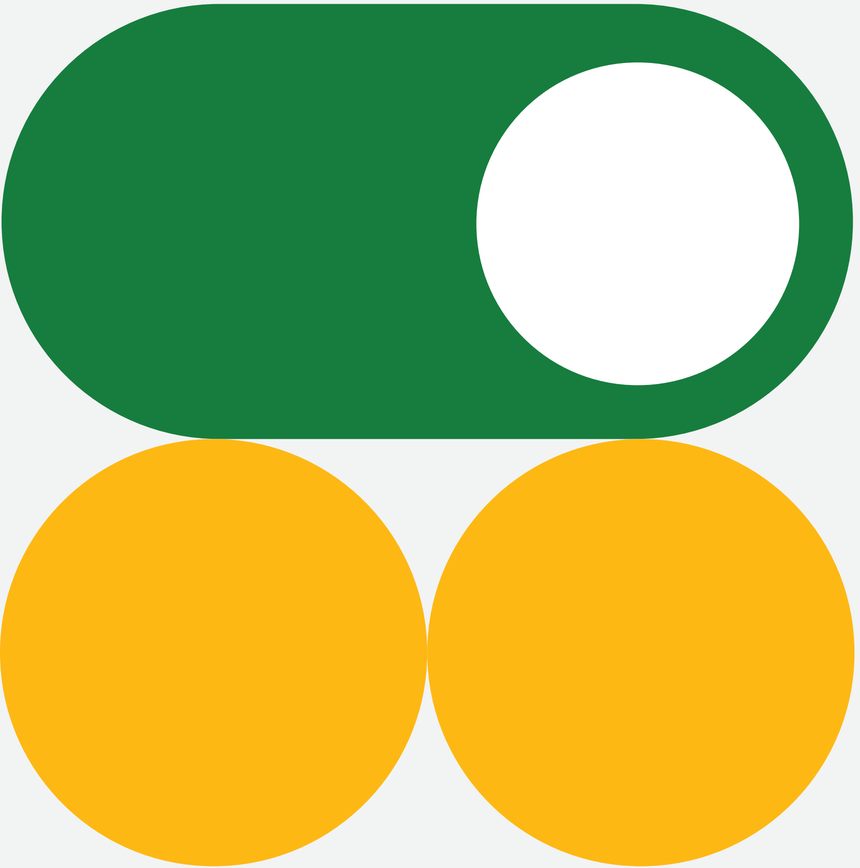
Microsoft Security

E-Book

Mehr Resilienz für Ihre Organisation gegenüber Cyberbedrohungen

Ein Crashkurs in Microsoft 365 Defender
und Microsoft Sentinel

Inhaltsverzeichnis



03

Einleitung

Multi-Plattform- und Multi-Cloud-Organisationen schützen

05

Kapitel 01

Für Klarheit und mehr Transparenz sorgen

08

Kapitel 02

Domänenübergreifende Cyberangriffe abwehren

10

Kapitel 03

Erkennung und Reaktion beschleunigen

13

Kapitel 04

Komplexe Cyberangriffe automatisch stoppen

15

Kapitel 05

Identitäten schützen

18

Kapitel 06

Zukünftige Cyberangriffe verhindern

20

Kapitel 07

Sicherheitsteams einen Vorsprung verschaffen

22

Fazit

Gegen KI-gesteuerte Cyberbedrohungen wappnen

Einleitung

Multi-Plattform- und Multi-Cloud-Organisationen schützen

Cybersicherheit ist zunehmend nicht mehr nur ein Thema für die IT, sondern eine grundlegende Anforderung an das gesamte Unternehmen. Seit mehr und mehr generative KI zum Einsatz kommt, hat das Thema sogar noch an Dringlichkeit gewonnen. Cyberkriminelle nutzen verstärkt KI für noch umfangreichere, komplexere Angriffe. Beispielsweise erstellen böswillige Akteure mittels KI nahezu fehlerfreie, professionell klingende Phishing-E-Mails. Unternehmen benötigen kosteneffektive Lösungen, die für Transparenz sorgen, Insights liefern und Automatisierung ermöglichen, um den KI-gesteuerten Cyberbedrohungen, die die Business Continuity gefährden, einen Schritt voraus zu sein.

Die durchgängige Security-Operations-Plattform von Microsoft verschiebt das Kräfteverhältnis zugunsten von Security Operations Centern (SOC) und liefert sämtliche Funktionen für eine effektive Verteidigung, beginnend bei Prävention und Erkennung über die Untersuchung von Cyberbedrohungen bis hin zur Reaktion auf Vorfälle. Durch die Kombination von Microsoft Defender XDR und Microsoft Sentinel entsteht eine einheitliche Plattform samt KI-gestützter Tools, mit denen das SOC Ihr Unternehmen schützen kann. Im Zusammenspiel mit Microsoft Copilot für Security liefert die Plattform Anweisungen und Empfehlungen, mit denen sich Untersuchungen beschleunigen und der allgemeine Sicherheitsstatus Ihrer Organisation verbessern lassen.

Defender XDR (Extended Detection and Response) schützt Geräte, E-Mails, Tools für die Zusammenarbeit, hybride Identitäten und Multi-Cloud-Anwendungen. Mithilfe von automatischen Funktionen werden Angriffe eingedämmt, und effektive Tools helfen bei der Untersuchung und Behebung komplexer Sicherheitsvorfälle.

Microsoft wurde 2023 im Gartner® Magic Quadrant™ for Endpoint Protection Platforms als führender Anbieter eingestuft.[1] [2]

Microsoft Sentinel ist eine cloudnative SIEM-Lösung (Security Information and Event Management), mit denen Ihre Teams kritische Cyberbedrohungen schnell erkennen und beseitigen können. Hierbei helfen integrierte SOAR-Funktionen (Security Orchestration, Automation and Response), die Analyse des Benutzer- und Entitätenverhaltens und Threat Intelligence.

Copilot ist eine Kombination aus dem leistungsstarken GPT-4-Modell von OpenAI und einem eigens von Microsoft entwickelten, sicherheitsspezifischen Modell. Diese KI-Sicherheitslösung automatisiert die Abfrageentwicklung, analysiert Code und gibt Anweisungen und Empfehlungen in natürlicher Sprache.

60 %

geringeres Risiko einer schwerwiegenden Sicherheitsverletzung[3]

1,6 Mio. USD

jährliche Einsparungen durch Anbieterkonsolidierung[3]

207 %

Return on Investment nach drei Jahren[3]

68.000

eingesparte Arbeitsstunden pro Jahr[3]

Kapitel 01

Für Klarheit und mehr Transparenz sorgen

Böswillige Akteure können von jedem Ort der Welt aus zuschlagen. Ich bin fest davon überzeugt, dass das Mehr an Transparenz, für das Microsoft 365 E5 sorgt, ein Muss für jede Organisation ist.

Neil Natic, Chief Information Officer, Georgia Banking Company

Böswillige Akteure respektieren keine Domänengrenzen. Sie breiten sich schnell in Anwendungen, Endpunkten, Identitäten und Clouds aus, um in der digitalen Umgebung eines Unternehmens Fuß zu fassen und einen Cyberangriff zu starten. Als Gegenmaßnahme muss Ihr Team die gesamte Umgebung überblicken, ein bestimmtes Ereignis oder einen Cyberbedrohungsakteur untersuchen und Zusammenhänge zwischen verschiedenen Sicherheitsdaten erkennen. Doch isolierte Sicherheitslösungen erschweren dies.

Die Security-Operations-Plattform bündelt Daten und Insights aus Ihrer Multi-Cloud- und Multi-Plattform-Umgebung. Sie verschafft Ihrem SOC Einblicke und stellt Tools bereit, mit denen es bei Bedarf Warnmeldungen, Entitäten und Cyberbedrohungsakteure untersuchen kann.

Mehrere Datenquellen, ein Portal

Unternehmen nutzen heute mehrere Clouds, und die Mitarbeitenden greifen von verschiedenen Standorten aus mit unterschiedlichen Geräten darauf zu. Der Arbeitsplatz ist dadurch flexibler und produktiver geworden, aber es eröffneten sich auch mehr Möglichkeiten für böswillige Akteure, sich unbefugt Zugang zu verschaffen.

Damit Ihr SOC sehen kann, was in der gesamten digitalen Umgebung vor sich geht, bietet Microsoft Sentinel mehr als 300 Connectors für Plattformen wie Microsoft Azure, Google Cloud Platform, AWS, CrowdStrike, Oracle und SAP. Über dieses zentrale Portal kann Ihr Team alle Geräte, Cloud-Apps sowie aktiven und inaktiven Identitäten überwachen.

Cyberbedrohungen im Kontext betrachten

Ein SOC wird normalerweise mit Sicherheitsdaten und Warnmeldungen überschwemmt, die nicht immer die ursächlichen Sicherheitsbedrohungen benennen. Die Teams verschwenden Zeit mit Fehlalarmen oder, schlimmer noch, übersehen etwas Wichtiges. Indem die Security-Operations-Plattform Warnmeldungen bündelt und daraus weniger, dafür aber aussagekräftigere Vorfälle ableitet, hilft sie Ihrem Team, Zeit zu sparen und der Alarmmüdigkeit vorzubeugen. Copilot fasst die Vorfälle zusammen und analysiert den Code, sodass sich die Analyst*innen auf die Untersuchung und Behebung der Probleme konzentrieren können, anstatt Warnmeldungen zu durchforsten.

Ungewöhnliche Aktivitäten lokalisieren

Microsoft Sentinel analysiert Daten aus allen eingebundenen Quellen mittels Machine Learning und definiert Referenzwerte für normales Verhalten. Basierend auf dem Verständnis dessen, was normal ist, identifiziert Microsoft Sentinel Aktivitäten, die von der Norm abweichen, und stellt fest, ob eine Ressource möglicherweise kompromittiert wurde. Defender XDR setzt einzelne Warnmeldungen mit Vorfällen in Beziehung, wodurch Analyst*innen einen wichtigen Kontext erhalten und die Anzahl der zu prüfenden Warnmeldungen reduziert wird.

Cyberangriffe visualisieren

Ein zentrales Portal, in dem sich die gesamte Umgebung überwachen lässt, muss den kompletten Zeitplan für den Cyberangriff visualisieren und Details zu jeder betroffenen Ressource liefern, sodass Analyst*innen den Kontext hinter einem größeren Vorfall besser verstehen können. Dadurch vergeudet das Team keine Zeit mit der manuellen Korrelation von Warnmeldungen.

Muster aufdecken

Sicherheitsexpert*innen können mit den KI-Funktionen von Copilot das Grundrauschen von Tausenden Warnmeldungen und komplexen Vorfällen durchdringen. Copilot fasst Vorfälle zusammen und bringt so wichtige Insights aus verschiedenen Datenquellen ans Licht, sodass Ihr Team nicht mehr Warnmeldungen aus verschiedenen Systemen korrelieren muss.

> *Der größte Vorteil in unseren Augen ist die verbesserte Transparenz in der gesamten Campari Group dank der Zusammenführung der Defender-Lösungen und Microsoft Sentinel.*

Andrea Mazzetti, Global IT Manager, Cybersecurity, Campari Group

Kapitel 02

Domänenübergreifende Cyberangriffe abwehren

Die Cyberangriffskette hilft Sicherheitsexpert*innen besser zu verstehen, wie Cyberkriminelle vorgehen, und skizziert die Phasen eines typischen Sicherheitsvorfalls, einschließlich:

Aufklärung: Bevor böswillige Akteure den ersten Schritt wagen, spionieren sie ihre Ziele aus, um Schwachstellen zu identifizieren und einen Plan zu entwickeln.

Infiltration: Cyberkriminelle verschaffen sich zunächst Zugang über Phishing-E-Mails, Diebstahl von Zugangsdaten oder Schwachstellen in Hard- und Software.

Rechteausweitung: Um Zugang zu den anvisierten Systemen und Daten zu erhalten, müssen Cyberkriminelle in der Regel ihre Kontorechte ausweiten, oft mit dem Ziel, in die Administratorrolle zu schlüpfen.

Laterale Ausbreitung: Böswillige Akteure breiten sich im ganzen System aus, um auf weitere Daten zuzugreifen oder ihre Berechtigungen auszuweiten.

Installation: Malware hilft Cyberangreifern, den Zugang auszuweiten, Daten zu exfiltrieren oder Systeme und Daten zu sperren.

Exfiltration: Oft ist das ultimative Ziel eines Cyberangriffs, Daten zu exfiltrieren, entweder um sie im Dark Web zu verkaufen oder um Lösegeld zu erpressen.

Ein gängiges Beispiel für einen Cyberangriff, der sich über mehrere Domänen erstreckt, läuft wie folgt ab: Ein Mitarbeiter erhält eine E-Mail mit einem Phishing-Link. Über den Link in der E-Mail gelangt der Mitarbeiter auf eine Website. Dort wird er gebeten, seine Anmeldedaten einzugeben. Kommt er der Bitte nach, stiehlt ein böswilliger Akteur seinen Benutzernamen und sein Passwort und meldet sich bei dem Konto an. Dort erstellt der Cyberkriminelle neue Postfachregeln, greift auf andere Geräte zu und exfiltriert Daten. Für diesen Cyberangriff kompromittierte der Übeltäter E-Mails, Identitäten, Endpunkte und Daten.

Weil sich Cyberkriminelle während der verschiedenen Phasen eines Angriffs über mehrere Domänen hinweg ausbreiten, mag es schwierig sein, ihre Aktivitäten zu erkennen. Doch die Security-Operations-Plattform sucht in jeder Phase der Cyberangriffskette nach verdächtigen Aktivitäten und korreliert Daten von Endpunkten, hybriden Identitäten, E-Mails, Tools für die Zusammenarbeit, Cloud-Apps und Cloud-Workloads, um gravierende Cyberbedrohungen aufzuspüren.

In vielen Fällen stoppen die automatisierten Erkennungs- und Reaktionsfunktionen Cyberangriffe bereits in der Frühphase. Defender XDR blockiert proaktiv Malware und bösartige Links in Apps, stellt Phishing-E-Mails unter Quarantäne, schützt Identitäten durch bedingten Zugriff und verhindert so, dass Cyberkriminelle Zugang zu Ihrer Umgebung erlangen. Auch bei Sicherheitsvorfällen, die nicht durch automatisierte Funktionen gestoppt werden können, ist Ihr Team besser gerüstet, denn es überblickt die gesamte Umgebung und verfügt über Tools, mit denen es einen bestimmten Vorfall genauer untersuchen und darauf reagieren kann.

Bei den 2023 MITRE Engenuity ATT&CK® Evaluations stellte Microsoft Defender XDR Transparenz und Analytics für alle Phasen der Cyberangriffskette unter Beweis.

Kapitel 03

Erkennung und Reaktion beschleunigen

Beim Thema Cybersicherheit ist Timing alles. Die Security-Operations-Plattform verkürzt die Untersuchungszeit um bis 65 %[3] und die Reaktionszeit um bis zu 88 %.[3] Dank der integrierten Tools können Teams Cyberangriffe erkennen und die Verteidigung übergreifend für die Multi-Plattform- und Multi-Cloud-Umgebung Ihrer Organisation koordinieren.

Untersuchung und Reaktion vereinfachen und beschleunigen

Sobald ein Cyberangriff bestätigt wurde, ermöglichen die Untersuchungs- und Reaktionstools der Plattform den Analyst*innen, die Geschehnisse zu ermitteln und schnell entscheidende Maßnahmen zu ergreifen. Anstatt dass Analyst*innen Insights aus unzusammenhängenden Warnmeldungen zusammensetzen, bündelt die Plattform niederschwellige Warnmeldungen in einem einzigen Vorfall und spart den Analyst*innen dadurch wertvolle Zeit.

Diagramme und detaillierte Informationen zu jedem Vorfall vermitteln Ihrem SOC Folgendes:

- Zeitleiste des Cyberangriffs
- welche Anomalien und verdächtigen Aktivitäten den Vorfall ausgelöst haben
- wie sich der Vorfall auf die betroffenen Entitäten auswirkt
- welche Verbindungen zu anderen Sicherheitsdomänen bestehen

Copilot gibt den Teams Anweisungen, Empfehlungen und Erklärungen in natürlicher Sprache, wie sich der Cyberangriff eindämmen lässt. Die in Microsoft Sentinel integrierten SOAR-Funktionen ermöglichen es den Teammitgliedern, die Reaktionsmaßnahmen untereinander zügig zu koordinieren. Und Playbooks mit Abhilfemaßnahmen automatisieren wichtige Aktivitäten wie die Isolierung von Malware, die Deaktivierung kompromittierter Konten und den Einsatz von Antivirenfunktionen.

Böswillige Akteure mit erweiterten Threat-Hunting-Funktionen ausmanövrieren

Die Cyberbedrohungslandschaft ist keineswegs statisch. Nationalstaatliche Akteure und Cyberkriminelle aller Größenordnungen entwickeln ständig neue Taktiken, mit denen sie sich einer Entdeckung entziehen.

Um diese verborgenen Cyberbedrohungen aufzudecken, bietet Microsoft Defender XDR mit Advanced Hunting ein abfragebasiertes Untersuchungstool, mit dem Sicherheitsexpert*innen die Rohdaten der vergangenen 30 Tage untersuchen können. Teams können versteckte Angreifer mithilfe von zwei Modi aufspüren:

Im **geführten Modus** lässt sich dank vorgefertigter Abfragen ganz einfach nach Anzeichen für einen neuen Cyberangriff suchen, ohne Code schreiben zu müssen.

Im **erweiterten Modus** erstellen Teams mithilfe der Kusto Query Language (KQL) individuelle Abfragen, um ihre Suche je nach Know-how und Kenntnisstand weiter zu verfeinern.

Analyst*innen, die KQL nicht beherrschen, aber eine individuelle Abfrage entwickeln müssen, können Copilot darum bitten. Copilot kann anhand des Advanced-Hunting-Datenschemas eine in natürlicher Sprache gestellte Anfrage in eine individuelle Abfrage umwandeln.

Teams können auch individuelle Erkennungsregeln festlegen, die automatisch nach Erkenntnissen wie vermuteten Sicherheitsverletzungen oder falsch konfigurierten Rechnern suchen und darauf reagieren.

Dass Microsoft Defender XDR Signale für das Threat-Hunting kombiniert und sowohl Identitäts- als auch Endpunktdaten verknüpft, um bedrohliche Ereignisse zu identifizieren, ist ein Gamechanger.

Krzysztof Kuźnik, Product Owner, ING

Kapitel 04

Komplexe Cyberangriffe automatisch stoppen

Ein Cyberangriff kann ein Unternehmen Millionen Euro kosten. Insbesondere Ransomware kann teuer werden. Sei es Erpressung oder Produktivitätsverlust: Diese Cyberangriffe verursachen enormen Schaden. Glücklicherweise kann ein lückenloser Bedrohungsschutz das Risiko eines Ransomware- oder anderen Cyberangriffs erheblich verringern.

Die in die Plattform integrierte automatische Angriffsunterbrechung ist eine zentrale Funktion, mit der sich laufende Cyberangriffe schnell eindämmen lassen. Dazu werden:

- Signale von Endpunkten, Identitäten, E-Mails, Tools und Cloud-Apps korreliert, um den Cyberangriff zu erkennen,
- die vom Angreifer gesteuerten Ressourcen identifiziert,
- die betroffenen Ressourcen isoliert und so Ransomware automatisch eingedämmt.

Die automatische Angriffsunterbrechung unterbindet eine laterale Ausbreitung frühzeitig und reduziert die Gesamtkosten für das Unternehmen, sodass mehr Zeit für die Behebung des Vorfalls bleibt. Weil Ihr Team die volle Kontrolle über die Untersuchung, Behebung und Wiederherstellung von Ressourcen behält, kann es auch schnell auf Fälle reagieren, in denen automatisierte Tools versehentlich ein Gerät aufgrund eines Fehlalarms gesperrt haben.

Könnte ich in die Zeit vor dem Ransomware-Angriff zurückreisen, würde ich mir selbst raten, unsere Endpunkt-Richtlinien zu stärken und alle Funktionen von Defender for Endpoint und Intune voll auszuschöpfen. Ich betrachte unsere Recovery nicht als Sieg, sondern vielmehr als Weckruf, die Sicherheitsmaßnahmen zu verdoppeln.

Eric McKinney, Enterprise Infrastructure Director, G&J Pepsi-Cola Bottlers

Kapitel 05

Identitäten schützen

Defender for Identity hat unsere Erwartungen übertroffen. Es entdeckte mehrere Red-Team-Angriffe auf unsere On-Premises-Identitäten während einer Simulation [...] Es gab kein Rauschen und keine Fehlalarme.

Andrew Vezina, Vice President and Chief Information Security Officer, Equitable Bank

Kompromittierte Konten sind nach wie vor eine der Hauptursachen für Datenschutzverletzungen. Bei vielen Cyberangriffen verleiten böswillige Akteure die Mitarbeitenden dazu, ihre Anmeldedaten preiszugeben. Anschließend nutzen sie diesen Zugang, um ihre Rechte auszuweiten und nach Schwachstellen im Netzwerk zu suchen.

Nicht nur Angestellte und Partner sind dem Risiko einer Kontokompromittierung ausgesetzt. Da Remote-Mitarbeitende auf mehrere Cloud-Apps und Geräte angewiesen sind, um produktiv zu arbeiten, nehmen böswillige Akteure bei ihren Cyberangriffen zunehmend „nicht-menschliche" Identitäten wie Apps und Dienste ins Visier.

Identitätsangriffe stoppen

Die Plattform bietet Unternehmen konsistenten Schutz für alle ihre Identitäten, ob menschlich oder nicht, unabhängig von der Umgebung oder dem Anbieter. Das in Defender XDR integrierte Microsoft Defender for Identity unterbindet im Zusammenspiel mit Microsoft Entra ID laufende Identitätsangriffe. Mit den vorgefertigten Connectors können Sie die Abdeckung auch auf On-Premises-Umgebungen und andere Identitätsanbieter ausweiten.

Microsoft Defender for Identity ermöglicht es SecOps-Teams:

- **domänenübergreifende Identitätsbedrohungen präzise zu erkennen,**
- **einen noch nie dagewesenen Einblick in Identitätsangriffe und den entsprechenden Kontext zu gewinnen,**
- **durch verbesserte Workflows und einheitliche Warnmeldungen portalübergreifend mit Identitätsadministrator*innen zu kooperieren,**
- **dank erprobter Abhilfemaßnahmen schnell auf Identitätsbedrohungen zu reagieren.**

Identitätssicherheitsstatus stärken

Defender for Identity erkennt Schwachstellen und gibt hilfreiche Tipps zu deren Behebung, um das Risiko eines Identitätsangriffs zu verringern. Viele Cyberkriminelle verschaffen sich beispielsweise über nicht sensible Konten Zugang und breiten sich dann im Unternehmen aus, bis sie eine Gelegenheit finden, ihre Rechte auszuweiten. Mit Defender for Identity können Sicherheitsteams die risikoreichsten Pfade aufdecken und verschließen, bevor ein Cyberkrimineller sie ausnutzt.

Defender for Identity versorgt die Teams mit Tools zur Untersuchung von Identitäten, die einem erhöhten Kompromittierungsrisiko ausgesetzt sind. Mithilfe von Analytics-Daten aus Ihren On-Premises- und Cloud-Umgebungen erkennt Defender for Identity verdächtige Konten und ordnet diese nach Priorität. Für die Untersuchung stehen personabasierte Ansichten bereit, in denen die Identitäten nach geteilten Verantwortlichkeiten, Erfahrungen, Zielen und Zugriffsrechten gruppiert sind. Ebenso können die Sicherheitsteams das Profil eines einzelnen Benutzers gründlich analysieren und sich eine Historie aktiver Warnmeldungen anzeigen lassen.

Kapitel 06

Zukünftige Cyberangriffe verhindern

Eine der besten Möglichkeiten, bei Security Operations Zeit und Geld zu sparen, besteht darin, Cyberangriffe von vornherein zu verhindern. Routinepraktiken wie das Patchen von Software und die ständige Überwachung von Benutzerberechtigungen haben einen enormen Einfluss auf die Sicherheit eines Unternehmens. 99 % aller Cyberangriffe ließen sich abwehren, würde man grundlegende Sicherheitsmaßnahmen beachten.[4] Das Problem für die meisten Unternehmen besteht darin, dass es oft Hunderte oder sogar Tausende potenzieller Sicherheitslücken gibt. Da mitzuhalten, kann sich als unlösbare Aufgabe erweisen.

Sicherheitsschwachstellen effektiv beseitigen

Die Plattform unterstützt Ihr SOC dabei, hochriskante Schwachstellen zu schließen, und gibt fachkundige Empfehlungen zu Sicherheitskonfigurationen und -richtlinien, um den Schutz für Ihre Organisation weiter zu verbessern. Microsoft Defender Vulnerability Management, das in Defender XDR integriert ist, priorisiert Probleme auf Windows-, macOS-, Linux-, Android-, iOS- und auf Netzwerkgeräten und hilft Ihrem Team, die Wahrscheinlichkeit eines Sicherheitsverstoßes vorherzusagen und das Risiko zu minimieren.

Die Funktionen für das Cloud Security Posture Management ermöglichen es Ihrem Team, Sicherheitsrisiken in Microsoft Azure, AWS und Google Cloud Platform aufzudecken und zu priorisieren. Dadurch können Verteidiger*innen:

- basierend auf einer kontinuierlichen Bewertung der in der Cloud laufenden Ressourcen den Sicherheitsstatus beurteilen,
- die kritischsten Schwachstellen beheben,
- die Compliance für regionale und branchenspezifische Vorschriften steuern und verbessern,
- durch kontextbezogene Insights in die Gefährdung sensibler Informationen Daten schützen.

Ihr SOC kann Copilot Fragen zur Umgebung stellen und um Empfehlungen bitten – alles in natürlicher Sprache. Copilot liefert Details zu bekannten Schwachstellen und arbeitet mit der Plattform zusammen, um aus den Erkenntnissen verständliche, umsetzbare Insights abzuleiten.

Aus vergangenen Sicherheitsvorfällen lernen

Opfer eines Cyberangriffs zu werden, ist stressig und potenziell kostspielig, aber sobald sich der Staub gelegt hat, ist Ihr Team klüger und kann die Verteidigung optimieren. Anstatt dass Analyst*innen ihre Zeit damit verbringen, Berichte zu erstellen, fasst Copilot Untersuchungen, Vorfälle und Schwachstellen in Minutenschnelle zusammen, sodass alle Teammitglieder wissen, was passiert ist und warum. Ihre Teams können sich dann auf wichtigere Aufgaben konzentrieren.

Microsoft Defender XDR analysiert die bei realen Cyberangriffen verwendeten Techniken und ordnet ihnen entsprechende Sicherheitsempfehlungen zu. Diese Empfehlungen geben Aufschluss darüber, welche Einstellungen ähnliche Cyberangriffe in Zukunft verhindern, und liefern den Teams Anhaltspunkte für Verbesserungen.

> *Ein starker Sicherheitsstatus und ein guter Schutz von Geräten, Identitäten und Daten sind entscheidend für die Business Continuity und eine Schlüsselkomponente für eine erfolgreiche Abwehr von Cyberangriffen.*
>
> Eric McKinney, Enterprise Infrastructure Director, G&J Pepsi-Cola Bottlers

Kapitel 07

Sicherheitsteams einen Vorsprung verschaffen

Verborgene Muster und Verhaltensweisen erkennen: Copilot nutzt die lückenlose Transparenz der Plattform, um Cyberbedrohungen in Echtzeit aufzudecken.

Sicherheitskräfte fortbilden: IT-Security-Wissen – vermittelt in natürlicher Sprache – ermöglicht es jedem Mitglied des Sicherheitsteams, selbst Nachwuchskräften, komplexe Untersuchungstechniken anzuwenden.

Komplexe Situationen schnell verstehen: Mit Sicherheitsdaten trainierte generative KI wandelt Bedrohungsdaten in verständliche Insights um und spart so den Teams wertvolle Zeit, wenn jede Minute zählt.

Untersuchungen beschleunigen: Copilot liefert verständliche Empfehlungen und detaillierten Kontext zu jedem Sicherheitsvorfall, darunter interne Daten über die Umgebung und externe Informationen über bekannte Bedrohungen.

Umfassende Berichte erhalten: Copilot erstellt in Sekundenschnelle maßgeschneiderte Berichte, die es Sicherheitsteams erleichtern, mit allen Stakeholdern zu kommunizieren.

Den nächsten Schritt eines Angreifers vorhersagen: KI-Modelle lernen kontinuierlich hinzu und können vorhersagen, was ein böswilliger Akteur als Nächstes tun könnte.

Generative KI erweist sich bereits jetzt als Gamechanger im Sicherheitsbereich, da sie Teams effektiver arbeiten lässt und die Untersuchungs- und Reaktionszeit verkürzt. Diese neue Technologie kann die natürliche menschliche Sprache interpretieren und komplexe Daten in leicht verständliche Informationen umwandeln. Dadurch können Sicherheitsteams Bedrohungen schneller abwehren und sogar zukünftige Cyberangriffe vorhersagen.

Copilot schöpft das GPT-4-Modell von OpenAI voll aus, um Unternehmen schnell und adäquat zu verteidigen. Sicherheitsexpert*innen werden in die Lage versetzt, innerhalb von Minuten statt Stunden oder Tagen auf Cyberbedrohungen zu reagieren.

„Wir sind begeistert davon, was mit Microsoft Copilot für Security möglich ist. So können Unternehmen künftigen Bedrohungen immer einen Schritt voraus sein.“

Jeremy J. Hyland, Director of Cyber Defense, Dow Inc.

Teams, die am Early-Access-Programm für Copilot teilnehmen, verzeichnen bereits positive Ergebnisse:

- Sämtliche Aufgaben konnten die Teilnehmenden 44 % präziser und 26 % schneller erledigen.[5]
- 86 % gaben an, Copilot habe ihnen geholfen, die Qualität ihrer Arbeit zu verbessern.[5]
- 83 % äußerten, Copilot haben den Arbeitsaufwand verringert.[5]
- 86 % sagten, Copilot habe ihre Produktivität gesteigert.[5]
- 90 % wollen Copilot auch das nächste Mal verwenden, sollte dieselbe Aufgabe anstehen.[5]

Fazit

Gegen KI-gesteuerte Cyberbedrohungen wappnen

Fortschritte im Bereich der KI verändern bereits die Cybersicherheit. Kriminelle setzen KI ein, um Cyberangriffe zu automatisieren und in kürzester Zeit raffinierte Malware und glaubwürdig klingende Phishing-E-Mails zu erstellen. Die Security-Community macht sich jedoch die neuesten KI-Fortschritte ebenso schnell zunutze und integriert sie in ihre Lösungen, wodurch sich Cyberbedrohungen effizienter und effektiver erkennen und entsprechende Maßnahmen ergreifen lassen.

Vereinfachen Sie zunächst Ihr Sicherheitsmodell, um Ihrem Unternehmen einen Vorteil zu verschaffen. Die durchgängige Security-Operations-Plattform und Copilot von Microsoft sorgen für mehr Transparenz in Ihrer digitalen Infrastruktur. Die leistungsstarken Tools stoppen Cyberangriffe schnell, ganz gleich, wo diese ihren Ursprung haben.

Für Unternehmen mit kleinen Teams oder Problemen bei der Personalgewinnung eignet sich Microsoft Defender Experts for XDR. Dieser Managed Service erweitert Ihr SOC um Expert*innen, die in Ihrem Namen Vorfälle einordnen, untersuchen und darauf reagieren.

Rüsten Sie Ihre Organisation gegen Cyberbedrohungen und setzen Sie dafür auf eine durchgängige Security-Operations-Plattform samt XDR, SIEM und generativer KI.

„Es gibt nicht besonders viele Anbieter auf der Welt, die in der Lage sind, eine Lösung zu entwickeln, die konsolidierte Einblicke in große, komplexe Umgebungen wie die unsere liefert. Deshalb haben wir uns für Microsoft entschieden."

Thomas Mueller-Lynch, Service Owner Lead for Digital Identity, Siemens

Entdecken Sie Ihre Bereitstellungsoptionen

Mehr über die durchgängige Security-Operations-Plattform erfahren

Mehr über Microsoft XDR erfahren

Mehr über Microsoft Sentinel erfahren

Mehr über Copilot erfahren

Verstärken Sie Ihr Team

Mehr über Microsoft Security Experts erfahren

[1] Gartner ist eine eingetragene Marke und Dienstleistungsmarke und Magic Quadrant eine eingetragene Marke von Gartner, Inc. und/oder seinen Tochtergesellschaften in den USA sowie international und werden in diesem Dokument mit Genehmigung verwendet. Alle Rechte vorbehalten. Gartner empfiehlt keine Anbieter, Produkte oder Dienstleistungen, die in deren Marktforschungsberichten vorgestellt werden und rät Technologieanwender*innen dazu, nicht nur die Anbieter mit den höchsten Bewertungen oder anderen Auszeichnungen auszuwählen. Die Gartner-Marktbetrachtungen beruhen auf den Meinungen der Gartner-Forschungsorganisation und sollten nicht als Sachverhalt aufgefasst werden. Gartner schließt alle ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich dieser Studie inklusive Marktgängigkeit oder Eignung für einen bestimmten Zweck aus.

[2] Gartner Magic Quadrant for Endpoint Protection Platforms, Evgeny Mirolyubov, Max Taggett, Franz Hinner, Nikul Patel, 31. Dezember 2023.

[3] The Total Economic Impact™ of Microsoft SIEM and XDR, eine Auftragsstudie, durchgeführt von Forrester im Dezember 2022. Ergebnisse über drei Jahre für ein hypothetisches Unternehmen, basierend auf den Angaben der befragten Kunden.

[4] Microsoft Digital Defense Report 2023, https://www.microsoft.com/en/security/security-insider/microsoft-digital-defense-report-2023/.

[5] Randomisierte kontrollierte Studie zu Microsoft Copilot für Security, durchgeführt von Microsoft Office of the Chief Economist, November 2023.