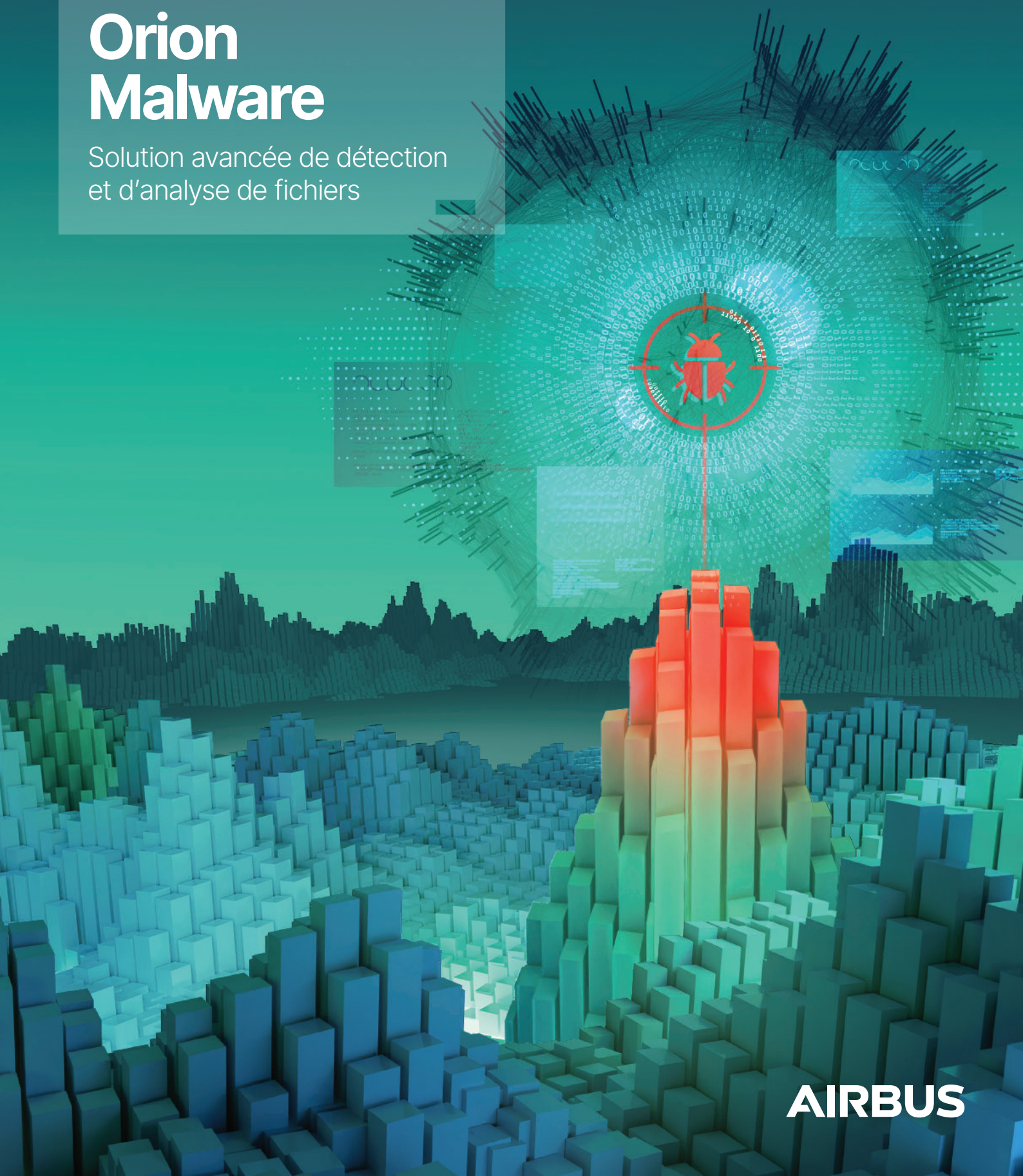
DEFENCE AND SPACE
Cyber

Orion Malware

Solution avancée de détection et d'analyse de fichiers



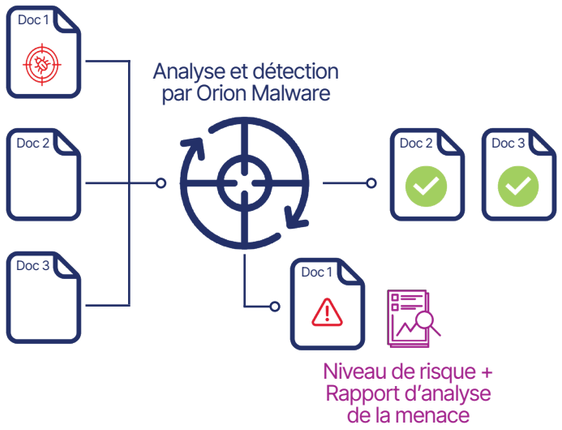
AIRBUS

Protégez vos organisations et systèmes des attaques par fichiers

LABEL FRANCE CYBERSECURITY 2022

Orion Malware **détecte les attaques par fichiers**, connues et inconnues, grâce à un **ensemble de moteurs d'analyses** combinant heuristiques, base de signatures, IA et analyse dynamique.

Déployable sur un serveur physique ou en tant que SaaS, Orion Malware est un soutien pour toutes vos équipes de cybersécurité et s'adapte à chaque cas d'usage métier SOC, CSIRT/CERT, ou TI.



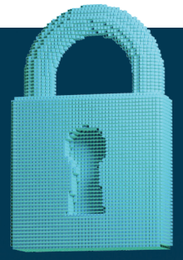
DÉTECTEZ LES MALWARES LES PLUS AVANCÉS

Les experts d'Airbus Defence and Space Cyber ont conçu Orion Malware en intégrant des antivirus et en développant des moteurs d'analyse statique avec Intelligence Artificielle (IA), et d'analyse dynamique dans le but de repérer les malwares les plus avancés.

GAGNEZ DU TEMPS D'ANALYSE

Orion Malware vous fait gagner un temps précieux en effectuant une analyse en profondeur de la menace et en fournissant des rapports détaillés incluant un niveau global de risque, les tactiques et techniques des malwares ainsi que l'export des Indicateurs de Compromission (IOC) pour prévenir les futures attaques ou les contenir en cas d'incident.

Les résultats d'analyses peuvent être envoyés automatiquement via notre connecteur syslog vers différents outils de votre chaîne de détection Cyber.



ORION MALWARE REMPLIT 3 FONCTIONS ESSENTIELLES

Détecter et analyser

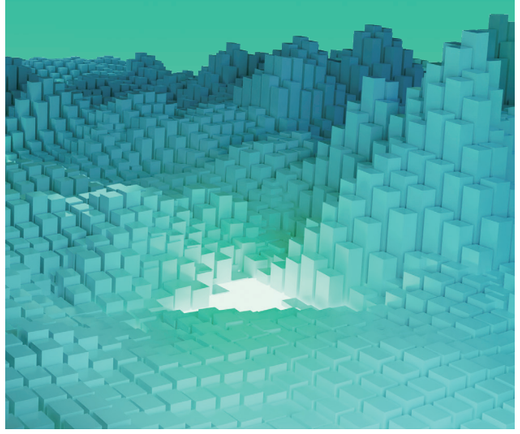
les menaces connues et non connues

Sécuriser

vos SI en partageant des indicateurs de compromission

Soutenir

toutes vos équipes engagées dans la cyber protection



Disponible dans deux versions en fonction de vos besoins en sécurité

Orion Malware est disponible en version 'All in One' incluant tous les moteurs d'analyse pour obtenir le meilleur de la détection cyber et en version 'Multi AV' pour une analyse rapide de premier niveau.

MOTEURS DE DÉTECTION	ALL IN ONE	MULTI-AV
Analyse Antivirus (jusqu'à 5 antivirus inclus)	✓	✓
Analyse Réputation (liste blanche + liste noire)	✓	
Analyse statique Scanner + IA	✓	
Règles YARA et Python	✓	
Analyse dynamique / comportementale (sans agent) pour Windows et Linux	✓	

Orion Malware propose deux portails d'accès pour s'adapter à tous types d'utilisateurs.

PORTAIL EXPERT : les équipes de cyber sécurité accèdent à toutes les fonctionnalités. Par exemple, ils peuvent définir le workflow d'analyse, rechercher et consulter des rapports complets, exporter des IoC, rejouer l'analyse, exporter un « dump » mémoire, etc.

PORTAIL LITE : les utilisateurs sans expertise préalable dans le domaine de la cyber sécurité peuvent vérifier les fichiers avant de les utiliser en cas de doute. Ils deviennent acteurs de la cyber sécurité de leur organisation. Le portail permet aux utilisateurs de soumettre leurs fichiers et d'obtenir un résultat simplifié.

Orion Malware répond à différents cas d'usage

PROTECTION DES SI CONTRE LES MENACES AVANCÉES ET RANSOMWARES

Qui l'utilise ?
RSSI, équipes Cyber et administrateurs ITT

Dans quel but ?
Améliorer la sécurité du SI pour se protéger efficacement contre les Ransomware ou des menaces plus avancées (APT)

Analyse automatique des fichiers via l'intégration avec firewall, proxy, sonde réseau, EDR, serveur de messagerie

Quels bénéfices ?
Détecter la menace et permettre de la bloquer

Mettre en place une chaine de détection complète

Permettre aux équipes cyber d'agir avant la compromission, le vol ou la destruction de données

INCIDENT DE SÉCURITÉ

Qui l'utilise ?
Analystes SOC et équipes CSIRT

Dans quel but ?
Levée de doute sur un ou plusieurs fichiers

Recherche d'indicateurs de compromission

Quels bénéfices ?
Détection des menaces connues et inconnues les plus avancées

Fournir une alternative aux services d'analyse en ligne non confidentiels
Gain de temps pour les équipes SOC et CSIRT avec une analyse approfondie en quelques minutes

Rapport d'analyse complet pour trouver rapidement les indicateurs de compromission les plus pertinents afin d'enrichir la base de connaissance

ANALYSE APPROFONDIE DES MALWARES

Qui l'utilise ?
Experts en analyse de malwares

Dans quel but ?
Comprendre le fonctionnement d'un malware et les techniques utilisées

Qualifier précisement le niveau de dangerosité d'un malware

Quels bénéfices ?
Permet un gain de temps important

Analyse comportementale (dynamique) approfondie avec un haut niveau de détails sur les activités du malware

Récupération de toutes les écritures du memory dump pour compléter l'analyse avec des outils tiers

Personnalisation de la détection comportementale

Fonctionnalités clés d'Orion Malware

Des moteurs d'analyse combinés de type statique et dynamique basés sur des heuristiques et des modèles de détection IA

- Cinq antivirus pour la détection des malwares connus
- Analyse dynamique des menaces les plus sophistiquées et inconnues dans un environnement virtuel sécurisé doté d'une technologie d'introspection indétectable par les malwares
- Double liste de réputation personnalisable pour identifier instantanément les fichiers légitimes (White List) et malveillants (Black list)
- Fonction Scanner d'analyse statique avancée basée sur des modèles d'heuristiques et d'intelligence artificielle
- Moteur d'analyse basé sur vos propres règles de détonation au format Yara, OpenIOC et Python

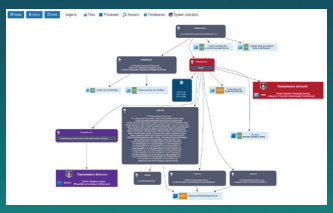
Une plateforme ouverte et modulaire

- 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

Intégration facilitée et soutien à vos services Threat Intelligence

- Portails Web spécifiques pour les fonctions d'analyse des fichiers et d'administration de la solution
- API REST et ICAP pour une analyse automatisée depuis vos équipements réseaux
- Export des résultats d'analyses au format SYSLOG pour les levées d'alerte au niveau du SIEM (Splunk, QRadar, ELK)
- Partage de la Threat Intelligence avec export des IOC et règles de détection au format STIX 2.1, MISP, CSV, OpenIOC
- Solution 100% fonctionnelle en mode déconnecté pour les environnements isolés
- Sécurisez vos pièces jointes avec le connecteur Orion Malware pour MS-Exchange
- Intégration avec l'EDR HarfangLab

RAPPORTS D'ANALYSE COMPLETS



- Indicateur global de dangerosité
- Analyse comportementale du malware
- Classification MITRE ATT&CK
- Indicateurs de compromission

NOTRE PARTENAIRE

GORILLE
CYBER-SECURITY SOFTWARE BY CYBER DETECT©

"Gorille" est un moteur de détection novateur qui réalise une analyse dite polymorphique des fichiers exécutables grâce à des modèles IA, des méthodes formelles et du reverse-engineering lui permettant de détecter les menaces non connues et leurs variants avec une capacité de classification. Gorille est intégré en tant que moteur additionnel au workflow d'analyse de la solution Airbus Orion Malware dans le but de couvrir un spectre toujours plus large de détection avec une précision renforcée.

UNE OFFRE COMPLÈTE ADAPTÉE À VOS BESOINS CYBER

Orion Malware dispose d'une gamme de serveurs intégrés (S, M, L, XL)

Orion Malware est également proposé sous le format d'abonnement SaaS

Mise à jour en continu du package de détection (bases antivirales, heuristiques, modèles de machine learning, templates d'analyse dynamique)

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

Airbus vous accompagne dans l'intégration d'Orion Malware à votre chaîne de cyberdéfense et le développement de connecteurs spécifiques

Airbus Defence and Space
France, Allemagne Royaume-Uni, Espagne

www.cyber.airbus.com
contact.cybersecurity@airbus.com
@Airbus Defence and Space Cyber

AIRBUS