Metrics That Matter

1. Patch Management Compliance Rate

Aligned with CMMC Practice: SI.1.210
Aligned with CRI Playbook: Software Update Management Tool

Definition: Percentage of critical security patches and updates addressed within a specified timeframe (e.g., 30 days), either through applying patches or implementing compensating controls. For example, if a critical firmware update is released for programmable logic controllers (PLCs) in an industrial facility, this metric tracks the proportion of PLCs updated within the 30-day window – ensuring vulnerabilities are promptly mitigated in the OT environment.

Value Proposition: Maintaining high patch compliance demonstrates your organization's proactive stance on security, increasing customer trust and competitive advantage in securing contracts. In an ICS context, it also reduces the risk of unplanned downtime or safety incidents caused by unpatched system vulnerabilities.

Measurement: Compliance Rate (%) = [(Number of critical patches applied or addressed with compensating controls within policy timeframe) ÷ (Total critical patches issued)] × 100. (For instance, if 10 out of 10 released PLC patches are applied or addressed within the timeframe, the compliance rate is 100%.)

Requires: Accurate asset inventory and vendor notification tracking, as well as adherence to industry standards for OT patch management (e.g., IEC 62443-2-3 program requirements).

2. Security Awareness Training Completion Rate

Aligned with CMMC Practice: AT.2.056
Aligned with CRI Playbook: Password+, Phishing, Employee Awareness and Training (Training Resources)

Definition: Percentage of personnel (employees, contractors, managed security provider and other external supporting resources) who complete annual cybersecurity awareness training aligned with the tools used for their job tasks. For example, control system engineers and plant operators may receive specialized training on industrial cybersecurity (e.g., safe remote access practices for OT/ICS and PLC systems); this metric addresses that such OT-focused training is completed by the relevant personnel.

Value Proposition: Organizations with high training completion rates demonstrate resilience to cyber threats, building trust with partners and clients while reducing operational risks and potential costs from security incidents. In an OT environment, a well-trained workforce is better equipped to recognize and respond to cyber-physical threats – preventing social engineering or errors that could disrupt industrial processes or safety.

Measurement: Training Completion Rate (%) = (Number of employees completing training ÷ Total employees) × 100. (For example, if 95 out of 100 employees have completed required training, the rate is 95%.)

Requires: Clear understanding and integration of security responsibilities across various job roles (IT and OT personnel alike).

3. Incident Response Preparedness

Aligned with CMMC Practice: IR.2.093
Aligned with CRI Playbook: Incident Response Plan (IRP)

Definition: Number of successful incident response tests or tabletop exercises performed annually, incorporating realistic scenarios and identifying both internal capabilities and external partnerships necessary for effective response. For example, one tabletop exercise scenario involved a simulated cyberattack through an external vendor's remote diagnostics connection (a known ICS threat vector). In the simulation, adversaries altered a PLC's operation, triggering abnormal process readings and forcing operators to initiate the alarm acknowledgement workflow. The incident response team had to detect the intrusion, coordinate with the vendor to disable remote access, quickly acknowledge and investigate the alarms, and execute the incident response plan to contain the breach and restore safe operations. This kind of realistic scenario validates that both technical response procedures and communication with external partners (e.g. the vendor) are effective, addressing potential adversary tactics like alarm suppression.

Value Proposition: Regular and realistic incident response exercises position your organization as reliable and prepared, enhancing customer confidence by demonstrating rapid recovery capabilities and strategic partnerships. This is especially critical in industrial sectors where a quick, coordinated response can prevent safety incidents and minimize downtime. (Notably, NIST SP 800-82 recommends periodic testing of incident response plans to address that OT environments can be rapidly recovered from incidents.)

Measurement: Incident Response Exercises = Total number of realistic, successful exercises conducted per year (minimum recommended: 1). (Each completed exercise — such as the vendor remote access breach simulation above — counts toward this metric.) See Appendix A for a detailed example scenario demonstrating this metric in action.

Requires: Structured coordination among internal teams (IT, OT operations, management), collaboration with security service providers, knowledge of insurance requirements, and established mutual aid relationships with law enforcement and peer organizations.

4. Critical Function Backup and Restore

Aligned with CMMC Practice: RE.2.138
Aligned with CRI Playbook: Business Continuity Plan

Definition: Number of critical function data elements successfully backed up and restored within a defined period (e.g., quarterly or annually). For instance, an industrial plant might back up the configuration files and logic programs for its critical PLCs and HMI/SCADA servers and then test restoring them every quarter. If out of 20 critical systems, 18 can be successfully restored from backup during a drill, the metric would be 90%, indicating most critical functions can be recovered as planned. Regular backup and restoration testing like this aligns with OT security guidance to back up system state and configurations at regular intervals to support rapid recovery.

Value Proposition: Consistent and verified backups and restoration capabilities address resilience, minimize operational downtime, and reinforce customer confidence in your organization's ability to maintain critical operations during adverse events. This is particularly important in ICS environments (energy, manufacturing, utilities) where even brief downtime or data loss can significantly impact safety and production continuity.

Measurement: Critical Data Backup and Restore Success (%) = (Number of critical function data elements successfully backed up and restored ÷ Total critical function data elements identified) × 100. (For example, if 18 of 20 identified critical data elements are recovered successfully in testing, the rate is 90%.)

Requires: Capability to identify critical functions and their essential data, backup creation mechanisms, secure custodial processes for backups, and reliable methods for selective data restoration across various device types (e.g., PLCs, engineering workstations, SCADA servers).

5. Active Event Notification Coverage for Critical Functions

Aligned with CMMC Practice: IR.2.094
Aligned with CRI Playbook: Incident Response Plan

Definition: The proportion of critical systems and processes that are actively monitored with real-time event notifications. This metric assesses how many of the organization’s critical functions (e.g. key ICS controllers or manufacturing cells) are tied into alarms or alerts that immediately notify security personnel of anomalies or failures. It attempts to address that all high-consequence operations have sensors or logging in place to catch suspicious activities (unauthorized access, parameter changes, etc.) and trigger instant alerts.

Value Proposition: Comprehensive alert coverage demonstrates a proactive security posture by ensuring potential incidents are caught in their earliest stages. Customers and partners gain confidence that the organization can assure critical functions through vigilant monitoring, reducing the risk of undetected breaches or process manipulation. In an audit or contract bid, a high coverage rate showcases robust situational awareness and commitment to operational resilience.

Measurement: Notification Coverage (%) = (Number of critical function systems with active and valuable event notifications configured ÷ Total number of identified critical function systems) × 100. For example, if 18 of 20 critical production controllers are feeding into a Security Incident and Event Management (SIEM) valuable alerts or ICS alarm system, the coverage is 90%. Higher percentages mean more complete visibility.

Requires: An up-to-date inventory of all critical assets and processes, and deployment of appropriate monitoring tools (e.g. OT-specific IDS/IPS sensors, system loggers, or PLC alarm systems). Clear alert criteria and roles must be defined so that when a sensor flags an event, notifications reach the right responders with actionable and precisely accurate authority without delay. It also requires tuning to avoid alert fatigue, and regular testing of alerts (as part of incident response drills) to addressing critical events (equipment deviations, unauthorized access attempts, etc.) reliably trigger the alarms and prompt swift action.

Appendix A: Manufacturing Incident Scenario Aligning with Metrics that Matter

Under development.