

Quiet Movement and Pre-Positioning Inside Nuclear Support Networks

A nuclear facility 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 4:46 AM, the cyber security lead at Red River Nuclear Station noticed that authentication and file-access activity from the plant support enclave did not line up with the overnight work plan. Nothing was fully disrupted, but the pattern was wrong: a service account touched two historian servers, a jump host recorded administrative tool use, and engineering file-share access appeared during a window with no scheduled support activity.

The lead reported it to the station IT manager, who reviewed endpoint telemetry and found **C:\ProgramData\sync-cache\svc-index.ps1** launched from **NPE-JH-03** at **2:18 AM**. The command used built-in Windows tools under **svc_plant_ops**. Firewall records then showed traffic from **10.77.18.25** toward **HIST-02**, **HIST-04**, and **ENG-FS-06** inside the plant support network.

That changed the concern from routine authentication noise to quiet movement and pre-positioning inside nuclear support infrastructure. The warning signs were connected behaviors: valid service-account use, built-in administrative tooling, repeated access timing, movement across historian and engineering records, scripted jump-host activity, and file-access records that did not line up with the approved work plan.

Investigator Arrives Onsite

Later that morning, the investigator arrives onsite at **Red River Nuclear Station**. The investigator speaks with the cyber security lead who noticed the access pattern, the station IT manager who reviewed the jump host, the historian administrator responsible for **HIST-02** and **HIST-04**, and the engineering records owner responsible for **ENG-FS-06**.

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, jump-host activity, built-in tools, historian access, engineering file-share access, and approved work-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

- **Identity and privileged-access records** showing service account use, session timing, privilege changes, token activity, and account ownership.
- **EDR and jump-host telemetry** showing process launches, script execution, scheduled tasks, command shells, and administrative tool use.
- **Firewall and network flow logs** showing traffic between jump hosts, historian servers, engineering file shares, plant support servers, and business network systems.
- **Historian access logs** showing reads, exports, account activity, query timing, and affected plant support records.
- **Engineering file-share logs** showing file access, folder enumeration, downloads, writes, and timestamps.
- **Windows event logs, PowerShell logs, and task scheduler records** showing local execution, persistence, and command history.
- **Work plans, support tickets, asset-owner records, and change approvals** showing whether the access pattern was authorized.

REMI Flagged

- **Service-account activity** involving **svc_plant_ops** outside the approved support window.
- **Jump-host script execution** involving **C:\ProgramData\sync-cache\svc-index.ps1** on **NPE-JH-03**.
- **Historian access** involving **HIST-02** and **HIST-04** during the same overnight window.
- **Engineering file-share activity** involving **ENG-FS-06** without a matching support ticket.
- **Internal network traffic** from **10.77.18.25** across historian and engineering support assets.
- **Shared evidence links** across account, jump host, script path, network flow, historian access, file-share activity, and work-plan 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, jump host, script path, network destination, historian record, file-share event, and operational timestamp.

REMI Correlated

- **Jump host and service account** linked through **NPE-JH-03**, **svc_plant_ops**, and the **2:18 AM** execution window.
- **Script execution and administrative tool use** linked through **C:\ProgramData\sync-cache\svc-index.ps1**, EDR telemetry, and PowerShell logs.
- **Internal traffic and historian servers** linked from **10.77.18.25** to **HIST-02** and **HIST-04** through firewall records.
- **Historian access and engineering file-share activity** linked by timestamp to **ENG-FS-06** file enumeration records.
- **Shared evidence path** connecting account, jump host, script path, network flow, historian access, engineering file share, and work-plan 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 nuclear-facility 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 Nuclear Support Networks

REMI confirmed that **NPE-JH-03** launched **C:\ProgramData\sync-cache\svc-index.ps1** at **2:18 AM** while the valid service account **svc_plant_ops** was active. Firewall and access records showed traffic and authentication events against **HIST-02**, **HIST-04**, and **ENG-FS-06** inside the plant support network.

REMI correlated the **service account**, **jump host**, **script execution**, **historian access**, **engineering file-share activity**, and **work-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 access pattern were connected.

The SITREP identified confirmed findings, including the **jump host**, **service account**, **script path**, **historian servers**, **engineering file share**, and **affected support records**. It also identified unresolved questions: who controlled **svc_plant_ops** during the access window, whether **svc-index.ps1** was staged by a prior access path, whether files were exfiltrated, and whether additional persistence remained on historian or engineering support systems.

REMI generated immediate next steps: preserve **identity records**, **EDR telemetry**, **PowerShell logs**, **firewall flows**, **historian access logs**, **engineering file-share logs**, **task scheduler records**, and a forensic copy of **svc-index.ps1**; disable exposed tokens tied to **svc_plant_ops**; isolate **NPE-JH-03** after preservation; review **HIST-02**, **HIST-04**, and **ENG-FS-06** access records; remove unauthorized scripts or scheduled tasks; and verify that account activity, historian access, and plant support traffic return to expected behavior.