NUCLEAR USE CASE

AI-Spawned Malware Controller Inside Engineering Support

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 5:18 AM, the plant systems engineer at Granite Ridge Nuclear Station noticed that engineering support records did not line up with the overnight work plan. Nothing was fully down, but the pattern was wrong: an engineering workstation showed command activity after the maintenance window, a historian support server recorded repeated reads, and outbound traffic appeared from a workstation that had no approved remote task.

The engineer reported it to the station IT manager, who reviewed endpoint telemetry and found **C:\Users\Public\npe-controller.exe** launched from **NPE-ENG-07** at **2:41 AM**. The binary created generated PowerShell scripts under **C:\ProgramData\npe-cache**, spawned a child process named **sim-link.exe**, and connected to **203.0.113.91**. Firewall records then showed internal traffic from **10.77.31.18** toward **HIST-04** and **ENG-FS-02**.

That changed the concern from workstation noise to an AI-spawned malware controller inside engineering support. The warning signs were connected behaviors: generated script creation, controller process activity, outbound callback traffic, historian reads, engineering file-share access, and support-system activity outside the approved work plan.

Investigator Arrives Onsite

Later that morning, the investigator arrives onsite at **Granite Ridge Nuclear Station**. The investigator speaks with the plant systems engineer who noticed the support-record mismatch, the station IT manager who reviewed the endpoint telemetry, the engineering systems owner responsible for **NPE-ENG-07**, and the historian administrator responsible for **HIST-04**.

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 malware controller, generated scripts, engineering workstation, callback traffic, historian access, and file-share activity fit together as a cyber attack path. The more complete the log package is, the wider the investigative coverage becomes.

Event Logs to Request

- **EDR and workstation telemetry** showing process launches, parent-child process chains, generated scripts, file creation, command shells, and persistence indicators.
- **PowerShell and Windows event logs** showing script execution, encoded commands, scheduled tasks, service creation, and local account activity.
- **Firewall and DNS logs** showing outbound callbacks, internal destinations, blocked traffic, allowed traffic, and domain resolution activity.
- **Historian and engineering file-share logs** showing reads, exports, file access, folder enumeration, timestamps, and affected support records.
- **Identity and privileged-access records** showing account use, token activity, group membership, MFA events, and privilege changes.
- **Maintenance plans, work orders, change tickets, and asset-owner records** showing whether the activity matched authorized work.

REMI Flagged

- **Malware controller execution** involving **C:\Users\Public\npe-controller.exe** on **NPE-ENG-07**.
- **Generated script creation** under **C:\ProgramData\npe-cache** during the same overnight window.
- **Child process activity** involving **sim-link.exe** after the controller launched.
- **Outbound callback** from **10.77.31.18** to **203.0.113.91**.
- **Historian and engineering file-share access** involving **HIST-04** and **ENG-FS-02**.
- **Shared evidence links** across workstation, file path, process chain, source IP, destination IP, historian record, 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 workstation, file path, process chain, source IP, callback destination, historian record, engineering file-share event, and operational timestamp.

REMI Correlated

- **Controller file and workstation** linked through **NPE-ENG-07**, **C:\Users\Public\npe-controller.exe**, and EDR process history.
- **Generated scripts and child process activity** linked through **C:\ProgramData\npe-cache**, **sim-link.exe**, PowerShell logs, and file creation records.
- **Outbound callback and internal movement** linked from **10.77.31.18** to **203.0.113.91**, **HIST-04**, and **ENG-FS-02** through firewall records.
- **Historian access and work-plan mismatch** linked by timestamp to the same overnight controller activity.
- **Shared evidence path** connecting workstation, malware file, generated scripts, process chain, callback traffic, historian access, file-share activity, 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-Spawned Malware Controller Inside Engineering Support

REMI confirmed that **NPE-ENG-07** launched **C:\Users\Public\npe-controller.exe** at **2:41 AM**. The process created generated scripts under **C:\ProgramData\npe-cache**, spawned **sim-link.exe**, and established outbound traffic from **10.77.31.18** to **203.0.113.91**.

REMI correlated the **controller file**, **generated scripts**, **child process chain**, **callback destination**, **historian access**, **engineering file-share activity**, and **work-plan mismatch** into one evidence path. The activity occurred during the same overnight window in which plant support records showed access outside authorized maintenance.

The SITREP identified confirmed findings, including the **malware controller**, **generated script directory**, **child process**, **source workstation**, **callback IP**, **historian reads**, and **engineering file-share access**. It also identified unresolved questions: which account launched the controller, whether the controller was staged by a prior remote session, whether generated scripts touched additional support systems, and whether any files were exported from **ENG-FS-02**.

REMI generated immediate next steps: preserve EDR telemetry, PowerShell logs, firewall flows, DNS records, historian logs, engineering file-share logs, and a forensic copy of **npe-controller.exe**; sandbox the controller and generated scripts; isolate **NPE-ENG-07** after preservation; remove unauthorized scripts, scheduled tasks, and services; and verify that historian access and outbound traffic return to expected behavior.