solch erfolgreiches SOC-Programm mit Studierenden.

— Sumit Jain, CISO
der Louisiana State University

LSU

Wenn es um Cybersicherheit geht haben die Studierenden der **Louisiana State University** das Ziel fest im Blick.

Zentrale Herausforderungen

Als führende Einrichtung im Bereich Cybersicherheit wollte die LSU ihren Studierenden praktische Erfahrungen im Security Operations Center (SOC) vermitteln und zugleich die Cybersicherheit der weiterführenden Schulen in ganz Louisiana verbessern.

Die LSU hat das geschafft – mit Splunk und dem Managed-Security-Anbieter TekStream. Mittlerweile ist das von Studierenden betriebene SOC-Programm an 18 Einrichtungen in Louisiana live, Tendenz steigend. So verbessert die LSU die Cybersicherheit akademischer Einrichtungen im ganzen Bundesstaat, leistet einen positiven Beitrag zur beruflichen Aus- und Weiterbildung und legt den Grundstein für einen bundesweit führenden Cybersecurity-Lehrplan.

Wichtige Ergebnisse

Für Sumit Jain, CISO der LSU, liegt der Hauptvorteil von Splunk darin, dass Splunk relevante Security-Events (sogenannte Notables) identifiziert und in einer verarbeitbaren Form meldet. „Die Möglichkeit, alle Incidents in einer einzigen Umgebung zusammenzufassen, hat sich am stärksten auf die Effizienz unseres Programms und die Sicherheit der teilnehmenden Einrichtungen ausgewirkt“, sagt Jain. Denn sonst müsste jede Einrichtung ihre Umgebungen selbst auf Notables überprüfen. „Stattdessen arbeiten wir mit einer zentralen Übersicht, mit der wir auf die zusammenfassenden Darstellungen auf Einrichtungsebene blicken“, erklärt er. „Ohne Splunk hätten wir kein solch erfolgreiches SOC-Programm mit Studierenden.“

1.000
Stunden SOC-Erfahrung für Studierende pro Jahr

18
geschützte Einrichtungen

Was das Programm auszeichnet, ist die Einbeziehung der gesamten Campus-Community. Von Studierenden betriebene SOCs richten sich normalerweise an Leute, die Abschlüsse in IT, Cybersecurity und Informatik anstreben. „Unser Führungsteam und der Verwaltungsrat wollen, dass alle diese Chance bekommen“, sagt CIO Craig Woolley. „Deshalb ist das Programm für Studierende aller Fachrichtungen offen. Das einzige Kriterium, auf das wir achten, ist die Fähigkeit, kritisch zu denken. Alles andere können wir ihnen beibringen.“

Der TDIR-Workflow im Detail

Von Bedrohungserkennung über Untersuchung bis hin zur Reaktion

Durch die Koordinierung der Aufgaben von Erkennung, Untersuchung und Reaktion können die SecOps-Teams die Mean Time to Resolution (MTTR) verkürzen, die Analysten von Routineaufgaben befreien und selbst ausgeklügelte Angriffe vereiteln. Im Folgenden gehen wir Schritt für Schritt ausführlich durch, wie dieser Workflow aussieht.

1. Daten erfassen

Datenaggregation und Triage

Datenerfassung ist die Grundlage für jegliches Security-Monitoring. Um grundlegende durchgängige Transparenz zu schaffen, müssen die Sicherheitsteams in der Lage sein, Log-Daten aus der gesamten Infrastruktur aufzunehmen, zu normalisieren und zu indizieren, sodass die Daten durchsuchbar und analysierbar werden. Durch Filtern, Verfremden und Weiterleiten von Daten können sich die Sicherheitsteams auf das Wesentliche konzentrieren und gleichzeitig Kosten und Komplexität kontrollieren.

Im Idealfall sammelt und kompiliert eine TDIR-Lösung Daten aus einer Vielzahl von Tools, Systemen und Anwendungen. Event-Daten werden je nach Use Case ausgefiltert und weitergeleitet. Sind die richtigen Datenquellen validiert, werden die Log-Einträge konsolidiert und zu einer Handvoll brauchbarer Warnmeldungen verdichtet. Die Teams können diese Meldungen außerdem mit Kontext aus weiteren Datenquellen anreichern und korrelieren.

Datenquellen, die erfasst werden sollten, sind insbesondere diese:

- **Endpunkte:** Anwendungs- und Prozessausführung, Monitoring der Dateiintegrität, Netzwerkverbindungen mithilfe von erweiterten EDR-Funktionen.
- **Anwendungen:** Geschäftskritische Anwendungen wie Finanzsysteme oder Systeme, die sensible Daten, Kundendaten und Logs von User-Aktivitäten verarbeiten.
- **Datenbanken:** Audit- und Transaktionslogs zur Identifizierung von Mustern ungewöhnlichen Verhaltens, von Änderungen oder Löschungen an Datensätzen und von möglicherweise unbefugtem Zugriff auf sensible oder gesperrte Datensätze.
- **Clouds:** SaaS-Geschäftsanwendungen (Software as a Service) zum User-Monitoring, ebenso IaaS- (Infrastructure as a Service) und PaaS-Umgebungen (Platform as a Service) wie AWS oder Azure.

Datenmanagement

Daten aus Multicloud-Services und diversen Datenspeichern zu durchsuchen und zugänglich zu machen, ist eine Herausforderung. Doch eine umfassende TDIR-Lösung kann per Datenföderation problemlos große Datenmengen durchforsten. So können Unternehmen auf relevante Daten in hoher Qualität aus jeder Umgebung im Unternehmen zugreifen, egal ob diese in einem Data Lake, bei einem Cloud-Anbieter oder anderswo abgelegt sind. Die Teams können dann ganz nach Bedarf ausgewählte Daten einbeziehen. Auf diese Weise bleibt die Datenintegrität gewahrt, die Latenzzeiten werden verringert, und vor allem wird umfassende Transparenz geschaffen, weil die Daten unabhängig vom Speicherort zugänglich und analysierbar sind.

Asset-Management

Einer einschlägigen ESG-Studie zufolge haben 69 % mindestens einen Cyberangriff erlebt, der bei einem Asset ansetzte, das nicht gemanagt oder dem Unternehmen gar nicht bewusst war.

Je größer und ausgedehnter ein Unternehmen wird, desto schwieriger wird es, alle Assets zu erfassen und zu inventarisieren, d. h. sämtliche Geräte, User und Anwendungen im gesamten Netzwerk zu identifizieren. Damit steigt das Risiko von Cyberangriffen, Datenpannen, Insider-Bedrohungen und Compliance-Verstößen.

Im SOC der Zukunft hat die kontinuierliche Asset Discovery idealerweise Priorität. Durch die Integration von detailliertem Asset- und Identitätskontext in einer einheitlichen TDIR-Lösung können die Analysten alles, was mit potenziellen Bedrohungen in Zusammenhang steht, überschauen, Incident-Untersuchungen beschleunigen und Compliance-Lücken identifizieren.

Analysten müssen bestimmen können, welche Ressourcen kritisch sind und zuerst geschützt und überwacht werden müssen. Durch eine Identifizierung und Definition der kritischen Assets im gesamten Sicherheitsstack können die SOC-Teams die Grundlage für Incident-Warnmeldungen, Risikoprofile und Bedrohungsmodelle schaffen. Zunächst müssen sie jedoch wissen, welche Daten sie ins Monitoring einbeziehen müssen, bevor sie diese vollständig schützen und nach Priorität ordnen können.

Das bedeutet, dass Sie einen Begriff davon haben müssen, was für das Unternehmen besonders wertvoll ist: die Kundendatenbank, personenbezogene Daten, die Finanzen in der Cloud etc. Danach können Sie die Assets im SOC entsprechend nach Priorität ordnen und sicherstellen, dass Warnmeldungen zu diesen Assets vorrangig behandelt werden.

2. Bedrohung(en) identifizieren und untersuchen

Modelle und Frameworks zur Erkennung nutzen

Analysten sehen sich das Gesamtbild an, wenn sie eine Bedrohung identifizieren, nicht nur einen Detailausschnitt. Deshalb arbeiten TDIR-Ansätze mit Best Practices wie dem MITRE-ATT&CK-Framework oder dem Threat-Intelligence-Framework von Splunk Enterprise. Damit können die Sicherheitsteams Angriffe anhand bekannter Taktiken, Techniken und Verfahren (TTPs) leichter ins Visier nehmen.

Mit Modellen und Frameworks zur Bedrohungserkennung (namentlich MITRE ATT&CK) können Sie Ihren Assets einfacher Risikowerte zuordnen und die daraus abzuleitenden Prozesse und Richtlinien festlegen, ebenso wie die zugehörigen Kompromittierungsindikatoren (IoCs), auf die es zu achten gilt, und die Maßnahmen, die auf dieser Grundlage zur Klärung und Behebung vorgesehen sind.

Wenn sich die Sicherheitsteams an Erkennungsframeworks wie MITRE ATT&CK halten, können sie das Warnmelderauschen deutlich reduzieren, weil dann eine Kombination aus statischen Erkennungen, ML-Erkennungen und risikobasierten Erkennungen greift. Die automatische Anreicherung durch Bedrohungsinformationen ist ebenfalls ratsam, weil die Warnmeldungen damit noch weiter verbessert werden und zusätzliche Indicators of Compromise zutage fördern.

Für TDIR werden z. B. die folgenden MITRE-ATT&CK-Taktiken zur Bestimmung bei einigen der wichtigsten Use Cases der Security-Erkennung verwendet:

- **Identify New User Accounts:** Diese Erkennung identifiziert im Netzwerk neue User bzw. neu erstellte Accounts der vergangenen Woche.
- **Powershell Disable Security Monitoring:** Diese Erkennung identifiziert Versuche, Sicherheitsfunktionen außer Kraft zu setzen.

Bedrohungsinformationen (Threat Intelligence)
Threat-Intelligence-Frameworks – hierzu gehören vor allem MITRE ATT&CK, das NIST Cybersecurity Framework und die Cyber Kill Chain von Lockheed Martin – helfen den Sicherheitsteams Kompromittierungsindikatoren zu erkennen, unabhängig von den konkreten Kontrollen und geschützten Systemen. Mit diesen Informationen können Unternehmen die Bedrohungslandschaft, insbesondere in Bezug auf die eigenen Systeme und User, besser verstehen und bekannte IoCs einfacher identifizieren, die klassischen oder isoliert arbeitenden Kontrollen entgehen würden.

Beispiele hierfür wären IP-Adressen, URLs oder Datei-Hashes, die mit Phishing-Aktivitäten in Verbindung gebracht werden, oder identifizierende Informationen zu SSL-Zertifikaten, von denen bekannt ist, dass sie für Schadzwecke verwendet werden.

Risikobasierte Warnmeldungen (Risk-based Alerting)
Ebenso ist es wichtig, das Risikoprofil der relevanten Assets und Systeme zu berücksichtigen. Die Risikobewertung ist eine zentrale Komponente der Sicherheitsanalyse und eine wesentliche Grundlage für die Priorisierung von Sicherheitswarnungen und Bedrohungserkennungen.

Hier zwei Beispiele für Risikoprofile:

- **Risikoprofil Assets:** Welche geschäftlichen Auswirkungen hätte ein Incident, der dieses Asset trifft? Wie hoch ist die Wahrscheinlichkeit eines Incidents für das Asset? Wie sieht der Sicherheitsstatus dieses Assets aus? Wie sensibel bzw. wichtig sind die Daten, die in diesem System verarbeitet werden oder abgelegt sind? Welche Arten von Usern greifen typischerweise auf dieses System zu oder arbeiten damit?
- **Risikoprofil Identitäten:** Wie wichtig ist die Identität? Handelt es sich um einen Service-Account, ein Verwaltungskonto, ein User-Konto auf Führungsebene oder einen Account externer Zulieferer? Handelt es sich um einen Account, der vermutlich eher zur Zielscheibe wird, oder ist das Konto vielleicht a priori nicht vertrauenswürdig? Welche Folgen hätte es, wenn diese Identität kompromittiert würde? Ließe sich der User überhaupt dingfest machen?

3. Sofortreaktion

Orchestrierung und Reaktion automatisieren und einsetzen

SOAR (Security Orchestration, Automation and Response) ist ein integraler Bestandteil von TDIR. SOAR sorgt dafür, dass auch die Tools, bei denen es zunächst hakt, reibungslos zusammenspielen, und dass sich sämtliche Daten fein säuberlich zu brauchbaren Informationen zusammenfinden, von Anfang bis Ende, sodass die Sicherheitsteams damit umgehen und, was noch wichtiger ist, auf Grundlage dieser Daten ihre Maßnahmen ergreifen können.

Gartner definiert SOAR als „Lösungen, die Incident Response, Orchestrierung und Automatisierung sowie Threat-Intelligence-Management-Funktionen auf einer einzigen Plattform vereinen". Ohne Sicherheitsautomatisierung und -orchestrierung müssten die Security-Teams jede Warnmeldung und jede Bedrohung einzeln manuell untersuchen. Das ist heutzutage gar nicht machbar und würde auf geradem Weg in die Katastrophe führen.

Optimale SecOps-Workflows mit SOAR

SOAR hat zwei zentrale Aspekte: Orchestrierung und Automatisierung.

- **Orchestrierung** bedeutet, dass alle Ihre Tools und Daten wissen, wie sie miteinander kommunizieren können und sollen, auch wenn sie in verteilten Systeme verstreut sind. Die Security-Orchestrierung fügt eine Reihe von Automatisierungsaufgaben zu einem vollständigen Workflow zusammen, mit Anfang und Ende.
- **Automatisierung** bedeutet im SOAR-Zusammenhang vor allem, dass konkrete Aufgaben vereinfacht und eben automatisiert werden. Das Muster lautet: Wenn dies passiert, dann sollte in Reaktion darauf jenes geschehen, damit die Angelegenheit geklärt wird.

Jede der beiden Methoden für sich kann ein leistungsfähiges Tool im SOC-Arsenal sein, doch am stärksten sind Automatisierung und Orchestrierung im Zusammenspiel. Die gestrafften, automatisierten Workflows ermöglichen schnellere Untersuchungen und schnellere Reaktionen, sie minimieren das Risiko eines erfolgreichen Angriffs. Das koordinierte Vorgehen bei Erkennung, Untersuchung und Reaktion beschleunigt nicht nur den Reaktionsprozess, sondern reduziert auch die Komplexität und den manuellen Aufwand, der immer noch allzu häufig anfällt. Unterm Strich ermöglicht SOAR damit den entscheidenden Schritt: vom Dauernotstand zur kompletten Kontrolle.

SOAR-Playbooks

Mit Playbooks können die Security-Teams Aktionen orchestrieren, z. B um automatisch schädliche Anhänge von Phishing-Mails zu erkennen und in die Quarantäne zu verschieben. Die Entwicklungsteams wiederum können synthetische Tests fahren und damit Probleme aufzeigen, bevor der Code freigegeben wird. Das User Monitoring gibt Einblick in die User Experience sowie in mögliche Probleme, sodass der Code bei Bedarf zurückgesetzt werden kann.

Angesichts der Zettabyte-Mengen an Daten, die es zu verarbeiten gilt, werden automatisierte Workflows immer wichtiger. Dies reicht von einfachen Maßnahmen – z. B. zur Anreicherung von Kompromittierungsindikatoren mit externen Bedrohungsinformationen – bis zu fortgeschrittenen automatisierten Prozessen, etwa bei der komplexen mehrstufigen Automatisierung des Umgangs mit Phishing-Mails, die von Beschäftigten gemeldet werden.

Ähnlich wie bei der Bedrohungserkennung sollte die Erstellung und Verwaltung dieser SOAR-Playbooks moderne Content-Management-Ansätze unterstützen, einschließlich einer vollständigen Unterstützung von CI/CD-Pipelines. Und wie bei der Bedrohungserkennung sollten sich die Inhalte der Playbooks an gängigen Frameworks wie MITRE D3FEND orientieren.

Im weiteren Zusammenhang betrachtet, kann SOAR drei große Sicherheitsherausforderungen lösen:

- Harmonisierung der Daten aus anderen Tools im übergeordneten Security-Stack
- Reduzierung des Rauschens mit Möglichkeit der Priorisierung von Warnmeldungen
- Schnelle und präzise Reaktionen auf Bedrohungen durch Automatisierung

Ein einheitlicher SecOps-Ansatz

Splunk unterstützt die Sicherheitsteams im gesamten TDIR-Workflow. Die Security Operations bekommen mit Splunk umfassenden Einblick in ihre Hybrid- und Edge-Technologielandschaften, dazu leistungsstarke Tools für Untersuchung und Reaktion, in jeder Größenordnung. Die Teams haben dann eine gemeinsame Sicht auf ihre Daten, mit einer gemeinsamen Suchsprache und mit Tools, die die teamübergreifende Zusammenarbeit erleichtern und die digitale Resilienz im gesamten Unternehmen stärken.

Mit Splunk wird TDIR ganz einfach

Mit einer Plattform auf Unternehmensniveau arbeiten die SOC-Teams mit einheitlichen Daten und Tools auf einer gemeinsamen Arbeitsfläche, was die Abstimmung innerhalb und zwischen den Teams und Technologien wesentlich verbessert.

- **Lassen Sie den Dauernotstand hinter sich:** Die Security-Lösungen von Splunk setzen auf einer KI-gestützten Plattform auf, die sich mit branchenführenden Produkten (Splunk Enterprise Security, Splunk SOAR, Splunk User Behavior Analytics, Splunk Attack Analyzer etc.) noch erweitern lässt. Das rein reaktive Chaos im SOC verwandeln Sie damit in eine moderne, einheitliche TDIR-Experience.
- **Geben Sie den Teams eine einheitliche Arbeitsfläche:** Damit sorgen Sie für effiziente SecOps. Sie vereinfachen die Sicherheits-workflows, indem Sie Abläufe als Reaktionsvorlagen codieren und damit wiederholbare Prozesse ermöglichen. Sie beschleunigen Ihre Security Operations auf Automatisierungstempo und starten gemeinsam von einer zentralen, modernen Arbeitsfläche aus – alle Beteiligten haben dort in Echtzeit auf ihren Dashboards alles im Blick, was für sie jeweils von Relevanz ist.
- **Reagieren Sie blitzschnell und automatisch:** Durch die Auto-matisierung manueller wiederkehrender Sicherheitsprozesse in Ihrem integrierten Security-Stack können Sie erreichen, dass ein dreiköpfiges Team mit der Schlagkraft von zehn Fachleuten agiert. Splunk SOAR bietet umfangreiche Funktionen für Orchestrierung, Automation und Reaktion, die Ihr SOC stärken: Wenn Sie Routine-prozesse automatisieren und Security Incidents schneller zuordnen und einstufen, dann arbeiten Ihre Sicherheitsanalysten smarter, nicht härter.

Suchen, Analysen und Visualisierungen für verwertbare Erkenntnisse aus all Ihren Daten, vom Edge bis in die Cloud.

Starten Sie jetzt Ihre kostenlose Testversion.

Bleiben Sie dran und reden Sie mit:

splunk>
a CISCO company

25_CMP_ebook_the-SecOps-handbook-to-TDIR_v5_GER