Resilmesh
securing cyber infrastructures

Open Call 2

Webinar 2 | 17/10/2025

Branka Stojanović (JR), Martin Husák (MUNI),
Tajana Medaković & Antonio Damasceno (F6S)

Funded by the European Union

CALL & TOPIC

HORIZON-CL3-2022-CS-01-01:
HORIZON Innovation Actions

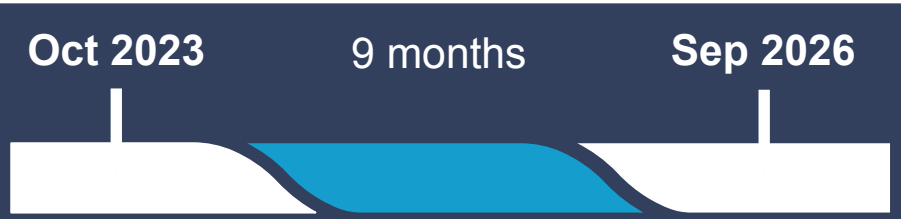
Horizon Europe

BUDGET

€5.6 million project budget

From which up to €360K will be granted to innovators in the Open Call #2

PROJECT DURATION



Funded by the European Union

WHO WE ARE?

13 Partners **7 Countries**

- **TUS**, Ireland [Coordinators]
- **GMV**, Spain
- **MUNI**, Czechia
- **SLP**, Ireland
- **F6S**, Ireland
- **JR**, Austria
- **UMU**, Spain
- **JAMK**, Finland
- **ALIAS**, Spain
- **Inforcert**, Italy
- **MURC**, Spain
- **KEMEA**, Greece
- **MONT**, France

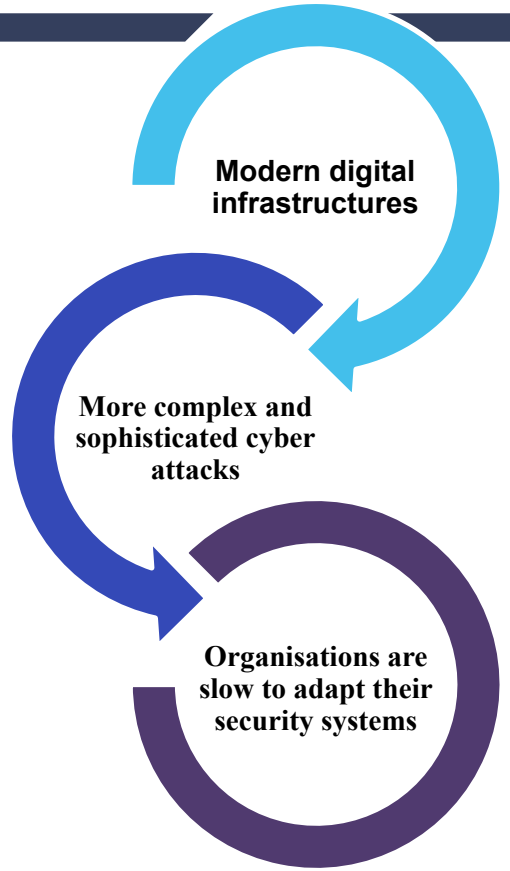
*Royal Holloway And Bedford New College [associated partner]

Funded by the European Union

Challenges

Modern digital infrastructures are complex and dispersed, leading to numerous attack vectors. Advanced persistent threats (APTs) target organizations with sophisticated, multi-vector attacks.

Many organizations are slow to adapt, needing modern security models like Zero Trust (ZT) and Secure Systems Edge (SSE) to manage these evolving threats.



Funded by the European Union

Resilmesh project aims to deliver an open and extensible security operations platform with advanced cyber situational awareness and detection/response capabilities to manage security and resilience in complex and dispersed digital services and infrastructures

FOCUS ON THREE STRATEGIC INFRASTRUCTURE CATEGORIES

>> **+ 5 Open Call** use cases

>> **8** pilots in total

>> **2** Open Calls

Funded by the European Union

Project Specific Objectives

- Improving end-to-end data aggregation and security control interoperability in dispersed digital infrastructures
- Giving CSIRTs better awareness of the service and asset dependencies of their network
- Helping CSIRTs to build cyber resilience capacity
- Developing AI based algorithms and tools for early and ongoing attack detection and prediction
- Developing a situation assessment system to view and forecast network level risk

Funded by the European Union

Open Call #2

Applications until Nov 5th 5PM CET

Evaluation & Onboarding until December

Challenges

Extensions to Resilmesh via the collaboration mesh IRP's

New Analytic Algorithms and Architectures

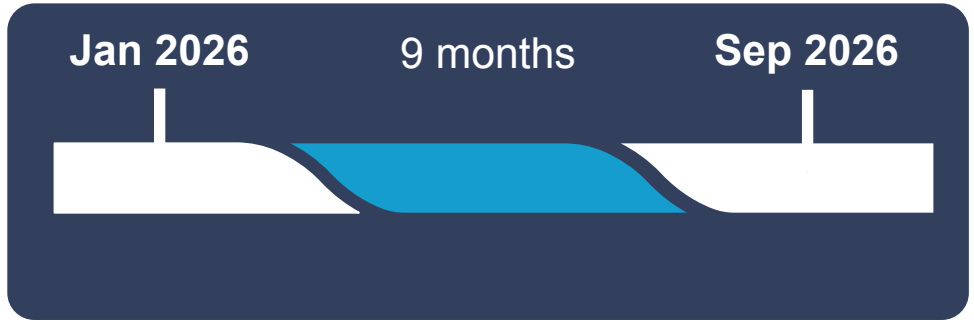
BUDGET

Open Call 2 budget: €360K

5 projects

Up to 72K per project

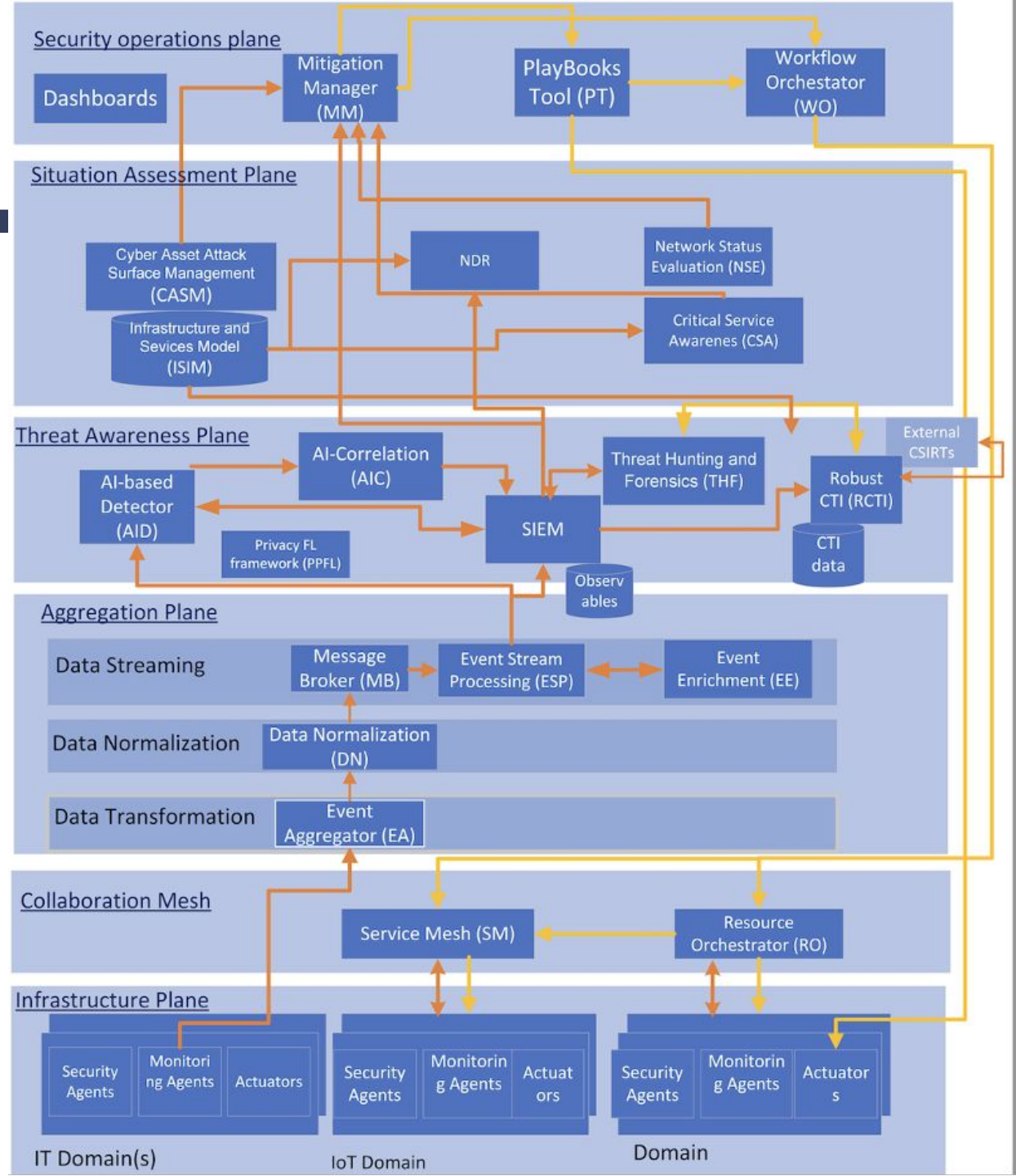
Projects' participation



Funded by the European Union

High level Architecture

- **Aggregation Plane -** collects, aggregates, normalizes and streams data and events from multiple heterogeneous sources including logs, IDS, network
- **Collaboration Mesh -** collaborating underlay enable the operation of the system across the dispersed digital infrastructure
- **Threat Awareness Plane-** suite of analytics functions to manage event correlation and alarming, attack detection and prediction, CTI sharing and threat hunting.
- **Situation Assessment Plane** - captures dependencies between services onto the IT/OT resources that realise them; visualises the current network risk status ; forecasts the near-term situation evolution
- **Security Operations Plane** – automates and orchestrates response and mitigation actions



Funded by the European Union

High level Architecture

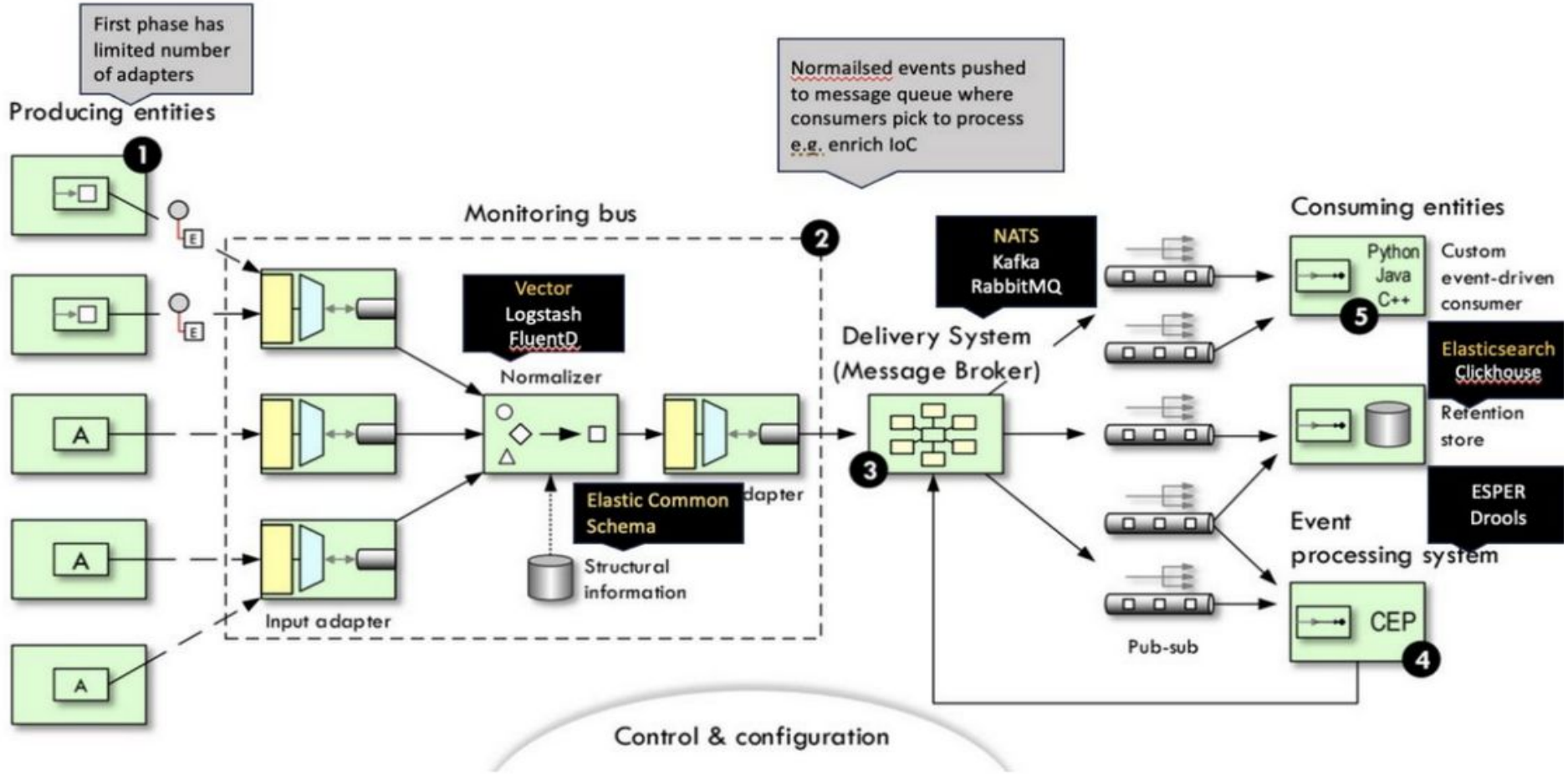


Figure 6 Resilmesh Aggregation and Service Layer Implementation Architecture

Challenge 1: Extensions to Resilmesh via the collaboration mesh IRP's

i) Connectivity Mesh

- Demonstrate how a K8S service mesh capability can provide adaptivity to improve the resilience of the Resilmesh platform
- Address known K8S security issues that could arise in the use of Kubernetes service mesh such as mTLS configuration issues,

ii) Interworking Mesh

- Extend the interoperability in the security application layers i.e. Threat Awareness, Situation Assessment and Security Operations- between Resilmesh components and other tools along the lines of the Open XDR Architecture (OXA) principles including the use of 'Meshroom' tool.

Funded by the European Union

Resilmesh
securing cyber infrastructures

Connectivity Mesh

Connectivity Mesh = Service Mesh

- Linkerd
- Istio

Provides communication security and resilience

- Service Discovery
- Load Balancing
- Communication Resiliency
- Security Observability
- Routing Control
- API
- Fault Injection

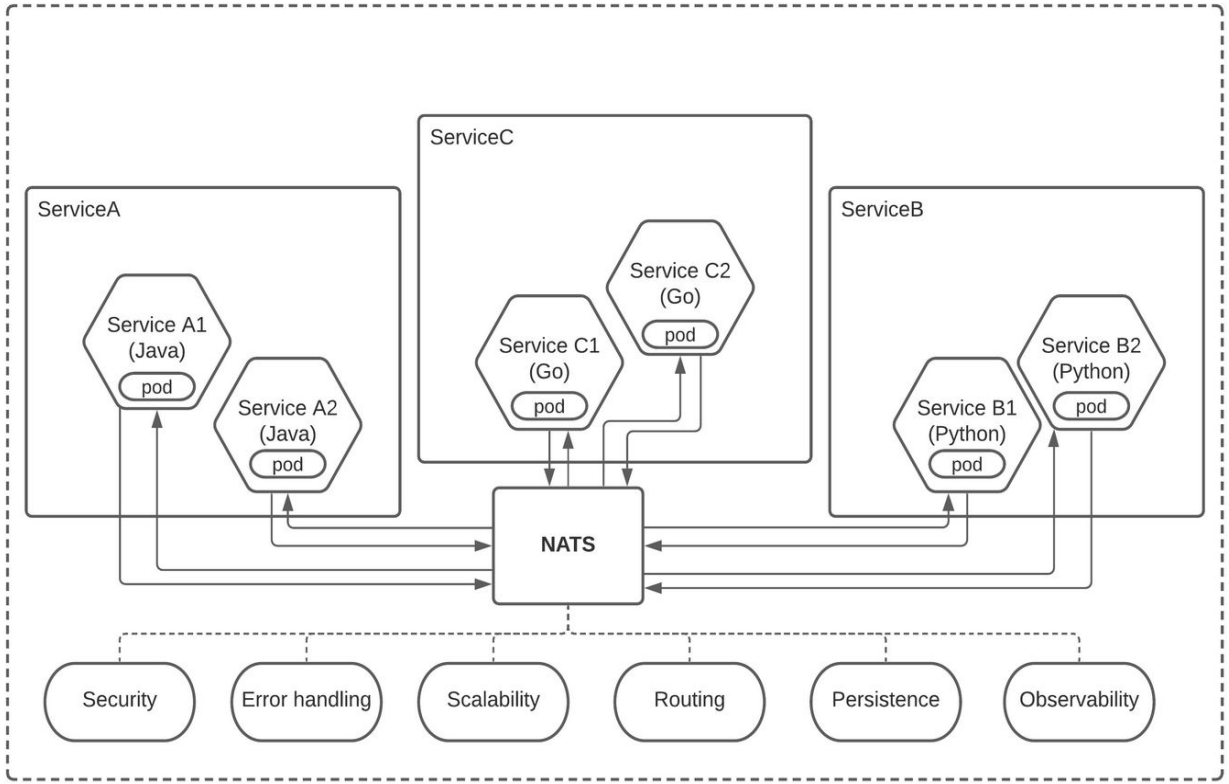
Funded by the European Union

NATS as Service Mesh

NATS can be used to implement service mesh capability

- See "**Using NATS to Implement Service Mesh Functionality**"

https://dale-bingham-soteriasoftware.medium.com/using-nats-to-implement-service-mesh-functionality-part-1-service-discovery-5f2e6088843b



Funded by the European Union

Connectivity Mesh Resilience

Service mesh offers service and communication security and resiliency

- How can these features be leveraged to improve the resiliency of the Resilmesh platform- specifically **redundancy** and **dynamic positioning** ?

Funded by the European Union

Platform Resilience

DYNAMIC POSITIONING:

Definition: Distribute and dynamically relocate functionality or system resource.

REDUNDANCY:

Definition: Provide multiple protected instances of critical resources.

* Cyber Resilient Systems, NIST SP800_160 v2

Resilmesh Property/ Resiliency Technique	**Resilmesh Approach**
Adaptive • **Redundancy (Platform)** • **Dynamic Positioning (Platform)** • **Adaptive Response**	Provide multiple protected instances of critical resources
	Flexible function allocation and composition
	Risk-based Mitigation Orchestration

Funded by the European Union

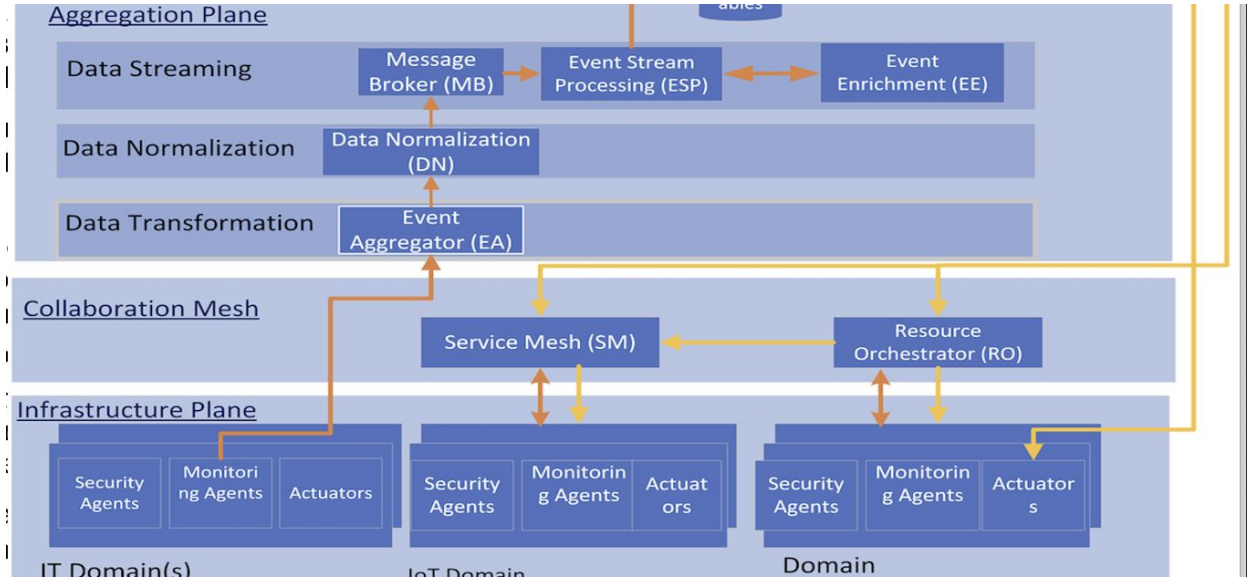
Service mesh to provide resilience

- How can a NATS service mesh be used to resilience in the Resilmesh platform? E.g.
  - If a Vector gateway fails; (reroute to alternative – DP)
  - If the event enrichment fails; (reroute / reconfigure)
  - If the the SIEM fails can a secondary SIEM be used (redundancy)
  - provide duplicated connection / fail over connection to high value components e.g. ISIM, SIEM, MM

Funded by the European Union

Platform K8S evaluation

- The Resilmesh platform must be deployed using K8S
- Evaluate known security issues such as
  - mTLS configuration issues,
  - sidecar injection vulnerabilities,
  - lack of ingress/egress controls,
  - certificate and key management risks
  - etc.



Funded by the European Union

Resilmesh
securing cyber infrastructures

Interoperability Mesh

- Use of open protocols, standards and best practices to enable ease of *integration* and *cooperation* between security applications/controls including third party tools

Funded by the European Union

Resilmesh
securing cyber infrastructures

Interoperability & Integration best practices

- Create a collaborative system of tools and controls to secure complex and dispersed distributed enterprise *, **.
- Adopt integration best practices through a mix of open standards and interfaces, proprietary APIs, and point integrations*, **
- Consolidated dashboards – providing end-to-end visibility on security tasks and risks*

* Cybersecurity Mesh, Gartner, ** Open Cyberecurity Alliance (OCA) Open XDR

Funded by the European Union

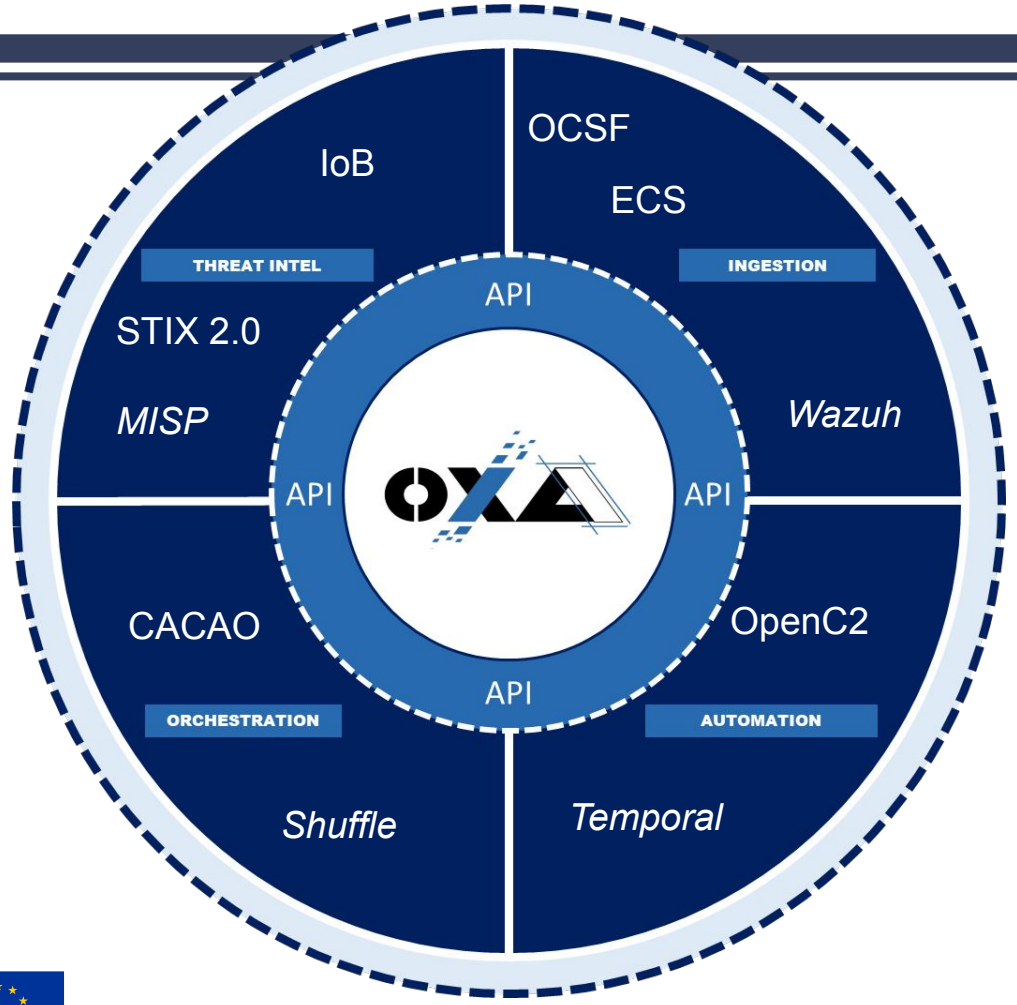
OpenXDR -OXA

Resilmesh
securing cyber infrastructures

OXA is a common set of libraries and interfaces that allows cybersecurity industry to interact

https://github.com/opencybersecurityalliance/oxa

IoB - Indicators of Behaviour



Funded by the European Union

Resilmesh Integration reference Point (IRP)

- *Sensor IRP (SIRP*) -the point at which security events and logs are ingested in the system from security sensors – shown as monitoring agents in the Infrastructure Plane.
- *Connectivity IRP (CIRP)* – provides connectivity and message delivery from any functional component to any other functional component across any type or range of network. The CIRP is implemented by the Message Broker – by default NATS
- *Wazuh IRP (WIRP)*- Wazuh plays a critical role as an integration function in Resilmesh. It can forward both unprocessed events (logs) or actual alerts to other applications and it also provides a query based API to allow applications to access its data.

Funded by the European Union

Resilmesh Integration reference Point (IRP)

- *Wazuh IRP (WIRP)*- Wazuh plays a critical role as an integration function in Resilmesh. It can forward both unprocessed events (logs) or actual alerts to other applications and it also provides a query based API to allow applications to access its data.
- *Asset IRP (AIRP)*- This IRP gives access to the asset management database to security applications for risk calculation, mission criticality analysis, attack mitigation manager, etc. This IRP is provided by the ISIM and CASM functional components.
- *Mitigation MIRP* – integrating new controls to the MM via OpenC2

Funded by the European Union

Resilmesh
securing cyber infrastructures

Examples

- Extending CASM to new domains such as cloud
- Integrating other CTI platforms or feeds (other than MISP)
- Sharing playbooks via CACAO with other systems
- Integrating new NIDS/HIDS feeds to Wazuh
- Integrating new security controls to MM

Funded by the European Union

Challenge 2: New Analytic Algorithms and Architectures

i) User and Entity Behaviour Analytics (UEBA)

UEBA can apply to both endpoint and network traffic behaviours. One approach here could be to extend the Resilmesh NDR functional component with network behaviour analytics

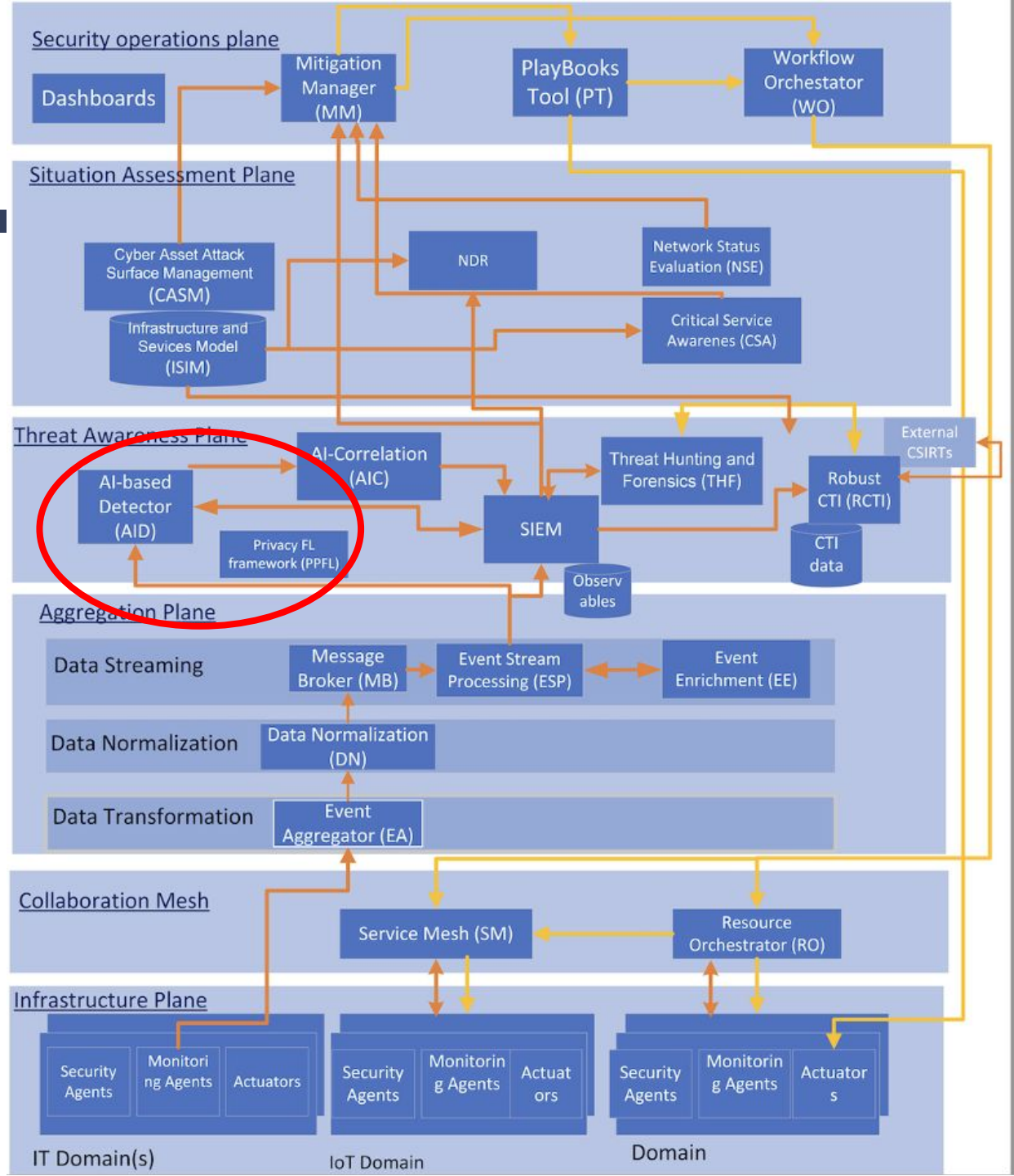
ii) **Novel edge AI AD architectures**

- Ensemble methods
- Distributed deep learning
- Incremental learning
- Edge-to-Edge Collaborative Anomaly Detection

Funded by the European Union

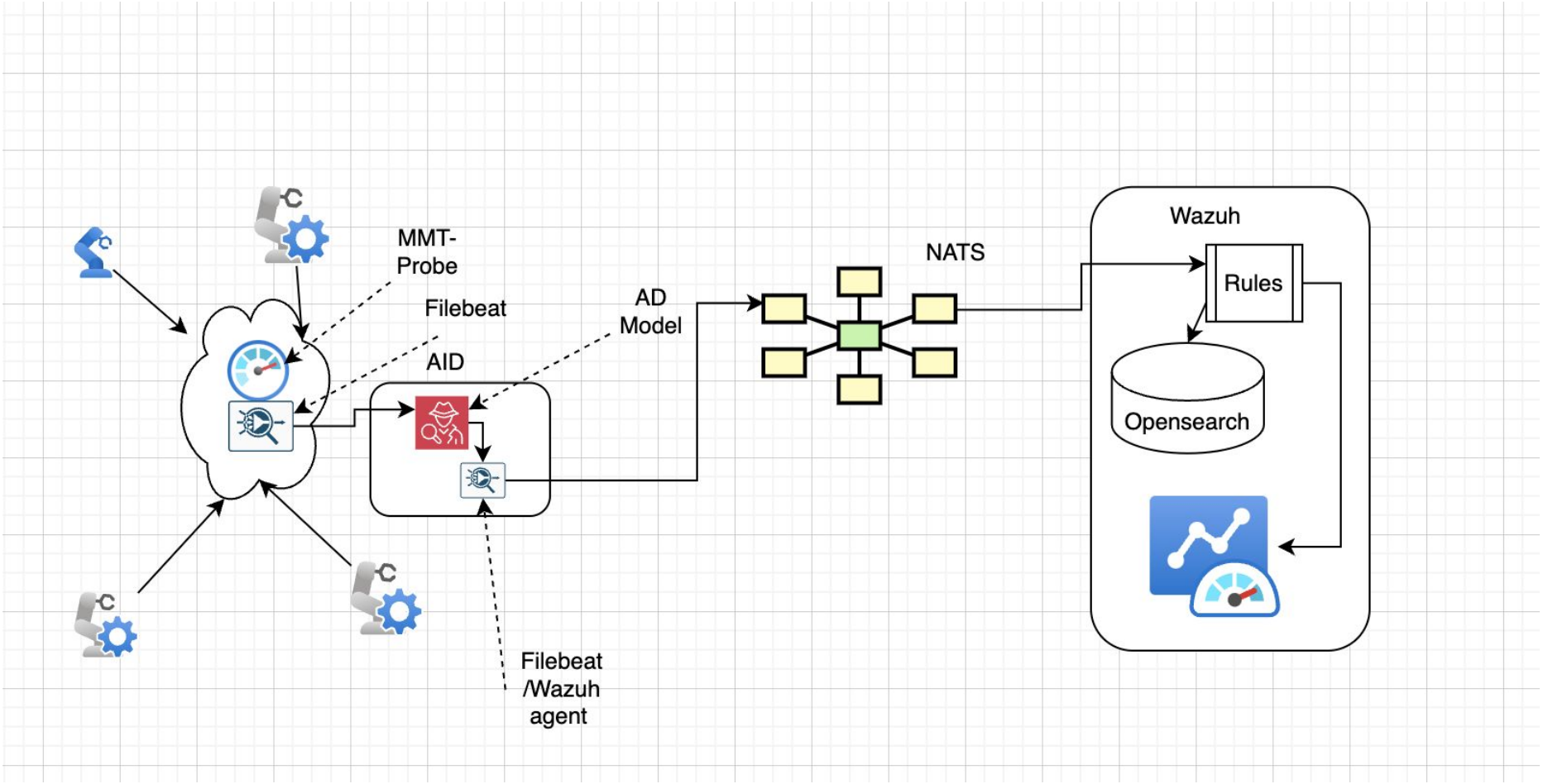
High level Architecture

- **Aggregation Plane -** collects, aggregates, normalizes and streams data and events from multiple heterogeneous sources including logs, IDS, network
- **Collaboration Mesh -** collaborating underlay enable the operation of the system across the dispersed digital infrastructure
- **Threat Awareness Plane-** suite of analytics functions to manage event correlation and alarming, attack detection and prediction, CTI sharing and threat hunting.
- **Situation Assessment Plane** - captures dependencies between services onto the IT/OT resources that realise them; visualises the current network risk status ; forecasts the near-term situation evolution
- **Security Operations Plane** – automates and orchestrates response and mitigation actions



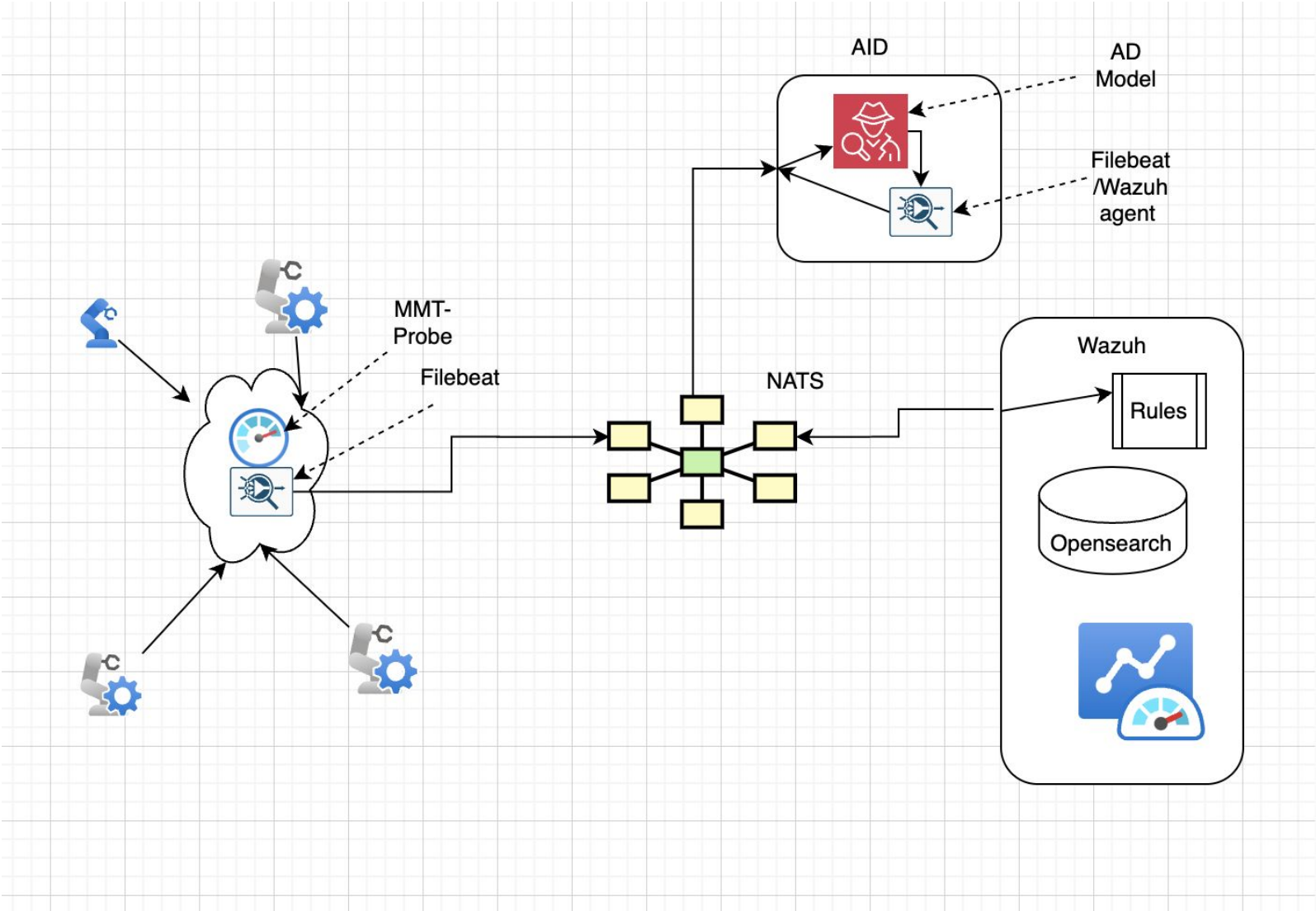
Funded by the European Union

AID: Edge analytics and detection



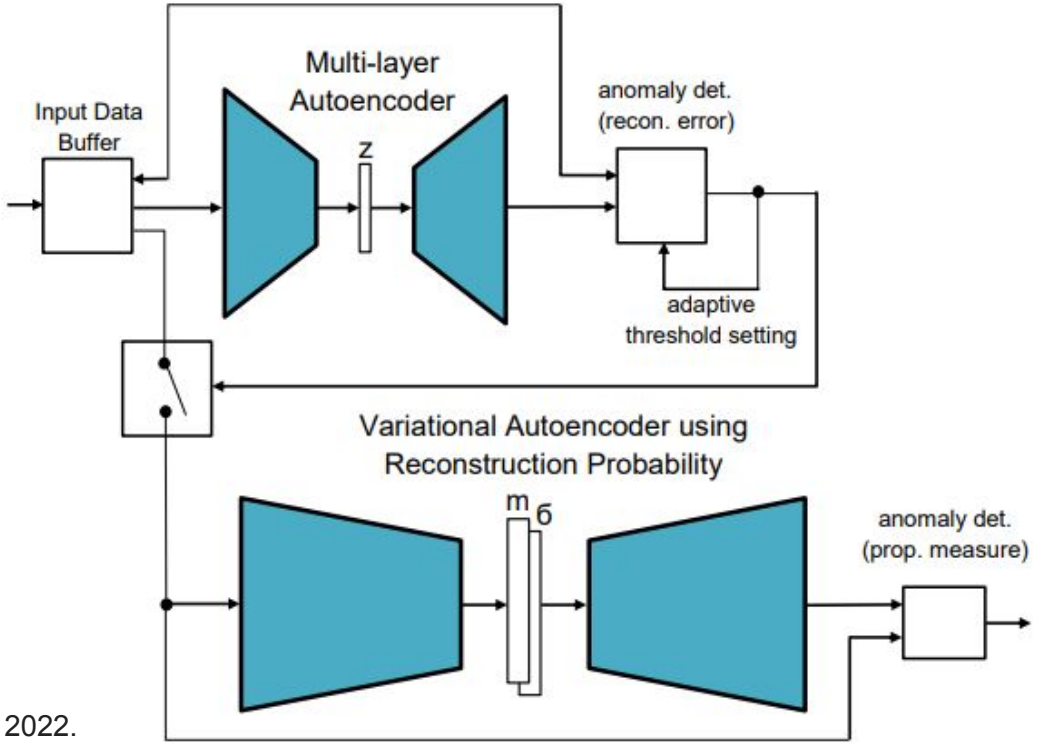
Funded by the European Union

AID: Centralised detection



AID: Autoencoders

- Two-stage anomaly detection using stacked Autoencoders



Neuschmied, H., Winter, M., Stojanović, B., Hofer-Schmitz, K., Božić, J. and Kleb, U., 2022. Apt-attack detection based on multi-stage autoencoders. *Applied Sciences*, *12*(13), p.6816. https://www.mdpi.com/2076-3417/12/13/6816

Funded by the European Union

AID: Data sources

- Network traffic – NetFlow data

No.	timestamp	Time	Source	Destination	Protocol	Length	Info
1	2023-01-22 04:10:36,642504	0.000000	185.175.0.3	185.175.0.4	TCP	66	51094 → 502 [ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
2	2023-01-22 04:10:36,642516	0.000012	185.175.0.4	185.175.0.3	TCP	66	502 → 51092 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197813679
3	2023-01-22 04:10:36,642527	0.000023	185.175.0.3	185.175.0.4	TCP	66	51092 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
4	2023-01-22 04:10:36,642540	0.000036	185.175.0.4	185.175.0.3	TCP	66	502 → 51090 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197813658
5	2023-01-22 04:10:36,642550	0.000046	185.175.0.3	185.175.0.4	TCP	66	51090 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
6	2023-01-22 04:10:36,642564	0.000060	185.175.0.4	185.175.0.3	TCP	66	502 → 51088 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197808652
7	2023-01-22 04:10:36,642574	0.000070	185.175.0.3	185.175.0.4	TCP	66	51088 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
8	2023-01-22 04:10:36,642588	0.000084	185.175.0.4	185.175.0.3	TCP	66	502 → 51086 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197808630
9	2023-01-22 04:10:36,642598	0.000094	185.175.0.3	185.175.0.4	TCP	66	51086 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
10	2023-01-22 04:10:36,642611	0.000107	185.175.0.4	185.175.0.3	TCP	66	502 → 51084 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197808608
11	2023-01-22 04:10:36,642621	0.000117	185.175.0.3	185.175.0.4	TCP	66	51084 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
12	2023-01-22 04:10:36,642634	0.000130	185.175.0.4	185.175.0.3	TCP	66	502 → 51082 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197808585
13	2023-01-22 04:10:36,642645	0.000141	185.175.0.3	185.175.0.4	TCP	66	51082 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
14	2023-01-22 04:10:36,642657	0.000153	185.175.0.4	185.175.0.3	TCP	66	502 → 51080 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197808563
15	2023-01-22 04:10:36,642667	0.000163	185.175.0.3	185.175.0.4	TCP	66	51080 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
16	2023-01-22 04:10:36,642681	0.000177	185.175.0.4	185.175.0.3	TCP	66	502 → 51078 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197803556
17	2023-01-22 04:10:36,642691	0.000187	185.175.0.3	185.175.0.4	TCP	66	51078 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
18	2023-01-22 04:10:36,642705	0.000201	185.175.0.4	185.175.0.3	TCP	66	502 → 51076 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197803534
19	2023-01-22 04:10:36,642716	0.000212	185.175.0.3	185.175.0.4	TCP	66	51076 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
20	2023-01-22 04:10:36,642729	0.000225	185.175.0.4	185.175.0.3	TCP	66	502 → 51074 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197803512
21	2023-01-22 04:10:36,642740	0.000236	185.175.0.3	185.175.0.4	TCP	66	51074 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
22	2023-01-22 04:10:36,642753	0.000249	185.175.0.4	185.175.0.3	TCP	66	502 → 51072 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197803489
23	2023-01-22 04:10:36,642763	0.000259	185.175.0.3	185.175.0.4	TCP	66	51072 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
24	2023-01-22 04:10:36,642775	0.000271	185.175.0.4	185.175.0.3	TCP	66	502 → 51070 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197803468
25	2023-01-22 04:10:36,642785	0.000281	185.175.0.3	185.175.0.4	TCP	66	51070 → 502 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=4197859519 TSecr=1694360154
26	2023-01-22 04:10:36,642801	0.000297	185.175.0.4	185.175.0.3	TCP	66	502 → 51068 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0 TSval=1694360154 TSecr=4197798461

ts	src_ip	src_port	dst_ip	dst_port	proto	service	duration	src_bytes	dst_bytes	conn_state	missed_byte	src_pkts	src_ip_bytes	dst_pkts	dst_ip_bytes
1554198358	3.122.49.24	1883	192.168.1.152	52976	tcp	-	8.054.953.026	1762852	41933215	OTH	0	252181	14911156	2	236
1554198358	192.168.1.79	47260	192.168.1.255	15600	udp	-	0	0	0	S0	0	1	63	0	0

dns_query	dns_qclass	dns_qtype	dns_rcode	dns_AA	dns_RD	dns_RA	dns_rejected	ssl_version	ssl_cipher	ssl_resumed	ssl_establish	ssl_subject	ssl_issuer
-	0	0	0	-	-	-	-	-	-	-	-	-	-
-	0	0	0	-	-	-	-	-	-	-	-	-	-

http_trans_d	http_metho	http_uri	http_referre	http_version	http_reques	http_respon	http_status_	http_user_a	http_orig_m	http_resp_m
-	-	-	-	-	0	0	0	-	-	-
-	-	-	-	-	0	0	0	-	-	-

Funded by the European Union

AID: Data sources

- Sensor readings (e.g. temperature, humidity…)
- Log files

Image source: https://www.semrush.com/blog/log-file-analysis/

Funded by the European Union

Example - D3FEND

Network Traffic Community Deviation

D3-NTCD

D3-NTCD (Network Traffic Community Deviation)

Definition

Establishing baseline communities of network hosts and identifying statistically divergent inter-community communication.

How it works

Hosts/users within a computer network are analyzed to identify communities of hosts which frequently communicate. Future communications between communities that don't usually communicate can then be detected. For example, if a community of hosts that communicate in support of a company's finance division suddenly starts to access the code server usually accessed only by engineers, this may indicate unauthorized activity.

Considerations

- Potential for false positives in very dynamic network environments.
- Attackers that move low and slow may not differentiate their behavior enough to trigger an alert.

Funded by the European Union

NDR base - Montimage MMT

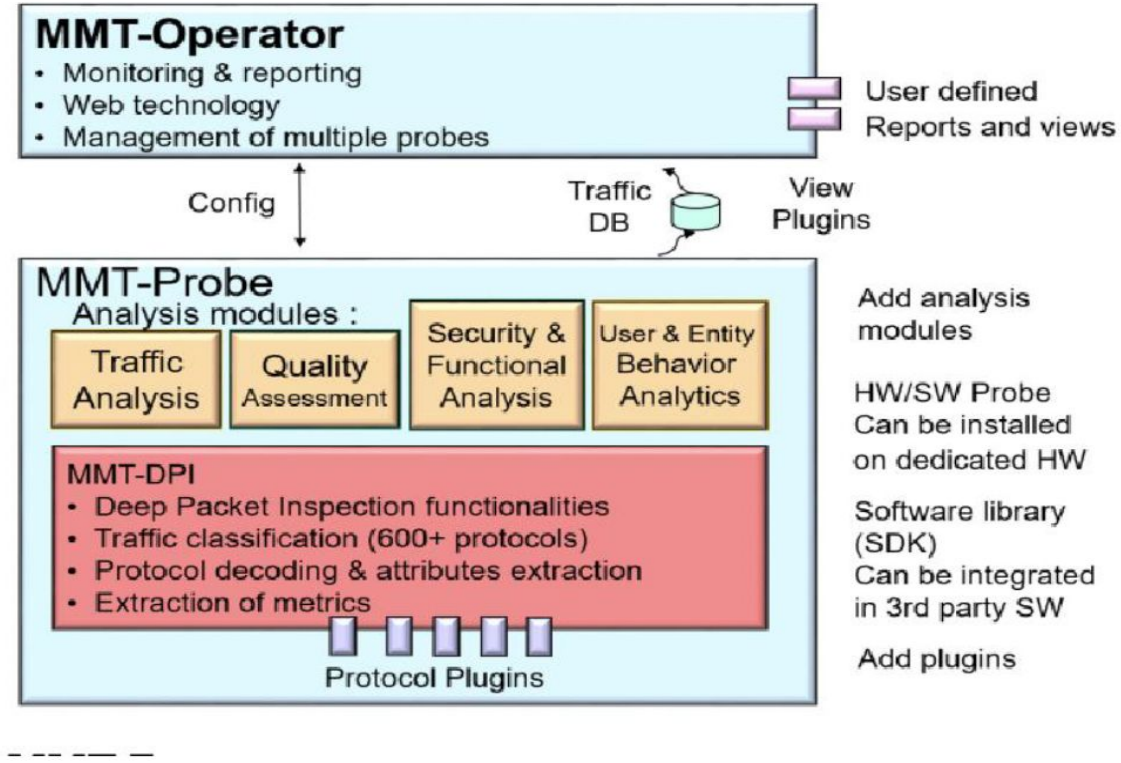


Figure 27 - NDR based on MMT

https://www.montimage.com/products/MMT_Brochure.pdf

Funded by the European Union

For more Information:

- **D2.3 System Architecture v2**

https://resilmesh.eu/wp-content/uploads/2025/09/Resilmesh-D2.3-0725-Resilmesh-Architecture-v2-B.pdf

- **D3.1 Resilmesh Platform Reference Implementation**

https://resilmesh.eu/wp-content/uploads/2024/07/Resilmesh_D3.1-0224_Platform_Reference_Implementation-_A-1.pdf

Funded by the European Union

HOW TO PARTICIPATE?

1

SELF ASSESSMENT

Are you:
1. Legal entity or
2. Consortia of legal entities

Elligible entities: mid-caps, SMEs or research organisations (RTOs or academia).

2

ADDITIONAL ELLIGIBILITY CRITERIA

Are you:

1. based in an eligible country?

2. addressing of the **two** challenges?

3

PREPARE APPLICATION

1. Attend webinars

2. Check out FAQ

3. Check out all the documents that you need to submit

4

SUBMIT APPLICATION

Apply to an open call submitting a detailed version of your project

BEFORE 05/11/2025 17:00 CET

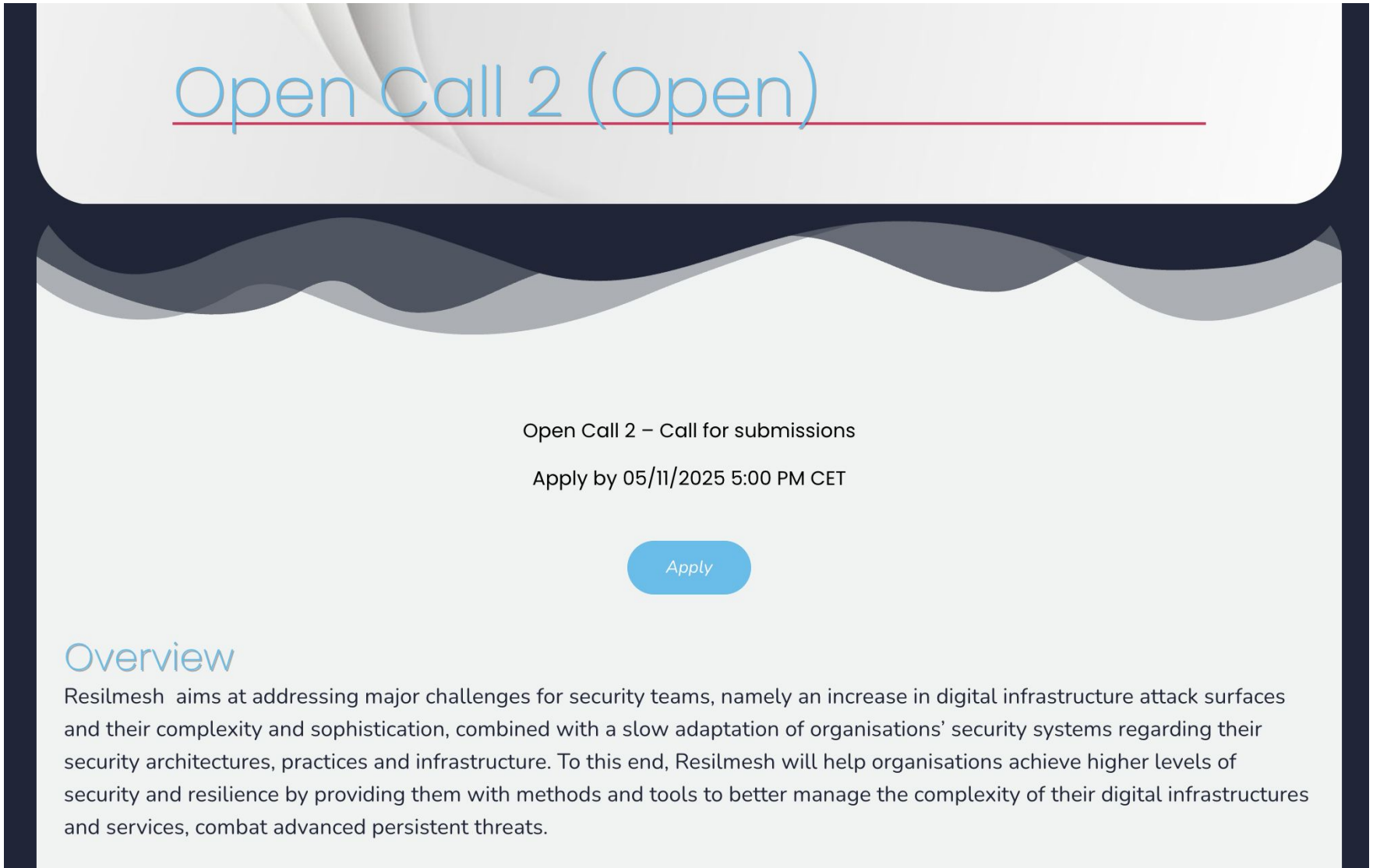
5

TRANSFORMATION

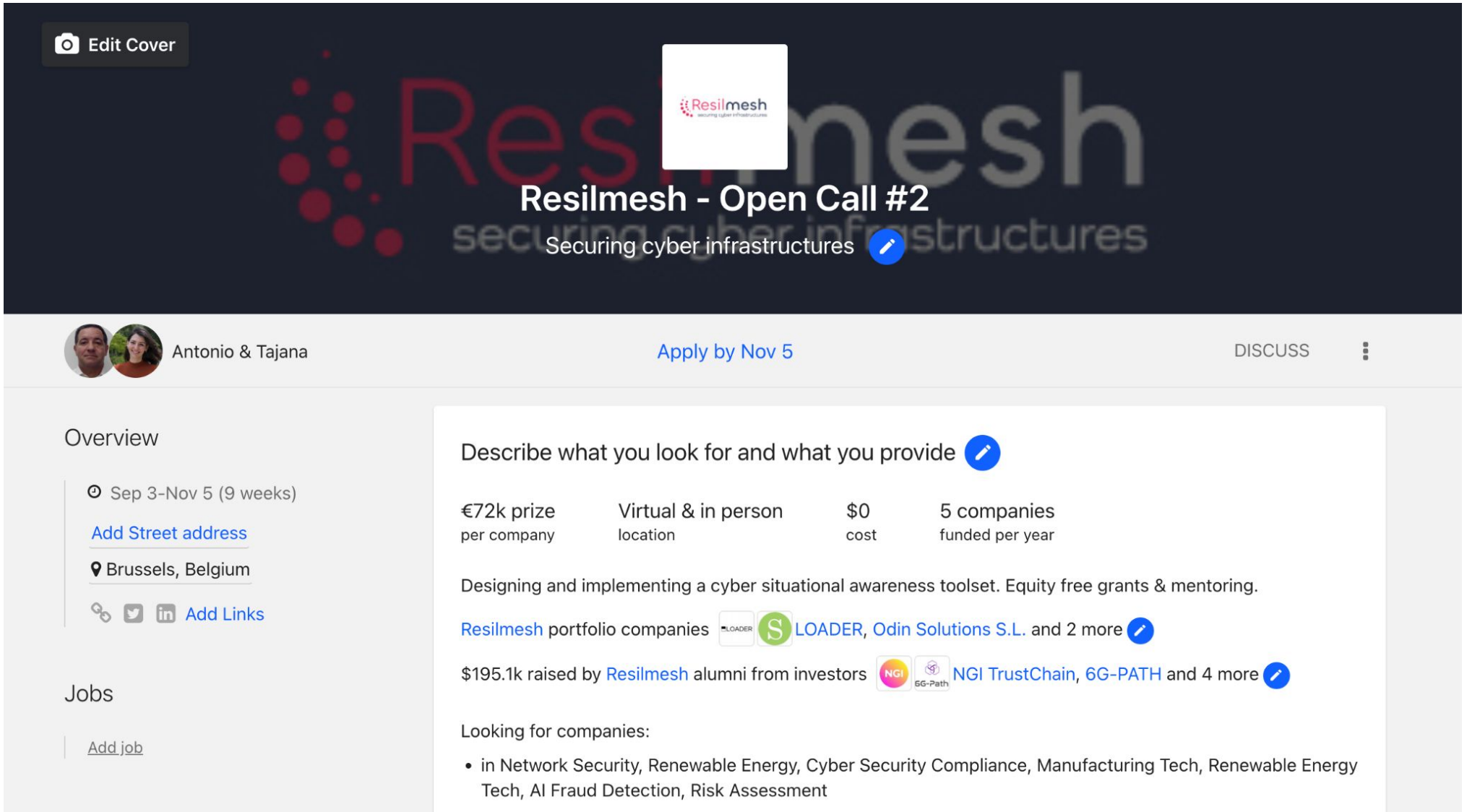
Once accepted: Initiate your transformation project, being accompanied during the process

Funded by the European Union

Step 1: Resilmesh website



Step 2: F6S platform



Step 3: Application form

SECTION 1: Proposal Identification

1 **Proposal Title ***

2 **Proposal Acronym ***

Should be different than the Proposal name

3 **Proposal Summary ***

Please provide a detailed summary that will be used for promotional purposes and made public.
Maximum length 1500 characters (including spaces).

SECTION 2: Applicant information

According to Guidelines for applicants Resilmesh Open Call #2 will finance

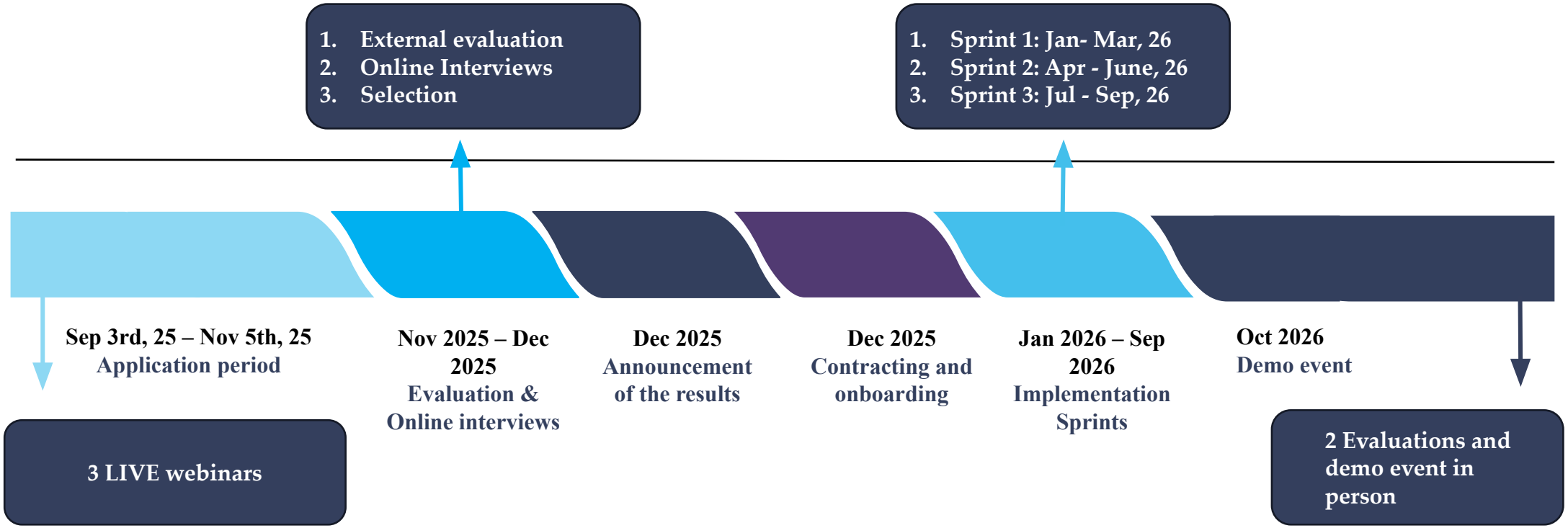
- Single entity - Micro, small and medium-sized enterprises (SMEs)

OR

- Consortium of maximum of 2 entities - Micro, small and medium-sized enterprises (SMEs)

Please note to justify the role of each organisation, and the capacity in terms of expertise and resources for the selected topic in the Annex 2 Proposal Technical Annex (template).
In case of a single entity application "Applicant 2" fields should not be answered.

TIMELINE



Funded by the European Union

Resilmesh
securing cyber infrastructures

Thank you for your attention!
Next webinar: 29/10 [10:00 AM CET]
Questions?

Funded by the European Union

Resilmesh

securing cyber infrastructures

More information:

www.resilmesh.eu

Stay informed about the progress of the project by subscribing to **our newsletter**

Ask questions directly:

Help desk: resilmesh@f6s.com

F6S discussion board: www.f6s.com/resilmesh-open-call-1/discuss