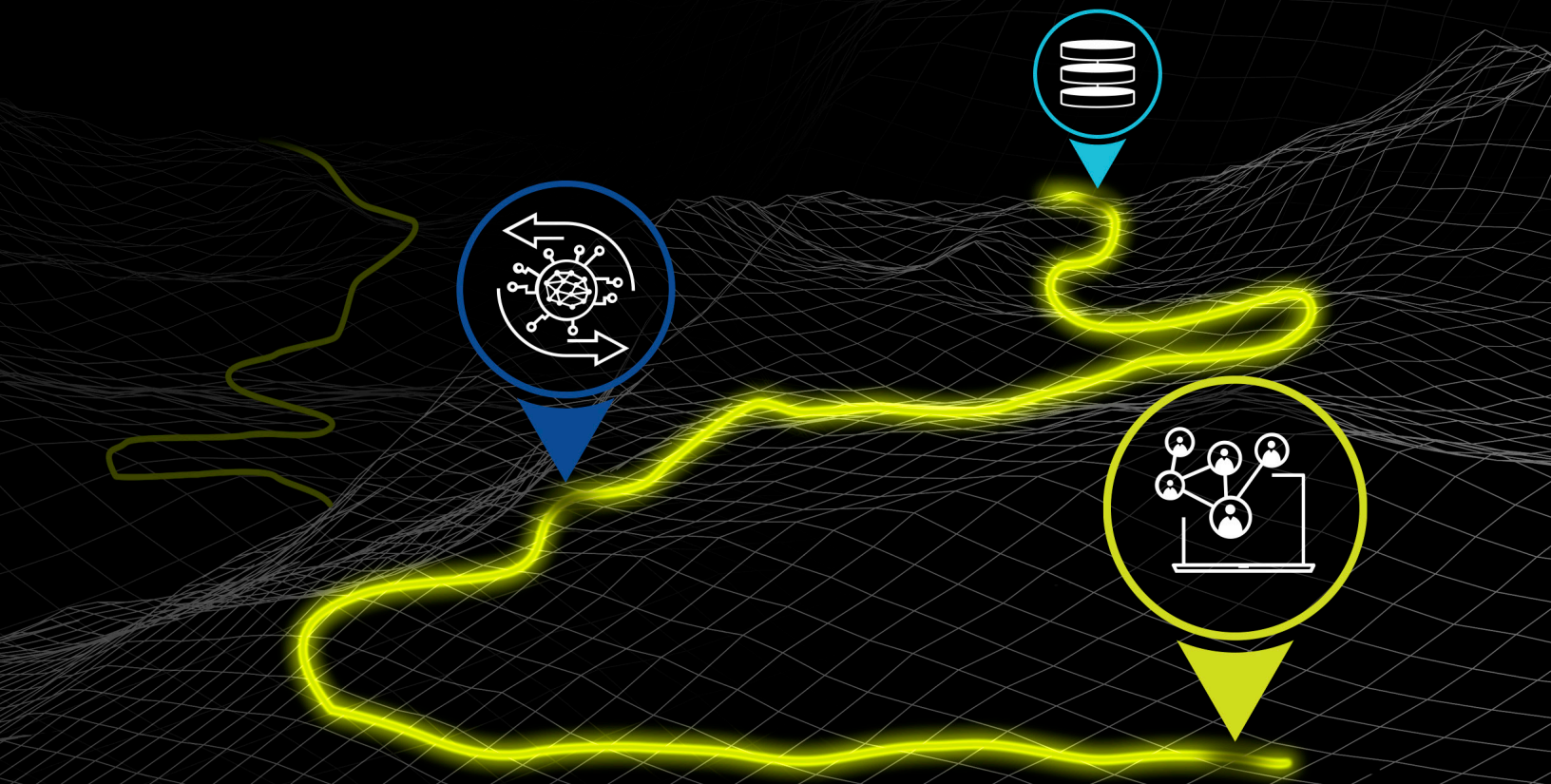
DEVO

Der Pfad zum eigenständigen SOC



aws Available in AWS Marketplace

KURZFASSUNG

Die Führungskräfte der heutigen Security Operations Center (SOC) stehen vor einem schwierigen Balanceakt. Sie müssen komplexe Infrastrukturen und Anwendungen im Zuge der Umstellung auf die Cloud absichern, die digitale Transformation vollziehen und Risiken bewältigen – und gleichzeitig in einem historisch angespannten Arbeitsmarkt qualifizierte Fachkräfte für die Cybersicherheit anwerben und binden.

Hinzu kommt eine sich schnell entwickelnde Bedrohungslandschaft, die sich sehr problematisch mit der zunehmenden Menge an komplexen Angriffen gestaltet: der fehlende Einblick in komplexe Betriebsumgebungen, die Unfähigkeit zur Analyse von Datenmengen in der Cloud und der Kampf um die Verbesserung der Teamleistung führen letztlich zu einer geminderten Produktivität und einem höheren Sicherheitsrisiko.

Der Bedarf an Automatisierung wird sich weiter rasant beschleunigen. Wie die SOCs setzen auch die Angreifer zunehmend Automatisierungsfunktionen ein, und das mit zunehmender Geschicklichkeit.

DAS SOC MUSS SICH WEITERENTWICKELN

Unternehmen, die der exponentiellen Zunahme von Daten aus unzähligen Quellen, dem anhaltenden Mangel an qualifizierten Analysten, der endlosen Liste böswilliger Akteure und dem Umfang und der Bedeutung von Cyberangriffen einen Schritt voraus sein wollen, müssen auf ein neues Modell setzen: das eigenständige SOC. Damit Unternehmen eine immer größere Bedrohungslandschaft erfolgreich abwehren können, wird das eigenständige SOC:

- Die Arbeit von Analysten interessanter und erfüllender gestalten.
- Vollständige Transparenz, Automatisierung und Analysen zusammen mit dem Zugriff auf das neueste Fachwissen der Community, Inhalte und Bedrohungsdaten bieten.
- Sich nahtlos in Sicherheits- und IT-Tools integrieren.
- Führungskräften die Möglichkeit zur Automatisierung von Triage, Untersuchung und Aufspürung eröffnen.

- Schnelle, effektive Erkennung und Reaktion auf Vorfälle für die Beseitigung von Bedrohungen in riesigen Cloud-First-Infrastrukturen bieten.

Mit dem eigenständigen SOC können Führungskräfte die Triage, Untersuchung und Aufspürung automatisieren, damit ihre Teams Bedrohungen in riesigen Cloud-First-Infrastrukturen schnell und effektiv erkennen und auf Vorfälle reagieren können.

WIE DAS EIGENSTÄNDIGE SOC DIESE ZIELE ERREICHEN WIRD

- Heutzutage sind die meisten SOCs als Team strukturiert, das eine Reihe von bewährten Prozessen befolgt und mit Tools und Methodologien ausgestattet istt, die sich in erster Linie auf die Erkennung von und Reaktion auf Bedrohungen konzentrieren.
- Aufkommende Technologien wie künstliche Intelligenz (KI) in Verbindung mit maschinellem Lernen (ML) versprechen eine proaktive Risikominderung durch die Verarbeitung von Datenanalysen im Umfang von Petabytes und die automatische Einstufung und Reaktion auf Vorfälle, zusammen mit von Communitys geführten Untersuchungen und Tools innerhalb einer kombinierten Endpunkt- und Cloud-Infrastruktur.
- Durch den Einsatz von KI-gesteuerter Automatisierung im SOC zur Bearbeitung sich wiederholender Aufgaben bei der Überprüfung von Warnmeldungen und zur Feststellung der erforderlichen Maßnahmen können sich die Analysten auf die Aufspürung, Untersuchung und Reaktion konzentrieren. Dadurch wird die Arbeit der Analysten wesentlich erfüllender, da sie ihre Fähigkeiten und Erfahrungen für eine gründliche Analyse der Bedrohungen und deren Beseitigung einsetzen können. Außerdem werden Unternehmen dadurch sicherer und weniger anfällig für komplexe Angriffe.

DIE SÄULEN DES EIGENSTÄNDIGEN SOC

Das eigenständige SOC stützt sich auf drei wichtige Säulen:

- **Daten**. Das eigenständige SOC wird über eine flexible und skalierbare Datenstruktur für die Aufnahme von Daten aus allen Quellen und Formaten verfügen. Mehrere Benutzer und die Möglichkeit, globale Daten zu erfassen und dabei Datenschutzbestimmungen einzuhalten, sind für die vollständige Realisierung der Vorteile des eigenständigen SOC selbst in den größten und komplexesten Unternehmen von entscheidender Bedeutung.

- **Analysen**. Das eigenständige SOC wird automatisierte KI/ML-basierte Analysen bereitstellen, damit Analysten auf Vorfälle auch in riesigen Cloud-First-Infrastrukturen reagieren können. Dank dieser verbesserten Sichtbarkeit können SOC-Teams Sicherheitswarnungen besser verwalten und auf Risiken im Zusammenhang mit der Compliance untersuchen.
- **Community**. Das eigenständige SOC wird vernetzt sein. Der Austausch von Gemeinschaftsressourcen, einschließlich Informationen und Inhalten, wird weiter zunehmen schneller und proaktiver zum Vorteil aller Unternehmen an Wert gewinnen. Auf diese Weise können SOC-Teams ihre Fähigkeiten zur Reaktion auf Vorfälle optimieren und die neuesten Angriffstechniken anwenden, wodurch die Verwaltung des SOC effizienter, effektiver und robuster wird.

Auf diesen Säulen wird die Automatisierung aufbauen. Das eigenständige SOC wird mit Automatisierungstechnologien ausgestattet sein, die es den Analysten ermöglichen, sich auf die Bedrohungslage als Ganzes zu konzentrieren und nicht nur auf die nächste Warnmeldung, die auf ihrem Bildschirm erscheint. Die Automatisierung der Triage, Untersuchung und Aufspürung von Bedrohungen bedeutet, dass die Analysten ihre Untersuchungen mit einem klaren Verständnis der gesamten Auswirkungen einer Bedrohung beginnen.

DIE VORTEILE DES EIGENSTÄNDIGEN SOC

Das eigenständige SOC wird unzählige Vorteile bieten, sowohl für Führungskräfte und Analysten als auch für die jeweiligen Unternehmen.

Für Führungskräfte:

- Alle Daten aus beliebigen Infrastrukturen und Anwendungen lassen sich mühelos erfassen, sodass Sicherheitsteams einen vollständigen Überblick über die gesamte Angriffsfläche erhalten.
- Dank der Kombination aus Erkennung, Untersuchung, Aufspürung, Automatisierung und forensischer Analyse in einer einzigen, benutzerfreundlichen Plattform können Sicherheitsteams schnell und entschlossen auf Bedrohungen reagieren.
- Mit der Implementierung eines Community-basierten Marktplatzes für Inhalte lassen sich die Möglichkeiten von Sicherheitsteams erweitern, die ihr Fachwissen durch die Zusammenarbeit mit Communitys für eine Vielzahl von Anwendungsfällen ausbauen können. Auf diese Weise kann Ihr Team seine Fähigkeiten zur Reaktion auf Vorfälle optimieren und die neuesten Angriffstechniken erkennen, wodurch die Verwaltung des SOC effizienter, effektiver und leistungsfähiger wird.

Für Analysten:

- Analysen, KI und ML werden Alarmmüdigkeit durch die Verbesserung der Qualität der Warnmeldungen verringern. Dabei werden alle Daten durchsiebt, um Bedrohungen zu erkennen, bevor sie sich zu Verstößen entwickeln, und Angriffe zu identifizieren, bevor sie Schaden anrichten.
- Durch die Automatisierung von Triage, Untersuchung und Aufspürung wird Burnout vermieden, was zu einer schnellen, effektiven Erkennung und Reaktion auf Vorfälle und somit zu einer raschen Beseitigung von Bedrohungen führt – egal ob vor Ort oder in der Cloud.
- Die Umstellung von Risikoberichterstatter zu Risikospezialisten macht SOC-Analysten zu Geschäftsexperten, die mit Hilfe von Geschäftsanalysen und Sicherheitswissen außergewöhnliche Geschäftsergebnisse erzielen können.

DAS EIGENSTÄNDIGE SOC ERFÜLLT:

- Die Notwendigkeit, umfassende Daten aus allen Quellen mit absoluter Genauigkeit und Transparenz zu sammeln und zu analysieren.
- Den Bedarf an effektiver, effizienter Aufspürung und Erkennung von Bedrohungen sowie an Untersuchung und Reaktion auf Vorfälle in komplexen Infrastrukturen.
- Die Fähigkeit, das Fachwissen einer „globalen" Community zu nutzen, effektive Sicherheitsinhalte zu erstellen, Informationen auszutauschen und sich über bewährte Verfahren auf dem Laufenden zu halten.

Mit jedem Schritt in Richtung eigenständiges SOC kommen Sicherheitsteams dem Ziel näher, ihrem Unternehmen eine umfassendere, wertvollere und widerstandsfähigere Sicherheits aufstellung zu bieten, als dies bisher möglich war.

Als Marktführer im Bereich der Cloud-nativen SIEM-Technologie der nächsten Generation konzentriert sich Devo auf den Einsatz von KI, ML und Automatisierung, um die vielen Vorteile des eigenständigen SOC für Unternehmen in jeder Branche weltweit nutzbar zu machen. Weitere Informationen über Devo und den Weg zum eigenständigen SOC erhalten Sie von Ihrem Vertriebsmitarbeiter oder auf unserer Website www.devo.com/de/.

INTRODUCTION

Today's security operations center (SOC) leaders face a difficult balancing act. They need to secure complex infrastructures and applications during cloud shift, achieve digital transformation, and manage risk — while attracting and retaining skilled cybersecurity talent.

Add in today's fast-evolving threat landscape with its increased volume of sophisticated attacks, and you have the perfect storm: the lack of visibility into complex operating environments, the inability to analyze cloud-scale volumes of data, and the struggle to enhance team performance, which results in lower productivity and higher security risk.

What do organizations need to address these challenges? The autonomous SOC.

The autonomous SOC will reinvent how security professionals work by providing simplified visualization, automation, analytics and access to the latest community expertise and content. The autonomous SOC will integrate seamlessly with security and IT tools. It will enable SOC leaders to automate triage, investigation and hunting so their teams will be able to perform fast, effective detection and incident response to resolve threats on large-scale, cloud-first infrastructures.

This eBook will answer the following questions, and more:

- Why does the SOC need to transform?
- What is the autonomous SOC?
- What benefits will the autonomous SOC deliver?

Like organizations transitioning from on-premises to cloud technologies, the autonomous SOC will require a cultural shift in thinking from C-suite executives to security analysts to recast the SOC and its operational profile for the unique challenges of the future.

WHY DOES THE SOC NEED TO TRANSFORM?

Since its debut, the SOC's mission has been to protect organizations from cyberthreats with quick, decisive action

while reducing risk and any financial impact on intellectual property and brand. Emerging technologies such as artificial intelligence (AI) and machine learning (ML) promise to provide proactive risk reduction by managing petabytes of data analytics, automatic incident triaging, and response. Community-powered investigation within a combined endpoint and cloud infrastructure is also part of the mix and will play an even bigger role down the road.

At a time when it's increasingly difficult for organizations to attract and retain skilled SOC analysts, the need for automation will continue to accelerate rapidly. As SOCs implement automation, so will increasingly sophisticated attackers. In light of these developments, the SOC will continue to evolve during the next decade, as its core mission becomes even more vital in the increasingly digital world.

THE HUMAN ELEMENT

Let's start with a hard truth: Security teams are cost centers. They don't generate revenue, so bean counters may be quick to discount their value. And because it's exceedingly difficult to quantify true cybersecurity risk, even when a significant breach occurs, it's challenging for security leaders to justify hiring additional SOC staff.

The autonomous SOC will provide simplified visualization, automation, analytics and access to the latest community expertise and content.

However, since the evolving SOC will continue to rely on human analysts, it's reasonable to expect there will be parallel challenges in the types of activities/events analysts will need to monitor, mediate and manage, including:

- A higher volume of increasingly sophisticated attacks
- A lack of visibility into complex operating environments
- An inability to analyze cloud-scale volumes of data

As their jobs are destined to become even more challenging, let's look at how SOC analysts work today. Chasing false-positive alerts all day is a crushing burden. Numerous studies have shown two things: First, SOC analysts expend significant effort chasing down alerts that turn out to be benign. And second, the sheer volume of false-positive

alerts that cross analysts' screens can be overwhelming.

Research shows that SOCs waste an average of 10,000 hours (and some $500,000) annually validating unreliable and incorrect vulnerability alerts. Organizations also report an average of 53 alerts a day with nearly half being false positives. Of course, this has a negative effect on SOC teams.

Alarmingly, more than one-third of IT security managers and SOC analysts ignore threat levels when the queue is full. Given those conditions, it's not surprising that 70% of organizations report understaffed teams, and 60% say their workloads have spiked recently.

This repetition and routine have directly led to widespread SOC analyst burnout. A survey of more than 1,000 global security professionals found that 75% of SOC analysts said they felt burned out on the job, according to the 2021 Devo SOC Performance Report™. Other findings include:

- 72% of respondents rated their pain of working in the SOC at a 7 or above on a 10-point scale.
- 68% of respondents said they have too many alerts to chase.
- 63% of respondents said the pain of SOC work led them to consider changing careers or leaving their current job.

THE ROLE OF AUTOMATION

While SOCs rely on a variety of tools, it's up to analysts to classify threats and decide which require further response. With an always-growing number of alerts and the explosion of data that needs to be protected against threats, identifying which alerts are "safe" to ignore is an almost impossible mission. That's where automation can be a game-changer.

Still, despite the promise of relieving them of tedious manual tasks, some analysts may fear automation will take their jobs. The opposite is true. Automation will elevate SOC analysts from risk commentators to risk advisers. Here's a good example of how automation will benefit analysts: A study found that 70% of analysts investigate 10 or more alerts each day. With each alert taking 10 minutes or more to investigate, that's nearly two hours per day spent investigating alerts, most of which turn out to be false positives.

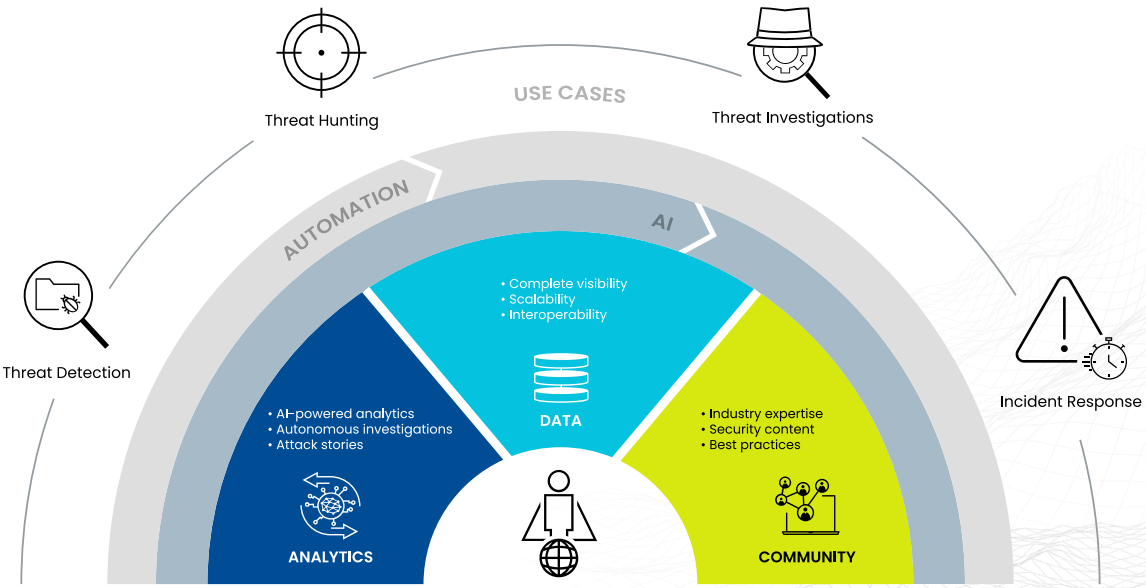
Deploying AI-driven automation in the SOC to handle the repetitive tasks of reviewing alerts to determine which require action, will free analysts to focus on hunting, investigating and responding to the threats that matter most to their business. This will make their work more fulfilling as they use their skills and experience to perform in-depth analysis of threats and how to eradicate them. That will help alleviate analyst burnout, improve SOC team morale, and make organizations more secure and less vulnerable to sophisticated attacks.

And, realistically, given the scarcity of SOC analysts that already exists, job security should not be a major concern as organizations deploy automation more widely. Especially since the number of vacant cybersecurity jobs grew by 350%, with 3.5 million open positions in 2021.

So, what's the solution to the many challenges facing SOC teams? The autonomous SOC.

WHAT IS THE AUTONOMOUS SOC?

The SOC of the future will perform the same primary function — but in a different way. That's why a new SOC model is required for organizations to stay ahead of the exponential increase in data, the continued shortage of skilled analysts, and the volume and severity of cyberattacks. This new model must enable teams to focus on their top priority: delivering positive security outcomes.



Autonomes SOC

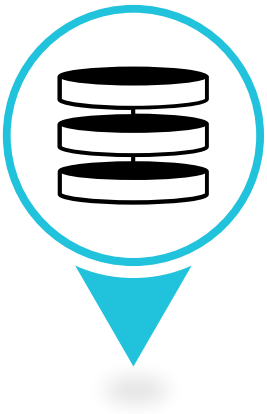
The autonomous SOC will:

- Deliver complete visibility, automation and analytics, along with access to the latest community expertise, content and threat intelligence
- Integrate seamlessly with security and IT tools
- Enable SOC leaders to automate triage, investigation and hunting
- Deliver fast, effective detection and incident response to resolve threats on large-scale, cloud-first infrastructures
- Reimagine the scope of analysts' work so it's more interesting and fulfilling

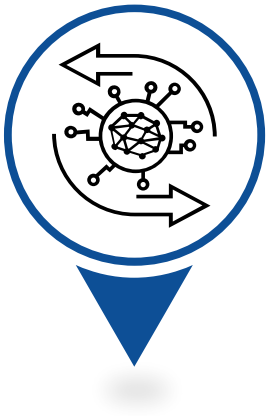
By embracing AI and ML, SOCs will become much more effective at detection, which will reduce the number of distinct alerts and false positives, ultimately lightening analysts' workloads.

THE PILLARS OF THE AUTONOMOUS SOC

Three key elements comprise the pillars of the autonomous SOC.



DATEN



ANALYSEN

COMMUNITY

Pillar #1:

DATA

Today, a growing technology stack, rapid digitization of business, and the expanding scope of enterprise assets have led to an explosion of data. More data attracts more unknown threats, more false-positive alerts, and more noise for SOC analysts to cut through. This is bad news for ill-prepared SOCs that are unable (or unwilling) to evolve. Consider the following aspects of data for which modern SOCs are responsible:

- An exponential increase in data volume
- Insufficient ability — or lack of resources — to collect that data
- An expanding attack surface without enough analysts to analyze it
- The continuing rapid transition of data from on-premises storage to the cloud and the need for SOC expertise to secure it

SOC analysts have well-defined roles and responsibilities (see sidebar). But with more data than ever to safeguard, and clever, relentless adversaries to battle, SOC teams need advanced technology to effectively protect the data that drives their organizations.

Analysts and the Autonomous SOC

Artificial intelligence and machine learning will address critical analyst pain points caused by a heavy load of repetitive, manual work.

Today, Tier-1 SOC analysts primarily monitor event logs for suspicious activities. When further investigation is needed, they collect information and escalate the incident to Tier-2 analysts.

Tier-2 analysts then dig deeper into suspicious activity to assess the nature of the threat and determine

In the autonomous SOC, intelligence informs the work of analysts. In terms of clicks or as a defensive posture, it's the ability to observe, learn, hunt and respond to all customers across all environments at all times. For example, what may have been a one-off attack that failed against one organization may have succeeded against another organization in the same industry. So, how does a SOC team learn from those disparate experiences and use that knowledge to defend their organization? AI-driven automation will play a key role in giving Tier-3 analysts the information they need to quickly identify — and stop — that previously seen attack.

The autonomous SOC will have a flexible and scalable data fabric to ingest data from all sources and formats. Support for multitenancy and the ability to collect global data while complying with privacy requirements are critical for realizing the full benefits of the autonomous SOC across even the largest, most complex organizations.

if and to what extent it may have penetrated the infrastructure. Once that's done, Tier-2 analysts begin to coordinate a remediation response.

The most experienced analysts — Tier-3 — are threat hunters. They support complex incident response and review forensic and telemetry data for threats that detection software may not have identified initially as suspicious.

Cutting-edge SOCs already are using automation to perform some Tier-1 activities, which enables Tier-2 activities to become a fusion of automation and artificial intelligence. In the future, most organizations will continue to rely on the expertise of Tier-3 analysts to ensure the highest level of SOC performance — incident response. But AI can accelerate many Tier-3 operations, as well a great deal of the work performed by Tier-1 and Tier-2 analysts, making them more effective and less likely to fall victim to burnout.

Pillar #2:

ANALYTICS

Traditional security information and event management (SIEM) solutions lack the intelligence to track, monitor and analyze every attribute of a potential security event efficiently and effectively. Security teams spend an inordinate amount of time sifting through volumes of false positives, wasting time they could better spend addressing threats that are more critical.

When SOCs can automate incident investigations and provide better context for alerts by filtering out noise, the volume of raw security alerts will decrease to a manageable number of concise, clearly categorized warnings.

Analytics in the autonomous SOC will include:

- Collecting data at any scale to support massive query loads
- AI and ML providing analysts with new insights into the enterprise and its security
- Using integrated threat enrichments and data lakes to apply new threat intelligence to external sources

- Applying automation orchestration to reduce workloads and pressure on Tier-1 and Tier-2 analysts
- The ability to sift through all data quickly and thoroughly to detect issues before they become incidents, and to identify attacks before they cause damage

In the autonomous SOC, analytics also will provide analysts with increased visibility into threats across on-premises and cloud environments. This enhanced visibility will help SOC teams more efficiently manage security alerts and investigate compliance-based risks.

The autonomous SOC will provide automated AI/ML-based analytics to empower analysts to perform incident response on large-scale, cloud-first infrastructures. These next-generation analytics seamlessly integrate with security and IT tools to accelerate incident response, including detection, triage, investigation and hunting.

When SOCs can automate incident investigation and provide better context for alerts, the volume of raw security alerts will decrease.

Pillar #3:

COMMUNITY

SOCs benefit greatly by leveraging the collective capabilities of the security community to build effective content, share intelligence, and exchange best practices. Community, in this context, means expanding analyst knowledge with access to industry-sourced content and on-demand expertise. SOC teams can tap into on-demand help for issues such as:

- How do I access expertise at the edges of my attack surface when I lack that collective defense in-house?
- How can I learn from security experts anywhere in the world about attacks they are actively battling, especially from organizations with similar environments in my industry?
- How can I share what I've learned about improving my organization's security?

Think of it as an IT version of the phone-a-friend element from "Who Wants to Be a Millionaire." When analysts need information, they can access a pool of global talent to

Analysts can access a pool of global talent to bring expertise into the SOC, apply it immediately, and resolve threats decisively.

bring expertise into the SOC, apply it immediately to their investigations, and resolve threats more quickly and decisively.

The autonomous SOC will be interconnected, making it easy for SOC teams to optimize their incident response skills and leverage the latest attack techniques, making SOC management more efficient, effective and robust. SOC teams also will be able to access and apply the latest community expertise and content across the entire threat management lifecycle.

The autonomous SOC will make it easy for SOC teams to optimize their incident response skills, making SOC management more efficient, effective and robust.

DIE ROLLE DER AUTOMATISIERUNG

Der Fokus der SOCs auf Warnmeldungen ist gebrochen. Sogar Warnmeldungen mit der höchsten Zuverlässigkeit erfordern eine teure, sich oft wiederholende manuelle Sichtung, um die Notwendigkeit einer umfassenden Untersuchung zu ermitteln. Die Anzahl der Warnmeldungen ist dabei nicht das größte Problem. Vielmehr verfügen SOC-Teams über keine automatisierte Methode, um festzustellen, welche Warnmeldungen tatsächlich eine Bedrohung für das Unternehmen darstellen, und keine Möglichkeit, sich ein vollständiges Bild von den potenziellen Auswirkungen einer Bedrohung zu machen.

Um über Warnmeldungen hinauszugehen, müssen Analysten eine Untersuchung, gewappnet mit dem Angriffsleitfaden, beginnen – also mit einem vollständigen Plan des Angriffs und einem vollständigen Verständnis seiner Auswirkungen.

Mit dem eigenständigen SOC können sich Analysten von zeitaufwändigen, oft ineffektiven traditionellen Aktivitäten abwenden und sich auf Bedrohungssituationen konzentrieren. Anstatt mit einer Warnmeldung zu beginnen, wird die KI die Szenarien, Fragen und Daten erkennen, die Analysten für die Triage von Warnmeldungen benötigen. Die KI liefert den Analysten automatisch die vollständige Bedrohungssituation, indem sie kontinuierlich Informationen über Ihre Umgebung sammelt, eine Echtzeitansicht aller Ressourcen und ihrer

Mit dem eigenständigen SOC können sich Analysten von zeitaufwändigen, oft ineffektiven traditionellen Aktivitäten abwenden und sich auf Bedrohungssituationen konzentrieren.

Beziehungen erstellt und selbstständig Details zu den Aktionen eines Angreifers und ihren potenziellen Auswirkungen auf Ihr Unternehmen zusammenstellt.

Durch die Automatisierung der Triage, Untersuchung und Aufspürung erhalten Analysten durchgängige Informationen über die Bedrohungen, sodass sie ihre Analysen mit einem klaren Verständnis der Auswirkungen einer Bedrohung beginnen können, einschließlich:

- Einer KI zum Aufspüren von Angriffen, die die Arbeitsweise von Analysten widerspiegelt, indem sie Fragen stellt und die Antworten notwendigen erhält, um von dem Ausgangspunkt einer Alarmmeldung ausgehend einen vollständigen Angriffsplan zu erstellen
- Einer sich ständig aktualisierende Echtzeitansicht aller Ressourcen und ihrer Beziehungen, die die autonome Erstellung von Bedrohungsberichten ermöglicht, in denen die Aktionen eines Angreifers und die möglichen Auswirkungen auf Ihr Unternehmen detailliert beschrieben werden.

Durch die Verfolgung von Angreiferaktivitäten über mehrere Geräte hinweg implementiert ein solches System eine Automatisierung, die Beziehungen zwischen Ereignisdaten aus den vorhandenen Telemetriequellen eines Unternehmens herstellt, um den Weg des Angreifers zu visualisieren, verdächtige Aktivitäten aufzuspüren und die Ereigniskette zu untersuchen, wodurch letztendlich die gesamte Angriffskampagne identifiziert wird.

DIE VORTEILE DES EIGENSTÄNDIGEN SOC

Das eigenständige SOC wird unzählige Vorteile für SOCs bieten.

Führungskräfte werden in der Lage sein:

- Alle Daten aus beliebigen Infrastrukturen und Anwendungen mühelos erfassen, sodass Sicherheitsteams einen vollständigen Überblick über die gesamte Angriffsfläche erhalten.
- Selbstständig Erkennung, Untersuchung, Aufspürung und forensische Analyse in einer einzigen, benutzerfreundlichen Plattform zu kombinieren.
- Das Fachwissen des Sicherheitsteams auf ein breites Spektrum von Anwendungsfällen durch die Nutzung eines Community-basierten Inhaltsmarktplatzes auszuweiten. Auf diese Weise wird die Verwaltung des SOC verbessert, da die Reaktionsfähigkeit auf Vorfälle und die Erkennung der neuesten Angriffstechniken optimiert wird.

Analysten werden in der Lage sein:

- Die Alarmmüdigkeit durch den autonomen Einsatz von Analysen, KI und ML zur Durchsicht aller Daten zu verringern. Dabei können sie zwischen Warnmeldungen mit geringer und hoher Auswirkung unterscheiden, bevor sie zu Verstößen werden, und Angriffe identifizieren, bevor sie Schaden anrichten.
- Durch die Automatisierung von Triage, Untersuchung und Aufspürung wird Burnout vermieden, was zu einer schnellen, effektiven Erkennung und Reaktion und somit zu einer raschen Beseitigung von Bedrohungen führt.
- Die Umstellung von der Berichterstattung von Risiken auf die Beratung von Risiken macht SOC-Analysten zu Geschäftsexperten, die mit Hilfe von Geschäftsanalysen und Sicherheitswissen außergewöhnliche Geschäftsergebnisse erzielen können.

Die Umstellung von der Berichterstattung von Risiken auf die Beratung von Risiken macht SOC-Analysten zu Geschäftsexperten, die mit Hilfe von Geschäftsanalysen und Sicherheitswissen außergewöhnliche Geschäftsergebnisse erzielen können.

Die von der KI gestützten Maschinen-zu-Maschinen-Intelligenz verbessert hervorragend die menschliche Reaktionsfähigkeit, von der viele, wenn nicht alle dieser Ergebnisse abhängen. In Verbindung mit plattformunabhängigen Inhalten (von Warnungen und Bedrohungserkennung bis hin zu Playbooks), die von der globalen Sicherheits-Community zur Verfügung gestellt werden, kann ein SOC die Wahrscheinlichkeit des Erfolgs erhöhen und Bedrohungen in Echtzeit abwehren.

DER WEG GEHT WEITER

Der Weg zur Umwandlung traditioneller SOCs in eigenständige SOCs ist ein Prozess. Die Analysten werden nicht mehr nur auf Warnmeldungen reagieren und versuchen herauszufinden, welche Warnmeldungen ernsthafte Bedrohungen darstellen. Sie werden zu wertschöpfenden Jägern, die KI und ML zum Schutz des Unternehmens einsetzen.

Nach seiner Realisierung wird das eigenständige SOC über eine flexible und skalierbare Datenstruktur für die Aufnahme von Daten aus allen Quellen und Formaten verfügen. Sie werden miteinander vernetzt sein, sodass es für SOC-Teams einfach ist, auf die neuesten Fachkenntnisse und Inhalte der Community zuzugreifen und diese über den gesamten Lebenszyklus des Bedrohungsmanagements hinweg anzuwenden. Das bietet einen effektiven und rechtzeitigen Schutz gegen die Bedrohungen - aktuell und zukünftig.

Der Weg dorthin erfordert ein entsprechendes Engagement der Führungskräfte, eine unternehmensweite Überzeugungsarbeit und die Unterstützung durch Partner. Der Aufbau eines eigenständigen SOC erfordert auch eine Kombination aus Philosophien, bewährten Methoden und den richtigen Tools, die letztlich die Widerstandsfähigkeit eines Unternehmens gegen komplexe Sicherheitsbedrohungen verbessern werden. Jeder Schritt in Richtung eigenständiges SOC bringt Unternehmen näher an eine umfassendere, hochwertigere und widerstandsfähigere Sicherheitslage als je zuvor.

Sind Sie bereit, den Weg zum eigenständigen SOC anzutreten? Mit Devo können Sicherheitsteams die Automatisierung mit der Skalierbarkeit der Cloud einsetzen. Wenden Sie sich an Ihren Vertriebsmitarbeiter, um eine Demo zu vereinbaren, oder besuchen Sie unsere Website, um mehr zu erfahren.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo ist die einzige Cloud-native Plattform für Logging und Sicherheitsanalysen, die das gesamte Potenzial Ihrer Daten für mutige, zuversichtliche Entscheidungen nutzt. Mit Hilfe der unübertroffenen Skalierbarkeit bei der Datenerfassung, der Zugriffsgeschwindigkeit auf Antworten, sowie der Übersichtlichkeit auf den wichtigsten Ansätzen zu fokusieren steht Devo Ihnen heute und in Zukunft beim Schutz Ihres Unternehmens zur Seite. Der Hauptsitz von Devo befindet sich in Cambridge, Massachusetts, und der europäische Hauptsitz in Madrid, Spanien.