Postmortem Notes - INC-2026-0211

Facilitator: CIO | Date: 2026-02-12 | Audience: Exec + Engineering

Root cause (provisional)

• No confirmed single root cause. Competing explanations remain plausible due to missing evidence exports.
• Containment actions coincide with service restoration, which weakly supports SOC hypothesis, but ISP instability was observed independently.

Decisions

Decision	Owner	Rationale
Treat as security incident pending evidence	CIO	Avoid false clearance; regulators expect conservative stance.
Rotate privileged credentials after scope confirmation	SOC Lead	Prevent attacker persistence; avoid breaking OT systems prematu
Implement OT network segmentation review	OT Engineer	Reduce blast radius.

Regulatory / policy constraints

If credible PII exposure is confirmed, notify relevant authorities within 72 hours. Evidence must be preserved (logs, images).

Next checks (decisive)

• Obtain EDR full report for WS-17 and list all detections + timestamps.
• Pull firewall logs for outbound traffic; confirm whether transfer volume exceeded baseline.
• Review authentication logs for privileged account anomalies during 02:45-04:30.