PANDORA

CYBER DEFENCE PLATFORM
FOR REAL-TIME THREAT HUNTING,
INCIDENT RESPONSE
AND INFORMATION SHARING

PROJECT OVERVIEW AND LATEST DEVELOPMENTS

Socrates Costicoglou Director IT Applications and R&D SPACE HELLAS

DUAL USE TECHNOLOGIES 2022: CYBERSECURITY AND DIGITAL APPLICATIONS IN DEFENCE

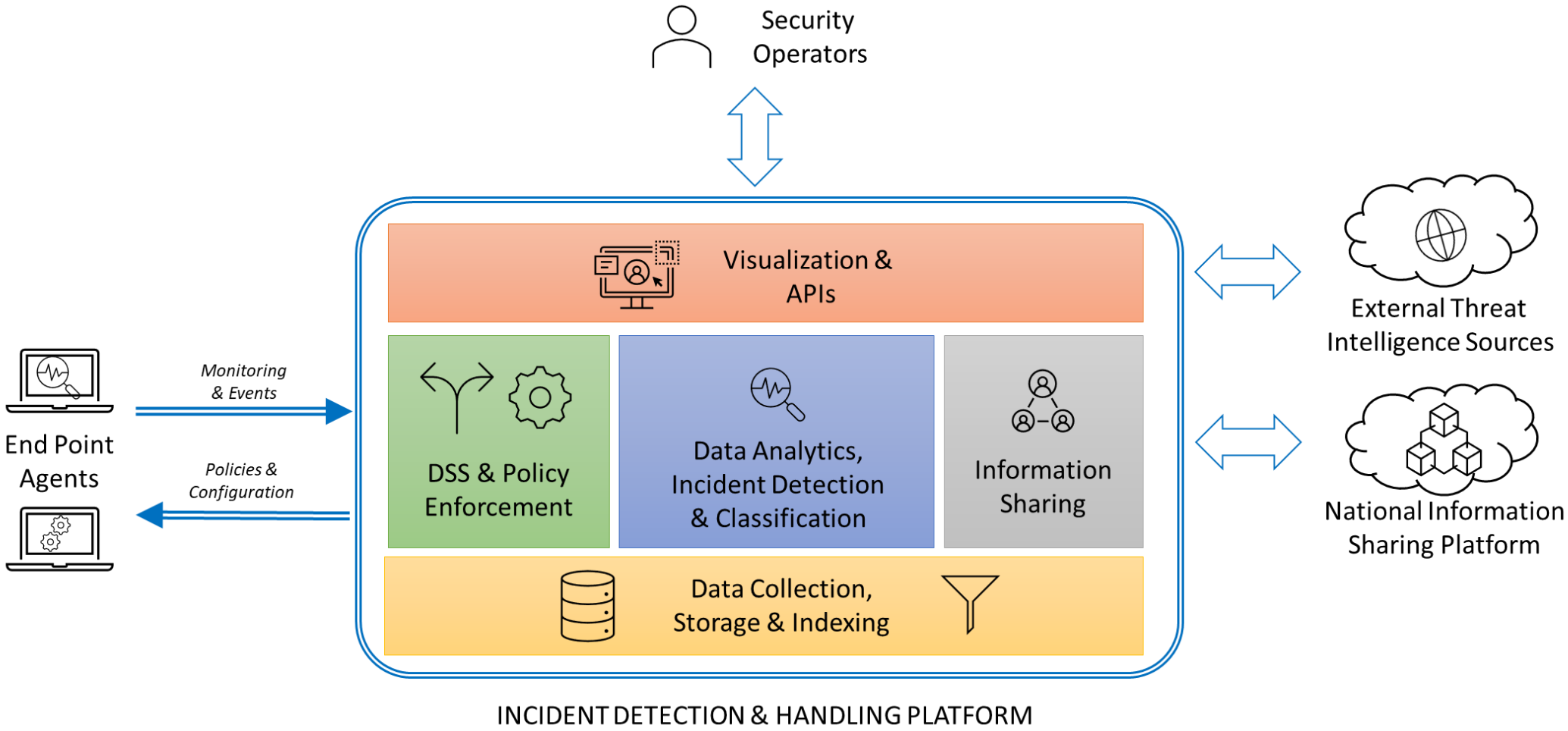
PROJECT IDENTITY

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)

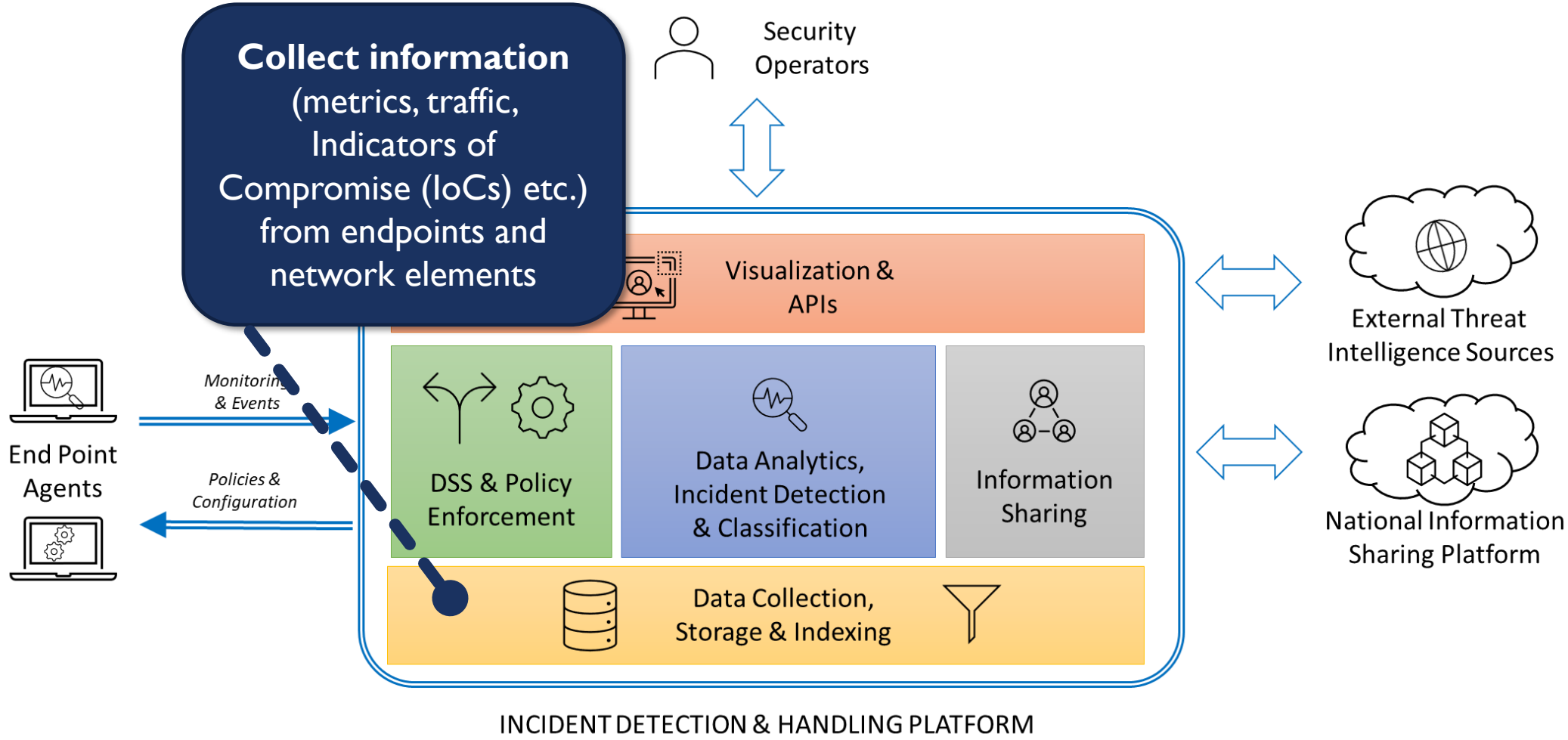
PANDORA PROJECT MISSION

"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

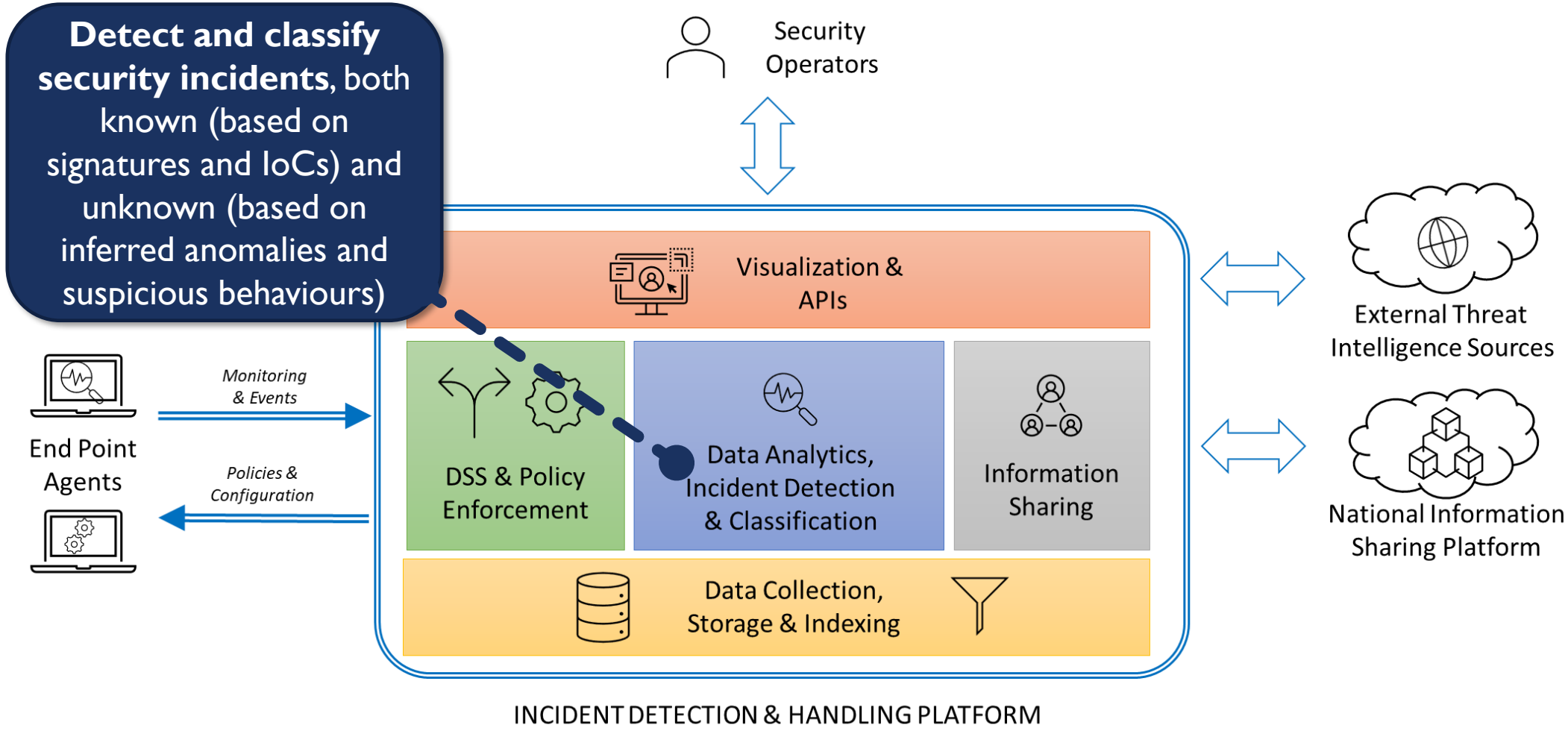


PANDORA PLATFORM – KEY FEATURES (1/5)



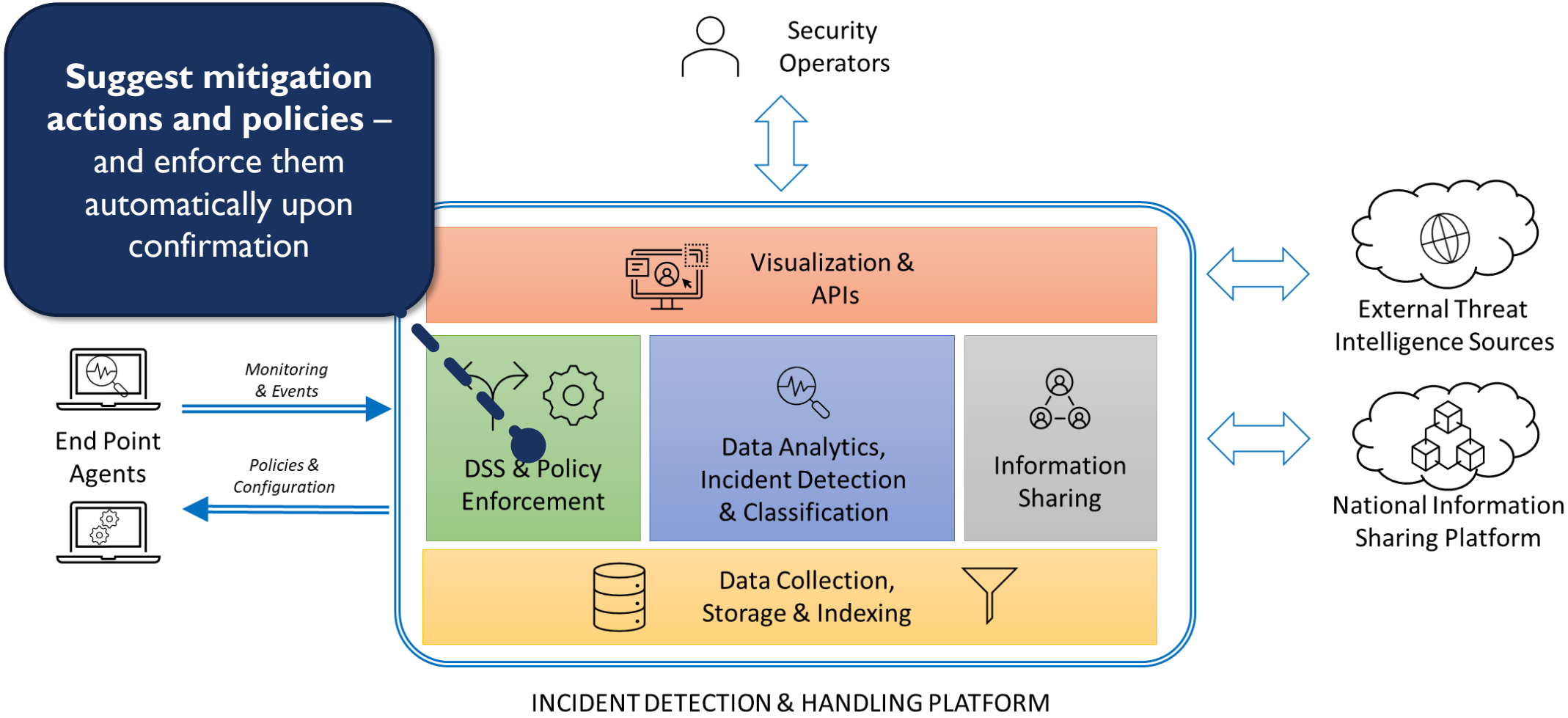
PANDORA PLATFORM – KEY FEATURES (2/5)

Detect and classify security incidents, both known (based on signatures and IoCs) and unknown (based on inferred anomalies and suspicious behaviours)

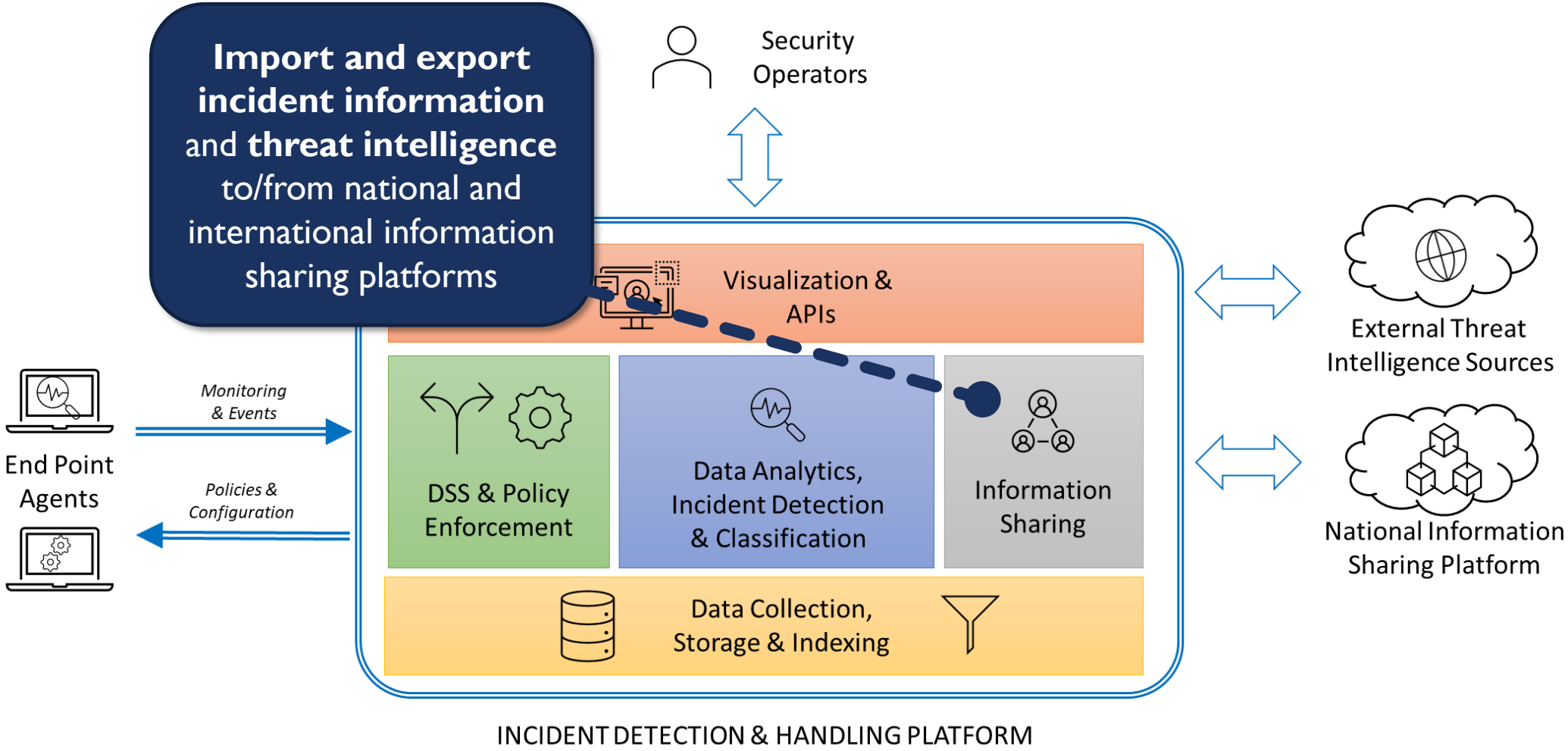


PANDORA PLATFORM – KEY FEATURES (3/5)

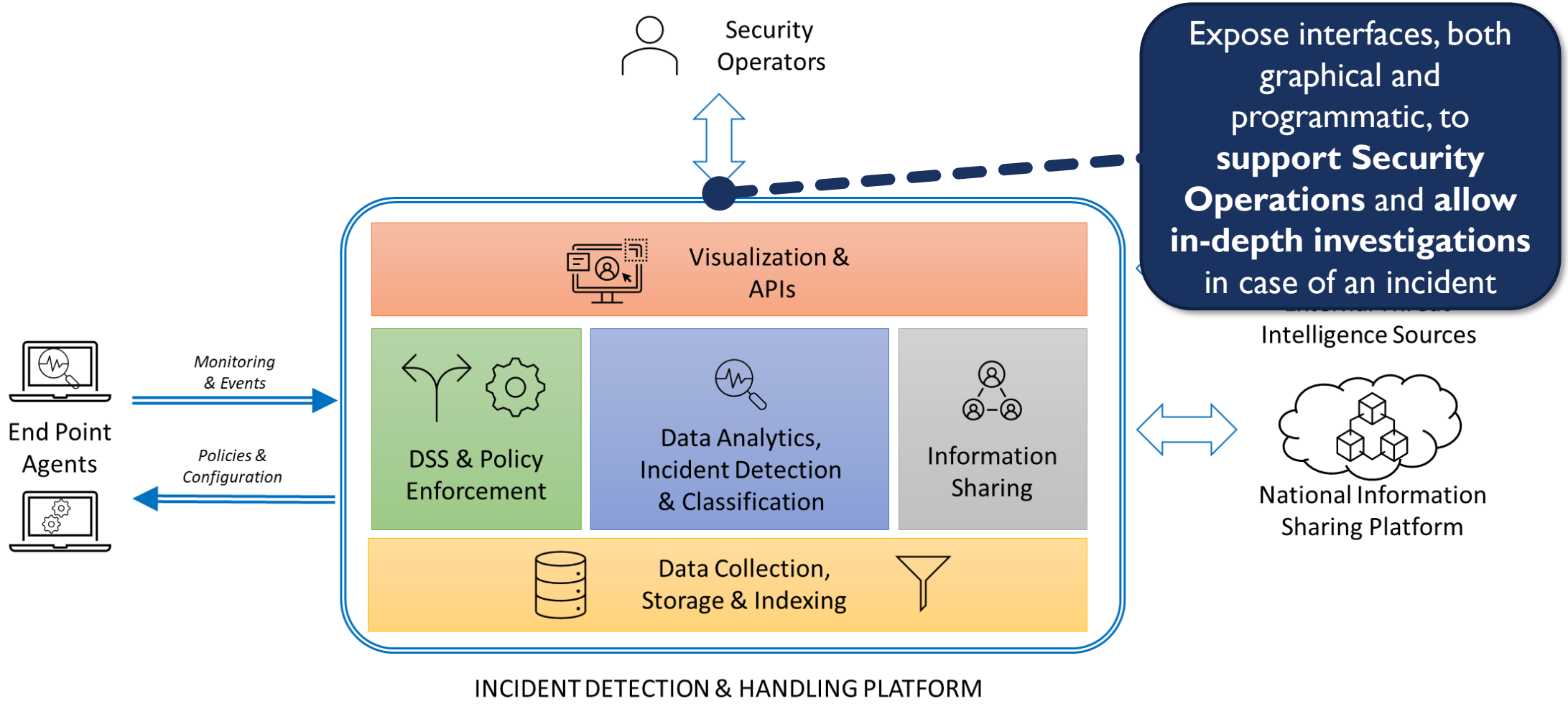
Suggest mitigation actions and policies – and enforce them automatically upon confirmation



PANDORA PLATFORM – KEY FEATURES (4/5)



PANDORA PLATFORM – KEY FEATURES (5/5)



BASELINE TECHNOLOGIES FOR IMPLEMENTATION (1/2)

MAIN PROJECT RESULTS

Use cases and requirements reports

System design documents

MISP Infrastructure

Incident Detection and Handling Platform

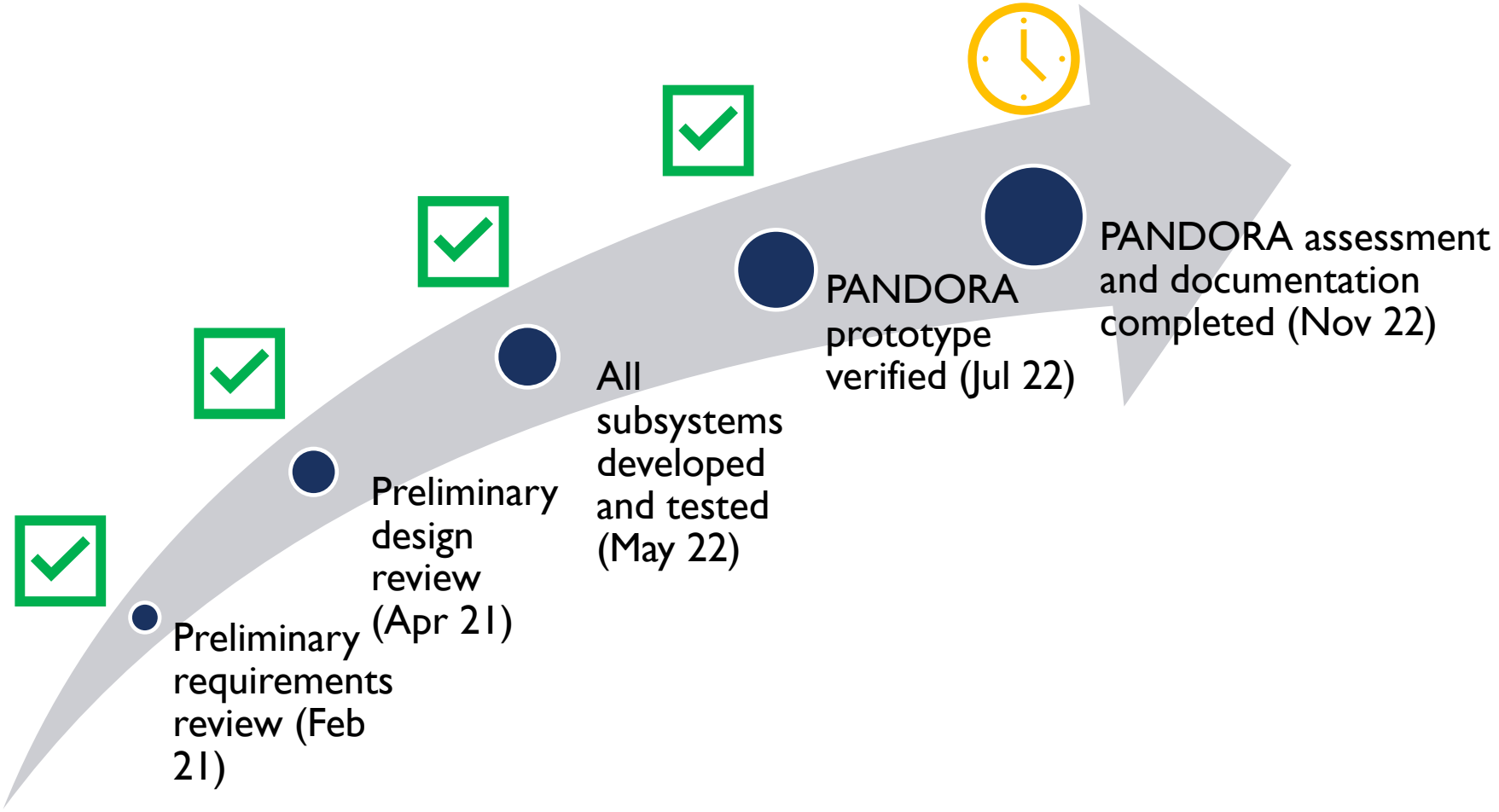
Windows and Linux EDR agents

Integrated PANDORA prototype

Use Case testbeds

Testing and evaluation reports

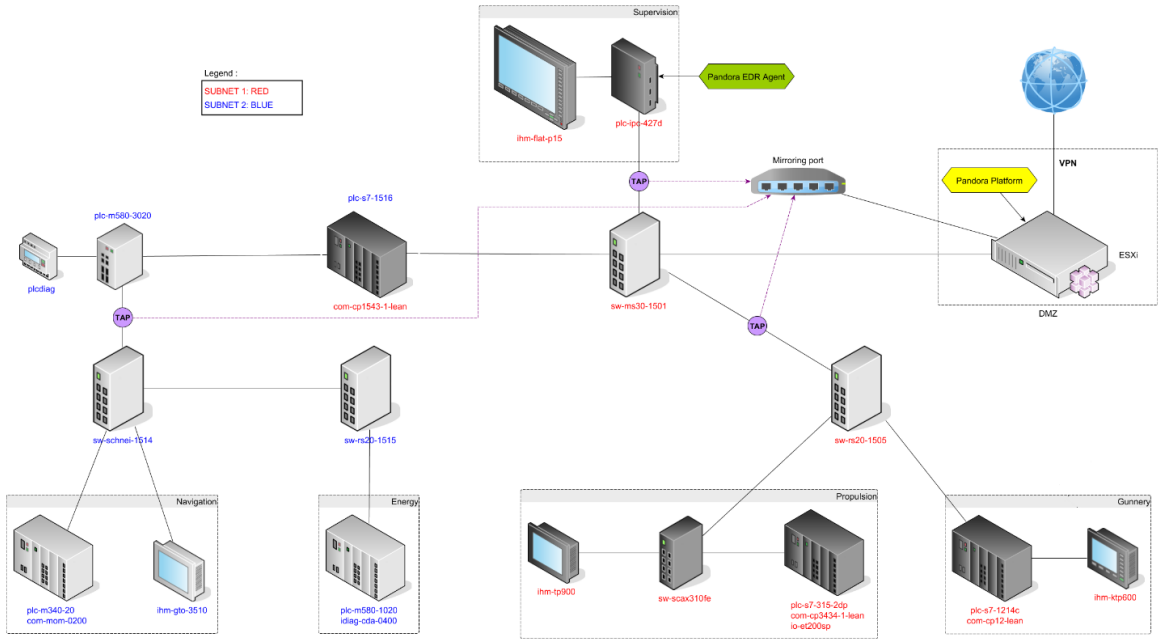
MAIN PROJECT MILESTONES



ASSESSMENT SCENARIO 1: NAVAL SECURITY (1/2)

- A hybrid warship platform is used based on real equipment and simulators.
- IT & OT technologies are present with implementation on both combat system and platform system.
- IT technologies that are used:
  - Client/server (Linux & Windows OS), Communication equipment, SCADA supervision (on Windows OS)
- OT technologies that are used :
  - Captors, Actuators, pumps and valves (fueling system); I/O modules to convert signals to IP communication
- Implementation of various panel of cyber threats (standards threats and advanced targeted threats)
- Threats may corrupt:
  - confidentiality (loss of secret) ,
  - Integrity and/or availability for sabotage with loss or corruption of functionality

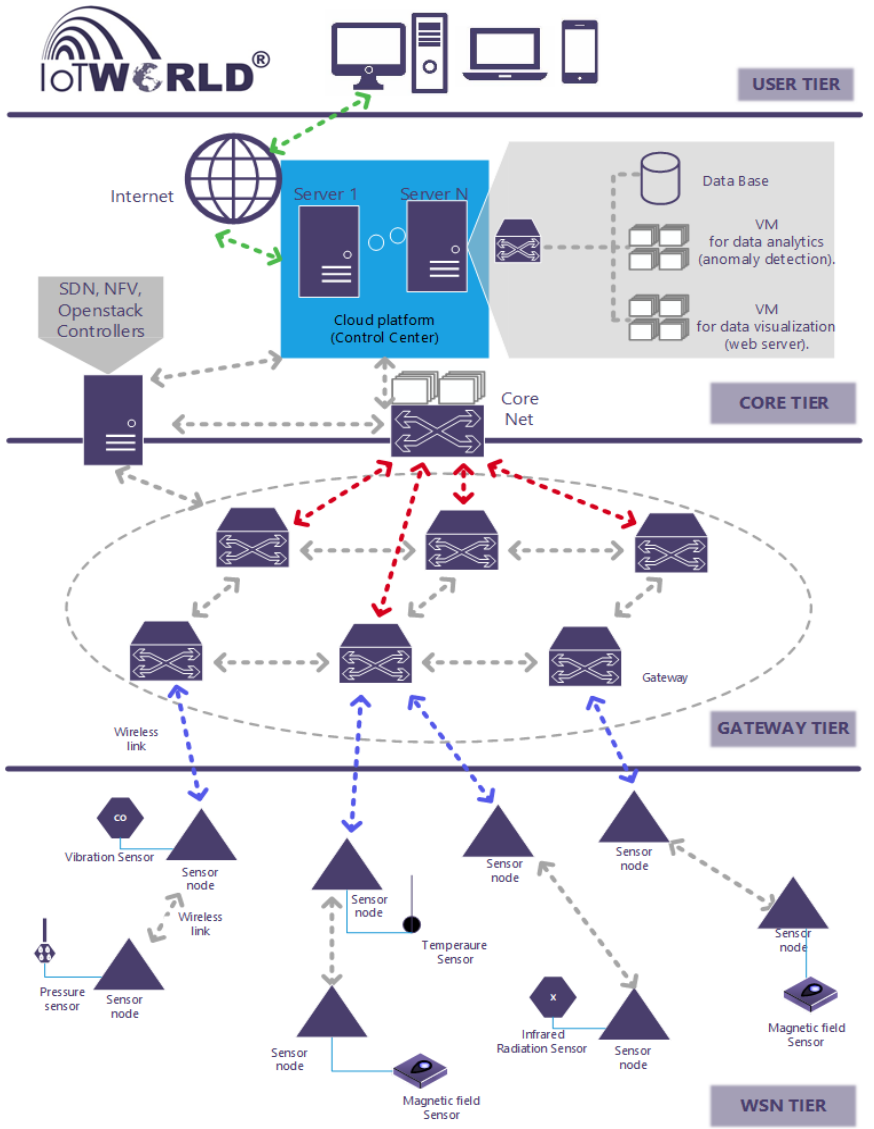
ASSESSMENT SCENARIO 1: NAVAL SECURITY (2/2)



- Scenarios to be tested emphasize on IT and OT protection and related attacks.
- Evaluating rule based and AI based detection capabilities and response capabilities of the platform.
- Emphasis to end to end scenarios to demonstrate the value of the platform.
- KPIs examined evaluate detection rate and total response time.

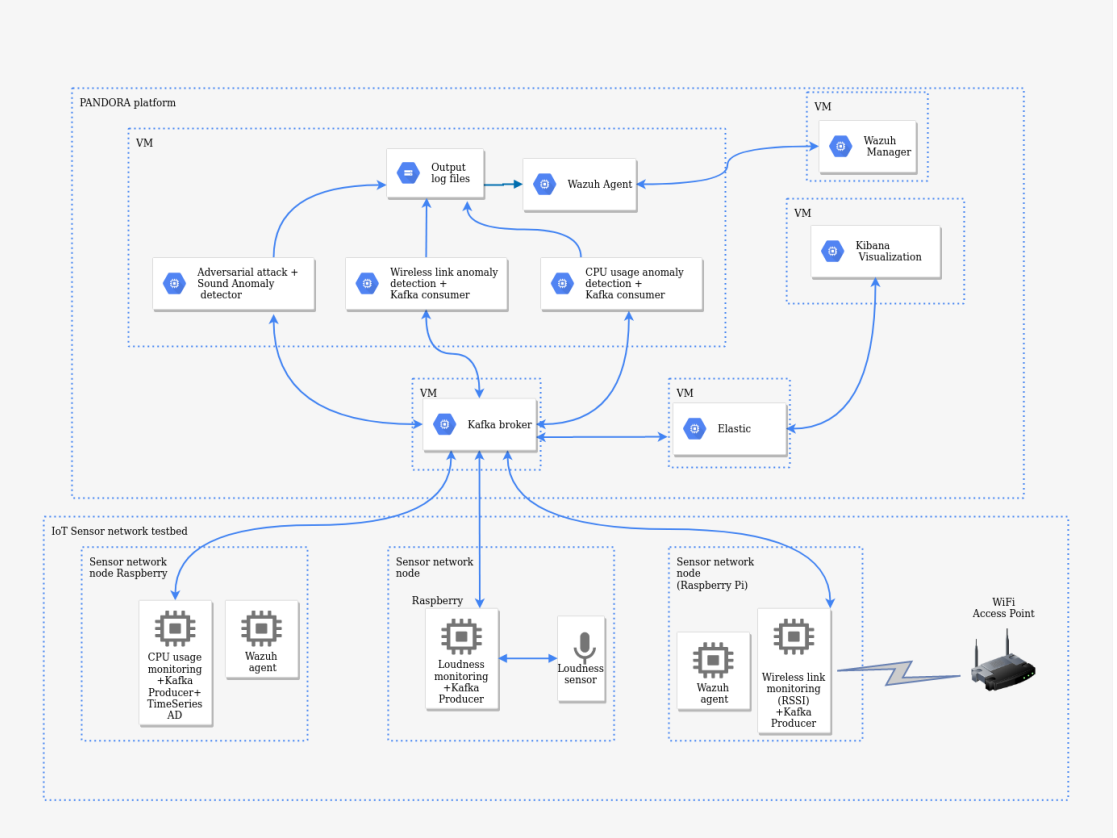
ASSESSMENT SCENARIO 11: SECURING MILITARY SENSOR N/W (1/2)

- Assessment of the incident detection and handling mechanisms in the context of cyber threats in military sensor networks.
- Threats that are considered:
  - Threats in communication links.
  - Threats in the sensor network nodes.
  - Threats in the information gathered by the WSN



ASSESSMENT SCENARIO 11: SECURING MILITARY SENSOR N/W (2/2)

- Attacks included in the evaluation:
  - Attacks to the sensor networks nodes resources
  - Jamming attack to the sensor network
  - Attacks to the sensor network data
- End to end scenarios are included, covering both detection and mitigation.
- Evaluation KPIs include:
  - Lost messages between the sensor network and the PANDORA platform.
  - True positive rate of the anomaly detector
  - Overall response time



PANDORA DEMONSTRATION EVENT – 7 DEC 2022

HELLENIC NATIONAL DEFENCE GENERAL STAFF
CYBER DEFENCE DIRECTORATE

kindly invites you to the

PANDORA PLATFORM ASSESSMENT-DEMONSTRATION event

that will be hosted (hybrid mode) in Athens, Greece
on 7th of December 2022

Introduction: PANDORA is an industrial cooperative project comprising fifteen entities from eight EU Member States, aiming to fulfill the High-Level Operational Requirements of the PESCO Project CTISP (Cyber Threats and Incident Response Information Sharing Platform). PANDORA is EDIDP funded and is supported by Hellenic and Cyprus MoDs with a commercial contract. This event is organized by the Hellenic National Defence General Staff / Cyber Defence Directorate and the PANDORA Industry Consortium Coordinator "Space Hellas S.A.", with the support of the Hellenic Ministry of National Defence and the Hellenic Ministry of Digital Governance.

Task: The TRL-7 system prototype of the PANDORA platform will be assessed and evaluated in a pre-operational environment against two relevant use cases: warship security and military sensor network security.

Agenda:

Thursday 07 Dec 2022			
	Time CET	Topics - Objectives	Remarks
1	09:00-09:15	Registration	Physical Attendees
2	09:15-09:30	Welcome and introductions	HNDGS/CD Directorate
3	09:30-10:00	Opening remarks	EL MoD, HNDGS & GDDIA
4	10:00-10:30	Project overview, key features and achievements	SPACE Hellas S.A.
5	10:30:10:45	Coffee Break	
6	10:45-11:15	PANDORA user interface and features walkthrough, testbed infrastructure	SPACE Hellas S.A.
7	11:15-12:30	Use Cases – presentation of topology and scenarios, demonstration	SPACE Hellas S.A.
8	12:30-12:45	Coffee Break	
9	12:45-13:00	Wrap-up and suggested roadmap for future developments	SPACE Hellas S.A.
10	13:00-13:30	Q&A - Discussion	
11	13:30-14:30	Lunch	

Participation: The PANDORA Platform Assessment-Demonstration event will be hosted in a HYBRID mode, virtually via the WebEx platform and physically at the premises of the Hellenic Ministry of Digital Governance (exact location provided below). To facilitate preparation of the event, each participant should register in the following registration link **NLT 30 Nov 2021 12:00 CET**:

https://bit.ly/pandora-demo

Points of Contact:

a. Col Nikolaos Stamatelatos
Email: n.stamatelatos@cd.mil.gr
Office: +30 210 657 6272

PANDORA

CYBER DEFENCE PLATFORM
FOR REAL-TIME THREAT HUNTING,
INCIDENT RESPONSE
AND INFORMATION SHARING

THANK YOU FOR YOUR ATTENTION

QUESTIONS?

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN DEFENCE INDUSTRIAL DEVELOPMENT PROGRAMME (EDIDP) UNDER GRANT AGREEMENT NO. EDIDP-CSAMN-SSS-2019-006-PANDORA

THIS PROJECT HAS RECEIVED FUNDING FROM THE MINISTRY OF NATIONAL DEFENCE OF THE HELLENIC REPUBLIC AND THE MINISTRY OF DEFENCE OF THE REPUBLIC OF CYPRUS