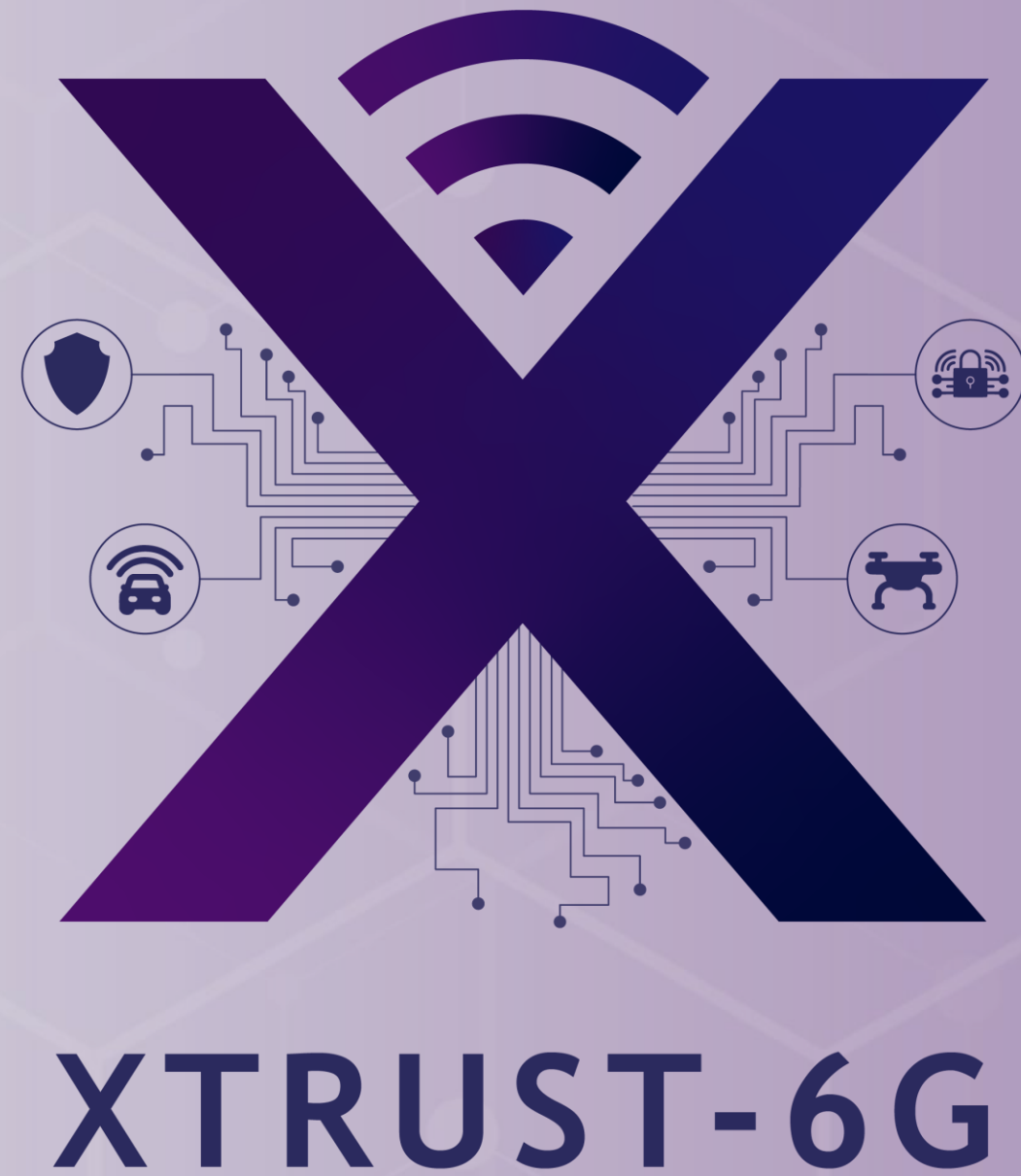




# XTRUST-6G: Trusted and Resilient Cybersecurity for Future 6G Critical Infrastructures

**Dr Gueltoom Bendiab and Dr Rinat Khusainov**  
**University of Portsmouth**



Co-funded by  
the European Union



Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# Why 6G is important for Critical Infrastructure?



**6G: A highly connected ecosystem where critical services, infrastructure, people, machines and autonomous systems interact.**

Critical services & public infrastructure

Smart energy & EV charging

Autonomous vehicles & transportation

UAVs & emergency operations

**6G**

Industrial systems & robotics

Massive IoT & edge devices

Cloud-edge-RAN infrastructures

Healthcare & connected medical systems



Co-funded by  
the European Union

**6G SNS**

Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# Why Cybersecurity for 6G Critical Infrastructure?



**Massive and heterogeneous connectivity:** Billions of devices, users, services and subnetworks increase the attack surface.

**Highly distributed and complex infrastructure:** Cloud, edge, RAN, core, IoT and specialised subnetworks make security monitoring and management difficult.

**Open and virtualised architectures:** O-RAN, open APIs, microservices and cloud-native components introduce new vulnerabilities and attack vectors.

**AI/ML-enabled attacks:** Adversarial AI, data poisoning, model manipulation and AI-driven attacks threaten increasingly autonomous 6G systems.

**Software and supply-chain risks:** Extensive use of open-source software and third-party components increases dependency and supply-chain vulnerabilities.



Co-funded by  
the European Union

6G SNS

Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# Why Cybersecurity for 6G Critical Infrastructure?



**Dynamic and evolving threats:** Sophisticated attacks require continuous detection, threat intelligence and adaptive security mechanisms.

**Difficult-to-define security perimeter:** Traditional perimeter-based security is no longer sufficient for distributed 6G ecosystems, requiring Zero Trust approaches.

**Security vs. sustainability:** Security mechanisms must protect highly connected infrastructures while maintaining low energy consumption, scalability and performance.

**The challenge is no longer just securing the network — it is securing a highly distributed, intelligent and interconnected critical infrastructure.**



Co-funded by  
the European Union

**6G SNS**

Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

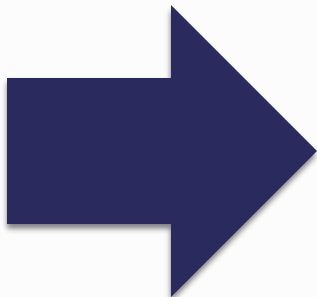
*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# From Traditional Security to Zero Trust



## New threats

- Advanced multi-stage attacks
- Lateral movement
- AI-enabled attacks
- Supply-chain vulnerabilities
- O-RAN/virtualisation attacks
- Privacy threats
- Quantum-era threats



## Critical Infrastructure Requires Continuous Trust

| Traditional Security       | Zero-Trust                     |
|----------------------------|--------------------------------|
| Trust inside the perimeter | Never trust, always verify     |
| Static access control      | Dynamic risk-based access      |
| Periodic security checks   | Continuous monitoring          |
| Isolated security tools    | Integrated security ecosystem  |
| Reactive response          | Proactive & automated response |



Co-funded by  
the European Union



Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# XTRUST-6G : Project Information



**19**  
Partners



**12**  
Countries

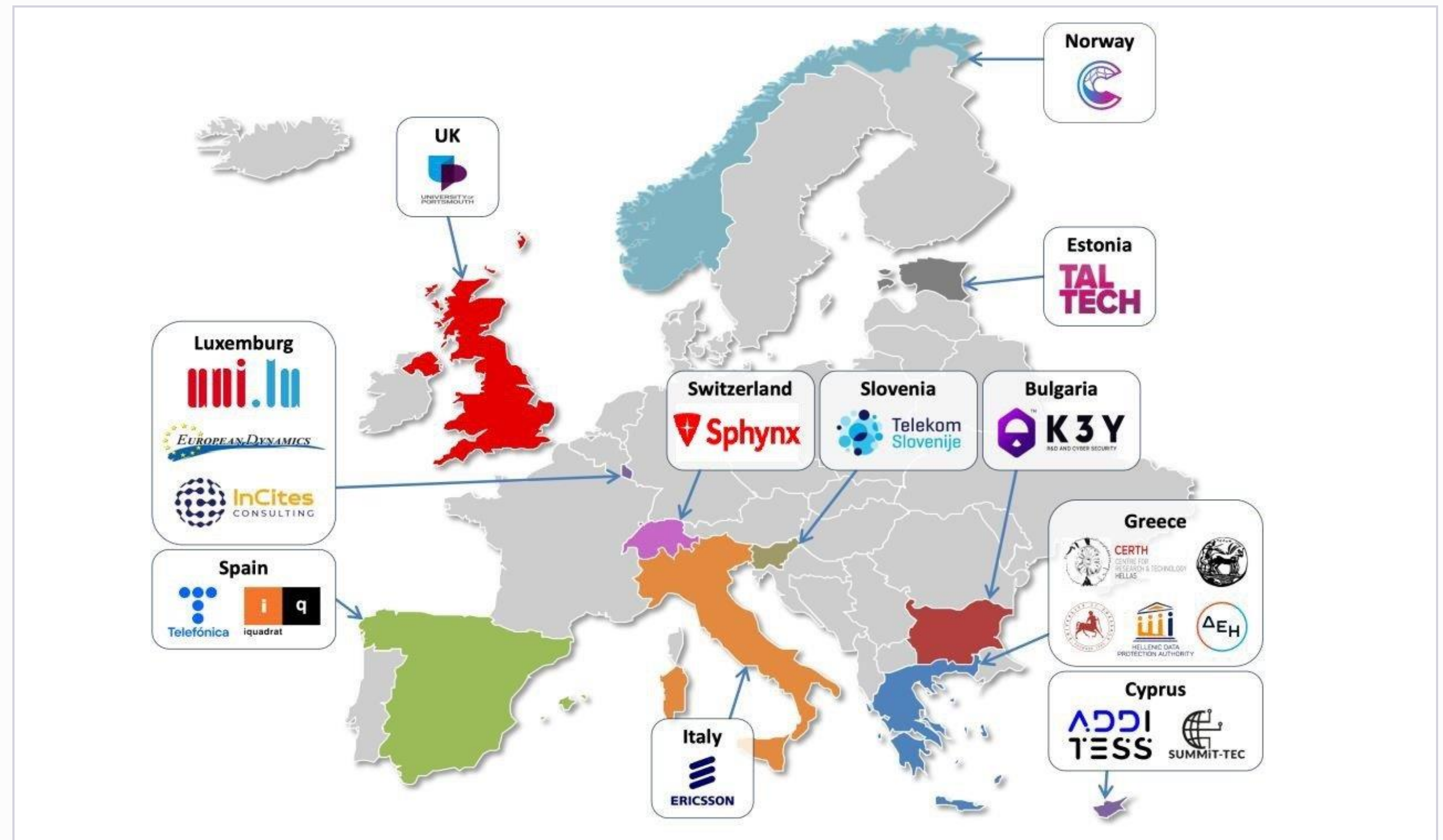


**36**  
Months



**Topic:**  
HORIZON-JU-SNS-  
2024-STREAM-B-01-04  
“Reliable Services and  
Smart Security–  
Standardisation and  
Follow-up/PoCs”

**Type:**  
HORIZON-RIA HORIZON  
Research & Innovation  
Actions



Co-funded by  
the European Union

**6G SNS**

Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# XTRUST-6G – Aim



**01**

Micro-segmentation of critical O-RAN assets

**02**

A zero-trust-based security framework

**03**

Advanced AI-driven tools for intrusion detection

**04**

Quantum-safe technologies and privacy-preserving AI/ML schemes

**05**

Enhanced supply chain security measures



**XTRUST-6G**



Co-funded by  
the European Union



Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# XTRUST-6G – Objectives



- 1) **Strengthen Zero-Trust security** and enforce least-privilege access across 5G+/6G networks.
- 2) **Enable proactive security** through threat intelligence, foresight, and risk-based situational awareness.
- 3) **Deliver AI-driven, zero-touch protection** using collaborative and federated threat detection.
- 4) **Improve network visibility and control** through real-time monitoring and security orchestration.
- 5) **Ensure trustworthy services** through blockchain-based identity, lifecycle management, auditing, and compliance.
- 6) **Secure the 5G+/6G supply chain** with OSS security assurance and automated vulnerability remediation.



Co-funded by  
the European Union



Project funded by



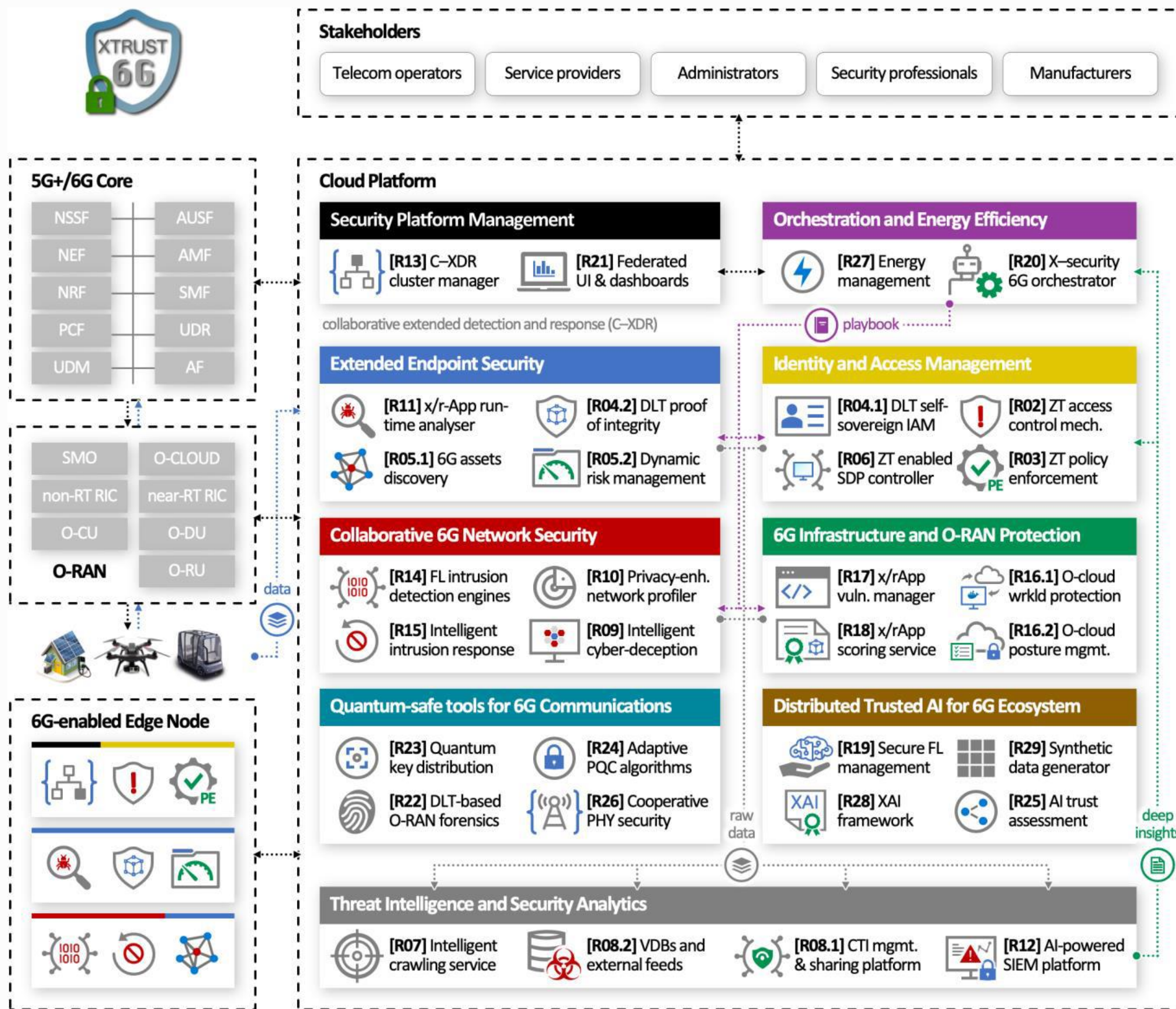
Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# XTRUST-6G – Architecture overview



- **MEC-based architecture:** Intensive computing is performed at the edge to enable real-time, collaborative security services with extremely low latency.
- The key building blocks forming the XTRUST-6G computing ecosystem:
  - **Cloud layer:** Hosts the core XTRUST-6G applications and services.
  - **Edge layer:** Edge devices, servers, or gateways perform pilot-specific processing and security functions.
  - **End devices / UEs:** Include autonomous vehicles, RSUs, EV chargers, smart meters, UAVs, and sensors.
- **Multi-access connectivity:** Supports NB-IoT, LTE-M, 5G, and 6G technologies across different pilot environments.



Co-funded by  
the European Union



Project funded by



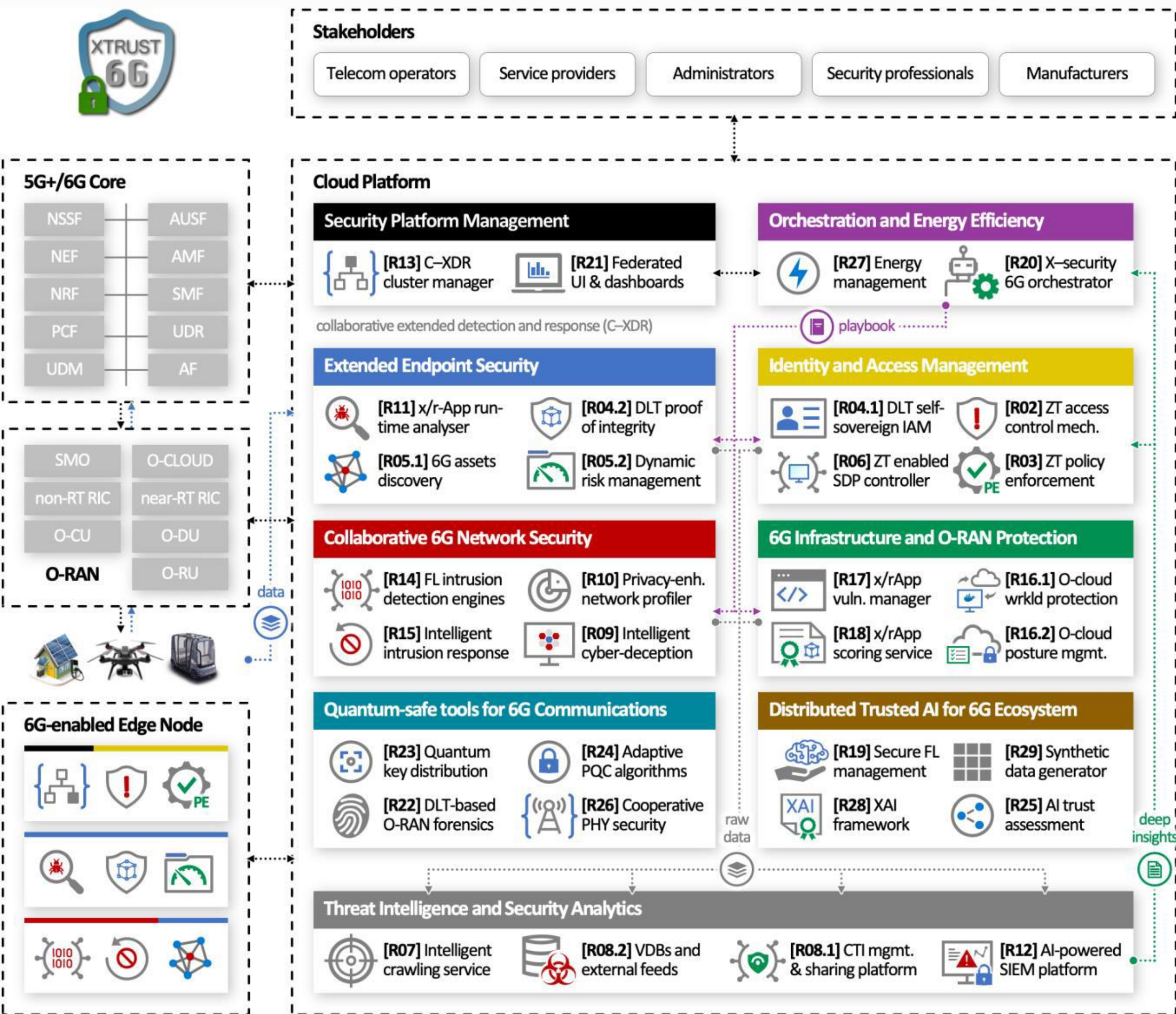
Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026

# XTRUST-6G – Architecture overview



## XTRUST-6G solutions are grouped into classes:

- 6G endpoints, UEs, applications & services
- 6G core networks & connected ecosystems
- O-RAN, O-Cloud & software supply-chain security
- Zero-Trust identity & access control
- Quantum-safe security (QKD & PQC)
- Trusted, explainable & privacy-preserving AI
- Enhanced security analytics & cyber-threat intelligence
- Automated security orchestration and response (SOAR)
- Collaborative XDR and FL for privacy-preserving detection
- Federated UI for accessing XTRUST-6G security solutions.



Co-funded by  
the European Union



Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026

# XTRUST-6G – Pilot use cases



## Pilot 1: 6G-enabled EV Charging Infrastructure Resilience:

Addresses vulnerabilities specific to 5G+/6G networks used by autonomous vehicles.

- **Hosted by** Public Power Corporation (PPC), Greece
- **Goal:** Secure and resilient 6G-enabled EV charging infrastructure
- **Zero-Trust & Zero-Touch:** Secure onboarding, communication, and continuous verification across the EV charging ecosystem
- **Open RAN & Edge Computing:** Secure network slicing for high-volume, real-time charging
- **AI-Driven Security:** Real-time intrusion detection and security monitoring
- **Resilience:** Protection against cyber-physical attacks and service disruptions
- **Impact:** Demonstrate trusted 6G for smart mobility, critical infrastructure, and citizen safety.



Co-funded by  
the European Union

6G SNS

Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# XTRUST-6G – Pilot use cases



**Pilot 2: Safeguarding 6G-connected Autonomous Vehicles:**  
Focuses on enhancing the security and reliability of electric vehicle (EV) charging systems.

- Hosted by **Tallinn University of Technology**,
- Tests Zero-Trust security and AI-driven cybersecurity for 6G-ready CAVs and smart-city infrastructure.
- It combines private 5G networks and future 6G capabilities to provide secure, low-latency vehicle-to-vehicle and vehicle-to-infrastructure communication.
- The pilot also uses AI-based anomaly detection and automated response to protect autonomous vehicles against cyberattacks, sensor spoofing, and data manipulation.



Co-funded by  
the European Union

**6G SNS**

Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# XTRUST-6G – Pilot use cases



## Pilot 3: Quantum Key Distribution for End-to-End 6G Security: focuses on Quantum Key Distribution for end-to-end 6G security.

- Hosted by the **University of Luxembourg, SNT**.
- Integrates QKD with 6G for secure end-to-end communications.
- Address challenges related to secure authentication, key distribution, and efficient key management, while maintaining network performance.
- **SNT** will use its Quantum Lab, 6GSpaceLab, and QKD infrastructure to design, implement, and validate QKD integration within 6G networks
- The pilot will be tested across the Belval and Kirchberg campuses, using dedicated QKD infrastructure and a 5G+/6G testbed.



Co-funded by  
the European Union



Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# XTRUST-6G – Pilot use cases



**Pilot 4: Securing UAV-assisted 6G Communications:** focuses on mitigating cybersecurity risks such as jamming, eavesdropping, and unauthorized access, using physical layer security (PLS) to protect UAV communications.

- Hosted by the ADITESS research company.
- The setup includes UAVs, a control vehicle, an edge application server, and a 5G+ O-RAN infrastructure, with the non-RT RIC deployed in the cloud and the near-RT RIC integrated into the UAV control environment.
- The pilot will demonstrate how O-RAN intelligence and security policies can be applied in real time to support secure and efficient UAV operations.
- Overall, it provides a real-world environment for validating secure, intelligent, and resilient 5G+/6G connectivity for UAV applications.



Co-funded by  
the European Union

6G SNS

Project funded by



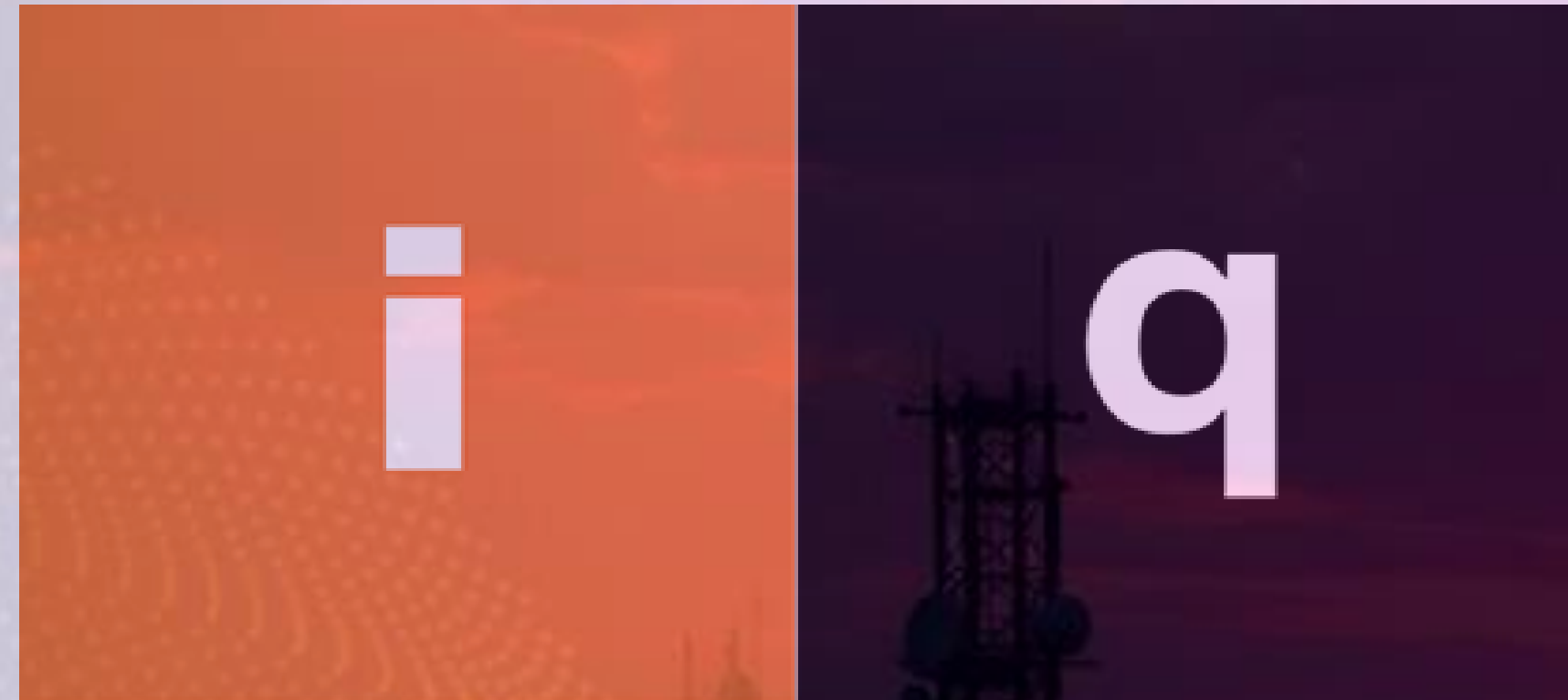
Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

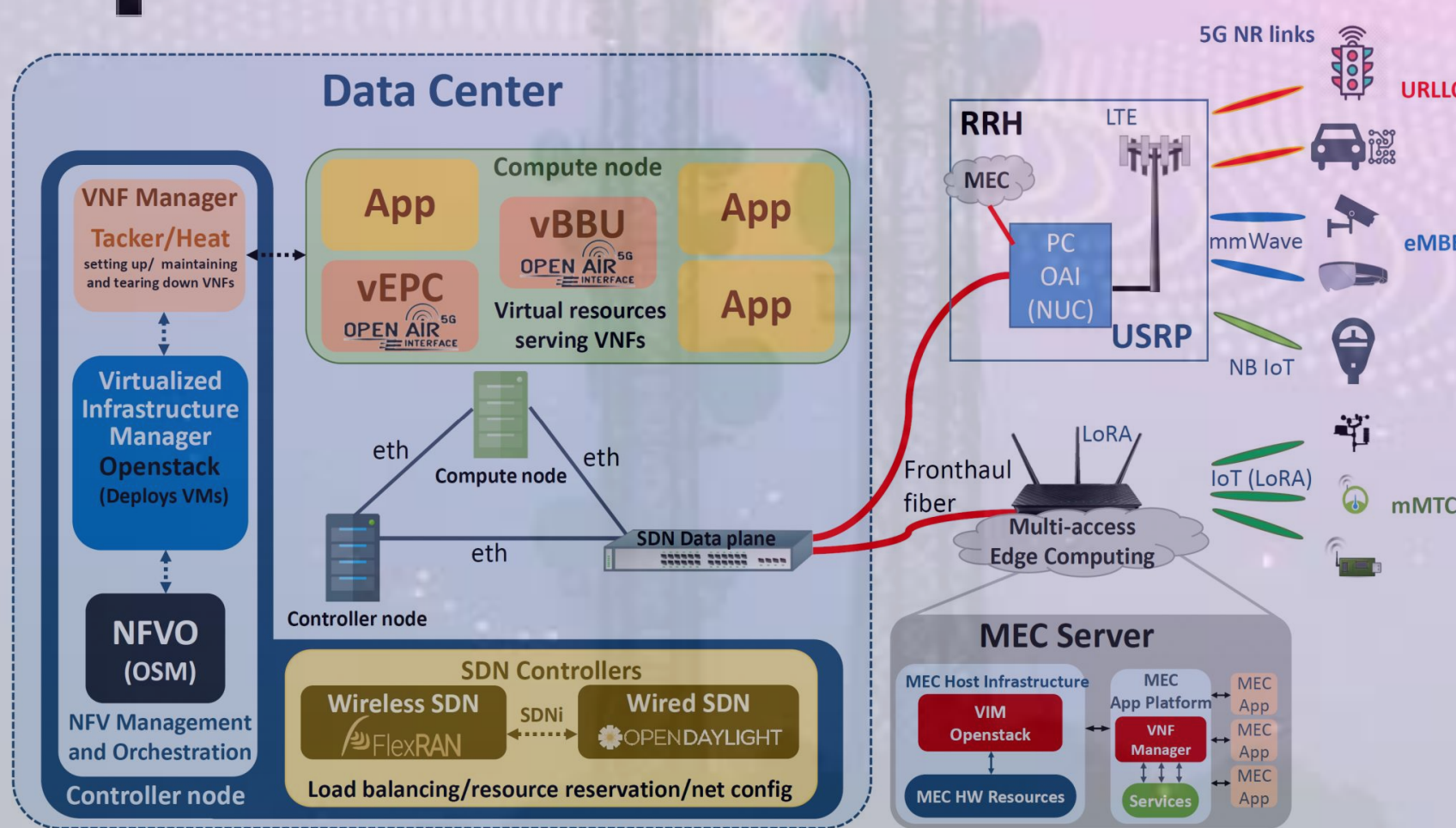
Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

# XTRUST-6G – Pilot use cases



## iquadrat



**Pilot 5: Thwarting Attacks Against O-RAN and Virtualized 6G Infrastructure:** focuses on mitigating cybersecurity risks against O-RAN architecture and virtualized 6G infrastructures.

- **Hosted by** the Iquadrat. Iquadrat offers one of the most complete end-to-end Private 5G testbeds in Europe, fully supporting 5G Rel-16 in Stand-Alone mode.
- **Threat coverage:** Cloud/edge vulnerabilities, lateral movement, software supply-chain risks, and DoS attacks.
- **Testbed:** Iquadrat 5G Standalone Rel-16 testbed with OpenStack, Kubernetes, O-RAN gNBs, SDN/NFV, and security orchestration.
- **O-RAN Evolution:** Extended to support the latest O-RAN 7.2 specifications.



Co-funded by  
the European Union

6G SNS

Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*



**XTRUST-6G**

# University of Portsmouth Activities



Co-funded by  
the European Union



Project funded by



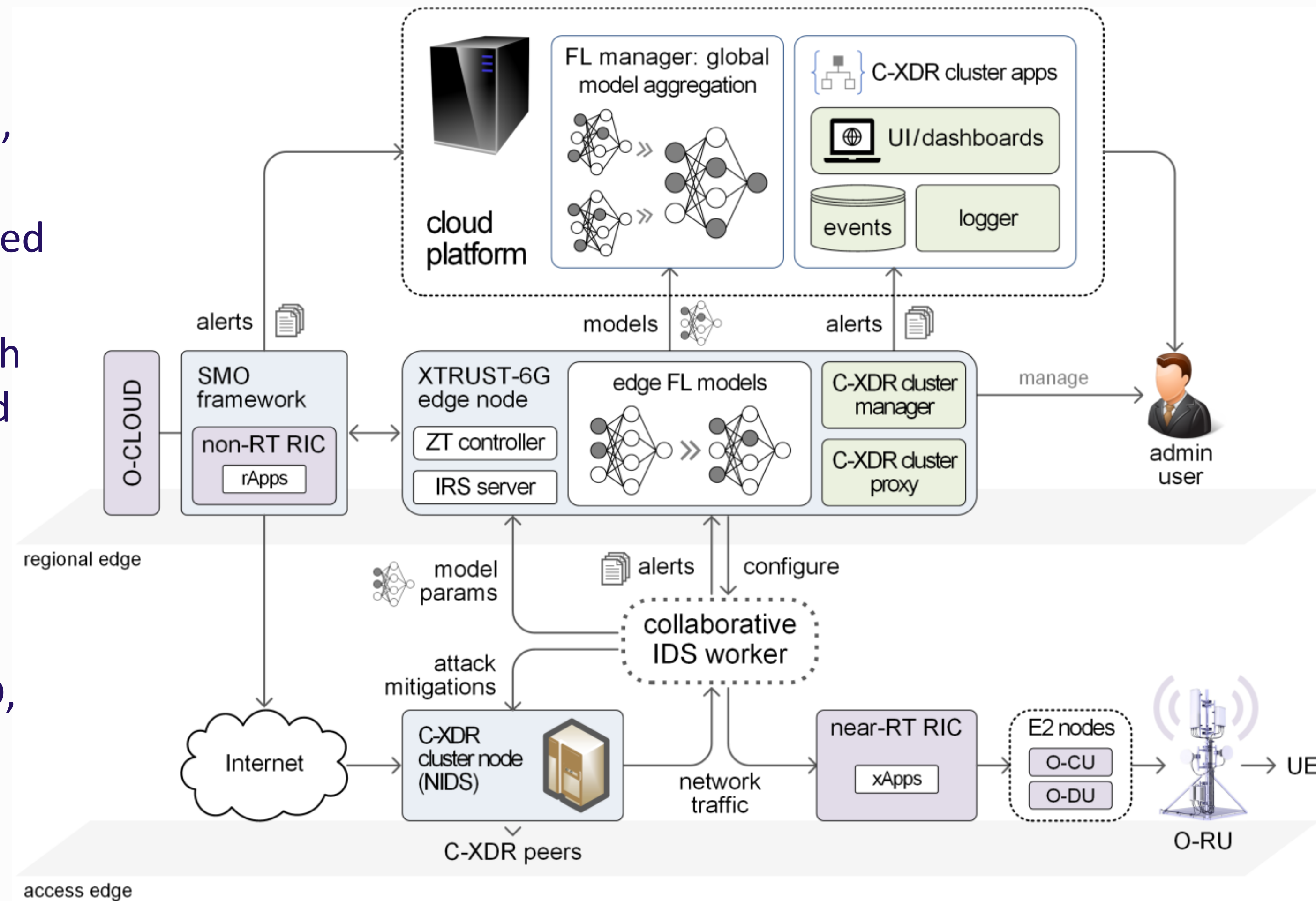
Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

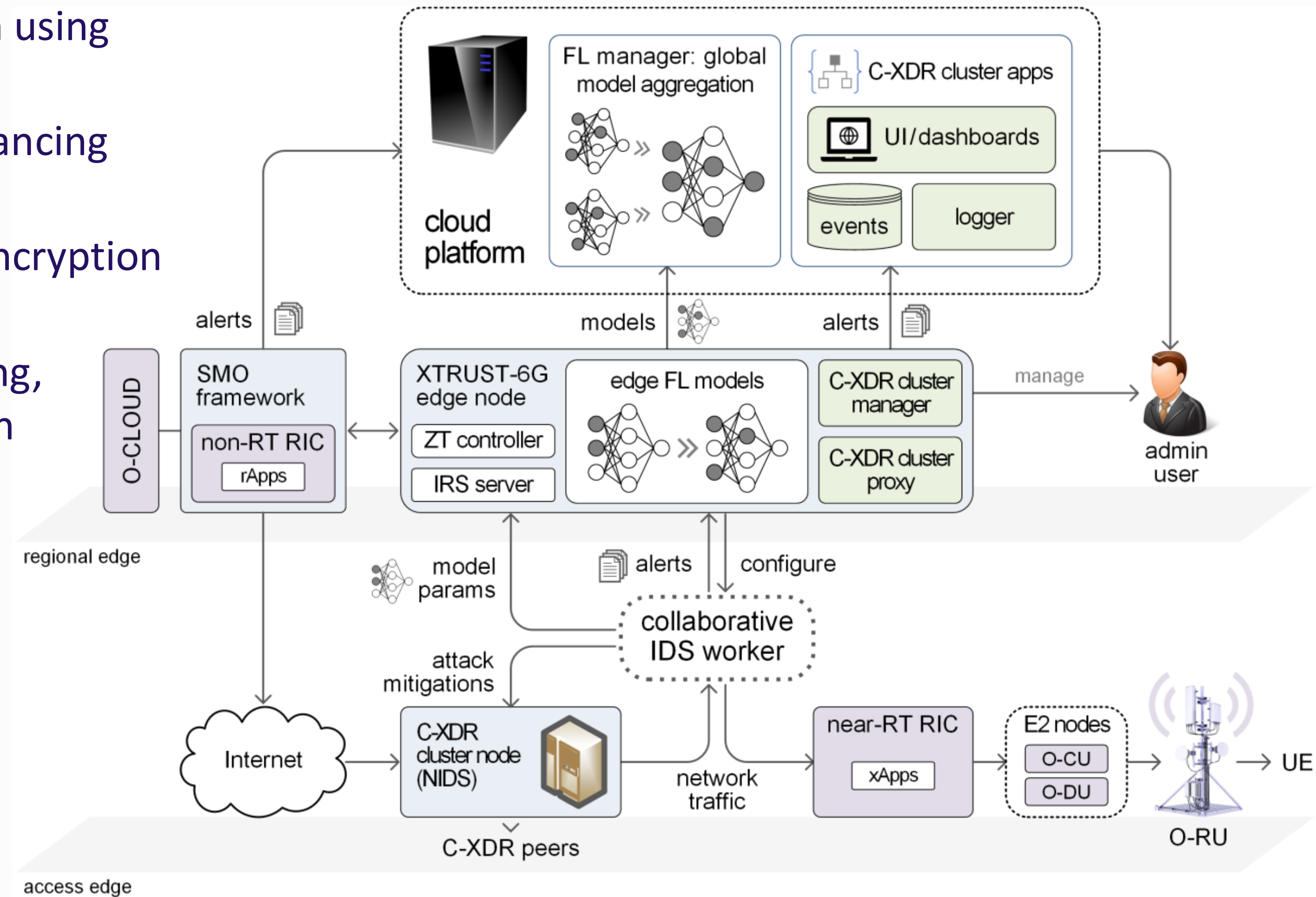
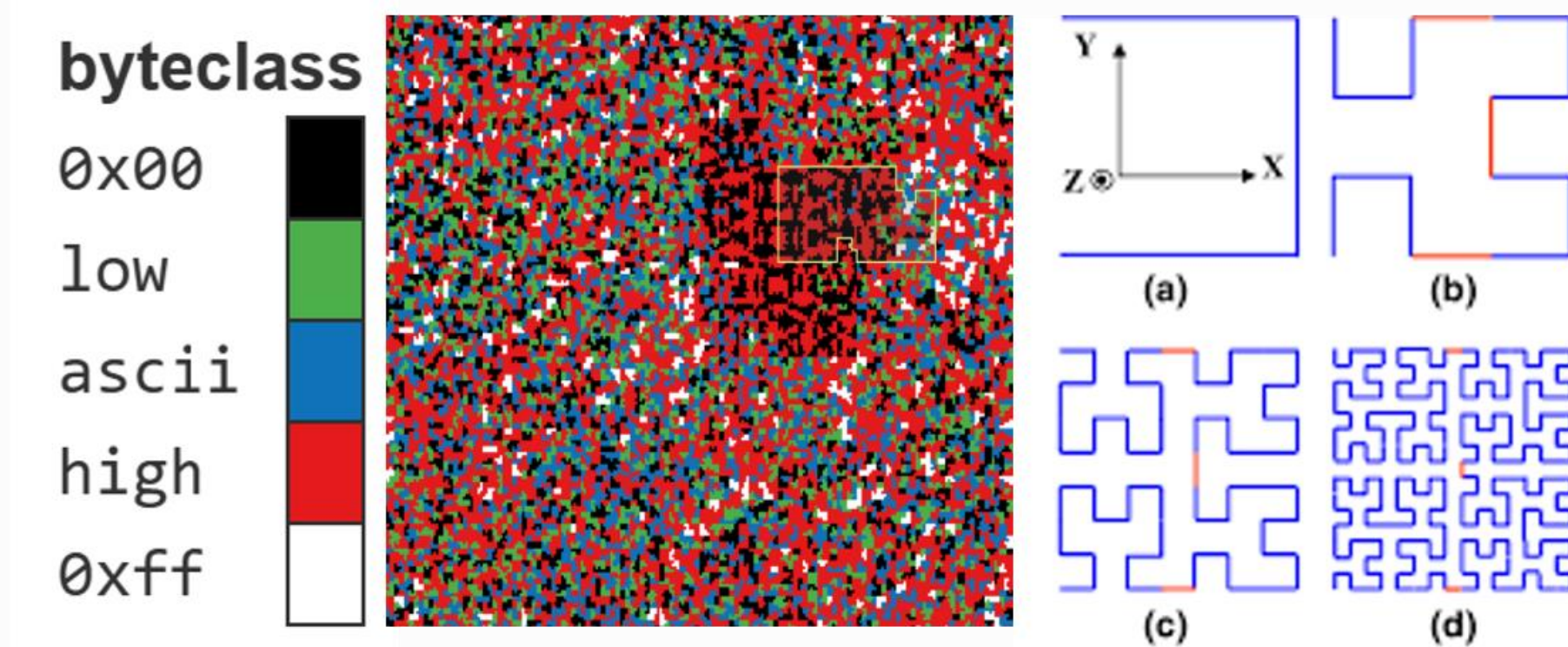
*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*

- Develop a scalable, secure, and intelligent C-XDR intrusion detection framework for distributed cloud, edge, and 6G/O RAN environments.
- Design a cluster-based IDS architecture for distributed cloud and edge 6G infrastructures.
- Enable centralized management and control through cloud-native cluster managers, agents, and a unified UI.
- Provide multi-layer threat detection across O-RAN, SMO, and O-CLOUD using network- and host-based monitoring.
- Integrate advanced AI detection through **ML-SQUID**, combining TLS inspection and AI-driven binary visualization.



# University of Portsmouth Activities

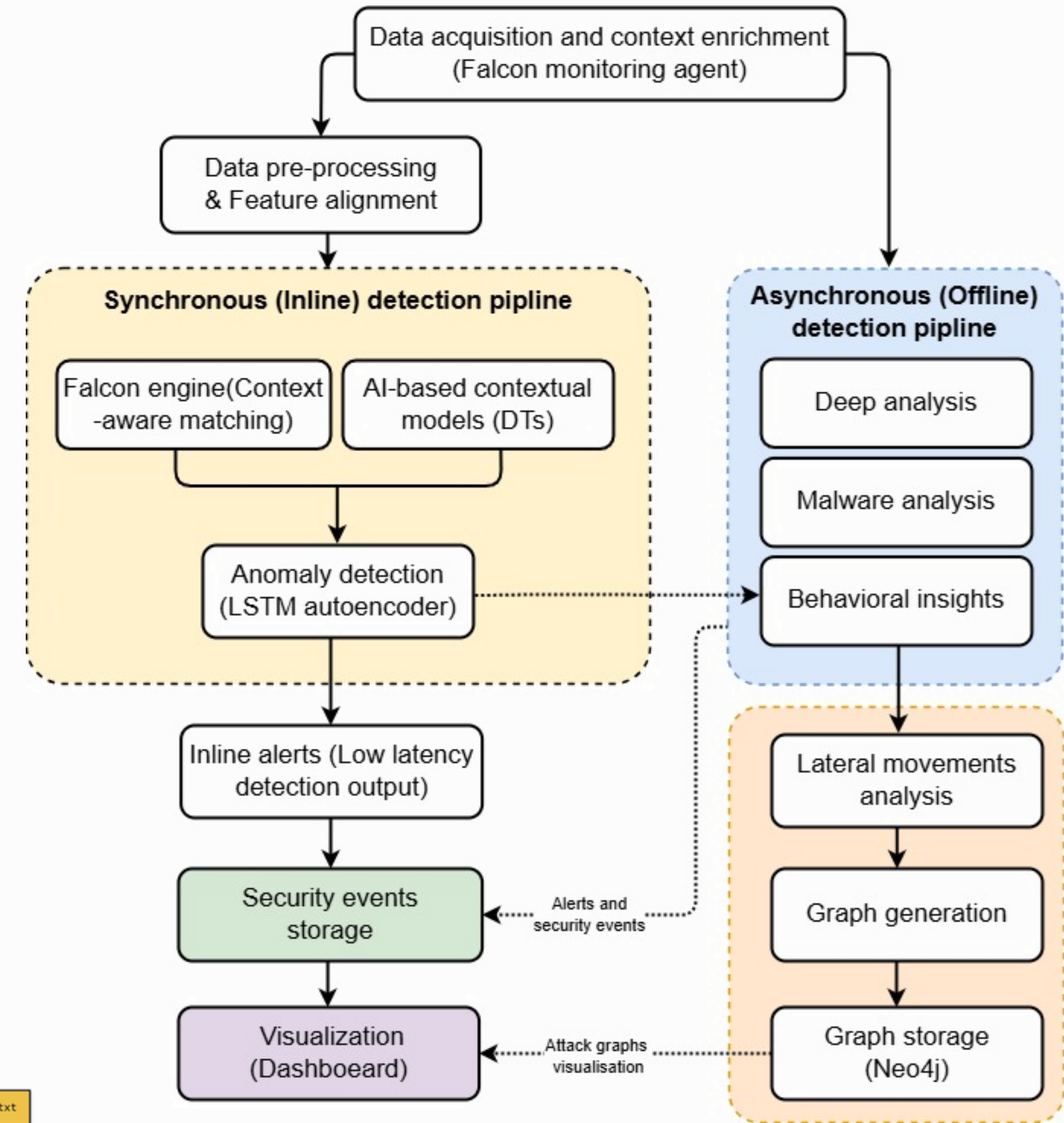
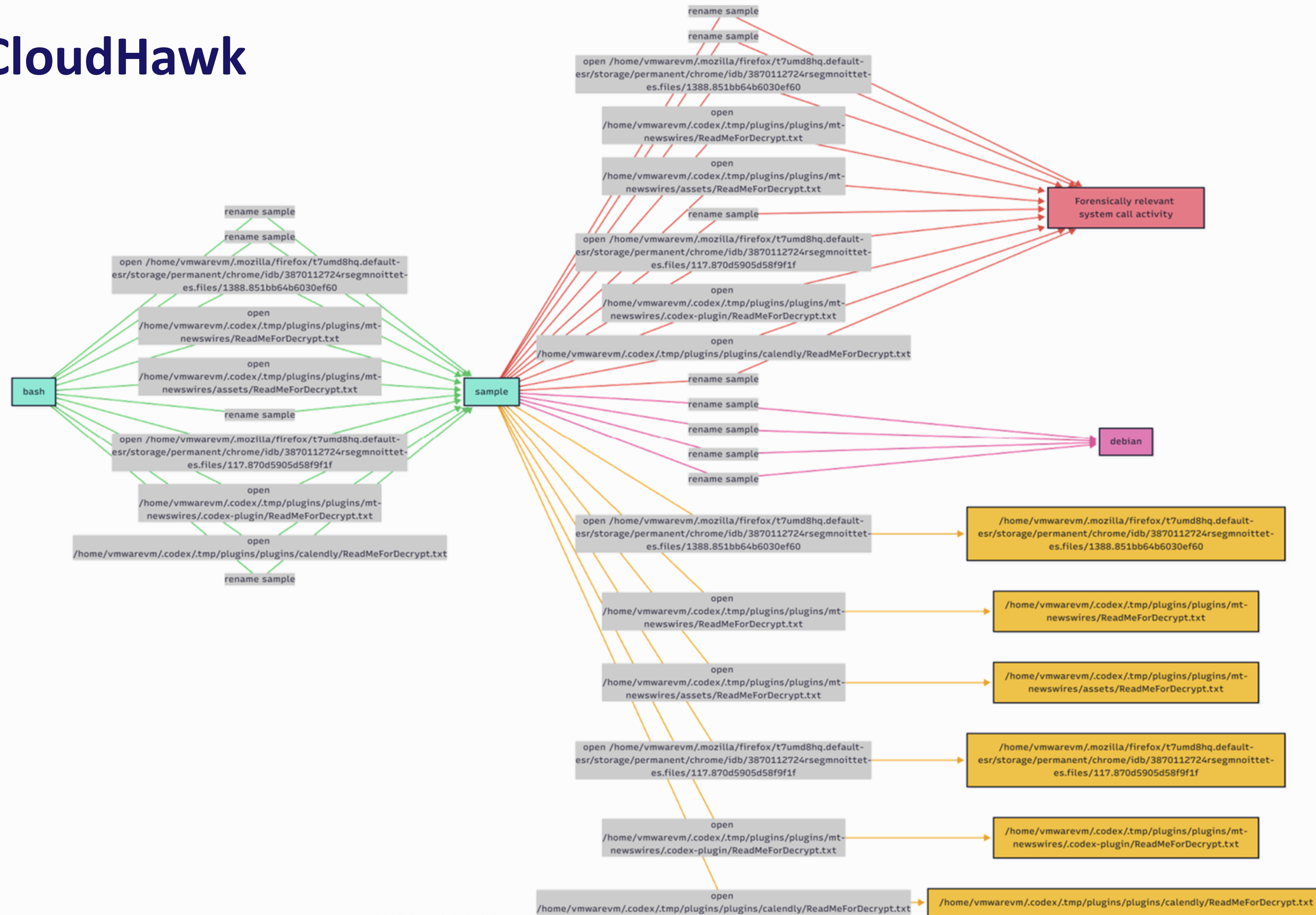
- Enable privacy-preserving collaborative detection using Federated Learning (FL).
- Ensure scalability and resilience through load balancing and multi-agent deployment across sites.
- Strengthen security and trust using end-to-end encryption and insider-threat mitigation.
- Centralize security visibility through unified logging, telemetry collection, correlation, and visualization



# University of Portsmouth Activities



## CloudHawk



Co-funded by  
the European Union



Project funded by



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
State Secretariat for Education,  
Research and Innovation SERI

Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026

## ZT Policy Enforcement Gateway

- **Objectives and key innovations:**
  - Developing a ZT PE Gateway for dynamic and risk-adaptive access control in 6G environments
  - Decouple policy enforcement from identity management
  - Continuous trust assessment beyond authentication and RBAC.
  - Detection of stolen tokens, session hijacking, anomalous user/service behaviour
  - Security-agnostic protected services (all enforcement at gateway level)
- **Architecture:** A three-layer architecture is proposed.
  - **pfSense Perimeter Layer:** Provides network segmentation, traffic filtering, and monitoring at the network boundary.
  - **Istio Service Mesh Layer:** Enforces JWT-based authentication via Keycloak/OIDC and fine-grained authorization policies.
  - **ML-Based PEP layer:** Performs behaviour-based trust evaluation and dynamic risk-adaptive access control.





**XTRUST-6G**

# Thank You

**Dr Gueltoum Bendiab, [gueltoum.bendiab@port.ac.uk](mailto:gueltoum.bendiab@port.ac.uk)**  
**Dr Rinat Khusainov, [rinat.khusainov@port.ac.uk](mailto:rinat.khusainov@port.ac.uk)**  
**University of Portsmouth**



**Co-funded by  
the European Union**



**Project funded by**



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,  
Education and Research EAER  
**State Secretariat for Education,  
Research and Innovation SERI**

*Trusted and Sustainable Cybersecurity for Critical Infrastructures, 28 September 2026*