



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

Module 3 Worked Example: Catching a CEO Impersonation (BEC)

CyberAid Learning Centre – EMTD Tutorial Course

October 2026

The scenario: an urgent request from the “CEO”

From	“Chief Executive Officer” <...@gmail.com>
Reply-To	a different Gmail address
SPF / DMARC	softfail / fail (as supplied)
Subject	Urgent – confidential payment

*“Please complete this payment today.
Don’t discuss this with anyone.”*

Why it is dangerous

Authority claim

Pressure to act today

Secrecy instruction

Mismatched reply path

Failed authentication

Stages 1-3: first signals, classification, selection

1

Stage 1

SPF softfail, DMARC fail
Reply-To mismatch
Display-name claim



2

Stage 2

LLM reads content + signals
Candidate: ATK-1.02
CEO / Executive
Impersonation



3

Stage 3

Trigger mappings select components for the candidate
Always-run checks retained



Stage 4: the evidence components contribute

Component	What it detects	Method	Confidence
SA-01.1 SPF Validator	Supplied SPF softfail	Rule	60%
SA-01.3 DMARC Evaluator	Supplied DMARC failure	Rule	90%
SA-02.8 Reply-To Mismatch	Replies go to a different Gmail domain	Rule	95%
SA-03.1 Display Name Check	CEO claim on a free-email domain	Rule	70%
SA-02.1 Urgency / Pressure	Pressure to pay “today”	LLM	LLM-assessed
SA-02.2 Secrecy / Isolation	“Don’t discuss” instructions	LLM	LLM-assessed

Rule confidences are configured outputs, not measured detection accuracy; LLM confidences depend on the analysis.

Evidence across component families

SA-01 Header authentication

SPF softfail

DMARC failure

SA-02 Content and semantics

Reply-To mismatch

Urgency / pressure (LLM)

Secrecy / isolation (LLM)

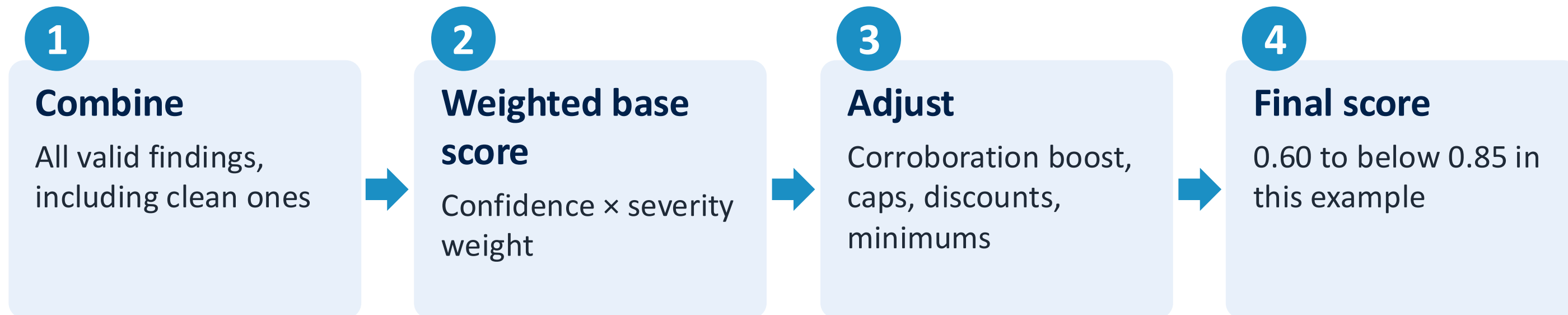
SA-03 Sender identity

CEO display name on free-email domain

Six findings, three families: the corroboration boost can apply

Boost: $\times 1.15$ for two families, $\times 1.25$ for three or more (suspicious CRITICAL findings)

From evidence to verdict



The analyst explanation

QUARANTINE – recommend analyst review

Likely CEO / Executive Impersonation (BEC), ATK-1.02.

Key evidence: DMARC failure and SPF softfail; replies directed to a different Gmail domain; CEO display name on a free-email address; pressure to pay today; instruction not to discuss.

Analysis completeness: all inputs reported; no degraded checks.

What to notice

Names the attack pattern
Lists the decisive evidence
States the verdict and next step
Reports completeness
Deterministic fallback if synthesis fails

Hands-on lab: what-if experiments

- | | | |
|---|-------------------------------|--|
| 1 | Reproduce | Run the base case and list the contributing families |
| 2 | Remove DMARC failure | Observe how score and evidence change |
| 3 | Single-family evidence | Keep only header findings: score is capped at 0.59 |
| 4 | Add a third family | Observe the 1.25 corroboration multiplier |
| 5 | Withhold an input | Check that degraded analysis is reported |

Reading incomplete or degraded analysis

Excluded from scoring

Skipped, stubbed and erroneous results

Reported

Missing inputs, unavailable checks, degraded analysis

PASS is not “safe”

Below the review threshold: inspect analysis completeness

Fallback

Deterministic explanation if synthesis fails



Key takeaways

- BEC attacks combine authentication, identity and wording signals
- Corroboration across families drives the verdict, not the count of checks
- Deterministic rule confidences are configured, not measured
- The explanation names the pattern, evidence and completeness
- Missing inputs are reported, not hidden



Thank you!

Connect With CyberAID:
LinkedIn: CyberAID

Next: Module 4 – Positioning EMTD Against the State of the Art



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