Der SOAR-Guide für transformative CISOs

Wie Sicherheitsteams mehr Zeit für proaktive und strategische Aufgaben gewinnen und so zum Innovationsgeist und Erfolg des Unternehmens beitragen

splunk>

Inhalt

Die Unternehmensführung braucht transformative Security-Teams

Die Rolle des Chief Information Security Officers (CISO) verändert sich.

Wie dies auch schon bei CIOs und CTOs der Fall war, entwickeln sich CISOs von einer Rolle mit begrenzten Verantwortungsbereichen zu stark in die Unternehmensführung eingebundenen Fachkräften, die die Transformation des Unternehmens strategisch vorantreiben. Die erfolgreichsten Unternehmen haben erkannt, dass eine echte digitale und unternehmerische Transformation von der Modernisierung der Sicherheit abhängt.

Laut einer PwC-Umfrage suchen 40 Prozent der Führungskräfte CISOs, die funktionsübergreifende, agile Teams leiten können, welche nicht nur mit der digitalen Transformation Schritt halten, sondern vielfach den Weg in die Zukunft weisen.[1]

Eine im Auftrag der Information Security Systems Association (ISSA) durchgeführte Studie ergab, dass Sicherheitsexperten rund um den Globus Kommunikations- und Führungsqualitäten als wichtigste Eigenschaften eines erfolgreichen CISO ansehen.[2]

Diese vier Qualitäten schätzt die Unternehmensführung am meisten:

1. **Strategisches Denken**
2. **Die Fähigkeit, kalkulierbare Risiken einzugehen**
3. **Führungsqualitäten**
4. **Die Fähigkeit, Innovationsmöglichkeiten zu erkennen und auszubauen**

Die ISSA-Umfrage zeigte zudem, dass die meisten Sicherheitsanalysten eine strategischer ausgerichtete Rolle übernehmen möchten und dass ihnen bewusst ist, dass sie Führungs-, Kommunikations- und Business-Fähigkeiten entwickeln müssen, um eine führende Rolle bei Wachstum und Wandel zu übernehmen.

„Informationssicherheit wird nicht mehr nur als Schutz vor Angriffen angesehen, sondern gilt mittlerweile als Möglichkeit, das Unternehmen zu unterstützen und das Geschäft zu fördern.“

– Yassir Abousselham, CISO, Splunk

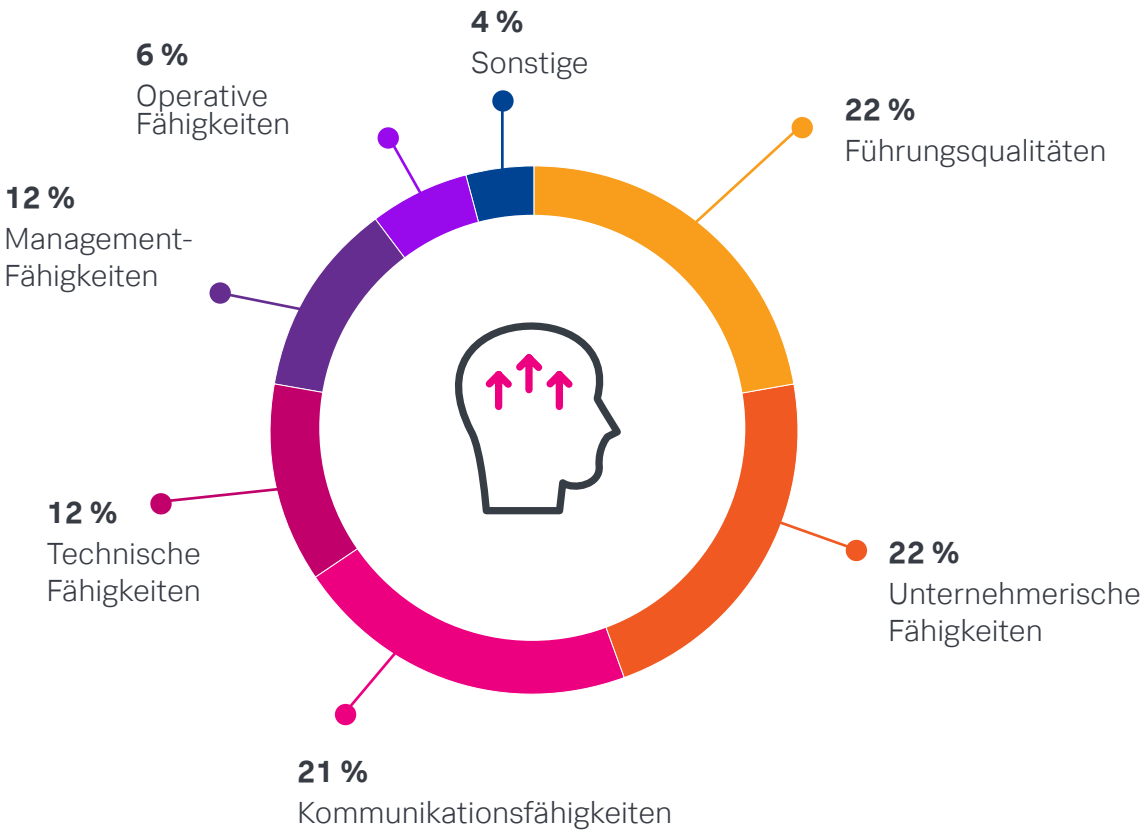
[1]https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/global-digital-trust-insights/cyber-strategy.html

[2]https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf

Sicherheitsanalysten wissen, dass sie mehr als technische Qualifikationen brauchen, um eine Führungsrolle auszufüllen

Die Enterprise Strategy Group fragte Sicherheitsanalysten, welche Fähigkeiten sie entwickeln mussten, um CSOs oder CISOs zu werden.

Quelle: Enterprise Strategy Group



Doch viel zu oft durchkreuzt die tagtägliche Realität aus **zu vielen Warnmeldungen und zu wenigen Mitarbeitern** die strategischen Pläne von Sicherheitschefs und Analysten.

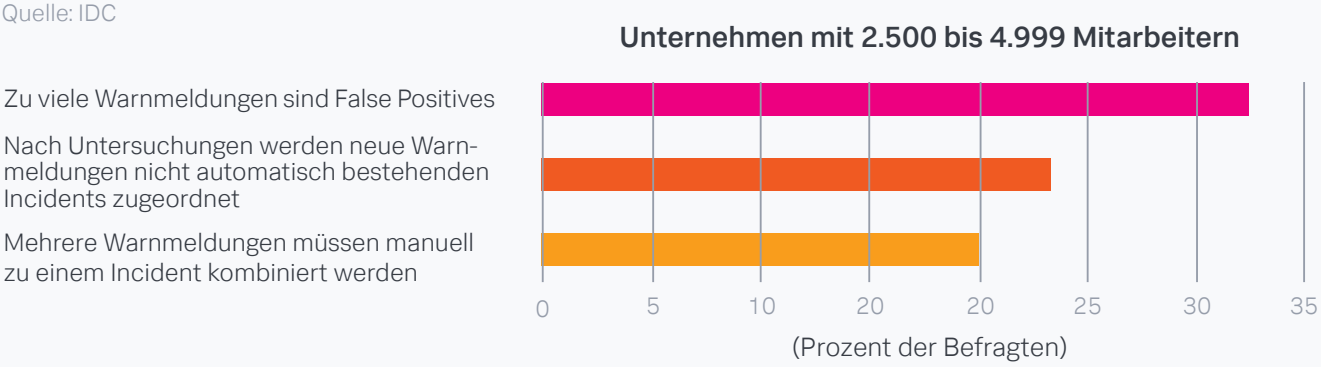
Von Überforderung zu voller Kontrolle

Im Rahmen der ISSA-Umfrage bezeichnete fast ein Drittel der Spezialisten für Cybersicherheit die „überwältigende Arbeitslast“ als den stressigsten Teil ihrer Arbeit. Diese überwältigende Arbeitslast kann sich auf Hunderte – wenn nicht Tausende – von Warnmeldungen pro Tag belaufen, die eine Priorisierung, Untersuchung und Reaktion erfordern.

Die drei Hauptgründe für nicht untersuchte Warnmeldungen

Was verhindert, dass Ihr Unternehmen ALLE verdächtigen Warnmeldungen untersucht und behandelt, die jeden Tag eingehen?

Quelle: IDC



Zu den Herausforderungen wegen der unendlichen Flut von Warnmeldungen kommt erschwerend noch ein Mangel an qualifizierten Fachkräften für Cybersicherheit hinzu. Es gibt schlicht nicht genügend qualifizierte Cybersicherheit-Spezialisten, um die SOCs weltweit ausreichend mit Mitarbeitern auszustatten. Dieser gut dokumentierte Fachkräftemangel, kombiniert mit dem schieren Volumen an Warnmeldungen pro Tag, erklärt, warum 64 Prozent der pro Tag generierten Sicherheits-Tickets nicht bearbeitet werden.[3] Die Analysten schaffen es nicht, sich jeden Tag sämtlichen Warnmeldungen zu widmen, und das macht ihre Unternehmen anfällig für Angriffe.

64 %
der täglichen Sicherheitswarnungen bleiben unbearbeitet[4]

Wenn Security-Teams damit kämpfen, die Warnmeldungen abzuarbeiten, können CISOs keine strategische Richtung vorgeben und Analysten haben keine Zeit, die wichtigen Engineering- und Optimierungsaufgaben durchzuführen, automatisierte Reaktionen auf Benachrichtigungen zu optimieren und proaktiv nach Bedrohungen zu suchen.

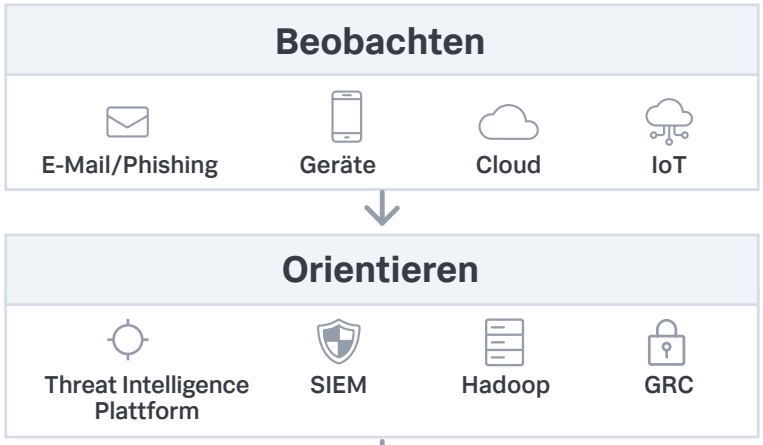
Die Lösung für diese Herausforderungen lautet SOAR (Security Orchestration, Automation and Response). SOAR-Plattformen wie Splunk SOAR verschieben das Kräfteverhältnis beim Thema Sicherheit. Wenn ein SOAR-Produkt Analysten monotone Routineaufgaben abnimmt und Sicherheitstools so orchestriert werden, dass sie zusammenarbeiten, können Teams mehr Zeit darauf verwenden, das Sicherheitsniveau des Unternehmens zu verbessern und das Business zu unterstützen.

[3]https://www.splunk.com/en_us/form/an-enterprise-management-associates-research-report.html

[4]https://www.splunk.com/pdfs/analyst-reports/an-enterprise-management-associates-research-report.pdf

Ein Tag im Leben eines Analysten

Ohne und mit SOAR



10.000 verdächtige Incidents pro Tag

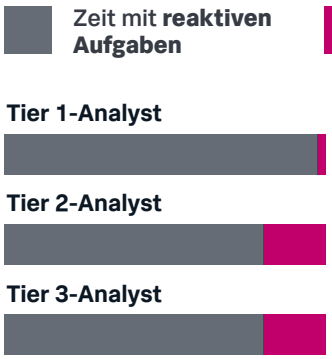
Ohne SOAR

Analysten müssen alle eingehenden Logs und Warnmeldungen **manuell sichten**, analysieren und verwalten

Analyst

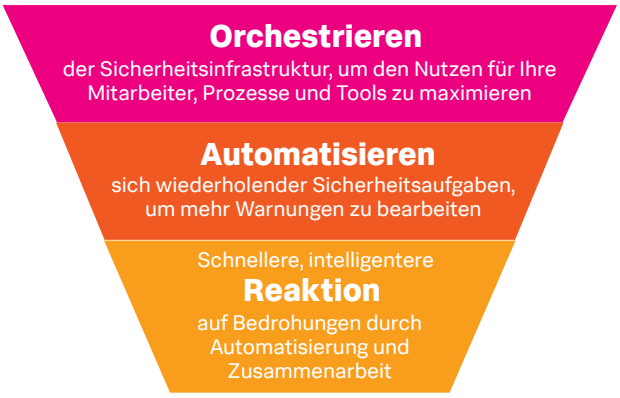
Entscheiden und handeln

Analysten aller Ebenen verbringen die meiste Zeit damit, **zu reagieren** und haben nur wenig Zeit für strategische Maßnahmen.



Zeitaufwand für die Reaktion:
30 Minuten

Mit SOAR

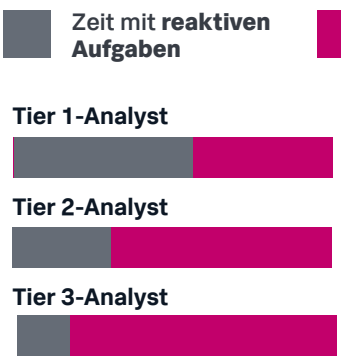


Analyst

Es wird jeden Tag auf jede Warnung reagiert

Entscheiden und handeln

SOAR vereinfacht den Workflow von Analysten: Sie arbeiten zusammen und reagieren schnell auf Sicherheits-Incidents.



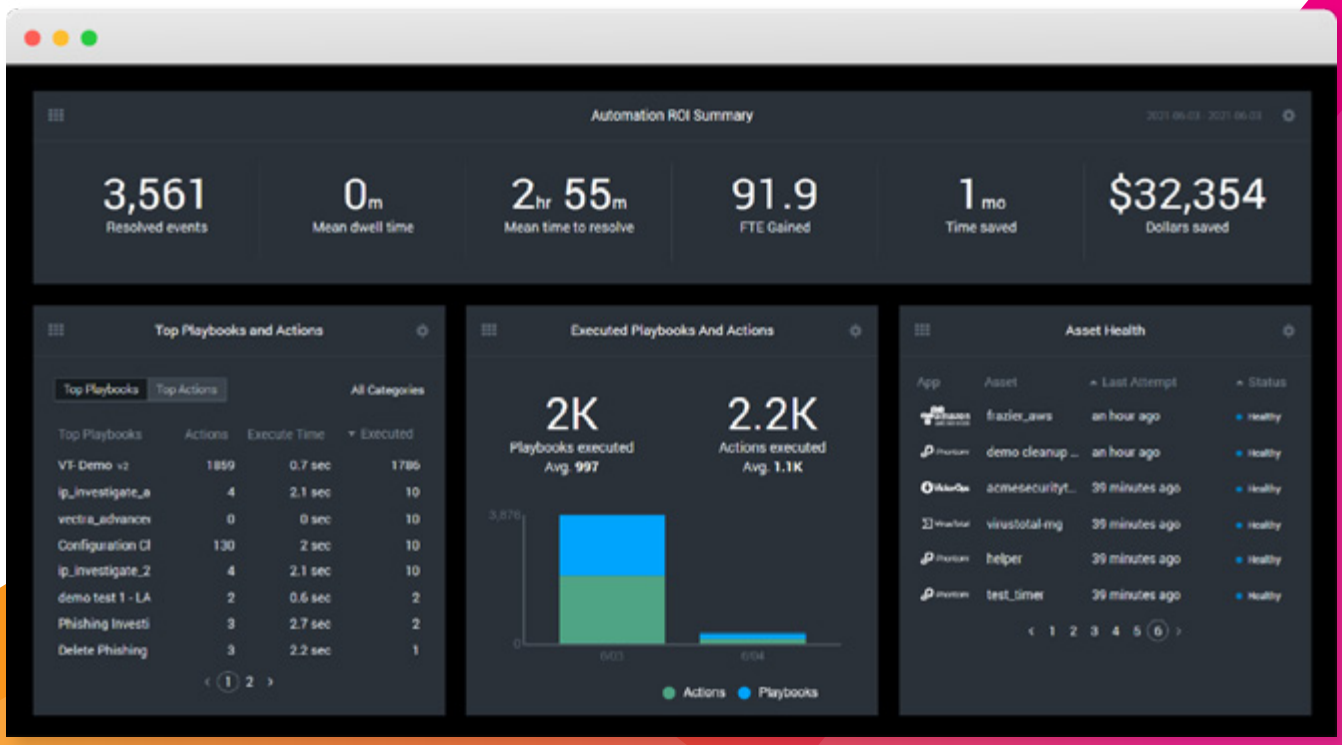
Zeitaufwand für die Reaktion:
30 Sekunden

Der ROI von SOAR

Laut Schätzungen belaufen sich die jährlichen Kosten für die Abwehr von Phishing-Angriffen auf fast 700.000 US-Dollar. Auch Ransomware kann hohe Kosten verursachen und den Ruf nachhaltig schädigen. SOAR spart Zeit und Geld.[5] Die Zeitersparnis wird in der entsprechenden manuellen Arbeitslast eines Vollzeitbeschäftigten gemessen. Mit einer SOAR-Plattform kann ein dreiköpfiges Analystenteam in einem SOC beispielsweise genauso viel bewirken wie ein Team mit 10 bis 15 Analysten, das alle Aufgaben manuell durchführt.

> **„Irgendwann ist man mit der Menge der anfallenden Arbeit überfordert, kann aber keine weiteren Mitarbeiter einstellen. Automatisierung ist dann die einzige Lösung.“**
>
> – Jason Mihalow, Senior Cloud Cyber Security Architect, McGraw Hill
>
> Case Study ansehen

Das Haupt-Dashboard von Splunk SOAR liefert Security-Teams eine Übersicht über SOC-Aktivitäten, relevante Events und Playbooks sowie eine Zusammenfassung des ROI der automatisierten Handlungen. Der Bereich „Automation ROI Summary“ zeigt die Auswirkungen der im SOC genutzten Automatisierung in Echtzeit, wie etwa die Zeitersparnis, die Kostenersparnis, die der Leistung entsprechende Zahl der Vollzeitbeschäftigen und die mittlere Verweildauer.



[5]https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

CASE STUDY

Norlys: Erfolg dank SOAR

Mit 1,5 Millionen Kunden ist Norlys Dänemarks größtes Versorgungs- und Telekommunikationsunternehmen. Nach dem Aufbau eigener Log-Analyse- und Incident Response-Systeme wurde das Security-Team von Norlys durch Routineaufgaben, zu viele Tools, langsame Web-Oberflächen und schwerfällige Prozesse ausgebremst. Mit Splunk konnte Norlys sich wiederholende Aufgaben automatisieren und Untersuchungen zentralisieren.

Case Study ansehen

Ergebnisse:

- 35 Stunden werden pro Woche eingespart
- Die Prozessdauer wurde von 30 Minuten auf 30 Sekunden gesenkt
- 98 % weniger Zeitaufwand für das Öffnen von Tickets

Dies sind die fünf monotonsten Aufgaben, die Norlys automatisiert hat:

1 Übertragen relevanter Ereignisse von Splunk ES an SOAR
Von **3 Minuten** auf **2 Sekunden**

2 Automatisieren der Untersuchung bei Antivirus-Warnungen
Von **40 Minuten** auf **10 Minuten**

3 Automatisieren der Untersuchung bei IOC-Treffern aus Bedrohungs-Feeds
Von **15 Minuten** auf **10 Sekunden**

4 Automatisieren des Abrufs des Browser-Verlaufs
Von **30 Minuten** auf **20 Sekunden**

5 Automatisiertes Öffnen von Tickets für externe Systeme
Von **10 Minuten** auf **10 Sekunden**

Sicherheit modernisieren, Unternehmens transformieren.

Damit CISOs die für Unternehmen notwendige strategische Rolle übernehmen können und Sicherheitsanalysten Möglichkeiten für die berufliche Weiterentwicklung finden, sind Orchestrierung und Automatisierung unerlässlich. Splunk SOAR ermöglicht es Security-Teams, das Potenzial der Investitionen in Sicherheits-Tools und Sicherheitsspezialisten voll auszuschöpfen.

Testen Sie jetzt Splunk SOAR

splunk>