HITACHI
Inspire the Next

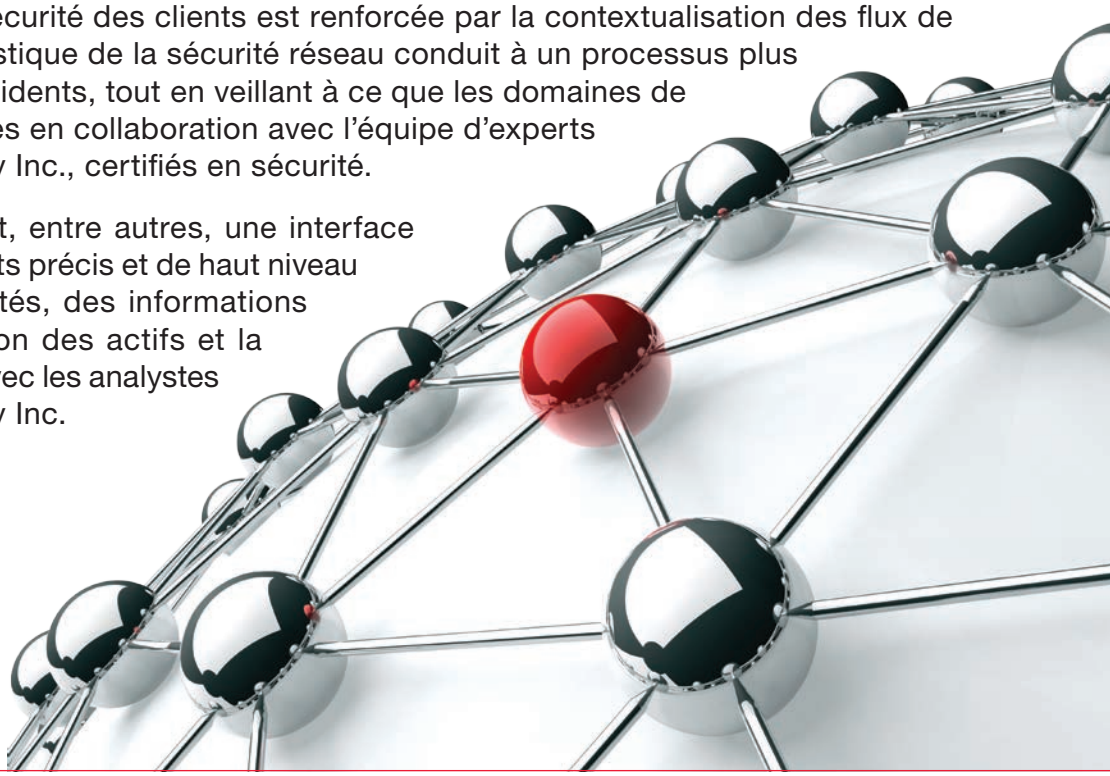
FICHE TECHNIQUE ARKANGEL

Afin de faire face aux pirates modernes et aux méthodologies sophistiquées qu'ils utilisent, Hitachi Systems Security Inc. a développé une approche holistique de la sécurité réseau centrée autour de sa plateforme ArkAngel. En corrélant de grandes quantités de données de sécurité, ArkAngel filtre le bruit produit par les solutions actuelles de technologies de sécurité dans le but de fournir une vue cohérente et ainsi faciliter le processus de gestion des incidents.

ArkAngel est une plate-forme intelligente de gestion des risques de l'information conçue pour transformer à partir de sources multiples, les données de sécurité en informations exploitables. La corrélation des évènements de sécurité à partir d'appareils distribués facilitent la détection des menaces et améliorent considérablement l'efficacité du processus de gestion de réponses aux incidents. L'approche techno-agnostique d'ArkAngel permet de collecter et d'agréger des alertes, des journaux et autres données spécifiques liées aux périphériques à partir de tous les réseaux informatiques, qu'il s'agisse de systèmes existants, de systèmes virtuels, de BYOD (Bring Your Own Device) ou même d'environnements Cloud.

Le moteur d'intelligence avancée ArkAngel brosse une image complète et précise du réseau du client. La posture de sécurité des clients est renforcée par la contextualisation des flux de données. Cette vision holistique de la sécurité réseau conduit à un processus plus proactif de gestion des incidents, tout en veillant à ce que les domaines de préoccupation soient traités en collaboration avec l'équipe d'experts d'Hitachi Systems Security Inc., certifiés en sécurité.

Le portail ArkAngel fournit, entre autres, une interface centralisée pour les rapports précis et de haut niveau portant sur les vulnérabilités, des informations sur les incidents, la gestion des actifs et la communication en direct avec les analystes d'Hitachi Systems Security Inc.



CARACTÉRISTIQUES D'ARKANGEL

CONTRÔLE CONTINU

L'équipe d'analystes d'Hitachi Systems Security Inc. surveille les alertes générées par des sondes, 24 heures sur 24, 7 jours sur 7 et ce, tous les jours de l'année.

SYSTÈMES DE PRÉVENTION ET DE DÉTECTION D'INTRUSION (SURVEILLANCE DES MENACES)

Le service de gestion des menaces consiste en une surveillance et une gestion 24/7 des menaces internes et externes au sein de votre réseau. Dès l'identification et la validation d'un événement de menace, d'une perte de données ou d'une activité malveillante, le service de gestion des menaces envoie des alertes et identifie la menace potentielle afin que des mesures correctives puissent être appliquées. Soutenus par nos analystes experts, notre corrélation d'événements sur mesure et notre déroulement intégré et automatisé des opérations de traitement des incidents s'adaptent aux processus et aux exigences de gestion de la menace de toute organisation.

TOUJOURS ACTIF

La surveillance matérielle et réseau Nagios vérifie l'état de toutes les sondes et tous les composants, informant immédiatement les analystes si un service se dégrade. Chacun des services d'ArkAngel s'autocontrôle et envoie un signal une fois par minute afin de s'assurer de la prise de connaissance immédiate par les analystes d'un arrêt dudit service. Les sondes stockent jusqu'à 300 Go, ce qui suffit à mettre en mémoire cache l'équivalent de quelques mois de données d'événement dans des conditions normales d'utilisation. Enfin, les sondes peuvent être configurés en parallèle pour se soutenir au besoin.

MOTEUR DE CORRÉLATION AVANCÉ

La logique avancée du Moteur de Corrélation permet une meilleure détection des événements pour des scénarios d'attaques en performant une analyse sur toutes les alertes du réseau client, afin d'identifier et de distinguer les motifs qui pourraient indiquer des menaces difficilement détectables à l'œil humain.

LES AVANTAGES D'ARKANGEL

ArkAngel facilite le processus de gestion des incidents et améliore la sécurité du réseau client en:

- Réduisant la période de temps entre la reconnaissance d'une alerte et la constatation de la présence ou de l'absence d'une activité malveillante.
- Augmentant la qualité de l'analyse pour créer un processus précis d'identification des incidents.
- Priorisant les risques pour les actifs informatiques des clients en fournissant des informations claires sur l'emplacement du risque et comment y faire face.
- Fournissant un canal de communication sécurisé entre les clients et les analystes d'Hitachi Systems Security Inc. avec un déroulement automatisé des opérations de gestion des incidents.
- Permettant aux clients de tirer parti des meilleures applications de sécurité. Avec ArkAngel, les clients n'ont pas besoin d'investir dans de nouveaux appareils dans la mesure où ArkAngel est suffisamment flexible pour fonctionner avec n'importe quelle infrastructure existante.
- Créant une vision transparente et à 360 degrés de la posture de sécurité du réseau des clients en fournissant un moyen de lier toutes les solutions de sécurité dans un modèle de risque cohérent.
- Analysant le "bruit" grâce à l'utilisation d'une corrélation d'informations de sécurité. Plus la durée d'engagement de nos analystes dans votre environnement sera longue, meilleures seront les corrélations. La valeur du service augmente donc au fil du temps.

Nous sommes vos partenaires en sécurité intégrée.

MOTEUR DE DÉTECTION D'ACTIFS

Conçu pour détecter les serveurs, les postes de travail et les appareils dès qu'ils apparaissent dans l'environnement client, le Moteur de Détection d'Actifs identifie les actifs les plus critiques dans les environnements réseau de nos clients, améliorant ainsi les capacités d'Hitachi Systems Security Inc. à anticiper et prévenir toute attaque.

COMMUNICATIONS SÉCURISÉES

Toutes les communications, qui sont par ailleurs cryptées, entre vous et Hitachi Systems Security Inc. s'effectuent via la plate-forme ArkAngel, en veillant à ce que vous seul y ayez accès. Un historique de toutes les communications est également maintenu de manière sécurisée, assurant la conformité aux politiques et règlements. Cela permet de faire le suivi historique.

STOCKAGE DE DOCUMENTS

Un stockage de documents sous contrôle de version sert de point central pour transmettre des informations entre votre équipe et la nôtre. Lorsque vous avez besoin de partager des plans de correction, des diagrammes réseau ou toutes autres informations confidentielles, il vous est possible de les transmettre via notre VPN entièrement crypté, plutôt que par e-mail, pour une sécurité optimale. Cela sert également de référentiel pratique pour le matériel de formation et autres informations essentielles. C'est un réel support pour votre propre personnel informatique.

BASE DE CONNAISSANCES

Une base de connaissances de type wiki contient des douzaines d'articles qui définissent et expliquent les nombreuses fonctionnalités du portail ArkAngel. Votre personnel informatique interne peut ainsi tout apprendre sur le produit sans avoir besoin de demander de l'aide. Une aide n'en reste pas moins disponible, si vous le souhaitez.

RÉTENTION DES JOURNAUX DE SÉCURITÉ

Tous les journaux de sécurité sont conservés par ArkAngel pour analyse historique pour une période prolongée. La durée de la période de rétention peut varier en fonction de vos besoins, que ce soit en vertu de la conformité réglementaire ou des règles de gouvernance interne.

REQUÊTE DE L'HISTORIQUE

Un langage de requête propriétaire permet à nos analystes, ou aux vôtres, de récupérer rapidement et facilement tous les journaux qui résident toujours sur le sonde. Cela permet aux auditeurs d'économiser du temps sur l'analyse des journaux via des scripts ou des commandes de console. Cela signifie que nos analystes consacrent moins de temps et d'effort à enquêter et bien plus à améliorer le service, notamment en guidant activement la correction ou en produisant de meilleures règles de corrélation pour votre environnement.

APPROCHE TECHNO-AGNOSTIQUE

L'approche techno-agnostique d'ArkAngel nous permet de nous intégrer facilement à n'importe quel dispositif de sécurité réseau pour collecter et agréger des alertes, des journaux et autres informations spécifiques. Qu'il s'agisse de systèmes maison, de systèmes virtuels, d'environnements BYOD (Bring Your Own Device) ou même d'environnements Cloud, ArkAngel intègre des journaux de systèmes de sécurité tiers tels que les systèmes anti-DDoS de Radware, IBM AS400 iSeries, les plateformes Linux/Unix, les systèmes d'exploitation Windows etc.

INFORMATIONS CONTEXTUALISÉES

La posture de sécurité de nos clients est renforcée par la contextualisation des flux de données de sécurité avec une logique spécifique au client, ce qui permet au moteur avancé d'intelligence ArkAngel de brosser un tableau complet et précis de votre réseau. Cette vision holistique de la sécurité du réseau conduit à un processus plus proactif de gestion des incidents.

CONFIGURATION DE LA RÉPUTATION IP

Les communications IP avec un moteur de réputation améliorent votre capacité en matière de surveillance de l'utilisation d'Internet. Elles vous préviennent également en cas de violation de politiques en facilitant l'identification des accès aux sites non fiables.

SURVEILLANCE DES JOURNAUX

Le service de surveillance des journaux d'événements étend les fonctionnalités de gestion des menaces en fournissant des données. Cela est essentiel pour mener de manière appropriée une enquête sur les violations de vos politiques. Ce service peut être un support aux audits et représente une composante obligatoire de nombreux programmes de conformité. Une année complète d'archivage est comprise dans le service de base. Elle peut également être prolongée comme souhaitée.

BALAYAGE DE VULNERABILITÉS

Le sonde ArkAngel est livré avec un scanner de vulnérabilité SAINT intégré. Cela peut être utilisé à tout moment pour tester la sécurité des hôtes au sein de votre environnement. Il fonctionne en envoyant des paquets sur tous les ports disponibles et en analysant les réponses par rapport aux signatures de vulnérabilité qui ont été publiées. Il s'agit d'un élément essentiel d'un programme de sécurité TI. Cela constitue également un élément essentiel des exigences de nombreux cadres de conformité, comme PCI DSS.

SERVICES DE GESTION DES VULNÉRABILITÉS

La gestion des vulnérabilités vulnérabilité fournit une analyse à la demande et une évaluation des vulnérabilités techniques au sein de votre infrastructure informatique. Les tableaux de bord détaillés et les rapports disponibles identifient, quantifient et hiérarchisent les forces et les faiblesses de votre environnement en matière de sécurité de l'information. Nos analystes experts vous assistent personnellement avec des instructions de correction tout en proposant un plan d'action pour réduire les risques de conséquences graves.

LE MODULE DE GOUVERNANCE

Le module de gouvernance permet aux cadres supérieurs de définir et de suivre leur inventaire d'actifs informatiques, de créer des groupes d'actifs (Systèmes d'Affaires) et de leur attribuer des scores de criticité.

Une fois définis, les utilisateurs peuvent obtenir en un coup d'œil la posture de sécurité spécifique aux actifs les plus critiques. Des vues individuelles axées sur les incidents, les journaux et les analyses de vulnérabilités fournissent des informations de haut niveau sur la posture de sécurité globale de l'organisation, ainsi que des informations plus spécifiques telles que le temps écoulé depuis la dernière analyse des serveurs et la durée nécessaire pour corriger les vulnérabilités découvertes.

SPÉCIFICATIONS TECHNIQUES

Spécifications matérielles des sondes ArkAngel

Modèle	Norme	Sonde Gigabit	Sonde Virtuel
Capacité	IPS/IDS: jusqu'à 250 Mbps *	IDS: jusqu'à 1 Gbps * Jusqu'à 2000 évènements par seconde, selon la taille des journaux	IDS: jusqu'à 800 Mbps sur les réseaux virtuels. Jusqu'à 200 Mbps par core *
Cores	4 [1x4]	10 [1x10]	4 cores maximum
Interfaces de surveillance	(1x4) cartes cuivre bypass 1 Gbps	(2 x 2) cartes cuivre bypass 1 Gbps	(1) Adaptateur virtuel flexible
Interfaces de gestion	(2)RJ45	(2)RJ45	(1+) Interface de l'hyperviseur
Détection des actifs	Compatible*	Compatible*	Compatible*
Moteur de corrélation	Compatible	Compatible	Compatible
Scanner des vulnérabilités	Compatible*	Compatible*	Compatible*
Collecteur de journaux	Compatible*	Compatible*	Compatible*
IPS	Compatible	Non Compatible	Non Compatible
Ram	16 Gb	24 Gb	2 Gb par core

**La performance exacte du réseau variera en fonction des conditions qui sont hors du contrôle d'Hitachi Systems Security Inc. La taille moyenne des paquets, les paquets par seconde, le nombre de sessions simultanées et l'utilisation du protocole peuvent avoir un impact sur les mesures de la performance.*

CORRÉLATION D'ÉVÉNEMENTS DE SÉCURITÉ

Il existe actuellement plus de 100 sources de données de sécurité.

ArkAngel peut accepter n'importe quelle source pertinente. Tant que le journal est non crypté et non binaire, des règles d'analyse peuvent facilement être créées. À leur demande, le client peut avoir la possibilité de créer directement des règles d'analyse personnalisées via l'interface Arkangel. De manière alternative, un client peut demander à Hitachi Systems Security Inc. de développer de telles règles.

Si l'intégration de nouvelles sources de données peut être réalisée en 3 jours d'effort ou moins, celle-ci sera comprise dans le prix du service. Des intégrations plus complexes ou urgentes peuvent être produites sur demande à un prix additionnel.

Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, bureau 244, Blainville (Québec) J7C 5J6 Canada
Tél: +1 450-430-8166 Fax: +1 450-430-1858
www.hitachi-systems-security.com