Brochure

Sécurité intelligente au service de l'entreprise ultraperformante

Atos High Performance Security, optimisé par Intel Security : la sécurité réinventée

intel Security

Atos

De nos jours, les organisations cybercriminelles et de cyberespionnage fonctionnent comme n'importe quelle entreprise.

Elles recrutent les meilleurs talents, investissent massivement dans la recherche et le développement et poursuivent l'expansion mondiale de leurs capacités de « distribution ».

Une nouvelle approche pour une nouvelle ère en matière de cybermenaces

Aujourd'hui plus que jamais, les entreprises s'appuient sur les données pour mener à bien leurs activités. Les informations constituent sans doute votre actif le plus précieux. Voilà pourquoi les cybercriminels dépensent des millions pour mettre au point des attaques extrêmement sophistiquées. Et pourquoi des entreprises concurrentes et des cyberactivistes se donnent autant de mal pour mettre la main sur vos données de propriété intellectuelle.

Il suffit de jeter un rapide coup d'œil aux titres de l'actualité pour prendre la mesure des difficultés que rencontrent les entreprises de tous types et de toutes tailles en matière de protection des données. Le défi tient au fait que, si la sécurité informatique ne fait pas partie de leur cœur de métier, les cybercriminels sont en revanche des experts en la matière.

De nos jours, les organisations cybercriminelles et de cyberespionnage fonctionnent comme n'importe quelle entreprise.

Elles recrutent les meilleurs talents, investissent massivement dans la recherche et le développement et poursuivent l'expansion mondiale de leurs capacités de « distribution ». Les cybercriminels peuvent parvenir à leurs fins à l'aide de services cybercriminels proposés sur le marché noir, qui offrent un accès rapide à des techniques et logiciels malveillants (malware) sophistiqués préconçus, notamment des logiciels de demande de rançon (ransomware) et des menaces persistantes avancées (APT).

Dans un tel contexte, comment une entreprise telle que la vôtre peut-elle espérer protéger ses données critiques, ses opérations stratégiques et sa réputation face à un ennemi aussi expert que motivé ?

Imaginez les investissements en termes de systèmes et de personnel nécessaires pour détecter sans relâche d'éventuels incidents liés à une cyberattaque, sans parler de la mise en place d'une protection en temps réel, intelligente et proactive.

Il est temps d'aborder la sécurité sous un nouvel angle, en faisant appel à un partenaire aux compétences pointues.

L'intelligence analytique au service de la cybersécurité

Le paysage des cybermenaces est en constante mutation. Les cybercriminels et les espions informatiques disposent déjà des outils nécessaires pour élaborer à moindre coût des attaques avancées et ne cessent d'innover. Il faut s'attendre à ce que les logiciels malveillants s'appuient de plus en plus souvent sur des techniques de contournement avancées pour échapper à la détection. De même, des attaques ciblées seront lancées plus efficacement et rapidement pour exploiter les vulnérabilités uniques affectant les systèmes d'entreprise.

La clé de la prévention des cyberattaques

Quels types de menaces une stratégie de sécurité digne de ce nom doit-elle prendre en considération ? Bien que leur paysage évolue constamment, il est possible de brosser un tableau assez fiable de ce que l'avenir nous réserve — et les types de menaces suivants seront probablement présents en grand nombre :

E-mails et SMS de phishing

Des attaques simples et difficiles à contrer, qui utilisent les informations de manière abusive en toute facilité.

Ransomware

Efficaces dans le cloud, sur les terminaux mobiles, partout. Difficiles à contrer et, surtout, à mettre en échec.

Attaques ciblant les terminaux de point de vente

Déjà bien présentes, elles sont vouées à se répandre avec la multiplication des types de paiement (applications mobiles).

Menaces internes

Celles-ci émanent d'employés mécontents ou résultent de défaillances de la protection de partenaires, voire de fuites de données à la suite du vol ou de la perte d'équipements mobiles.

Logiciels malveillants sur mobiles

La prolifération des terminaux mobiles élargit la surface d'attaque de l'environnement mobile et du BYOD.

Logiciels malveillants pour systèmes d'exploitation non-Windows

Dans le sillage de la vulnérabilité Shellshock, les attaquants ciblent les équipements Unix et Linux vulnérables.

Attaques ciblant l'Internet des objets (IoT)

Les pirates multiplieront ces attaques pour récolter les données de valeur présentes sur ces objets connectés. Il est probable que leur fréquence, leur gravité et leur rentabilité augmentent.

Menaces persistantes avancées (APT) : cyberguerre et espionnage informatique

Ces manœuvres surviendront probablement entre des États. Les gouvernements recourront davantage à des logiciels malveillants pour surveiller les activités de personnes d'intérêt et organiser des attaques ciblées. Les cybercriminels et les rivaux commerciaux utiliseront également des attaques complexes pour espionner les activités des entreprises et dérober leurs éléments de propriété intellectuelle.

Malgré tous ces dangers, votre entreprise ne peut pas se permettre de verrouiller ses systèmes et données si elle veut rester compétitive. La libre circulation des informations encourage l'innovation, booste la productivité, améliore l'expérience des clients et facilite les opérations d'arrière-guichet — en fait, elle optimise presque toutes les activités des utilisateurs à chaque moment de la journée. La solution consiste à mettre en place une approche de la sécurité tenant compte du contexte des données et fondée sur la cyberveille. Une solution qui ne soit pas une charge budgétaire ou opérationnelle supplémentaire pour l'équipe informatique.

Source : Intel Security, *Rapport de McAfee Labs sur le paysage des menaces*, novembre 2014, et site myarklamiss.com de NBC News, *The Year in Cybersecurity: 5 Threats to Watch in 2015* (L'année de la cybersécurité : cinq menaces à surveiller en 2015)

Intel Security a la solution qu'il vous faut

Grâce à McAfee Enterprise Security Manager (ESM), la solution SIEM d'Intel Security, les grandes entreprises et les organismes publics peuvent collecter, consolider, mettre en corrélation, évaluer et classer par priorité les événements de sécurité émanant des solutions d'Intel Security et d'éditeurs tiers, et ce en temps réel.

Ils se dotent ainsi d'une approche de la sécurité des informations soutenue par l'intelligence analytique, idéale pour les environnements opérationnels hautes performances actuels.

McAfee ESM est capable de répondre à plusieurs requêtes relatives à des événements et activités au sein de votre environnement. Pour ce faire, la solution analyse l'activité réseau, notamment des sessions complètes de base de données, parallèlement à d'autres critères, comme le comportement des utilisateurs, l'emplacement des appareils et les rôles utilisateur, ou encore le contenu des documents transmis. Elle associe ensuite ces données au profil de risque particulier de votre entreprise ou organisme pour évaluer le caractère nuisible ou malveillant de certaines activités. Toutes ces opérations s'effectuent en temps réel, de sorte que quelques millisecondes à peine s'écoulent entre la détection et l'endiguement d'une attaque.

McAfee ESM se connecte à McAfee Global Threat Intelligence, base de données mondiale de renseignements sur les menaces, pour comparer les événements suspects aux signatures de logiciels malveillants connues.

En outre, Threat Intelligence Exchange, technologie unique de McAfee, distribue les données d'événement aux produits de sécurité connectés (par exemple, des firewalls NG et des systèmes de prévention des intrusions), créant ainsi un cadre essentiel pour le partage de renseignements de sécurité.

La puissance de McAfee ESM tient principalement à son interface unique qui rassemble et présente toutes les données de surveillance proactive, consigne les activités de gestion des événements et génère des rapports automatisés pour quelque 240 réglementations en matière d'utilisation de données.

Pour vous garantir une protection maximale, McAfee ESM peut évoluer en fonction de vos besoins et prendre en charge des centaines de milliers d'événements par seconde. Cette solution vous paraît exceptionnelle ? Il est pourtant possible d'améliorer encore ses fonctionnalités.

Découvrons comment...

Résoudre les problèmes ensemble...

Atos High Performance Security : révolutionnez votre sécurité

Nous avons choisi McAfee Enterprise Security Manager d'Intel Security pour renforcer notre puissant service de sécurité managé : Atos High Performance Security (AHPS).

AHPS propose une approche globale de la sécurité des informations, soutenue par notre philosophie en trois phases : évaluation et conception, transformation et exécution. Forts de plus de 25 ans d'expérience dans l'offre de solutions de sécurité à une clientèle de grandes entreprises, nous réalisons les activités suivantes avec votre collaboration :

Évaluation et conception

Permet d'analyser vos besoins de sécurité sur la base des meilleures pratiques du secteur afin de déterminer votre profil de risque et vos obligations de conformité en matière de données et de définir les contrôles nécessaires. Nous veillons ensuite à mettre en œuvre la solution la mieux adaptée à vos besoins spécifiques.

Transformation

Consiste à améliorer votre niveau de sécurité en modelant AHPS de manière à ce que le service intègre les fonctions de protection et de génération de rapports dont votre entreprise a besoin. Cette phase peut comporter des activités telles que des preuves de concept et des tests de la solution.

Exécution

Correspond à la mise en œuvre de votre service AHPS à partir de nos centres d'opérations de sécurité (SOC) ultramodernes situés partout dans le monde.

En pratique, notre méthodologie de gestion de services (voir la figure 1) génère une boucle de rétroaction dynamique basée sur l'intelligence analytique. Ainsi, nous sommes à même de concevoir une solution qui reconnaît l'évolution de vos besoins métier et s'adapte en conséquence, analyse votre profil de risque particulier et surveille les comportements anormaux afin d'assurer une réponse en temps réel aux incidents. Nous mesurons également l'efficacité de votre solution par rapport à des renseignements sur les menaces externes et nous y apportons des ajustements permanents pour garantir la sécurité de vos systèmes et données critiques. La combinaison de cette méthodologie et de fonctionnalités uniques permet à AHPS d'offrir des avantages hors pair à votre entreprise :

Tranquillité d'esprit

Vous avez la certitude que vos données sont surveillées et protégées 24 h sur 24 et 7 j sur 7 par un réseau mondial d'analystes en sécurité chevronnés. Votre équipe se chargera de surveiller constamment votre environnement, d'évaluer les événements de sécurité potentiels et d'entreprendre des investigations de manière précoce pour vous aider à bloquer toute attaque.

Économies

Le service managé et centralisé permet de réaliser d'importantes économies d'échelle. Votre entreprise serait-elle en mesure d'embaucher les milliers de spécialistes de la sécurité que nous mettons à votre disposition ?

Simplicité

Nous prenons soin de chaque aspect du service proposé, de A à Z, sans aucun intermédiaire, et vous disposez d'un point de contact unique dédié.

Intelligence analytique directement exploitable

En tant qu'intégrateur systèmes de renom, nous pouvons vous aider à tirer le meilleur parti des renseignements de sécurité fournis par notre technologie SIEM. En intégrant cette dernière avec vos propres solutions de protection des terminaux, nous vous permettons de créer un ensemble continu et robuste de données de sécurité grâce auquel vous pourrez appliquer immédiatement des mesures de protection contre les menaces les plus sophistiquées.

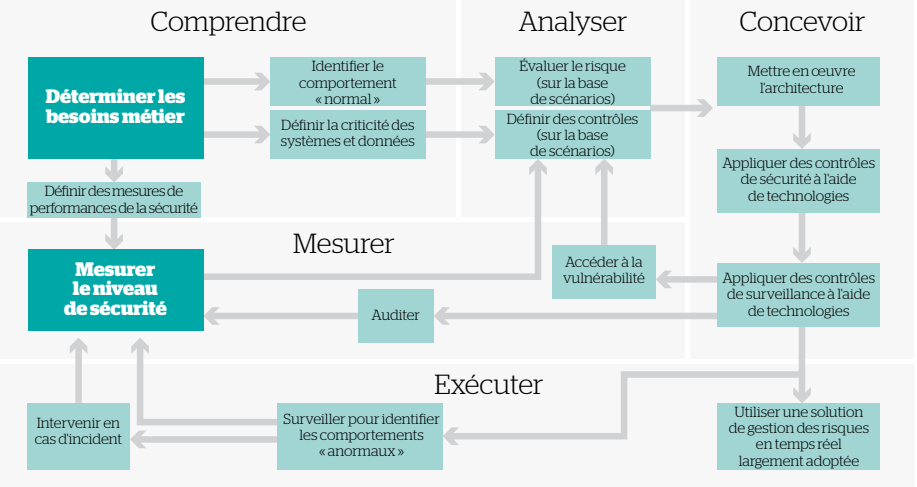

Figure 1

Plus forts ensemble...

L'union fait la force

Lorsque nous avons conçu le service Atos High Performance Security, nous avons pris la peine d'évaluer de nombreuses technologies SIEM : nous avons réalisé des preuves de concept, analysé les résultats obtenus et défini des feuilles de route en matière d'innovation. Nous nous démarquons par notre choix de la meilleure solution disponible sur le marché, McAfee Enterprise Security Manager. Nous sommes convaincus que cette solution, soutenue par la force d'Intel, offre des fonctionnalités inégalées qui permettent la mise en place d'une sécurité robuste, proactive et connectée.

Certaines entreprises parmi les plus prestigieuses au monde, comptant parmi nos clients, partagent cette opinion. Elles ont confié à Atos et à Intel Security le soin de protéger conjointement leurs systèmes et informations critiques de manière à ce que ceux-ci contribuent pleinement au succès de leurs activités.

Le fait que l'innovation soit au cœur même de notre stratégie d'entreprise nous oblige à conserver continuellement une longueur d'avance sur les auteurs d'attaques. C'est dans cet esprit que la communauté scientifique d'Atos, véritable instigatrice d'innovations, met tout en œuvre pour anticiper les mutations du paysage mondial des menaces et élaborer des orientations stratégiques pragmatiques en la matière tout en développant des solutions révolutionnaires afin de relever le défi permanent de la sécurité.

Ce soutien offert à nos clients leur permet de tirer parti de nouvelles technologies en toute sécurité pour réinventer leurs modèles de croissance et se démarquer durablement de leurs concurrents. Cela illustre notre engagement à collaborer avec l'ensemble de nos clients, en partageant les connaissances opérationnelles et les renseignements de sécurité essentiels afin de réduire le risque qu'une cyberattaque soit menée à bien dans leur environnement.

Avec plus de quatre milliards de spectateurs rassemblés à l'occasion des Jeux olympiques de 2012, les Jeux de Londres ne pouvaient pas se permettre le moindre incident de sécurité. Nous avons relevé le défi haut la main. Et réitéré cet exploit aux Jeux de Rio en 2016.

Pendant les Jeux olympiques, la plate-forme SIEM d'Atos a reçu plus de 255 millions de messages syslog.

4,5 millions d'événements significatifs ont été identifiés parmi ces messages bruts.

Pour 5 324 événements, la plate-forme SIEM a soumis des incidents internes à l'évaluation des SOC.

686 de ces incidents internes ont été portés à la connaissance des sites sous la forme de tickets d'assistance.

Pendant les Jeux olympiques, aucun incident de sécurité n'est venu perturber le déroulement des compétitions.

Découvrez comment nous renforçons votre sécurité pour que vous puissiez vous concentrer sur le succès de vos activités.

Pour plus d'informations, contactez-nous à l'adresse **security@atos.net** ou visitez la page **atos.net/security**.

À propos d'Atos

Atos SE (Societas Europaea) est une entreprise leader dans le secteur des services numériques, avec 100 000 collaborateurs environ dans 72 pays et un chiffre d'affaires annuel pro forma d'environ 12 milliards d'euros. Au service d'une clientèle mondiale, le groupe propose des services de conseil et d'intégration de systèmes, des services managés et des solutions d'externalisation des processus métier (EPM), des opérations cloud, des solutions de gestion des grands volumes de données (Big Data) et de cybersécurité, ainsi que des services transactionnels par le biais de Worldline, leader européen des services de paiements et de transactions. Disposant d'une expertise technologique solide et d'une connaissance approfondie du secteur, le groupe compte des clients issus de divers secteurs d'activité : défense, services financiers, santé, industrie, médias, services aux collectivités, secteur public, commerce de détail, télécommunications et transport.

Atos se concentre sur les technologies métier synonymes de progrès, qui aident les entreprises à façonner leur avenir. Coté sur le marché Euronext Paris, le groupe est le partenaire informatique mondial des Jeux olympiques et paralympiques. Atos exerce ses activités sous les noms de marque Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify et Worldline.

Pour en savoir plus :
atos.net
ascent.atos.net

Ensemble, ouvrons le débat.

À propos d'Intel Security

McAfee fait désormais partie d'Intel Security. Au travers de sa stratégie Security Connected, de son approche innovante de la sécurité optimisée par le matériel et de McAfee Global Threat Intelligence, réseau mondial de renseignements sur les menaces, Intel Security met tout en œuvre pour développer des solutions et des services de sécurité proactifs et réputés, qui assurent la protection des systèmes, des réseaux et des équipements mobiles à usage privé et professionnel partout dans le monde. Intel Security associe le savoir-faire et l'expérience de McAfee aux innovations et aux performances reconnues d'Intel pour faire de la sécurité un élément essentiel de toute architecture et de toute plate-forme informatique. Intel Security s'est fixé pour mission de permettre à chacun de vivre et de travailler en toute sécurité dans le monde numérique.

intelsecurity.com

CT_160808_VG_Intel-security-brochure