ELECTRIC GRID USE CASE

Quiet Movement and Pre-Positioning Inside the Grid

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 4:18 AM, the transmission control-room operator at North Valley Electric noticed that breaker-status changes from three substations did not line up with the overnight operating plan. Nothing was fully offline, but the pattern was wrong: **East Ridge**, **Mill Creek**, and **South Yard** each showed short command-and-acknowledgement bursts within the same twenty-minute window.

The operator reported it to the utility's IT manager, who reviewed the SCADA workstation logs and found command activity from **SCADA-OPS-03** under the valid account **ops_svc_grid**. The commands used normal system tools, but EDR telemetry showed **C:\Windows\Temp\grid-sync.ps1** launched from the workstation at **2:44 AM**. Firewall records then showed internal traffic from **10.42.18.25** toward substation gateways **SUB-GW-11**, **SUB-GW-14**, and **SUB-GW-19**.

That changed the concern from isolated status noise to quiet movement and pre-positioning inside electric-grid infrastructure. The warning signs were connected behaviors: valid credential use, built-in administrative tooling, repeated command timing, multi-substation reach, scripted workstation activity, and breaker/SCADA records that did not line up with the approved operating plan.

Investigator Arrives Onsite

Later that morning, the investigator arrives onsite at **North Valley Electric Operations Center**. The investigator speaks with the transmission control-room operator who noticed the substation pattern, the utility IT manager who reviewed the SCADA workstation, the SCADA lead responsible for **SCADA-OPS-03**, and the protection engineering lead responsible for the affected substations.

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 valid credentials, scripted workstation activity, SCADA commands, substation gateways, breaker-status changes, and operating-plan records fit together as an adversarial cyber operation. The more complete the log package is, the wider the investigative coverage becomes.

Event Logs to Request

- **SCADA command logs** showing command source, operator or service account, target substations, acknowledgements, and timestamps.
- **Identity and privileged-access records** showing service account use, session timing, privilege changes, token activity, and account ownership.
- **EDR and SCADA workstation telemetry** showing process launches, script execution, scheduled tasks, command shells, and administrative tool use.
- **Firewall and OT network flow logs** showing traffic between SCADA workstations, historian servers, control centers, and substation gateways.
- **Substation gateway and relay records** showing breaker status changes, relay communication, sequence-of-events logs, and command acknowledgements.
- **EMS, DMS, historian, and alarm records** showing operating state, load changes, alarms, suppressed alerts, and time-aligned status changes.
- **Switching orders, operating plans, maintenance tickets, and asset-owner records** showing whether the activity was approved.

REMI Flagged

- **SCADA command activity** from **SCADA-OPS-03** at **2:44 AM**.
- **Valid service account use** involving **ops_svc_grid** outside the approved operating window.
- **Script execution** involving **C:\Windows\Temp\grid-sync.ps1** on the SCADA workstation.
- **Traffic to multiple substation gateways** involving **SUB-GW-11**, **SUB-GW-14**, and **SUB-GW-19**.
- **Breaker-status changes** at **East Ridge**, **Mill Creek**, and **South Yard** inside the same command window.
- **Shared evidence links** across account, workstation process, command timing, substation gateway, breaker status, 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, workstation process, command timing, substation gateway, breaker status, relay event, SCADA record, and operational timestamp.

REMI Correlated

- **SCADA workstation and service account** linked through **SCADA-OPS-03**, **ops_svc_grid**, and the **2:44 AM** command window.
- **Script execution and command activity** linked through **C:\Windows\Temp\grid-sync.ps1**, EDR telemetry, and SCADA command history.
- **Internal traffic and substation gateways** linked from **10.42.18.25** to **SUB-GW-11**, **SUB-GW-14**, and **SUB-GW-19** through firewall records.
- **Multi-substation breaker activity** linked by timestamp across **East Ridge**, **Mill Creek**, and **South Yard**.
- **Shared evidence path** connecting account, workstation process, script path, command sequence, substation gateway, breaker status, 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.

Quiet Movement and Pre-Positioning Inside the Grid

REMI confirmed that **SCADA-OPS-03** launched **C:\Windows\Temp\grid-sync.ps1** at **2:44 AM** while the valid service account **ops_svc_grid** was active. SCADA command history showed command-and-acknowledgement bursts against **East Ridge**, **Mill Creek**, and **South Yard** inside the same twenty-minute window.

REMI correlated the **service account**, **SCADA workstation**, **script execution**, **substation gateway traffic**, **breaker-status changes**, and **operating-plan mismatch** into one evidence path. The activity used trusted credentials and built-in tools, which kept the individual records quiet until the timing, targets, and command pattern were connected.

The SITREP identified confirmed findings, including the **SCADA workstation**, **service account**, **script path**, **substation gateways**, **breaker-status changes**, and **affected substations**. It also identified unresolved questions: who controlled **ops_svc_grid** during the command window, whether **grid-sync.ps1** was staged by a prior access path, whether any relay settings were changed, and whether additional persistence remained on SCADA or historian systems.

REMI generated immediate next steps: preserve **SCADA command logs**, **EDR telemetry**, **identity records**, **firewall flows**, **substation gateway logs**, **relay records**, **historian records**, and a forensic copy of **grid-sync.ps1**; disable exposed tokens tied to **ops_svc_grid**; isolate **SCADA-OPS-03** after preservation; review **East Ridge**, **Mill Creek**, and **South Yard** relay settings against baseline; remove unauthorized scripts or scheduled tasks; and verify that command activity, breaker status, and substation traffic return to expected behavior.