Détectez et analysez les malwares qui circulent sur vos systèmes grâce à notre plateforme Orion Malware

Les Systèmes d'Informations (SI) des entreprises et institutions font régulièrement face à des cyberattaques basées sur l'utilisation de malwares. Pour prévenir le risque, il est indispensable de pouvoir détecter les menaces, même les plus furtives, puis de les analyser afin d'y répondre de manière appropriée et limiter leur impact en cas d'incident.

Orion Malware permet de prévenir le risque et de répondre aux incidents grâce à ses moteurs de détection complémentaires et à ses rapports d'analyses actionnables. Votre chaine de sécurité est renforcée via le partage des informations avec vos autres équipements de sécurité. Orion Malware est un soutien pour toutes vos équipes de cybersécurité et s'adapte à chaque cas d'usage métier SOC, CSIRT/CERT, TI.

DÉTECTEZ LES MALWARES LES PLUS AVANCÉS

Notre solution se nourrit des fichiers transmis par les équipements de sécurité existants ou par les utilisateurs.

Les experts d'Airbus CyberSecurity ont conçu Orion Malware en intégrant des antivirus et en développant des moteurs d'analyse statique avec machine learning et d'analyse dynamique dans le but de repérer les malwares les plus furtifs dont le développement est parfois sponsorisé par les Etats.

PRÉPAREZ LA RÉPONSE À INCIDENT

Orion Malware vous fait gagner un temps précieux dans la réponse à incident grâce aux rapports d'analyse. Ceux-ci indiquent une note de risque, un résumé compréhensible par des non experts ainsi que tous les indicateurs de compromissions découverts.

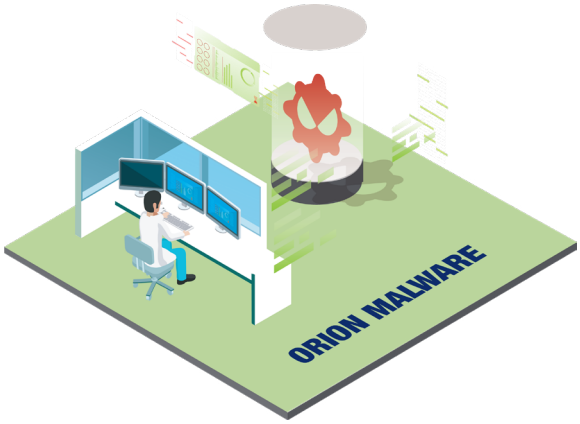
Ces rapports peuvent être exportés vers les SIEM ou SIRP des équipes SOC ainsi que les TIP des équipes de threat intelligence.

ORION MALWARE REMPLIT 3 FONCTIONS ESSENTIELLES :

DÉTECTER ET ANALYSER
les menaces connues et encore inconnues

SÉCURISER
vos SI en partageant des indicateurs de compromission

SOUTENIR
toutes vos équipes engagées dans la cyber protection



AIRBUS

LES FONCTIONNALITÉS CLÉS D'ORION MALWARE

Analyse combinée : statique, dynamique, heuristique et intelligence artificielle

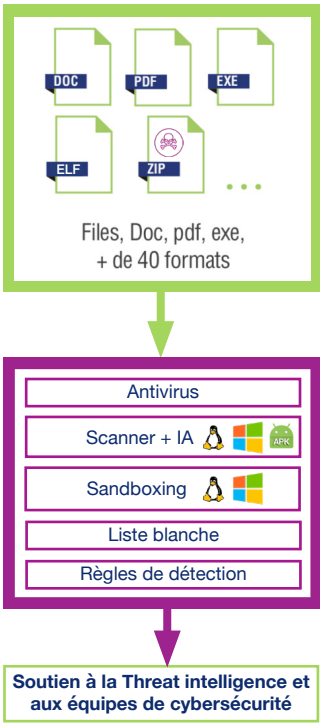
- Cinq antivirus pour la détection instantanée des malwares connus
- Détonation en Sandbox souveraine avec système anti-évasion et hooking indétectable pour les malwares avancés ou inconnus
- Liste blanche pour la détection instantanée des fichiers certifiés sains
- Fonction Scanner d'analyse statique avancée basée sur des modèles d'heuristiques et de machine learning (IA)
- Fonction d'identification des langages de script par Deep learning (IA)
- Moteur d'analyse basé sur vos propres règles de détonation au format Yara, OpenIOC et Python

Une plateforme ouverte et modulaire pour répondre précisément à vos besoins

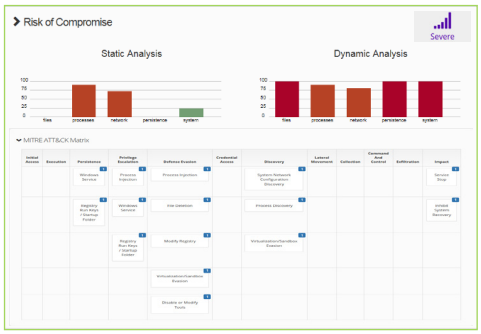
- Configuration des workflows d'analyse (activation/désactivation des moteurs, durée d'analyse, choix par défaut de la VM de détonation, extraction des PCAP, choix du navigateur, etc)
- Management des heuristiques dynamiques et comportementales et des modèles IA

Une intégration facilitée et un soutient à vos services de Threat Intelligence

- Interface Web dédiée à l'analyse par les utilisateurs et l'administrateur de la solution
- API REST et ICAP pour une analyse automatisée depuis vos équipements réseaux
- Export des analyses au format SYSLOG pour une exploitation par votre SIEM (Splunk, QRadar, ELK)
- Partage de la Threat Intelligence avec export des IOC et de règles de détection au format OpenIOC



Des rapports d'analyses complets



- **Analyse des impacts** sur le système infecté et production de rapports
- **Indicateurs global de dangerosité** pour une prise de décision rapide
- **Rapport complet** des antivirus et des analyses statique et dynamique
- Classification **MITRE ATT&CK** et **timeline**
- Liste exhaustive des **indicateurs de compromission**
- Liste des **payloads détectés**

Une offre complète adaptée à vos besoins cyber

4 modèles d'appliance (S, M, L et XL) selon la puissance d'analyse requise

Tous nos modèles bénéficient des **mêmes capacités de détection**

Bénéficier des mêmes capacités de détection qu'avec notre appliance grâce à **notre offre Cloud**. Nous proposons une large variété d'abonnements pour répondre à l'ensemble de vos besoins

Mise à jour des versions et du package de détection (base antivirale et heuristique de détection).

Support technique et fonctionnel (FR/EN). **Trois formations disponibles** (Analyste, Expert, Administratreur)

Orion Malware vous accompagne dans **l'intégration à votre écosystème**, la mise en place et le **développement de connecteurs spécifiques**

AIRBUS

FRANCE
Metapole 1, boulevard Jean Moulin
CS 40001 / 78996 Elancourt Cedex
France

ALLEMAGNE
Willy-Messerschmitt-Str. 1
82024 Taufkirchen
Allemagne

ROYAUME-UNI
Quadrant House / Celtic Springs
Coedkernew / South Wales
NP10 8FZ / Royaume-Uni

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com