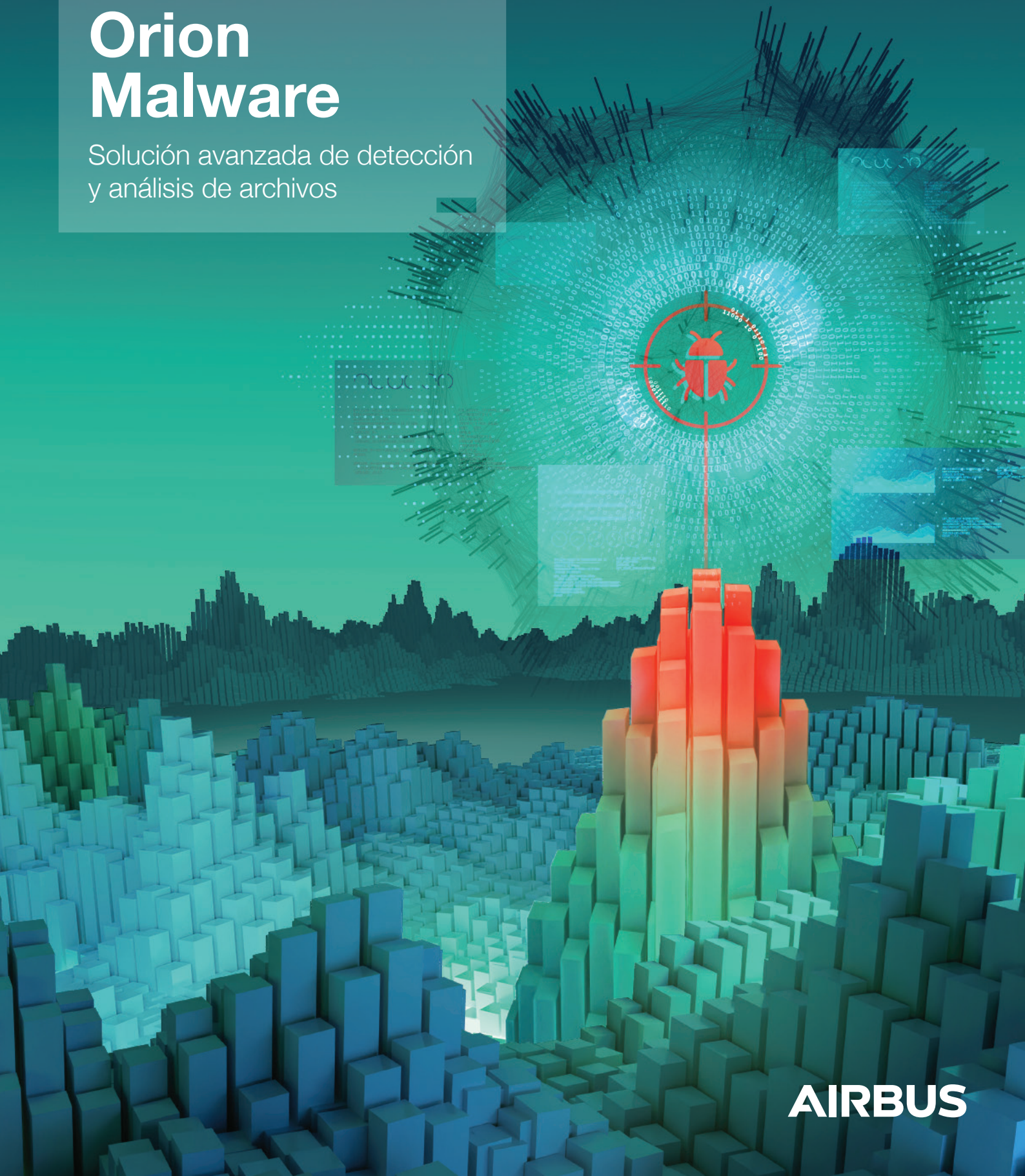
DEFENCE AND SPACE
Cyber

Orion Malware

Solución avanzada de detección y análisis de archivos



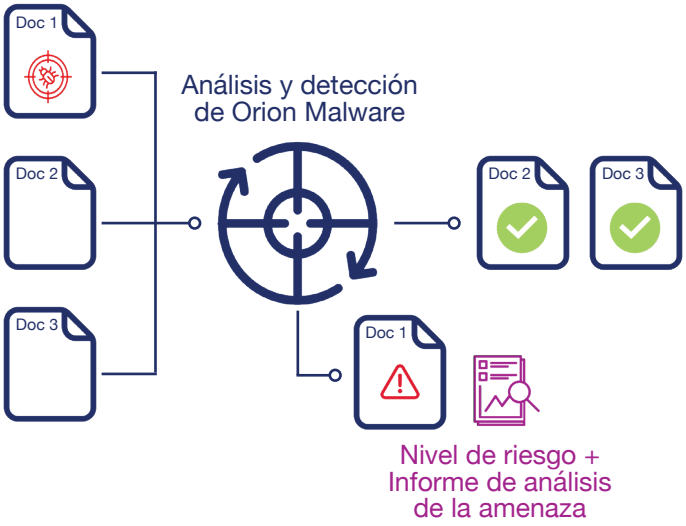
AIRBUS

Proteja sus organizaciones y sistemas de ataques con archivos

LABEL FRANCE CYBERSECURITY 2022

Orion Malware **detecta ataques con archivos**, conocidos y desconocidos, utilizando un **conjunto de motores de análisis** que combinan heurística, base de firmas, IA y análisis dinámico.

Orion Malware, **instalado en un servidor físico o como SaaS**, apoya a todos los sistemas de ciberseguridad y se adapta a cualquier caso de uso de sus equipos de SOC, CSIRT/CERT o TI.



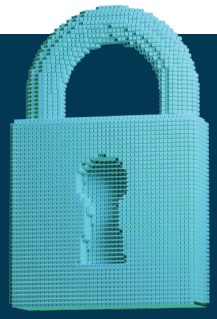
DETECTE EL MALWARE MÁS AVANZADO

Los expertos de Airbus Defence and Space Cyber han creado Orion Malware en el que han integrado antivirus y desarrollado motores de análisis estático con Inteligencia Artificial (IA) y dinámico capaz de identificar el malware más sofisticado.

MÁS CAPACIDAD DE REACCIÓN

Orion Malware le permite reaccionar con más rapidez, ya que realiza un análisis profundo de la amenaza, le proporciona informes que detallan el nivel global de riesgo y las tácticas y técnicas del malware, y exporta los indicadores de compromiso (IoC) para prevenir futuros ataques o contenerlos en caso de incidente.

Los resultados del análisis se pueden enviar automáticamente a las distintas herramientas de su cadena de detección de ciberataques utilizando nuestro conector syslog.



ORION MALWARE CUMPLE 3 FUNCIONES FUNDAMENTALES

Detectar y analizar

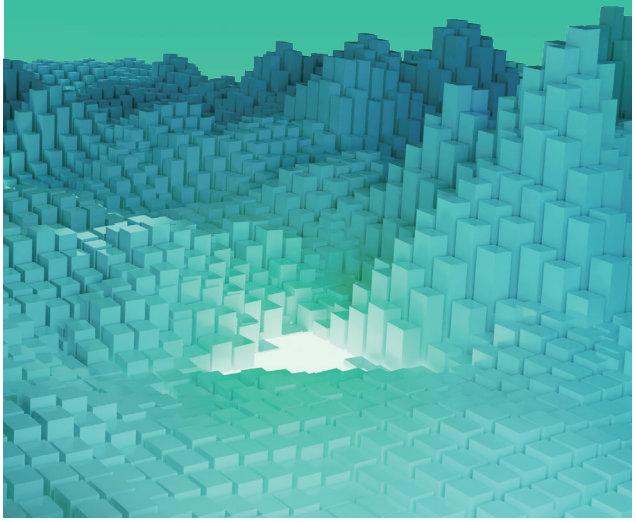
las amenazas conocidas y desconocidas

Asegurar

sus sistemas de información compartiendo indicadores de compromiso

Apoyar

a todos los equipos que se ocupan de la ciberprotección



Disponible en dos versiones según sus necesidades de seguridad

Orion Malware ofrece una versión 'All in One', que incluye todos los motores de análisis para una ciberdetección completa, y una versión 'Multi AV' que realiza un análisis rápido de primer nivel.

MOTORES DE DETECCIÓN	ALL IN ONE	MULTI-AV
Análisis antivirus (hasta 5 antivirus)	✓	✓
Análisis de reputación (lista blanca + lista negra)	✓	
Análisis estático: escáner + IA	✓	
Reglas YARA y Python	✓	
Análisis dinámico/de comportamiento (sin agente) para Windows y Linux	✓	

Orion Malware ofrece dos portales de acceso para adaptarse a todos los usuarios

PORTAL EXPERT: los equipos de ciberseguridad tienen acceso a toda la funcionalidad. Por ejemplo, pueden definir el flujo del análisis, buscar y consultar informes completos, exportar los IoC, repetir el análisis, exportar un volcado de memoria, etc.

PORTAL LITE: los usuarios sin experiencia previa en ciberseguridad pueden comprobar los archivos antes de usarlos en caso de duda. Así se implican activamente en la seguridad de su organización. Los usuarios pueden enviar sus archivos y recibir un informe simplificado con el resultado.

Orion Malware se adapta a distintos casos de uso

PROTECCIÓN DE LOS SI CONTRA AMENAZAS AVANZADAS Y RANSOMWARE

¿Quién lo utiliza?
CISO, equipos de ciberseguridad y administradores de TI

¿Con qué fin?
Mejorar la seguridad de los SI para protegerse eficazmente contra ransomware o amenazas más avanzadas (APT)Análisis automático de archivos al integrarlo con firewalls, proxys, sondas de red, EDR y servidores de correo

¿Cuáles son las ventajas?
Detecta la amenaza y permite bloquearla
Dispone de una cadena completa de detección
Permite a los equipos de ciberseguridad actuar antes del compromiso, el robo o la destrucción de los datos

INCIDENTE DE SEGURIDAD

¿Quién lo utiliza?
Analistas de SOC y equipos de CSIRT

¿Con qué fin?
Verificar la seguridad de uno o más archivos
Identificar indicadores de compromiso

¿Cuáles son las ventajas?
Detecta las amenazas conocidas y desconocidas más avanzadas
Ofrece una alternativa a los servicios de análisis no confidenciales en línea
Mayor capacidad de reacción de los equipos de SOC y CSIRT que cuentan con un análisis detallado en minutos
Informe completo del análisis para identificar con rapidez los indicadores de compromiso más relevantes y ampliar la base de conocimiento

ANÁLISIS EN PROFUNDIDAD DEL MALWARE

¿Quién lo utiliza?
Expertos en análisis de malware

¿Con qué fin?
Entender cómo funciona el malware y qué técnicas utiliza
Precisar el nivel de amenaza que supone el malware

¿Cuáles son las ventajas?
Permite actuar lo antes posible
Analiza en profundidad el comportamiento (dinámico) con gran nivel de detalle sobre la actividad del malware
Recupera todas las entradas del volcado de memoria para completar el análisis con herramientas de terceros
Se personaliza la detección de comportamientos

Funcionalidad clave de Orion Malware

Motores de análisis estático y dinámico basados en heurística y en modelos de detección de IA

- Cinco antivirus para detectar el malware conocido
- Análisis dinámico de las amenazas más sofisticadas y desconocidas en un entorno virtual seguro usando tecnología de inspección que el malware no detecta
- Doble lista de reputación personalizable para identificar al instante archivos legítimos (lista blanca) y maliciosos (lista negra)
- Análisis estático avanzado con función de escáner basado en modelos heurísticos y de inteligencia artificial
- Motor de análisis basado en las reglas de detección del cliente en formatos Yara, OpenIOC y Python

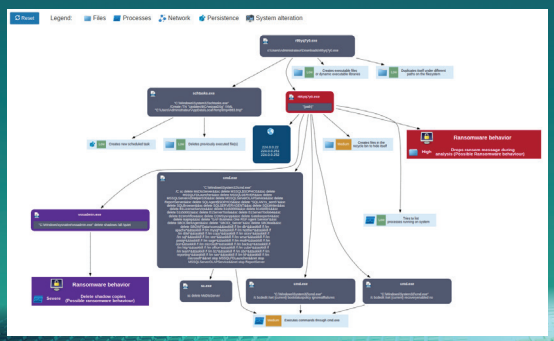
Una plataforma abierta y modular

- Configuración de flujos de análisis (activación/desactivación de motores, duración del análisis, elección de la VM de detección por defecto, extracción de PCAP, selección del navegador, etc.)
- Gestión de heurística dinámica y de comportamiento, y de modelos de IA

Fácil integración y soporte a sus servicios de inteligencia de amenazas

- Portales web específicos para el análisis de archivos y la gestión de la solución
- API REST e ICAP para un análisis automático desde sus dispositivos de red
- Exportación en formato SYSLOG de los resultados del análisis para que la SIEM (Splunk, QRadar, ELK) genere alertas
- Difusión de inteligencia de amenazas exportando IoC y reglas de detección en formato STIX 2.1, MISP, CSV, OpenIOC
- Solución 100% operativa en desconexión para entornos aislados
- Proteja sus ficheros adjuntos con el conector Orion Malware para MS-Exchange
- Integración con el sistema EDR de HarfangLab

INFORMES DE ANÁLISIS COMPLETOS



- Indicador global de riesgo
- Análisis del comportamiento del malware
- Clasificación MITRE ATT&CK
- Indicadores de compromiso

UNA OFERTA COMPLETA ADAPTADA A SUS NECESIDADES DE CIBERSEGURIDAD

Orion Malware cuenta con una gama de servidores integrados (S, M, L, XL)

Orion Malware también se ofrece en forma de suscripción SaaS

Actualización continua del paquete de detección (bases antivirus, heurística, modelos de aprendizaje automático, plantillas de análisis dinámico)

Soporte técnico y operativo (FR/EN). Tres cursos disponibles (Analista, Experto, Administrador)

Airbus le apoya a la hora de integrar Orion Malware en su cadena de ciberdefensa y en el desarrollo de conectores específicos

Airbus Defence and Space
Francia, Alemania, Reino Unido, España

www.cyber.airbus.com

contact.cybersecurity@airbus.com

@Airbus Defence and Space Cyber

AIRBUS