AgriNova - IT Incident Summary (Manufacturing Network)

Incident ID: INC-2026-0211 | Date: 2026-02-11 | Severity: SEV-1 | Prepared for: COO, CIO

What happened

At 03:12 local time, the plant MES became unreachable. Production line stopped for 2h 45m. SOC observed unusual outbound traffic from workstation WS-17 to external IP 185.77.88.12.

Network team initially attributed outage to ISP instability. SOC believes a malware beacon was active. Evidence is incomplete: the EDR full report is referenced but not attached in this pack.

Impact

Metric	Value	Notes
Downtime	2h 45m	Line A stopped; Line B ran at reduced speed.
Estimated lost output	38 tonnes	Based on average 14 t/h at nominal speed.
Cloud billing spike	+28% week-over-week	Possibly due to log ingestion + incident tooling.
PII exposure risk	UNKNOWN	No confirmation of exfiltration; logs incomplete.

Conflicting hypotheses

• H1 (Network): ISP outage + flapping route caused MES disconnect. Expect no lateral movement indicators.
• H2 (SOC): Malware beacon + credential reuse; outage linked to containment (port shutdown). Expect EDR detections on WS-17 and auth anomalies.

Referenced but not attached

• EDR_Report_INC-2026-0211.pdf (referenced in SOC ticket; not attached).
• Firewall export (pcap) for 03:00-04:00 (not attached).