NUCLEAR USE CASE

# AI-Directed Pre-Positioning Across Nuclear Support Systems

## 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 4:37 AM, the cyber security lead at Granite Ridge Nuclear Station noticed that low-volume access across plant support systems did not line up with the overnight work plan. Nothing triggered a major alarm, but the pattern was wrong: a service account touched historian servers, a jump host launched administrative tools, and an engineering file share recorded folder enumeration during a window with no approved support activity.

The lead reported it to the station IT manager, who reviewed EDR and firewall records and found **C:\ProgramData\syscache\model-sync.ps1** launched from **NPE-JH-05** at **2:09 AM**. The command used **svc_npe_ops**, touched **HIST-02**, **HIST-05**, and **ENG-FS-08**, and created a small encrypted archive named **ops-map.dat**. Firewall records showed repeated short connections from **10.77.18.25** to plant support destinations.

That changed the concern from routine authentication noise to AI-directed pre-positioning inside nuclear support infrastructure. The warning signs were connected behaviors: valid service-account use, built-in administrative tooling, generated script execution, historian access, engineering file-share enumeration, staged archive creation, and work-plan records that did not match the access pattern.

## Investigator Arrives Onsite

Later that morning, the investigator arrives onsite at **Granite Ridge Nuclear Station**. The investigator speaks with the cyber security lead who noticed the low-volume access pattern, the station IT manager who reviewed the jump-host activity, the historian administrator responsible for **HIST-02** and **HIST-05**, and the engineering records owner responsible for **ENG-FS-08**.

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 service account, jump host, generated script, historian access, engineering file-share enumeration, archive creation, and work-plan mismatch fit together as a cyber attack path. 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, token activity, account ownership, and privilege changes.
- **EDR and jump-host telemetry** showing process launches, generated scripts, scheduled tasks, command shells, archive creation, 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 folder enumeration, downloads, writes, archive creation, and timestamps.
- **PowerShell, Windows event, and task scheduler logs** showing local execution, persistence, and command history.
- **Work plans, support tickets, asset-owner records, and change approvals** showing whether the access was authorized.

## REMI Flagged

- **Service-account activity** involving **svc_npe_ops** outside the approved support window.
- **Jump-host script execution** involving **C:\ProgramData\syscache\model-sync.ps1** on **NPE-JH-05**.
- **Historian access** involving **HIST-02** and **HIST-05** during the same overnight window.
- **Engineering file-share enumeration** involving **ENG-FS-08**.
- **Staged archive creation** involving **ops-map.dat**.
- **Internal network traffic** from **10.77.18.25** across plant support assets.
- **Shared evidence links** across account, jump host, script path, archive, 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, generated script path, archive name, network destination, historian record, file-share event, and operational timestamp.

## REMI Correlated

- **Service account and jump host** linked through **NPE-JH-05**, **svc_npe_ops**, and the **2:09 AM** execution window.
- **Generated script and archive creation** linked through **C:\ProgramData\syscache\model-sync.ps1**, **ops-map.dat**, EDR telemetry, and PowerShell logs.
- **Internal traffic and historian servers** linked from **10.77.18.25** to **HIST-02** and **HIST-05** through firewall records.
- **Historian access and engineering file-share enumeration** linked by timestamp to **ENG-FS-08** access records.
- **Shared evidence path** connecting account, jump host, generated script, archive, 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, operations, and system owners.**
- **Artifacts to preserve or sandbox** before cleanup.
- **Malware paths, generated 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.

### AI-Directed Pre-Positioning Across Nuclear Support Systems

REMI confirmed that **NPE-JH-05** launched **C:\ProgramData\syscache\model-sync.ps1** at **2:09 AM** while **svc_npe_ops** was active. Firewall records showed repeated short connections from **10.77.18.25** toward **HIST-02**, **HIST-05**, and **ENG-FS-08**. File records showed creation of **ops-map.dat** during the same window.

REMI correlated the **service account**, **jump host**, **generated script**, **staged archive**, **historian access**, **engineering file-share enumeration**, and **work-plan mismatch** into one evidence path. The activity used valid 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**, **archive file**, **historian servers**, **engineering file share**, and **plant support traffic**. It also identified unresolved questions: who controlled **svc_npe_ops** during the access window, whether **model-sync.ps1** was staged by a prior access path, whether **ops-map.dat** left the network, and whether additional persistence remained on 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 **ops-map.dat**; disable exposed tokens tied to **svc_npe_ops**; isolate **NPE-JH-05** after preservation; remove unauthorized scripts or scheduled tasks; and verify that account activity, historian access, and plant support traffic return to expected behavior.