CyberSecurity

AIRBUS

Orion malware appliance

Orion
Malware appliance

Detect targeted attacks and ransomware with a military grade integration product combining most accurate detection engines.

Key Benefits:

- **Improved malware detection with simplicity** Airbus cybersecurity experts have selected best detection engines with threat intelligence around the globe. You aren't reliant on a single engine and benefit from a ready to use appliance with latest updated security feeds provided by Airbus cybersecurity.
- **Detect unknown malware:** and Even nation state sponsored attacks with sandboxing at the kernel level, behavioural analysis, multi vendors heuristics, machine learning, Rules engine to use Yara, openIOC, custom python script, inject easyly signatures provided by your country.
- **High performance delivered :** Orion malware appliances are designed and quality tested to analyse thousands of files per hour and many at the same time through API or ICAP.
  User can track performance via SIEM technologies and ajust the sensitivity of detection at a very low false positive rate with Goodware detector.
- **Stay under the radar and free:** Build your on-premise malware analysis solution with complete control of incoming and outbound communications. Create your Own cyber threat intelligence without sharing any sample on internet but only with your Threat intelligence platform.
- **Speed up incident response:** spread orionmalware service to your users providing them a powerfull and simple file analysis tool, training and support provided by Airbus experts. Connect orion malware to your IDS sensor to detect ransomware and forge signatures

Key features

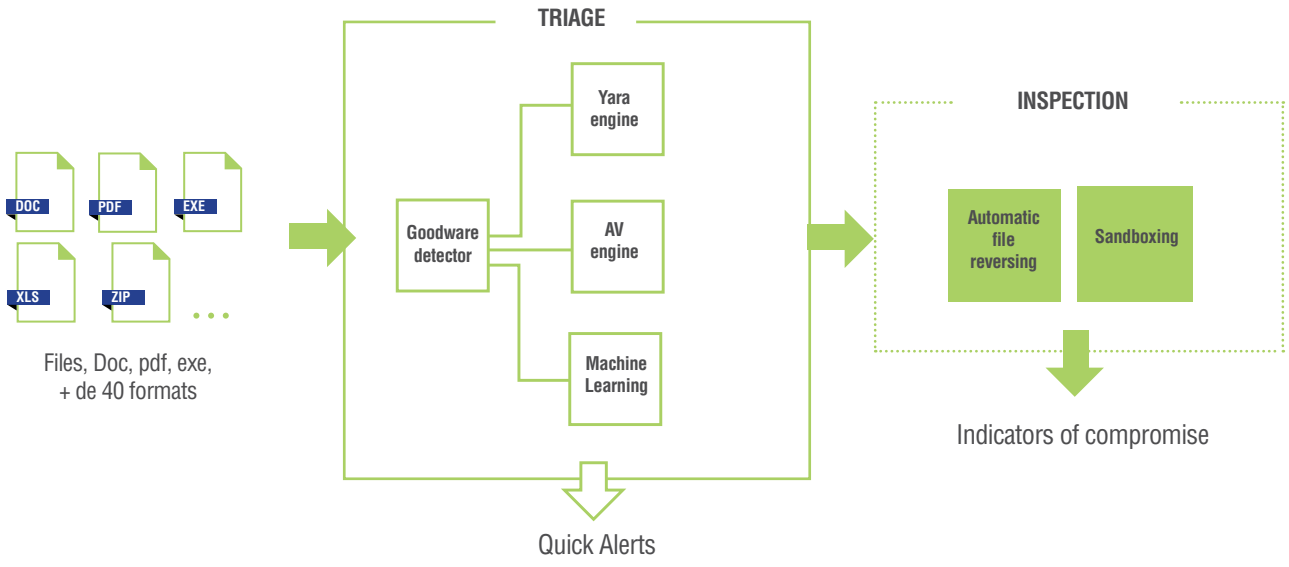
Patented Multi scanning	• Multiple antivirus • Machine learning • Sandboxing at the kernel level • Orchestration & policy	• Custom heuristics or rules (Python, Yara) • Goodware detector • Risk evaluator, > 40 file format
Kernel level sandboxing	• System supported : winXP, 7,10 ,linux, android • Thousand of heuristic included	• Create your own heuristic • Anti-evasion unique technology
Seemless integration	• Interface REST API, ICAP, http, email, syslog • EDR, DPI, PROXY, IDS, UTM, SIEM, websites, Threat intelligence plateform, MISP	
Custom malware analysis	• Add your python scripts, Yara rules • Customize the analysis with workflow and templates (detonation, engines, OS...) • Get screenshot, PCAP, payload	• Timeline automatic generation • Recursive analysis, cyphered file analysis • Generate reports (HTML,pdf, JSON, OpenIOC) and save to MISP
Cyber threat intelligence services	• Cyber Threat Intelligence feeds • Malware analysis training • Malware reversing engineering	

Product range

Available form factors	• On premise all in one appliance 4 models	

Use cases

- malware detection in airgapped networks
- as a service analysis tool for users
- Cyber threat intelligence IoC trusted collector
- SOC CSIRT common file analysis platform



FOR MORE INFORMATION:
Airbus CyberSecurity

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

UNITED ARAB EMIRATES
Etihad Towers T3 / Corniche Road,
19th floor / P.O.Box: 72186 /
Abu Dhabi / United Arab Emirates

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

AIRBUS