VECTRA
SECURITY THAT THINKS

WHITE PAPER

Automatisierung mit künstlicher Intelligenz im Security Operations Center

INHALTSVERZEICHNIS

Vectra® schützt Unternehmen durch Erkennen und Stoppen von Cyber-Angriffen.

Is führender Anbieter für Netzwerk-Erkennung und Response (NDR) schützt Vectra® Ihre Daten, Systeme und Infrastruktur. Mit Vectra AI kann Ihr Team Angriffsversuche erkennen und reagieren, noch bevor die Attacke startet.

Dabei erkennt Vectra AI schnell verdächtige Verhaltensweisen und Aktivitäten in Ihrem gesamten lokalen und Cloud-Netzwerk, kennzeichnet sie und benachrichtigt Ihr Security-Team, damit es sofort reagieren kann.

Vectra AI steht für *Security that thinks*®. Mit künstlicher Intelligenz verbessern wir die Erkennung und Response im Laufe der Zeit und vermeiden False Positives – damit Sie sich auf die echten Bedrohungen konzentrieren können.

90 %

Cognito Detect nutzt KI zur Automatisierung von Bedrohungsuntersuchungen und spart dadurch bis zu 90 % Zeit. Dadurch können sich die SOC-Teams auf die Verhinderung und Behebung von Datenlecks konzentrieren.

HIGHLIGHTS

- Der wichtigste Faktor bei der Erkennung von Netzwerkkompromittierungen ist die Zeit. Zum Schutz wichtiger Assets vor Diebstahl oder Manipulation müssen die Cyber-Angreifer in Echtzeit erkannt werden.
- Die besten KI-gestützten Sicherheitslösungen sind rund um die Uhr aktiv und automatisieren einen Großteil der Arbeit von Tier-1-Analysten. Das senkt den Personal- und damit auch den Kostenaufwand für das SOC und verkürzt zudem erheblich die Zeitspanne bis zur Erkennung und Behebung von Bedrohungen.
- Die automatisierte Erkennung von Cyber-Angriffen ist ein zentraler Vorteil von Cognito Detect. Unser Ansatz basiert auf einem einfachen Prinzip zum Aufspüren verborgener Bedrohungen: Wir wenden KI auf die aussagekräftigste Datenquelle an – den Netzwerk-Traffic.
- Cognito Detect nutzt Algorithmen zur Verhaltenserkennung für die Analyse von Metadaten aus erfassten Paketen. Auf diese Weise werden verborgene und unbekannte Angreifer in Echtzeit aufgespürt, selbst wenn der Traffic verschlüsselt ist.
- Dank des Echtzeit-Einblicks in Angriffe und kontinuierlichem Threat Hunting mit selbstlernenden Verhaltensmodellen können SOCs die Verweildauer von Cyber-Kriminellen verkürzen und die Reaktionsmaßnahmen beschleunigen.

Immer mehr Unternehmen richten zur Abwehr der zunehmenden Cyber-Attacken Security Operations Center (SOCs) ein.

Der Grund: Nicht nur die Zahl der Risiken, der Bedrohungen und der Angreifer steigt, sondern auch die Raffinesse und das Schadenspotenzial der Attacken. Besonders gefährlich sind gezielte Angriffe auf einzelne Organisationen – und der Zeitaufwand, sie aufzudecken, ist extrem hoch.

Mit einem SOC kann ein Unternehmen seinen Sicherheitsstatus erhöhen und die Erkennung (Detection) sowie die Gegenwehr (Response) im Fall von Incidents verbessern. Es herrscht heute allgemein Konsens darüber, dass ein funktionierendes SOC auf drei Säulen baut: Menschen, Richtlinien und Technik. Die Aufgabe, ein SOC mit vertretbaren Kosten aufzubauen und effektiv einzurichten, stellt viele Organisationen allerdings vor kaum lösbare Probleme.

Vectra nutzt KI dazu, die manuelle und zeitaufwändige Tier-1-Analyse von Security-Events zu automatisieren und reduziert so die Arbeit von Wochen oder gar Monaten auf wenige Minuten. Bis zu 90 Prozent des Zeitaufwands für Bedrohungsanalysen lassen sich einsparen, sodass sich die SOC-Teams auf die Prävention und Eindämmung von drohenden Datenverlusten konzentrieren können.

Dieses Whitepaper untersucht die Hindernisse, die Unternehmen überwinden müssen, wenn sie den Kampf gegen Bedrohungen aufnehmen. Es zeigt außerdem, in welchem Maße Security-Lösungen auf der Basis künstlicher Intelligenz (KI) zu einer unverzichtbaren Komponente moderner SOCs geworden sind. KI-gestützte Lösungen können SOC-Teams unterstützen, um deren Tätigkeit effizienter zu gestalten. Außerdem sind sie der Lage, bereits frühe Anzeichen eines Angriffs in Echtzeit zu erkennen – noch bevor wichtige Assets gestohlen oder geschädigt werden.

Die KI-gestützte Cybersecurity-Plattform von Vectra Networks kombiniert menschliche Fertigkeiten und aktuelle Ansätze der Bedrohungsforschung mit einer großen Bandbreite an Techniken für Data Science und modernes maschinelles Lernen, um auf dieser Basis eine rund um die Uhr aktive, automatisierte Bedrohungserkennung, -triage und -korrelation über komplette Organisations-Infrastrukturen hinweg zu ermöglichen.

Vectra reduziert die Zeitspanne und die Kosten für die Bedrohungserkennung, indem die Lösung die Erhebung von Daten, den eigentlichen Erkennungsvorgang, die Analyse und die Response-Funktionen automatisiert. Sie stellt SOC-Teams belastbare Informationen zur Verfügung – die Grundlage dafür, Angriffe binnen kürzester Frist zu stoppen.

Vectra nutzt KI dazu, die manuelle und zeitaufwändige Tier-1-Analyse von Security-Events zu automatisieren und reduziert so die Arbeit von Wochen oder gar Monaten auf wenige Minuten. Bis zu 90 Prozent des Zeitaufwands für Bedrohungsanalysen lassen sich einsparen, sodass sich die SOC-Teams auf die Prävention und Eindämmung von drohenden Datenverlusten konzentrieren können.

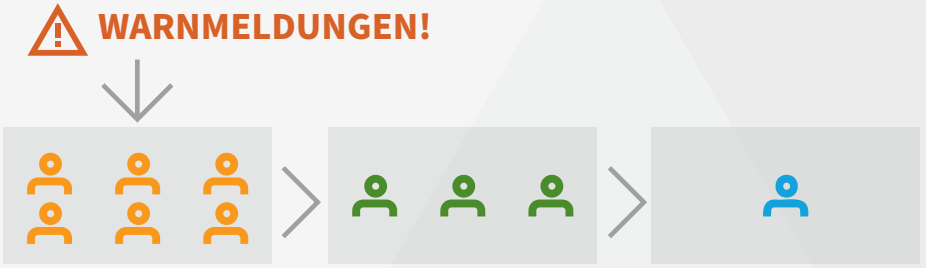
Hindernisse beim SOC-Aufbau

Beim Aufbau eines SOCs stoßen Unternehmen gewöhnlich auf gleich mehrere Hindernisse. Mit einigen dieser Herausforderungen befassen sich die folgenden Abschnitte dieses Whitepapers

Personalmangel

In ein SOC gehören gut ausgebildete, praxiserfahrene Abwehr-spezialisten aus dem Cybersecurity-Bereich. Unglücklicherweise übersteigt die Nachfrage nach bewährten Fachkräften dieser Art und für Data Science bei weitem das Angebot, das der Arbeitsmarkt hergibt. Deshalb ist es schwierig, talentierte Bewerber zu gewinnen und die besten ans Unternehmen zu binden. Nimmt man die USA als Beispiel, klafft derzeit eine Lücke von 40.000 unbesetzten Cybersecurity-Stellen pro Jahr.

Üblicherweise verlangt die Personalstruktur eines SOCs nach der Besetzung von Positionen auf mehreren Ebenen. Man benötigt Analysten der „Tiers“ 1-3, wobei mit jeder Ebene die Anforderungen an die Expertise steigen.



Tier 1
Überwachung und Triage

Tier-1-Analysten tragen die Verantwortung für eine permanente Überwachung der IT-Systeme und für die Triage eventueller Alarme. Vor dem Hintergrund der großen Datenmengen, die sie analysieren müssen, stellen sie die zahlenmäßig größte Gruppe im SOC. Viele Unternehmen beschäftigen zwei oder drei Spezialisten dieser Kategorie, nicht selten aber auch sechs oder mehr.

Tier 2
Eindämmung und Behebung

Kann das Tier-1-Team eine Bedrohung nicht neutralisieren, eska-liert es sie gewöhnlich an Tier-2-Analysten, deren Hauptaufgabe die Eingrenzung und Bereinigung solcher Fälle ist. Gelingt es auch den Tier-2-Spezialisten nicht, den Vorfall zu bewältigen, kommen die Top-Analysten der Tier-3-Stufe zum Zuge.

Tier 3
Forensik und Intelligence

Anders als ihre Tier-1-Kollegen arbeiten Tier-2- und Tier-3-Ana-lysten nicht rund um die Uhr. Sie sind aber 24 Stunden am Tag einsatzbereit und greifen ein, wenn es der Schweregrad eines Incidents und die geforderte Reaktionszeit notwendig machen.

Der Ernst einer Attacke kann von „kritisch“ – unmittelbare Gegen-wehr erfordernd – bis „gering“ reichen, wobei im letzten Fall auch Response-Zeiten akzeptabel sind, die mehrere Stunden oder einen ganzen Tag umfassen. Weil Tier-3-Analysten im Abwehrszenario die teuerste Mitarbeitergruppe darstellen, ist es wichtig, dass sie grundsätzlich die schwierigsten und mit den höchsten Risiken behafteten Fälle bearbeiten.

Je nachdem, welche Prozesse und Ressourcen einem Unter-nehmen zur Verfügung stehen, kann ein SOC mit einem dedizierten Response-Team ausgestattet sein oder auf unterschiedliche Ressourcen zurückgreifen, um kritische Incidents zu bewältigen. In der Praxis kann dies bedeuten, dass im Fall der Fälle ein internes Einsatz-Team gebildet oder externe Analysten und sonstige Fachkräfte aktiviert werden.

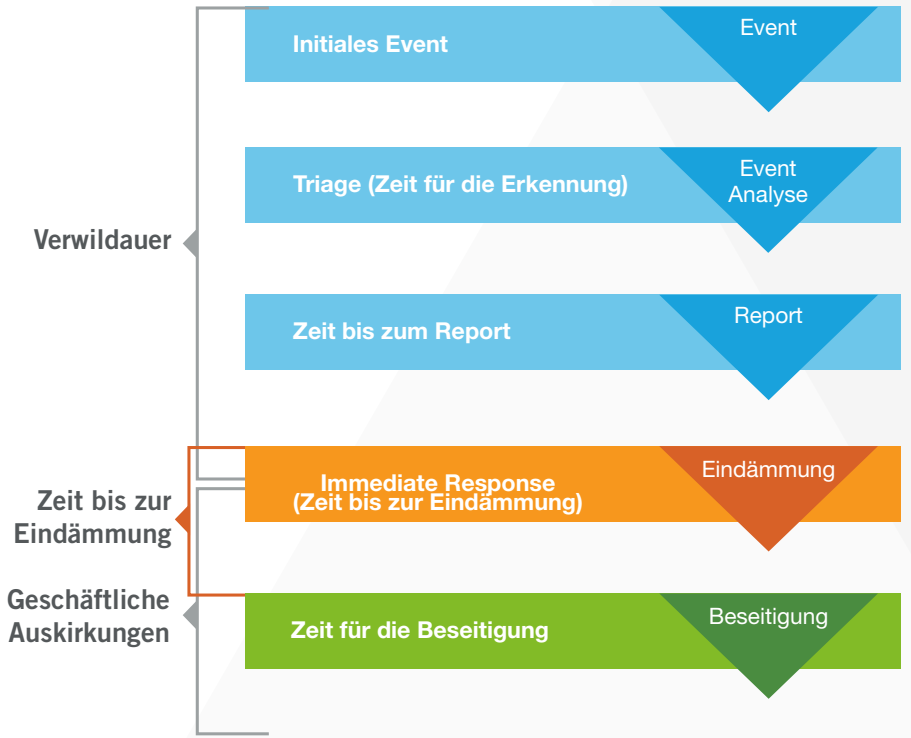
Organisationen, die freie Forensik-Spezialisten ins Team holen, um gegen groß angelegte Verletzungen der Informationssicherheit oder komplexe Bedrohungsfälle vorzugehen, geben dafür oft mehr als eine Million Dollar pro Incident aus.

Manuelle Prozesse

Ausgefuchste Angreifer haben sich längst darauf eingestellt, signaturgestützte Security-Mechanismen, Sandboxes und andere Techniken der Perimeter-Sicherheit zu überwinden. Schafft es ein Angreifer erst einmal, diese Hürden zu umgehen, wird die Aufdeckung seiner Aktivitäten zu einem Vorgang, der viel Handarbeit und Zeit erfordert.

Nachforschungen auf diesem Gebiet verlangen nach breit aufgestellten Fähigkeiten und zugleich nach Spezialkenntnissen. Sie umfassen die Gebiete der Malware-Analyse, der forensischen Untersuchung von Netzwerk-Paketen und Log-Dateien, und die Korrelation einer ungeheuren Datenmenge aus unterschiedlichsten Quellen. Die Untersuchung von sicherheitsrelevanten Events kann Stunden dauern, und die vollständige Analyse einer Bedrohung der aktuellen Generation verlangt eventuell nach tagelanger, wochenlanger oder sogar monatelanger Arbeit.

Zeit ist der wichtigste Faktor, wenn es um die Erkennung von Verletzungen der Netzwerksicherheit geht. Wer zentrale Assets vor Diebstahl oder Schäden schützen will, muss Angreifern in Echtzeit auf die Spur kommen.



Verweildauer + Zeit für die Eindämmungsaktivitäten = Dauer des unautorisierten Zugriffs auf ein Asset

KI ist eine der Schlüsseltechniken dafür, das große Volumen an Traffic in heutigen Netzwerken überwachen und analysieren zu können. Wenn man sie richtig einsetzt, können KI-gestützte Lösungen rund um die Uhr laufen und einen großen Teil der Arbeit eines Tier-1-Analysten automatisieren. Unternehmen müssen dann weniger und weniger teures SOC-Personal einstellen, während gleichzeitig die Zeitspanne bis zur Erkennung und Beseitigung einer Bedrohung signifikant sinkt.

Sicherheitstechnik für Experten

Historisch gesehen war es immer schwierig, Security-Produkten belastbare Cybersecurity-Informationen zu entlocken. Auch Spezialisten, die dafür gut ausgebildet waren, mussten dafür viel Zeit aufwenden.

Unternehmen benötigen deshalb neue Ansätze und Werkzeuge. Gefordert sind Systeme und Verfahren, die Netzwerke, Anwender und Applikationen kontinuierlich auf verdächtige Verhaltensweisen hin überwachen und automatisch die entscheidenden Daten für Security-Analysten zusammenstellen. Diese kritischen Informationen sollten aus einer umfassenden Auswahl an Quellen stammen – darunter die Netzwerk-Flow-Analyse, Log-Daten verschiedener Systeme, Instanzen des Endpoint-Enforcements, der Kontext des Identitäts- und Asset-Managements, die Bedrohungsanalyse und Security-Events.

KI ist eine der Schlüsseltechniken dafür, das große Volumen an Traffic in heutigen Netzwerken überwachen und analysieren zu können. Wenn man sie richtig einsetzt, können KI-gestützte Lösungen rund um die Uhr laufen und einen großen Teil der Arbeit eines Tier-1-Analysten automatisieren. Unternehmen müssen dann weniger und weniger teures SOC-Personal einstellen, während gleichzeitig die Zeitspanne bis zur Erkennung und Beseitigung einer Bedrohung signifikant sinkt.

Kennzahlen für die Effektivität eines SOCs

Der Reifegrad und die Effektivität sind zwei der wichtigsten Messgrößen für die Leistung eines SOCs. Der Reifegrad reflektiert, welches Niveau ein Unternehmen in Bezug auf seinen Ansatz zum Management von Cybersecurity-Risiken erreicht hat. Dazu gehören die Sensibilität für Risiken und Bedrohungen, die Wiederholbarkeit sinnvoller Maßnahmen und die Anpassungsfähigkeit an neue Bedrohungsszenarien.

Das National Institute of Standards and Technology (NIST) misst den Reifegrad anhand von „Implementierungsstufen“. Die niedrig-ste Stufe ist die der partiellen Implementierung, gekennzeichnet durch informelle, rein reaktive Response-Fähigkeiten. Die höchste erreichbare Stufe impliziert eine Implementierung mit hoher Anpassungsfähigkeit, die sich durch Agilität auszeichnet und dadurch, dass sie auf belastbaren Risiko-Abwägungen basiert.

Effektivität bemisst sich am besten anhand von Metriken aus der Praxis des Security-Betriebs und der Jagd auf Bedrohungen. Dazu gehören:

1. **Verweildauer der Angreifer** – Hier handelt es sich um die bedeutsamste einzelne Kennzahl. Sie hält fest, wie lange ein Angreifer im Netzwerk einer Organisation aktiv sein kann, und zwar von der Erstinfektion bis zur Entdeckung und zur Eindämmung der Attacke. Die Messgröße hat das tatsächliche Gefahrenpotenzial im Blick, das Verlangsamen der Angriffsschritte durch Gegenmaßnahmen, die Fähigkeit der Organisation zur Bedrohungsanalyse und ihre Kapazitäten auf dem Gebiet der Response.

2. **Transparenz des Netzwerkgeschehens** – Was gar nicht im Blickfeld ist, kann man auch nicht erkennen. SOC-Teams müssen das gesamte Netzwerkgeschehen beobachten können: aufs Internet gerichteten Traffic, internen Traffic, Managed Hosts, Unmanaged Hosts, persönliche Geräte, IoT-Devices, virtuelle Server und Cloud-Ressourcen.

3. **Lateral Movement** – Der Indikator „Lateral Movement“ verrät, wie einfach und frei sich ein Angreifer im Netz bewegen kann und wie viele Systeme kompromittiert sind.

4. **Zeit bis zur Gegenwehr (Response)** – Wieviel Zeit vergeht, bis ein SOC auf Security-Events reagiert? Die hier gemessene Zeitspanne umfasst alle Aktivitäten des Abwehr-Teams zur Erkennung, Triage und zum Reporting bis hin zur Eindämmung einer Bedrohung oder eines Incidents.

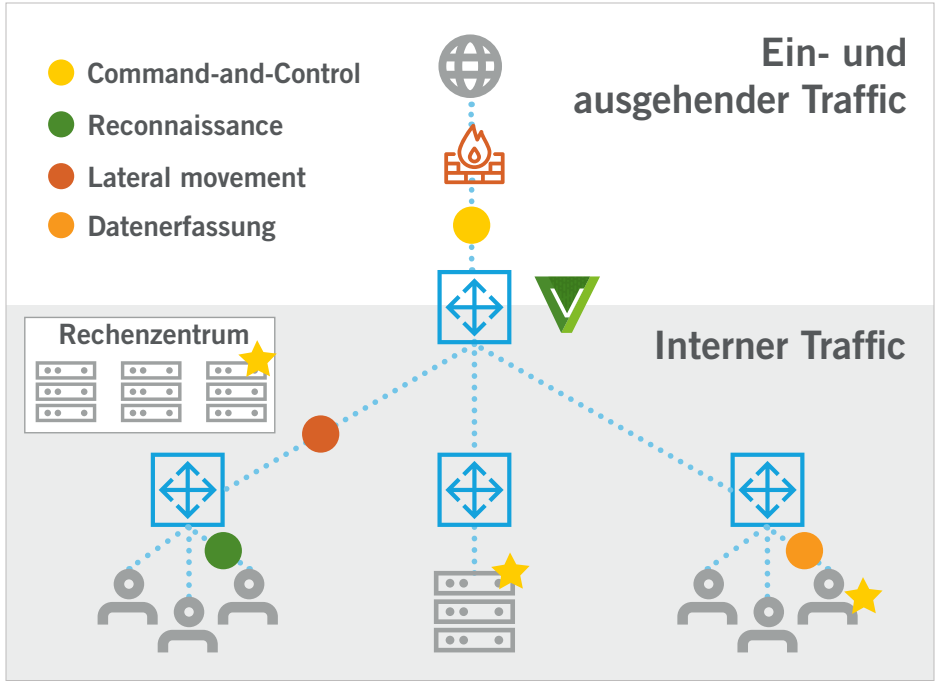
5. **Zahl wiederkehrender Infektionen** – Wie oft wurde Ihre Orga-nisation zum Ziel von Attacken und wie häufig musste sie wiederholte Kompromittierungen durch denselben Gegner oder dieselbe Bedrohung hinnehmen?

Data Science: Die Intelligenz hinter der Vectra-Plattform

Der Personalmangel auf dem Cybersecurity-Sektor, die lang-wierigen manuellen Prozesse und die Komplexität der Werkzeuge für Informationssicherheit stehen wirksamer Incident Response im Wege. Vectra adressiert diese Herausforderungen durch die Kombination menschlicher Expertise mit einem breit angelegten Arsenal an Data-Science-Techniken und Verfahren maschinellen Lernens für die Erkennung, das Reporting und die Triage von Bedrohungen – für jene Funktionen also, die normalerweise den Kern der Tätigkeit eines Tier-1-Analysten bilden.

Die automatisierte Jagd nach Bedrohungen und deren Erkennung bilden das zentrale Element der Cybersecurity-Plattform von Vectra. Unser Ansatz basiert auf einem einfachen Prinzip, versteckte Bedrohungen zu finden: KI, angesetzt auf die verlässlichste Datenquelle – den Netzwerk-Traffic.

Vectra bietet tiefgreifende, kontinuierliche Analyse des gesamten Netzwerk-Traffics und erkennt so jene grundlegenden Aktivitäten und Verhaltensweisen, auf die Cyber-Kriminelle



zwangsläufig zurückgreifen müssen, wenn sie im Netzwerk einer Organisation spionieren und sich dort ausbreiten, um zentrale Assets ausfindig zu machen und zu stehlen.

Um ganze Netzwerke abdecken zu können und die Vorgänge darin transparent zu machen, überwachen Vectra-Lösungen den gesamten Netzwerk-Traffic rund um die Uhr und analysieren ihn. Sie haben dabei den internen Traffic (Ost-West) genauso im Blick wie den aufs Internet gerichteten Verkehr (Nord-Süd). Auch interner Traffic zwischen physischen und virtuellen Hosts mit eigenen IP-Adressen ist inbegriffen.

Abdeckung und Transparenz erstrecken sich auf alle Geräte – Laptops, Server, Drucker, BYOD- und IoT-Devices, auf alle Betriebssysteme und Anwendungen sowie auf Traffic zwischen virtuellen Workloads im Rechenzentrum und der Public Cloud.

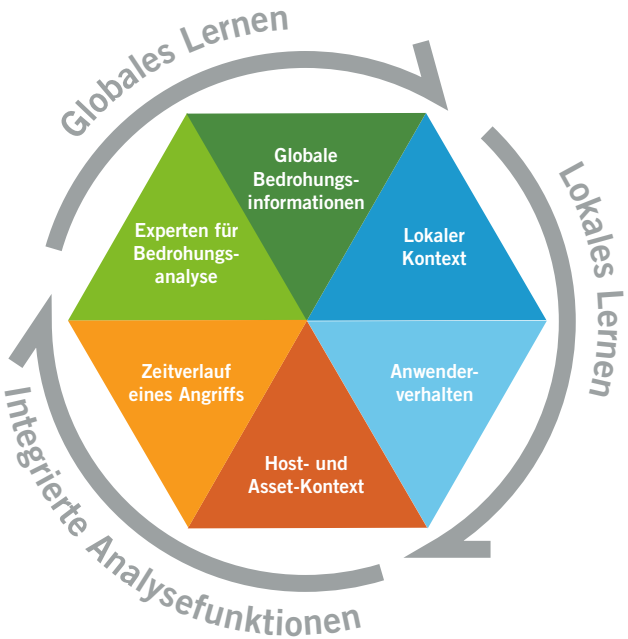
Darüber hinaus überwacht und erkennt Vectra auch verdächtige Zugriffe auf kritische Assets, die von autorisierten Mitarbeitern ausgehen, und Richtlinienverletzungen im Zusammenhang mit der Nutzung von Cloud-Speichern, USB-Speichern und anderen Methoden, die es erlauben, Daten aus dem Netzwerk heraus zu bewegen.

Vectra setzt kombinierte Analyse-Techniken dazu ein, automatisch alle Phasen einer Cyber-Attacke zu erkennen, darunter:

- Command-and-Control sowie andere Formen verborgener Kommunikation
- Internal Reconnaissance
- Lateral Movement
- Missbrauch von Zugangsdaten für Konten
- Exfiltration von Daten
- Frühe Indikatoren für Ransomware-Aktivitäten
- Botnet Monetization
- Angriffskampagnen, darunter das Mapping aller Hosts auf ihnen zugeordnete Angriffs-Indikatoren

Indem Vectra Algorithmen für Verhaltenserkennung dazu einsetzt, Metadaten festgehaltener Pakete zu analysieren, erkennt die Lösung versteckt operierende und unbekannte Angreifer in Echtzeit – unabhängig davon, ob der Traffic verschlüsselt ist oder nicht. Vectra untersucht ausschließlich die Metadaten, um die Privatsphäre der Anwender zu schützen. Ein Herumspionieren in sensiblen Nutzdaten ist unnötig.

Die folgenden Abschnitte werfen einen Blick auf die Technik der Cybersecurity-Plattform von Vectra, um nachvollziehbar zu machen, wie sie den Folgen der Personalknappheit entgegenwirkt und SOC-Prozesse rationalisiert.



Globales Lernen

Beim globalen Lernen geht es darum, die grundlegenden Eigenschaften zu identifizieren, die den Bedrohungen gemeinsam sind. Globales Lernen bei Vectra beginnt mit den Vectra Threat Labs, einer Gruppe von Cybersecurity-Experten und Bedrohungsanalysten, die ausschließlich und kontinuierlich Malware, Angriffswerkzeuge und -techniken analysieren. Sie erarbeiten außerdem geeignete Methoden, um neue und möglicherweise umwälzende Trends innerhalb der Bedrohungslandschaft zu identifizieren.

Ihre Ergebnisse fließen in die Data-Science-Modelle der Cybersecurity- Plattform von Vectra ein, zu denen unter anderem überwachtes maschinelles Lernen gehört. Dieses Verfahren dient dazu, große Mengen an schädlichem und mit Angriffen einhergehendem Traffic zu analysieren und daraus jene zentralen Eigenschaften abzuleiten, die für bösartigen Traffic charakteristisch sind.

Überwachtes maschinelles Lernen lässt sich beispielsweise daraufhin auslegen, die Identifizierung der speziellen Verhaltensweisen von Remote-Access-Tools (RATs) zu ermöglichen. Dazu lernen die Systeme, wie sich der Traffic solcher Angriffswerkzeuge von normalem Traffic unterscheidet. Vectra verschafft sich auf diese Weise die Fähigkeit, verlässlich und in Echtzeit auch neue, für einen konkreten Angriff maßgeschneiderte und noch unbekannte RATs zu erkennen, ohne dabei auf Signaturen zurückzugreifen.

Lokales Lernen

Mit lokalem Lernen lässt sich herausfinden, welche Vorgänge in einem lokalen Netzwerk normal sind und welche nicht, damit Angriffsmuster sichtbar werden. Die Kerntechniken dazu sind unüberwachtes maschinelles Lernen und Anomalie-Erkennung.

Vectra setzt Verfahren unüberwachten maschinellen Lernens dazu ein, Vorgänge in einer spezifischen Kundenumgebung zu verstehen, ohne dass ein Data Scientist den Lernvorgang direkt überwacht. Vectra erkennt auf dieser Basis zum Beispiel, wenn sich ein Anwender unversehens anders verhält als zuvor.

Statt sich lediglich darauf zu konzentrieren, Anomalien aufzudecken und zu melden, sucht Vectra allerdings gezielt nach Indikatoren für wichtige Phasen einer typischen Attacke oder nach Angriffstechniken wie der Erkundung eines Netzwerks, der Überprüfung von Hosts auf ihren Nutzen für einen Angriff und nach dem Einsatz gestohlener Anmeldedaten.

Um diese Vorgehensweisen zu erkennen, ist zunächst eine Art Langzeitgedächtnis für alle Parameter einer lokalen Netzwerkum-gebung vonnöten, darunter die längerfristig immer wieder ge-nutzten Netzwerkadressen. Die voranschreitende Sammlung und Bereitstellung von Daten lässt sich ebenfalls beobachten. Dazu allerdings muss die Langzeiterfassung von Vorgängen mit intelligenten Analysefähigkeiten kombiniert werden, damit Kontextverständnis entsteht und vor seinem Hintergrund sichtbar wird, dass immer wieder ähnliche Mengen von Informationen zu unterschiedlichen Zeiten zunächst gesammelt und dann aus der Netzwerkumgebung heraustransferiert (exfiltriert) werden.

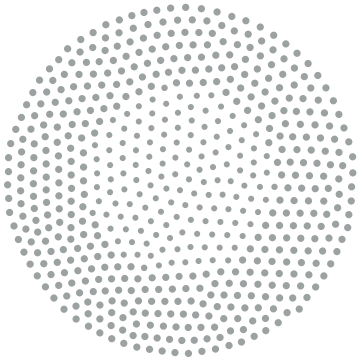
Unüberwachtes Lernen und damit verbundene Verfahren stellen mächtige Mechanismen der Security-Analyse dar. Vectra nutzt sie, um verdächtige Aktivitäten in Echtzeit aufzudecken – darun-ter den Diebstahl gültiger Anmeldedaten von einem bereits kompromittierten Host.

Integrierte Analysefunktionen

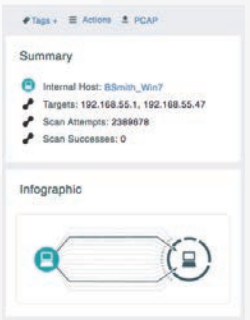
Heutige Cyber-Attacken sind komplexe, mehrstufige Operationen, die sich stetig weiterentwickeln und eine große Bandbreite an unterschiedlichen Methoden und Strategien aufbieten. Den Angreifern gelingt es damit, sich immer tiefer in die Netzwerke vorzuarbeiten.

Dies hat zur Folge, dass die Verfahren zur Angriffserkennung unbedingt mir der notwendigen analytischen Intelligenz ausgestattet werden müssen, alle verfügbaren Informationen zur Identifizierung einer größer angelegten Attacke heranzuziehen und

Erkennung: Ein einzelner erkannter Vorfall stützt sich auf Hunderte bis Tausende analysierter und zusammengefasster Events und Netzwerk-Daten



Report: Analysten benötigen für ihre Entscheidungen und Empfehlungen zum weiteren Vorgehen eine hinreichende Informationsbasis



Triage: Auffälligkeiten werden automatisch korreliert, um physische Hosts im Zentrum einer Attacke exakt zu lokalisieren

SOC

- SIEM
- Incident Response

Vectra integriert sich mit Lösungen für die Durchsetzung von Sicherheitsmaßnahmen (Enforcement Points) und mit Incident-Response-Plattformen

- Firewall
- Endpoint
- NAC

nicht nur die offensichtlich zusammengehörigen Event-Komponenten. Außerdem müssen die Lösungen die Vorgänge auch im Zeitverlauf verfolgen können.

Vectra zieht für einen einzigen konkreten Hinweis auf einen Angriff Tausende von Events und Daten zum Netzwerkstatus heran. Verfahren wie die Event-Korrelation und das Scoring von Host-Daten dienen als Basis folgender Aktivitäten:

- Korrelieren aller erkannten Events mit genau jenen Hosts, die Zeichen bedrohungstypischen Verhaltens zeigen.
- Automatisches Scoring jeder erkannten Auffälligkeit und jedes Hosts in Bezug auf die Ernsthaftigkeit einer Bedrohung und in Bezug auf die Wahrscheinlichkeit, mit der sie tatsächlich vorliegt. Hierzu dient der Vectra Threat Certainty Index als Grundlage.
- Verfolgung jedes Events im Zeitverlauf und über alle Phasen der „Kill-Chain“ einer Cyber-Attacke hinweg.

Vectra rückt speziell jene Events in den Fokus, die zentrale Assets im Netzwerk gefährden können oder die für einen Angreifer von strategischem Wert sind. Priorisiert werden außerdem Geräte, an denen sich Verhaltensweisen zeigen, die für gleich mehrere Phasen einer Cyber-Attacke bedeutsam sind.

Das Resultat dieser Vorgehensweise ist, dass Kunden unverzüglich einen genauen Überblick über jene Angriffsaktivitäten und jene Hosts im Netzwerk gewinnen, die mit dem höchsten Grad an Wahrscheinlichkeit die höchsten Risiken bergen.

Die Vorteile des Vectra-Ansatzes

Vectra kombiniert menschliches Expertenwissen mit einer ganzen Reihe von KI-Techniken und automatisiert so die manuelle, zeit-aufwändige Tier-1-Analyse von Security-Events. Daraus ergeben sich für Kunden gleich mehrere Vorteile.

Unterstützung für SOC-Teams durch Automatisierung der Tier-1-Analyse

Vectra automatisiert Security-Nachforschungen, die normalerweise Stunden manueller Anstrengungen bestens ausgebildeter Security-Analysten und Data-Scientists erfordern. Aufgaben im Bereich der Erkennung, des Reportings und der Triage, die typischerweise von Tier-1-Analysten ausgeführt werden, laufen komplett automatisch ab, sodass SOC-Teams effizienter und produktiver arbeiten.

Um ein Beispiel zu nennen: Hat Vectra einen verdächtigen Vorfall erkannt, zeigt das System die Informationen darüber mittels einer eingängig und einfach gestalteten „Dashboard“-Oberfläche an und priorisiert dabei jene kompromittierten Hosts, die das höchste Risiko bergen, Änderungen der Host-Scores für Risiko und Ein-trittswahrscheinlichkeit und zentrale Assets, die möglicherweise betroffen sind. Die erwähnten Scores lösen außerdem gege-benenfalls Meldungen ans SOC-Personal aus.

Diese kompakten, auf jeweils einer Seite zusammengefassten Mitteilungen erläutern jeden erkannten Vorfall. Sie verweisen auf die zugrundeliegenden Events und den historischen Kontext, die zu seiner Aufdeckung geführt haben, und auf mögliche Auslöser, Ursachen, die Auswirkungen auf den Geschäftsbetrieb sowie auf Maßnahmen, mit denen sich der Vorfall verifizieren lässt.

Die SOC-Teams haben das Voranschreiten der Bedrohung im zeitlichen Ablauf vor Augen und können sich deshalb sofort auf dieGegenwehr konzentrieren, statt wertvolle Zeit mit der Bestimmung des Schweregrads und der Priorität einer Attacke zu verlieren.

Vectra alarmiert das SOC-Team auch dann, wenn Datentransfers nicht konform zu etablierter Praxis ablaufen oder Regeln verletzen. Die Lösung liefert außerdem Informationen über den Host, der die Daten überträgt, und zeigt, welches Ziel sie nehmen, um welchen Umfang es geht und welche Techniken zum Transfer genutzt werden.

Darüber hinaus können SOC-Teams auf einfache Weise verfolgen, in welchem Maße frühere Infektionen erneut auftreten. Dazu stellen sie ein „Dashboard“ zusammen, das anzeigt, wenn Hosts von derselben Malware mehrfach angegriffen werden oder wenn sie wiederholt eine als bösartig eingestufte Site kontaktieren.

Die Reichhaltigkeit der Informationen, die die Vectra-Plattform bietet, macht sie zu einem unerlässlichen Trainings-Werkzeug, das Mitglieder des SOC-Teams darüber instruiert, welche Vorgänge im Netz sie als normal betrachten können und wie sich tatsächliche Angriffe entfalten und voranschreiten.

Auslösende Faktoren

- Ein interner Host kommuniziert mit einer IP-Adresse im Internet per HTTPS, während ein anderes Protokoll innerhalb der HTTPS-Sitzungen aktiv ist
- Dies bedeutet, dass ein versteckter Tunnel existiert, in dem mehrere Sitzungen über einen längeren Zeitraum hinweg stattfinden und sich dabei als normaler, verschlüsselter Web-Traffic tarnen
- Die Bedrohungs-Einstufung (der Score) des Vorfalls errechnet sich aus der Menge der durch den Tunnel transferierten Daten und die Dauer der Sitzungen
- Der Score zur Eintrittswahrscheinlichkeit (Certainty Score) errechnet sich aus der Zahl und Beständigkeit der Sitzungen

Vielen Kunden eröffnen der Automatisierungsgrad und die Benutzerfreundlichkeit der Vectra-Systeme eine Chance, in höherem Maße Security-Generalisten wie etwa Werksstudenten zu beschäftigen oder erfahrene Security-Analysten primär auf gehobenen Positionen einzusetzen, für die kaum Nachwuchs zur Verfügung steht.

So notierte beispielsweise der CISO einer Organisation aus dem Gesundheitswesen: „Bei uns beschäftigte Praktikanten haben einen hervorragenden Job gemacht, weil ihnen Vectra zur Verfügung stand“. Die Arbeitslast für das übrige SOC-Team sank dabei um 75 Prozent.

Das Texas A&M University System ging unmittelbar nach der Implementierung von Vectra daran, College-Praktikanten mit dem Schutz ihrer hochwertigen wissenschaftlichen Informationen und Forschungsdaten zu betrauen. Studenten, die an einer Cybersecurity-Karriere interessiert sind, erlernen die Arbeit als Tier-1-Analysten im SOC und in diesem Zusammenhang den Einsatz von Vectra.

„Die Vectra-Lösung ist so intuitiv und benutzerfreundlich gestaltet, dass selbst Praktikanten in Minuten entscheiden können, ob sie sich direkt mit einer erkannten Bedrohung befassen sollten oder ob es sinnvoller ist, sie für intensivere Untersuchungen an einen Tier-2-Analysten weiterzureichen“, erklärt Daniel Basile, Executive Director of SOC bei Texas A&M. „Bei uns können die Mitarbeiter, die als Tier-1-Analysten tätig waren, deshalb jetzt als Tier-2-Ana-lysten arbeiten. Das ist der Punkt, wo Vectra wirklich glänzt.“

Mehr Bedrohungen erkannt, Eindämmung schneller erreicht

Vectra bietet Echtzeit-Einblicke in Angriffsvorgänge und verfolgt Bedrohungen permanent und automatisch. Das System stützt sich dabei auf Verhaltensmodelle, die sich durch maschinelles Lernen stetig weiterentwickeln. Mithilfe dieser Funktionen können SOCs die Verweildauer der Cyberkriminellen in den Netzen verkürzen und schneller mit Response-Maßnahmen reagieren. So kann es SOC-Teams gelingen, den höchsten NIST-Level in Sachen Reifegrad der Implementierung zu erreichen.

Vectra reduziert dramatisch die Zeit, die für die Untersuchung von Bedrohungen aufgewendet werden muss. Security-Teams können sich deshalb auf Data Loss Prevention und die Schadensein-grenzung konzentrieren. Einigen Kunden ist es gelungen, den Zeitaufwand für Nachforschungen um nicht weniger als 90 Prozent.zu verringern. Das SOC-Team bei Texas A&M beispielsweise schaffte es, diesen Zeitbedarf von Tagen auf Minuten zu drücken.

Darüber hinaus entdeckte Vectra Security-Events, die sonst im Verborgenen geblieben wären. Dies führte zu einer Nettozunahme der Zahl der Events und damit zu präziseren und rechtzeitigen Incident-Response-Maßnahmen.

Im ersten Jahr des Vectra-Einsatzes fand Texas A&M sieben aktive Bedrohungen im eigenen Netzwerk. Die Lösung stellte dem SOC-Team alle Informationen zur Verfügung, die es benötigte, um schnell gegen jede Bedrohung vorzugehen und kritische Assets zu schützen.

Die Kosten reduzieren

Wenn ein Angriff stattgefunden hat, sind oft teure Incident-Response-Maßnahmen vonnöten und Dienstleistungen für die forensische Analyse. Vectra hilft Organisationen, die Kosten für extern vergebene Nachforschungen komplett zu vermeiden. Gleichzeitig verringert die Lösung die Abhängigkeit von manueller Log-Analyse.

Vectra hat Texas A&M erhebliche Einsparungen ermöglicht. Mit Vectra „fand unser Security-Operations-Team die Angreifer in kurzer Zeit und so früh, dass wir keine teuren Analysten für die nachträgliche Forensik beauftragen mussten, wie sie typischerweise in die Organisation geholt werden, wenn der Schaden bereits einen Monat zurückliegt“, berichtet Basile.

„Sie haben es mit Kosten von ungefähr einer Million Dollar zu tun, die jedes Mal anfallen, wenn Sie im Anschluss an eine Verletzung der Informationssicherheit spezialisierte Forensiker ins Boot holen“, ergänzt er. „Weil Vectra dies unnötig gemacht hat, konnte uns das System in einem Jahr Ausgaben in Höhe von 7 Millionen Dollar ersparen.“

Die Effizienz steigern

Vectra stellt eine ganze Reihe von Kommunikations-Verfahren und automatisierte Response-Mechanismen zur Verfügung, die ein besseres Erkennen und Einschätzen der Situation ermöglichen, den Austausch von Informationen fördern und Unterstützung fürs Incident-Response-Management bieten, sodass SOC-Prozesse effizienter ablaufen. Folgende Funktionen sind enthalten:

- Echtzeit-Alarme per E-Mail, Syslog oder mithilfe anderer Tools, die sich über REST-APIs integrieren lassen.
- Ein vorkorrelierter Ausgangspunkt für Security-Nachforschungen innerhalb von Security-Information-and-Event-Management-Systemen (SIEM) und für den Einsatz forensischer Werkzeuge.
- Unterstützung der SOC-Teams bei der Weiterleitung von Informationen – auf Abruf oder gemäß einem vorgegebenen Zeitplan mithilfe der Reporting-Engine, die sich kundenspezifisch anpassen lässt.
- Abarbeitung dynamischer Response-Regeln und automatisches Anstoßen von Response-Maßnahmen mittels anderer Security-Enforcement-Lösungen.
  - Vectra integriert sich mit der Identity Services Engine (ISE) von Cisco, um einen Host unverzüglich isolieren oder in Quarantäne schicken zu können.
  - Vectra arbeitet mit Carbon Black zusammen, um ein Host-Gerät im Falle einer erkannten Bedrohung schnell zu isolieren oder in Quarantäne zu schicken sowie schädliche Prozesse zu stoppen.
  - Vectra integriert sich mit Next-Generation-Firewalls von Palo Alto Networks, Cisco und Juniper Networks, um ein kompromittiertes Host-Gerät blockieren zu können.
  - Vectra arbeitet mit SIEM-Systemen wie Splunk, HPE ArcSight und IBM QRadar zusammen, um Arbeitsabläufe im Security-Operations-Bereich zu automatisieren.

„Seit wir Vectra einsetzen, kann unser Team die gesamte Texas-A&M-Netzwerkinfrastruktur auf Cyber-Angriffe hin überwachen und das Security Operations Center mit unglaublicher Effizienz betreiben, obwohl wir nur über einen extrem kleinen Stab verfügen“, merkt Basile an.

KI ins SOC integrieren

Der Kampf gegen Cyber-Bedrohungen wird auch weiterhin eine der größeren Herausforderungen bleiben, denen sich große und kleine Unternehmen stellen müssen. Hier zu bestehen, erfordert KI-gestützte Lösungen, die das SOC automatisieren. Die Data-Science-Verfahren hinter der Vectra-Lösung repräsentieren eine beispiellose Innovation auf dem Sektor der Erkennungsmethodik.

Mit seinen Funktionen für kontinuierliches, ununterbrochenes Monitoring des Netzwerk-Traffics und mit dem Einsatz von KI für die Bedrohungserkennung, die Triage und das Incident Reporting bringt Vectra automatisch Bedrohungen im gesamten Unternehmensnetzwerk zur Strecke – eingeschlossen externe Büros, komplette Niederlassungen, Rechenzentren und Systeme in der Cloud.

Das Ergebnis ist, dass Anwender des Systems Security-Incidents schneller bewältigen können und keine zusätzlichen Cybersecurity-Spezialisten einstellen müssen. Tier-1-Analysten, die bereits zum Team gehören, können sich auf Data Loss Prevention und die Schadensbegrenzung konzentrieren.

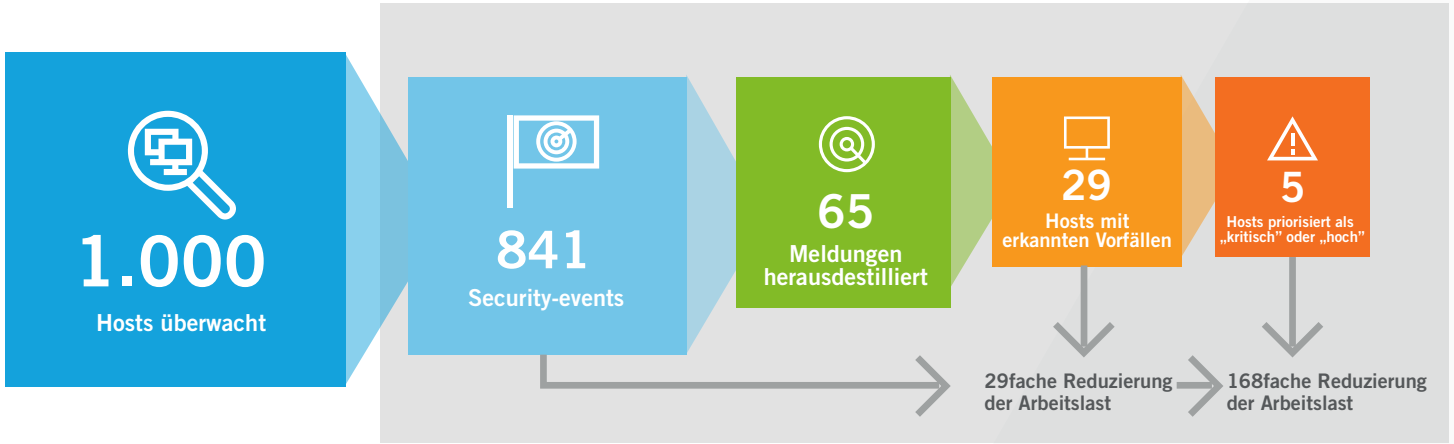
Vectra arbeitet permanent daran, die Leistung seiner Plattform zu verbessern. Kunden übermitteln dazu auf freiwilliger Basis Metadaten, sodass den Vectra Threat Labs eine kontinuierliche Feedback-Schleife zur Verfügung steht. So lassen sich die Algorithmen für die Angriffserkennung in kurzen Abständen weiterentwickeln und die existierenden Algorithmen in der lokalen Umgebung des Kunden optimieren.

Als ein weiteres Resultat der Auswertung von Metadaten aus Kundennetzen gibt Vectra quartalsweise Benchmark-Reports heraus. Diese geben erstens die Spielarten des Angriffsverhaltens wieder, die innerhalb von Organisationen registriert werden, und vermitteln zweitens ein Verständnis für die tatsächliche Reduktion der Arbeitslast, die durch den Einsatz der KI als Assistenz für die menschlichen Analysten konkret erreicht werden kann.

Unsere Benchmark-Reports stützen sich auf eine normalisierende Analyse. Sie spiegelt die erhobenen Daten zur Reduzierung der Arbeitslast auf ein Netzwerk mit 1000 Hosts, um der Tatsache gerecht zu werden, dass die Informationen von Installationen unterschiedlicher Größe stammen. Die Normalisierung erleichtert es, die Verbreitung von Bedrohungen in einem Netzwerk auf einer „Pro-Kopf"-Basis zu vergleichen. Als Host gilt hierbei jedes Gerät, das eine IP-Adresse aufweist, darunter virtuelle Workloads, Server, IoT-Geräte, Smartphones, Tablets und Laptops.

Die Vectra-KI reduziert die Arbeitslast für die Untersuchung von Bedrohungen auf der Seite der Security-Analysten um den Faktor 29, wenn man als Vergleichsmaßstab den manuellen Analyse-Aufwand für alle Security-Events und alle Indikatoren für kompromittierte Host-Devices heranzieht. Nimmt man die Fähigkeit der Vectra-KI hinzu, Hosts zu priorisieren, deren Risiko-Level als „kritisch" oder „hoch" eingestuft wird, steigt die Reduktion der Arbeitslast menschlicher Analysten durch die KI-Assistenz auf einen noch höheren Faktor von 168.

So sind es am Ende zwei Faktoren, die Vectra zu einem willkom-menen Werkzeug für den Aufbau effizienter und zugleich kosten-günstig zu betreibender Security Operations Center machen: Die Lösung entlastet die Security-Teams in signifikantem Maße von zeitaufwendigen Analysen, und sie unterstützt sie tatkräftig dabei, Angreifer schnell zu enttarnen und dann zu stoppen.



Für weitere Informationen wenden Sie sich bitte an einen Servicemitarbeiter unter info@vectra.ai.

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