Slack Thread Export - #incident-warroom (INC-2026-0211)

Window: 2026-02-11 03:10 to 06:30 | Participants: SOC, Network, OT Engineer, IT Ops

Excerpt

03:18 SOC: Seeing outbound to 185.77.88.12 from WS-17. EDR shows 'Suspicious PowerShell' (need full report).

03:20 Network: ISP is dropping packets; looks like upstream issue. Rebooting edge router.

03:27 OT: MES down. Line A stopped. PLCs OK. Need ETA.

03:41 SOC: Isolated WS-17 at switch port 3/17. If MES returns now, cause may be host-based.

04:05 IT Ops: MES back online. Do we have proof of exfil?

04:07 SOC: Not yet. Need firewall export + EDR full report (referenced in ticket).

Screenshots referenced (not attached)

• Screenshot: EDR alert details (WS-17) - uploaded in Slack (not included in export).
• Screenshot: switch port shutdown confirmation (not included).