NUCLEAR USE CASE

AI-Generated Logic Package Disguised as Vendor Maintenance

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 6:04 AM, the control systems engineer at Granite Ridge Nuclear Station noticed that auxiliary support values did not line up with the approved post-maintenance baseline. The plant support system was stable, but the pattern was wrong: a controller showed a new active revision, the upload time came after the approved vendor window, and the package name matched a work order while the behavior did not match the signed baseline.

The engineer reported it to the station IT manager, who reviewed the engineering workstation and found activity from **vendor_ctrl_19** on **NPE-ENG-12**. The uploaded package was named **AUX-TRAIN-B_Q1.apx**, but its checksum differed from the approved package hash. Firewall records showed traffic from **10.77.42.26** toward **PLANT-GW-18** before the controller upload, and EDR showed generated script staging under **C:\ProgramData\vendor-cache**.

That changed the concern from vendor maintenance review to adversarial controller manipulation. The warning signs were connected behaviors: approved-looking package naming, generated staging scripts, vendor-account activity, checksum mismatch, plant gateway traffic, controller upload, and historian values that did not match the approved baseline.

Investigator Arrives Onsite

Later that morning, the investigator arrives onsite at **Granite Ridge Nuclear Station**. The investigator speaks with the control systems engineer who noticed the baseline mismatch, the station IT manager who reviewed the workstation activity, the plant gateway owner responsible for **PLANT-GW-18**, and the vendor coordinator responsible for the maintenance package.

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 vendor account, generated staging scripts, controller logic package, checksum mismatch, plant gateway traffic, and controller upload fit together as a cyber attack path. The more complete the log package is, the wider the investigative coverage becomes.

Event Logs to Request

- **Controller logic files and hashes** showing approved baseline, uploaded package, checksum, active revision, and package history.
- **PLC and controller event logs** showing upload time, logic activation, restarts, forced values, configuration changes, and device responses.
- **Engineering workstation telemetry** showing file access, controller software activity, generated scripts, command shells, and process execution.
- **Vendor access and identity records** showing account use, session timing, MFA approval, assigned technician, and privilege changes.
- **Firewall and plant support network flow logs** showing traffic between engineering workstations, jump hosts, plant gateways, and controller networks.
- **Historian and alarm records** showing equipment state, operating trends, alarm acknowledgements, and time-aligned support changes.
- **Vendor work orders, maintenance packages, change tickets, and asset-owner approvals** showing whether the upload matched authorized work.

REMI Flagged

- **Controller package upload** involving **AUX-TRAIN-B_Q1.apx** after the authorized maintenance window.
- **Checksum mismatch** between the uploaded package and the approved baseline.
- **Generated staging scripts** under **C:\ProgramData\vendor-cache** before the upload.
- **Vendor-account activity** involving **vendor_ctrl_19** on **NPE-ENG-12**.
- **Traffic toward plant gateway PLANT-GW-18** from **10.77.42.26** before the upload.
- **Shared evidence links** across vendor account, workstation, script path, package name, checksum, gateway, controller event, and maintenance 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 vendor account, workstation, generated script path, logic package, checksum, plant gateway, controller event, historian record, and maintenance timestamp.

REMI Correlated

- **Vendor account and workstation** linked through **vendor_ctrl_19**, **NPE-ENG-12**, and engineering software activity.
- **Generated scripts and package upload** linked through **C:\ProgramData\vendor-cache**, **AUX-TRAIN-B_Q1.apx**, and EDR file history.
- **Checksum mismatch and active controller revision** linked through controller logs, approved hash records, and package history.
- **Plant gateway traffic and upload sequence** linked from **10.77.42.26** to **PLANT-GW-18** before the controller event.
- **Shared evidence path** connecting account, workstation, staging script, package name, checksum, gateway traffic, controller upload, historian trend, and maintenance 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-Generated Logic Package Disguised as Vendor Maintenance

REMI confirmed that **vendor_ctrl_19** accessed **NPE-ENG-12** and that **AUX-TRAIN-B_Q1.apx** was uploaded after the authorized maintenance window. The package name matched the work order, but the uploaded checksum did not match the approved baseline. EDR records showed generated script staging under **C:\ProgramData\vendor-cache** before the upload.

REMI correlated the **vendor account**, **engineering workstation**, **generated script path**, **logic package**, **checksum mismatch**, **plant gateway traffic**, **controller event**, and **historian baseline mismatch** into one evidence path. The activity used an approved-looking maintenance artifact, which kept individual records quiet until the file hash, timestamp, and controller event were connected.

The SITREP identified confirmed findings, including the **vendor account**, **generated staging path**, **logic package**, **checksum mismatch**, **PLANT-GW-18 traffic**, **controller upload**, and **active revision**. It also identified unresolved questions: who controlled **vendor_ctrl_19** during the upload window, where the generated scripts were created, whether additional packages were altered, and whether the changed logic affected related support systems.

REMI generated immediate next steps: preserve controller package files, approved hashes, PLC event logs, EDR telemetry, vendor access records, firewall flows, historian records, and maintenance tickets; sandbox **AUX-TRAIN-B_Q1.apx** and the generated scripts; restrict **vendor_ctrl_19**; restore the approved controller logic after preservation; and verify that controller communication and historian values return to expected behavior.