VECTRA

# Spezifikationen der Cognito-Plattform

Die Cognito-Plattform von Vectra für automatisierte Bedrohungserkennung und Response gewährt uneingeschränkte Einblicke in die Verhaltensweisen, die mit Cyber-Angriffen einhergehen, und zwar von Workloads in der Cloud und im Rechenzentrum bis hin zu Systemen für Endanwender und IoT-Geräten. Unabhängig von der Größe oder der geographischen Ausdehnung Ihrer Umgebung bietet Cognito eine konsequente und lückenlose Abdeckung Ihrer Systeme bei der Angriffserkennung. Cognito nimmt Angreifern auf diese Weise jedwede Chance, sich irgendwo zu verstecken.

Cognito hat ein zentrales „Gehirn“ und verfügt über eine Vielzahl von Sensoren, die diese Einheit mit Input versorgen. Es handelt sich um eine Applikation, die auf der X-Series-Appliance läuft und Daten von den S-Series-Sensoren empfängt.

S-Series-Sensoren können physische oder virtuelle Maschinen sein. Sie werden von Systemen anderer Anbieter mit Daten versorgt, zum Beispiel in Form von Logs, die ihren Ursprung in anderen Security-Produkten, Authentifizierungs-Systemen oder SaaS-Anwendungen haben. Auch „Indicators of Compromise“ – Hinweise auf einen Angriff, die aus einem fremden Monitoring-System stammen – werden ausgewertet.

Weil Cognito über künstliche Intelligenz verfügt, analysiert, triagiert, korreliert und priorisiert das System automatisch Bedrohungen über komplette Unternehmensumgebungen hinweg in Echtzeit und reduziert die Arbeitslast der Security-Analysten um den Faktor 29.

Um Cognitos Reichweite zu erhöhen, lassen sich S-Series-Sensoren leicht an entfernten Lokationen installieren – oder auch mit Access-Switches in internen Netzwerk-Segmenten. S-Series-Sensoren überwachen passiv den Netzwerk-Traffic, extrahieren kritische Metadaten und leiten sie an das Cognito-„Gehirn“ zur Analyse und Bedrohungserkennung weiter.

S-Series-Sensoren lassen sich auf verschiedene Weise implementieren: In-Line als „Bump in the Wire“ (Fail-Open-Modus) oder an einem SPAN-Port oder Network-TAP. Die geringe Größe und das einfache Implementierungsmodell der S-Series-Sensoren stellen eine umfassende Abdeckung des gesamten Netzwerks sicher, auch in externen Dienststellen, Praxen und Verkaufsstellen.

In Netzwerk-Umgebungen, die skalierbare Sensoren erfordern, kann die X-Series-Appliance als Sensor verwendet werden und Daten an die zentrale Verarbeitungseinheit senden. X-Series-Systeme, die die Sensorenrolle übernehmen, werden an SPAN-Ports oder Network-TAPs eingesetzt.

## Virtuelle Sensoren

Virtuelle Sensoren (vSensors) laufen unter VMware ESXi 5.0 und unter späteren Versionen. Sie machen es einfach, die Bedrohungserkennung von Cognito über das gesamte physische Netzwerk hinweg und in virtualisierte Rechenzentren hinein auszudehnen. vSensors können mit jedem beliebigen VMware-vSwitch im Rechenzentrum verbunden werden, verschaffen Ihnen Einblicke in den gesamten Traffic und decken dabei Bedrohungen auf, die sich in der virtuellen Umgebung zwischen den Workloads bewegen. Cognito integriert sich überdies auch mit VMware vCenter und gelangt so an aussagekräftige, immer hochaktuelle Informationen über die virtuelle Umgebung.

# X-Series Appliances
# S-Series Sensoren

## ALGORITHMEN

| | | |
|---|---|---|
| **Validiert gemäß FIPS 140-2** | *FIPS-zertifizierte Algorithmen:*<br>• AES (Cert. #2273)<br>• HMAC (Cert. #1391)<br>• DSA (Cert. #709); ECDSA (Cert. #368)<br>• RSA (Cert. #1166)<br>• SHS (Cert. #1954)<br>• Triple-DES (Cert. #1420)<br>• DRBG (Cert. #281)<br>• CVL (Cert. #44)<br>• RNG (Cert #1132) | *Andere Algorithmen:*<br>• RSA (Key Wrapping)<br>• Die Key-Establishment-Methode bietet eine Verschlüsselungstiefe zwischen 112 und 256 Bits<br>• Weniger als 112 Bits Verschlüsselungstiefe gilt als nicht compliant<br>• EC Diffie-Hellman Schlüssel-Austausch<br>• Die Key-Establishment-Methode bietet eine Verschlüsselungstiefe zwischen 112 und 256 Bits<br>• Weniger als 112 Bits Verschlüsselungstiefe gilt als nicht compliant |

## SPEZIFIKATIONEN

| | S2-Sensor | X24-Appliance | X29-Appliance | X80-Appliance |
|---|---|---|---|---|
| **Capture-Ports** | • Vier 10/100/1000BASE-T<br>• Insgesamt 2 Ports können im Passiv-Modus betrieben werden | • Vier 10/100/1000BASE-T<br>• Zwei 10 Gigabit Ethernet SFP+ | • Zwei 10/100/1000BASE-T<br>• Zwei 10 Gigabit Ethernet SFP+ | • Vier 10 Gigabit Ethernet SFP+ |
| **Management -Ports** | • Ein 10/100/1000BASE-T Out-of-Band-Management-Port<br>• Ein 10/100/1000BASE-T Out-of-Band-Support-Port<br>• Ein serieller RJ-45-Konsolen-Port | • Zwei 10/100/1000BASE-T-Ports<br>• Eine VGA-Video-Schnittstelle<br>• Zwei USB-2.0-Ports<br>• Eine serielle DB-9-Schnittstelle | • Zwei 10/100/1000BASE-T<br>• Eine VGA-Video-Schnittstelle<br>• Zwei USB-3.0-Ports<br>• Eine serielle DB-9-Schnittstelle | • Ein 1000BASE-T-Port<br>• Ein 10 Gigabit Ethernet SFP+<br>• Eine VGA-Video-Schnittstelle<br>• Zwei USB-2.0-Ports<br>• Eine serielle DB-9-Schnittstelle |
| **Speicher-kapazität** | • 1 TB Festplatte | *Unkonfigurierter Speicher:*<br>• 4-TB-Festplatte<br>*Konfigurierter Speicher:*<br>• Vier redundante 1-TB-Festplatten für Betriebssystem und Data-Striping | *Unkonfigurierter Speicher:*<br>• 6-TB-Festplatte<br>*Konfigurierter Speicher:*<br>• Vier 1,2-TB-Festplatten für Data-Striping<br>• Zwei redundante 480-GB -Festplatten für Datenbanken<br>• Ein 240-GB-SSD-Drive für das Vectra-System | *Unkonfigurierter Speicher:*<br>• 12-TB-Festplatte<br>*Konfigurierter Speicher:*<br>• Zwei redundante 1-TB-SSD-Drives für das Betriebssystem<br>• Acht 1-TB-Festplatten, Daten werden per Disk-Striping geschrieben |
| **Eingangs-spannung** | • 100-240 VAC, 50-60 Hz | • Auto-sensing 100-240 VAC, 50-60 Hz | • Zwei modulare Stromver-sorgungen; Auto-sensing 100-240 VAC, 50-60 Hz | • Zwei modulare Stromversorgun-gen; Auto-sensing 100-240 VAC, 50-60 Hz |
| **Leistung** | • 60 Watt | • 1800 Watt | • 685 Watt | • 1800 Watt |
| **Strom-verbrauch** | • 5 A | • 7.5 A-18 A | • 5,7 A bei 120 VAC, 2,85 A bei 240 VAC | • 7.5 A-18 A |
| **Abmessungen** | • 44,19 mm (1,74 in.) H x 230,88 mm (9,09 in.) B x 196,59 mm (7,74 in.) L | • 43 mm (1,7 in.) H x 437 mm (17,2 in.) B x 707 mm (27,82 in.) L | • 45 mm (1,75 in.) H x 432 mm (17 in.) B x 660 mm (26 in.) L | • 43 mm (1,7 in.) H x 437 mm (17,2 in.) B x 707 mm (27,82 in.) L |
| **Gewicht** | • 2,3 kg (5,18 lbs) | • 11,8 kg (26 lbs) | • 12 kg (27 lbs) | • 11,8 kg (26 lbs) |
| **Betriebs- und Lagertempe-ratur** | *Betriebstemperatur:*<br>• 0° bis 40° C (32° bis 104° F)<br>*Lagertemperatur:*<br>• -20° bis 70° C (-4° bis 158° F) | *Betriebstemperatur:*<br>• 10° bis 35° C (50° bis 95° F)<br>*Lagertemperatur:*<br>• -40° bis 70° C (-40° bis 158° F) | *Betriebstemperatur:*<br>• 0° bis 35° C (32° bis 95° F)<br>*Lagertemperatur:*<br>• 0° bis 50° C (32° bis 122° F) | *Betriebstemperatur:*<br>• 10° bis 35° C (50° bis 95° F)<br>*Lagertemperatur:*<br>• -40° bis 70° C (-40° bis 158° F) |

## VIRTUELLE SENSOREN

| | | | | |
|---|---|---|---|---|
| **Durchsatz** | • 400 Mbps<br>• 1 Gbps<br>• 2 Gbps<br>• 5 Gbps | • 2 virtuelle CPU-Cores<br>• 4 virtuelle CPU-Cores<br>• 8 virtuelle CPU-Cores<br>• 16 virtuelle CPU-Cores | • 8 GB RAM<br>• 8 GB RAM<br>• 16 GB RAM<br>• 64 GB RAM | • 100 GB Festplattenkapazität<br>• 150 GB Festplattenkapazität<br>• 150 GB Festplattenkapazität<br>• 600 GB Festplattenkapazität |
| **Anforde-rungen** | • VMware ESXi 5.0 oder später<br>• Intel- oder AMD-CPUs mit Unterstützung für SSE3 und SSE4<br>• Zwei Netzwerkschnittstellen | | | |

VECTRA®

**E-Mail** info_DACH@vectra.ai **Tel.** +41 43 810 47 52 / +49 69 202 328 10 https://vectra.ai/dach