



AI-Driven Cybersecurity for Financial Service Providers

Module 5

Integrating EMTD into the CyberAid Architecture and Platform

CyberAid Learning Centre – EMTD Tutorial Course

October 2026



CyberAid architecture recap

PROACTIVE

Pentesting, risk assessment, digital twin, code analysis

MONITOR

Wazuh SIEM/XDR and eBPF monitoring

REPORT

Incident response, vulnerability tracking, compliance reporting

LLM

Open-source LLMs, agent orchestration, vector DB, HITL

BLUEPRINTS

Reference architectures for banks, insurers, payment processors

SERVICES + LEARNING CENTRE

Front-end, dashboards, training



The CyberAid agent ecosystem

Central Router Agent (CRA)

Triage · dispatch · conflict resolution · synthesis

Threat Intelligence

Vulnerability
Assessment

Compliance
Verification

Behavioural
Analysis

Incident Response

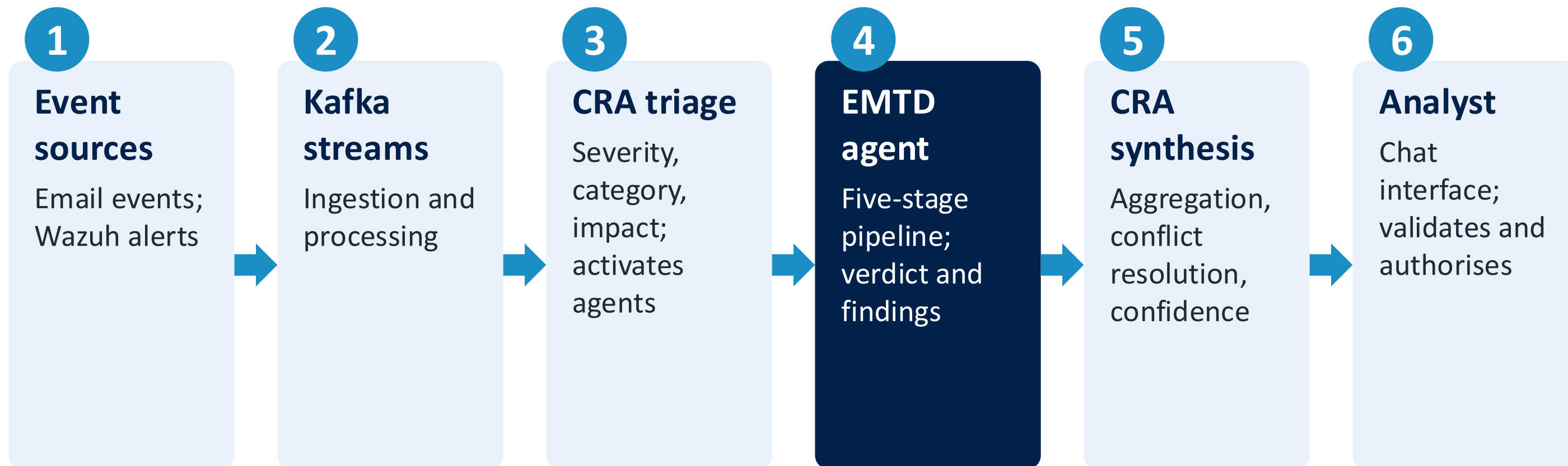
Forensic Analysis

DevSecOps / Code

EMTD (email
threats)

EMTD as a specialised agent is the proposed integration pattern; the other agents are as defined in the CyberAid grant agreement.

End-to-end event flow



Proposed pattern, based on the CyberAid agent workflow (Wazuh, Kafka, Central Router Agent, human oversight).

The EMTD agent interface (proposed)

Input

Headers, auth results
Body and attachments
Organisational context
CRA triage context

Output

Verdict and threat score
Findings per family
Attack pattern (ATK-x.xx)
Explanation, completeness

```
{ "verdict": "QUARANTINE",  
  "score": 0.72,  
  "candidate_attack": "ATK-1.02",  
  "findings": [  
    {"component": "SA-01.3", "family": "SA-01",  
     "suspicious": true, "confidence": 0.90} ],  
  "explanation": "...",  
  "completeness": {"degraded": false,  
                   "missing_inputs": []},  
  "recommended_action": "analyst_review" }
```

Illustrative schema only; values are examples, not measured output.



Reusing shared CyberAid services

Model Gateway + guardrails

Audited LLM access; protection against prompt injection, hallucination and data leakage

Vector DB + knowledge base

Financial-security context for retrieval-augmented analysis

CTI and OSINT feeds

Support for SA-08 open-source intelligence components

Kafka + Wazuh API

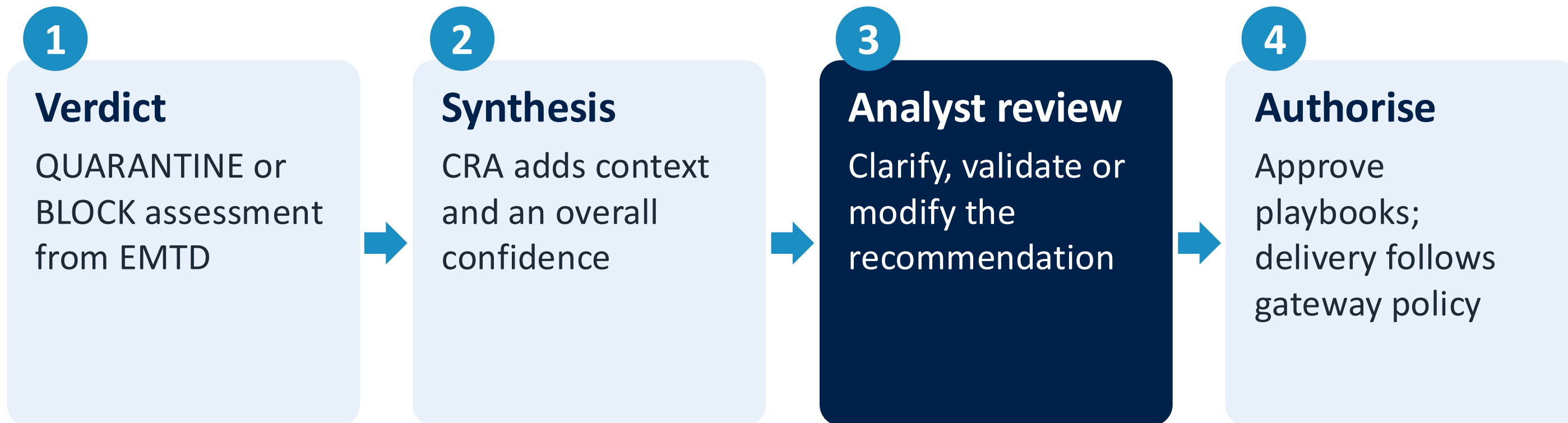
Event delivery and additional context on demand

Agent collaboration around EMTD

Agent	Proposed exchange with EMTD
Threat Intelligence	IoCs for URLs, domains and hashes in the email (SA-06, SA-08)
Behavioural Analysis	User and entity behaviour context (SA-04)
Compliance Verification	Regulatory and financial-process context (SA-07)
Incident Response	Containment playbooks after a QUARANTINE or BLOCK verdict
Forensic Analysis	Evidence preservation and timeline reconstruction

Proposed integration points to be confirmed in the integration specification.

Human-in-the-loop oversight





Downstream: response, reporting and forensics

Response

Containment and recovery steps from the Incident Response Agent

Reporting

Incident records and regulatory reporting (e.g. DORA, GDPR) in CyberAid-REPORT

Forensics

Evidence preservation and attack-timeline reconstruction

Feedback (possible extension)

Analyst decisions inform threshold and ontology tuning

Deployment and operations

Bounded concurrency

Parallel components without overloading the platform

Latency budget

Fast pre-checks; slower model-assisted stages

Graceful degradation

Report unavailable checks; deterministic fallback

Audit and configuration

Logged model access; versioned thresholds and ontology

Untrusted content

Apply guardrails against prompt injection in email content

Policy separation

Verdict is an assessment; delivery follows gateway policy

Integration lab

- 1 Send** a sample email event into the flow
- 2 Inspect** the CRA triage and the EMTD activation
- 3 Examine** the verdict payload against the schema
- 4 Review** the recommendation in the analyst view
- 5 Check** that the incident reaches the reporting component



Course wrap-up and next steps

- Module 1: the email threat problem in financial services
- Module 2: the five-stage pipeline and its scoring
- Module 3: a worked CEO impersonation example
- Module 4: positioning against the state of the art
- Module 5: integration as an agent in CyberAid
- Next: take the end-of-course quiz in the Learning Centre



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