Hewlett-Packard Entreprise France
ZA de Courtaboeuf
1 Avenue du Canada
91937 Les Ulis Cedex

hpe.com

Communiqué de presse

Hewlett Packard Enterprise mène la transformation de l'industrie de la cyberdéfense grâce à une approche « built it in » et « stop it now »

Une nouvelle architecture de référence, de nouvelles offres et partenariats permettent aux entreprises de renforcer leur sécurité et arrêter net les attaques

Contact presse

Aurélie Chambon
Interfuse
aurelie.chambon@interfusecomms.com
Tel : 33(0) 1 53 32 56 88

Boulogne, le 1er mars 2016 – A l' occasion de la conférence RSA, Hewlett Packard Enterprise annonce de nouvelles offres de sécurité afin d'aider les organisations à bâtir au sein de leurs entreprises des protections et arrêter les attaques grâce à des capacités de détection et d'intervention complètes. Annonçant une nouvelle architecture de référence cyber reference architecture, des offres de sécurité mobile et un écosystème élargi de partenaires, HPE Security aide les organisations à concevoir des processus de sécurité et de gestion des risques dans les opérations informatiques pour répondre à un ensemble de menaces actuelles sophistiquées et offrir un environnement plus sûr adapté aux besoins de l'entreprise de demain.

Avec l'émergence de l'Internet des Objets, la croissance rapide des systèmes numériques et convergés, les professionnels de la sécurité sont mis au défi de protéger les actifs business critiques sans ralentir l'innovation. Selon IDC, l'évaluation des dispositifs IoT ainsi que la nécessité d'atténuer les risques qui leur sont liés incite les organisations à obtenir de la visibilité sur le trafic réseau généré par ces appareils connectés. IDC prévoit que ce soit un moteur important de la croissance dans le segment des informations de sécurité et de gestion des événements de 1,7 milliard de dollars en 2014 à 2,6 milliards de dollars en 2019, alors que les organisations cherchent à accroître leur capacités de sécurité et d'analyse dans les déploiements de technologies émergentes[1].

« *L'approche sécurité traditionnelle qui se focalise uniquement sur la défense du réseau et le contrôle du périmètre s'est avérée insuffisante face à l'évolution actuelle du paysage des menaces* », a déclaré Sue Barsamian, Sénior Vice-président senior et *Directeur Général de l'entité HPE Security Products de Hewlett Packard Enterprise.*

«Les organisations ont besoin d'une feuille de route de risque et de résilience qui va au-delà de cette approche traditionnelle. Elles renforcent la sécurité dans l'ensemble de leur système informatique – depuis l'infrastructure jusqu'aux applications et aux données – grâce à des capacités de détection et d'intervention complètes, qui guideront la prochaine génération d'opérations de sécurité axées sur le renseignement. »

Bâtir un cadre pour construire la cyber-résilience

Alors que les entreprises doivent gérer les risques au mieux dans un contexte de menaces qui évolue rapidement, HPE introduit l'architecture de référence HPE Cyber Reference Architecture (ARC). Il s'agit d'un cadre structurel de sécurisation globale de l'entreprise, conçu pour aider à construire des organisations résilientes, capables de stopper les menaces actuelles de sécurité les plus complexes. Composée de 12 domaines, 63 sous-domaines et plus de 350 fonctions de sécurité distinctes, l'architecture de référence HPE Cyber Reference Architecture propose des solutions aux défis actuels les plus complexes en matière de cyber-sécurité, y compris le cloud, la mobilité, Machine-to-Machine (M2M) et l'Internet des Objets (IoT).

«Face à la croissance du nombre de menaces actuelles et à leurs complexités dans les technologies émergentes, les entreprises sont aujourd'hui mises au défi de l'identification et de la gestion des risques tout en gardant leur rythme d'innovation», a déclaré Art Wong, Senior Vice-Président, HPE Security Service, Hewlett Packard Enterprise. " HPE Cyber Reference Architecture fournit aux organisations un cadre pour la résilience, s'appuyant sur 350 architectures de sécurité différentes portant sur les éléments de base et les initiatives nécessaires pour renforcer la sécurité et arrêter les attaques."

Sécuriser l'environnement mobile

HPE dévoile les résultats d'une étude selon laquelle plus de la moitié des applications mobiles collectent des quantités inquiétantes de données utilisateurs, sans pour autant prendre les mesures nécessaires pour protéger ces informations sensibles. L'étude s'est appuyée sur HPE Security Fortify on Demand afin de passer au crible plus de 36 000 applications mobiles iOS et Android. Elle montre l'impact de la collecte croissante des données et propose des recommandations aux organisations, aux entreprises et aux développeurs pour transformer leurs approches sur la sécurité afin de mieux protéger leurs données.

Afin d'aider les organisations à atteindre le but d'une sécurisation totalement intégrée au sein des applications mobiles, HPE annonce également HPE SecureData Mobile, une solution de cryptage des données de bout-en-bout, destinée à protéger les informations sensibles échangées dans les environnements mobiles. Cette offre permet aux organisations d'intégrer dans les applications mobiles des mécanismes de sécurisation des données et de protéger celles-ci tout au long de leur existence – qu'elles soient dormantes, en cours de transfert ou d'utilisation – et d'étendre la

sécurité au-delà des technologies classiques telles que le protocole TLS, le déploiement de réseaux VPN et le chiffrement de stockage. Cette offre s'appuie également sur HPE Format-Preserving Encryption, un cryptage basé sur des standards, qui permet d'apporter des modifications minimes aux applications existantes, tout en assurant la sécurisation des données pour les applications mobiles et les achats réalisées sur des mobiles.

Elargir l'écosystème d'HPE ArcSight pour amplifier la détection et la réponse aux menaces

Le contenu du programme Technology Alliances Partner (TAP) autour du portefeuille de solutions HPE ArcSight a augmenté de 30 % depuis un an. Aujourd'hui, HPE annonce plusieurs nouveaux partenariats stratégiques ArcSight-powered qui favorisent la collaboration entre des leaders de l'industrie dans le domaine de la sécurité, afin de déployer un modèle de sécurité « stop it now » global aux capacités de défense maximales :

- **HPE Security ArcSight & HPE Security Services: une defense unie**
  HPE a annoncé l'évolution continue de son portfolio Threat Defense Services, qui qui intègre des outils de supervision de la sécurité et des services de sécurité managés Security Information and Event Management (SIEM) s'appuyant sur HPE ArcSight. Les améliorations apportées au portfolio de services comprennent des services d'alerte automatisés pour la sécurité, des investigations et interventions, des solutions d'analyses de logiciels malveillants, de comportements des utilisateurs et du profilage des attaquants.

- **HPE & Aruba ClearPass: la mobilité sécurisée**
  HPE Security ArcSight a désormais une intégration bidirectionnelle plus forte avec Aruba ClearPass. S 'appuyant sur la capacité de HPE Security ArcSight à traiter l'ensemble des appareils, des utilisateurs et des événements provenant de ClearPass, la solution HPE leader du marché en matière de gestion de la politique de réseau, ArcSight offre désormais une analyse de la sécurité pour mettre en quarantaine ou supprimer les points d'accès via ClearPass lorsqu'un comportement malveillant est détecté.

- **HPE Security ArcSight et vArmour : sécuriser le cloud d'entreprise**
  Pendant longtemps, il a été difficile d'effectuer le suivi et l'analyse de l'activité des applications hébergées dans des datacenters virtualisés ou dans le cloud. Avec vArmour DSS, les utilisateurs d HPE Security ArcSight ESM disposent d'une totale visibilité sur la communication des applications et sur chaque charge de

travail, qu'il s'agisse d'un cloud privé ou public. De plus, les organisations seront capables de répondre en temps réel aux menaces identifiées par HPE ArcSight ESM en effectuant des changements dans leurs politiques de sécurité avec la micro-segmentation applicative de vArmour, et de stopper les attaques.

- **HPE Security ArcSight et Fortinet : élargir la visibilité sur les appareils**
  Le couplage entre HPE Security Logger et Fortinet FortiGate va créer un ensemble de solutions de sécurité innovantes et évolutives proposées par deux leaders de la sécurité, qui va au-delà du pare-feu afin de donner une visibilité en profondeur sur tous les équipements déployés au sein de l'organisation. Grâce à ce partenariat, les entreprises peuvent collecter, stocker et analyser des informations de sécurité, et accélérer ainsi leurs actions d'investigation et de recherche, tout en répondant aux attentes de leurs contraintes règlementaires

- **HPE Security ArcSight & IT-ISAC: partager les renseignements**
  HPE Threat Central, une plateforme de renseignement de sécurité communautaire qui inclut la notation et l'analyse des menaces dynamiques, a été sélectionnée par l'organisation IT-ISAC en tant que principale plateforme pour le partage et l'analyse des menaces afin d'échanger des connaissances avec ses membres. Avec son approche agnostique vis-à-vis des produits et le support des standards de l'industrie comme STIX ou TAXII, HPE Threat Central apporte des renseignements pertinents et générateurs d'actions à la fois sur des interfaces de machine-à-machine et d'homme-à-homme.

- **HPE Security ArcSight & PwC: améliorer la visibilité réseau**
  La practice Cyber Security de PwC va désormais intégrer la solution HPE DNS Malware Analytics (DMA) dans son portfolio. Les organisations clientes de PwC pourront enrichir la visibilité sur leur réseau, détecter et identifier plus facilement les serveurs infectés par des logiciels malveillants, des bots ou toute autre menace inconnue.

Des informations complémentaires sur les solutions et les services de sécurité de HPE sont disponibles sur le stand HPE n°3411 sur la RSA Conférence. Mercredi 2 mars à 23h40, Martin Fink, Executive Vice-Président Exécutif et CTO de Hewlett Packard Enterprise, animera une keynote dévoilant des approches radicalement nouvelles et des architectures pour protéger les données destinées aux Security Operation Centers (SOC's) de prochaine génération. Pour être informé des événements de la Conférence RSA et de HPE, suivez le hashtag #RSAC et le compte @HPE_Security.

About HPE Security

HPE Security helps organizations detect and respond to cyber threats while safeguarding continuity and compliance to effectively mitigate risk and incident impact. Delivering an integrated suite of market-leading products, services, threat intelligence and security research, HPE Security helps customers proactively protect the interactions among users, applications and data, regardless of location or device. With a global network of security operations centers and more than 5,000 IT security experts, HPE Security empowers customers and partners to safely operate and innovate while keeping pace with the speed of today's idea economy. Find out more about HPE Security at https://www.hpe.com/us/en/solutions/security.

Rejoignez HPE Software sur LinkedIn et suivez @HPE_Software sur Twitter. Pour en savoir plus sur les produit et services proposés par HPE Enterprise Security, suivez @HPE_Security sur Twitter, et rejoignez le groupe HPE Enterprise Security sur LinkedIn.

À propos de Hewlett Packard Enterprise

Hewlett Packard Enterprise est une entreprise leader dans l'industrie des technologies qui permet à ses clients d'aller plus loin, plus vite. Avec l'offre la plus complète du marché, allant du cloud computing, aux datacenters en passant par les solutions de travail collaboratif, nos technologies et nos services aident nos clients à travers le monde à améliorer l'efficacité, la performance et la sécurité de leurs systèmes d'information.

[1]*IDC, Worldwide Security and Vulnerability Management Forecast, 2015–2019, Doc # 259615, October 2015*

Forward-Looking Statements

This document contains forward-looking statements within the meaning of the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Such statements involve risks, uncertainties and assumptions. If such risks or uncertainties materialize or such assumptions prove incorrect, the results of Hewlett Packard Enterprise could differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements, including any statements of the plans, strategies and objectives of Hewlett Packard Enterprise for future operations; other statements of expectation or belief; and any statements of assumptions underlying any of the foregoing. Risks, uncertainties and assumptions include the possibility that expected benefits may not materialize as expected and other risks that are described in Hewlett Packard Enterprise's filings with the Securities and Exchange Commission, including but not limited to the risks described in Hewlett Packard Enterprise's Registration Statement on Form 10 dated July 1, 2015, as amended August 10, 2015, September 4, 2015, September 15, 2015, September 28, 2015 and October 7, 2015. Hewlett Packard Enterprise assumes no obligation and does not intend to update these forward-looking statements.