Bitdefender
BUILT FOR RESILIENCE

GravityZone XDR

Extended Detection and Response

Die Häufigkeit von Cyberangriffen und deren Komplexität sind exponentiell angestiegen. Immer wieder waren ganze Unternehmen nach einem einfachen Klick auf eine URL in einer E-Mail plötzlich offline. ATPs (Advanced persistent threats) können monatelang unbemerkt bleiben und während dieser Zeit Unternehmensdaten abschöpfen, Ransomware platzieren und Dateien aus geschäftsentscheidenden Systemen löschen. Hinzu kommt, dass durch das Arbeiten im Homeofficesowie die Nutzung hybrider Arbeitsmodelle neue Angriffsvektoren entstanden sind, die von Cyberkriminellen ausgenutzt werden können. Obwohl die Technologien zur Vorbeugung gegen Cyberkriminalität immer effektiver geworden sind, haben die Sicherheitsexperten festgestellt, dass hundertprozentige Sicherheit nicht erreichbar ist, weil sich die Angreifer taktisch, technisch und von der Vorgehensweise her ständig weiterentwickeln. Angesichts dieser Tatsache sind Informationen für die Sicherheitsteams A und O, um die Zeit bis zur Erkennung eines Angriffs zu verkürzen und damit letztendlich das Schadensrisiko zu verringern und die Cyberresilienz zu erhöhen.

Die Notwendigkeit, unzusammenhängende Sicherheitsinformationen zu erfassen und zu analysieren, hat zur Entwicklung von EDR (Endpoint Detection and Response) bis hin zu XDR (Extended Detection and Response) geführt. XDR erweitert die Fähigkeiten von EDR noch, weil mehr Datenquellen mit einbezogen werden können und somit ein klareres Bild der einzelnen Schritte eines Angriffs entsteht, sodass sich effektivere Möglichkeiten zur Reaktion finden lassen.

Die Technologie XDR wurde als Antwort auf die erhöhte und mehrere Vektoren umfassende Komplexität von Cyberangriffen entwickelt. Ein effektives XDR-System muss folgende Funktionalität aufweisen:

- Daten aus Quellen erfassen, die bei einem Cyberangriff als Einfallstore wirken können.
- Die Daten mit erweiterten Funktionen aus den Bereichen maschinelles Lernen und KI durchforsten, um Informationen zu finden, die auf einen Angriff hindeuten könnten.
- Durch Entfernen von unnötigen Störfaktoren aus der Angriffsermittlung Alarmmüdigkeit vermeiden.
- Den Sicherheitsteams Mittel für Sofortmaßnahmen an die Hand geben.

Zusammengefasst

GravityZone XDR analysiert und entdeckt Angriffe innerhalb der gesamten IT-Infrastruktur und den Anwendungen eines Unternehmens. Erkennung und Reaktion erfolgen dabei äußerst präzise und schnell. GravityZone XDR deckt die Bereiche Systeme, Produktivitätsanwendungen, Cloud-Workloads, Identität und Netzwerke ab und ermöglicht es den Sicherheitsteams, sich auf die von den Cyberkriminellen hauptsächlich ins Visier genommenen Bereiche zu konzentrieren. GravityZone XDR liefert Analysen und einen umfassenden Sicherheitskontext, um nicht in Zusammenhang miteinander stehende Alarmmeldungen zu korrelieren, Vorfälle schnell zu selektieren und die Angriffe über automatisierte und gesteuerte Reaktionen einzudämmen. All dies mit einer einzigen intuitiven Verwaltungskonsole – und ohne dass bei den Sicherheitsteams durch unnötig viele Alarme Alarmmüdigkeit aufkommt.

Hauptfunktionen

- **Erkennung von Cyberangriffen in den Bereichen Systeme, Produktivitätsanwendungen, Cloud-Workloads, Identität und Netzwerke**
- **Lieferung von Ursachenanalysen zur Prüfung durch die Sicherheitsteams**
- **Visualisierung der gesamten Angriffskette in einem leicht verständlichen Format zur Identifizierung von Schwachstellen in der Sicherheitskette**
- **Schnelles Ergreifen von Gegenmaßnahmen: Löschen von böswilligen E-Mails, Isolation von Hosts, Deaktivierung von Benutzerkonten usw.**
- **Vereiteln von Angriffen, bevor sie zum Tragen kommen, durch vielfach ausgezeichnete Präventionsfunktionen**

"GravityZone XDR zeichnet sich dadurch aus, dass es Vorfälle über längere Zeiträume in unseren gesamten Betriebsaktivitäten korreliert, und wir waren sofort vom Wert dieser Lösung überzeugt. Der Vorteil einer Lösung aus einer Hand, die vorkonfigurierte Erkennungsfunktionen zur Identifikation und Untersuchung bekannter und unbekannter Bedrohungen bietet, und unseren Experten einerseits die Erkenntnisse liefert, um was für einen Vorfall es sich handelt und wie er aufgetreten ist, und andererseits optimale Gegenmaßnahmen anbietet, kann gar nicht hoch genug bewertet werden."

Mahmood Haq, Chief Information Security Officer, MyVest

So erweitert XDR Erkennung und Reaktion über den Endpunkt hinaus

GravityZone XDR kombiniert die vielfach ausgezeichneten Erkennungs- und Präventionstechnologien von Bitdefender mit leistungsfähigen XDR-Sensoren auf den Ebenen der Systeme, Produktivitätsanwendungen, Cloud-Workloads, Identität und Netzwerke. Mit GravityZone XDR können die Sicherheitsteams den gesamten Lebenszyklus eines Angriffs nachverfolgen — vom anfänglichen Einfallstor bis zur bis zur horizontalen Verbreitung — und vieles mehr. GravityZone XDR bietet eine detaillierte Ursachenanalyse und erweitert die Sichtbarkeit auf Bedrohungen jenseits des Endpunkts. Mit den Funktionen von GravityZone XDR erhalten Sicherheitsteams unmittelbar Zugriff auf korrelierte Ereignisquellen, zugrundeliegende Daten und einen aussagekräftigen Kontext, sodass sie die mit einem Cyberangriff zusammenhängend Aktionskette in der gesamten Umgebung schnell erkennen können. Die erweiterte Funktionalität von GravityZone in den Bereichen maschinelles Lernen und KI ermöglichen den Sicherheitsteams Einblicke in Verhaltensmuster, aus denen sich sinnvolle Maßnahmen ableiten lassen. Diese Technologie verringert das Risiko für Fehlalarme und beugt somit Alarmmüdigkeit vor.

GravityZone XDR erfasst Daten aus einer Vielzahl von verschiedenen Systemen:

- Endpunkte und Server – sowohl auf lokalen Systemen als auch in der Cloud
- Microsoft Office 365™: Produktivitätsanwendungen und E-Mail-Programme
- Cloud-Workloads
- Microsoft® Active Directory® für Identitätsmanagement
- Netzwerke

Alle Sicherheitstools für diese Umgebungen lassen sich von einer einzigen intuitiven GravityZone-Konsole aus verwalten.

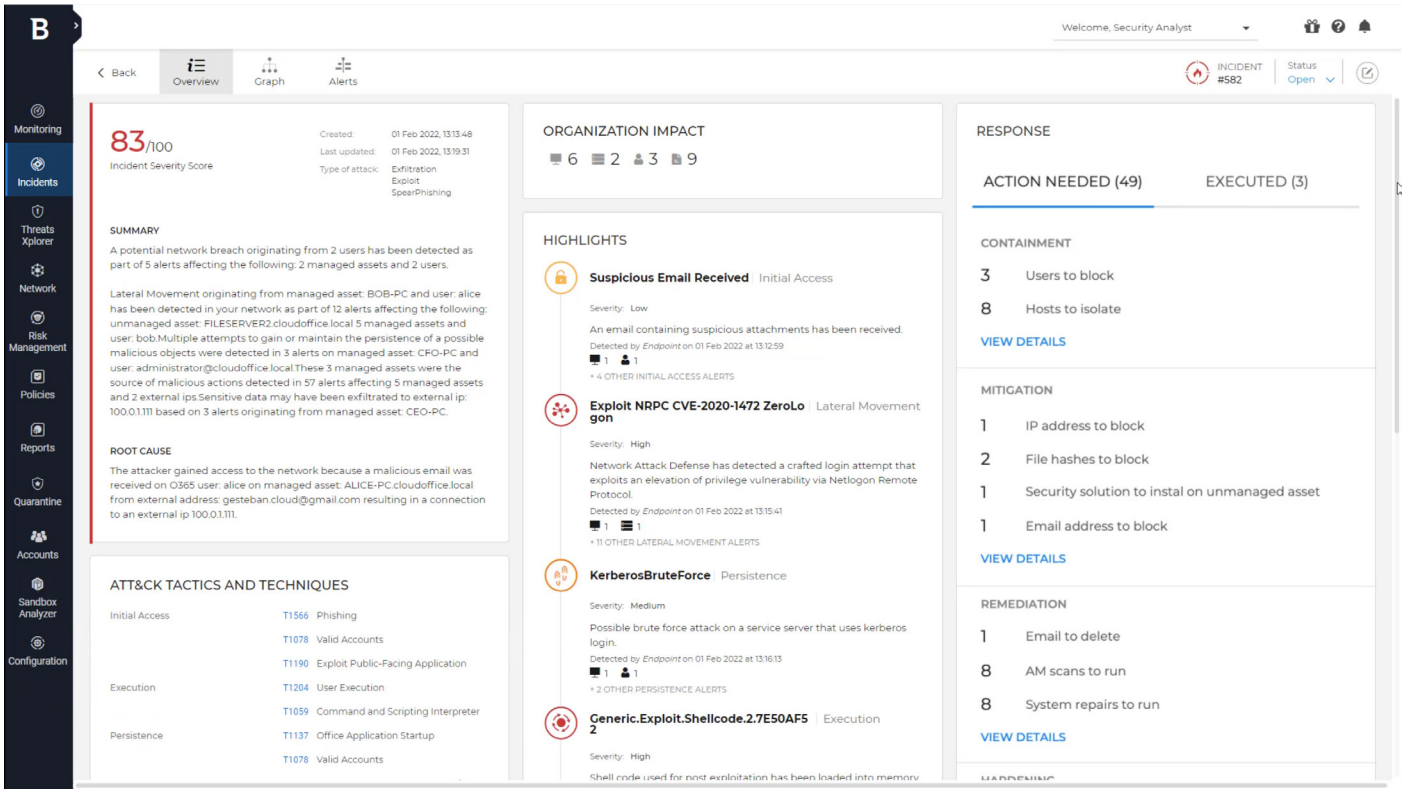

Abb. 1: GravityZone XDR stellt den Sicherheitsteams detaillierte Informationen zu Angriffen bereit. Dies ermöglicht rasche Einblicke in Sicherheitsvorfälle und Ereignisdetails, potenzielle Auswirkungen auf das Unternehmen, vermutliche Ursachen und empfehlenswerte Maßnahmen.

So verbessert XDR Angriffserkennung und Reaktion

GravityZone XDR nutzt GravityZone Business Security Enterprise mit einem oder mehreren XDR-Sensoren. GravityZone bietet branchenweit führende Technologien für Cybersicherheit – Endpunktschutz, Endpunkterkennung und -reaktion, Analyse von Benutzer- und Endpunktrisiken, Abwehr von Netzwerkangriffen, Filterung von Webinhalten, adaptierbares maschinelles Lernen, flexible Richtlinienverwaltung, ausführliches Berichtswesen und vieles mehr – und all dies über eine einzige intuitive Cloud-basierte Verwaltungskonsole. Mit XDR-Sensoren erweitert Bitdefender die Erkennungsfunktionalität über Endpunkte hinaus.

GravityZone XDR unterstützt vier zusätzliche Sensortypen. Diese Sensoren erfassen Informationen von mehren Quellen und leiten sie in eine in eine Engine für erweitertes maschinelles Lernen. GravityZone XDR analysiert die von dieser Engine verarbeiteten Daten und erstellt daraus eine detaillierte Zeitachse des Angriffs, die dann im Modul Incident Advisor dargestellt wird. Mit GravityZone EDR können bereits heute effektive Gegenmaßnahmen getroffen werden, wie z. B. Isolieren eines Hosts, Hochladen von Dateien in die GravityZone-Sandbox zur weiteren Analyse, Beenden von Prozessen und Öffnen einer Remote Shell an Endpunkten. GravityZone XDR erweitert diese Möglichkeiten für Reaktionsmaßnahmen durch Einbindung der nachfolgend beschriebenen Sensoren.

Productivity Applications Sensor

Unter Cyberkriminellen wird das Hacken von Microsoft Office-365-Konten eines der erstrebenswertesten Ziele angesehen. Dabei werden die Opfer oft durch Phishing dazu verleitet, ihre wertvollen Anmeldedaten für Office 365 preiszugeben. Einblicke in dieses Verhalten sind für die Sicherheitsteams von unschätzbarem Wert. GravityZone XDR erkennt sowohl Angriffe, die gegen Konten und E-Mails von Office 365 gerichtet sind, als auch Angriffe, die von solchen stammen.

Das Modul Productivity Applications Sensor (Sensor für Produktivitätsanwendungen) ermittelt Eigentümlichkeiten in Office-365-Konten, die auf die Aktionen von Cyberkriminellen hinweisen können. Der Sensor erkennt folgende Arten von Aktionen:

- Deaktivierung des Anti-Phishing-Schutzes von Office 365
- Dubioses Benutzerverhalten, wie beispielswiese die Erstellung eines neuen Benutzerkontos, für das keine Multi-Faktor-Authentifizierungsanforderungen gelten
- Hochladen von Dokumenten mit verdächtigen Makros auf SharePoint oder OneDrive
- Hochladen von ausführbaren Dateien auf Office-365-Konten
- Verdächtige Zugriffsanforderungen, wie beispielsweise die Anforderung von Zugriff für einen Benutzer auf mehrere Dateien bzw. Verzeichnisse an verschiedenen SharePoint-Standorten innerhalb eines kurzen Zeitraums

Der Sensor erkennt auch ungewöhnliche Benutzeraktivitäten, die vom Referenzmodell für normales Verhalten abweichen. Dies wären beispielsweise eine unübliche Anzahl von administrativen Aktivitäten oder Dokumentbearbeitungsvorgängen an einem bestimmten Tag, die mit dem betreffenden Benutzerkonto normalerweise nicht in dieser Art und Weise durchgeführt werden.

Die Erkennung von verdächtigem Verhalten bei Office 365 erstreckt sich auch auf E-Mails. Der Productivity Applications Sensor erkennt auch die folgenden zweifelhaften Aktivitäten innerhalb von Microsoft Exchange Online™:

- Manipulierte E-Mails, die zum Herunterladen von Dateien von einem gehackten Benutzerkonto verwendet wurden.
- E-Mails für Spearphishing – damit sollen Benutzer zur Preisgabe ihrer Konto-Anmeldedaten verleitet werden.
- Verdächtige Berechtigungsaktivitäten für Postfächer. Beispiel: Ein Benutzer erhält innerhalb eines kurzen Zeitraums die Berechtigung, auf eine Reihe verschiedener Postfächer zuzugreifen.
- Von einem Benutzerkonto aus wird eine große Anzahl von E-Mails aus einem Postfach gelöscht, das nicht dem betreffenden Benutzer gehört.

Neben der Erkennung dieses verdächtigen Verhaltens unterstützt GravityZone XDR die Sicherheitsteams dabei, Maßnahmen zum Schutz ihres Unternehmens zu ergreifen. Mithilfe des Sensors für Office 365 können die Sicherheitsteams vom GravityZone-Dashboard aus E-Mails in Office-365-Organisationen löschen und Office-365-Konten vorübergehend deaktivieren.

Cloud Sensor

Mit dem Modul XDR Cloud Sensor überwacht GravityZone XDR Aktivitäten, aus denen ersichtlich sein kann, ob die Sicherheit von Cloud-Umgebungen, wie beispielsweise Amazon Web Services® (AWS)„ beeinträchtigt ist. Der Sensor überwacht die Umgebung auf mehrere Angriffsindikatoren.

Das Modul Cloud Sensor erkennt Abweichungen dadurch, dass zunächst ein Referenzmodell für normales Verhalten erstellt wird. Jede Aktivität wird dann mit diesem Referenzmodell abgeglichen, sodass "Ausreißer" sofort entdeckt werden. GravityZone erkennt, wenn ein Benutzer eine Aktion durchführt, die nicht zum Referenzmodell passt, wenn eine Datei mit einer verdächtigen Dateierweiterung hochgeladen wurde und außerhalb des Referenzverhaltens liegt und wenn von einer Cloud-Funktion eine Aktion kommt, die vom üblichen Aktivitätsumfang abweicht. Dazu kommen weitere Cloud-spezifische Erkennungsfunktionen.

Außerdem erkennt Cloud Sensor verdächtige Aktivitäten im Zusammenhang mit zahlreichen granularen Cloud-Servicefunktion wie beispielsweise AWS Lambda®. Der Sensor stellt fest, wenn ein Angreifer eine Lambda-Funktion ausgeführt hat, die eine verdächtige Aktion anstößt. Ein Beispiel wäre die Ausführung eines verdächtigen automatischen Codes, wie die Nutzung einer Lambda-Funktion zur Erstellung eines Zugriffsschlüssels, um die Zugrifsskontrolle AWS Identity and Access Management (IAM) auszutricksen. Weiteres Beispiel: GravityZone XDR erkennt die Nutzung einer Lambda-Funktion, mit der durch Aktualisierung einer Sicherheitsgruppe ein bestimmter Port für den Zugriff geöffnet werden soll, als Versuch eines Angreifers, auf die Cloud-Instanz zuzugreifen.

Das Modul Cloud Sensor von GravityZone XDR erkennt auch weitere verdächtige Aktionen, wie beispielsweise wenn ein unbekannter Benutzer oder Host die Standardverschlüsselung aus einem Bucket von AWS Simple Cloud Storage (S3) entfernt. Mit dieser Aktion hebt der Angreifer den Schutz bei allen (über serverseitige Verschlüsselung) verschlüsselten Objekten in diesem S3-Bucket auf. XDR bemerkt, wenn ein Angreifer Services zur Überwachung deaktiviert, indem er z. B. den Anmeldedienst CloudTrail von Amazon anhält oder Protokolle aus dem AWS-Überwachungsdienst CloudWatch löscht. Ferner bleiben auch Erkundungsaktionen der Angreifer in einem S3-Bucket nicht verborgen. Ein typischer Indikator für ein gehacktes Konto, bei dem GravityZone XDR ebenfalls sofort anschlägt, ist die gleichzeitige Anmeldung durch einen Benutzer von mehreren Regionen aus.

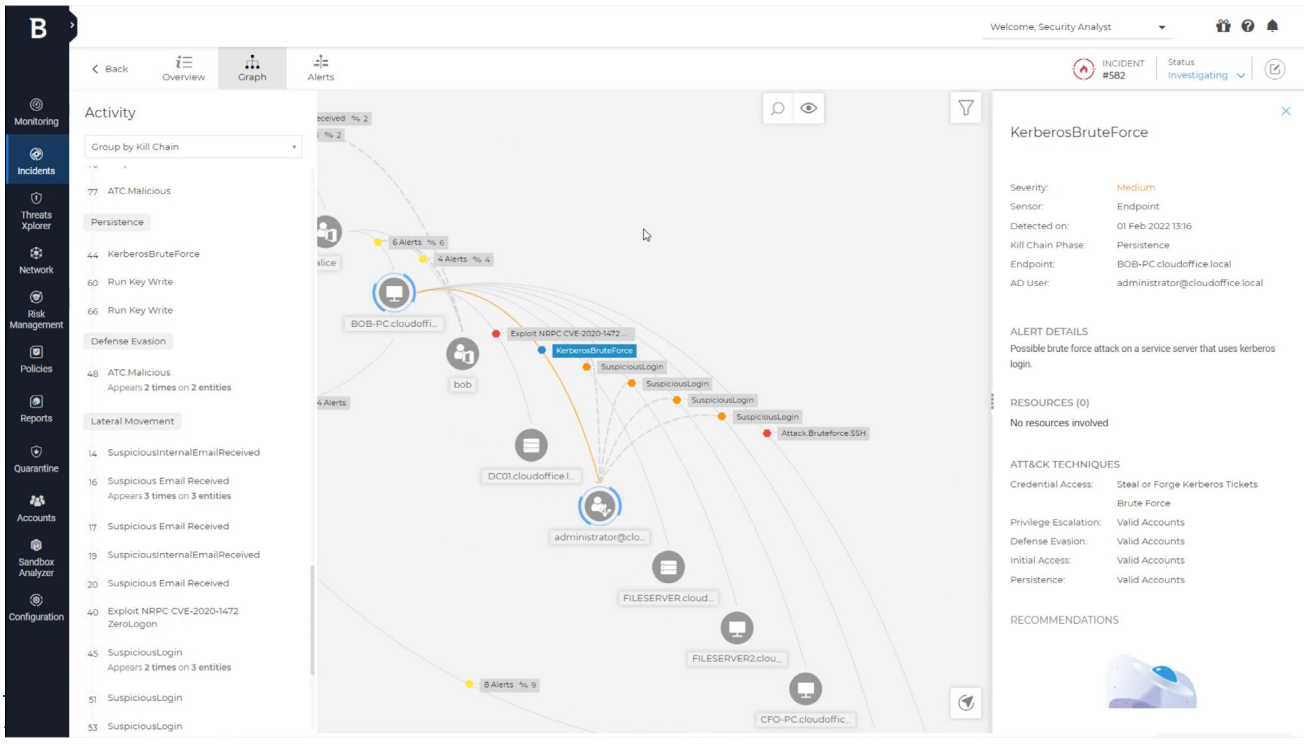

Abb. 2: Sicherheitsteams können detaillierte Informationen zu jedem Aspekt eines Angriffs in der Ansicht Extended Incidents einsehen und prüfen. Unsere Sensoren überwachen Aktivitäten über verschiedene Datenquellen hinweg und korrelieren die Ergebnisse. So stehen die Details zu jedem Angriffspunkt in einem einfach verständlichen Format zur Verfügung. Ja nachdem, wie die Sicherheitsteams Angriffe analysieren möchten, können die Aktivitäten nach Datum/Zeit oder Kill-Chain sortiert werden.

Identity Sensor

Das Modul Identity Security ist eine wesentliche Komponente zur Stärkung der Cyberresilienz. Anhand der Erkennung verdächtiger Authentifizierungsaktivitäten für Anwendungen, DevOps-Tools, Datenbanken, Systeme, Cloud-Umgebungen und andere kritische Ressourcen kann der potenzielle Schaden durch einen Cyberangriff verhindert oder zumindest abgemildert werden. Sobald die Anbindung des Moduls Identity Sensor an das Active Directory erfolgt ist, werden jegliche mit Angriffen im Zusammenhang stehende Aktivitäten entdeckt, bei denen versucht wird, gehackte Konten, Token und Objekte zu nutzen. Dies beschränkt sich nicht auf die Konten von Endbenutzern allein, sondern umfasst auch System- und API-Konten.

Identity Sensor erkennt auch Angriffsversuche, die sich gegen das Netzwerk-Authentifizierungsprotokoll Kerberos richten. Zu den unterstützten Erkennungsfunktionen gehört auch die Fähigkeit festzustellen, ob ein Angreifer versucht, mit einer Kerberos-Anmeldung Brute-Force-Angriffe gegen ein System vorzunehmen. Bei einem Brute-Force-Angriff versucht der Hacker, über in schneller Folge generierte Passwörter oder Verschlüsselungscode Zugriff auf ein System zu erhalten. Der Sensor erkannt auch weitere Aktivitäten im Zusammenhang mit Kerberos. Dazu gehören die Verwendung gestohlener Kerberos-Tickets zur horizontalen Bewegung in einem Netzwerk, die Anforderung von Tickets mit schwacher Verschlüsselung – ein untrügliches Zeichen für böse Absichten – sowie Replay Attacks. Bei diesen Wiederholungsangriffen werden Pakete aus dem Netzwerk entwendet und an einen Service oder eine Anwendung weitergeleitet.

Das Modul Identity Sensor erkennt auch verdächtige Anmeldungen nach der Aufdeckung eines Brute-Force-Angriffs. Der Sensor schlägt an, wenn ein Angreifer im Active Directory einen unseriösen Domänencontroller registriert und über diesen böswillige Objekte in weitere Domänencontroller innerhalb derselben AD-Infrastruktur einschleust. Er erkennt auch, wenn ein Angreifer verschiedene Aktivitäten an einem Active Directory-Objekt durchführt und sich mit gestohlenen Anmeldedaten bei Remote-Systemen anmeldet.

Die leistungsfähige Erkennungskomponente des Moduls Identity Sensor von GravityZone XDR wird durch Funktionen ergänzt, mit denen Sicherheitsteams zielgerichtete Maßnahmen ergreifen können: beispielsweise direkt aus der Verwaltungskonsole von GravityZone ein AD-Konto deaktivieren oder das Zurücksetzen eines Passwords erzwingen.

Network Sensor

Das Modul Network Sensor von GravityZone ist eine virtuelle Appliance zur Überwachung des Datenverkehrs im Netzwerk auf Anzeichen für einen Angriff. Cyberkriminelle versuchen häufig, ihren Angriff im Netzwerk eines Unternehmens dadurch auszuweiten, dass sie von einem System zum nächsten wechseln. Network Sensor unterstützt die Sicherheitsteams dabei, solche horizontalen Bewegungen in ihrem Netzwerk zu entdecken. Das Modul schlägt an, wenn ein Angreifer versucht, Daten an Standorte außerhalb der Organisation zu auszuschleusen. XDR Network Sensor erkennt Techniken zum Scannen von Ports sowie aus dem Netzwerk stammende Brute-Force-Angriffe.

Mit GravityZone XDR Network Sensor können Sie nicht nur netzwerkbasierte Attacken vereiteln, sondern erhalten auch transparent alle notwendigen Informationen, um die Auswirkungen eines Cyberangriffs abzumildern und die Gesamtzeit bis zur Behebung des Problems zu verkürzen.

Erstklassige Sicherheitstools in Kombination mit dem entsprechenden Know-how

GravityZone XDR bietet Unternehmen eine umfassende Cybersicherheitslösung, in der vielfach ausgezeichnete Präventionstechnologie zusammen mit hochmodernen Erkennungs- und Reaktionstechnologien während und nach einem Cyberangriff zielgerichtete Informationen liefern. GravityZone XDR unterstützt Erkennung und Reaktion in den Bereichen Systeme, Produktivitätsanwendungen, Cloud-Workloads, Identität und Netzwerke, sodass die Cyberkriminellen keine Möglichkeit finden, sich vor der Entdeckung zu verbergen. Unternehmen, die einen Sicherheitsbetrieb rund um die Uhr wünschen, bietet Bitdefender Managed Detection and Response (MDR), eine Reihe von Services , die GravityZone XDR nutzen. Unsere MDR-Mitarbeiter sind äußerst erfahrene, zertifizierte Experten mit insgesamt mehr als 100 Jahren Know-how in Cybersicherheit bei Wirtschaftsunternehmen und staatlichen Nachrichtendiensten. Mit MDR erhalten Sie die optimale Kombination aus Sicherheitsfunktionen und Know-how für bestmöglichen Schutz vor den Cyberbedrohungen von heute.

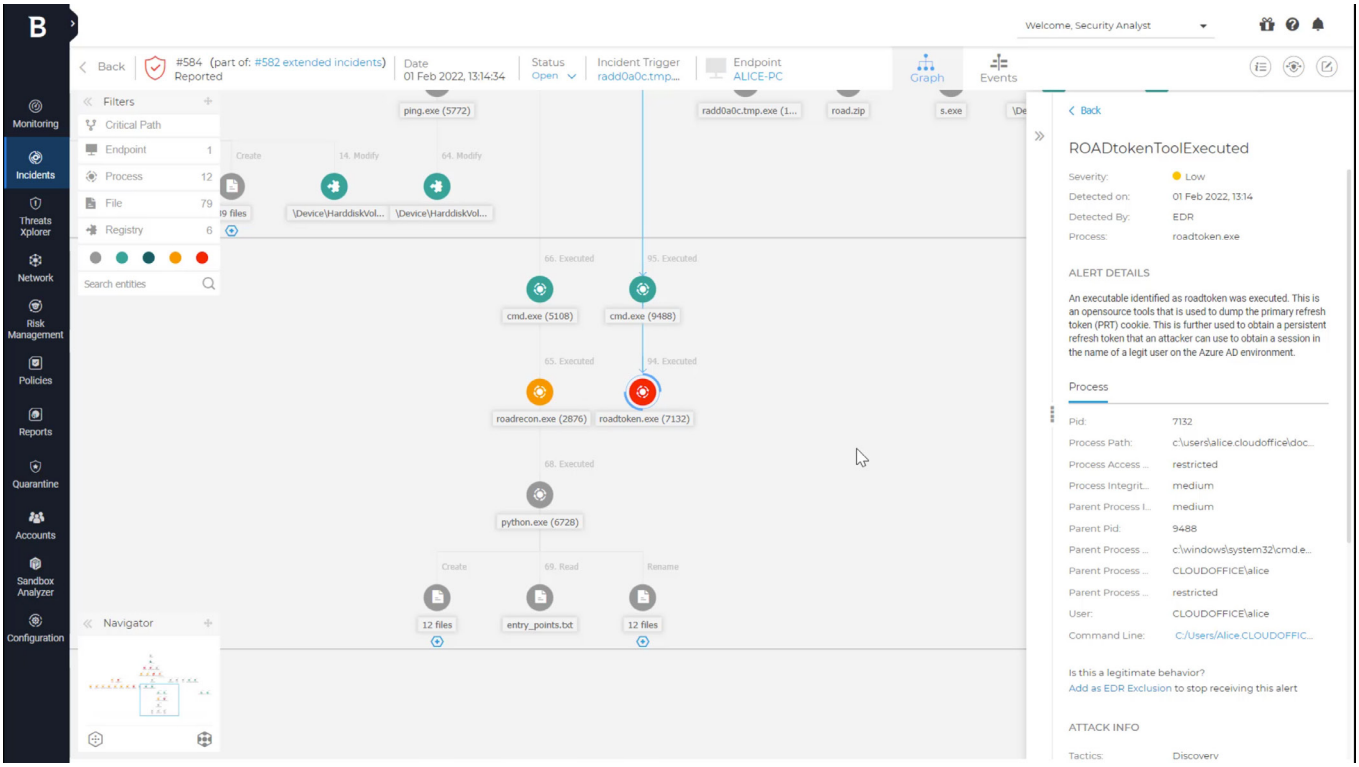

Abb. 3: GravityZone XDR bietet eine detaillierte Visualisierung von Angriffen , die es den Sicherheitsteams ermöglicht, den kritischen Pfad jedes Angriffs nachzuverfolgen. Dabei stehen umfassende Analysen jeder einzelnen an einem Angriff beteiligten Datei zur Verfügung, sodass geeignete Maßnahmen zur Reaktion ergriffen werden können. So können Dateien auf eine Blacklist gesetzt werden, zur weiteren Analyse in die GravityZone-Sandbox hochgeladen werden, der betreffende Host kann isoliert werden usw.

Bitdefender
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, USA

Als führender Anbieter von Cybersecurity-Software bietet Bitdefender weltweit einzigartige Lösungen für die Prävention, Erkennung und Bereinigung von Bedrohungen. Millionen von Heimanwendern, Unternehmen und Behörden vertrauen Bitdefender als zuverlässigem Experten für die Beseitigung von Bedrohungen, den Schutz Ihrer Daten und Privatsphäre und den Aufbau von Cyberresilienz. Bitdefenders umfassende Investitionen in Forschung und Entwicklung zahlen sich aus: So entdecken die Bitdefender Labs mehr als 400 neue Bedrohungen pro Minute und prüfen jeden Tag 40 Milliarden Bedrohungsabfragen. Bitdefender zeichnet für zahlreiche bahnbrechende Innovationen im Malware-Schutz, der IoT-Sicherheit, bei Verhaltensanalysen und künstlicher Intelligenz verantwortlich, und die daraus resultierenden Technologien werden von über 150 Tech-Unternehmen aus aller Welt eingesetzt. Bitdefender wurde 2001 gegründet, betreut Kunden in 170 Ländern und ist weltweit mit Niederlassungen vertreten.

Weitere Informationen erhalten Sie unter https://www.bitdefender.de.

Bitdefender_BSG_XDR_TechnicalBrief_NoPrint_NoLocalization_DEX592P-de_DE
CD-May/06/2022 • MD-May/06/2022