SENTINEL | OT

PROJECT SCOPE

Cedar Ridge Regional Water Authority: Full Assessment and Remediation

DOCUMENT	Project Scope and Statement of Work
DATE	May 15, 2026
PREPARED BY	Sentinel OT
CLASSIFICATION	Confidential
REFERENCE	Report ID: pbcwud_cedar-ridge_sample_2026-05-12

Background

On May 12, 2026, Sentinel OT delivered a Comprehensive Vulnerability Assessment Report to Cedar Ridge Regional Water Authority (CRRWA) documenting the results of a full external and internal assessment of the Cedar Ridge Water Treatment Plant. The assessment combined passive external reconnaissance (April 14 to 15, 2026) with a five-day on-site assessment (May 5 to 9, 2026).

The assessment identified **seven Critical findings**, **five High findings**, and **four Medium findings** across the facility's operational technology infrastructure. Key findings include:

- Three Critical CVEs (CVSS 9.8) on two internet-exposed Rockwell Automation CompactLogix 1769-L18ER controllers, including CVE-2021-22681, which is listed in the CISA Known Exploited Vulnerabilities catalog with a federal remediation deadline that has already passed.
- No network segmentation in the OT environment. All devices share a single flat 192.168.1.0/24 subnet connected through an unmanaged Allen-Bradley Stratix 2000 switch.
- An HMI workstation (Dell OptiPlex 7070) running end-of-life Windows 10 Pro 21H2 with no security updates since January 2025 and no endpoint protection software.
- A FactoryTalk Historian SE database accessible with default vendor credentials from any device on the flat network.
- No PLC program backups or change management. The most recent backup is 22 months old.
- Shared operator credentials across all staff and the contracted systems integrator, with no individual accounts.
- No logging or monitoring infrastructure anywhere in the OT environment.

Phase 1 compensating controls were applied April 23 to 25, 2026, eliminating direct internet exposure of the PLCs prior to the on-site assessment. Those controls remain in place but depend on a single network device (the Microhard BulletPlus cellular gateway) and do not address any of the internal findings.

This document defines the scope, deliverables, timeline, and cost for a full remediation engagement addressing all findings from the Comprehensive Vulnerability Assessment. It is designed to accompany a grant application under the State and Local Cybersecurity Grant Program (SLCGP) or the Drinking Water State Revolving Fund (DWSRF).

Engagement Objectives

1. **Eliminate internet exposure** of all industrial control system assets and establish defense-in-depth that does not depend on a single device.
2. **Remediate all Critical and High findings** identified in the May 12 assessment report, or document formal risk acceptance with compensating controls where hardware limitations prevent full remediation.
3. **Establish a segmented, defensible network architecture** with zone-based access controls per IEC 62443-3-3, replacing the current flat network and NAT/port-forwarding model.
4. **Harden all OT endpoints** including the HMI workstation, historian server, and radio telemetry link.
5. **Implement individual accountability** through named user accounts, role-based access, and audit logging.
6. **Deploy logging and monitoring** capable of detecting unauthorized access and configuration changes.
7. **Establish a controller change management program** with golden image baselines and a documented comparison procedure.
8. **Produce compliance-grade documentation** satisfying AWIA Section 2013, IEC 62443, and NIST SP 800-82 Rev 3 requirements.

Scope of Work

Phase 1: Immediate Compensating Controls (Days 1 to 3)

No plant downtime required. All work performed remotely at the network edge.

TASK	DESCRIPTION	ADDRESSES
1.1	Configure access control lists on the Microhard BulletPlus gateway to drop all inbound traffic to ports 44818/tcp and 44818/udp from any source other than a designated operator jump host	EXT-1, EXT-2

TASK	DESCRIPTION	ADDRESSES
1.2	Block inbound traffic to ports 80/tcp and 443/tcp on both public IPs at the gateway	EXT-3
1.3	Block inbound traffic to port 602/tcp (XetaWave radio management)	EXT-4
1.4	Disable FTP (21/tcp) and Telnet (23/tcp) services on the Microhard gateway	EXT-6
1.5	Rotate all credentials on the Microhard gateway, PLC web interfaces, and SSH services. Replace default “UserDevice” credentials with strong, unique passwords	EXT-6
1.6	Restrict the open DNS resolver on port 53/tcp to the internal interface only	EXT-5

Deliverable: Compensating Controls Verification Report confirming all six tasks are complete, with before-and-after evidence from passive scan validation.

Phase 2: Comprehensive On-Site Assessment (Days 4 to 14)

On-site work at the Cedar Ridge Water Treatment Plant. Conducted by two qualified OT security assessors over five days, plus pre-assessment planning and post-assessment analysis.

TASK	DESCRIPTION
2.1	Validate all passive external findings against physical infrastructure. Confirm device inventory, firmware versions, and network topology against CIP identity responses and device faceplates.
2.2	Map the complete OT network architecture: controllers, HMI, historian, cellular gateway, radio links, switches, and any additional field devices or connections not visible from passive reconnaissance.
2.3	Perform controller integrity baseline. Upload the running program from each PLC and compare against the last known-good backup from the plant integrator. Document the comparison result, including any unexplained differences.

TASK	DESCRIPTION
2.4	Audit the Microhard BulletPlus gateway configuration: internal firewall rules, NAT table, VPN configuration, service enable state, and logging posture.
2.5	Assess all internal OT assets for vulnerabilities: HMI operating system and patch level, endpoint protection, historian database access controls, USB device policy, radio link encryption, and physical access controls.
2.6	Evaluate access management practices: shared vs. individual credentials, password age, integrator remote access procedures, and audit trail capability.
2.7	Assess logging and monitoring posture: log sources, retention periods, alerting capability, and evidence preservation.
2.8	Conduct AWIA-aligned risk and resilience assessment for cybersecurity components, per Section 2013 requirements.
2.9	Interview plant operations staff and the contracted systems integrator to document current access procedures, change management practices, backup procedures, and incident response capabilities.

Deliverable: Comprehensive Vulnerability Assessment Report including validated asset inventory, network architecture diagram, controller integrity baseline results, internal and external vulnerability register with risk ratings, and standards compliance gap analysis.

Phase 3: Network Architecture Remediation (Days 15 to 50)

Requires coordination with plant operations for scheduled maintenance windows. Two on-site visits anticipated.

TASK	DESCRIPTION	ADDRESSES	ESTIMATED DOWNTIME
3.1	Replace the current NAT/port-forwarding model on the Microhard BulletPlus gateway with a VPN-only architecture. All remote access will terminate through an encrypted tunnel with certificate-based authentication.	EXT-1 through EXT-6	4 to 6 hours
3.2	Deploy an industrial firewall between the cellular gateway and the OT network. Configure zone-based access control rules per IEC 62443-3-3 SR 5.1. Firewall options: Fortinet FortiGate Rugged 60F (estimated $2,770 list plus annual FortiGuard subscription) or Cisco ISA 3000 (estimated $5,750 list plus annual subscription).	INT-1, EXT-1 through EXT-3	2 to 4 hours
3.3	Replace the unmanaged Allen-Bradley Stratix 2000 switch with a managed industrial Ethernet switch supporting VLANs (e.g., Cisco IE-3300-8T2S-E at approximately $2,350 list). Configure VLAN segmentation with four zones: (1) controller/PLC, (2) HMI/engineering, (3) historian/data, (4) network edge/gateway.	INT-1	2 to 4 hours

TASK	DESCRIPTION	ADDRESSES	ESTIMATED DOWNTIME
3.4	Configure inter-VLAN routing rules on the industrial firewall. Restrict traffic between zones to only required protocols and ports (e.g., EtherNet/IP from HMI zone to PLC zone only, SQL from historian zone to HMI zone only).	INT-1	Included in 3.2 and 3.3
3.5	Establish a secure remote access jump host for authorized operator and integrator access. Require multi-factor authentication. Deploy on a hardened workstation or virtual machine in the network edge zone.	EXT-1 through EXT-6, INT-6	No downtime
3.6	Perform segmentation verification testing. Confirm that zone boundaries enforce the intended access controls. Document all permitted and denied traffic flows.	INT-1	No downtime

Deliverable: Network Architecture Remediation Report with updated network diagrams showing zone boundaries, firewall rule documentation, VLAN configuration, VPN configuration records, and segmentation verification test results.

Phase 4: Controller and Endpoint Remediation (Days 35 to 75)

Requires scheduled maintenance windows. Controllers updated in sequence, never simultaneously. Two on-site visits anticipated.

TASK	DESCRIPTION	ADDRESSES	ESTIMATED DOWNTIME
4.1	Coordinate with Rockwell Automation to identify the latest supported firmware for the 1769-L18ER platform. Validate compatibility with the existing Studio 5000 project. If a Rockwell TechConnect support contract is required, coordinate procurement with CRRWA.	EXT-1, EXT-2, EXT-3	No downtime (planning)
4.2	Upgrade controller firmware to the latest supported version. If the platform supports CIP Security (Logix Designer v33 or later), enable authentication and integrity on EtherNet/IP sessions.	EXT-1, EXT-2, EXT-3	2 to 4 hours per controller
4.3	If CIP Security is not supported on the 1769-L18ER platform, document formal risk acceptance with compensating controls per IEC 62443-3-3 SR 1.1 and include controller replacement in the FY2027 capital request.	EXT-1, EXT-2	No downtime

TASK	DESCRIPTION	ADDRESSES	ESTIMATED DOWNTIME
4.4	Enable Controller Change Detection if supported by the firmware version. Establish a golden image baseline from the programs uploaded during Phase 2. Define a monthly comparison procedure.	EXT-2, INT-4	30 minutes per controller
4.5	Rotate all cached authentication keys on both controllers.	EXT-1	30 minutes per controller
4.6	Rebuild the HMI workstation (HMI-01) with a supported operating system. Install Windows 10 IoT Enterprise LTSC 2021 (approximately $350 per license) or Windows 11 IoT Enterprise LTSC. Reinstall FactoryTalk View SE Client and Studio 5000 on the rebuilt system. Apply all current security updates.	INT-2	8 to 12 hours (can be performed on replacement hardware with cutover)

TASK	DESCRIPTION	ADDRESSES	ESTIMATED DOWNTIME
4.7	Deploy application whitelisting on the rebuilt HMI workstation. Configure Windows Defender Application Control (WDAC) policies to allow only authorized applications (FactoryTalk View SE, Studio 5000, and required system processes). Restrict execution of unsigned binaries.	INT-2	Included in 4.6
4.8	Disable USB mass storage on the HMI workstation via Group Policy. Whitelist only authorized USB HID devices (keyboard, mouse). If USB file transfer is operationally required, document a media sanitization procedure.	INT-5	1 hour
4.9	Harden the FactoryTalk Historian SE database on HIST-01. Change the SQL Server Express SA password, disable the SA account, and create named service accounts with least-privilege roles. Restrict SQL Server connections to the historian VLAN only (dependent on Phase 3 segmentation).	INT-3	1 to 2 hours

TASK	DESCRIPTION	ADDRESSES	ESTIMATED DOWNTIME
4.10	Enable AES-256 encryption on the XetaWave XETA9-E point-to-point radio link between the treatment plant and the booster station. Requires configuration on both ends of the link.	INT-8	15 to 30 minutes
4.11	Install an electronic keypad or badge-access lock on the server closet housing HIST-01 and network equipment. Restrict access to authorized personnel.	INT-9	No downtime

Deliverable: Controller and Endpoint Remediation Report with firmware upgrade records, CIP Security configuration evidence (or formal risk acceptance), HMI rebuild documentation, application whitelisting policy records, historian hardening evidence, radio encryption verification, and golden image baseline documentation.

Phase 5: Access Management, Logging, and Monitoring (Days 50 to 80)

Minimal downtime required. Most tasks are additive and do not interrupt running processes.

TASK	DESCRIPTION	ADDRESSES	ESTIMATED DOWNTIME
5.1	Create individual named accounts for each plant operator, the contracted systems integrator, and any other personnel requiring access. Configure accounts on the HMI workstation (Windows local accounts or Active Directory if available), FactoryTalk View SE, and the Microhard gateway.	INT-6	No downtime
5.2	Implement role-based access control. Define three roles: Operator (view and acknowledge alarms), Engineer (program and configure), and Administrator (system configuration). Assign each user the minimum required role.	INT-6	No downtime
5.3	Implement a password policy requiring unique passwords per user, minimum 12-character length, and rotation at least annually. For the integrator remote access account, require MFA through the VPN architecture deployed in Phase 3.	INT-6	No downtime

TASK	DESCRIPTION	ADDRESSES	ESTIMATED DOWNTIME
5.4	Deploy a centralized syslog server for the OT network. Install on a dedicated small form factor PC or virtual machine on the historian server (estimated hardware cost $1,200 to $1,800 if dedicated). Use open-source log management (Wazuh or Graylog Open).	INT-7	No downtime
5.5	Configure log forwarding from the Microhard BulletPlus gateway, HMI workstation (Windows Security Event Log), historian server (Windows Security Event Log and SQL Server audit), and the industrial firewall deployed in Phase 3. Configure a minimum 90-day log retention policy.	INT-7	No downtime
5.6	Define alerting rules for high-priority events: failed login attempts (3 or more in 5 minutes), gateway configuration changes, new device connections, and controller access events if supported by the Studio 5000 version.	INT-7	No downtime

TASK	DESCRIPTION	ADDRESSES	ESTIMATED DOWNTIME
5.7	Establish a formal change management procedure for PLC programs. Document the procedure covering: written change request before any modification, program backup before and after every change, comparison of running program against golden image on a monthly schedule. Store backups on encrypted removable media in a locked cabinet and/or secure cloud storage.	INT-4	No downtime
5.8	Conduct operator training session (half day). Cover: new login procedures, role-based permissions, USB media policy, change management procedures, how to read and respond to syslog alerts, and escalation contacts.	INT-6, INT-7	No downtime

Deliverable: Access Management and Monitoring Report with user account registry, role definitions, password policy documentation, syslog server configuration, log forwarding verification, alerting rule documentation, change management procedure, and operator training attendance record.

Phase 6: Documentation and Compliance (Days 70 to 95)

TASK	DESCRIPTION
6.1	Produce a complete AWIA-compliant Risk and Resilience Assessment document incorporating all findings from the Comprehensive Vulnerability Assessment, all remediations performed in Phases 1 through 5, and all residual risks with documented risk acceptance where applicable.
6.2	Produce an AWIA-compliant Emergency Response Plan update reflecting the new network architecture, access procedures, logging capabilities, and escalation contacts.
6.3	Produce a Standards Compliance Mapping document showing alignment with IEC 62443-3-3, NIST SP 800-82 Rev 3, and CISA CPG 2.0. Document the pre-engagement and post-engagement compliance state for each applicable requirement.
6.4	Produce an as-built network architecture document with zone diagrams, IP assignments, VLAN configuration, firewall rules, and VPN topology. This becomes the authoritative reference for the OT network and must be updated whenever changes are made.
6.5	Deliver an Executive Summary suitable for presentation to the CRRWA Board of Directors and municipal counsel, including total investment, risk reduction achieved, and recommended next steps.
6.6	Conduct a closeout briefing with plant operations staff and the contracted systems integrator covering all changes made, new procedures, and ongoing responsibilities.

Deliverable: Complete compliance documentation package (RRA, ERP update, standards mapping, as-built network documentation, executive summary).

Phase 7: Ongoing Monitoring (Month 4 onward)

TASK	DESCRIPTION
7.1	Continuous passive monitoring of all CRRWA internet-facing assets to detect any re-exposure or new services appearing on public IPs.

TASK	DESCRIPTION
7.2	Vulnerability alerting for all Rockwell Automation products deployed at the facility, including new CVE publications, CISA advisories, and KEV catalog additions.
7.3	Quarterly posture report summarizing monitoring findings, syslog alert review, any new advisories, and recommended actions.
7.4	Annual review of compensating controls, risk acceptances, and residual risks documented during the engagement.

Deliverable: Quarterly Monitoring Reports. Ongoing alert notifications delivered within 24 hours of relevant advisory publication. Annual compensating control review report.

Timeline

PHASE	DURATION	DEPENDENCIES
Phase 1: Compensating Controls	Days 1 to 3	None. Can begin immediately upon contract execution.
Phase 2: On-Site Assessment	Days 4 to 14	Phase 1 complete. Plant access coordinated with CRRWA operations.
Phase 3: Network Architecture	Days 15 to 50	Phase 2 complete. Maintenance windows scheduled with operations. Hardware procurement lead time (2 to 4 weeks for industrial firewall and managed switch).
Phase 4: Controller and Endpoint	Days 35 to 75	Phase 2 complete. Rockwell coordination initiated. Overlaps with Phase 3. HMI rebuild can begin as soon as replacement OS license is procured.

PHASE	DURATION	DEPENDENCIES
Phase 5: Access and Monitoring	Days 50 to 80	Phase 3 substantially complete (segmentation required for historian access controls). Phase 4 HMI rebuild complete (for WDAC and account configuration).
Phase 6: Documentation	Days 70 to 95	Phases 3, 4, and 5 substantially complete.
Phase 7: Monitoring	Month 4 onward	Phases 1 through 6 complete. Continuous.

Total engagement duration (Phases 1 through 6): approximately 95 calendar days.

Cost Estimate

Professional Services

PHASE	DESCRIPTION	HOURS	RATE	COST
Phase 1	Compensating Controls (remote)	16	$300/hr	$4,800
Phase 2	Comprehensive On-Site Assessment (5 days, 2 assessors, travel, reporting)	Blended	Blended	$52,000
Phase 3	Network Architecture Remediation (design, procurement support, 2 on-site implementation trips, testing)	140	$300/hr	$42,000
Phase 4	Controller and Endpoint Remediation (firmware coordination, HMI rebuild, historian hardening, 2 on-site trips)	120	$300/hr	$36,000

PHASE	DESCRIPTION	HOURS	RATE	COST
Phase 5	Access Management, Logging, and Monitoring (account setup, syslog deployment, change management, training)	80	$300/hr	$24,000
Phase 6	Documentation and Compliance (AWIA RRA, ERP, standards mapping, as-built, executive summary, closeout)	72	$300/hr	$21,600
	Professional Services Total			**$180,400**

Rate note. The $300/hr rate reflects the market rate for ICS/OT security specialists with experience in water and wastewater SCADA environments. Published rate surveys (SANS ICS, Dragos) indicate a range of $200 to $350/hr for qualified OT assessors. Phase 2 is quoted as a blended fixed fee covering two senior assessors, travel, per diem, specialized assessment tooling, and post-assessment report production.

Hardware and Software

ITEM	SPECIFICATION	ESTIMATED COST
Industrial firewall	Fortinet FortiGate Rugged 60F (list $2,770) plus 1-year FortiGuard IPS/IDS subscription ($630/yr). Alternative: Cisco ISA 3000 (list $5,750 plus subscription).	$3,400
Managed industrial switch	Cisco IE-3300-8T2S-E, 8x GE copper + 2x GE SFP, Network Essentials license. Replaces unmanaged Stratix 2000.	$2,350
Secure jump host	Hardened small form factor workstation (Dell OptiPlex Micro or equivalent) with MFA token hardware (YubiKey 5 series, 3 units at $50 each).	$1,350
HMI OS license	Windows 10 IoT Enterprise LTSC 2021, single OEM license for HMI-01 rebuild.	$350

ITEM	SPECIFICATION	ESTIMATED COST
Syslog/ logging server	Dedicated small form factor PC (Dell OptiPlex Micro or equivalent) with 2 TB SSD for log storage. Software: Wazuh (open source, no license cost).	$1,400
SFP modules	2x 1000BASE-T SFP modules for Cisco IE-3300 uplinks.	$180
Cabling and installation	Cat6A shielded patch cables, cable management, DIN rail adapters for industrial switch mounting, patch panel.	$1,200
Server closet access control	Electronic keypad lock with audit trail (Kaba/dormakaba or equivalent).	$650
Spares and contingency	One spare SFP module, spare patch cables, configuration backup media (encrypted USB drives, 3 units).	$420
Hardware and Software Total		**$11,300**

Firewall note. Cost estimate uses the Fortinet FortiGate Rugged 60F. If the Cisco ISA 3000 is selected during Phase 3 design, the hardware total increases by approximately $3,000. Final hardware selection will be made during Phase 3 based on compatibility, feature requirements, and CRRWA procurement preferences.

Total Project Budget

CATEGORY	AMOUNT
Professional services	$180,400
Hardware and software	$11,300
Total project cost	**$191,700**

Grant Budget (SLCGP 60/40 Split)

CATEGORY	AMOUNT
Total project cost	$191,700
Federal share (60%)	$115,020
Non-federal match (40%)	$76,680

CRRWA will provide the 40% non-federal cost share from its capital improvement fund. Sentinel OT provides grant application support at no additional cost during the engagement, including narrative drafting, cost justification documentation, and coordination with the state administrative agency (SAA).

Optional: Rockwell TechConnect Support Contract

A Rockwell Automation TechConnect support contract provides direct access to Rockwell technical support for firmware compatibility verification, upgrade planning, and post-upgrade validation. TechConnect is not required to perform firmware upgrades, but is strongly recommended. Estimated annual cost for a small site: $9,000 to $12,000/year. This cost is not included in the project budget above because it is a direct contract between CRRWA and Rockwell Automation.

Grant Eligibility

This engagement falls within the eligible activities defined by the State and Local Cybersecurity Grant Program (SLCGP) under the Infrastructure Investment and Jobs Act of 2021. Eligible categories include:

- **Cybersecurity assessments** (Phases 1 and 2)
- **Implementation of security measures** (Phases 3, 4, and 5)
- **Cybersecurity planning** (Phase 6)
- **Workforce development** (Phase 5, Task 5.8, operator training)
- **Addressing imminent cybersecurity threats** (Phase 1, given CISA KEV status of CVE-2021-22681)

The Drinking Water State Revolving Fund (DWSRF) and the Water Infrastructure Finance and Innovation Act (WIFIA) program may also provide funding pathways for the infrastructure components of this engagement.

Assumptions and Exclusions

Assumptions

- CRRWA will provide physical access to the Cedar Ridge Water Treatment Plant for on-site work during Phases 2 through 5.
- CRRWA will coordinate maintenance windows for Phases 3, 4, and 5 with plant operations staff. Estimated total downtime across all phases: 20 to 30 hours, distributed across four to six maintenance windows over approximately 10 weeks.
- The existing plant integrator will be available to provide the last known-good controller program backup and to support firmware upgrade compatibility validation.
- Remote access to the Microhard BulletPlus gateway for Phase 1 compensating controls will be provided within 24 hours of contract execution.
- CRRWA will procure hardware (firewall, managed switch, jump host, syslog server, server closet lock) per the specifications in this document. Sentinel OT will provide procurement support and configuration, but CRRWA is the purchasing entity.
- HMI-01 (Dell OptiPlex 7070) will be rebuilt in place. If CRRWA prefers to procure a replacement workstation (estimated $1,500 to $2,000), the old hardware can serve as a cold spare.

Exclusions

- Active penetration testing or exploitation of any vulnerability.
- Hardware procurement (quoted separately, specifications provided above).
- Modifications to the SCADA/HMI application logic or controller program logic beyond firmware updates, security configuration, and application whitelisting policy.
- Physical security assessments beyond the server closet access control noted in Task 4.11.
- IT network assessments outside the OT/SCADA environment.
- OT network monitoring sensor deployment (passive DPI). This is recommended as a future capital investment and is referenced in the Comprehensive Vulnerability Assessment Report, but is not included in this scope due to the cost of commercial OT monitoring platforms (Nozomi, Claroty, or Dragos typically start at $25,000 to $50,000 for a single small-site sensor plus annual subscription).
- Legal or regulatory filing on behalf of CRRWA.
- Rockwell Automation TechConnect support contract (direct between CRRWA and Rockwell).

Acceptance Criteria

Each phase is considered complete when the corresponding deliverable has been submitted to CRRWA and accepted in writing. Acceptance is based on the following criteria:

1. All tasks listed for the phase have been completed or a documented exception has been agreed upon.
2. Before-and-after evidence demonstrates that each finding addressed by the phase has been remediated or mitigated.
3. Network segmentation verification testing (Phase 3) confirms that zone boundaries enforce intended access controls.
4. Documentation meets the standards referenced in Phase 6 (AWIA, IEC 62443, NIST SP 800-82).
5. CRRWA operations staff have been briefed on any changes affecting daily operations.
6. All deliverable documents have been reviewed by CRRWA's designated point of contact and any requested revisions have been incorporated.

Findings Addressed by Phase

FINDING	SEVERITY	PHASE
EXT-1: CVE-2021-22681 (Auth Bypass, KEV)	Critical	Phase 1 (compensating control), Phase 3 (VPN, firewall), Phase 4 (firmware upgrade)
EXT-2: CVE-2022-1161 (Stealth Logic Mod)	Critical	Phase 1 (compensating control), Phase 4 (firmware, change detection), Phase 5 (change management)
EXT-3: CVE-2019-10952 (Web Server RCE)	Critical	Phase 1 (compensating control), Phase 3 (firewall), Phase 4 (firmware upgrade)

FINDING	SEVERITY	PHASE
INT-1: No Network Segmentation	Critical	Phase 3 (firewall, managed switch, VLANs, zone-based rules)
INT-2: HMI End-of-Life OS, No Endpoint Protection	Critical	Phase 4 (OS rebuild, WDAC application whitelisting, patch management)
INT-3: Historian Default Database Credentials	Critical	Phase 4 (SA password, named accounts, access restriction)
INT-4: No PLC Backups or Change Management	Critical	Phase 2 (baseline established), Phase 4 (change detection), Phase 5 (change management procedure)
EXT-4: XetaWave Radio UI Exposed	High	Phase 1 (compensating control), Phase 3 (firewall)
EXT-6: Cleartext FTP/Telnet, Default Credentials	High	Phase 1 (services disabled, credentials rotated)
INT-5: USB Ports Enabled, No Media Controls	High	Phase 4 (USB mass storage disabled, Group Policy)
INT-6: Shared Operator Credentials	High	Phase 5 (individual accounts, RBAC, password policy, MFA)
INT-7: No OT Logging or Monitoring	High	Phase 5 (syslog server, log forwarding, alerting, 90-day retention)
EXT-5: Open DNS Resolver	Medium	Phase 1 (restricted to internal)

FINDING	SEVERITY	PHASE
INT-8: Radio Link Unencrypted	Medium	Phase 4 (AES-256 encryption on XetaWave link)
INT-9: Server Closet Unlocked	Medium	Phase 4 (electronic keypad lock)

Sample document. Cedar Ridge Regional Water Authority is a fictional operator used to illustrate the format and depth of a Sentinel OT project scope. No real utility, facility, or IP address is depicted. This document accompanies the sample Comprehensive Vulnerability Assessment Report (Report ID: pbcwud_cedar-ridge_sample_2026-05-12).