



# EU-FUNDED R&D INITIATIVES ON CYBER DEFENCE

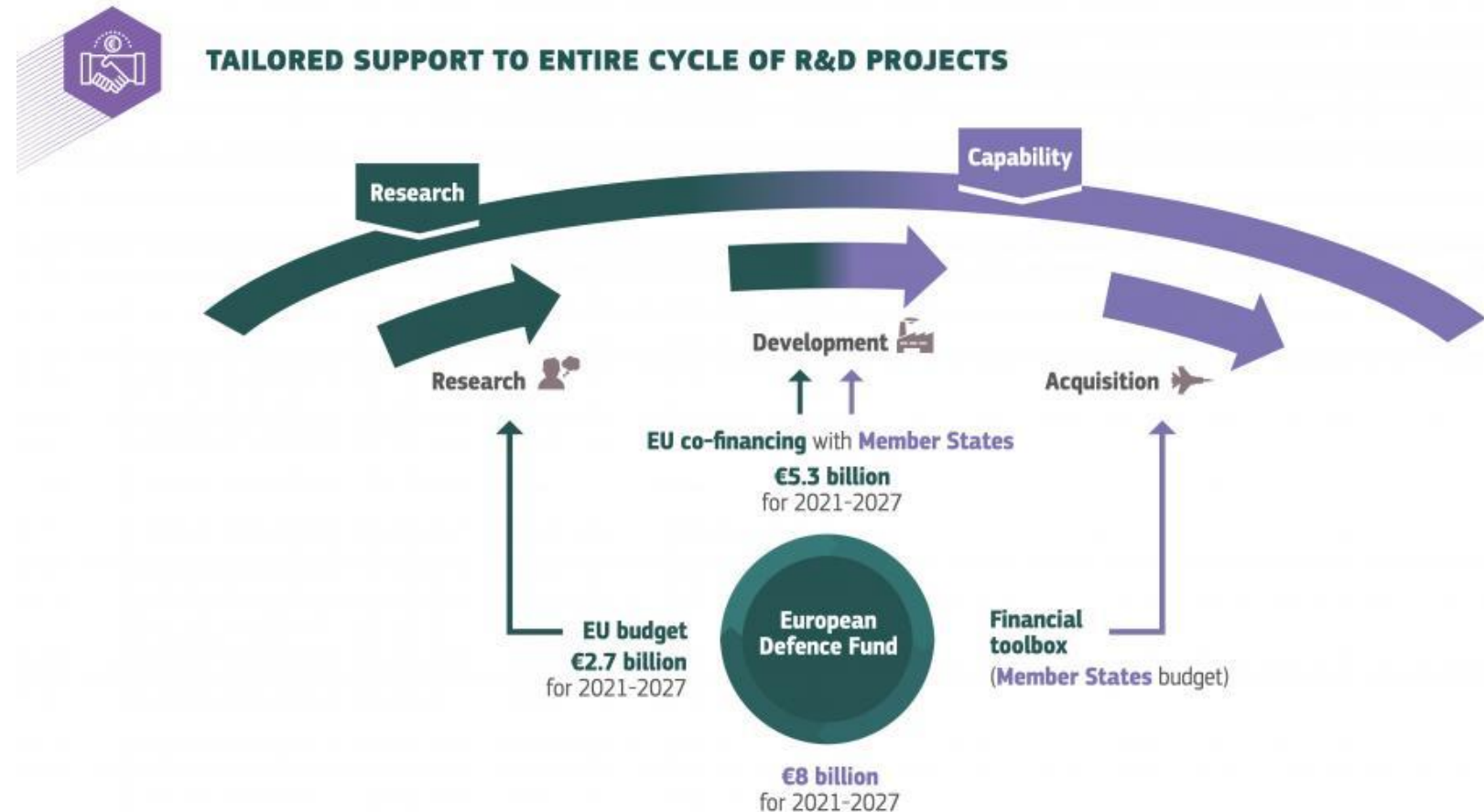
DR. GEORGIOS GARDIKIS

R&D MANAGER, SPACE HELLAS S.A.



# THE EUROPEAN DEFENCE FUND (EDF)

- The Commission's initiative to support collaborative defence research and development
- Defence R&D is no longer excluded



# THE EUROPEAN DEFENCE FUND (EDF)



Defence medical response, Chemical Biological Radiological Nuclear (CBRN), biotech and human factors



Space



Air combat



Information Superiority



Digital transformation



Air and missile defence



Advanced passive and active sensors



Energy resilience and environmental transition



Ground combat



Cyber



Materials and components



Force protection and mobility



Naval combat



Disruptive technologies



Open calls for innovative defence technologies

# EDF – CYBERSECURITY TOPICS

- EDF Call 2021:
  - Improving cyber defence and incident management with artificial intelligence
  - Improved efficiency of cyber trainings and exercises
- EDF Call 2022 (not officially released yet):
  - Adapting Cyber Situational Awareness for Evolving Computing Environments
  - Cyber and information warfare toolbox
  - Cybersecurity and systems for improved resilience

# EDIDP PANDORA PROJECT - IDENTITY

## Proposal title

**PANDORA:** Cyber Defence Platform for Real-time Threat Hunting, Incident Response and Information Sharing

## Topic identifier

**EDIDP-CSAMN-SSS-2019:** Software suite solution, enabling real-time cyber threat hunting and live incident response, based on shared cyber threat intelligence (PESCO Project CTISP)

## Coordinator

Space Hellas S.A.

## Consortium

15 organizations, 8 Member States

## Total budget

7.63 M€

## Duration

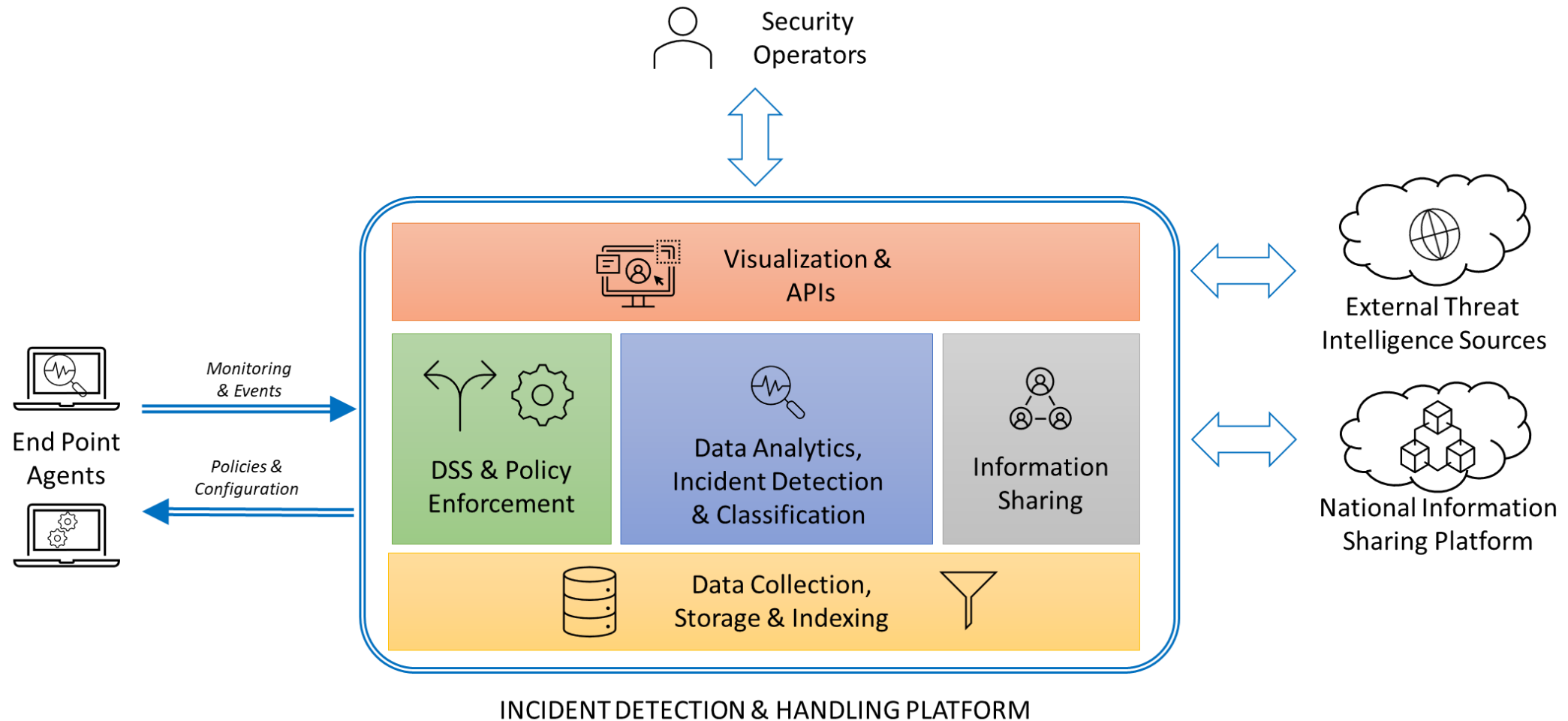
24 months (December 2020 – November 2022)

# PANDORA PROJECT MISSION

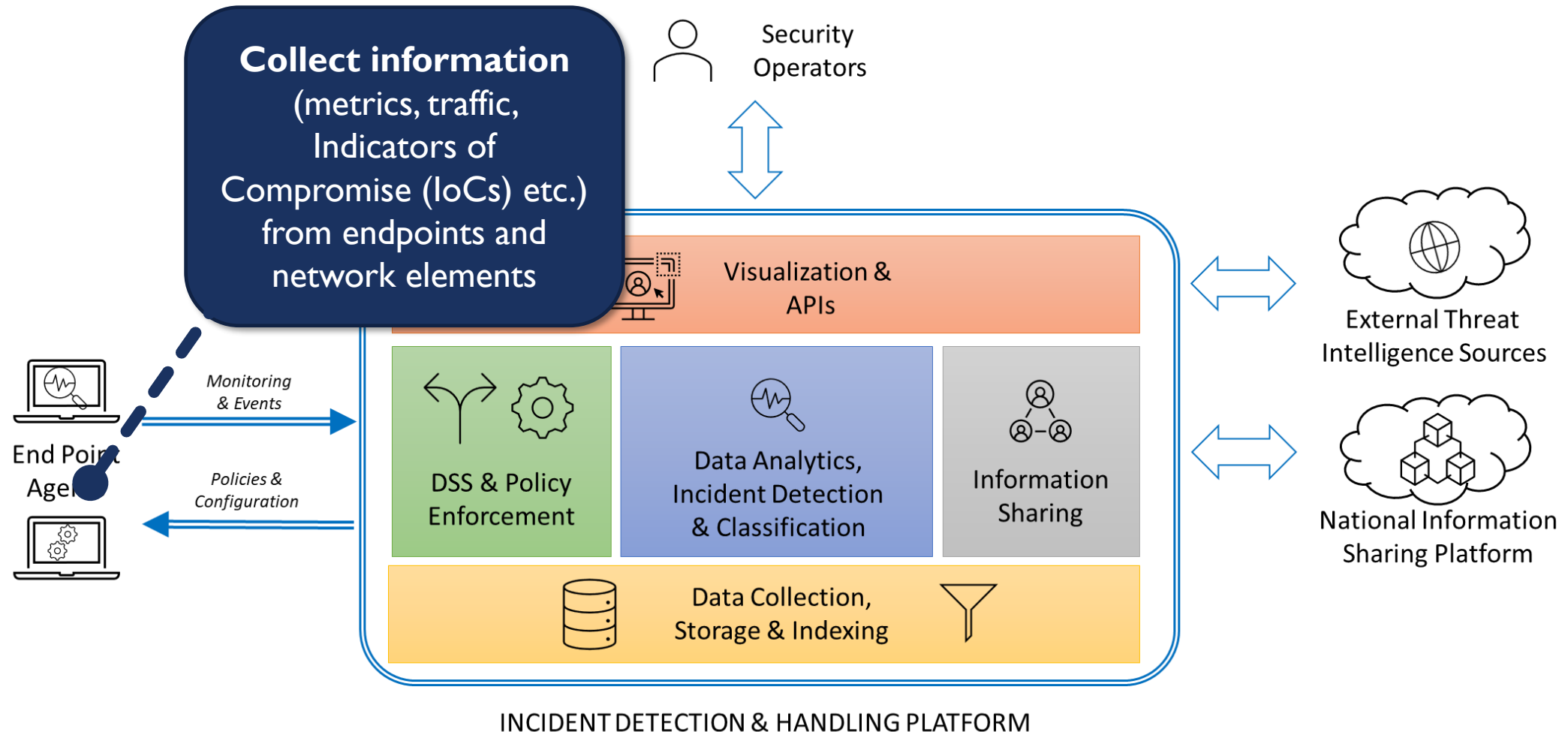


“To contribute to EU cyber defence capacity building, by designing and implementing an open technical solution for real-time threat hunting and incident response, focusing on endpoint protection, as well as information sharing.”

# PANDORA PLATFORM – KEY COMPONENTS

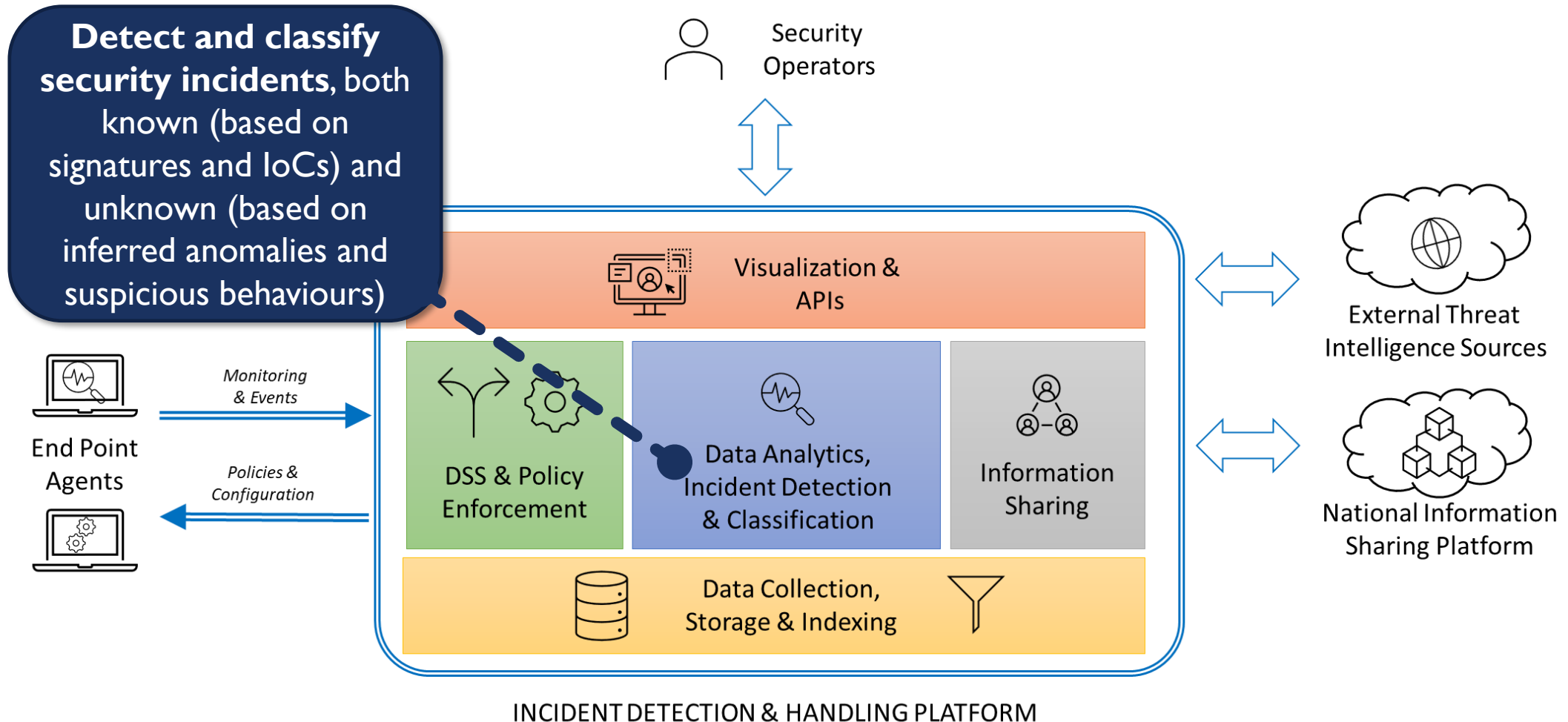


# PANDORA PLATFORM – KEY FEATURES (1/5)

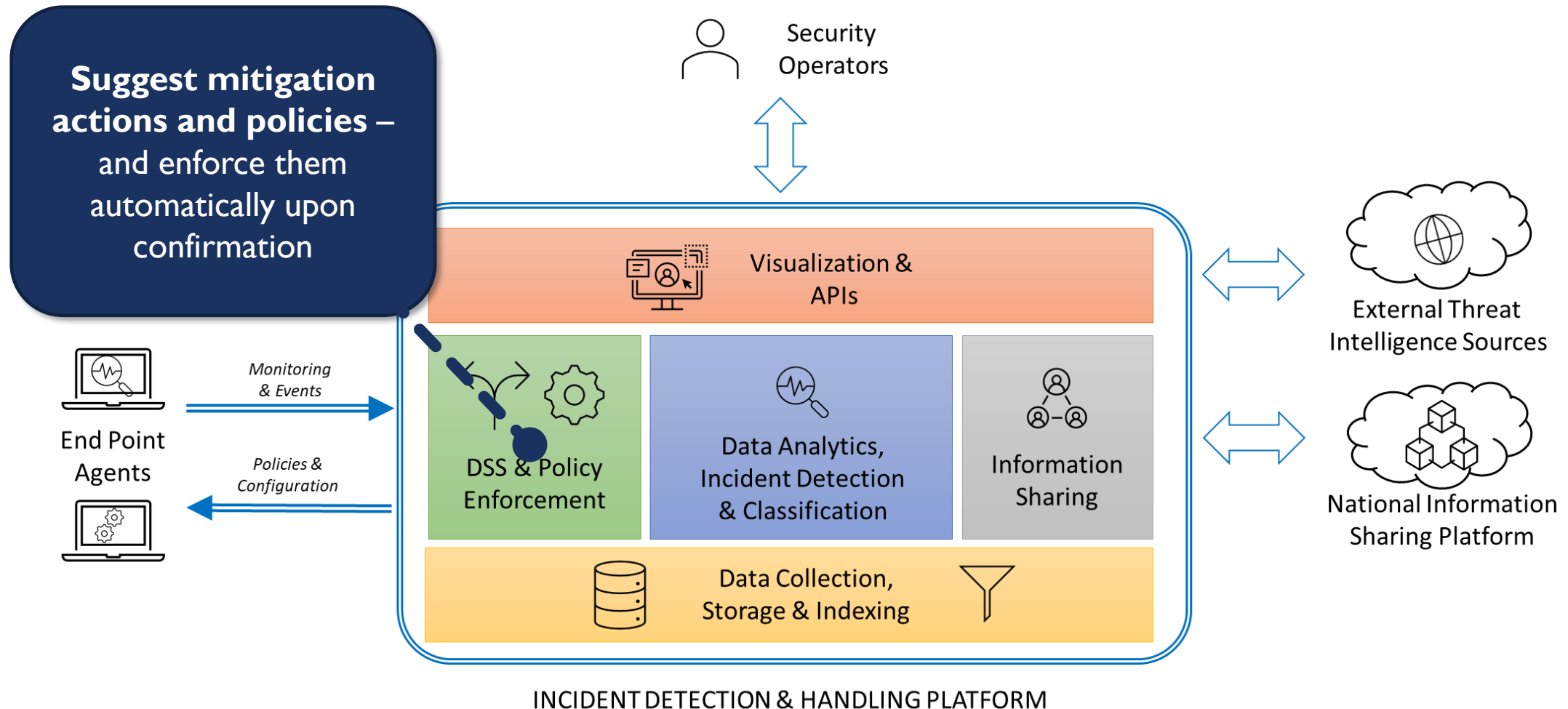




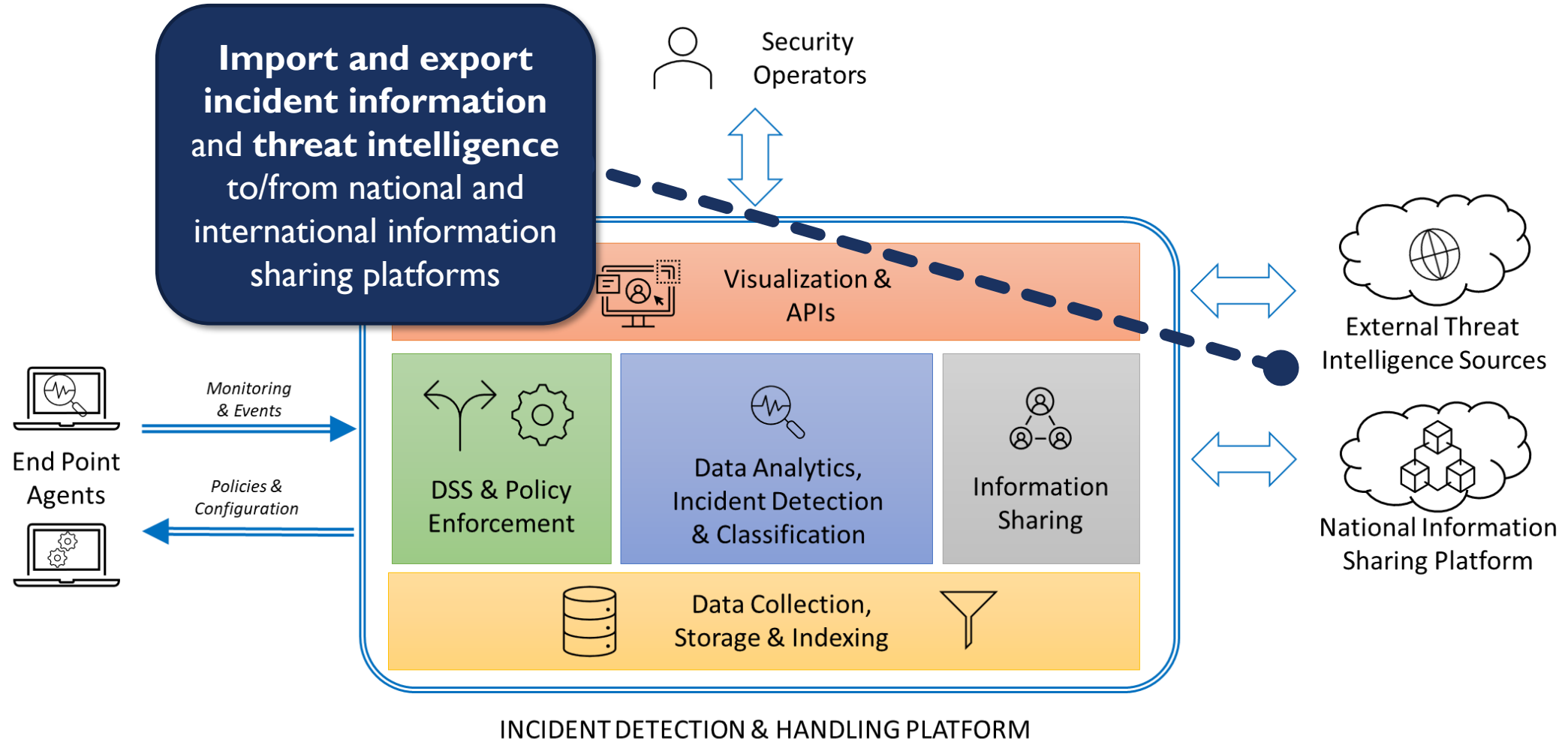
# PANDORA PLATFORM – KEY FEATURES (2/5)



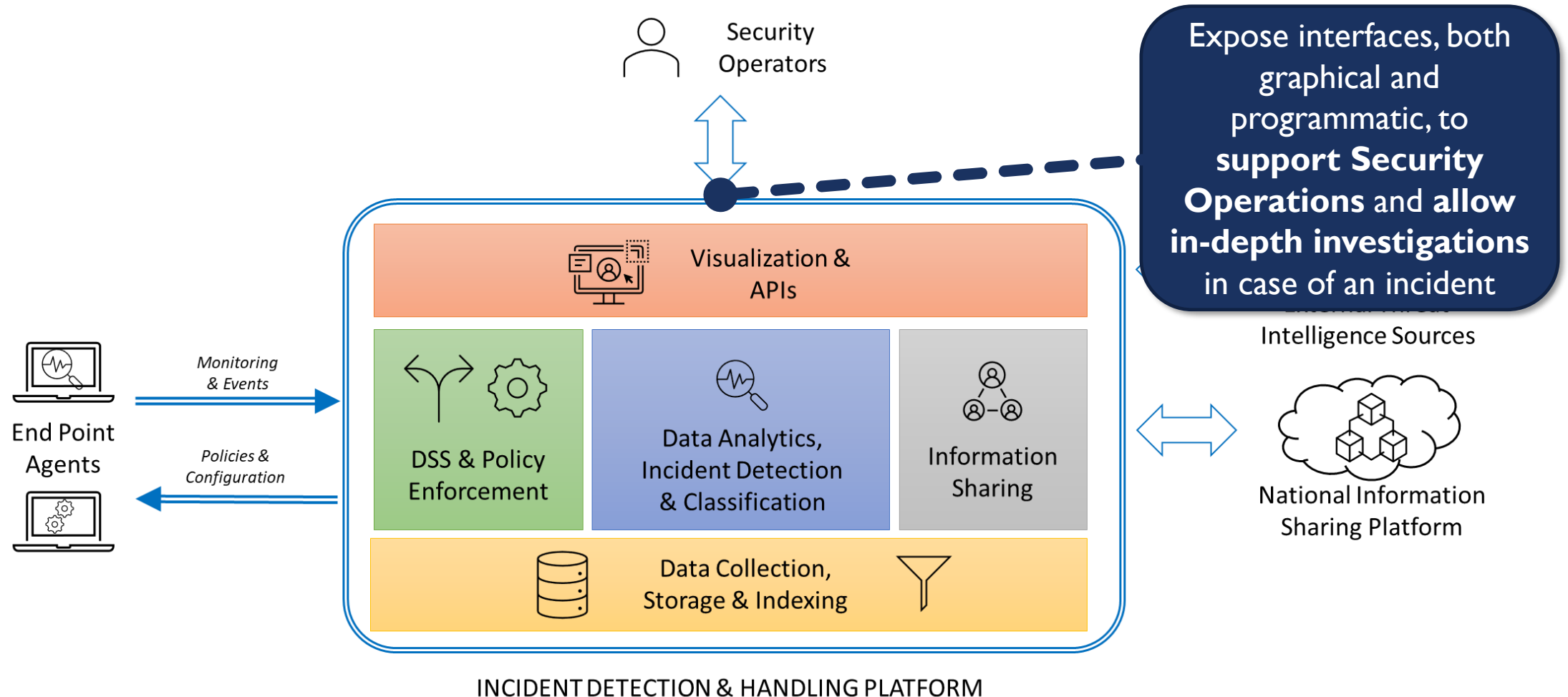
# PANDORA PLATFORM – KEY FEATURES (3/5)



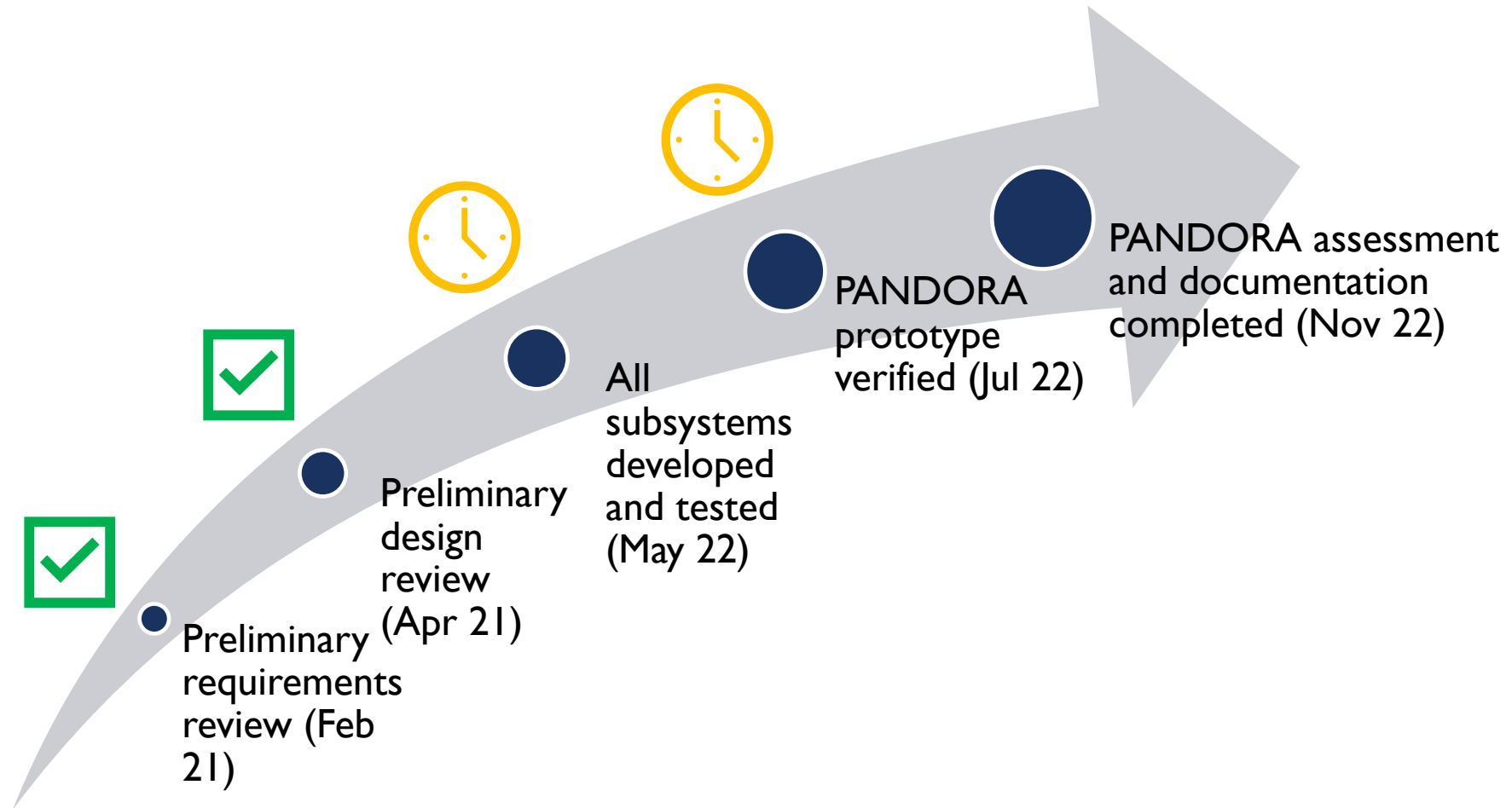
# PANDORA PLATFORM – KEY FEATURES (4/5)



# PANDORA PLATFORM – KEY FEATURES (5/5)



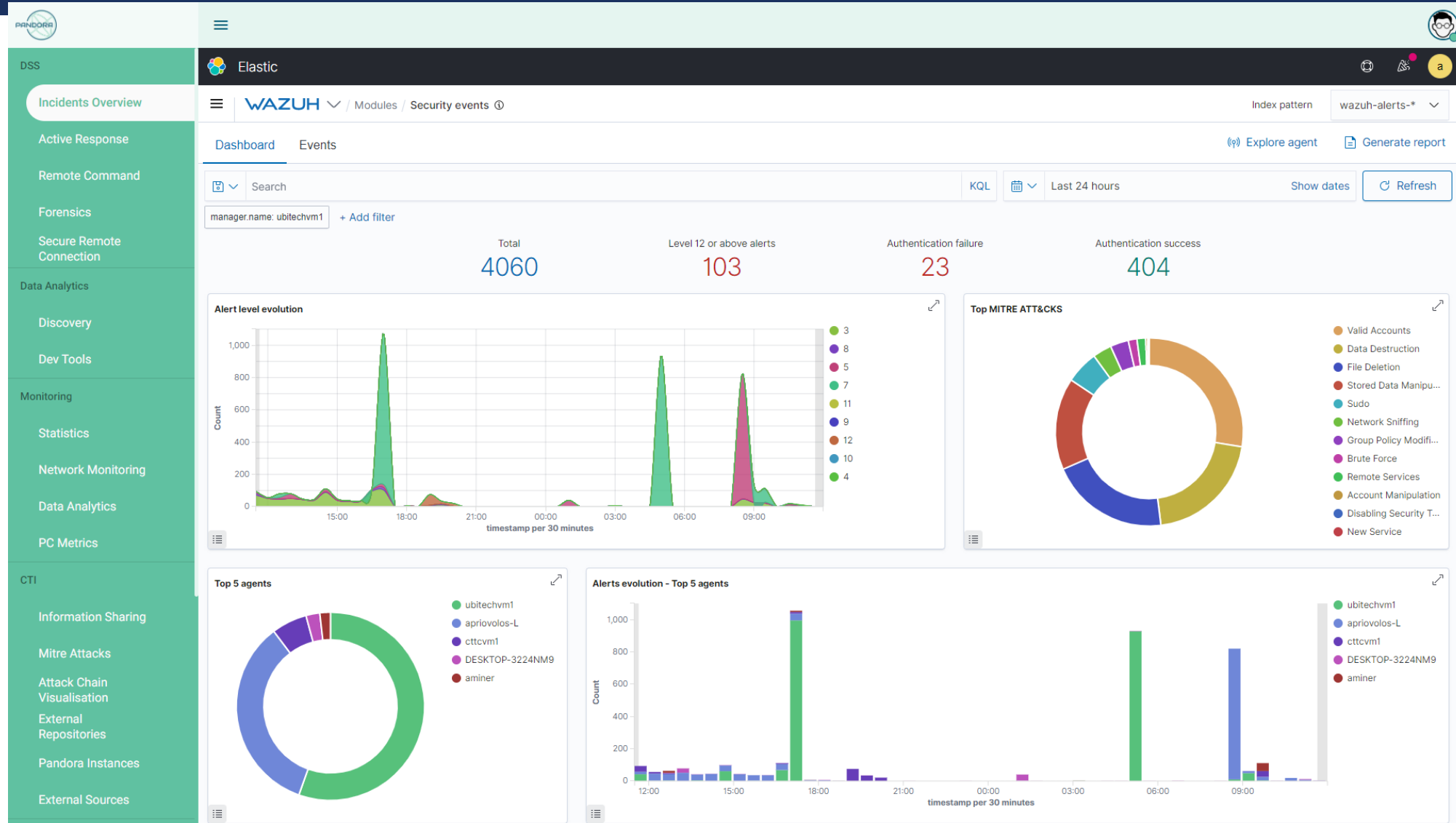
# MAIN PROJECT MILESTONES




# BASELINE TECHNOLOGIES FOR IMPLEMENTATION



# PANDORA GUI



# PANDORA GUI



Incidents Overview

Active Response

Remote Command

Forensics

Secure Remote Connection

Data Analytics

Discovery

Dev Tools

Monitoring

Statistics

Network Monitoring

Data Analytics

PC Metrics

CTI

Information Sharing

Mitre Attacks

Attack Chain Visualisation

External Repositories

Pandora Instances

External Sources

MISP Search

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Mirai' Malware Report from https://bazaar.abuse.ch/sample/4a704f42c8d341af5466f87e15affce86a986e79a4518471f5eee79ed715dd50/  
Attributes: 6 | Event Tags: 3 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Mirai' Malware Report from https://bazaar.abuse.ch/sample/a18de6484bbd6c766acd7dde3438eb5831f9fd5ddac54ba1adc84695c67f59c4/  
Attributes: 6 | Event Tags: 3 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Mirai' Malware Report from https://bazaar.abuse.ch/sample/a806533988440b26a03e85c5837c0f3b9ff87c64ae148d6c40c500c03cea3914/  
Attributes: 6 | Event Tags: 3 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Grandoreiro' Malware Report from https://bazaar.abuse.ch/sample/e538e6aa72721a0af5c82b49a550de0072bd54ffc9d76a46e15c054357d1f5f/  
Attributes: 8 | Event Tags: 3 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Mirai' Malware Report from https://bazaar.abuse.ch/sample/499c6b7f19aa9c9425ac83eb1dea08e4db25cfd58014e72c7bb346b0e6225e70/  
Attributes: 3 | Event Tags: 4 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Mirai' Malware Report from https://bazaar.abuse.ch/sample/90d58fb9dc399a59fd05f5a1b3e9786bc375905fd812ffe2c710f9fd61cf6e8c/  
Attributes: 3 | Event Tags: 4 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Mirai' Malware Report from https://bazaar.abuse.ch/sample/9b0fa9623525cb81930395cb9255313f1f70cb8bd42c3957402c2239d0894409/  
Attributes: 3 | Event Tags: 4 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Mirai' Malware Report from https://bazaar.abuse.ch/sample/ddc961695eb86e75a4519fe5149c50e573dc604731d57b4aafb53bf565eef129/  
Attributes: 5 | Event Tags: 4 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Mirai' Malware Report from https://bazaar.abuse.ch/sample/1bd38f23812c0410bbf95f460993ce3cd676e15f444e85c4fd5f5528ebfb7bdc/  
Attributes: 4 | Event Tags: 4 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Mirai' Malware Report from https://bazaar.abuse.ch/sample/774a10b62e1de9d748138fc78329d691b42b0a14356357485249feffe892bc62/  
Attributes: 5 | Event Tags: 4 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) Report from https://phishstats.info/phish\_score.csv  
Attributes: 4 | Event Tags: 5 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Mirai' Malware Report from https://bazaar.abuse.ch/sample/46cb1397c68098d5f8c37ac584e9dd7d41e54bfb4610fb1f4e9c081d4b7463f8/  
Attributes: 4 | Event Tags: 4 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) Report from https://hybrid-analysis.com/sample/2b13e318be8b41deffa80c3bd7fdec20de9688d5ceedfbb56cf43d4996a62bed/5c76c803038838f3847b23c8  
Attributes: 7 | Event Tags: 3 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) of 'Mirai' Malware Report from https://bazaar.abuse.ch/sample/a6743f52941af363352d55e32f70e1fa84df175d4beb7d3ad6ed2f63d09354b9/  
Attributes: 4 | Event Tags: 4 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) Report from https://openphish.com/  
Attributes: 3 | Event Tags: 3 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) Report from https://phishstats.info/phish\_score.csv  
Attributes: 2 | Event Tags: 2 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) Report from https://phishstats.info/phish\_score.csv  
Attributes: 3 | Event Tags: 2 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) Report from https://phishstats.info/phish\_score.csv  
Attributes: 2 | Event Tags: 2 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM

ORGANISATION\_ONLY

INITIAL

UNDEFINED

Indicator(s) Report from https://twitter.com/i/web/status/1511536298481356805  
Attributes: 2 | Event Tags: 2 | Date: 2022-04-07 | Published: Jan 1, 1970, 2:00:00 AM



## NEXT STEPS (IDEAS FOR FUTURE PROJECTS)

- Heavy use of AI for tasks as:
  - Intrusion detection
  - Incident classification
  - CTI export and ingest
  - Alert fusion
  - Root cause analysis
  - Generation and optimization of response actions
- Security Automation, Orchestration and Response (SOAR) in a military context
- Integration of OT cyber threats – cyber/physical threat scenarios

---

# THANK YOU FOR YOUR ATTENTION!

<https://www.space.gr/en>

<https://www.pandora-edidp.eu/>

