Factsheet

Security Intelligence mit Vectra

DATA CENTER SOLUTIONS

DC-CONSULTING | DC-ENGINEERING | DC-MANAGEMENT

Neu definierte Sicherheit

Cyberangriffe stellen für Unternehmen jeder Grösse und in jeder Branche inzwischen einen Teil des Alltags dar. In den Nachrichten liest man beinahe täglich über einen weiteren, schweren Fall des Datendiebstahls, bei dem Kreditkartennummern oder andere persönliche Informationen gestohlen wurden oder eine Reportage über die Schattenwelt der Cyberkriminellen.

So gut wie alle Organisationen haben infizierte Hosts innerhalb ihrer Netzwerke. Am Netzwerkperimeter bereitgestellte, präventionszentrierte Sicherheitslösungen bieten eine nur unvollständige Lösung, um einen Angriff aufzuhalten. Haben sich Angreifer erst einmal Zugriff zum Netzwerk verschafft, können sie ihre Ausbeutung dort ganz ungehindert ausserhalb des Überwachungsbereichs der Perimeterlösung durchführen.

Der Schaden am Ruf und Namen eines Unternehmens oder der Verlust des geistigen Eigentums oder der Geschäftsgeheimnisse einer Organisation kann verheerende Auswirkungen haben.

Alle Entdeckungen werden automatisch ausgewertet, korreliert und die grössten Bedrohungen schnell priorisiert, so dass Sie den Angriff stoppen und seine Auswirkungen eindämmen können.

Die Vectra X-Serien-Plattform bietet als erstes System ein neues Niveau der Intelligenz und Automatisierung und kann einen Cyberangriff während der Durchführung erkennen und die Handlungen des Angreifers verfolgen. Die Technologie prägt sich die typischen Muster des Netzwerkverkehrs sowie unterschiedliche beobachtete Verhaltensweisen ein und erkennt so über Stunden, Tage und Wochen beobachtetes anomales Verhalten.

Die Zeit ist reif für ein intelligentes Sicherheitssystem, das mitdenkt

Die Implementierung von automatisierten Funktionalitäten zur Angriffserkennung und -berichterstattung in Echtzeit, die vielfältige Möglichkeiten bieten, einen Angriff aufzuhalten, hat bei Sicherheitsexperten heute oberste Priorität. Sicherheitstechnologien müssen in der Lage sein, Daten ununterbrochen zu beobachten, zu verarbeiten, aufzurufen und automatisch zu analysieren, um so den nächsten Schritt des Angreifers antizipieren zu können.

Die Vectra-Technologie setzt dort an, wo Perimetersicherheit aufhört. Die Bereitstellung einer gründlichen, kontinuierlichen Analyse des internen sowie des Internet-Netzwerkverkehrs ermöglicht die automatische Erkennung aller Phasen eines unbefugten Zugriffs, beim Versuch der Spionage, des Datendiebstahls und der Ausbreitung eines Angreifers in Ihrem Netzwerk.

Durch die Kombination aus Methoden der Data Science, maschinellen Lernverfahren sowie der Verhaltensanalyse erkennt Vectra proaktiv die Anwesenheit bekannter und unbekannter Bedrohungen und erfordert dabei keine Signaturen oder komplizierte Konfiguration.

Eine Lösung – zahlreiche Vorteile

- ✓ Entdeckung von Angriffen unabhängig der Methode und dem Ort des ursprünglichen Eindringens
- ✓ Bedrohungsmeldung über mehrere Phasen eines komplexen, zielgerichteten Angriffs
- ✓ Entdeckung von Bedrohungen ohne Signaturen mithilfe einer Kombination aus Data Science und maschinellem Lernen
- ✓ Einfach zu implementieren
- ✓ Identifiziert Angriffe auf allen Betriebssystemen, Anwendungen, Geräten und Browsern
- ✓ Intuitives, adaptives Reporting
- ✓ Erkennung und Berichterstattung in Echtzeit
- ✓ Erlernt die typischen Muster und Verhaltensweisen automatisch

Kompromisslose, visuelle Klarheit von laufenden Cyber-Attacken in Echtzeit

Vectra beobachtet, erlernt und merkt sich Verhaltensweisen mit der Zeit

Vectra überwacht ständig anstatt nur gelegentlich Scans durchzuführen und weiss daher, wann ein Angriff beginnt, sich ändert oder sich zurückzieht. Und weil es innerhalb der Netzwerkperimeter bereitgestellt wird, kann Vectra den Fluss des Benutzerdatenverkehrs vom und zum Internet sowie von und zum Rechenzentrum überwachen, um anomales Verhalten zu identifizieren. Vectra identifiziert Angriffe auf allen Betriebssystemen, Anwendungen, Geräten und Browsern. Vectra erlernt die typischen Muster und Verhaltensweisen im Netzwerkverkehr und erkennt über Stunden, Tage und Wochen beobachtetes anomales Verhalten. Ein Notebook, das E-Mails verschickt, ist nicht auffällig, aber wenn das E-Mail-Aufkommen plötzlich stark ansteigt oder das Notebook das Innere des Netzwerkes ausspioniert, kann dies auf ein grösseres Problem hinweisen.

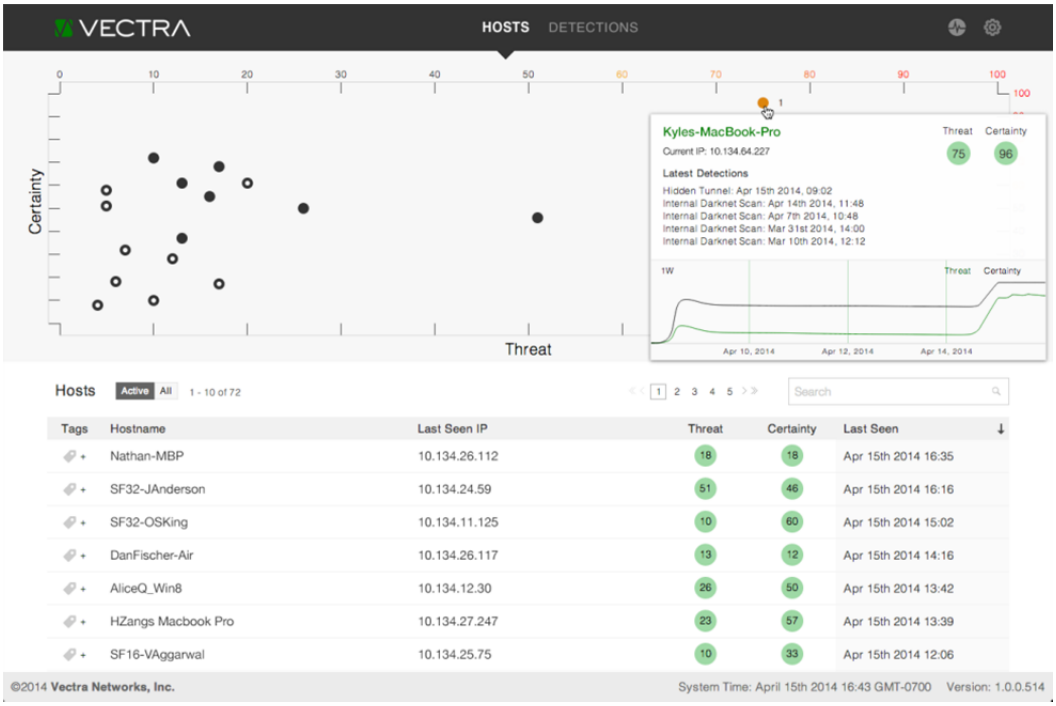
Priorisierte Bedrohungserkennung

Der innovative Vectra Threat Certainty Index zeigt grössere Bedrohungen in Echtzeit automatisch an, basierend auf einem kontextuellen Scoring-Prozess. Vectra überwacht, erlernt und merkt sich Verhaltensweisen und erkennt dabei bestimmte Verhaltensprozesse, die sich im Laufe der Zeit wiederholen. Vectra destilliert davon die wichtigsten Verhaltensweisen und analysiert diese über Tage, Wochen oder sogar Monate hinweg.

Vectra verfügt über einen längerfristigen Speicher als andere Echtzeit-Produktlösungen der neuesten Generation und kann daher einen Angriff in Kontext setzen und das Risiko für das Unternehmen besser einschätzen. Administratoren müssen keine Gigabytes an Log-Dateien durchforsten oder Analysetools für grosse Datenmengen benutzen, um festzustellen, ob eine Bedrohung real ist.

Aufschlussreiches Reporting in Echtzeit

Vectra bietet kompromisslose, visuelle Klarheit. Sicherheitsadministratoren können die Details einer Bedrohung im Drilldown-Verfahren ganz genau analysieren, einschliesslich der Paket-Erfassungen, die die Identifikation des Verhaltens ermöglichen. Die Berichterstattung von Vectra kann das sukzessive Fortschreiten einer Bedrohung dokumentieren.



Eine Rundumlösung

Moderne Netzwerke und das «Internet der Dinge» umfassen oft eine verwirrende Anzahl von Geräten, Betriebssystemen und Anwendungen und es ist praktisch unmöglich, dass Signaturen, Sandboxen, Host-Detailansichten und Endpoint-Agenten diese alle unterstützen. Durch die Anwendung von Methoden der Data Science kann Vectra im Netzwerk beobachtete Verhaltensweisen und Muster des Datenverkehrs analysieren und Bedrohungen auf der gesamten, äusserst variablen Angriffsfläche erkennen.

Sofort einsatzbereit

Vectra-Plattformen werden im passiven Modus eingesetzt und sind in unterschiedlichen Bauformen erhältlich. Die Plattformen der All-in-One-X-Serie eignen sich für grosse Netzwerkinfrastrukturen und werden häufig in der Nähe der zentralen Netzwerk-Switche oder WAN-Gateways eingesetzt, wo sie den gesamten Benutzerdatenverkehr zum Internet und zu Ihrem Rechenzentrum überwachen können.
Die Sensoren der S-Serie arbeiten in Verbindung mit einer X-Serien-Plattform und bieten so eine erweiterte Abdeckung zur Überwachung des Datenverkehrs von Access Layer-Switchen oder Remote-Arbeitsplätzen.

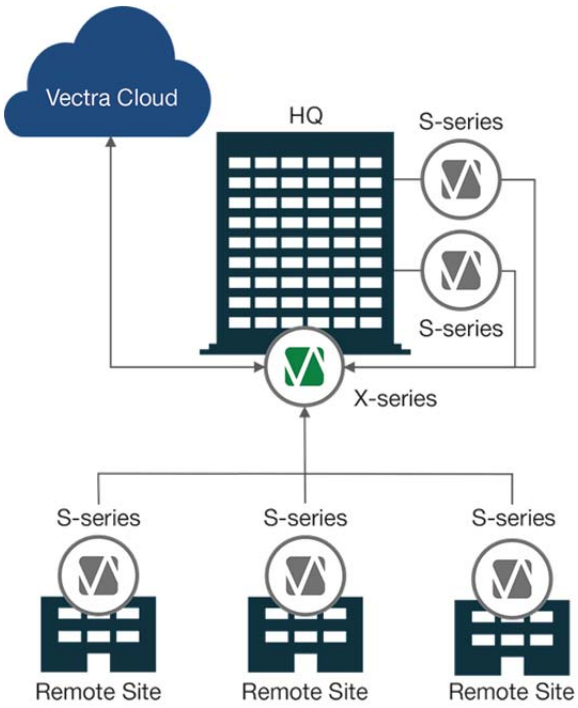
Die Implementierung beider Vectra-Lösungen ist sehr einfach und voll automatisiert. Konfigurieren Sie einfach die Management-IP-Adresse und die Plattform erlernt alle weiteren benötigten Details von selbst.

Immer auf dem neusten Stand

Vectra erledigt alle komplexen, sicherheitsbezogenen Arbeiten und entlastet durch seine Sicherheitsüberwachung in Echtzeit die Netzwerkverwaltung. Administratoren müssen keine detaillierte, zeitaufwendige Konfiguration durchführen oder Wochen mit dem Tuning der Plattform verbringen. Wenn die Vectra-Plattform an das Netzwerk angeschlossen ist, erlernt sie automatisch alles, was sie wissen muss und erstellt Modelle normaler Verhaltensweisen der mit dem Netzwerk verbundenen Geräte. Vectra wird automatisch über einen Cloud-Service aktualisiert, damit der Schutz auf dem neuesten Stand ist.

Skalierbare, verteilte Architektur

Die skalierbare, verteilte Architektur von Vectra Networks ermöglicht Kunden die uneingeschränkte Einsicht in ihr Netzwerk und zwar unabhängig von der Grösse und der geografischen Verteilung ihres Unternehmens. Die Sensoren der S-Serie und die X-Serien-Plattformen können auf Netzwerke jeder beliebigen Grösse und über unterschiedliche Standorte hinweg skaliert.



Das Vectra-Portfolio

Die X-Serie Plattform

Die Software der X-Serie-Plattform ist auf einem rackmontierbaren Gerät erhältlich, das selbst auf die grössten Netzwerke skaliert werden kann. Die X-Serie-Plattform kann daher entweder als All-in-One-Gerät zur Überwachung von Datenverkehr zur Echtzeit-Erkennung von Bedrohungen oder in Kombination mit den Sensoren der S-Serie, die Datenverkehr überwachen und Metadaten von den Sensoren auswerten, eingesetzt werden.

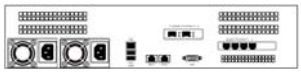
Die X-Serie Plattform führt die Erkennung, Analyse und Korrelation der Bedrohungen auf den Metadaten von Sensoren durch.

Die S-Serie Sensoren

Bei den Sensoren der S-Serie handelt es sich um kleine, spezielle Sensoren, die leicht an Remote-Standorten oder mit Access-Switchen bereitgestellt werden können. Die Sensoren überwachen passiv den Netzwerkverkehr, extrahieren daraus kritische Metadaten und leiten die Metadaten zur Gefährdungsanalyse an eine X-Serie-Plattform weiter.

Die kleine Grösse und das einfache Bereitstellungsmodell der S-Serie ermöglicht Unternehmen eine umfassende Abdeckung des gesamten Netzwerks, insbesondere von Remote-Standorten, einschliesslich in kleinen Büros, Kliniken und Einzelhandelsfilialen.

Die Zeit ist reif für ein intelligentes Sicherheitssystem – lassen Sie Vectra die Arbeit erledigen.
Sprechen Sie mit uns!

	S2 Sensor	X4 Plattform	X20 Plattform
Capture-Ports	▪ 4x 10/100/1000BASE-T Ports	▪ 4x 10/100/1000BASE-T Ports	▪ 4x 10/100/1000BASE-T ▪ 2x 10 Gigabit Ethernet SFP+
Management-Ports	▪ 1x 10/100/1000BASE-T Out-of-Band-Support Port ▪ 1x RJ 45 Serial Console Port	▪ 2 x 10/100/1000/BASE-T Ports ▪ 1x VGA Video Port ▪ 2x USB 2.0 Ports ▪ 1x DB 9 Serial Port	▪ 2 x 10/100/1000BASE-T Ports ▪ 1x VGA Video Port ▪ 2x USB 2.0 Ports ▪ 1x DB 9 Serial Port
Speicherkapazität	▪ 1 TB Festplatte	*Raw Storage* ▪ 4 TB Festplatte *Konfigurierter Speicher* ▪ 2 vollständig redundante 1 TB Festplatten für das Betriebssystem ▪ 2 x 1 TB Festplatten zum Disk-Striping für Daten	*Raw Storage* ▪ 6.8 TB Festplatte *Konfigurierter Speicher* ▪ 2 vollständig redundante 1 TB Festplatten für das Betriebssystem ▪ 8x 600 GB Festplatten zum Disk-Striping für Daten
Eingangsspannung	Automatische Erkennung 100-240 VAC, 50-60 Hz	Automatische Erkennung 100-240 VAC, 50-60 Hz	Automatische Erkennung 100-240 VAC, 50-60 Hz
Leistung	60 W	1800 W	1800 W
Strom	5A	7,5A-18A	7,5A-18A
Abmessungen	1,74 Zoll (44,19 mm) H 9,09 Zoll (230,88 mm) B 7,74 Zoll (196,59 mm) T	1,7 Zoll (43,18 mm) H 17,2 Zoll (436,88 mm) B 31 Zoll (787,40 mm) T	3,5 Zoll (88,90 mm) H 17,2 Zoll (436,88 mm) B 31 Zoll (787,40 mm) T
Gewicht	2,3 kg	21,8 kg	24,5 kg
Rückseite			

DATA CENTER SOLUTIONS

Als innovatives, international tätiges Schweizer Unternehmen bietet LC Systems seit über 25 Jahren qualitativ hochwertige Data Center Services sowie umfassende und etablierte Services für den Bereich Data Analytics entlang der gesamten Wertschöpfungskette: von der strategischen Beratung über die Realisierung und Weiterentwicklung bis hin zum Managed Service. LC Systems beschäftigt über 100 Data Center- und Data Analytics-Spezialisten an den Standorten in der Schweiz und in Deutschland.

LC Systems-Engineering AG
Postfach 40, Seestrasse 24
CH-9326 Horn
Telefon +41 (0)58 360 80 60
info@lcsystems.ch

LC Systems GmbH
Landsberger Straße 302
D-80687 München
Telefon +49 (0)89 416 11 8870
info@lcsystems.de

Office Basel
Reinacherstrasse 129
CH-4053 Basel
Telefon +41 (0)58 360 89 00

Office Bern
Talweg 17
CH-3063 Ittigen BE
Telefon +41 (0)58 360 84 00

www.lcsystems.ch