WATER TREATMENT USE CASE

AI-Spawned Malware Controllers and Vendor OT Setting Changes

A water utility 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 4:42 AM, the treatment supervisor at North Valley Water Treatment Plant noticed that chlorine feed values from the south chemical room were drifting outside the normal morning range. The plant was still operating, but the pattern was wrong: a dosing value had changed without a matching operator note, and the historian showed a short burst of controller activity during a window when no chemical-feed adjustment was scheduled.

The supervisor contacted the utility's IT manager, who reviewed the OT support console and saw overnight activity from the vendor workstation **VOT-ENG-12**. The workstation was used for vendor diagnostics, but EDR telemetry showed execution of **C:\ProgramData\ctl-sync.exe** at **3:58 AM**, followed by script activity from **C:\Temp\dose-check.ps1**. HMI records later showed a setpoint change against **CHEM-PLC-02**, the controller supporting chemical-feed operations.

That combination changed the concern from abnormal process behavior to active compromise concern. The warning signs were connected behaviors: unexplained vendor OT workstation activity, AI-spawned controller tooling, script execution, a chemical-feed setting change, and historian values that did not line up with the expected operating record.

Investigator Arrives Onsite

Later that morning, the investigator arrives onsite at **North Valley Water Treatment Plant**. The investigator speaks with the treatment supervisor who noticed the dosing drift, the operator responsible for the south chemical room, the utility IT manager who reviewed the vendor workstation, and the vendor coordinator responsible for scheduled OT maintenance.

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 whether the setting change was approved maintenance, compromised vendor activity, unauthorized controller interaction, or malware-driven manipulation of the OT support path. The more complete the log package is, the wider the investigative coverage becomes.

Event Logs to Request

- **EDR and vendor workstation telemetry** showing process activity, file creation, script execution, callbacks, and malware indicators.
- **HMI action logs** showing operator screens, setpoint changes, acknowledgement activity, and user context.
- **PLC and controller event logs** showing write events, forced values, configuration changes, downloads, and control actions.
- **Historian and alarm records** showing chlorine feed values, alarm state, alarm silence, acknowledgements, and trend changes.
- **Firewall and OT network flow logs** showing traffic between vendor workstations, HMI hosts, historian servers, and controller networks.
- **Vendor work orders, change tickets, shift logs, and asset-owner records** showing whether the setting change was expected.

REMI Flagged

- **Vendor OT workstation activity** on **VOT-ENG-12** during an unscheduled maintenance window.
- **AI-spawned controller tool** execution involving **C:\ProgramData\ctl-sync.exe** at **3:58 AM**.
- **Script activity** from **C:\Temp\dose-check.ps1** after the controller tool launched.
- **HMI setpoint change** affecting **CHEM-PLC-02** in the south chemical room.
- **Historian anomaly** showing chlorine feed values drifting outside the expected operating range.
- **Shared evidence links** across workstation, process, file path, HMI action, controller event, timestamp, and historian 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, process, file path, HMI action, controller event, alarm state, and operational timestamp.

REMI Correlated

- **Vendor OT workstation and spawned tool** linked through **VOT-ENG-12**, **C:\ProgramData\ctl-sync.exe**, and the **3:58 AM** execution window.
- **Spawned process and script activity** linked from **ctl-sync.exe** to **C:\Temp\dose-check.ps1** through EDR and command-history records.
- **HMI activity and controller event** linked by timestamp to the setpoint change affecting **CHEM-PLC-02**.
- **Controller activity and historian anomaly** linked through the same operating window as the chlorine feed drift.
- **Shared evidence path** connecting workstation, executable, script, HMI action, controller event, alarm state, and historian 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 water-treatment 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 Controllers and Vendor OT Setting Changes

REMI confirmed that **VOT-ENG-12** executed **C:\ProgramData\ctl-sync.exe** at **3:58 AM**. EDR records showed follow-on script activity from **C:\Temp\dose-check.ps1**, and HMI records later showed a setpoint change against **CHEM-PLC-02** in the south chemical room.

REMI correlated the **vendor OT workstation**, **AI-spawned controller tool**, **script execution**, **HMI setpoint change**, **controller event**, and **chlorine feed historian anomaly** into one evidence path. The activity occurred during the same overnight window in which chlorine feed values drifted outside the expected operating range.

The SITREP identified confirmed findings, including the **workstation execution event**, **spawned tool path**, **script path**, **HMI action**, **controller target**, and **historian anomaly**. It also identified unresolved questions: whether the change matched an approved **maintenance ticket**, whether the vendor tool was authorized, whether **CHEM-PLC-02** should have accepted the change during that window, and whether additional payloads remained on **VOT-ENG-12** or adjacent OT support hosts.

REMI generated immediate next steps: preserve **EDR telemetry**, **HMI logs**, **PLC event records**, **historian records**, **alarm records**, and forensic copies of **ctl-sync.exe** and **dose-check.ps1**; request the related **vendor work order** and **change ticket**; compare **CHEM-PLC-02** settings against approved baselines; isolate **VOT-ENG-12**; sandbox the spawned controller tool; remove staged scripts after preservation; and verify that the chemical-feed setting, workstation processes, and OT network traffic return to expected behavior.