Formula 1

Content placeholder

Formula 2

Content placeholder

Detailed Explanation

The SCADA Cyber Incident Response Playbook serves as a field-deployable framework for organizations operating supervisory control and data acquisition systems—commonly found in critical infrastructure sectors including energy, water/wastewater, transportation, and manufacturing. Unlike general-purpose IT incident response plans, it explicitly addresses OT-specific challenges such as legacy protocols (e.g., Modbus, DNP3), air-gapped or segmented networks, deterministic timing requirements, and the high consequence of unplanned downtime or unsafe process states. The playbook structures response into four phases—Preparation, Detection & Analysis, Containment/Eradication/Recovery, and Post-Incident Activity—with integrated checklists, decision trees, and communication templates designed for cross-functional teams (e.g., control room operators, system integrators, cybersecurity analysts, and regulatory liaisons). Crucially, it incorporates CISA’s validated playbooks for common SCADA threats—including PLC memory corruption, HMI credential compromise, and malicious RTU firmware updates—and mandates integration with asset inventories, network diagrams, and baseline behavioral profiles to support rapid forensic triage without disrupting operational continuity.

Key Components

#	Component
1	Incident Classification Matrix (OT-Specific Severity Tiers)
2	SCADA-Specific Communication Protocols & Coordination Workflow

#	Component
3	Role-Based Response Checklists (e.g., Control Engineer, ICS SOC Analyst, Site Supervisor)

Applications

#	Application
1	Rapid containment of ransomware targeting HMI servers in water treatment facilities
2	Forensic isolation and recovery of compromised RTUs following a spear-phishing campaign
3	Regulatory reporting and evidence preservation aligned with CISA’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) requirements

Related Concepts

#	Concept
1	NIST SP 800-82 (Guide to Industrial Control Systems Security)
2	IEC 62443-3-3 (Security Risk Assessment and System Design)
3	MITRE ATT&CK for ICS

Tags

> SCADA, ICS Security, CISA, Incident Response, OT Cybersecurity