Leitfaden für SIEM-Käufer

Ihr Leitfaden für moderne, datengesteuerte Sicherheitslösungen für die hybride Welt

splunk>
turn data into doing®

Inhalt

Die letzten beiden Jahre waren eine wilde Fahrt. Die Art und Weise, wie wir leben und arbeiten, hat schwindelerregende Veränderungen durchgemacht, und wir sind in einer Welt, die seit der Pandemie kaum wiederzuerkennen ist, durch enorme Unvorhersehbarkeiten gekurvt. In der Wirtschaft ist die digitale Transformation von einer vordringlichen Aufgabe zu einer absoluten Notwendigkeit geworden, nahezu jedes Unternehmen ist aus der Not heraus ein Technologieunternehmen geworden. Aber Not macht auch erfinderisch. Diese beispiellosen und unbeständigen Zeiten haben uns zu rasend schnellen Innovationen gezwungen. Und was treibt die entscheidenden Innovationen? Beschleunigte Cloud-Technologien und die Power der Daten.

Um in dieser hybriden Welt nicht nur zu überleben, sondern zu wachsen, brauchen Unternehmen Lösungen, die leistungsstark, flexibel und schnell sind – Lösungen, die mit Daten arbeiten. Auf einem starken Fundament aus Daten und Technologie können Unternehmen schnell reagieren, egal was auf sie zukommt, können sich vor immer neuen Bedrohungen schützen und ihre Daten in innovative Taten verwandeln.

Aber nicht jedes Unternehmen ist bereits in der Lage, diese Datenpower für sich zu nutzen. Das liegt an drei großen Herausforderungen:

- **Separate Datensilos:** Durch die Menge an Tools, die in den Teams zum Einsatz kommen, liegen die Daten oft verteilt und fragmentiert vor und sind schwer zu überblicken. Die Folgen davon sind Ineffizienz und Schwachstellen.
- **Mangelnde Transparenz:** Ohne kontextbezogene Daten ist es kaum möglich, Geschäftsprozesse von Anfang bis Ende durchgängig zu verfolgen. Das erschwert Fehler-Ursachen-Analysen und die Suche nach Optimierungsmöglichkeiten.
- **Security und Compliance:** Sicherheits-, Datenschutz- und Compliance-Vorschriften ändern sich laufend. Den Zugriff auf die richtigen Daten zur richtigen Zeit und mit der richtigen Governance zu regeln, wird damit noch schwieriger.

Die Folge davon ist, dass es vielen Unternehmen schwerfällt, Erkenntnisse aus ihren Daten zu ziehen und angemessene Maßnahmen zu ergreifen. Es ist zu ressourcenaufwendig und dauert einfach zu lange.

Aber es gibt eine Lösung: Ihr Unternehmen kann diese Herausforderungen meistern, sicher bleiben und die Datenpower nutzen, wenn es das richtige SIEM (Security Information and Event Management) einsetzt – eine Lösung, die Cloud-basiert und datengesteuert ist.

Was ist ein SIEM?

Ein SIEM ist wie das Radarsystem eines Piloten. Wie Piloten brauchen auch die Analysten, die bei Ihnen im SOC-Cockpit (Security Operation Center) sitzen, ein Radar, damit sie sicher durch all das steuern können, was um sie herum ist, was vor ihnen liegt und was sich möglicherweise außerhalb des Sichtfelds verbirgt. Ein SIEM ist eine Security-Plattform, mit deren Hilfe SOC-Analysten die gesamte IT des Unternehmens überblicken und Bedrohungen erkennen können, die sich in den hintersten Winkeln der ihnen anvertrauten Systeme verstecken. Ohne SIEM fliegen sie blind.

Security-Anwendungen, Netzwerksicherheit und Systemsoftware fangen zwar einzelne Angriffe ab, erkennen anormales Verhalten und protokollieren dies, doch gerade die gefährlichsten Bedrohungen von heute sind verteilte Bedrohungen – mit diesen Tools allein kommt man nicht dagegen an. Die Hacker greifen dabei im Verbund über mehrere Systeme hinweg an und nutzen fortschrittliche Tarntechniken, damit sie nicht entdeckt werden.

Die Angreifer nutzen Schwachstellen mit Vorliebe in Stresssituationen aus – z. B. in einer Phase des plötzlichen Wechsels ins Homeoffice, wie in der Pandemie.

Mitten in dieser dringenden Umstellung fiel den SOC-Teams die Aufgabe zu, die Systeme zu sichern, obwohl sie keinen direkten Zugang zu den Sicherheitstools und -prozessen hatten, auf die sie sich sonst verlassen hatten.

Situationen wie diese sind der Grund, warum ein modernes SIEM wichtiger denn je ist. Ohne das richtige SIEM können sich Cyberangriffe zu Totalkatastrophen auswachsen, die selbst die besten SOC-Analysten nicht kommen sehen. Und wenn sie die verwundbare Stelle dann doch entdeckt haben, etwa bei einem Ransomware- oder Lieferkettenangriff, können sie sich nur noch in Schadensbegrenzung üben – und sich auf die Suche nach einem neuen CISO machen.

In diesem Leitfaden für SIEM-Käufer gehen wir näher darauf ein, was genau ein SIEM ist, was es leistet, wie es sich von anderen Instrumenten unterscheidet und wie Sie die richtige SIEM-Lösung für Ihr Unternehmen finden.

Was genau macht ein SIEM eigentlich?

Gartner definiert SIEM als „Technologie zur Bedrohungserkennung und zur Reaktion auf Sicherheitsvorfälle durch die Echtzeiterfassung und retrospektive Analyse von Sicherheitsereignissen aus einer Vielzahl von Event- und Kontextdatenquellen“. Im Grunde ist ein SIEM dazu da, dass die Analysten im Security Operations Center (SOC) ihre Arbeit besser machen können. Es ist eine Plattform, die Event-Logs einspeist und den Fachleuten einen zentralen Überblick über ihre Daten verschafft – und noch mehr Erkenntnisse.

Ein modernes SIEM kann drei große Sicherheitsprobleme lösen:

- **Mangelnde Sichtbarkeit:** Ein SIEM schafft durchgängige Transparenz und gibt in Echtzeit Einblick in die Sicherheitslage.
- **Fehlalarme:** Ein SIEM sorgt dafür, dass bei den Analysten weniger falsch positive Warnungen eingehen; die Alerts werden priorisiert, Erkennungen und Untersuchungen sind schneller möglich.
- **Mangelnde Flexibilität:** Ein SIEM kann unterschiedlichste Arten von Bereitstellungsumgebungen, Tools, Technologien und Bedrohungsinformationen unterstützen bzw. integrieren.

Wie gehen Unternehmen ohne SIEM diese Herausforderungen an? Nun, die längste Zeit hat man es mit den klassischen Einzellösungen und Tools wie XDR (Extended Detection and Response) versucht – mit eher gemischten Ergebnissen. Sehen wir uns diese Optionen zunächst kurz an, dann wollen wir auf die effektivere Lösung eingehen: ein modernes SIEM.

Ältere SIEMs sind Dinosaurier

Natürlich nicht im Wortsinne. Aber ältere SIEM-Technologien sind einfach nicht in der Lage, mit den sich wandelnden Sicherheitsherausforderungen Schritt zu halten. Sie brauchen abgegrenzte Umgebungen und können nur eine gewisse Menge Daten aufnehmen, Abfragen und Untersuchungen dauern lange, und die Software ist außerdem nicht gut skalierbar.

Viele IT-Abteilungen, die in SIEM-Plattformen investiert hatten, mussten dies auf die harte Tour lernen: Am Ende stellten sie fest, dass es sehr lange dauert, bis man alle Daten in ein solches Legacy-SIEM eingespeist hat, und dass das zugrunde liegende Datensystem letztlich statisch ist. Zwar gibt es auf dem Markt zahllose Software-Optionen zum Sammeln, Speichern und Analysieren von reinen Sicherheitsdaten, doch nur wenige Lösungen können diese Daten in verwertbare Informationen verwandeln. Legacy-SIEMs jedenfalls nicht.

Und dann ist da noch die Frage der Geschwindigkeit. Ihre SOC-Analysten dürfen bei einer Sicherheitswarnung keine Zeit verlieren. Ein herkömmliches SIEM kann aber nicht mit dem Tempo mithalten, in dem die Fachleute die Daten untersuchen müssen.

Es kommt noch schlimmer: Klassische SIEMs arbeiten ausschließlich mit Sicherheitsdaten. Security-Events mit all dem zu korrelieren, was in der restlichen IT-Umgebung passiert, ist damit unmöglich. Das hat vor zehn Jahren vielleicht noch funktioniert, aber nicht in unserer hybriden IT-Welt, in der manche aus dem Homeoffice arbeiten, andere ihre Privatgeräte mitbringen und alles eng vernetzt ist und laufend sicherheitsrelevante Daten generiert.

Vor allem angesichts der beschleunigten Cloud-Migration, aus der sich immer neue Angriffsvektoren ergeben, müssen Unternehmen heute ein Monitoring aller wichtigen Cloud- und SaaS-Dienste (Software as a Service) einrichten, das Benutzeraktivitäten, Verhalten und Anwendungszugriff erfasst. Erst dann werden potenzielle Bedrohungen und Angriffe in vollem Umfang ersichtlich.

Sieben Gründe, Ihr altes SIEM zu ersetzen

Unternehmen sind oft an die überholten Architekturen klassischer SIEMs gefesselt, die meist eine SQL-Datenbank mit fixem Schema verwenden. Dies kann zu einem Single Point of Failure werden oder führt zu Skalierungs- und Leistungseinbußen.

1. **ABGEZÄHLTE SICHERHEITSTYPEN**	Eine Einschränkung der eingespeisten Daten wirkt sich negativ auf die Erkennungs-, Untersuchungs- und Reaktionszeiten aus.
2. **KEINE EFFEKTIVE DATENÜBERNAHME**	Bei älteren SIEMs wird das Einlesen von Daten unter Umständen sehr umständlich oder sehr teuer.
3. **LANGSAME UNTERSUCHUNGEN**	Grundlegende Aktionen wie z. B. direkte Log-Durchsuchungen nehmen bei älteren SIEMs oft viel Zeit in Anspruch – Stunden oder sogar Tage.
4. **INSTABILITÄT UND SCHLECHTE SKALIERBARKEIT**	Je größer SQL-Datenbanken werden, desto instabiler werden sie. Darunter leidet dann die Kundschaft, weil die Performance nachlässt oder ein Dienst ganz ausfällt, wenn Event-Spitzen dazu führen, dass der Server in die Knie geht.
5. **AUSLAUFPRODUKT ODER MIT UNGEWISSER ZUKUNFT**	Wenn ältere SIEMs von einem anderen Anbieter übernommen werden, kommen Forschung und Entwicklung oft zum Erliegen. Ohne kontinuierliche Investitionen und Innovationen können die Sicherheitslösungen aber nicht mit der sich wandelnden Bedrohungslandschaft Schritt halten.
6. **GESCHLOSSENES ÖKOSYSTEM**	Ältere SIEMs können oft nicht mit anderen Tools integrieren. Die Kundschaft muss sich also mit dem begnügen, was das SIEM mitbringt – oder zusätzlich Geld für eigene Entwicklung und für professionelle Dienstleister ausgeben.
7. **MANGELNDE REICHWEITE**	Herkömmliche SIEMs können oft nur mit On-premises-Bereitstellungen umgehen. Die Sicherheitsteams müssen aber mit Daten von Cloud-, Multi-Cloud-, On-premises- und Hybrid-Workloads arbeiten können.

Und was gibt es sonst noch?

Zunächst sollten wir einen Blick darauf werfen, was Punktlösungen und Plattformlösungen wirklich unterscheidet. Wenn Anbieter von Einzellösungen nämlich behaupten, dass sie das, was ein modernes SIEM kann, genauso können, dann sagen sie nicht die Wahrheit. Sie können in der Regel ein oder zwei Dinge wirklich sehr gut, aber sie schaffen damit oft zusätzliche Komplexität im SOC. Punktlösungen erfordern zusätzliche Konfiguration und Verwaltung, und sie müssen erst in den vorhandenen Technologie-Stack integriert werden. Wenn Ihre SOC-Analysten die Daten aber nicht zentral überschauen können, bleibt ihnen am Ende das Entscheidende verborgen.

Dann gibt es noch XDR (Extended Detection and Response). XDR ist eine relativ neue Entwicklung, die für viel (Marketing-)Wirbel gesorgt hat. Mit solchen Hypes sollte man vorsichtig sein. XDR ist eine Weiterentwicklung von EDR (Endpoint Detection and Response), das normalerweise eine zusätzliche Datenquelle für das SIEM ist – und kein Ersatz. XDR kann man zwar in Kombination mit einem modernen SIEM verwenden, aber XDR allein reicht nicht.

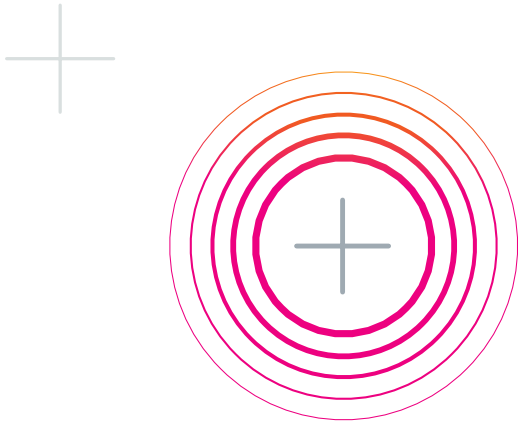
Ohne Einblick in die Sicherheitslage wird die Arbeit der SOC-Analysten geradezu ein Ding der Unmöglichkeit. Und das ist so ungefähr das Letzte, was Sie wirklich wollen: Ihren SOC-Analysten das Leben schwer machen. Denn es gibt einfach nicht genug gute SOC-Analysten. Und der ewige Mangel an Sicherheitsfachleuten hat sich seit der Pandemie nur noch verschlimmert.

Um noch einmal auf die Sichtbarkeit zurückzukommen: Ohne durchgängige Transparenz können Security-Untersuchungen nur an der Oberfläche eines Vorfalls kratzen – und das führt letztlich zu weiteren Schwachstellen. Je weniger Einblick Ihr Unternehmen hat, desto anfälliger wird es für Angriffe und Datenlecks, wie man sie groß in der Zeitung liest, mit Verlusten in Millionenhöhe und dauerhaft beschädigtem Ruf. Als CEO möchten Sie den Namen Ihres Unternehmens nicht in einer solchen Bloomberg-Schlagzeile lesen. Und als CISO möchten Sie nicht erklären müssen, was da passiert ist.

Die Evolution zum datenzentrierten SIEM

Man darf sich das wie natürliche Selektion vorstellen: Die älteren SIEMs konnten sich nicht mehr anpassen, und neuartige Lösungen konnten das Problem nur ausschnitthaft angehen. Also entwickelte sich das moderne SIEM zu einer robusten, analysegestützten Lösung, die es tatsächlich mit der Raffinesse und dem Tempo der heutigen Angriffe aufnehmen kann.

Was SOC-Analysten heute brauchen, ist eine einfache Möglichkeit, Informationen über alle sicherheitsrelevanten Daten hinweg zu korrelieren. Eine Lösung, mit der die IT-Abteilung die Sicherheitslage einfach überschaut. SOC-Analysten müssen vorhersehen können, welche Bedrohungen lauern, und Maßnahmen ergreifen, mit denen sie die Verwundbarkeit des Unternehmens in Echtzeit minimieren. Dazu brauchen Unternehmen ein datenzentriertes, modernes SIEM, das dem SOC-Team vollen Einblick in die Daten gibt, die das Unternehmen generiert. Eine Lösung, die mehr als nur Protokolldaten verarbeitet und Analysen mit einfachen Korrelationsregeln durchführt. Die besten SIEMs können heute Event-Logs in Langzeitspeicherung mit Echtzeit-Monitoring kombinieren und ermöglichen Ihrem Team damit ein ganzheitliches Verständnis der Unternehmenssicherheit.



Kernkomponenten moderner SIEM-Lösungen

Der Gartner Magic Quadrant 2021 für Security Information und Event Management ist praktisch Pflichtlektüre für alle, die sich mit dem SIEM-Markt befassen. Im Laufe der Zeit hat der Report auch Open-Source-SIEM-Anbieter und andere Einsteiger im weiteren Sinne aufgenommen. Woran können Sie also erkennen, ob eine Lösung wirklich gut ist?

Im Bericht „Critical Capabilities for Security Information and Event Management" stellt Gartner die fünf wesentlichen Funktionen heraus, die ein modernes SIEM auszeichnen.

Fünf wesentliche Funktionen moderner SIEM-Lösungen

1. **Security-Event-Logs und Telemetriedaten in Echtzeit sammeln, zur Bedrohungserkennung und für Compliance-Use-Cases.**
   Eine modernes SIEM kann Log-Daten aus jedem Ökosystem von Teams, Tools, Peers und Partnern sammeln, verwenden und analysieren. Das geschieht in Übereinstimmung mit branchenspezifischen Vorgaben zu Compliance und Reporting sowie im Hinblick auf die Anforderungen aktueller Bedrohungserkennung.
2. **Telemetriedaten fortlaufend in Echtzeit analysieren, um Angriffe und andere kritische Aktivitäten zu erkennen.**
   Ein modernes SIEM kann sämtliche Event-Logs sammeln, verwenden und analysieren, sodass sich ein umfassender Echtzeitüberblick über die Vorgänge im gesamten Security Stack ergibt. IT- und Sicherheitsteams haben damit die Möglichkeit, Ereignis-Logs zentral zu managen, und einzelne Events über mehrere Rechner oder mehrere Tage hinweg zu korrelieren und um weitere Datenquellen wie Registry-Änderungen und ISA-Proxy-Protokolle zu ergänzen. Sicherheitsfachleute können sämtliche Event-Logs außerdem zentral für Audits und das Reporting nutzen.
3. **Vorfälle untersuchen und ihren Schweregrad bzw. ihre Auswirkungen auf das Geschäft bestimmen.**
   Ein modernes SIEM kann auch den Schweregrad und die Wahrscheinlichkeit eines Vorfalls aufgrund festgestellter Probleme bestimmen. Damit lassen sich dann Prioritäten setzen und Korrekturmaßnahmen festlegen.
4. **Befunde in Reports festhalten.**
   Ein modernes SIEM kann ferner Berichte mit Sicherheitsinformationen zu jedem einzelnen Teil der Infrastruktur erstellen – ein wichtiges Hilfsmittel für Dokumentation und Compliance.
5. **Relevante Events und Logs speichern.**
   Und schließlich kann ein modernes SIEM historische Log-Daten in Langzeitspeicherung vorhalten. Damit fällt Analysten die Einhaltung von Compliance-Vorgaben ebenso leichter wie die diachrone Korrelation von Daten.

Sieben unverzichtbare SIEM-Strategien

Gleich noch eine Liste? Aber klar doch. Listen sind prima – besonders solche, die Ihnen die Arbeit erleichtern. Hier also sieben wichtige Strategien, wie Sie Ihr Unternehmen schützen (und wie Sie diese Strategien mit einem modernen SIEM umsetzen):

1. **Sicherheitsmonitoring und -analyse in Echtzeit:** Bedrohungen schnell erkennen und darauf reagieren.
2. **Cloud-Sicherheit:** Bedrohungen in Hybrid-, Cloud- und Multi-Cloud-Umgebungen erkennen und darauf reagieren.
3. **Incident Response:** Vorfälle identifizieren, sobald sie auftreten. Ereignisse verfolgen, weiterleiten und kommentieren.
4. **Threat Intelligence:** Direkt aus dem Produkt heraus auf kuratierte Erkenntnisse der Sicherheitsforschung zu alten und neuen Bedrohungen zugreifen.
5. **Vorfalluntersuchung und Forensik:** Threat Hunting optimieren, die Menge der Warnungen reduzieren und den Anteil von richtig positiven Alerts heben.
6. **Erkennung von fortgeschrittenen Bedrohungen und Insider-Bedrohungen:** Die Erkennungsquote exponentiell steigern, sodass Zeit und Ressourcen für gut bestätigte komplexe Bedrohungen frei werden.
7. **Compliance:** Durch insgesamt mehr Sichtbarkeit die drei Compliance-Komponenten zusammenbringen – Menschen, Prozesse und Technologie.

1. Sicherheitsmonitoring und -analyse in Echtzeit

Unternehmen müssen in der Lage sein, Bedrohungen so schnell wie nur möglich zu erkennen und darauf zu reagieren – unabhängig von der Art und Schwere des Angriffs. Damit dies gelingt – und zwar richtig –, ist ein Sicherheitsmonitoring unerlässlich. Und zum Glück leistet ein modernes SIEM ein robustes Monitoring in Echtzeit.

Wie funktioniert das? – Das SIEM bezieht und speichert Kontextdaten zu Usern, Geräten und Anwendungen (z. B. Bestands- und Identitätsdaten) aus On-premises-, Cloud-, Multi-Cloud- und Hybrid-Umgebungen. Alle relevanten Daten fließen dann in einen Workflow, der das potenzielle Risiko bewertet. Auf diese Weise lassen sich unterschiedliche Arten von schädlichem und/oder anormalem Verhalten erkennen und bestimmen.

Durch das Monitoring und die Einspeisung von Maschinendaten aus einer Vielzahl von Quellen unterschiedlicher Bereitstellungen bekommen die Sicherheitsteams einen umfassenden Überblick über potenzielle Sicherheitsereignisse, was die Erkennung und Verfolgung von Schadakteuren erheblich erleichtert. Ein erstklassiges SIEM sollte eine Bibliothek mit anpassbaren, vordefinierten Korrelationsregeln mitbringen, eine Konsole zur Echtzeitdarstellung von Sicherheitsereignissen sowie Dashboards zur Visualisierung laufender Bedrohungsaktivitäten in Echtzeit.

Das Security-Monitoring lässt sich außerdem durch einsatzfertige Korrelationssuchläufe ergänzen, die dann live oder nach Zeitplan aufgerufen werden. Diese Suchvorgänge können z. B. über eine intuitive Benutzeroberfläche durchgeführt werden, sodass Analysten oder Admins ohne spezielle Abfragesprache auskommen. Schließlich verfügt ein modernes SIEM noch über eine lokale historische Suchfunktion, sodass man die Log-Daten leicht durchsuchen kann, ohne die Netzwerke unnötig mit Traffic zu belasten.

2. Cloud-Sicherheit

Der Weg zu Cloud-nativen Apps und Services bringt es unweigerlich mit sich, dass das Risiko steigt – vor allem dann, wenn das Unternehmen bei Netzwerkkontrollen, Zugriffsmanagement oder Cloud-Konfiguration nicht ganz auf dem neuesten Stand ist. Wenn dann noch eine wachsende Angriffsfläche und mangelnde Sichtbarkeit hinzukommen, wird eine Kompromittierung immer wahrscheinlicher. Das klassische Monitoring reicht dann nicht mehr aus. Ihre Sicherheitsteams brauchen jetzt ein modernes SIEM, damit sie Daten aus einer Vielzahl von Quellen und jederlei Umgebung einspeisen und analysieren können.

Wie funktioniert das? – Bei einem erstklassigen SIEM erhalten Sie einsatzfertige Out-of-the-box-Inhalte zum Cloud-Monitoring. Die Erkennung von Bedrohungen in hybriden, Cloud- und Multi-Cloud-Umgebungen wird damit wesentlich erleichtert, ebenso wie die Reaktion darauf. Hinzu kommen ausgefeilte Erkennungsregeln für Cloud-Angriffe sowie Tools, mit denen Sie Ihre Cloud-Erkennungen in Angriffssimulationen testen und optimieren können.

Gerade im Zeitalter der Telearbeit müssen Sie in der Lage sein, sämtliche Cloud- und Endpunktdaten zu erfassen und zu analysieren, unabhängig von Volumen, Umgebung und Geschwindigkeit. Durch das Monitoring von Uptime, Verfügbarkeit und Vorgängen in sämtlichen Cloud-Bereitstellungen verschafft Ihnen ein modernes SIEM vollständigen Einblick in Ihre Cloud-Services, einschließlich Amazon Web Services (AWS), Azure und Google Cloud Platform. Die Erkenntnisse daraus lassen sich direkt in Maßnahmen umsetzen.

Slack sorgt durch Daten für optimale Zusammenarbeit

Aufgrund der Corona-Pandemie musste Slack über 1600 Mitarbeiter auf Homeoffice umstellen. Gleichzeitig wollte Slack seiner rasant wachsenden Benutzerbasis weiterhin einen sicheren Service bieten, der höchsten Unternehmensanforderungen entspricht. Mit Splunk konnte Slack seine Belegschaft bruchlos in die Cloud bringen, die Sicherheit durch ein Zero-Trust-Framework steigern und sämtliche Aktivitäten bei seinen Cloud-Diensten im Blick behalten. Mit Splunk konnte Slack außerdem …

- Verhaltensmuster bei kritischen Anwendungen erkennen,
- Anwender im Zero-Trust-Network autorisieren und authentifizieren sowie
- innovativ und im Gleichtakt mit den Kunden bleiben – aber trotzdem sicher.

Betrieb eines sicheren Ökosystems

Aufgrund des heftigen Anstiegs der Nachfrage in der Pandemie musste Slack für effektive Sicherheit sorgen. Das Unternehmen richtete daher eine neue API ein und schuf ein sicheres Zero-Trust-Netzwerk. Durch die Splunk-Integration der Analyse-API bekamen die Kunden alle nötigen Informationen, und das Management blieb leichter in Kontakt. Alle kritischen Slack-Anwendungen übermittelten nun Logging-Inhalte an Splunk, sodass die Daten zentral zusammengeführt waren und Einblick in bestimmte Verhaltensmuster gaben.

Der Betrieb in einem Zero-Trust-Netzwerk, in dem alle Benutzer erst authentifiziert und autorisiert werden, hat auch die Sicherheit von Slack verbessert. „Splunk ist ein wesentlicher Faktor dafür, dass Slack ein Zero-Trust-Netzwerk betreiben kann“, sagt Larkin Ryder, Director of Product Security bei Slack. „Denn Splunk macht für uns sämtliche Aktivitäten sichtbar, die in all unseren Cloud-Services stattfinden.“

„Mit Splunk stellen wir sicher, dass unser Sicherheitsprogramm im gesamten Unternehmen und in allen Apps so funktioniert, wie wir es erwarten und wie wir es für die Integrität unseres Unternehmens benötigen.“ Mehr erfahren.

3. Incident Response

Ein modernes Unternehmen braucht auch eine zeitgemäße Vorfallreaktion. Ein modernes SIEM hilft Ihnen dabei, Incidents zu erkennen, sobald sie auftreten. Sie können Ereignisse dann nachverfolgen, weiterleiten und kommentieren.

Wie funktioniert das? – Mit einem modernen SIEM können Sie Ereignisse zusammenführen (von Hand oder automatisch), es unterstützt Systeme von Drittanbietern (was den Datenaustausch mit ganz unterschiedlichen Quellen erleichtert), es stellt aktuelle Bedrohungsinformationen bereit und ermöglicht automatisierte Reaktionen (etwa mit Playbooks), die Cyberangriffe unterbinden bzw. blockieren, entweder schon im Vorfeld oder sofort nach Entdeckung.

Dazu sollte das SIEM der Dreh- und Angelpunkt des ganzen Incident-Response-Workflows sein. Da Sicherheitsereignissen jeweils eine Dringlichkeitsstufe zugewiesen wird, lassen sich potenzielle Bedrohungen am Dashboard identifizieren, kategorisieren und sortieren, bevor sie den Analysten zur Überprüfung zugewiesen werden. So sorgt ein SIEM für zuverlässigere Behebung und gibt Ihren Teams das Kontextwissen, das sie für die nächsten Schritte benötigen.

Ein SIEM macht es auch leichter, den Umfang der – mitunter riesigen – Analysen zu erweitern oder zu reduzieren. So können die SOC-Analysten Filter verwenden und damit die Unmenge der Log-Daten eingrenzen; sie können Events, Aktionen und Anmerkungen auf einer Zeitleiste anordnen und diese Zeitleisten dann als wiederverwendbare Kill-Chain-Methoden für bestimmte Ereignistypen festhalten und bei Bedarf aktualisieren.

4. Threat Intelligence

Bedrohungsinformationen sind ein weiteres unverzichtbares Standbein. Nur müssen die Analysten diesen Input oft erst manuell aufbereiten, weil die Rohdaten zu verrauscht sind. Bei der Eingabe von Hand geht aber im Laufe der Untersuchung der Kontext verloren oder die Daten werden zu ungleichartig, die Anreicherung in Playbooks ist wiederum zu umständlich. Erschwerend kommt hinzu, dass die wertvollsten Daten oft in Silos eingeschlossen liegen.

Zum Glück gibt es einen rasch wachsenden Threat-Intelligence-Markt, sodass ein modernes SIEM Bedrohungsinformationen in jeder Phase der Vorfallreaktion ergänzen und verfügbar machen kann.

Wie funktioniert das? – Threat Intelligence verwandelt interne und externe Quellen von Sicherheitsinformationen über Teams und Tools hinweg in fundierte, umsetzbare Automatisierungen und erleichtert den Informationsaustausch mit internen und externen Stakeholdern. Ihr Team kann damit Angriffen zuvorkommen und komplexe Pipelines aufbauen – und dazu müssen sie nicht einmal Skripte im Backend schreiben bzw. pflegen. Threat Intelligence ist in die meisten modernen SIEMs integriert oder wird als Cloud-nativer SaaS-Dienst angeboten, der sich nahtlos in moderne SIEM-Plattformen integrieren lässt.

Die Informationen umfassen in der Regel Kompromittierungsindikatoren (IOCs), gegnerische Taktiken, Techniken und Verfahren sowie zusätzlichen Kontext für verschiedene Arten von Vorfällen und Vorgängen. Das macht es viel leichter, anormale Aktivitäten zu erkennen, denn Ihre Analysten verfügen damit über alle Informationen, die sie benötigen, um die Risiken, Folgen und Ziele eines Angriffs – egal wie raffiniert – zu bewerten und angemessen zu reagieren.

Die Informationen lassen sich auch mit Maschinendaten kombinieren, sodass man Beobachtungslisten, Korrelationsregeln und Abfragen einrichten kann, um die Erkennung und die Reaktion zu optimieren. Die Informationen können außerdem automatisch mit Ereignisdaten korreliert und in Dashboards oder Reports eingepflegt werden. Oder man leitet sie direkt weiter, damit die betreffende Schwachstelle rasch behoben wird.

5. Vorfalluntersuchung und Forensik

Vermutlich verbringt Ihr Sicherheitsteam zu viel Zeit mit Alerts, die letztlich zu nichts führen. Eng definierte Erkennungen ergeben meist viele Fehlalarme und starkes Rauschen, was die Leute an der Front nur belastet. Darum brauchen Sie eine vernünftige SIEM-Strategie für Vorfalluntersuchung und Forensik.

Wie funktioniert das? – Ein modernes SIEM visualisiert und korreliert Daten, indem es kategorisierte Ereignisse einer Kill Chain zuordnet oder Heatmaps erstellt, aus denen sofort ersichtlich ist, ob ein Angreifer Taktiken verfolgt, die sich in einem Security-Framework wiederfinden lassen.

Die Risikozuweisung verbessert auch das Threat Hunting und reduziert die Menge der Benachrichtigungen, sodass der Anteil der richtig positiven Ergebnisse steigt. Zugleich kommen mehr komplexe Bedrohungen ans Tageslicht, z. B. niedrigschwellige oder verzögerte Angriffe, die von den meisten Korrelationssuchen übersehen werden. Dadurch werden Zeit und Ressourcen für die Suche nach echten (oft komplexen) Bedrohungen frei, und die Abläufe orientieren sich an den bewährten Cybersecurity-Frameworks.

Kurzum: Wenn sich Ihre Analysten auf die wirklich wichtigen Aufgaben konzentrieren können, sind sie besser in der Lage, bei Kompromittierungen schnell und effizient zu reagieren – ein Ziel, aufs Innigste zu wünschen.

Obendrein kann Ihr Team mit den umfassenden Funktionen für Zusammenarbeit und Berichterstattung im Untersuchungsworkflow moderner SIEMs besser fundierte Entscheidungen treffen und forensische Beweise sammeln.

6. Erkennung von fortgeschrittenen Bedrohungen und Insider-Bedrohungen

Sicherheitsbedrohungen entwickeln sich ständig weiter, sie mutieren und finden Wege, Standardverfahren zu umgehen. Und je raffinierter der Angriff, desto schwieriger wird es für Ihr Team, ihn zu erkennen und zu klären. Angesichts der sich wandelnden Bedrohungslandschaft und der Gerissenheit neuer Bedrohungen war eine solide Strategie zur Erkennung von fortgeschrittenen Bedrohungen und Insider-Bedrohungen noch nie so wichtig wie heute.

Die meisten herkömmlichen Sicherheitstools kommen mit dieser Aufgabe nicht zurecht. Sie verlassen sich auf bestehende Regelsätze und Signaturen, sodass sie nur einfache und bekannte Gefahren erkennen, nicht aber die Komplexität fortgeschrittener Bedrohungen wie Insider-Angriffe, Zero-Day-Attacken, Malware in Seitwärtsbewegung oder kompromittierte Accounts erfassen.

Wie funktioniert das? – Glücklicherweise kann sich ein modernes SIEM auf diese Bedrohungen ausrichten, indem es Verbindungen zwischen Anomalien erkennt und sie im Rahmen des Incident-Response-Workflows korreliert; hinzu kommen Funktionen wie Endpoint Detection und Verhaltensanalysen. Durch die Festlegung mehrdimensionaler Verhaltensgrundlinien und mit dynamischen Peer-Group-Analysen – im besten Fall in Verbindung mit unüberwachtem maschinellem Lernen – lassen sich kompromittierte bzw. missbrauchte Konten rasch erkennen.

Das Ziel besteht darin, nicht nur versteckte Bedrohungen zu erkennen, sondern auch das Ausmaß eines Angriffs zu bestimmen und festzustellen, wie man ihn am besten eindämmen kann. Dazu benötigt Ihr Team Echtzeitansichten und Berichtsfunktionen, die eine beliebige Anzahl von Anwendungen und Drittanbieterdiensten mit einbeziehen können.

Mit dieser Art von Analysen und Verhaltensprofilen kann ein SIEM den Erkennungserfolg exponentiell verbessern. Außerdem werden Zeit und Ressourcen frei, damit sich Ihr Team wieder auf komplexe, gut bestätigte Bedrohungen konzentrieren kann, bevor es zu spät ist.

Expo 2020 Dubai – sicheres Mega-Event dank Splunk

Eine Veranstaltung wie Weltausstellung 2020 zu sichern, ist kein leichtes Unterfangen – auch angesichts des Risikos von Insider-Bedrohungen. Und obwohl Cybersicherheit bei der Expo Dubai von Anfang an hohe Priorität hatte, sollten die Schrauben vor dem Event noch einmal angezogen werden.

Dazu benötigte die Expo 2020 eine Sicherheitsplattform, die schnell skalierbar ist, die operative Sicherheit für Hunderte unterschiedlicher Datenquellen und Technologielösungen verwalten kann und flexibel genug für die veränderlichen Cybersicherheitsanforderungen der Veranstaltung ist. Splunk erwies sich als die beste Lösung, um diese Anforderungen zu erfüllen. Splunk konnte u. a. bei diesen Aufgaben helfen:

- Monitoring auf verdächtige und anomale Verhaltensweisen bzw. Aktivitäten, mit Kennzeichnung und Klassifikation.
- Sofortreaktion auf potenzielle Bedrohungen, inklusive Abhilfemaßnahmen.

Das Risiko von Insider-Bedrohungen minimieren

Bei Mega-Events und Großunternehmen zählen Insider-Bedrohungen oft zu den größten Risiken. Um seine Technologie-Ökosysteme vor Angreifern zu schützen, verließ sich die Expo auf die Echtzeitüberwachung von Splunk, um verdächtiges Verhalten zu erkennen. Auch um ihre Technologie-Ökosysteme vor potenziellen Angriffen zu schützen, setzten die Verantwortlichen der Expo auf das Echtzeitmonitoring, mit dem Splunk verdächtiges Verhalten identifizieren kann.

Splunk half der Expo außerdem, datengestützt schnellere und bessere Entscheidungen zu treffen, sodass die Cyberresilienz insgesamt gestärkt wurde und die Teams auf Bedrohungen sofort mit Gegenmaßnahmen reagieren konnten.

„Da Splunk viel Flexibilität bietet, konnten wir die Bereitstellung problemlos an den veränderten Bedarf der Expo während der Pandemie anpassen, insbesondere mit Blick auf die Verschiebung des Events um ein Jahr."
Mehr erfahren.

7. Compliance

Ob es um Cybersicherheit geht, um forensische Analysen, Datenschutz, Betrugsprävention oder um Risikomanagement – unterschiedliche Teams benötigen aus Compliance-Gründen jeweils eigene Datenansichten und -prozesse. Indem ein modernes SIEM durchgängige Sichtbarkeit schafft, hilft es, die drei Compliance-Komponenten – Menschen, Prozesse und Technologie – zusammenzuführen.

Wie funktioniert das? – Ein modernes SIEM verfolgt grundlegend einen ganzheitlichen Compliance-Ansatz, der nicht nur Compliance-Teams, Silos und Technologiebereiche verbindet, sondern die Compliance-bezogenen Abläufe insgesamt effizienter macht. Das bedeutet, dass die mühsame Arbeit der gesetzlich vorgeschriebenen Log-Prüfung endlich ein Ende hat. Ihre Analysten können produktiver arbeiten und das aufgeräumte, dokumentierte Risikomanagement fortführen, das man von ihnen erwartet.

Mit einem modernen SIEM haben Unternehmen den gesamten Security Stack im Blick und sind nicht mehr darauf angewiesen, dass Abteilungen oder Funktionseinheiten Daten herausrücken. Die Analysten können Maschinendaten aus einer Vielzahl von Quellen durchsuchen, Berichte erstellen, die Erfüllung regulatorischer Anforderungen anhand von Audit-Protokollen nachweisen und in Sekundenschnelle branchenspezifische Compliance-Berichte erstellen.

Und jetzt: Splunk

Splunk bietet eine analysegestützte SIEM-Lösung auf einer flexiblen Cloud-Plattform. Mit Splunk haben Unternehmen all ihre Daten im Blick, können schnell Erkenntnisse gewinnen und präzise, handlungssicher und einfach reagieren – alles mit einer einheitlichen, integrierten Lösung. Für SOC-Analysten ist das sozusagen das ultimative Radar.

Das Monitoring mit Splunk kann Daten aus jeder Quelle und in beliebigem Maßstab erfassen und analysieren. Mit dabei sind integrierte Lösungen für durchgängige Observability im gesamten Stack und einheitliche Sicherheit sowie eine Vielzahl von benutzerdefinierten Anwendungen – also praktisch unbegrenzte Möglichkeiten, aus Daten Erkenntnisse zu gewinnen.

Als datengestützte Security-Operations-Plattform ohne Kompromisse bietet Splunk die Power und Flexibilität, mit der moderne Unternehmen komplexe Compliance-Aufgaben bewältigen und auf Bedrohungen adäquat reagieren – sodass sie innovativ bleiben und wachsen können, und zwar sicher.

Splunk erfasst auch Daten aus Multi-Cloud- und Hybrid-Umgebungen. Dazu stellt es robuste Tools für Untersuchungen, Analysen und Orchestrierung bereit, mit denen Unternehmen Bedrohungen schnell und präzise aufspüren und beseitigen können.

Splunk Enterprise optimiert Ihre IT-, Sicherheits- und Unternehmensleistung durch Monitoring und Analysen Ihrer Maschinendaten. Mit intuitiven Analysen, maschinellem Lernen, Anwendungspaketen und offenen APIs ist Splunk Enterprise eine flexible Plattform, die frei skalierbar ist, von ganz konkreten Anwendungsfällen bis hin zur Funktion als unternehmensweites Analyse-Backbone.

Splunk Cloud Platform ist eine flexible, sichere und kosteneffiziente Datenplattform, mit der Sie ihre Daten durchsuchen, analysieren und visualisieren können – und auf dieser Basis optimal reagieren. Mit diesem sicher, zuverlässig und skalierbar als Service bereitgestellten und gemanagten Splunk erhalten Sie schnelle, flexible Leistung, starkes und integriertes Streaming, Suchläufe und maschinelles Lernen, dazu eine kalkulierbare Preisgestaltung, die sich am tatsächlichen Wert bemisst.

Splunk als Ihr SIEM

Komplexe Technologie und neue Bedrohungen erfordern moderne Security-Verfahren, mit denen Unternehmen ihre Geschäfts- und Sicherheitsrisiken effektiv ausbalancieren und zugleich rasch handeln können.

Die Sicherheitslösungen von Splunk erfüllen nicht nur die Anforderungen an ein modernes SIEM, sondern wappnen Sie auch für die Zukunft. Splunk bietet eine Security-Operations-Plattform, die Daten aus beliebigen Quellen in Cloud-, On-premises- und Hybrid-Umgebungen beziehen kann und präzise Bedrohungserkennung, detaillierte Untersuchungen und automatisierte Reaktionen ermöglicht. Und da Splunk als offenes Ökosystem ausgelegt ist, haben Sie volle Freiheit bei der Wahl Ihrer Tools und Versionen.

Mit Splunk erhalten Sie Einblick in sämtliche Vorgänge, gewinnen umsetzbare Erkenntnisse, können Untersuchungen schneller durchführen und die Zeit bis zur Behebung deutlich verkürzen. Die fortschrittlichen Analysen liefern wertvollen Kontext und die Übersicht, die Ihr Sicherheitsteam braucht, damit es in komplexen Umgebungen die richtigen Entscheidungen treffen kann.

Neben durchgängiger End-to-End-Transparenz bringt Splunk noch eine eigene Schema-on-Read-Technologie und verteilte Indizierung (Distributed Indexing) mit, damit das Sammeln und Analysieren von Daten einfach wird. Dabei bietet Splunk auch flexible Optionen für Unternehmen, die ihr SIEM starten oder wechseln wollen, ebenso wie Varianten für Cloud, Hybrid und eigene Server.

Für den Einstieg können Sie zwischen Splunk Enterprise und Splunk Cloud Platform wählen. Beide bieten die Kernfunktionen für Sammlung, Indizierung, Suche und Reporting. Viele Splunk-Kunden erstellen auf dieser Grundlage dann ihre eigenen Echtzeit-Suchläufe und Dashboards für wichtige Sicherheitsanwendungen. Sie können aber auch die von Splunk entwickelten Lösungen für Suche und Reporting, Sicherheit und Observability nutzen oder auf die Splunkbase zugreifen, die bereits Tausende von Apps bereithält.

Ihr aufgebohrtes SIEM

Geht da noch mehr? Da geht noch mehr! Splunk Enterprise Security (ES) ist die SIEM-Lösung der nächsten Generation von Splunk: schnell, leistungsstark, flexibel. Splunk ES schafft mit Daten volle Sichtbarkeit in Sachen Sicherheit. Nicht umsonst ist Splunk ES seit etlichen Jahren Marktführer im SIEM-Segment.

Mit unvergleichlichen Funktionen, fortschrittlichen Analysen, integrierter KI und einsatzfertigen Security-Inhalten beschleunigt Splunk ES Erkennung, Untersuchung und Reaktion. Splunk ES vereint maschinelles Lernen, Anomalieerkennung und Kriterienkorrelation in einer einzigen Security-Analytics-Lösung. Es läuft auf Splunk Enterprise, Splunk Cloud und auf beidem zugleich.

Splunk ES ist flexibel und gut kombinierbar. Mit dieser offenen, skalierbaren Datenplattform bleibt ihr Unternehmen stets agil, auch wenn sich Bedrohungen und Business-Anforderungen ändern. Durch das umfangreiche Splunk-Ökosystem und die flexiblen Bereitstellungsoptionen bleibt gesichert, dass Ihre Technologie-Investitionen immer mit ihrem SIEM zusammenarbeiten, egal an welchem Punkt Ihrer Reise in Cloud- oder Hybrid-Welten Sie sich befinden.

Mit Splunk ES können Sie Events im zeitlichen Verlauf visuell in Beziehung setzen und Details mehrstufiger Angriffe einfach kommunizieren. Außerdem können Sie Bedrohungen, Angriffe und andere ungewöhnliche Aktivitäten leicht in Echtzeit erkennen, überwachen und melden. Und: Splunk ES bietet jetzt neue, native risikobasierte Alerts und Cloud-Sicherheitsfunktionen.

Die risikobasierten Warnmeldungen (Risk-based Alerts) von Splunk ES reduzieren die Menge der eingehenden Meldungen, sodass sich Ihr Team auf die Warnungen konzentrieren kann, auf die es wirklich ankommt. Und sie erkennen komplexe Bedrohungen besser, die sonst leicht übersehen werden. Bei risikobasierten Warnmeldungen wird Benutzern und Systemen ein Risikowert zugeordnet und nur dann Alarm geschlagen, wenn Schwellenwerte überschritten werden. Das Resultat sind mehr richtig positive Meldungen. Und das Risk-based Alerting von Splunk ist – anders als bei anderen Lösungen – auf SOC-Effizienz getrimmt, sodass sich die Teams leichter an ihren jeweiligen Cybersecurity-Frameworks orientieren können.

Für fortgeschrittene Use Cases bietet Splunk ES einsatzfertige, anpassbare Dashboards, Suchläufe und Berichte. Splunk ES umfasst auch die Incident-Nachbereitung und externe Threat-Intelligence-Feeds, damit die Erkennung und Untersuchung von Bedrohungen noch schneller geschehen kann.

Fünf komplexe Probleme, die Sie mit Splunk Enterprise Security lösen können

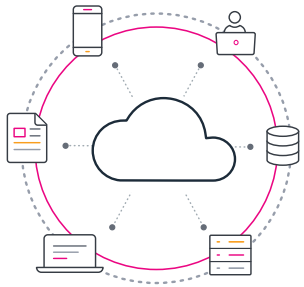
Problem	Lösung	Funktionsweise	Ergebnis
1. Keine umfassende Sicht auf Daten aus unterschiedlichen Quellen (Audits, Firewalls, Windows, Unix, Linux, Endpunkte, Logs).	**Security-Monitoring und Analysen in Echtzeit**	Damit versammeln Sie alle Ihre Daten auf einer zentralen Plattform, sodass Sie sämtliche Vorgänge in Ihrer Umgebung durchsuchen und nachvollziehen können.	Vollständig transparente Sicherheitslage plus die Möglichkeit von sofortigen Suchläufen, Analysen und Priorisierungen sobald ein Problem auftritt.
2. Fortgeschrittene Angriffe und Insider-Bedrohungen, die unbemerkt bleiben und Verluste oder Rufschädigung zur Folge haben..	**Erkennung von fortgeschrittenen Angriffen und Insider-Bedrohungen**	Mit erweiterten Analysen spüren Sie komplexe Bedrohungen und übel gesinnte Insider auf, die sich herkömmlichen Erkennungsmethoden entziehen.	Frühzeitige und rasche Verhinderung von Sicherheitsvorfällen, noch ehe sie unwiderruflichen Schaden anrichten.
3. Keine Möglichkeit, Daten zu durchsuchen, sodass Untersuchungen langsam und umständlich werden.	**Vorfalluntersuchung und Forensik**	Sie bekommen den kompletten Kontext eines Events, die Fehler-Ursachen-Analyse wird einfacher, und sowohl Suche als auch Reporting geschehen schnell und flexibel.	Schnelle und einfache Untersuchung von Sicherheitsereignissen, Beweismittelsicherung und Schadensrisikobewertung.
4. Keine zentrale Datenübersicht für Drill-downs und Suchläufe, keine vorausschauenden Analysen oder maschinelles Lernen, sodass die Bedrohungssuche langsam und umständlich wird.	**Threat Hunting**	Flexible Suchfunktionen, maschinelles Lernen und zusätzliche Bedrohungsinformationen ermöglichen eine gründliche Suche und Analyse.	Proaktive Suche nach Cyberbedrohungen, die sonst zunächst unentdeckt geblieben wären.
5. Mangelnde Transparenz und keine Möglichkeit der Analyse von IT- und Sicherheitskontrollen, was Compliance-Verstöße zur Folge haben kann (sowie empfindlich hohe Geldbußen).	**Compliance**	Damit führen Sie kontinuierliche Risikobewertungen durch, führen Daten aus dem gesamten Unternehmen zusammen, analysieren sie, erstellen belastbare Reports und halten die relevanten Bestimmungen zuverlässig ein.	Nachweis und Demonstration der effektiven Erfüllung von Compliance-Anforderungen und regulatorischen Vorgaben.

Das SIEM aus der Cloud, für die Cloud

Die meisten Unternehmen sind derzeit unterwegs in die Cloud. Die vielen Tools und Services, die Compliance und die Migration selbst machen das Monitoring dann zu keiner leichten Aufgabe. Die Sicherheitsteams benötigen Tools, die sich problemlos in ihre Clouds integrieren lassen. Splunk ES bietet Ihnen Security-Monitoring-Inhalte, die diese Arbeit einfacher machen. Egal wo Ihre Daten liegen.

Splunk ES bringt einsatzfertige Erkennungen und Untersuchungen mit, die speziell auf die wichtigsten Cloud-Anbieter zugeschnitten sind: Amazon Web Services, Google Cloud Platform (GCP) und Microsoft Azure. Damit funktioniert das Monitoring sowohl von On-premises-Daten als auch von Cloud-Daten, die Sie nahtlos in Ihre Erkennungs- und Untersuchungsworkflows einbinden können. Splunk ES arbeitet unabhängig vom Cloud-Provider. Das gibt Ihnen die Sicherheit, einen IT-Infrastruktur- und Anwendungsanbieter zu wählen, der für Ihr Unternehmen am sinnvollsten ist. Sie haben also weiterhin volle Freiheit bei der Wahl Ihrer IT-Infrastruktur und Apps.

Und da es mittlerweile praktisch alles „as a Service“ gibt – warum sollte gerade Ihr SIEM nicht ein SIEM-Service sein? Wenn Sie die Bereitstellung von Splunk Enterprise Security über Splunk Cloud wählen, kann sich Ihr Team sofort auf wirklich lohnende Aufgaben konzentrieren. Splunk ES auf Splunk Cloud ist hochgradig skalierbar, sodass Ihr Monitoring Terabyte an Daten pro Tag bewältigen kann. So verbinden Sie die wirtschaftlichen Vorteile und die raschere Wertschöpfung der Cloud mit den starken marktführenden SIEM-Funktionen, die ein Unternehmen braucht.



Mehr Sicherheit auf guter Grundlage

Splunk ES ist Teil eines umfassenderen Sicherheitsportfolios, das auf Splunk Enterprise oder Splunk Cloud als zentraler Datenplattform aufsetzt. Hierzu gehören noch weitere Produkte, mit denen Ihr Team die MTTD (Mean Time to Detect) verkürzen und besser auf Incidents reagieren kann:

- **Splunk UBA (User Behavior Analytics)** erkennt komplexe Bedrohungen und anormales Verhalten mithilfe von maschinellem Lernen.
- **Splunk SOAR (Security Orchestration, Automation and Response)** beschleunigt die Sicherheitsworkflows durch Incident-Response-Automatisierung und -Orchestrierung.
- **Splunk Intelligence Management (Threat Intelligence)** automatisiert die Datenorchestrierung, sodass Bedrohungsinformationen zentralisiert, strukturiert und gewichtet durchgängig zur Verfügung stehen.

Intelligente Sicherheit mit ML und Automatisierung

Splunk UBA, das Tool zur Verhaltensanalyse, kann mithilfe von maschinellem Lernen (ML) unbekannte Bedrohungen und Anomalien erkennen, die von herkömmlichen Sicherheitstools meist übersehen werden. Ihre Analysten arbeiten damit deutlich produktiver, weil es Hunderte von Abweichungen als einzige Bedrohung identifiziert. Tiefgreifende Untersuchungen und trennscharfe Verhaltensgrundlinien sorgen für schnelleres Threat Hunting.

Splunk SOAR sorgt dafür, dass Ihr Team smarter arbeitet, schneller reagiert und Vorfälle effizienter bewältigt. Das Tool automatisiert wiederkehrende Aufgaben, sodass Ihre Sicherheitsfachleute ihre Zeit und Aufmerksamkeit den Incidents und Aktionen widmen können, auf die es wirklich ankommt. Splunk SOAR reduziert die Verweildauer durch automatisierte Untersuchungen und verkürzt die Reaktionszeiten durch Playbooks, die in Maschinengeschwindigkeit ablaufen. Splunk SOAR bezieht auch Ihre übrige Sicherheitsinfrastruktur mit ein, sodass jeder Teil davon aktiv an der Verteidigungsstrategie beteiligt ist und alle Teile zusammenarbeiten.

Splunk Intelligence Management ist das Tool, das Bedrohungsinformationen schnell und einfach verfügbar macht. Es bricht Datensilos auf, stärkt Cyberresilienz und operative Effizienz und trägt so dazu dabei, die Sicherheitseffektivität an den Geschäftszielen auszurichten. Mit Splunk Intelligence Management kann Ihr Team die relevanten Informationsquellen einfach auswählen, ob Open Source, von Premium-Anbietern oder Sammlungen vergangener Ereignisse und Warnmeldungen. Darauf lassen sich dann Prioritätsbewertungen, Safelists und Filter nach Indikatortyp oder Attribut anwenden; die aufbereiteten Daten können in Datenrepositories abgelegt oder gezielt an eine ausgewählte Anwendung übermittelt werden.

Noch mehr Integrationen und Sicherheit

Für Splunk ES gibt es außerdem die Unified App. Sicherheitsfachleuten fällt es damit leichter, rasch Erkenntnisse abzurufen, sodass sie Bedrohungen schneller im Kontext einordnen und Prioritäten setzen können. Analysten verschaffen sich damit Einblick in aktuelle Angriffstrends, indem sie die Daten in Splunk mit Threat-Intelligence-Feeds und Case-Management-Daten anreichern.

Abgesehen davon gibt es in der Splunkbase noch Tausende von sicherheitsrelevanten Apps mit einsatzfertigen Suchläufen, Berichten und Visualisierungen für Produkte einzelner Drittanbieter. Diese Apps, Dienstprogramme und Add-ons leisten Ihrem Team beim Umgang mit Security Monitoring, Next-Generation Firewalls, erweiterten Bedrohungsmanagement und vielem mehr gute Dienste.

Und am Ende können Sie sich immer noch auf Splunk SURGe verlassen. Dieses Team aus engagierten Splunk-Fachleuten, die auf Security, Threats und Beratung spezialisiert sind, unterstützen Sie mit zeitnahen Untersuchungen, technischen Anleitungen und taktischen Empfehlungen.

Nicht zuletzt haben Sie als Basis für Splunk ES ja die Splunk-Datenplattform. Sie können also auch sonst Erkenntnisse gewinnen und Probleme lösen, die nicht direkt die Sicherheit betreffen. Die gleichen Daten können Sie sich auch für praktisch beliebige IT-, DevSecOps- und Business-Projekte zunutze machen.

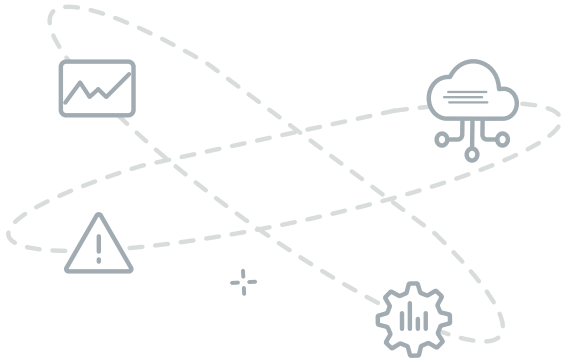
Reden wir über den ROI

Aber ist ein datengestütztes modernes SIEM nicht ziemlich teuer? – Das kommt darauf an, wie man es betrachtet. Wirklich teuer wird es, wenn Sie Opfer einer Insider-Kompromittierung, eines Ransomware-Angriffs oder einer anderen Bedrohung werden, was gleichermaßen kostspielig und rufschädigend ist. Wenn Sie das Risiko dieser Kosten in Betracht ziehen, dann ist eine datengestützte Sicherheitslösung eine ziemlich kluge Investition.

Ein modernes SIEM rentiert sich unmittelbar, weil Sie damit Kompromittierungen vermeiden und Ihr Unternehmen proaktiv vor internen und externen Angreifern schützen. Das ist aber noch nicht der gesamte ROI.

Ein datengestütztes SIEM leistet außerdem bei IT-Themen wie Compliance, Betrugs-, Diebstahl- und Missbrauchserkennung wertvolle Dienste. Hilfreich ist es auch für IT-Betrieb, Service Intelligence, Anwendungsbereitstellung und Geschäftsanalytik. Mit Splunk als SIEM arbeitet Ihr Sicherheitsteam eng mit den anderen IT-Bereichen zusammen, was zu einer besseren abteilungsübergreifenden Zusammenarbeit führt – und einen insgesamt höheren ROI ergibt.

Worin der Wert eines datengestützten SIEM liegt, begreift man am besten, wenn man sich anhört, was diejenigen sagen, die bereits damit arbeiten.



Die Arizona State University enttarnt Betrüger und spart mit Splunk 780.000 Dollar pro Jahr

Als größte Bildungseinrichtung der Vereinigten Staaten setzt die Arizona State University (ASU) weltweit Standards in Sachen Hochschulsicherheit. Um Studierende und Dozenten vor Bedrohungen wie Betrug zu schützen, griff man zu Splunk, um die Systeme zu sichern.

Seitdem verzeichnet die ASU u. a. die folgenden Verbesserungen:

- Weniger Betrug bei Gehaltsabrechnungen und Überweisungen in einem 889-Millionen-Dollar-Haushalt mit über 14.600 Beschäftigten.
- Einsparungen von rund 780.000 Dollar pro Jahr.
- Zentrale Zusammenführung von Schlüsseldaten, was den Umgang damit deutlich erleichtert, auch für Studierende und Universitätsangehörige.

Die ASU nutzt Splunk nämlich nicht nur zur Sicherheit, sondern auch für ein weiteres wichtiges Ziel: die Verbesserung der User Experience von Studierenden und Beschäftigten. Indem die Universität die Schlüsseldaten des gesamten Campus zentral zusammenführte, hat sie Einblick in zuvor getrennte Systeme, kann Probleme schneller beheben und sorgt so für einen reibungslosen Studienverlauf.

Sehen Sie sich das Video dazu an und erfahren Sie, wie Hochschulen und Universitäten mit Splunk ihre Effizienz steigern.

ASU Arizona State University

> **„Dank Splunk können wir jetzt sehen, wie Studierende die Uni erleben, wir können Daten sammeln, aggregieren und auswerten, sodass wir Geschäftsentscheidungen schneller als je zuvor treffen.“**
>
> — Nate Plamondon, Splunk Architect, Arizona State University

InfoTeK baut mit Splunk eine Security-Intelligence-Plattform für die öffentliche Hand

Vielerlei Organisationen sind auf SIEM-Software angewiesen, zum Monitoring von Bedrohungen, für Untersuchungen und für die Vorfallreaktion. Bei einer US-Bundesbehörde scheiterte dies jedoch daran, dass das alte SIEM (HP ArcSight) nicht ganz halten konnte, was es versprochen hatte. Man wandte sich also an InfoTeK, einen führenden Anbieter von Cybersicherheitslösungen, Software und Systementwicklung, der das alte SIEM ersetzen sollte.

Seit der Einführung von Splunk Enterprise mit Splunk ES verzeichnet das Unternehmen deutliche Verbesserungen:

- Bereitstellung an einem einzigen Wochenende und direkte Abwehr eines Angriffs schon am nächsten Tag.
- 75 % Ersparnis bei den laufenden SIEM-Kosten.
- Deutlich weniger Einzeltools, darunter auch Log-Aggregatoren und Endpunktlösungen.

Mit Splunk Enterprise und Splunk ES verfügt die Behörde nun über ein analysegestütztes SIEM, das dem IT-Team verwertbare Sicherheitsinformationen zu vertretbaren Kosten zur Verfügung stellt. InfoTeK konnte die Splunk-Software an einem einzigen Wochenende beim Kunden implementieren. Und schon am nächsten Tag konnte die Software ihren Wert unter Beweis stellen: Das IT-Team durchsuchte die Security Events und konnte sofort einen Angriff erfolgreich abwehren.

Lesen Sie die ganze Fallstudie und erfahren Sie, wie InfoTeK die SIEM-Kosten um 75 % senken konnte.

INFOTEK

”Was mit anderen Produkten Stunden, Tage oder sogar Wochen dauerte und immer wieder Wechsel zwischen verschiedenen Tools erforderlich machte, kann jetzt mit Splunk in Sekunden, Minuten oder Stunden erledigt werden.“

”Wir konnten schon vor der vollständigen Bezahlung einen Produkt-ROI erzielen, da der Kunde erfolgreich eine Bedrohung stoppte, die einen kompletten Neuaufbau des Netzwerks erforderlich gemacht hätte.“

— Jonathan Fair, Senior Incident Handler and Security Engineer, InfoTeK

Heartland Automotive schützt seine Marke und sichert seine Daten mit Splunk

Heartland Automotive Services, Inc., besser bekannt als Jiffy Lube, ist das größte Ölwechsel-Franchise-Unternehmen in den USA. Dort brauchte man dringend eine Cybersicherheitsplattform, denn es galt, sowohl die Marke zu schützen als auch die wichtigste Ressource: die Daten.

Seit der Einführung von Splunk ES und Splunk UBA als integrierte SIEM-Plattform verzeichnet Heartland Automotive deutliche Verbesserungen, darunter diese:

- Rasche Wertschöpfung durch die SIEM-Implementierung (mit Schutz vor Insider-Bedrohungen) in nur drei Wochen.
- Größere Innovationskraft durch Plattformunterstützung bei 25 % geringeren Gesamtbetriebskosten (TCO).
- Sicherheitsuntersuchungen in Echtzeit und wirksamer Schutz vor Insider-Bedrohungen.

SIEM-Implementierungen sind oft komplex, da es bei großen Unternehmen viele Datenquellen gibt und die Konfiguration der Warnmeldungen Wochen dauern kann. Doch laut Chidi Alams hat das Team von Splunk Professional Services es geschafft, den gesamten Prozess – von der Identifizierung der Datenquellen über die Ausarbeitung des SIEM-Designs bis zur Konfiguration der Alerts – reibungslos zu gestalten.

Lesen Sie die ganze Fallstudie und erfahren Sie, wie Heartland Automotive mit Splunk für Innovation sorgt und 25 % TCO einspart.

jiffy lube®

„Eine minimale Vorlaufzeit war uns wichtig – wir konnten das SIEM samt Erkennung von Insider-Bedrohungen in drei Wochen implementieren. Normalerweise dauert so etwas drei Monate.“

„Der Chief Financial Officer und das obere Management waren von der Time-to-Value sehr beeindruckt. Das Produkt gezeigt zu bekommen und am nächsten fast schon implementiert zu sehen – das hat sie sehr zuversichtlich gemacht, das wir schnell zu Ergebnissen kommen.“

— Chidi Alams, Head of IT and Information Security, Heartland Automotive Services

Zukunftssicher aufgestelltes SIEM

Die Sicherheitsbedrohungen werden sich weiter entwickeln, und die technologischen Umstände werden bestimmt auch nicht einfacher. Sich mit einem SIEM zufriedenzugeben, das gerade die heutigen Anforderungen erfüllt, ist also keine gute Idee. Vor allem, wenn Sie eins bekommen könnten, das Ihnen hilft, die Herausforderungen von morgen zu meistern.

Ein datenzentriertes SIEM mit robusten Funktionen wie Echtzeitmonitoring, automatisierter Vorfallreaktion, User-Monitoring, erweiterten Analysen etc. ist eine solide Grundlage für die Zukunft. Und durch die Kombination eines datenzentrierten SIEM mit fortschrittlicher Bedrohungserkennung und SOAR-Technologien auf einer einzigen Plattform ist Ihr SOC noch besser für die Aufgabe gerüstet, Ihr Unternehmen heute und in Zukunft zu schützen.

Eine zukunftsfähige Security-Operations-Plattform, mit der ihr Team Sicherheitsereignisse über deren gesamten Lebenszyklus hinweg kontrollieren kann – und zwar durchgängig auf einer gemeinsamen Oberfläche –, ist für die schnelle Eindämmung und Behebung von Cyberangriffen absolut entscheidend. Ihr Team kann dann schnell auf die immer neuen Bedrohungen reagieren und Ihr Unternehmen schützen, indem es Daten, Analysen und operative Lösungen immer wieder optimiert und aktualisiert.

Splunk selbst entwickelt fortlaufend neue Sicherheitsfunktionen und Integrationen, die Ihnen für die Zukunft helfen sollen. Dazu zählen z. B. integrierte Bedrohungsinformationen, eine leistungsstarke Verhaltensanalytik aus der Cloud und erweiterte risikobasierte Warnmeldungen.

Mit geballter Datenpower

Ihr Job war immer schon hart genug. In den letzten Jahren ist er noch härter geworden. Es ist jetzt an der Zeit, Ihre Daten zum Einsatz zu bringen. Ihr Unternehmen braucht leistungsstarke, flexible und schnelle Lösungen – Lösungen, die mit Daten arbeiten.

Mit einer starken Daten- und Technologiebasis können Unternehmen rasch reagieren – ganz gleich, was auf sie zukommt. Splunk ist die Datenplattform für die hybride Welt. Mit Splunk können Unternehmen Innovationen freisetzen, ihre Sicherheit verbessern und ihre Widerstandskraft härten.

Mit Splunk als Cloud-basiertem, analysegestütztem SIEM schafft Ihr Unternehmen Sichtbarkeit bei sämtlichen Datenquellen und Prozessen, hält Schritt mit allen Sicherheits- und Compliance-Vorschriften und bleibt Cyberbedrohung stets einen Schritt voraus.

Sind Sie bereit, Splunk zu Ihrer SIEM-Lösung zu machen? Hier erfahren Sie mehr.

Erste Schritte.

Sind Sie bereit, mehr über das analysegestützte SIEM von Splunk zu erfahren und darüber, wie es dazu beitragen kann, die Sicherheitslage Ihres Unternehmens zu verbessern? Sprechen Sie jetzt mit einer Expertin oder einem Experten von Splunk.

22-23827-Splunk-SIEM Buyers Guide-EB-102_GER

splunk> turn data into doing