CYBERAID

AI-Driven Cybersecurity for Financial Service Providers

Module 5
Operations, Privacy and Compliance

CyberAId Learning Centre – eBPF Tutorial Course

October 2026

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The project funded under Grant Agreement No 101249596 is supported by the European Cybersecurity Competence Centre

CYBERAID

Deployment readiness checklist

Kernel readiness

Check kernel version and BTF support for portable CO-RE programs

Least privilege

CAP_BPF and CAP_PERFMON instead of full root; restrict who loads programs

Performance

Benchmark CPU and memory under peak transaction load

Privacy by design

Metadata only; never transaction payloads

Kubernetes

Complement host probes with Cilium identity-aware policy

Governance

Change control for rules; retention for forensics and reporting

From proof of concept to pilots

1

Simulated stack

BCC tracers and traffic generators

2

Digital twin

Cyber-range testing; Wazuh and Tetragon integration under investigation

3

CO-RE agents

Portable, hardened production agents

4

Pilot sites

Benchmarks under load; Kubernetes with Cilium

Pilot plan to be confirmed; overhead figures will come from pilot benchmarks.

CYBERAID

Securing the eBPF layer itself

1. Control who may load programs: capabilities and change control
2. Treat rules and probes as security content: versioned, reviewed, signed
3. Monitor the monitor: alert on unexpected program loads and detached probes
4. Harden kernels: restrict unprivileged eBPF, keep patched
5. Separate duties between rule authors and enforcement approvers

Privacy and data protection

Data minimisation

Process, user and connection metadata only; no transaction content

Purpose limitation

Used for security monitoring and incident identification

Controlled uprobes

TLS-library probes off by default; strict controls and a legal basis

Retention and access

Role-based access via the Security Context; retention matched to forensic and reporting needs

Orientation only; not legal advice. Confirm with the institution's data protection officer.

Regulatory alignment

Regulation	What it asks, in short	How the approach helps
DORA	ICT risk management, monitoring, incident reporting	Host-level telemetry, retained evidence, incident narratives
NIS2	Risk-management measures and incident handling	Detection coverage; findings mapped to obligations
GDPR	Data minimisation, security of processing	Metadata-only collection; role-based access
EU AI Act	Human oversight of AI systems	Tiered human-in-the-loop; audited agent actions

High-level mapping for orientation; compliance depends on each institution's implementation.

Operating the detection content

1. **Author**
   Rule and profile with thresholds
2. **Test**
   Digital twin or replayed events
3. **Review**
   Approval under change control
4. **Deploy**
   Versioned pack
5. **Tune**
   Analyst feedback informs evaluation

Proposed lifecycle; to be aligned with the CyberAId governance of extension packs.

How to measure success

Detection quality

Precision and recall per threat scenario

Quality per severity band

Operational cost

False-positive burden on analysts

Time to triage

Performance overhead

CPU and memory at peak load

Event loss under stress

Evidence quality

Completeness of findings

Traceability to events

Proposed evaluation approach; to be run on realistic financial-sector data and in the CyberAId pilots.

Limitations and open points

1. Pilot evidence on overhead and detection quality still to come
2. Agent integration patterns to be agreed with the agent and runtime teams
3. SIEM path versus direct path to the bus to be confirmed
4. Thresholds and profiles need calibration per institution
5. Linux-centric coverage; rule governance and program-load alerting to be operationalised

Course wrap-up and next steps

- Module 1: eBPF fundamentals and the visibility gap
- Module 2: state of the art, tooling and positioning
- Module 3: the Kernel-Level Monitor and financial threat detection
- Module 4: integration into the CyberAId architecture and agents
- Module 5: operations, privacy and compliance
- Next: take the end-of-course quiz in the Learning Centre



CYBERAID

Thank you!

Connect With CyberAID:
LinkedIn: CyberAID

Course complete – continue with the end-of-course quiz

CyberAID has received funding from the DIGITAL EUROPE Programme under grant agreement No. 101249596