# Die fünf wichtigsten SIEM-Trends 2022

splunk>
turn data into doing®

SIEM-Systeme (Security Incident and Event Management) gibt es schon seit etlichen Jahren, die Kernfunktionen reichen sogar mehr als ein Jahrzehnt zurück. Seitdem haben sich SIEM-Lösungen von Tools fürs Log-Management zu Informationsplattformen entwickelt, wobei der SIEM-Markt größtenteils von den Anforderungen aus dem Enterprise-Segment bestimmt wird. Allein in den letzten Jahren ist der SIEM-Markt von 2 Milliarden Dollar auf unglaubliche 4,1 Milliarden Dollar gewachsen.

Untersuchungen führender Marktanalysten haben außerdem ergeben, dass die Kosten von Datensicherheitsverletzungen im Jahr 2024 vermutlich die 5-Billionen-Dollar-Marke übersteigen werden. Das wäre fast das Doppelte der Summe aus dem Jahr 2019, die sich auf lockere 3 Billionen US-Dollar belief. Doch dank der neueren Funktionen von SIEM-Software können Unternehmen diese Art von Risiko minimieren und die meisten (wenn auch nicht alle) Bedrohungen stoppen, bevor ernsthafter Schaden entsteht. Der Gartner Magic Quadrant für Security Information und Event Management hebt diese Entwicklungen hervor, vor dem Hintergrund, dass die Anbieter ihre SIEM-Software ständig weiterentwickeln und verbessern.

## Mit Blick auf die vielen spannenden Funktionen, die sich abzeichnen, stellen wir Ihnen hier **fünf SIEM-Trends für 2022 vor:**

1. Cloud- und App-Sicherheit werden weiterhin höchste Priorität haben.
2. Der Schwerpunkt wird stärker auf risikobasierten Warnungen liegen.
3. Bedrohungsdaten und integrierte Security-Inhalte sind jetzt erfolgsentscheidend.
4. Automatisierung steigert die Effizienz, Produktivität und Reaktionsfähigkeit.
5. Insider-Bedrohungen werden leichter zu erkennen und zu bewältigen sein.

01

# Cloud- und App-Sicherheit werden weiterhin höchste Priorität haben

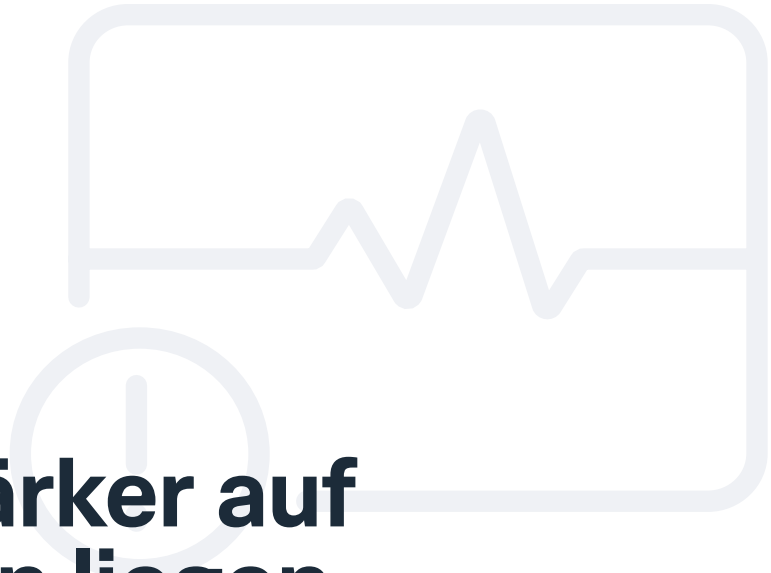
Seit ein immer größerer Teil der Arbeit mit Cloud-Lösungen geschieht – was zuletzt vor allem mit Covid-19 und dem massenhaften Umzug ins Homeoffice zu tun hat –, ist eine moderne Sicherheitslösung unerlässlich geworden, für große und für kleine Unternehmen gleichermaßen. Die Wirtschaft migriert in einem unglaublichen Tempo in die Cloud, und da so viele Unternehmen zu Cloud-Infrastrukturen wechseln, wird immer deutlicher, wie dringend notwendig es jetzt ist, die Cloud-Strategie zu schärfen und aktualisieren – oder endlich eine zu formulieren.

Die technische Komplexität der Migration ist nur eine der Herausforderungen, denen sich ein Unternehmen auf dem Weg zu Cloud-nativen Lösungen stellen muss. Wenn einzelne Teams mit Digitalisierungsprojekten vorpreschen, übersehen sie dabei meist die allgemeinen Sicherheitsanforderungen, weil es ihnen nur darum geht, schneller als der Wettbewerb zu sein und die veränderten Bedürfnisse zu decken. Dies führt letztlich zu höheren Risiken, vor allem dann, wenn das Unternehmen bei Netzwerksicherheit, Zugangskontrolle und Cloud-Konfigurationsoptionen nicht auf dem neuesten Stand ist.

In Verbindung mit einer zunehmenden Angriffsfläche und mangelnder Transparenz ist eine Kompromittierung dann nur mehr eine Frage der Zeit. Genau aus diesem Grund sollte eine robuste SIEM-Lösung sofort einsatzbereite Out-of-the-box-Inhalte fürs Cloud-Security-Monitoring mitbringen; dann fällt es leichter, Bedrohungen in Cloud-, Hybrid- und Multi-Cloud-Umgebungen zu erkennen und darauf zu reagieren. Dazu gehören am besten auch fortgeschrittene Erkennungsregeln für Cloud-Angriffe sowie eine breite Palette bekannter Cloud-Angriffsmuster, damit man die Erkennung laufend testen und verbessern kann.

Im Zeitalter der Telearbeit muss eine SIEM-Lösung in der Lage sein, sämtliche Cloud- und Endpunktdaten zu erfassen und zu analysieren – unabhängig von Volumen, Art und Geschwindigkeit. Die herkömmliche Überwachung reicht längst nicht mehr aus. Sicherheitsteams müssen Daten aus einer Vielzahl von Quellen und über alle Arten von Umgebungen hinweg analysieren und erfassen können, wenn sie wissen wollen, wo genau ein Security-Ereignis stattfindet und was es bedeutet.

02



# Der Schwerpunkt wird stärker auf risikobasierten Warnungen liegen

Mit Alarmmüdigkeit (Alert Fatigue) haben arglose Analysten jeden Tag zu kämpfen. Warnmeldungen auf der Grundlage von weit gefassten Erkennungsdefinitionen können zu einer hohen Anzahl von Fehlalarmen und einer Menge zusätzlichem Rauschen im SOC (Security Operations Center) führen, was die Leute an der Front dann schnell überfordert und überlastet.

Es ist also kein Wunder, dass SIEMs besser werden müssen, wenn sie gezielte Angriffe und Sicherheitsverletzungen effektiv erkennen und darauf reagieren sollen. Namentlich die Technologie risikobasierter Warnungen (RBA/Risk-based Alerting) – eine neuere Methode zur Identifizierung von Bedrohungen – kann Benutzern und anderen Entitäten definierte Risikowerte zuweisen. RBA löst einen Alarm aus, sobald bestimmte Verhaltens- und Risikoschwellenwerte überschritten werden.

Auf diese Weise geht die Anzahl der Warnmeldungen zurück, während der Anteil der richtig positiven Meldungen steigt, auch dadurch dass die Sicherheitsteams nun auch ausgeklügelte Angriffe aufdecken, die bei herkömmlichen Suchvorgängen oft übersehen werden.

Ein SIEM, das mit solchen Verhaltensprofilen in Kombination mit Bedrohungsdaten und Analysen arbeitet, kann den Erkennungserfolg exponentiell verbessern, weil es Zeit und Ressourcen freisetzt, sodass die Sicherheitsfachleute sich auf komplexe Bedrohungen mit hoher Eintrittswahrscheinlichkeit konzentrieren können. Analysten weisen den einzelnen Entitäten das jeweilige Risiko im Abgleich mit einem ausgewählten branchenüblichen Sicherheits-Framework zu (MITRE ATT&CK, NIST Cybersecurity Framework etc.).

03

# Bedrohungsdaten und integrierte Security-Inhalte sind jetzt erfolgsentscheidend

Es ist keine leichte Aufgabe, die Regelsätze eines Sicherheitsprogramms zu pflegen und weiterzuentwickeln. Bei so vielen unterschiedlichen Quellen und der Vielzahl von Datenstrukturen und -formaten, die es zu durchforsten gilt, kann es lange dauern, bis man endlich mühsam die nötigen Bedrohungsinformationen eingearbeitet hat. Das gilt ganz besonders dann, wenn den Sicherheitsteams nur wenig bis gar keine Bandbreite für die Erstellung der erforderlichen Erkennungen und Playbooks zur Verfügung steht.

Heutzutage kann eine moderne SIEM-Lösung die erforderlichen Bedrohungsdaten (Threat Intelligence) aber bereits integrieren (d. h. kuratierte, im Produkt integrierte Erkenntnisse der Security-Forschung zu bekannten und zu neuen Bedrohungen), sodass sie in jeder Phase des Incident-Response-Workflows zur Hand sind – ebenso wie für das gesamte Ökosystem aus Teams, Tools, Peers und Partnern. Die ebenfalls bereitgestellten Anleitungen helfen den Anwendern außerdem, Angriffen zuvorzukommen und komplexe Pipelines zu erstellen, ohne dass sie im Backend Skripte schreiben oder pflegen müssten.

Und schließlich hat sich ein schnell wachsender Intelligence-Markt für Bedrohungsdaten ausgebildet, auf dem vielerlei kommerzielle ebenso wie Open- und Community-Quellen vertreten sind. Mit diesen Ressourcen im Rücken können SIEM-Lösungen mittlerweile einfacher die neuesten technischen Anleitungen und Hintergrundinformationen zum Kontext integrieren – wer steckt hinter dem Angriff, welche Techniken verwendet er? –, sodass die Analysten sie bei der Untersuchung und der Reaktion auf eine Warnung Schritt für Schritt abarbeiten können.

# 04

# Automatisierung steigert die Effizienz, Produktivität und Reaktionsfähigkeit

Manche Sicherheitsaufgaben sind einfach zu umfangreich und zu zäh, als dass die Teams sie von Hand erledigen sollten. Ganz zu schweigen davon, dass es aufgrund des Fachkräftemangels im Sicherheitsbereich ohnehin schwierig ist, genügend Talente zu finden (und zu gewinnen), die das Arbeitsaufkommen des Unternehmens bewältigen könnten. So kommt es, wie es kommen muss: Die Überlastung durch Routinearbeiten führt zum Burn-out bei den Analysten, während wirklich dringende Bedrohungen unbemerkt bleiben. Der einzige Weg zu mehr Produktivität, Effizienz und Geschwindigkeit – ohne dass die Analysten dabei wahnsinnig werden – führt über die Automatisierung.

An dieser Stelle hat SOAR seinen großen Auftritt (Security Operations, Automation and Response). Heutzutage erwartet man von einer SIEM-Lösung, dass sie SOAR integriert, die Analysten von Routinearbeit entlastet und Sicherheitsvorfälle in Rekordzeit löst – mit Reaktionen in wenigen Sekunden statt in Minuten oder gar Stunden.

Ein SOAR-Tool schafft das, indem es Informationen aus mehreren Tools zusammenführt, die Alarmdaten damit anreichert und das Ganze auf einer einzigen Oberfläche anschaulich darstellt. Durch die Automatisierung der Datenzusammenführung bekommen die Analysten in dem Moment, in dem eine Warnmeldung auftaucht, auch schon wertvolle Details angezeigt, die mit der Warnung in Zusammenhang stehen.

Unterm Strich ermöglichen Orchestrierung und Automatisierung den Sicherheitsteams sehr viel schnellere Untersuchungen und Reaktionen. Außerdem reichert SOAR die gesammelten Daten um zusätzliche Informationen an, die das Tool aus verschiedenen Quellen bezieht und bündelt. Wenn die Entscheidungen und Maßnahmen von Untersuchung, Priorisierung und Reaktion auf diese Weise orchestriert sind, können die Sicherheitsteams auch bei großen Mengen von Warnmeldungen den Risikograd schnell bestimmen und entsprechend reagieren.

05

# Insider-Bedrohungen werden leichter zu erkennen und zu bewältigen sein

Weil Insider-Bedrohungen am schwersten zu entdecken sind – und potenziell am meisten Schaden anrichten – hat sich UEBA (User and Entity Behavior Analytics) etabliert, als ein wichtiges Instrument zur Erkennung verdächtiger Muster, die auf den Diebstahl von Zugangsdaten, Betrug und andere Schadaktivitäten hindeuten können. Im Prinzip identifiziert UEBA sämtliche Anwender und Entitäten und beobachtet deren Verhalten in den Umgebungen des Unternehmens; diese Informationen durchlaufen eine Reihe von Algorithmen, sodass sich Verhaltensweisen erkennen lassen, die vom üblichen und erwarteten abweichen.

In der Vergangenheit war UEBA nur ein Schritt im Rahmen eines mehrstufigen Ansatzes: Die Unternehmen fingen mit einem SIEM-Kernsystem an und erweiterten es irgendwann um UEBA und/oder SOAR (und mehr). Heute wird UEBA von Gartner als eine Schlüsselfunktion im Sicherheitsgefüge angesehen. Es sollte eng mit der SIEM-Lösung zusammenarbeiten, im Idealfall wirklich bruchlos, damit die Verhaltensmuster im Netzwerk möglichst deutlich sichtbar werden.

Unternehmen, die auf eine einzige Plattform mit der kombinierten Power von UEBA und SIEM setzen, profitieren von den Vorteilen, die sich aus der Bedrohungserkennung sowohl bei menschlichem als auch bei maschinellem Verhalten ergeben. Wenn Sie UEBA als Teil Ihres SIEM einsetzen, können Sie Verhaltensanomalien besser erkennen und bekommen zusätzlichen Kontext zu bereits bekannten und zu neuen Bedrohungen. Das spart den Analysten Zeit und steigert die Effizienz Ihres Teams, weil damit falsch positive Ergebnisse eliminiert und stattdessen Bedrohungen mit hoher Eintrittswahrscheinlichkeit aufgezeigt werden, die eine regelbasierte Korrelation nicht erkannt hätte.

Mehr zu aktuellen SIEM-Trends und Best Practices von führenden Security-Fachleuten finden Sie im *Gartner SIEM Magic Quadrant Report.*

Report laden

splunk>
turn data into doing®



22-22392-Splunk-Top 5 SIEM Trends to Watch in 2022-LS-104_GER