CyberSecurity

Cyber Threat Intelligence

Comprendre pour anticiper les menaces ciblées

Description du service

Pour protéger nos clients des APT très ciblées, nous synthétisons les modes opératoires des attaquants pour en identifier les spécificités et en suivre l'évolution (outils et infrastructures réseaux) afin d'anticiper de futures campagnes.

Une surveillance proactive de plus de 130 groupes d'APT est opérée, grâce à laquelle nous prévenons nos clients des menaces émergentes afin qu'ils puissent prendre les meilleures dispositions pour s'en prémunir ou réduire leurs impacts.

Nous avons développé nos services de CTI pour disséminer une connaissance utile dans des formats facilitant la prise de décision, l'intégration dans vos équipements de sécurité tout en optimisant les coûts de vos équipes opérationnelles.

Bénéfice client

- Anticipation des menaces ciblant l'entreprise ou son vertical
- Recommandations pour une meilleure prise de décision
- Maintien en condition de détection des équipements
- Optimisation des coûts opérationnels

AIRBUS

Rapport exécutif sur la menace Cyber

Description : Rapports trimestriels personnalisés fournissant une vue stratégique des menaces Cyber avancées à destination des responsables sécurité informatique d'une organisation. Ces rapports offrent les renseignements nécessaires pour anticiper des décisions stratégiques et faciliter la mise en place de politiques de sécurité à l'échelle de l'organisation.

Thèmes abordés (fonction de l'actualité ou sur demande client) :

- Evolution de la menace Cyber générale
- Evolution de la menace spécifique à un vertical métier ou zone géographique,
- Risques liés à l'émergence de nouvelles technologies (IoT, ICS, Cloud, mobilité...)
- Description de groupes d'attaquants, leurs motivations, techniques, tactiques et procédures etc...

Cible : Responsable de la sécurité des systèmes d'information, membres de comité exécutif

Format : Rapport PDF

Flux de description de menaces Cyber avancées

Description : Flux de description de menaces Cyber avancées. Issu de notre base de connaissance, le flux proposé contient le résultat des analyses effectuées par notre équipe CTI sur plus de 130 groupes liés à des attaques avancées. Liant des indicateurs techniques et des éléments de contexte (TTP, motivations etc..), le flux est structuré dans des formats standards pour être facilement ingéré et utilisé par vos équipes d'analystes SOC/CERT/CSIRT/CTI dans toute la gestion de votre protection.

Contenu :

- +130 groupes d'attaquants suivis
- +150 familles de malware décrites
- 10.000 indicateurs de compromissions qualifiés et contextualisés
- Techniques, Tactiques et Procédures
- Motivations

Cible : Equipes opérationnelles de sécurité (SOC, CSIRT, CTI)

Format : MISP, STIX, CSV. Flux téléchargeable sur le portail de la CTI d'Airbus CyberSecurity

Règles et signatures de détection

Description: flux de règles et de signatures issu de notre connaissance des menaces avancées. Fournis dans plusieurs formats standards facilitant leur intégration dans les produits de sécurité courant du marché, ces flux contiennent les éléments techniques nécessaires à une détection des menaces au niveau réseau, système et journaux.
La qualification des marqueurs ainsi que les éléments de contexte fournis permettent une détection efficace et une réaction rapide des menaces APT.

Cible : Equipements de sécurité (IDS, SIEM, analyse de malware, AV, FW etc…)

Format :

- Règles et signatures SNORT, YARA, openIOC, liste d'IP / noms de domaine pour backlog dans SIEM
- Eléments de contexte pour la qualification des alertes: PDF & CSV
- Flux téléchargeable sur le portail de la CTI d'Airbus CyberSecurity

Airbus CyberSecurity
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France
Willy-Messerschmitt-Str. 1 / 82024 Taufkirchen / Germany
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / United Kingdom
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / United Arab Emirates
www.airbus-cyber-security.com / contact.cybersecurity@airbus.com