Critical Vulnerabilities in IACS

Consequence: Tangible
- Lost Production
- Dissatisfied Customers
- Declining Share Price

Consequence: Intangible
- Website Unavailable
- No Email
Threat and Vulnerability Management

- Vulnerability Aggregator: View vulnerabilities from multiple sources in one central location
- Vulnerability Reporting: Provide consistent remediation updates to key stakeholders
- Vulnerability Mitigation Tracking: Track vulnerability mitigations as they happen
- Network Map/Canvas: View flows from vulnerable hosts for context and awareness
Sensor Management

Vulnerability Aggregator
- Monitor vulnerabilities to ensure appropriate signatures/rules exist

Network Map/Canvas
- Identify overlaps or potentially malicious connections

Vulnerability Reporting
- Periodically report vulnerable sensors for prompt mitigation
High-Security Remediation

- **Vulnerability Aggregator**
  - Monitor for critical vulnerabilities

- **Vulnerability Mitigation Tracking**
  - Track high-security remediation efforts

- **Vulnerability Reporting**
  - Metrics (i.e., number of critical vulnerabilities per month)
Incident Response

- Vulnerability Aggregator: Situational awareness
- Vulnerability Reporting: Provide consistent remediation updates to key stakeholders
- Vulnerability Mitigation Tracking: Track incident eradication/mitigation
- Network Map/Canvas: Situational awareness Outline containment Monitor recovery
Threat Intelligence

- Network Map/Canvas: Monitor for new or suspicious flows
- Vulnerability Mitigation Tracking: Situational awareness (threat perspective)
- Threat Dashboard: Current state of affairs – internal perspective
Security Monitoring

Vulnerability Aggregator
- Monitor for new, unassigned vulnerabilities

Threat Dashboard
- Monitor activities
- Risk timeline monitor

Vulnerability Reporting
- Metrics for operations management

Network Map/Canvas
- Monitor for new or suspicious flows
Stay tuned for more!