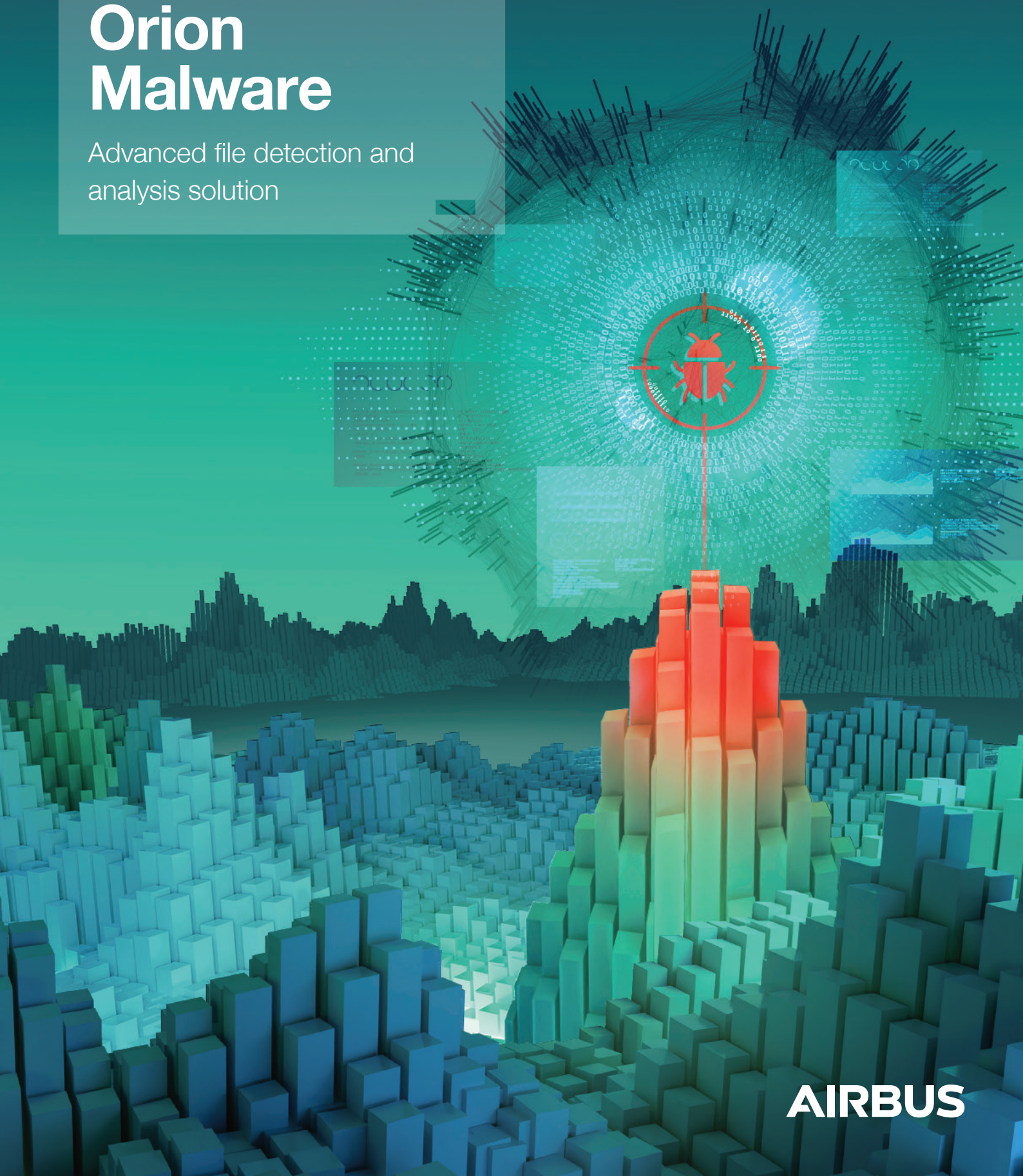
DEFENCE AND SPACE
Cyber

Orion Malware

Advanced file detection and analysis solution



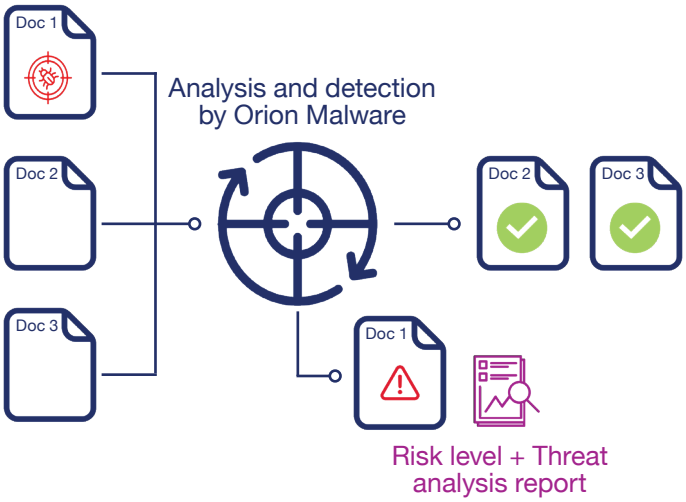
AIRBUS

Protect your organisations and systems from file-based attacks

LABEL FRANCE CYBERSECURITY 2022

Orion Malware **detects known and unknown file-based attacks** using a set of analysis engines combining heuristics, signature database, AI and dynamic analysis.

Deployable on a physical server or as SaaS, Orion Malware **supports all your cybersecurity teams** and adapts to every SOC, CSIRT/CERT or Threat Intelligence.



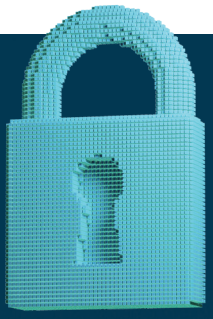
DETECT THE MOST ADVANCED MALWARE

The experts at Airbus Defence and Space Cyber have designed Orion Malware by integrating antivirus and developing static analysis engines with Artificial Intelligence (AI) and dynamic analysis, with the aim of spotting the most advanced malware.

REDUCE ANALYSIS TIME

Orion Malware saves you valuable time by carrying out in-depth threat providing detailed reports including an overall level of risk, malware tactics and techniques and the export of Indicators of Compromise (IOCs), to prevent future attacks or contain them in the event of an incident.

Analysis results can be sent automatically via our syslog connector to various tools in your Cyber detection chain.



ORION MALWARE FULFILS 3 ESSENTIAL FUNCTIONS

Detect and analyse

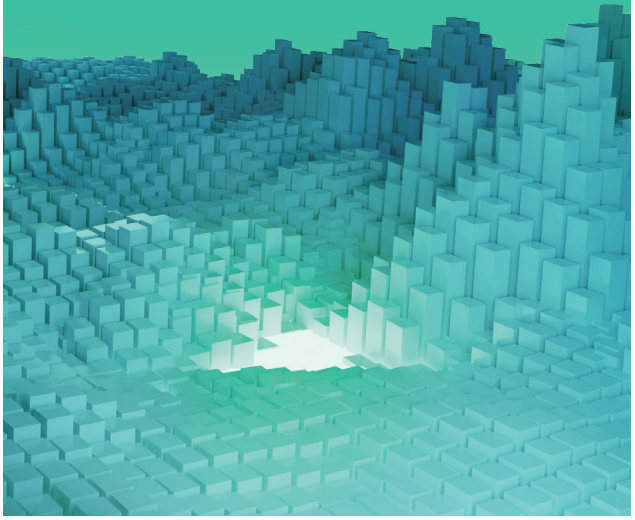
known and unknown threats

Secure

your information systems by sharing IOCs

Support

all your teams involved in cyber protection



Available in two versions to suit your safety requirements

Orion Malware either available as all-in-one version, including all the analysis engines for the very best in cyber detection, or as a multi-AV version for rapid first-level analysis.

DETECTION ENGINES	ALL-IN-ONE	MULTI-AV
Antivirus analysis (up to 5 antiviruses included)	✓	✓
Reputation analysis (whitelist + blacklist)	✓	
Static analysis Scanner + AI	✓	
YARA and Python rules	✓	
Dynamic / behavioural analysis (agentless) for Windows and Linux	✓	

Orion Malware offers two access portals to suit all types of user.

EXPERT PORTAL: Cyber security teams can access all functionalities. For example, they can define the analysis workflow, search and consult full reports, export IoCs, replay the analysis, export a memory dump etc.

LITE PORTAL: Users with no prior expertise in cyber security can check files before using them if in doubt. They become involved in their organisation's cyber security. The portal enables users to submit their files and obtain a simplified result.

Orion Malware covers a wide range of use cases

PROTECTION AGAINST ADVANCED THREATS AND RANSOMWARE

Who uses it?
CISOs, Cyber teams and ITT administrators

For what purpose?
Improve IS security to protect effectively against Ransomware or more advanced threats (APT).

Automatic analysis of files via integration with firewalls, proxies, network probes, EDR, mail servers, etc.

What are the benefits?
Detect the threat and enable it to be blocked.

Set up a complete detection chain.

Enable cyber teams to act before data is compromised, stolen or destroyed.

SAFETY INCIDENT

Who uses it?
SOC analysts and CSIRT teams

For what purpose?
To remove any doubt about one or more files.

Search for indicators of compromise.

What are the benefits?
Detection of the most advanced known and unknown threats.

Provides an alternative to non-confidential online analysis services.

Saves time for SOC and CSIRT teams with an in-depth analysis in just a few minutes.

Comprehensive analysis report to quickly find the most relevant indicators of compromise to enrich the knowledge base.

IN-DEPTH MALWARE ANALYSIS

Who uses it?
Malware analysis experts

For what purpose?
To understand how malware operates and the techniques used.

To precisely qualify the level of danger posed by a piece of malware.

What are the benefits?
Significant time savings.

In-depth (dynamic) behavioural analysis with a high level of detail on malware activity.

Recovers all memory dump entries to complete the analysis with third-party tools.

Customisation of behavioural detection.

Orion Malware key features

Combined static and dynamic scanning engines based on heuristics and AI detection models

- Five antivirus engines for detection of known malware
- Dynamic analysis of the most sophisticated and unknown threats in a secure virtual environment with introspection technology undetectable by malware
- Customisable dual reputation list to instantly identify legitimate (White List) and malicious (Black List) files
- Advanced static analysis scanner based on heuristics and artificial intelligence models
- Analysis engine based on your own detonation rules in Yara, OpenIOC and Python formats

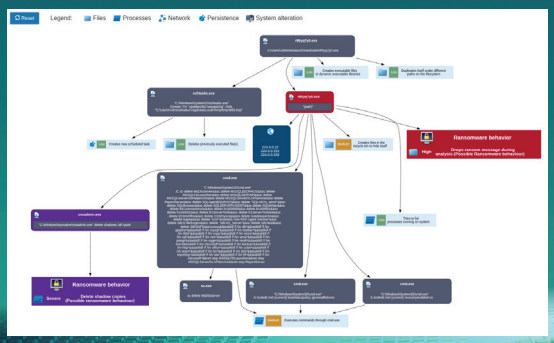
An open, modular platform

- Configuration of analysis workflows (activation/deactivation of engines, analysis duration, default choice of detonation VM, choice of browser, etc)
- Management of dynamic and behavioural heuristics and IAI models

Easy integration and support for your Threat Intelligence services

- Specific Web portals for file analysis and solution administration functions
- REST and ICAP APIs for automated analysis from your network equipment
- Export of analysis results in SYSLOG format for SIEM alert raising (Splunk, QRadar, ELK)
- Threat Intelligence sharing with export of IOCs and detection rules in STIX 2.1, MISP, CSV and OpenIOC formats
- 100% functional solution in disconnected mode for isolated environments
- Secure your attachments with the Orion Malware connector for MS-Exchange
- Integration with HarfangLab EDR

COMPREHENSIVE ANALYSIS REPORTS



- Global threat indicator
- Malware behavioural analysis
- MITRE ATT&CK classification
- Indicators of compromise

A COMPLETE OFFERING TAILORED TO YOUR CYBER NEEDS

Orion Malware has a range of integrated servers (S, M, L, XL)

Orion Malware is also available as a SaaS subscription.

Continuous updating of the detection package (antivirus databases, heuristics, machine learning models, dynamic analysis templates)

Technical and functional support (FR/EN). Three training courses available (Analyst, Expert, Administrator)

Airbus can help you integrate Orion Malware into your cyber defence chain and develop specific connectors.

Airbus Defence and Space
France, Germany, United Kingdom, Spain

www.cyber.airbus.com

contact.cybersecurity@airbus.com

@Airbus Defence and Space Cyber

AIRBUS