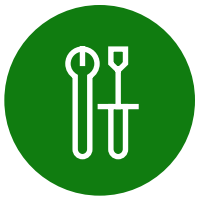
Microsoft Security

Drei Gründe für eine Umstellung auf integrierten Bedrohungsschutz

Inhaltsverzeichnis

Einführung



Ein Unternehmen nutzt zurzeit im Durchschnitt mehr als 30 verschiedene Sicherheitstools, die oft nicht zusammenhängen und nachträglich auf vorhandene Strukturen „aufgesetzt“ werden.

Das Thema IT-Sicherheit hat einen Wendepunkt erreicht. Die Cyberattacken werden immer raffinierter. Unternehmen haben gleichzeitig weiterhin mit Herausforderungen wie Fachkräftemangel, Budgeteinschränkungen und dem zunehmend hybriden Arbeitsumfeld zu kämpfen.

Zugleich ist der Sicherheitsmarkt inzwischen fragmentierter und komplexer denn je. Ein Unternehmen nutzt zurzeit im Durchschnitt mehr als 30 verschiedene Sicherheitstools, die oft nicht zusammenhängen und nachträglich auf vorhandene Strukturen „aufgesetzt“ werden. Sie bieten daher für die Security Operation Center (SOCs) nur eingeschränkte Transparenz und unzureichende Insights.

Sicherheits- und Compliance-Verantwortliche benötigen einen besseren Überblick über die neuesten Risiken und Bedrohungen, aber sie müssen auch wissen, was funktioniert und was nicht und wo es Lücken gibt.

Auch wenn der Umfang der heutigen Sicherheitsherausforderungen überwältigend erscheinen mag, gibt es für CISOs, die die Effizienz ihrer Sicherheitsprozesse verbessern möchten, dennoch Anlass zu Optimismus. Die Antwort liegt in einem integrierten, durchgängigen Ansatz zum Schutz vor Cyberbedrohungen, der Unternehmen helfen wird:

Grund 1: Erreichen Sie mehr mit weniger Aufwand

Konsolidierung von Einzellösungen und Verringerung des Aufwands für den Sicherheitsbetrieb (SecOps).

Grund 2: Sorgen Sie dafür, dass SecOps-Teams sich auf wichtige Aufgaben konzentrieren können

Setzen Sie Tools ein, die mehr Effizienz bieten und auch Nachwuchsanalyst*innen besser denn je unterstützen.

Grund 3: Steigern Sie die Mitarbeiterproduktivität

Schützen Sie Ihr Unternehmen, sodass Mitarbeiter*innen Entwicklungen und Innovationen vorantreiben können, ohne sich Sorgen um die Sicherheit machen zu müssen.

Dieser Ansatz wird durch die Integration einer XDR-Lösung (Extended Detection and Response) und eines cloudnativen SIEM-Systems (Security Information and Event Management) ermöglicht, das künstliche Intelligenz (KI) und Automatisierungsfunktionen nutzt. Die integrierte Lösung kann Ihrem SOC im gesamten Unternehmen zu einem vorausschauenden, proaktiven und präventiven Vorgehen gegen Angriffe verhelfen.

Grund 1

Erreichen Sie mehr mit weniger Aufwand

Durch die Konsolidierung von Tools mit der integrierten Lösung von Microsoft können Sie außerdem Kosten einsparen, indem Sie nur für das bezahlen, was Sie auch tatsächlich nutzen.

Viele Unternehmen haben sich im Hinblick auf Sicherheitstools vor allem auf die besten Einzellösungen konzentriert. Bei diesem Ansatz kann es für Sicherheitsexpert*innen schwieriger sein, Bedrohungen schnell zu erkennen und entsprechend zu reagieren. Zudem können negative Auswirkungen auf die IT-Ausgaben und die Produktivität der Anwender*innen entstehen.

Wenn Unternehmen mit weniger Aufwand mehr erreichen möchten, ist ein integrierter Ansatz wie bei den Microsoft-Lösungen für SIEM und XDR hilfreich. Er kann die Komplexität durch die Konsolidierung einzelner Tools verringern. Da es sich um eine cloudnative Lösung handelt, kann sie auch die Leistung und Skalierbarkeit verbessern.

Durch die Konsolidierung von Tools mit der integrierten Lösung von Microsoft können Sie außerdem Kosten einsparen, indem Sie nur für das bezahlen, was Sie auch tatsächlich nutzen. Zudem sind Sie in der Lage, den für die Verwaltung von Lösungen erforderlichen SecOps-Overhead zu reduzieren, indem Sie den Grad an Automatisierung und Integration verbessern.

> Die Einführung neuer Sicherheitstools ist zu Beginn einfach, da Sie von breiten Lücken ausgehen. Im weiteren Verlauf werden Sie jedoch bald erkennen, dass sich die Tools verschiedener Anbieter im Hinblick auf ihre Aufgaben möglicherweise überlappen. Eine solche Überlappung mag bei Kontrollen und Abgleichungen wünschenswert sein, **kann aber auch zu erheblichen finanziellen Nachteilen führen**."
>
> **Jonathan Cassar**
> Chief Technology Officer, MITA

1,6 Millionen USD

jährliche Einsparungen aus der Anbieterkonsolidierung

Microsoft beauftragte Forrester Consulting mit der Durchführung einer Total Economic Impact™(TEI)-Studie, um den ROI (Return on Investment) zu ermitteln, den Unternehmen generieren könnten, wenn sie Microsoft SIEM und XDR bereitstellen. Nachfolgend werden einige der wichtigsten Erkenntnisse für ein hypothetisches Unternehmen mit insgesamt 8.000 Mitarbeiter*innen und zehn Sicherheitsexpert*innen aufgeführt:

- **Einsparungen von fast 1,6 Millionen USD pro Jahr durch Anbieterkonsolidierung.** Dank der Investition in SIEM- und XDR-Lösungen von Microsoft kann das Unternehmen die Kosten für sein früheres SIEM (560.000 USD), die zugehörige On-Premises-Infrastruktur (über 360.000 USD), drei XDR-Einzellösungen (192.000 USD) und die laufenden Arbeitskosten für deren Verwaltung (480.000 USD) senken.

- **Verringerung des Risikos erheblicher Verstöße um 60 %.** Durch effizientere Arbeitsabläufe bei Sicherheitsprüfungen und -maßnahmen, optimierte Security-Response-Automatisierung und bessere Funktionen für den Schutz aller Computing-Umgebungen, einschließlich Multi-Cloud-Schutz, reduziert das Unternehmen das Risiko von Sicherheitsverstößen und Datenschutzverletzungen, was zu einer jährlichen Einsparung von 1,6 Millionen USD führt.

- **Generierung eines ROI von 207 %.** Repräsentative Befragungen und Finanzanalysen haben ergeben, dass ein Unternehmen in drei Jahren einen Ertrag von 17,68 Millionen USD erzielt. Die Kosten in dieser Zeit belaufen sich auf 5,76 Millionen USD. Das ergibt einen Kapitalwert (Net Present Value, NPV) von 11,92 Millionen USD.

Grund 2

Sorgen Sie dafür, dass SecOps-Teams sich auf wichtige Aufgaben konzentrieren können

Es ist wichtig, SIEM und XDR zu integrieren, um Warnmeldungen zu korrelieren, die größten Bedrohungen zu priorisieren und Maßnahmen im gesamten Unternehmen zu koordinieren.

SecOps-Teams sind mit der Menge der zu analysierenden Signale häufig überfordert. Es gibt viele Signale mit niedriger Zuverlässigkeit, die manuell nur schwer oder gar nicht zu erkennen und zu neutralisieren sind. Angesichts zunehmender Bedrohungen kann ein überlastetes SOC nur schwer am Ball bleiben, insbesondere bei der Analyse von Daten aus mehreren Einzellösungen. Die Antwort kann nicht darin bestehen, das Personal immer weiter aufzustocken. Schließlich stellt auch das Finden einer ausreichenden Anzahl kompetenter Sicherheitsfachleute eine nie endende Herausforderung dar.

Daher ist die Integration von SIEM und XDR umso wichtiger, um Warnungen zu korrelieren, die größten Bedrohungen zu priorisieren und Maßnahmen im gesamten Unternehmen zu koordinieren – mit fortschrittlicher KI und Automatisierung für die proaktive Erkennung und Beseitigung von Bedrohungen.

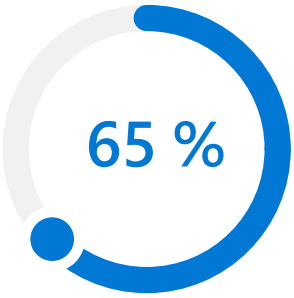
Angenommen, ein traditionelles SIEM schenkt einem einzelnen, niederstufigen Signal keine Beachtung. Ein cloudnatives SIEM hingegen kann dieses Signal mithilfe von KI automatisch mit Signalen aus anderen Quellen im gesamten Unternehmen vergleichen und dabei über mehrere Datensätze hinweg Korrelationen herstellen. Auf diese Weise lassen sich auch mehrstufige Angriffe erkennen.

Die Integration von SIEM und XDR verschafft SecOps-Ressourcen Zeit für höherwertige Aufgaben und stärkt auch Nachwuchsanalyst*innen durch mehr Fähigkeiten und Vertrauen.

Das System normalisiert, analysiert und korreliert dann die Daten und liefert gleichzeitig Informationen darüber, wie der Cyberangriff in die Infrastruktur eingedrungen ist und wie er sich ausgebreitet hat. Auf diese Weise können SOC-Teams die Sicherheitsverletzung – über eine zentrale Konsole – visualisieren und effektiv bekämpfen.

> Viele CISOs sehen weder **den Aufwand, den sie ihren Teams mit 20 verschiedenen Verwaltungsumgebungen** oder Einzellösungen zumuten, noch die damit verbundenen jährlichen Kosten ... Diese Probleme haben wir durch einen einzigen Anbieter weitestgehend gelöst."
>
> **Terence Jackson**
> Chief Information Security and Privacy Officer, Thycotic

Ein Unternehmen sollte kein fundiertes Fachwissen benötigen müssen, um eine Sicherheitslösung optimal ausnutzen zu können. Die Integration von SIEM und XDR verschafft SecOps-Ressourcen Zeit für höherwertige Aufgaben und stärkt auch Nachwuchsanalyst*innen durch mehr Fähigkeiten und Vertrauen.



Der integrierte Ansatz von Microsoft SIEM und XDR verkürzt die Zeit zur Untersuchung von Bedrohungen um 65 %.

Die von Microsoft bei Forrester in Auftrag gegebene Studie zum Total Economic Impact™ (TEI) hat diese Art von SecOps-Effizienz in einem hypothetischen Unternehmen aufgezeigt:

- **Verkürzung der Zeit zur Untersuchung von Bedrohungen um 65 % und Verkürzung der Reaktionszeit bei Bedrohungen um 88 %.** Der integrierte Ansatz von Microsoft SIEM und XDR bei der Untersuchung von Sicherheitsbedrohungen und Umsetzung entsprechender Maßnahmen sorgt für effizientere Arbeitsabläufe bei Sicherheitsfachleuten des Unternehmens. Sie müssen nicht mehr zwischen mehreren Tools wechseln, um Bedrohungen zu identifizieren, während Sicherheitsautomatisierungsfunktionen die Reaktionsabläufe weiter verbessern.

- **Verkürzung der Zeit für die Erstellung eines neuen Workbooks um 90 % und der Zeit für die Einarbeitung neuer Sicherheitsexpert*innen um 91 %.** Der integrierte Ansatz von Microsoft SIEM und XDR sorgt zudem für effizientere Arbeitsabläufe weiterer Sicherheitsfachleute. Da SIEM-Protokolldateien in der gesamten Lösungssuite integriert sind, erfolgt die Erstellung von Workbooks nahezu automatisiert, und gleichzeitig sorgt die zentralisierte Anmeldung dafür, dass die Einarbeitungszeit für neue Sicherheitsfachleute um fast 16 Wochen beschleunigt wird.

Grund 3

Steigern Sie die Mitarbeiterproduktivität

Eine integrierte SIEM- und XDR-Lösung kann Ihrem Unternehmen zu mehr Anwenderproduktivität verhelfen.

Eine integrierte SIEM- und XDR-Lösung hilft Ihrem Unternehmen nicht nur, mit weniger Aufwand mehr zu erreichen und die Effizienz von SecOps-Teams zu steigern, sondern auch die Anwenderproduktivität zu verbessern.

Wie SecOps-Teams wissen, umgehen die Menschen die Sicherheitsvorkehrungen, wenn diese zu komplex sind. Wenn Anwenderumgebungen die Produktivität von Mitarbeiter*innen eher behindern als unterstützen, können Unternehmen daher anfälliger für Sicherheitsrisiken und höhere Kosten sein. Schwache oder verlorene Kennwörter, der ungesicherte Zugriff über persönliche Geräte oder die uneingeschränkte Weitergabe sensibler Daten stellen nur einige der Herausforderungen dar.

> [In der Vergangenheit] sind wir eher plump vorgegangen, wenn ein Problem aufgetaucht ist. Wir haben uns abgeschottet und den Zugriff gesperrt, was sich negativ auf unser Unternehmen ausgewirkt hat. Das war allen klar, weil vorübergehend nichts mehr funktionierte. Mit Microsoft Sentinel besitzen wir ein leistungsstarkes Werkzeug, mit dem wir gezielt auf die Geschehnisse reagieren können. **Das Unternehmen weiß in der Regel nicht einmal, wann wir auf eine Bedrohung reagieren**, das ist ein wirklich wichtiger Maßstab für unseren Erfolg."
>
> **Rick Gehringer**
> Chief Information Officer, Wedgewood

Fast
68.000

Die Produktivität anderer Mitarbeitenden wurde durch Microsoft SIEM und XDR um fast 68.000 Gesamtstunden pro Jahr erhöht.

Der integrierte Ansatz von SIEM und XDR unterstützt Sie bei der Bereitstellung nahtloser User-Experiences, die die Produktivität und Sicherheit Ihrer Mitarbeiter*innen in allen Bereichen ihrer täglichen Arbeit gewährleisten. Er kann negative Auswirkungen auf die Produktivität verringern, z. B. das Deaktivieren von Diensten oder das Isolieren und anschließende Reimaging von Rechnern. Der integrierte Ansatz von SIEM und XDR kann aber auch neue Chancen zur Produktivitätssteigerung bei Anwender*innen schaffen, z. B. durch mehr Self-Service-Sicherheitssupport, bessere Dashboards und Berichte sowie eine höhere Reaktionsfähigkeit und schnellere Bootzeiten durch Ausführung weniger Sicherheitsagents.

In der von Microsoft bei Forrester in Auftrag gegebenen Studie zum Total Economic Impact™ (TEI) verzeichnete das hypothetische Unternehmen mit 8.000 Mitarbeiter*innen eine Steigerung der Mitarbeiterproduktivität durch die Bereitstellung von Microsoft SIEM und XDR:

- **Steigerung der Produktivität anderer Mitarbeiter*innen um fast 68.000 Gesamtstunden pro Jahr.** SIEM- und XDR-Lösungen von Microsoft verhindern negative Auswirkungen ineffizienter Sicherheitsprozesse auf andere Mitarbeiter*innen. Beispielsweise spart das Unternehmen 4.000 Stunden pro Jahr, dank der neuen Möglichkeit der IT-Expert*innen, sich selbst um Sicherheitsupdates und Empfehlungen zu kümmern. Zudem ermöglichen sie auch die Remote-Behandlung von Sicherheitsproblemen auf den Rechnern der Mitarbeiter*innen und reduzieren die Anzahl der darauf ausgeführten Sicherheitsagents, was zu einer Einsparung von fast 64.000 Stunden pro Jahr bei der Anwenderproduktivität führt.

Sicherheit ist zu einem unverzichtbaren Wegbereiter für den technologischen Erfolg geworden. Daher benötigen Unternehmen Sicherheitsmaßnahmen, die so viel Resilienz wie möglich gegen Angriffe bieten, um die Produktivität und Innovationskraft, die das Wachstum vorantreiben, zu schützen und zu fördern.

Profitieren Sie von integriertem Schutz vor Cyberbedrohungen mit SIEM und XDR

Diese Integration von branchenführenden Produkten bietet Prävention, Erkennung und Reaktion auf Cyberbedrohungen in einer einzigen umfassenden Lösung.

Microsoft bietet die erste und einzige integrierte SIEM- und XDR-Lösung, die durchgängige Transparenz für alle Clouds und Plattformen schafft. Diese Integration von branchenführenden Produkten bietet Prävention, Erkennung und Reaktion auf Cyberbedrohungen in einer einzigen umfassenden Lösung.

Microsoft SIEM und XDR nutzen die Leistungsfähigkeit von KI und Automatisierung sowie umfangreiche, kontinuierliche Investitionen in die Erkennung und Analyse von Cyberbedrohungen – mit Expertenwissen und Insights in 43 Billionen Signale pro Tag. Durch die Integration dieser Produkte verfügen SOC-Teams über mehr Kontext als je zuvor, um kritische Cyberbedrohungen schneller aufzuspüren und zu beseitigen:

Microsoft Sentinel

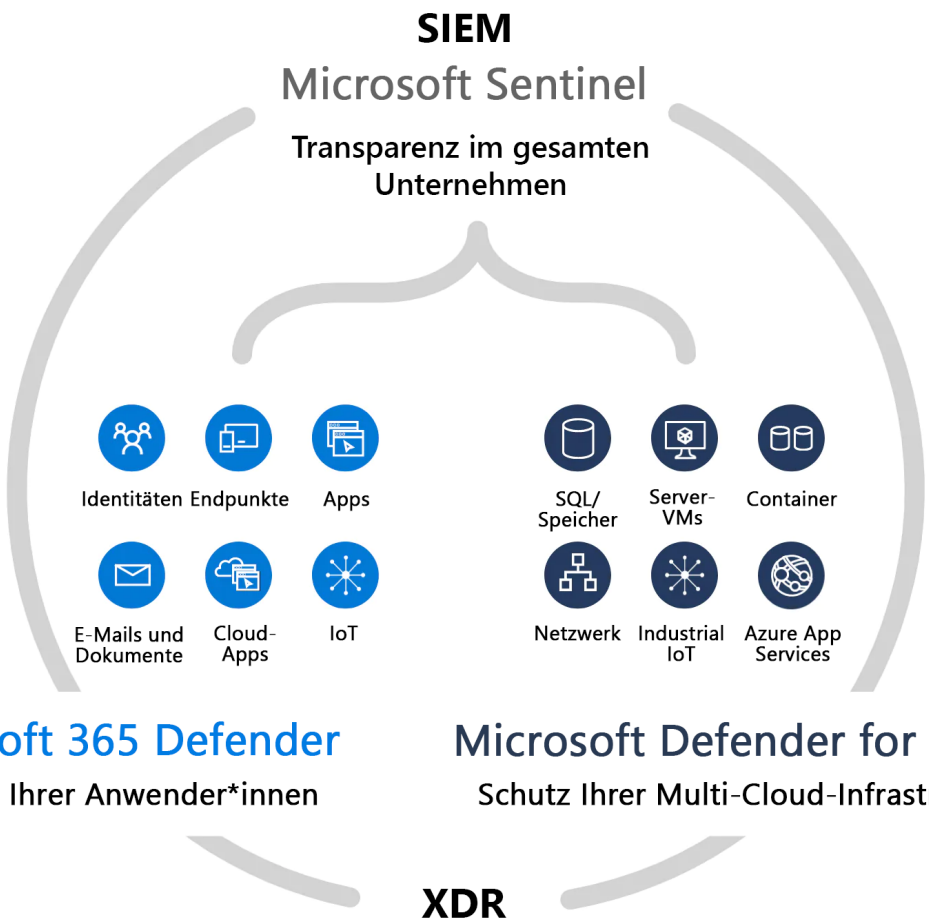
Verschaffen Sie sich mit dem cloudnativen SIEM von Microsoft einen Überblick über das gesamte Unternehmen. Sammeln Sie Sicherheitsdaten aus praktisch jeder Quelle und wenden Sie KI an, um Störgeräusche von legitimen Ereignissen zu trennen, Alarme über komplexe Cyberangriffsketten hinweg zu korrelieren und die Reaktion auf Cyberbedrohungen durch integrierte Orchestrierung und Automatisierung zu beschleunigen.

Microsoft Defender XDR

Erkennen und verhindern Sie Cyberangriffe auf Ihre Identitäten, Endgeräte, Anwendungen, E-Mails, Daten und Cloud-Anwendungen mit XDR-Funktionen. Untersuchen Sie Cyberangriffe und reagieren Sie darauf mit einem sofort einsatzbereiten, erstklassigen Schutz. Suchen Sie nach Bedrohungen, und koordinieren Sie Ihre Reaktion mühelos über ein einziges Dashboard.

Microsoft Defender for Cloud

Schützen Sie Multi-Cloud- und Hybrid Cloud-Workloads mit integrierten XDR-Funktionen. Sichern Sie u. a. Server, Speicher, Datenbanken und Container. Konzentrieren Sie sich dank priorisierter Warnungen auf die wichtigsten Punkte.



Verwenden Sie keine aufgesetzten Sicherheitslösungen, sondern setzen Sie auf Integration.

Geben Sie den richtigen Personen die richtigen Tools und Kenntnisse an die Hand. Schützen Sie sich mit einer durchgängigen, cloudnativen, integrierten Lösung vor modernen Angriffen.

Erfahren Sie mehr über den integrierten Schutz vor Cyberbedrohungen mit SIEM- und XDR-Lösungen von Microsoft. >

Microsoft Security