CyberSecurity

AIRBUS

ORION MALWARE

DETECT AND ANALYSE MALWARE IN YOUR SYSTEMS WITH OUR ORION MALWARE PLATFORM

Organisations are increasingly being targeted by cyber attacks - and a significant number of these attacks include malware. In order for security teams to provide an appropriate response and mitigate the impact of an attack, it is essential to ensure that even the most covert threats can be detected and analysed.

Orion Malware enables you to prevent malware attacks and to respond to incidents through both its **complementary detection engines** and actionable **analytics reports**. Your security chain is also strengthened through shared information with your existing security assets. Orion Malware provides support for all of your cyber security teams: e.g. SOC, CSIRT/CERT, IT.

DETECT THE MOST SOPHISTICATED MALWARE

Our solution can check files coming from your security equipment, but also via user submission.

To design Orion Malware, Airbus CyberSecurity has developed and/or integrated antivirus software, static scanning engines, machine learning and dynamic analysis, enabling users to detect even the most clandestine attacks; the development of which may be state sponsored.

PREPARE INCIDENT RESPONSE

Orion Malware saves you valuable time in incident response thanks to analysis reports. These reports provide a risk score, a summary that is easy to understand by non-experts as well as all discovered indicators of compromise.

These reports can be exported to the SIEM or SIRP of SOC teams as well as the TIPs of threat intelligence teams.

ORION MALWARE FULFILS THREE ESSENTIAL FUNCTIONS:

DETECT AND ANALYSE
known and unknown threats

SECURE
your information systems by providing indicators of compromise

SUPPORT
all your teams engaged in cyber protection

PROTECT YOUR SYSTEMS AND SUPPORT YOUR CYBER TEAMS

ORION MALWARE KEY FEATURES

Combined analysis: static, dynamic, heuristics and artificial intelligence (AI)

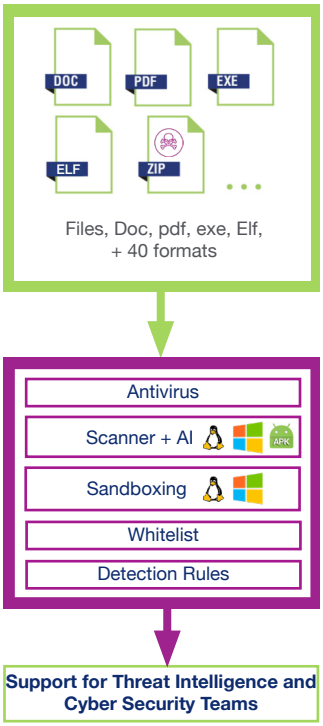
- Five antivirus software for instant detection of already known malware
- Detonation in sovereign Sandbox with anti-evasion system and undetectable hooking for the advanced or unknown malware
- Whitelist for instant detection of certified clean files
- Advanced static analysis scanner function based on heuristic and machine learning models
- Scripting language identification function based on Deep learning
- Analysis engine based on your own detonation rules in Yara, OpenIOC and Python format

An open and modular platform to meet your precise needs

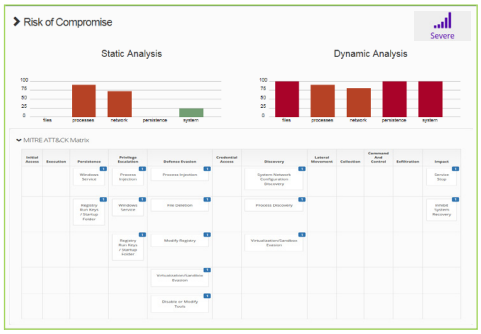
- Analysis workflows configuration (engines activation/deactivation, analysis duration, default choice of detonation VM, extraction of PCAPs, choice of browser, etc.)
- Dynamic and behavioural heuristics and AI models management

Easy integration and support for your threat intelligence services

- Web interface for IT security teams and administrator
- REST API and ICAP for automated analysis from your network equipment
- Analyses export in SYSLOG format for an exploitation by your SIEM (Splunk, QRadar, ELK)
- Sharing of Threat Intelligence with IOCs and detection rules in OpenIOC format exports
- 100% fully functional solution in offline mode for isolated environments



COMPREHENSIVE ANALYSIS REPORTS



- Impacts on the infected system **analysis and reporting**
- **Global risk level** for fast decision making
- **Full report** of antivirus and static/dynamic scans
- **MITRE ATT&CK** classification and **timeline**
- Exhaustive list of **indicators of compromise**
- List of **detected payloads**

A COMPLETE OFFER TAILORED FOR YOUR CYBER NEEDS

4 appliance models (S, M, L and XL) depending on the analysis power required

All our models benefit from the **same detection capabilities**

Versions and detection package (antiviral base and detection heuristics) **updates**

Technical and functional support (FR/EN)

Three trainings sessions available to fully use the capabilities of Orion Malware

Analyst, Expert, Administrator

Orion Malware supports you with the **integration into your IT system,** the **implementation** and **development of specific connectors**

AIRBUS

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

GERMANY
Willy-Messerschmitt-Str. 1
82024 Taufkirchen
Germany

UNITED KINGDOM
Quadrant House / Celtic Springs
Coedkernew / South Wales
NP10 8FZ / United Kingdom

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