VECTRA
SECURITY THAT THINKS®

KURZVORSTELLUNG

Absicherung der nationalen kritischen Infrastruktur mit Netzwerk-Erkennung und Response (NDR)

Unternehmen aus dem öffentlichen und privaten Sektor – von Behörden und dem Militär bis hin zu Banken, dem Energie- und Transportsektor – werden immer digitaler und erhoffen sich daraus wirtschaftliche Einsparungen, Produktivitätsvorteile sowie Mehrwert für Kunden und Bürger.

Hinter dieser digitalen Transformation steht eine Vielzahl neuer Technologien und Ansätze, z. B. Mobilgeräte, IoT, Cloud und überall verfügbare Internet-Hochgeschwindigkeitsverbindungen. Sie alle ermöglichen Innovationen und neue Nutzungsmöglichkeiten, vergrößern jedoch auch die Cyber-Angriffsfläche.

Diese wichtigen Services und Infrastrukturen sind Komponenten der nationalen kritischen Infrastruktur (Critical National Infrastructure, CNI). Sie sind verlockende Ziele für staatliche Bedrohungsakteure, Hacktivisten und Terrororganisationen, die das tägliche Leben stören wollen.

„Die Frage ist meiner Meinung nach nicht ob, sondern wann, und wenn wir es bis zum Ende des Jahrzehnts ohne Kategorie-1-Angriff schaffen, haben wir enormes Glück gehabt."

Ciaran Martin
CEO, National Cyber Security Centre, Großbritannien[1]

62 %

Laut einer Umfrage des SANS Institute zu Incident Response führten 62 % der erkannten Zwischenfälle zu einer Kompromittierung von Informationen, Geräten oder Systemen.[3]

HIGHLIGHTS

- Eine Gemeinsamkeit ist die Forderung nach kontinuierlicher Sicherheitstransparenz und Netzwerküberwachung, mit der Anzeichen aktiver Bedrohungen erkannt und abgewehrt werden können. In vielen Fällen wird die Netzwerkinfrastruktur explizit als Prüfpunkt vorgegeben.
- Das Ausbremsen der Angreifer ist nur ein Teil des Problems. Ebenso wichtig sind schnellere Abläufe bei den Verteidigern. CNI-Unternehmen müssen Angreifer, die erfolgreich in ihre Systeme eingedrungen sind, schnell erkennen, verstehen und abwehren können sowie ihre Aktionen rückgängig machen.
- Eine grundsätzliche Schwäche von Bedrohungssignaturen besteht darin, dass sie nach bekannten böswilligen Schaddaten suchen, während die Anomalieerkennung nur Abweichungen feststellt und sie nicht von schädlichem Verhalten unterscheiden kann.
- Mit Cognito Recall™ können Security-Analysten ausgedehnte Recherchen in zuverlässigen, verwertbaren Informationen zu Vorfällen durchführen, die von Cognito Detect™ – einer Untersuchungs-Workbench für das proaktive Threat Hunting – erkannt wurden.
- Durch den Einsatz von KI zur Automatisierung von Bedrohungserkennung und Response mit der Cognito NDR-Plattform können CNI-Unternehmen die Sicherheitsprozesse, die bislang Tage, Wochen oder gar Monate dauerten, auf wenige Minuten verkürzen. Das gibt Security-Teams die Möglichkeit, Maßnahmen zu ergreifen, um Beschädigungen oder Kompromittierungen von Daten zu verhindern.

CNI-Organisationen müssen bereit und in der Lage sein, sich vor einer Vielzahl von Bedrohungen zu schützen, die sie bestehlen, lahmlegen, schädigen oder ihre Abläufe in anderer Weise zu unterbrechen versuchen. Gut ausgestattete und motivierte Angreifer sind gefährlich kompetent und so hartnäckig, dass die Zahl versuchter Angriffe immer weiter steigt.

Die zugrundeliegenden Netzwerke und Informationssysteme, die hinter den kritischen Services und Funktionen stehen, sind mittlerweile reguliert. Ziel ist dabei, das Cyber-Risiko zu senken und die Resilienz zu stärken. Das US-amerikanische NIST-Framework sowie die NIS-Direktive der Europäischen Union identifizieren wichtige, als kritisch betrachtete Branchen und Sektoren und definieren entsprechende Schritte zur Absicherung von Services.

Diese Initiativen wiesen den Weg für landesspezifische Regularien dafür, wie CNI in Unternehmen geschützt werden muss. Beispiele sind KRITIS in Deutschland, MELANI in der Schweiz sowie das australische Critical Infrastructure Centre. Sie alle haben die Forderung nach kontinuierlicher Sicherheitstransparenz und Netzwerküberwachung gemeinsam, mit der erste Anzeichen aktiver Bedrohungen erkannt und abgewehrt werden können. In vielen Fällen wird die Netzwerkinfrastruktur explizit als Prüfpunkt vorgegeben.

Schnellere Abläufe für die Verteidiger

- Einblicke in Bedrohungen und Kontext
- Detaillierte Detektionen mit wenigen False Positives
- Schnelle und genaue Informationen
- Effektive Response
- Bestätigte Wiederherstellung
- Erkenntnisse und Anpassungen

Ausbremsen der Angreifer

- Minimierung der Angriffsflächen
- Schutz des Perimeters
- Defensive Kontrollen
- Informationsverwaltung

Transparenz und Agilität als Grundlage für effektive Incident Response

Keine Schutzmaßnahme ist perfekt. Eine Untersuchung aus dem Jahr 2019 zeigte, dass Bedrohungsakteure sich im Mittel 56 Tage lang in Unternehmensnetzwerken verbergen und darin frei bewegen können.[2] Die Verweildauer bei solchen Angriffen kann schwerwiegende Schäden ermöglichen. Tatsächlich führten laut einer Umfrage des SANS Institute zu Incident Response 62 % der erkannten Zwischenfälle zu einer Kompromittierung von Informationen, Geräten oder Systemen.[3]

Logische erste Schritte sind die Identifizierung potenzieller Bedrohungen sowie die Festlegung entsprechender Sicherheitskontrollen. Gleichzeitig muss jedoch berücksichtigt werden, dass hartnäckige, motivierte und kompetente Angreifer stets einen Weg in die digitale Infrastruktur eines Unternehmens finden werden.

„Das größte Problem ist für mich immer wieder die Geschwindigkeit. Ich fordere vom Team regelmäßig Vorschläge, um schneller und flexibler zu werden."

Adm. Michael Rogers,
Director der National Security Agency, Commander des U.S. Cyber Command und Chief of the Central Security Service (2014-2018)[4]

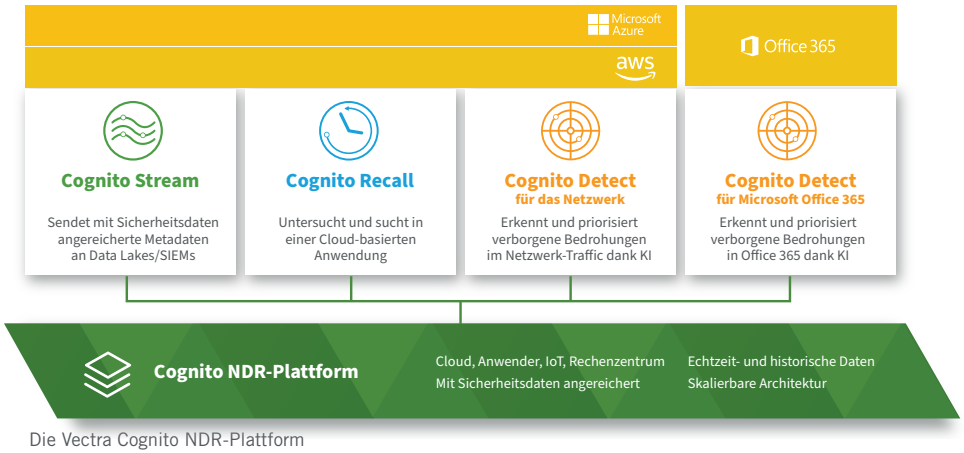
Das Ausbremsen der Angreifer ist nur ein Teil des Problems. Ebenso wichtig sind schnellere Abläufe bei den Verteidigern. CNI-Unternehmen müssen Angreifer, die es in die Cloud, das Rechenzentrum oder die IT- bzw. IoT-Netzwerke geschafft haben, schnell entdecken, analysieren, abwehren und ihre Aktionen rückgängig machen.

Jedes Element eines CNI-Unternehmens – ganz gleich, ob Cloud-Service, Rechenzentrum, Netzwerkgerät oder Anwender – stellt eine Angriffsfläche dar. Viele Komponenten (z. B. IoT-Geräte) verfügen nur über wenige oder gar keine direkten Sicherheitskontrollen oder Überwachungsmöglichkeiten.

Cloud, Rechenzentrum, IT- und IoT-Netzwerke bieten Eintrittspunkte, über die Angreifer in die Infrastruktur eindringen und sich dort ausbreiten können. Doch der Umfang der Daten sowie die Zahl der verwertbaren Spuren der Angreifer bedeuten, dass manuelle Analysen und Erkennungen nicht mit der notwendigen Reichweite, Geschwindigkeit oder Effizienz erfolgen können.

Die Vectra® Cognito®-Plattform für Netzwerk-Erkennung und Response (NDR) liefert automatisierte und zuverlässige Warnmeldungen. Gleichzeitig verhindert sie falsche Erkennungen sowie False Positives. Die Plattform erfasst auch Metadaten aus dem gesamten Netzwerk-Traffic, also Cloud, Rechenzentrum, IT- und IoT-Netzwerke, und reichert sie mit Sicherheitsinformationen und Kontext an.

Dadurch können Security-Teams forensische Spuren schneller und umfassender auswerten sowie proaktiv nach Bedrohungen suchen.



Die Vectra Cognito NDR-Plattform

Die Cognito NDR-Plattform bietet zusätzliche Erkenntnisse zu den Bedrohungsdaten, die von EDR-Tools (Endgeräte-Erkennung und Response) geliefert werden, und erkennt Angreiferverhalten, das nur in der Cloud, in Rechenzentren sowie in IT- und IoT-Netzwerken sichtbar ist.

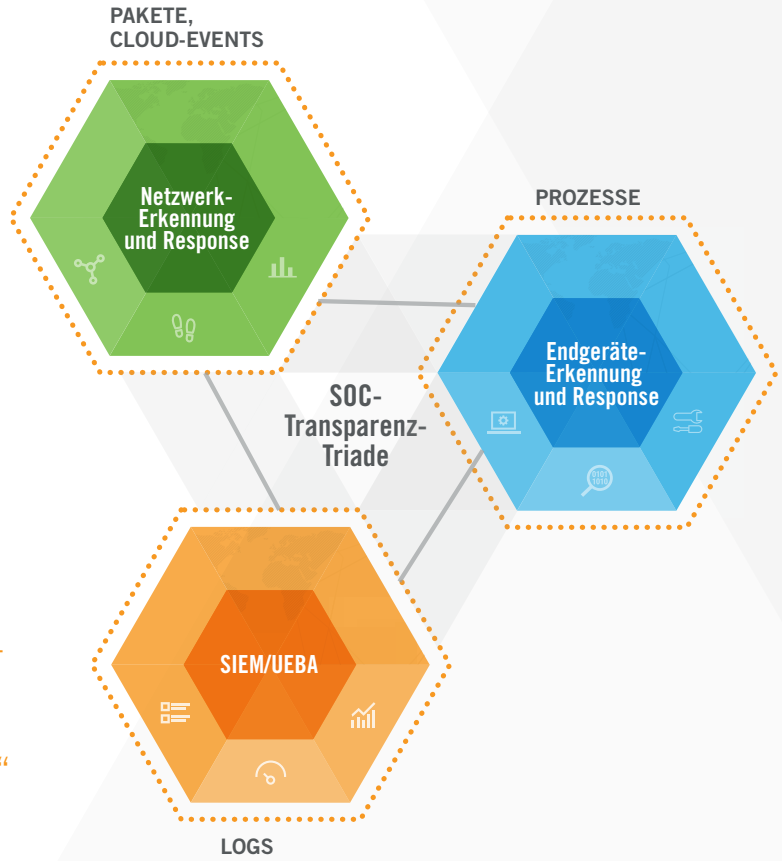
Die Security Operations Center (SOCs) von CNI-Unternehmen können Daten zu erkannten Bedrohungen aus EDR- und NDR-Tools in einem SIEM-System zusammenführen. Dieses agiert als Bindeglied für alle Security-Daten sowie für SOAR (Security Orchestration and Response).

„Das Besondere an Vectra ist die einzigartige Flexibilität und Agilität bei der Erkennung grundlegender Angriffsverhaltensweisen, z. B. Command & Control-Kommunikation, Missbrauch von Zugangsdaten für Konten, Exfiltration von Daten, Botnet Monetization und frühe Indikatoren für Ransomware-Aktivitäten."

Vikrant Gandhi,
Industry Director bei Frost & Sullivan

Diese Automatisierung ermöglicht die dringend notwendige Beschleunigung vieler Response-Aufgaben, was auch als SOC-Transparenz-Triade bekannt ist. Damit wird das Risiko unerkannt agierender Angreifer in einem Unternehmen erheblich verringert.

Für führende EDR-, SIEM- und SOAR-Tools stellt Vectra ergänzende technische Integrationskits bereit, die das Deployment vereinfachen, Risiken verringern und Arbeitsprozesse beschleunigen.



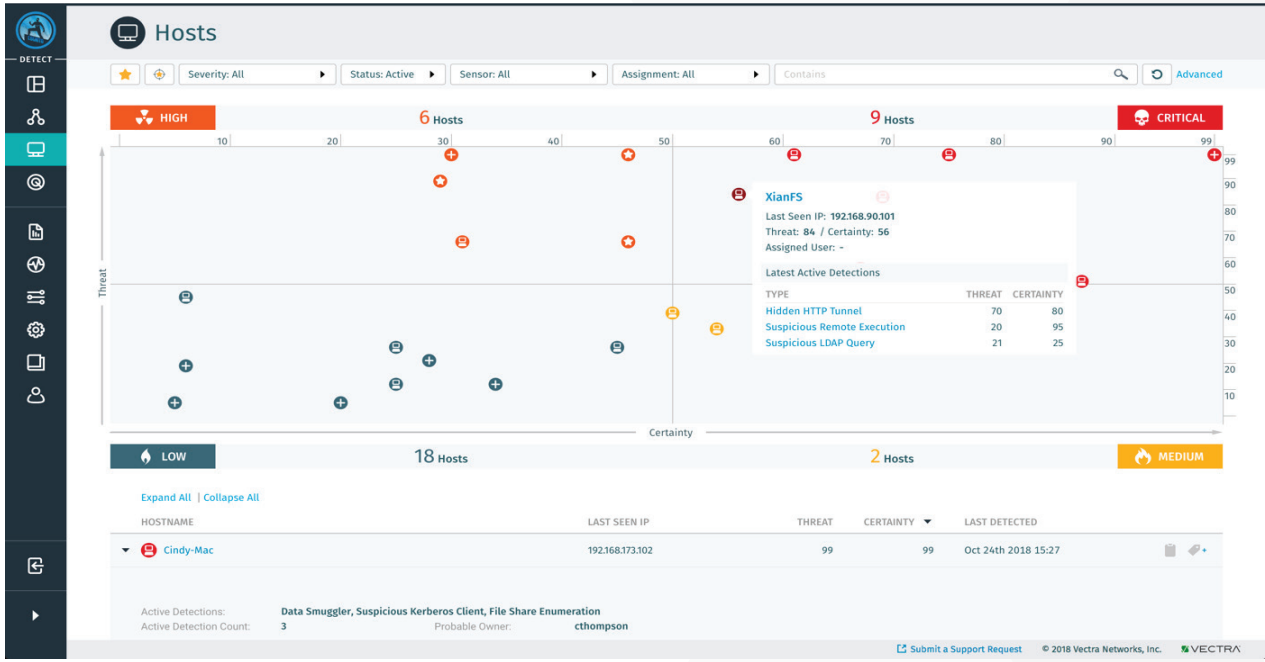
Erkennung der stets vorhandenen Verhaltensweisen von Angreifern

Die Erkennung aktueller hochentwickelter Angriffe stützt sich nicht mehr auf herkömmliche Bedrohungssignaturen oder die Aufdeckung einfacher ungewöhnlicher Verhaltensweisen. Eine grundsätzliche Schwäche von Signaturen besteht darin, dass sie nach bekannten böswilligen Schaddaten suchen, während die Anomalieerkennung nur Abweichungen feststellt und sie nicht von schädlichem Verhalten unterscheiden kann. Damit ist es für Angreifer ein Leichtes, solche Sicherheitskontrollen zu unterlaufen, indem sie sich wie reguläre Anwender verhalten und lediglich normale Verhaltensweisen zeigen.

Moderne Erkennungsansätze konzentrieren sich darauf, grundlegende böswillige Verhaltensweisen zu identifizieren. Vergleichen lässt sich das mit der Suche nach böswilligen Verben statt nach böswilligen Substantiven.

Den Angreifern steht ein nahezu unbegrenztes Arsenal von Tools zur Verfügung, mit denen sie im Netzwerk spionieren, sich bewegen und Daten stehlen können. Dennoch folgen sie dabei stets den gleichen Verhaltensweisen.

Eine grundsätzliche Schwäche von Signaturen besteht darin, dass sie nach bekannten böswilligen Schaddaten suchen, während die Anomalieerkennung nur Abweichungen feststellt und sie nicht von schädlichem Verhalten unterscheiden kann.



Kritische Hosts priorisiert nach Threat Certainty Index in Cognito Detect

Durch die Überwachung und Erkennung solcher böswilligen Verhaltensweisen in der CNI-Infrastruktur lassen sich aktive Angreifer aufdecken.

Dieser Ansatz ist langfristig sehr nützlich, lässt sich ohne Vectra jedoch nur schwer umsetzen. Deshalb kombiniert Cognito Detect die Erkenntnisse aus Bedrohungsforschung, Datenwissenschaft, fortschrittlichen Algorithmen für maschinelles Lernen sowie Verhaltensanalysen.

Cognito Detect ist Bestandteil der Cognito NDR-Plattform und soll die Absicht von Netzwerk-Traffic ermitteln und so böswilliges Verhalten offenlegen, ohne dabei von anderen Anwendungen abhängig zu sein – selbst wenn der Traffic verschlüsselt ist. Bei diesem Ansatz werden verschiedene Aktivitäten aufgedeckt, auf die Angreifer nicht verzichten können, was ihnen die Möglichkeit zum Verstecken nimmt.

Cognito Detect wendet algorithmische Modelle direkt auf den Netzwerk-Traffic und Cloud-Ereignisse an, um zugrundeliegendes Angriffsverhalten zu enttarnen. Diese Daten werden automatisch mit Informationen aus Sekundärquellen wie Authentifizierungsprotokollen und Threat-Intelligence angereichert. Auch wenn die Sekundärquellen für die Aufdeckung der Angreifer nicht notwendig sind, bieten sie Kontext und beschleunigen den Erkennungs- und Response-Prozess von Security-Analysten.

Detektionen werden triagiert, bewertet, priorisiert und im Threat Certainty Index™ des Cognito Detect-Dashboards angezeigt. Dabei sind alle Detektionen einem Host sowie privilegierten Identitätskonten zugeordnet. Zudem werden sie mit anderen Hosts und privilegierten Identitätskonten korreliert, die an der gleichen Angriffskampagne beteiligt sind. Eine aktuelle Untersuchung von Cognito Detect-Deployments zeigte, dass der Arbeitsaufwand von Tier-1-Security-Analysten um das 38-fache verringert wird.[5]

Untersuchung von Zwischenfällen und Threat Hunting

Eine weitere Komponente der Cognito NDR-Plattform ist Cognito Recall. Damit können Security-Analysten umfangreiche Untersuchungen der von Cognito Detect offengelegten Zwischenfälle durchführen. Durch die detaillierten und verwertbaren Daten ist es als Untersuchungs-Workbench für das proaktive Threat Hunting unverzichtbar.

Cognito Recall extrahiert mit Sicherheitsdaten angereicherte Netzwerk-Metadaten aus allen Datenpaketen und erlaubt so Analysen des Netzwerk-Traffics. Metadaten werden in unbegrenztem Umfang in der Cloud gespeichert und können dort durchsucht, analysiert und für retrospektives Threat Hunting genutzt werden.

Jedes IP-fähige Gerät im Netzwerk wird identifiziert und überwacht. Sie legen fest, wie lange die erfassten Daten gespeichert werden sollen. Die erfassten Metadaten umfassen den gesamten internen Traffic, Internet-basierten Traffic sowie Traffic und Events in der virtuellen Infrastruktur und in Cloud-Computing-Umgebungen.

VERRINGERTER AUFWAND PRO 10.000 GERÄTE, NACH BRANCHE

Branche	Erfasste Events	Detektionen	Geräte mit Detektionen	Kritischer Schweregrad	Hoher Schweregrad	Verringerung des Aufwands
Bildungswesen	12.666	617	650	11	34	19x
Energie-versorgung	18.617	598	338	8	16	55x
Finanzwesen	19.510	511	361	8	20	54x
Behörden	9.328	249	268	6	12	35x
Gesundheits-wesen	15.423	381	411	7	16	38x
Fertigungs-unternehmen	17.064	431	323	6	15	53x
Einzelhandel	9.437	421	283	7	24	33x
Dienstleistungen	14.679	430	365	12	20	40x
Technologie	18.100	1.193	634	12	23	29x

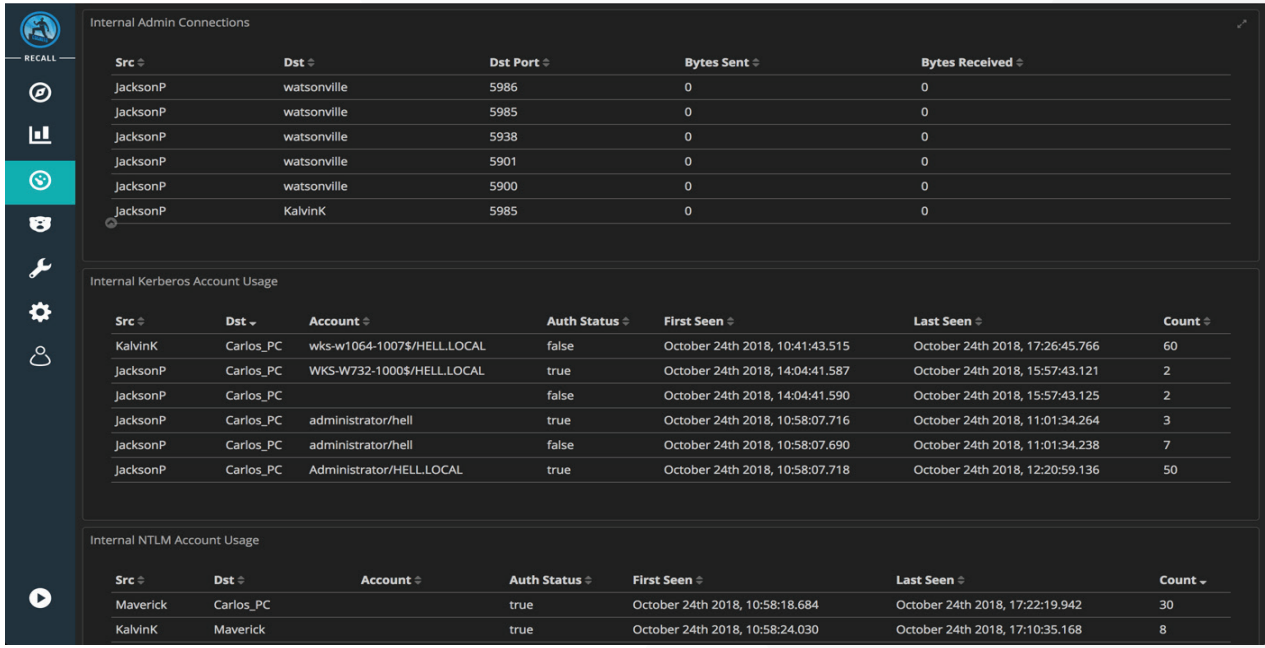
Cognito Detect verringert den Arbeitsaufwand für Tier-1-Security-Analysten

Das bezieht Laptops, Server, Drucker, BYOD- und IoT-Geräte sowie Betriebssysteme und Anwendungen ein. Abgedeckt wird auch der Traffic zwischen virtuellen Workloads in der Cloud und in Rechenzentren – selbst SaaS-Anwendungen. Daten aus Systemauthentifizierungs- und SaaS-Protokollen liefern Kontext für die Analyse der Netzwerk-Metadaten und ermöglichen die genaue Identifizierung von Systemen und Anwendern.

Dank Funktionen zur vollständigen Metadaten-Suche und unbegrenzter Speicherkapazitäten können Security-Analysten mit Cognito Recall feststellen, ob die Metadaten Hinweise auf Kompromittierungen enthalten. Dabei werden Anwender, IP-Adressen und Domains berücksichtigt.

Cognito Recall liefert zudem detailliertere Informationen für effizienteres Threat Hunting, z. B. PowerShell-Befehle von einem Remote-System an einen Server oder eine bestimmte Verbindungsart von einem Remote-Standort.

In einigen Fällen können Anomalien mehrere dieser Verhaltensweisen enthalten, z. B. wenn ungewöhnliche Datenmengen an eine ungewöhnliche IP-Adresse gesendet werden.



Erweiterte kontobasierte Untersuchungen in Cognito Recall

Dank der engen Verzahnung von Cognito Recall und Cognito Detect können Analysten eigene Erkennungsmodelle erstellen und Suchen speichern, um spezifische Untersuchungen und Erkennungsmaßnahmen für ihr Unternehmen anzupassen.

Dabei können Security-Analysten problemlos der damit zusammenhängenden Kette von Ereignissen folgen – ganz gleich, ob der Angreifer zuerst von Cognito Detect, einem Security-Produkt eines anderen Anbieters oder mithilfe durchsuchbarer, hochwertiger Threat Intelligence in historischen Netzwerk-Metadaten entdeckt wurde.

Sobald Cognito Recall Ereignisse oder Warnmeldungen von Cognito Detect oder einem Drittanbieter-Security-Produkt erfasst, erhalten Security-Analysten einen vollständigen Rundumblick auf alle Workload- und Geräte-Aktivitäten.

Dank der engen Verzahnung von Cognito Recall und Cognito Detect können Analysten eigene Erkennungsmodelle erstellen und Suchen speichern, um spezifische Untersuchungen und Erkennungsmaßnahmen für ihr Unternehmen anzupassen.

Mit Cognito Recall lassen sich außerordentlich effiziente Untersuchungen durchführen. Dazu steht Security-Analysten der gesamte Kontext von Vorfällen zur Verfügung, ergänzt um relevante Details zu involvierten Geräten, Konten und zur Netzwerkkommunikation.

Ein weiterer Eckpfeiler der Cognito NDR-Plattform ist Cognito Stream™. Diese Komponente leitet mit Sicherheitsdaten angereicherte Metadaten zur Analyse und Archivierung an den Data Lake des CNI-Unternehmens oder an weitere Tools weiter. Dadurch haben Security-Analysten unmittelbaren Zugriff auf die richtigen Daten sowie den richtigen Kontext und können Zwischenfälle noch schneller untersuchen.

Cognito Stream extrahiert hunderte Metadaten-Attribute, die in der Cloud sowie im Unternehmen erfasst wurden, und stellt die verwertbaren, mit Sicherheitsdaten angereicherten Metadaten im kompakten und leicht verständlichen Zeek-Format dar.

So erhalten Analysten alle benötigten Details – ohne die problematische Speicherungskomplexität von NetFlow und den Zusatzaufwand durch kontinuierliche Paketerfassungen und -aufzeichnungen. Cognito Stream lässt sich in weniger als 30 Minuten einrichten und erfordert keine Leistungsoptimierung oder kontinuierliche Wartung.

„Vectra hat sich für uns bei der Implementierung einer Threat Hunting-Initiative hervorragend bewährt.“

Security-Analyst, Behörde in Nordamerika

Durch die Analyse anonymisierter Metadaten aus hunderten Deployments der Cognito NDR-Plattform konnte Vectra Verhaltensweisen und Taktiken von Angreifern identifizieren.

Erkenntnisse über das Verhalten von Angreifern in CNI-Unternehmen

Dank Vectra können hunderte Unternehmen auf der ganzen Welt ihre nationale kritische Infrastruktur absichern. Der Vorteil von Vectra: geringere Gefahr von Kompromittierungen, effizientere Security Operations, Unterstützung bei der Einhaltung von Compliance-Vorschriften sowie Ausdehnung von Cyber-Sicherheit auf Cloud-Prozesse.

Durch den Einsatz von KI zur Automatisierung von Bedrohungserkennung und Response mit der Cognito NDR-Plattform können CNI-Unternehmen die manuellen Sicherheitsuntersuchungen, die bislang Tage, Wochen oder gar Monate dauerten, auf wenige Minuten verkürzen. Das gibt SOC-Teams die Möglichkeit, sofort Maßnahmen zu ergreifen, um Beschädigungen oder Kompromittierungen ihrer Daten zu verhindern.

Durch die Analyse anonymisierter Metadaten aus hunderten Deployments der Cognito NDR-Plattform konnte Vectra Verhaltensweisen und Taktiken von Angreifern identifizieren. In vielen Fällen können diese Taktiken nicht vollständig blockiert werden, ohne legitime Abläufe erheblich zu beeinträchtigen. Deshalb ist frühzeitige und effektive Erkennung und Response unverzichtbar.

Fazit

Da Security-Teams nur über begrenzte Ressourcen verfügen, gewinnt KI immer größere Bedeutung für die Absicherung von CNI-Unternehmen. Dabei soll KI die Mitarbeiter nicht ersetzen, sondern sie mit Security-Analysen, Kontext und detaillierten Erkenntnissen unterstützen, die schneller und umfangreicher zur Verfügung stehen, als das für Menschen möglich wäre.

Die Security-Teams von CNI-Unternehmen müssen davon ausgehen, dass Kompromittierungen unausweichlich sind, und sich auf die frühzeitige Erkennung und Abwehr raffinierter Angreifer konzentrieren. Mit der KI-gestützten Cognito NDR-Plattform von Vectra können die SOC-Teams von CNI-Unternehmen verborgene Bedrohungen in der Cloud, im Rechenzentrum sowie in IT- und IoT-Netzwerken schneller aufspüren und darauf reagieren.

1. The Guardian: „Major cyber-attack on UK a matter of ‘when, not if’ – security chief“ (Sicherheitsverantwortlicher: Schwerwiegende Cyber-Angriffe in Großbritannien nur eine Frage der Zeit), 2018.
2. M-Trends 2020.
3. SANS Institute: SANS 2019 Incident Response (IR) Survey“ (Umfrage des SANS Institute zu Incident Response), 2020.
4. The Hill: „Our focus on Russian hacking obscures the real problem“ (Unsere Fixierung auf russische Hacker ignoriert das wahre Problem), 2017.
5. Vectra: „2020 Attacker Behavior Industry Report“ (Branchenbericht zum Verhalten der Angreifer 2020).

Weitere Informationen finden Sie unter www.vectra.ai/industries/cni

E-Mail: info@vectra.ai vectra.ai/de