



**AI-Driven Cybersecurity for
Financial Service Providers**

Module 1 The Email Threat Problem in Financial Services

CyberAid Learning Centre – EMTD Tutorial Course

October 2026

Learning objectives

- 1 Explain why email remains a primary entry point for fraud and compromise
- 2 Recognise the main attack patterns targeting wealth managers and financial institutions
- 3 Understand why financial context changes what “suspicious” means
- 4 Place EMTD within the CyberAid platform and the five-module course

Why email remains the weak link

Universal channel

Clients, counterparties, advisers and staff are all reachable by email

A human decides last

Every message ends with a person choosing whether to click, reply or pay

Money moves on instruction

One convincing request can trigger a payment or a change of bank details

Trust is the target

Long-standing relationships make impersonation credible

The attack patterns EMTD looks for

24

attack patterns in the
EMTD threat ontology

ATK-1.02

CEO / Executive
Impersonation (BEC)

ATK-2.03

Invoice Fraud

ATK-2.06

Capital Call / Distribution
Fraud

ATK-3.04

QR Code Phishing

Client impersonation is also covered. The ontology gives the LLM explicit categories for analysis and for explaining findings.

What makes wealth management different

What a generic filter sees

Sender reputation

Known bad links and files

Spam-like wording

Each message on its own

What financial context adds

Client and executive impersonation

Payment instructions and IBAN changes

Capital calls and distribution notices

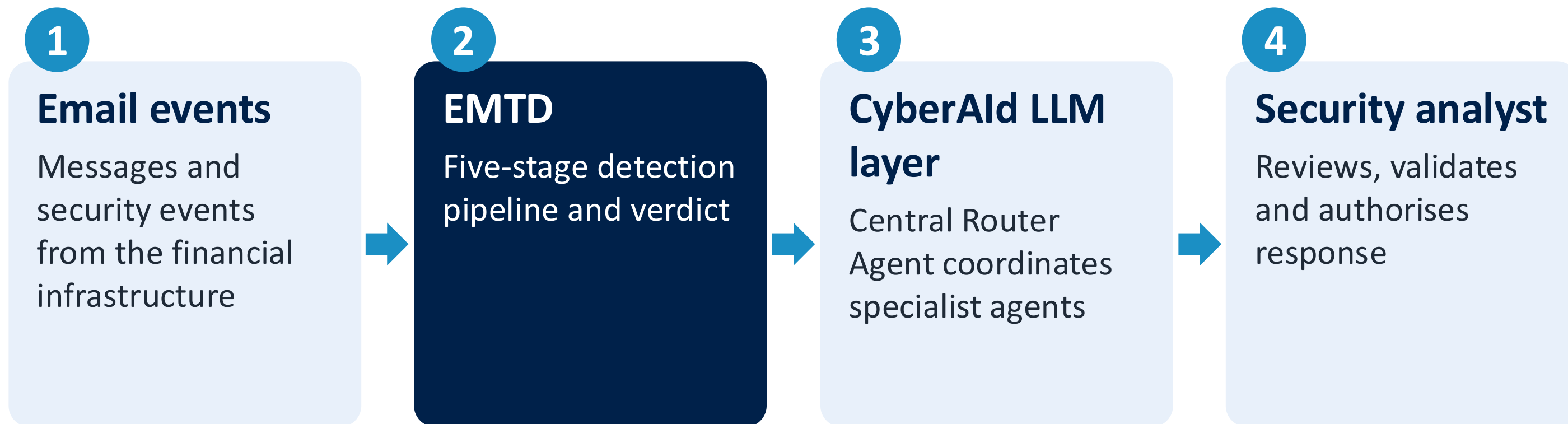
Known versus first-time contacts

Regulatory and organisational context

Design requirements and EMTD's response

Challenge	EMTD design response
Authentication-clean but malicious messages	LLM-assisted content and semantic analysis alongside rules
Opaque verdicts	Deterministic weighted scoring plus an analyst explanation
Cost of running every check every time	Catalogue-driven selection of specialist components
Missing or unavailable inputs	Degraded analysis is reported; deterministic fallback
Governed use of models in finance	All LLM calls go through an audited Model Gateway

Where EMTD sits in CyberAid



Integration details are covered in Module 5.

Course roadmap

1

The problem

Email threats in finance

2

EMTD in depth

Five-stage pipeline

3

Worked example

CEO impersonation lab

4

State of the art

Positioning EMTD

5

Integration

Agents and platform



Thank you!

Connect With CyberAID:
LinkedIn: CyberAID

Next: Module 2 – EMTD in Depth: The Five-Stage Pipeline



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