ELECTRIC GRID USE CASE

Stolen Engineering Laptop Used for Remote VPN Access

An electric grid use case showing how REMI turns event logs and source records into a cyber SITREP with confirmed findings, unresolved questions, and immediate next steps.

At 5:48 AM, the distribution control-room operator at North Valley Electric noticed that feeder status values from the East Ridge substation did not line up with the morning switching schedule. Nothing was fully offline, but the pattern was wrong: a breaker status changed without a matching operator note, relay communication showed overnight activity, and a substation engineering workstation appeared active outside the approved maintenance window.

The operator reported it to the utility's IT manager, who checked the remote-access console and saw a VPN session from **r.hale** at **1:36 AM**. The account belonged to a relay engineer, but the login came from **203.0.113.44**, a source IP the IT manager did not recognize. The session first touched **10.42.18.25** on the corporate network, then traffic appeared later toward **SUB-ENG-07**, a workstation used to support relay settings and substation maintenance.

The protection engineering lead then connected the VPN activity to a cyber event from the prior week: **REL-LT-14**, the relay engineer's field laptop, had been stolen from a Disney-area hotel. That changed the concern from odd grid-system behavior to compromised remote access. The warning signs were connected behaviors: a stolen engineering laptop, an off-hours VPN login, a new source location, corporate-network access, movement toward substation engineering, and relay/SCADA records that did not line up with the approved switching schedule.

Investigator Arrives Onsite

Later that morning, the investigator arrives onsite at **North Valley Electric Operations Center**. The investigator speaks with the distribution control-room operator who noticed the feeder-status mismatch, the utility IT manager who reviewed the VPN session, the protection engineering lead responsible for **SUB-ENG-07**, and the asset coordinator responsible for the stolen field laptop record.

After those conversations, the investigator requests copies of the available event logs and source records so they can be analyzed in REMI. The goal is to determine how the stolen laptop, relay engineering account, VPN session, corporate-network destination, and later substation-engineering traffic fit together as a cyber attack path. The more complete the log package is, the wider the investigative coverage becomes.

Event Logs to Request

- **VPN logs** showing remote-access sessions, source IPs, session times, and assigned accounts.
- **MFA and identity records** showing authentication results, approvals, resets, account ownership, and privilege changes.
- **MDM, device certificate, and stolen-laptop records** showing the status of **REL-LT-14**, remote wipe activity, certificate revocation, and last known device activity.
- **Firewall and network flow logs** showing internal destinations, blocked traffic, allowed traffic, and movement between zones.
- **EDR and workstation telemetry** showing process activity, file creation, script execution, callbacks, and malware indicators.
- **Substation engineering logs** showing access to relay workstations, SCADA support systems, historian servers, or OT-adjacent assets.
- **Relay, SCADA, and switching records** showing breaker status changes, relay communication, command acknowledgements, and approved operating activity.
- **Engineering work orders, relay-setting tickets, switching orders, and asset-owner records** showing whether the access path was expected.

REMI Flagged

- **Remote VPN login** by **r.hale** at **1:36 AM**.
- **New source IP** of **203.0.113.44** for that relay engineering account.
- **Stolen field laptop** record involving **REL-LT-14** one week before the VPN session.
- **Corporate-network access** to **10.42.18.25** after the VPN connection.
- **Traffic toward substation engineering** involving **SUB-ENG-07**.
- **Operational anomaly** involving breaker status activity that did not match the switching schedule.
- **Shared evidence links** across account, stolen device record, IP address, timestamp, destination system, session activity, relay records, and SCADA records.

Correlation and SITREP Output

The raw logs are imported into REMI for analysis. REMI identifies the flagged behaviors inside the evidence package, then correlates records that share the same account, stolen device record, source IP, session window, destination systems, relay events, SCADA records, and operational timestamps.

REMI Correlated

- **VPN session and relay engineering account** linked through **r.hale**, the **1:36 AM** session window, and remote-access records.
- **Stolen laptop and remote-access path** linked through **REL-LT-14**, device-management records, certificate status, and identity activity.
- **New source IP and internal destination** linked from **203.0.113.44** to **10.42.18.25** through VPN and firewall records.
- **Corporate-network access and substation engineering traffic** linked by timestamp, session activity, and later movement toward **SUB-ENG-07**.
- **Substation engineering workstation activity and operational anomaly** linked through the same overnight window as the East Ridge feeder status mismatch.
- **Shared evidence path** connecting account, stolen laptop, IP address, destination system, session window, firewall flow, workstation activity, relay records, and SCADA records.

SITREP Output Includes

- **Confirmed findings** showing what the evidence proves.
- **Unresolved questions** showing what still needs confirmation.
- **Additional source data needed** to close specific answer gaps.
- **Questions to ask IT, engineering, vendors, and system owners.**
- **Artifacts to preserve or sandbox** before cleanup.
- **Malware paths, scripts, services, or scheduled tasks to remove** after preservation.
- **Verification steps** to confirm the activity does not return.

How REMI Reconstructs It

The following simulated electric-grid excerpt shows the level of case-specific detail REMI can produce inside a SITREP. Names, accounts, IP addresses, systems, files, and records are examples, but the structure reflects the level of detail REMI is designed to generate from the evidence package.

Stolen Engineering Laptop Used for Remote VPN Access

REMI confirmed that **r.hale** established a remote VPN session at **1:36 AM** from **203.0.113.44**. Device-management records showed that **REL-LT-14**, the relay engineer's field laptop, had been reported stolen from a Disney-area hotel one week earlier. The VPN session reached **10.42.18.25** on the corporate network, and firewall records later showed traffic from that path toward **SUB-ENG-07** in the substation engineering environment.

REMI correlated the **stolen laptop record**, **VPN login**, **relay engineering account**, **source IP**, **corporate-network destination**, **substation engineering workstation traffic**, and **East Ridge feeder status mismatch** into one evidence path. The activity occurred during the same overnight window in which relay communication and breaker status values did not match the approved switching schedule.

The SITREP identified confirmed findings, including the **stolen laptop record**, **VPN session**, **source location**, **internal destination**, **substation engineering traffic**, and **operational anomaly**. It also identified unresolved questions: whether the laptop certificate was revoked before the VPN session, whether **MFA** was approved from the stolen device or a new device, whether **10.42.18.25** was used as an intermediate system, and whether **SUB-ENG-07** received script execution or outbound callback activity.

REMI generated immediate next steps: preserve **VPN logs**, **MFA records**, **MDM records**, **device certificate logs**, **firewall flows**, **EDR telemetry**, **relay records**, **SCADA records**, and **SUB-ENG-07 workstation logs**; request the stolen-device report and certificate revocation record for **REL-LT-14**; confirm ownership of **10.42.18.25**; disable exposed credentials and certificates tied to **r.hale**; isolate **SUB-ENG-07** if EDR confirms script execution or outbound callback traffic; and verify whether the feeder-status anomaly was caused by unauthorized activity from the compromised access path.