DEFENCE AND SPACE
Cyber

Orion Malware

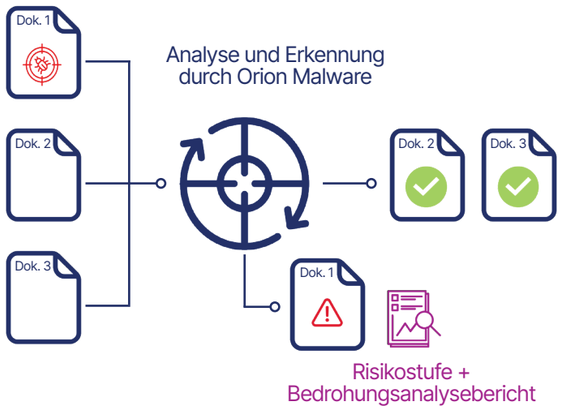
Fortschrittliche Lösung zur Erkennung und Analyse von Dateien

AIRBUS

Schützen Sie Ihre Organisationen und Systeme vor Angriffen über Dateien

Orion Malware **erkennt bekannte und unbekannte Angriffe über Dateien** mithilfe **verschiedener Analysemodule**, die Heuristiken, Signaturdatenbanken, KI und dynamische Analysen kombinieren.

Orion Malware kann auf einem physischen Server oder als SaaS bereitgestellt werden, um Ihre Cyber-Sicherheitsteams zu unterstützen, und lässt sich außerdem an beliebige branchenspezifische Anwendungsfälle in den Bereichen SOC, CSIRT/CERT oder TI anpassen.



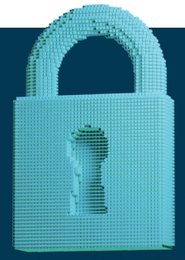
ERKENNUNG FORTSCHRITTLICHER MALWARE

Bei der Konzeption der Orion Malware haben die Experten von Airbus Defence and Space Cyber ein Virenschutzprogramm integriert und Routinen für die statische Analyse mit KI (künstliche Intelligenz) sowie die dynamische Analyse mit dem Ziel der Erkennung modernster Malware entwickelt.

ZEITERSPARNIS BEI ANALYSEN

Mit Orion Malware sparen Sie wertvolle Zeit, da die Lösung eine umfassende Bedrohungsanalyse durchführt und detaillierte Berichte generiert, die neben einer globalen Risikostufe auch Taktiken und Techniken von Malware sowie den Export von Kompromittierungsindikatoren (IOC, Indicators of Compromise) für die Abwehr zukünftiger Angriffe bzw. die Eindämmung von Sicherheitsvorfällen enthalten.

Die Analyseergebnisse können automatisch über unseren Syslog-Konnektor an verschiedene Werkzeuge Ihrer Cyber-Erkennungskette gesendet werden.



ORION MALWARE ERFÜLLT 3 WESENTLICHE FUNKTIONEN

Erkennen und Analysieren

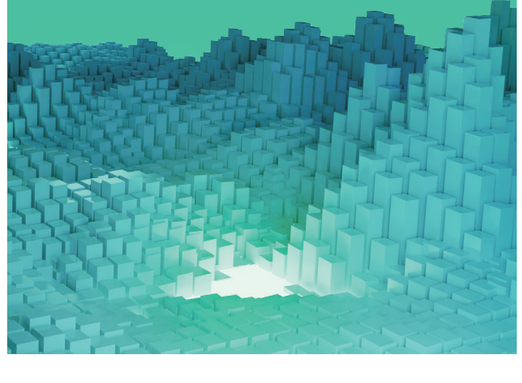
bekannter und unbekannter Bedrohungen

Absichern

Ihrer IT-Systeme durch Teilen der Kompromittier-ungsindikatoren

Unterstützen

Ihrer Teams bei der Cyberabwehr



Je nach Sicherheitsanforderungen erhältlich in zwei Versionen

Orion Malware ist als All-in-One-Lösung mit allen Analysemodulen für eine optimale Erkennung von Cyber-Vorfällen und als Multi AV-Version für eine schnelle Analyse auf der ersten Ebene erhältlich.

ERKENNUNGSROUTINEN	ALL IN ONE	MULTI-AV
Virenschutzanalyse (mit bis zu 5 Virenschutzprogrammen)	✓	✓
Reputationsanalyse (weiße Liste + schwarze Liste)	✓	
Statische Analyse: Scanner + KI	✓	
YARA- und Python-Regeln	✓	
Dynamische und verhaltensbasierte Analyse für Windows und Linux	✓	

Orion Malware bietet zwei Zugangsportale für eine Anpassung an alle Arten von Benutzern.

EXPERT-PORTAL: Cyber-Sicherheitsteams haben Zugang zu allen Funktionen. So können sie beispielsweise den Analyseworkflow definieren, Berichte suchen und anzeigen, IoC exportieren, Analysen wiederholen, einen Speicherauszug exportieren usw.

LITE-PORTAL: Benutzer ohne Vorkenntnisse im Bereich der Cyber-Sicherheit können bei Zweifeln Dateien vor der Verwendung prüfen. Auf diese Weise werden sie zu Akteuren im Bereich der Cyber-Sicherheit. Das Portal ermöglicht Benutzern das Prüfen ihrer Dateien und Anzeigen vereinfachter Ergebnisse.

Orion Malware eignet sich für verschiedene Anwendungsfälle

SCHUTZ DER IT-SYSTEME VOR KOMPLEXEN BEDROHUNGEN UND RANSOMWARE

Wer nutzt sie?
RSSI, Cyberteams und ITT-Administratoren

Mit welchem Ziel?
Erhöhung der IT-Sicherheit für einen effektiven Schutz vor Ransomware oder komplexen Bedrohungen (APT)

Automatische Analyse von Dateien durch die Integration von Firewalls, Proxys, Netzwerksonden, EDR, Mailservern

Welche Vorteile?
Erkennung und Abwehr von Bedrohungen

Einrichtung einer umfassenden Erkennungskette

Ergreifung von Maßnahmen durch Cyber-Teams vor der Kompromittierung, dem Diebstahl oder der Löschung von Daten

SICHERHEITSVORFALL

Wer nutzt sie?
SOC-Analysten und CSIRT-Teams

Mit welchem Ziel?
Kontrolle von einer oder mehreren Dateien

Suche nach Kompromittierungsindikatoren

Welche Vorteile?
Erkennung bekannter und unbekannter komplexer Bedrohungen

Bereitstellung einer Alternative für nicht vertrauliche Online-Datenanalysedienste

Zeitersparnis für SOC- und CSIRT-Teams mit einer gründlichen Analyse in einigen wenigen Minuten

Erstellung eines ausführlichen Analyseberichts zum schnellen Auffinden relevanter Kompromittierungsindikatoren und Erweitern der Wissensdatenbank

GRÜNDLICHE ANALYSE VON MALWARE

Wer nutzt sie?
Experten für die Analyse von Malware

Mit welchem Ziel?
Verständnis der Funktionsweise einer Malware und der verwendeten Techniken

Präzise Einstufung des Gefährdungspotenzials einer Malware

Welche Vorteile?
Erhebliche Zeitersparnis

Gründliche verhaltensbasierte (dynamische) Analyse mit einer hohen Detailgenauigkeit in Bezug auf die Aktivitäten der Malware

Abruf aller Zeilen des Speicherauszugs für eine zusätzliche Analyse mit Drittlösungen

Personalisierung der verhaltensbasierten Erkennung

Wichtige Funktionen der Orion Malware

Auf Heuristik und KI-Erkennungsmodellen basierende Module für die statische und dynamische Analyse

- Fünf Virenschutzprogramme für die Erkennung bekannter Malware
- Dynamische Analyse hoch komplexer und unbekannter Bedrohungen in einer gesicherten virtuellen Umgebung mit einer von Malware unentdeckbaren Selbstprüfungstechnologie
- Doppelte personalisierbare Reputationsliste für die unmittelbare Identifizierung legitimer (weiße Liste) und bösartiger (schwarze Liste) Dateien
- Scanner-Funktion für eine komplexe statische Analyse basierend auf heuristischen Modellen und künstlicher Intelligenz
- Analysemodul basierend auf Ihren eigenen Detonationsregeln im Format Yara, OpenIOC und Python

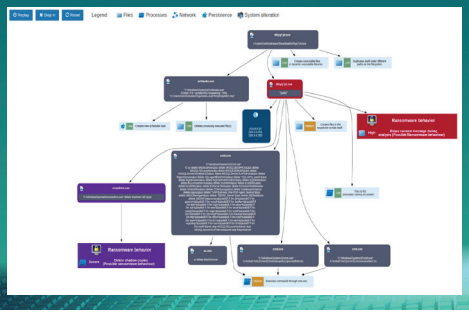
Eine offene und modulare Plattform

- Konfiguration der Analyseworkflows (Aktivierung/Deaktivierung der Module, Analysedauer, Standardauswahl der VM für die Detonation, Extraktion der PCAP, Wahl des Browsers usw.)
- Verwaltung der dynamischen und verhaltensbasierten Heuristiken und KI-Modelle

Einfache Integration und Unterstützung Ihrer Threat Intelligence-Dienste

- Spezifische Internetportale für Dateianalyse- und Lösungsverwaltungsfunktionen
- REST- und ICAP-API für eine automatisierte Analyse über Ihre Netzwerkgeräte
- Export der Analyseergebnisse im Format SYSLOG für Entwarnungen auf der SIEM-Ebene (Splunk, QRadar, ELK)
- Gemeinsame Nutzung der Threat Intelligence mit einem Export der IoC und der Erkennungsregeln im Format STIX 2.1, MISP, CSV, OpenIOC
- 100%ige Funktionsfähigkeit in einer isolierten Umgebung im Offline-Modus
- Absicherung Ihrer Anhänge: mit dem Orion Malware-Konnektor für MS-Exchange
- Integration mit der EDR-Technologie HarfangLab

DETAILGENAUE ANALYSEBERICHTE



- Globaler Gefährlichkeitsindikator
- Verhaltensbasierte Analyse der Malware
- MITRE-ATT&CK-Einstufung
- Kompromittierungsindikatoren

EIN KOMPLETTES, AN IHRE CYBER-BEDÜRFNISSE ANGEPASSTES ANGEBOT

Orion Malware verfügt über eine Palette integrierter Server (S, M, L, XL)

Orion Malware ist auch in Form eines SaaS-Abos erhältlich

Kontinuierliche Aktualisierung der Erkennungspakete (Virendatenbanken, Heuristiken, Machine-Learning-Modelle, dynamische Analysevorlagen)

Technische und funktionale Unterstützung (FR/EN). Drei Schulungen stehen zur Wahl (Analyst, Experte, Administrator)

Airbus begleitet Sie bei der Integration von Orion Malware in Ihre Cyberabwehrkette und der Entwicklung spezifischer Konnektoren

Airbus Defence and Space
Frankreich, Deutschland, Vereinigtes Königreich, Spanien

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

AIRBUS