WATER TREATMENT USE CASE

Vendor-Infected Firmware Update at Pump Station

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 7:35 AM, the distribution supervisor at North Valley Water Treatment Plant noticed that the east pressure zone was cycling more than expected. Nothing had failed, but the pattern was wrong: the East Ridge pump station showed repeated short starts, the pressure trend dipped during normal demand, and the local controller reported a firmware version that did not match the maintenance record.

The supervisor contacted the utility's IT manager, who reviewed the maintenance console and saw that a firmware package named **ERPS_FW_4.8.2.bin** had been applied to **PS-PLC-07** at **1:22 AM**. The update appeared to come through the vendor support path used by **vendor_ops_17**, but there was no matching approved change ticket for that overnight window. Firewall records also showed traffic from the pump-station subnet back to **198.51.100.77** after the firmware update completed.

That combination changed the concern from equipment instability to supply-chain compromise concern. The warning signs were connected behaviors: an unapproved firmware update, vendor-support account activity, a controller version mismatch, pump cycling after the update, and outbound traffic from the pump-station network to a vendor-adjacent external address.

Investigator Arrives Onsite

Later that morning, the investigator arrives onsite at **North Valley Water Treatment Plant**. The investigator speaks with the distribution supervisor who noticed the pressure-zone cycling, the operator responsible for the East Ridge pump station, the utility IT manager who reviewed the maintenance console, and the vendor coordinator responsible for firmware update approvals.

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 firmware update was approved vendor maintenance, a compromised vendor package, unauthorized controller activity, or a firmware-driven disruption of pump-station operations. The more complete the log package is, the wider the investigative coverage becomes.

Event Logs to Request

- **Firmware management logs** showing package name, upload source, install time, checksum, controller target, and reboot activity.
- **PLC and controller event logs** showing firmware write events, configuration changes, forced values, restarts, and post-update faults.
- **Pump telemetry and historian records** showing starts, stops, pressure trend, flow, tank level, and abnormal cycling after the update.
- **Vendor access and identity records** showing account use, remote-support path, MFA approval, session timing, and assigned technician.
- **Firewall and OT network flow logs** showing traffic between the pump-station subnet, maintenance console, vendor endpoints, and external IPs.
- **Vendor work orders, firmware release notes, change tickets, shift logs, and asset-owner records** showing whether the update was expected.

REMI Flagged

- **Firmware update** applied to **PS-PLC-07** at **1:22 AM** outside the approved maintenance window.
- **Vendor-support account activity** tied to **vendor_ops_17** during the same update window.
- **Firmware package mismatch** involving **ERPS_FW_4.8.2.bin** and the approved controller baseline.
- **Pump cycling anomaly** at East Ridge pump station after the firmware update completed.
- **Outbound network traffic** from the pump-station subnet to **198.51.100.77** after the controller reboot.
- **Shared evidence links** across account, firmware package, controller event, pump telemetry, timestamp, and firewall 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, firmware package, controller target, pump telemetry, network destination, and operational timestamp.

REMI Correlated

- **Vendor-support account and firmware package** linked through **vendor_ops_17**, **ERPS_FW_4.8.2.bin**, and the **1:22 AM** update window.
- **Firmware install and controller restart** linked to **PS-PLC-07** through controller event logs and maintenance-console records.
- **Pump telemetry and controller event** linked by timestamp to repeated short starts at the East Ridge pump station.
- **Firmware update and outbound traffic** linked through the same post-reboot window and destination **198.51.100.77**.
- **Shared evidence path** connecting vendor account, firmware package, checksum, controller event, pump telemetry, firewall records, and change 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.

Vendor-Infected Firmware Update at Pump Station

REMI confirmed that **ERPS_FW_4.8.2.bin** was applied to **PS-PLC-07** at **1:22 AM**. Firmware management records showed the install and controller reboot, while vendor access records tied the update window to **vendor_ops_17**.

REMI correlated the **vendor-support account**, **firmware package**, **controller target**, **pump cycling anomaly**, **post-reboot outbound traffic**, and **pressure-zone historian trend** into one evidence path. The activity occurred during the same overnight window in which East Ridge pump station began repeated short starts.

The SITREP identified confirmed findings, including the **firmware install event**, **controller reboot**, **package name**, **vendor account**, **pump telemetry change**, and **external network destination**. It also identified unresolved questions: whether the update matched an approved **change ticket**, whether the firmware checksum matched the vendor release, whether **PS-PLC-07** should have accepted the package, and whether the outbound connection to **198.51.100.77** was part of approved vendor telemetry.

REMI generated immediate next steps: preserve **firmware management logs**, **PLC event records**, **historian records**, **firewall flows**, **vendor access logs**, and a forensic copy of **ERPS_FW_4.8.2.bin**; request the related **vendor work order**, **release notes**, and **checksum record**; compare **PS-PLC-07** firmware against the approved baseline; restrict the vendor-support path; sandbox the firmware package; roll back or reimage the controller after preservation if required; and verify that pump cycling, controller events, and outbound traffic return to expected behavior.