CyberSecurity

Orion Malware

Orion Malware is designed to detect sophisticated malwares in your network by combining the performance of Static analysis, Sandboxing and Machine learning. Orion Malware provides SOC; CTI & Incident Response teams advanced capabilities for investigating emerging threats.

Key Benefits:

- **Multi-Analysis:** Consolidates reports coming from static and behavioural analysis engines. It detects and recursively analyses the payloads hidden in the original file, offering a detailed picture of its impacts on the targeted system. The generated report contains sections including comprehensive threat assessment indicators for quick and efficient responses as well as detailed views of artefacts.
- **Best of Breed Detection:** Sandbox embeds counter-measures for the most common escape technics used by attackers. To fit with each customer unique needs, Orion Malware enables you to design your detection policy.
- **Modularity and Scalability:** To ensure the ability to detect new threats at a reasonable costs, the modular architecture of Orion Malware allows the addition of new analysis components (Ex : static modules, 3rd party antiviruses, whitelist, sandbox running Window 7, Windows 10, Linux and Android).
- **Connected intelligence:** Offers a web interface for human submission and a machine to machine interface. Thus the solution can share threat intelligence indicators and rapid growth of the knowledge base for the benefit of all customers.
- **Powered by Airbus CyberSecurity:** The CSIRT and CTI teams power Orion Malware with the latest Threat Intelligence information using best of breed detection capabilities and the latest contextual information about APT, malwares and ransomwares.
- Orion Malware is available as appliance from all-in-one packaging to cluster mode.

AIRBUS

Key features

All-in-one malware analysis platform	• Qspy sandbox for dynamic analysis, • Magic analyzer for static analysis (Magic automatically reverses the file), • Scanner analyzer* explores the file format and associated heuristics; Scanner analyzer delivers as well machine learning results, • Triage : Whitelist, Yara, Antivirus option • Antiviruses (option). Orion embeds recognized third party antivirus solutions (Q4 2017)
Orchestration & policy analysis	Orion Malware embeds advanced orchestration capabilities so It can be configured to query one or multiple modules of analysis.
Templates for dynamic analysis (Qspy Sandbox)	• For Windows environment Qspy sandbox can customized to run or Window 7 + Office 2007 + a Web browser or Windows 10 + Office 2010 + a Web browser • Available web browsers: Firefox, IE, Chrome.
Dynamic analysis specificities (Qspy sandbox)	Main detection features: System alteration, Ransomware behavior, 0-day detection, recursive analysis, process injection techniques, modification in the firewall configuration, file execution & installation, file systems, registry keys accessed and network activity
Threat Intelligence inputs/outputs	• End-users have the possibility to add new and customized detection rules. Exports and ingests OpenIOC rules and exports MDE rules for Keelback Sensor. • Airbus Cybersecurity: delivers detection rules supported by Yara and Magic engines.
Reports, Data & Interfaces	• Analysis reports are delivered in PDF, HTML, JSON • Sample & PCAP file download, REST API, ICAP, Syslog interfaces, Email connector, Drag and Drop submission • Native integration: KeelbackNet sensors, Cymerius, Stormshield SNS, Proxy web (Q4 2017 and more to come)
Maximal size/file	20MB
Performance	~70 sec per analysis: Static & dynamic analysis combined (whiteout AV and whitelists)

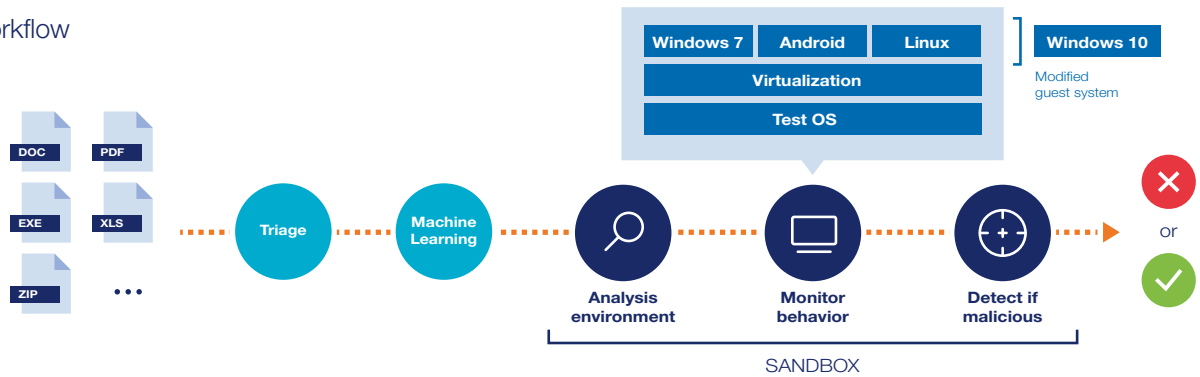
Supported files & environment

Microsoft Office (97 to 2003) and open office	doc, docx, docm, dotx, dotm, xls, xlsm, xltm, ppt, pptx, ppsm, ppsx,pptm, potm, potx, ods, odt, odp
Executable, binary, dll	PE32, PE32+, DOS
APK	Android application files
Archive files	Zip, rar, 7zip, tar
Rich Text Format and PDF	RTF , PDF files 1.5, 1.6, 1.7
Macromedia Flash, Java and javascript files	SWF , JS , JAR
EMAIL	SMTP mail, RFC 822 mail, MIME entity, HTML
Microsoft Help files	Windows help file «.chm»
ELF (static analysis)	Linux/GNU/SOlaris/BSD binary files X86, PPC, ARM, ARMeb, MIPS, MIPSEL, SPARC, ARCH, SH4
Auto extractibles	exe, cab, msi
Data	All type accepted

Product range

Available form factors	Appliance Cluster, Software, OEM software

Workflow



Airbus CyberSecurity
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France
Willy-Messerschmitt-Str. 1 / 82024 Taufkirchen / Germany
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / United Kingdom
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / United Arab Emirates
www.airbus-cyber-security.com / contact.cybersecurity@airbus.com