Unit 42 : services de Threat Intelligence et de réponse aux incidents

Toujours informés. Toujours prêts.

Une expérience incomparable

Qu'il s'agisse de répondre à une compromission ou de gérer les cyber-risques, nous comprenons vos défis. Issus d'agences gouvernementales américaines, des forces de police et de grands acteurs privés de la sécurité, les conseillers Unit 42 sont intervenus sur certains des cas de compromission les plus marquants de l'histoire. Notre équipe de réponse aux incidents (IR) est l'une des plus sollicitées au monde, avec plus de 1 300 incidents traités par an. Cette manne d'expérience exceptionnelle nous sert à développer nos solutions de gestion du risque et à baser nos évaluations et recommandations sur les vecteurs d'attaque observés chaque jour dans les entreprises. Nos équipes ont réalisé des milliers de bilans de cyber-risque et collaboré avec des structures du monde entier pour identifier et neutraliser les cybermenaces.

Une équipe rapide et efficace

Nous agissons rapidement dans l'intérêt de nos clients. Du déploiement à la livraison de nos conclusions, en passant par l'analyse, tout est fait pour répondre en un temps record. Quelques minutes suffisent pour mobiliser des équipes IR dotées des compétences nécessaires – consultants forensiques, analystes de malwares, chefs d'équipe, etc. Nous œuvrons rapidement pour endiguer et investiguer les menaces, puis pour coordonner notre réponse. Et nous travaillons avec vous pour faire le point sur la situation et vous aider à prendre les bonnes décisions pour revenir rapidement à la normale. Dans nos missions de gestion des risques, nous savons que les dépenses de sécurité représentent un investissement pour nos clients. C'est pourquoi nous veillons à prendre en compte les priorités de vos budgets de sécurité afin d'obtenir le meilleur retour sur investissement en termes de réduction des risques. Nous fournissons des solutions dans les délais, dans les budgets et avec un maximum d'impact.

Une innovation continue et des technologies avancées

La lutte contre des menaces en perpétuelle évolution passe par une innovation constante et des technologies de pointe. Chez Palo Alto Networks, nous sommes fiers des efforts de recherche, de développement et de créativité que nous déployons pour résoudre les problématiques de sécurité de nos clients. Nous développons continuellement des solutions technologiques ultra-puissantes de prévention des menaces, de détection et de réponse aux incidents. Nous plaçons le cloud et les technologies IA/ML au service de nos équipes pour leur permettre d'intervenir auprès d'entreprises d'envergure mondiale en quelques minutes seulement. Nos produits permettent à Unit 42 de déployer nos solutions plus rapidement, de traquer la menace plus efficacement, d'effectuer des investigations plus poussées et de neutraliser complètement les attaques.

Pour plus d'informations, rendez-vous sur www.paloaltonetworks.com/unit42.

15
années d'expérience en moyenne

> 1 000
dossiers en 2021

24h/365j
de disponibilité pour la réponse aux incidents

Unit 42 : services de Threat Intelligence et de réponse aux incidents

Réponse aux incidents

Réponse aux incidents

Investigation des compromissions de messagerie professionnelle (BEC)
Réponse et récupération suite à des accès non autorisés à votre environnement de messagerie professionnelle. Endiguement de l'incident ; identification de la cause racine, de la fenêtre de compromission et des activités malveillantes ; quantification des données sensibles exposées.

Investigation des ransomwares
Réponse et récupération suite à une attaque par ransomware. Endiguement de la menace ; identification de la cause racine, de la fenêtre de compromission et des activités malveillantes ; quantification des données sensibles exposées. Si besoin, négociation avec les cybergangs, récupération et validation des clés de déchiffrement, et mise en œuvre d'un plan de reprise.

Réponse aux incidents cloud
Réponse et récupération suite à une attaque cloud. Endiguement de la menace ; identification du vecteur d'attaque initial, de l'étendue des accès non autorisés, des données exfiltrées et des systèmes à restaurer. Définition et implémentation de protections supplémentaires.

Compromission des applications web
Réponse et récupération suite à une attaque web. Endiguement de la menace, analyse des journaux, revue de code, quantification des données sensibles exposées ou perdues, et recommandations pour les mesures de renforcement.

Investigation des menaces persistantes avancées (APT)
Réponse et récupération suite à un incident causé par une menace APT. Endiguement de la menace ; identification de la cause racine, de la fenêtre de compromission et des activités malveillantes ; quantification des données sensibles exposées.

Investigation PCI
Réponse et récupération suite à une compromission de carte bancaire. Suivi du processus PCI. Endiguement de la menace ; identification de la cause racine, de la fenêtre de compromission et des activités malveillantes ; quantification des données PCI exposées.

Analyses des malwares
Analyse d'échantillons de malware à l'aide d'une CTI open-source, sandboxing, retroingénierie, et remise d'un rapport détaillant le comportement et les fonctionnalités du malware.

Data mining
Identification et quantification de données sensibles (PHI, PII, PCI, et autres informations sensibles et réglementées) potentiellement exposées suite à une compromission, dans le cadre d'une procédure de notification des autorités compétentes.

Gestion des cyber-risques

Conseils stratégiques

Conseils aux CA et RSSI
Évaluation et examen des cyber-risques, création d'un état des lieux et élaboration d'une stratégie de sécurité à présenter au Comex et au conseil d'administration.

Audit de cybersécurité préalable aux fusions-acquisitions (Due Diligence)
Évaluation des personnes, des processus et des technologies pour identifier les failles, mettre en évidence les risques de sécurité cachés et obtenir un bilan indépendant du niveau de maturité global du programme InfoSec dans le contexte d'une fusion ou d'une acquisition.

Évaluation des cyber-risques
Évaluation des risques de sécurité sur la base d'un framework ou d'exigences réglementaires (NIST, CIS, ISO, CCPA, HIPAA, etc.) pour dresser un état des lieux des contrôles et des failles, puis créer un plan stratégique de renforcement du programme InfoSec.

Évaluations proactives

Évaluation de compromission
Recherche d'indicateurs de compromission (IoC) passés ou présents pour recueillir les preuves d'accès ou d'activité non autorisés (cloud, e-mails, terminaux).

Évaluation du centre opérationnel de sécurité (SOC)
Services de conception et de conseil pour la mise en place d'un SOC de nouvelle génération.

Bilan de sécurité du cloud
Évaluation des contrôles dans l'environnement cloud (calcul et services), des configurations de sécurité et des politiques d'identification des risques de sécurité.

Évaluation des risques de la supply chain
Évaluation des risques de sécurité relatifs aux fournisseurs et sous-traitants pour identifier et neutraliser les menaces ciblant la supply chain.

Évaluation de l'état de préparation aux compromissions de messagerie professionnelle (BEC)
Évaluation ciblée des contrôles et des personnes, processus et technologies nécessaires pour contrer les menaces BEC et autres attaques par e-mail.

Évaluation de l'état de préparation aux ransomwares
Recommandations de renforcement des contrôles, de mesures correctives et de bonnes pratiques pour atteindre vos objectifs de préparation aux ransomwares.

Simulation d'incidents

Exercices de simulation
Simulation de votre réponse à un incident de sécurité majeur au travers de scénarios personnalisés, basés sur des compromissions réelles et des menaces spécifiques à votre secteur.

Exercices Purple Team
Équipe Unit 42 chargée de lancer une attaque en conditions réelles pour identifier les vulnérabilités de vos systèmes d'alerte, renforcer vos défenses et améliorer vos opérations de sécurité.

Tests d'intrusion
Tests permettant de mesurer l'efficacité de vos contrôles et de votre sécurité réseau face aux modes opératoires déployés par les acteurs cyber pour compromettre votre environnement et s'y implanter durablement.

Unit 42 : services de Threat Intelligence et de réponse aux incidents (suite)

Réponse aux incidents

Analyses forensiques

Investigation numérique
Collecte de données forensiques, analyse, restauration et rapport rédigé sur la base d'informations collectées sur des supports numériques à l'aide de méthodes scientifiques, l'objectif étant de reconstituer le déroulement d'une attaque ou la manière dont le support a été utilisé.

Investigation des menaces internes et enquête sur des salariés sur le départ
Investigation sur l'utilisation abusive d'accès privilégiés accordés à des salariés considérés comme dignes de confiance (identification des données consultées ou des actions détournées et/ou indésirables prises par des collaborateurs internes, etc.).

Analyses des données structurées
Collecte et analyse des environnements de bases de données SQL et NoSQL, y compris les journaux externes.

Témoignage/Expertise judiciaire/ Assistance juridique
Examen des preuves numériques, témoignage, déposition et rédaction d'un rapport d'expert à présenter aux autorités compétentes (commission, tribunal, etc.).

Gestion des cyber-risques

Bilan de préparation à une compromission
Évaluation des personnes, processus et technologies nécessaires pour répondre efficacement aux menaces, et définition d'une feuille de route stratégique pour atteindre l'état de préparation souhaité.

Threat Intelligence et consulting sécurité

Conception d'un programme de sécurité
Conception de cadres de gouvernance, de modèles opérationnels et d'une feuille de route pour votre programme InfoSec (politiques et standards, framework de contrôle, stratégie de défense en profondeur, etc.).

RSSI virtuel
RSSI par intérim ou à temps partiel chargé d'identifier les cyber-risques et de développer votre programme InfoSec. Le RSSI virtuel établit une stratégie de cyberdéfense et travaille avec les équipes IT, de sécurité et de direction pour répondre aux questions relatives à la posture de sécurité de l'entreprise.

Élaboration d'un plan de réponse aux incidents
Service d'évaluation et de conseil sur l'état de préparation de votre équipe face aux attaques par ransomware : prévention, détection, réponse et reprise d'activité.

Session d'information sur les menaces
Briefing stratégique délivré par un analyste Unit 42 pour vous offrir une vue personnalisée des menaces pour votre entreprise, avec un accès à des données détaillées sur les terminaux, le réseau et le cloud.

Contrat d'astreinte Unit 42

Serez-vous prêt en cas d'incident de sécurité majeur dans votre entreprise ? La rapidité de votre réponse, l'efficacité de vos outils et la précision de vos playbooks détermineront la vitesse à laquelle vous reprendrez le cours normal de vos opérations. Avec les services Unit 42 de réponse aux incidents et de gestion des cyber-risques, votre équipe n'est plus seule pour affronter la crise.

Des menaces internes aux groupes étatiques, en passant par les opérations du crime organisé, Unit 42 réalise plus de 1 000 missions de réponse à incident par an. Avec le contrat d'astreinte d'Unit 42, vous déterminez des accords de niveau de service (SLA) en amont pour accéder immédiatement à une expertise approfondie en analyse forensique et en réponse aux incidents le jour J.

Vous pouvez également allouer ces heures d'astreinte aux services Unit 42 de gestion des cyber-risques pendant la durée du contrat. Définition d'une stratégie de sécurité, évaluation des contrôles techniques en place, bilan de maturité globale de votre sécurité… nos conseillers de confiance accompagnent votre équipe dans de nombreux domaines.

À propos d'Unit 42

L'équipe Unit 42 de Palo Alto Networks rassemble des chercheurs, spécialistes IR et consultants sécurité de réputation mondiale, toujours munis de la dernière CTI et toujours prêts à aider les clients à gérer les cyber-risques de façon proactive. Forte de sa réputation et de son statut de leader de la Threat Intelligence, Unit 42 a étendu ses missions à la réponse à incident et aux services de gestion du cyber-risque. Conseillers de confiance, nos consultants vous accompagnent pour évaluer et vérifier vos contrôles de sécurité face aux menaces qui vous concernent directement. L'objectif : transformer votre stratégie de sécurité à l'aide d'une approche CTI et accélérer la réponse aux incidents. Rendez-vous sur paloaltonetworks.com/unit42.

Intégration aux programmes de cyber-assurance

Unit 42 est un fournisseur approuvé par plus de 70 grandes compagnies d'assurance. Vous désirez souscrire les services d'Unit 42 dans le cadre d'une déclaration d'incident ? Nous pouvons appliquer le tarif préférentiel en place avec la compagnie d'assurance en question. Pour bénéficier d'un tarif donné, il suffit d'en informer Unit 42 au moment de la demande de service.

Victime d'une attaque ?

Vous pensez que votre entreprise a été compromise ? Vous devez faire face à une urgence ? Contactez l'équipe Unit 42 de réponse aux incidents en écrivant à unit42-investigations@paloaltonetworks.com ou en composant l'un des numéros suivants : +1 866 486 4842 (Amérique du Nord), +31 20 299 3130 (EMEA), +44 20 3743 3660 (Royaume-Uni), +65 6983 8730 (APAC), +81 50 1790 0200 (Japon).

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam, Pays-Bas
Téléphone : +31 20 888 1883
www.paloaltonetworks.fr

© 2022 Palo Alto Networks, Inc. Palo Alto Networks est une marque déposée de Palo Alto Networks. Pour obtenir la liste de nos marques commerciales, rendez-vous sur https://www.paloaltonetworks.com/company/trademarks.html. Toutes les autres marques mentionnées dans le présent document appartiennent à leurs propriétaires respectifs.
unit42_ds_threat-intel-incident-response-services_042122-fr