VECTRA®

Spécifications de la plate-forme Cognito

Cognito™ est la plate-forme de détection des menaces et d'aide à la résolution des incidents de Vectra®. Elle assure une visibilité complète sur les comportements liés aux cyberattaques, que leur cible soit le cloud, les centres de données, les appareils connectés ou les terminaux des utilisateurs. Indépendamment de l'ampleur et de la distribution géographique des attaques, Cognito offre une couverture de détection homogène, sans angle mort, qui ne laisse aucune chance aux cyberpirates.

Cognito possède un centre névralgique (« cerveau ») et de nombreux capteurs destinés à l'alimenter en données. Ce centre névralgique, exécuté sur l'appliance de la série X, reçoit les données des capteurs de la série S.

Ces capteurs, physiques ou virtuels, peuvent quant à eux recevoir des informations de sources externes (journaux de solutions de sécurité, systèmes d'authentification, applications SaaS, indicateurs de compromission, etc.).

Grâce à sa technologie d'intelligence artificielle, Cognito analyse automatiquement les menaces, les trie, les met en corrélation et les classe par ordre de priorité. Toutes ces opérations sont exécutées en temps réel à l'échelle de l'entreprise, réduisant ainsi considérablement la charge des analystes en sécurité.

Pour étendre la portée de Cognito, les capteurs de la série S peuvent être facilement déployés sur des sites distants ou avec des commutateurs d'accès sur les segments du réseau interne. Ils peuvent effectuer une surveillance passive du trafic réseau, extraire les métadonnées importantes et les transmettre au centre névralgique dans un but d'analyse et de détection des menaces.

Les capteurs de la série S peuvent être déployés en ligne ou en tant que dispositifs annexes de type BITW (bump-in-the-wire) garantissant la disponibilité en cas d'incident, ou encore sur un port SPAN ou un TAP réseau. Leur format compact et leur simplicité de déploiement permettent une couverture complète de l'ensemble du réseau — y compris dans ses composants excentrés tels que les sites distants, les points de vente, etc.

Pour les emplacements réseau nécessitant des capteurs qui acceptent une montée en charge, il est également possible de déployer l'appliance de la série X en tant que capteur pour le centre névralgique. Dans un tel modèle de déploiement, l'appliance de la série X est alors déployée sur un port SPAN ou un TAP réseau.

Capteurs virtuels

Les capteurs virtuels (vSensor) s'exécutent dans VMware ESXi 5.0 ou version ultérieure, ce qui permet d'étendre très facilement la couverture de détection des menaces de Cognito à l'ensemble du réseau physique et aux centres de données virtualisés. Ces capteurs virtuels peuvent être connectés à n'importe quel commutateur virtuel (vSwitch) VMware dans le centre de données pour offrir une visibilité sur l'ensemble du trafic et détecter des menaces qui se déplacent entre les charges de travail de l'environnement virtuel. Cognito s'intègre également avec VMware vCenter pour offrir des vues de référence, constamment actualisées, de l'environnement virtuel.

Appliances de la série X
Capteurs de la série S

ALGORITHMES

Conformes à la norme FIPS 140-2	*Algorithmes conformes à FIPS :* • AES (Cert. n° 2273) • HMAC (Cert. n° 1391) • DSA (Cert. n° 709) ; ECDSA (Cert. n° 368) • RSA (Cert. n° 1166) • SHS (Cert. n° 1954) • Triple-DES (Cert. n° 1420) • DRBG (Cert. n° 281) • CVL (Cert. n° 44) • RNG (Cert. n° 1132)	*Autres algorithmes :* • RSA (enveloppement de clés) • La méthodologie de génération de clés offre une puissance de chiffrement comprise entre 112 et 256 bits. • Non conforme si la puissance de chiffrement est inférieure à 112 bits. • Échange de clés Diffie-Hellman basé sur les courbes elliptiques. • La méthodologie de génération de clés offre une puissance de chiffrement comprise entre 112 et 256 bits. • Non conforme si la puissance de chiffrement est inférieure à 112 bits.

SPÉCIFICATIONS

	Capteur S2	Appliance X24	Appliance X29	Appliance X80
Ports de capture	• 4 ports 10/100/1000BASE-T • 2 ports max. peuvent être utilisés en mode passif.	• 4 ports 10/100/1000BASE-T • 2 ports 10 Gigabit Ethernet SFP+	• 2 ports 10/100/1000BASE-T • 2 ports 10 Gigabit Ethernet SFP+	• 2 ports 10 Gigabit Ethernet SFP+
Ports de gestion	• 1 port de gestion hors bande 10/100/1000BASE-T • 1 port de support hors bande 10/100/1000BASE-T • 1 port de console série RJ-45	• 2 ports 10/100/1000BASE-T • 1 port vidéo VGA • 2 ports USB 2.0 • 1 port série DB-9	• 2 ports 10/100/1000BASE-T • 1 port vidéo VGA • 2 ports USB 3.0 • 1 port série DB-9	• 1 port 1000BASE-T • 1 port 10 Gigabit Ethernet SFP+ • 1 port vidéo VGA • 2 ports USB 2.0 • 1 port série DB-9
Capacité de stockage	• Disque dur de 1 To	*Capacité de stockage brute :* • Disque dur de 4 To *Capacité de stockage configurée :* • 4 disques durs redondants de 1 To pour le système d'exploitation et l'entrelacement des données	*Capacité de stockage brute :* • Disque dur de 6 To *Capacité de stockage configurée :* • 4 disques de 1,2 To pour l'entrelacement des données • 2 disques SSD redondants de 480 Go pour le système Vectra • 1 disque SSD de 240 Go pour le système Vectra	*Capacité de stockage brute :* • Disque dur de 12 To *Capacité de stockage configurée :* • 2 disques SSD redondants de 1 To pour le système d'exploitation • 8 disques durs de 1 To pour l'entrelacement des données
Tension d'entrée	• 100-240 Vca, 50-60 Hz	• Détection automatique 100-240 Vca, 50-60 Hz	• Double alimentation modulaire ; détection automatique 100-240 Vca, 50-60 Hz	• Double alimentation modulaire ; détection automatique 100-240 Vca, 50-60 Hz
Puissance	• 60 W	• 1 800 W	• 685 W	• 1 800 W
Courant	• 5 A	• 7,5 A-18 A	• 5,7 A sous 120 Vca, 2,85 A sous 240 Vca	• 7,5 A-18 A
Dimensions	• H 44,19 mm x L 230,88 mm x l 196,59 mm	• H 43 mm x L 437 mm x l 707 mm	• H 45 mm x L 432 mm x l 660 mm	• H 43 mm x L 437 mm x l 707 mm
Poids	• 2,3 kg	• 11,8 kg	• 12 kg	• 11,8 kg
Environnement	*Température de fonctionnement :* • 0 à 40 °C *Température en veille :* • -20 à 70 °C	*Température de fonctionnement :* • 10 à 35 °C *Température en veille :* • -40 à 70 °C	*Température de fonctionnement :* • 0 à 35 °C *Température en veille :* • 0 à 50 °C	*Température de fonctionnement :* • 10 à 35 °C *Température en veille :* • -40 à 70 °C

CAPTEURS VIRTUELS

Débit	• 400 Mbit/s • 1 Gbit/s • 2 Gbit/s • 5 Gbit/s	• 2 cœurs de processeur virtuels • 4 cœurs de processeur virtuels • 8 cœurs de processeur virtuels • 16 cœurs de processeur virtuels	• 8 Go de RAM • 8 Go de RAM • 16 Go de RAM • 64 Go de RAM	• 100 Go d'espace disque • 150 Go d'espace disque • 150 Go d'espace disque • 600 Go d'espace disque
Configuration requise	• VMware ESXi 5.0 ou version ultérieure • Processeurs Intel ou AMD prenant en charge SSE3 et SSE4 • Deux interfaces réseau			

VECTRA®

E-mail : Info_France@vectranetworks.com / info_DACH@vectranetworks.com **Téléphone :** +41 43 810 47 52 / +33 (0)6 29 12 41 19
www.vectra.ai