CYBERSECURITY SERVICES

Cybersecurity Incident Response Preparedness Services

Organization assessments and incident response exercises

INCIDENT RESPONSE PREPARATION

Operation technology (OT) systems are the ultimate target for adversaries who intend to create destabilizing events. That's why it's critical to have a plan that clearly dictates how to prepare for, detect, and prevent attacks as well as how to respond in the event of a compromise.

SEL employs a team of industry-certified cybersecurity specialists who provide immediate incident preparedness and response services. Our specialists adhere to several incident response frameworks, including those developed by NIST and the SANS Institute.

STAGES OF PREPARATION

Creating and maintaining an incident response plan is crucial. It ensures there is a clearly defined response team with designated roles and instructions, exposes potential security gaps before a crisis occurs, provides documentation of accountability, and more.

Below are key areas all critical infrastructure organizations should evaluate.

Build Your Team

- Define the team and each member's role in an attack scenario.
- Understand ownership of each task.
- Assign a scribe for each team—the person who will document all decisions, activities, and actions during an incident.

Plan Your Response and Strategy

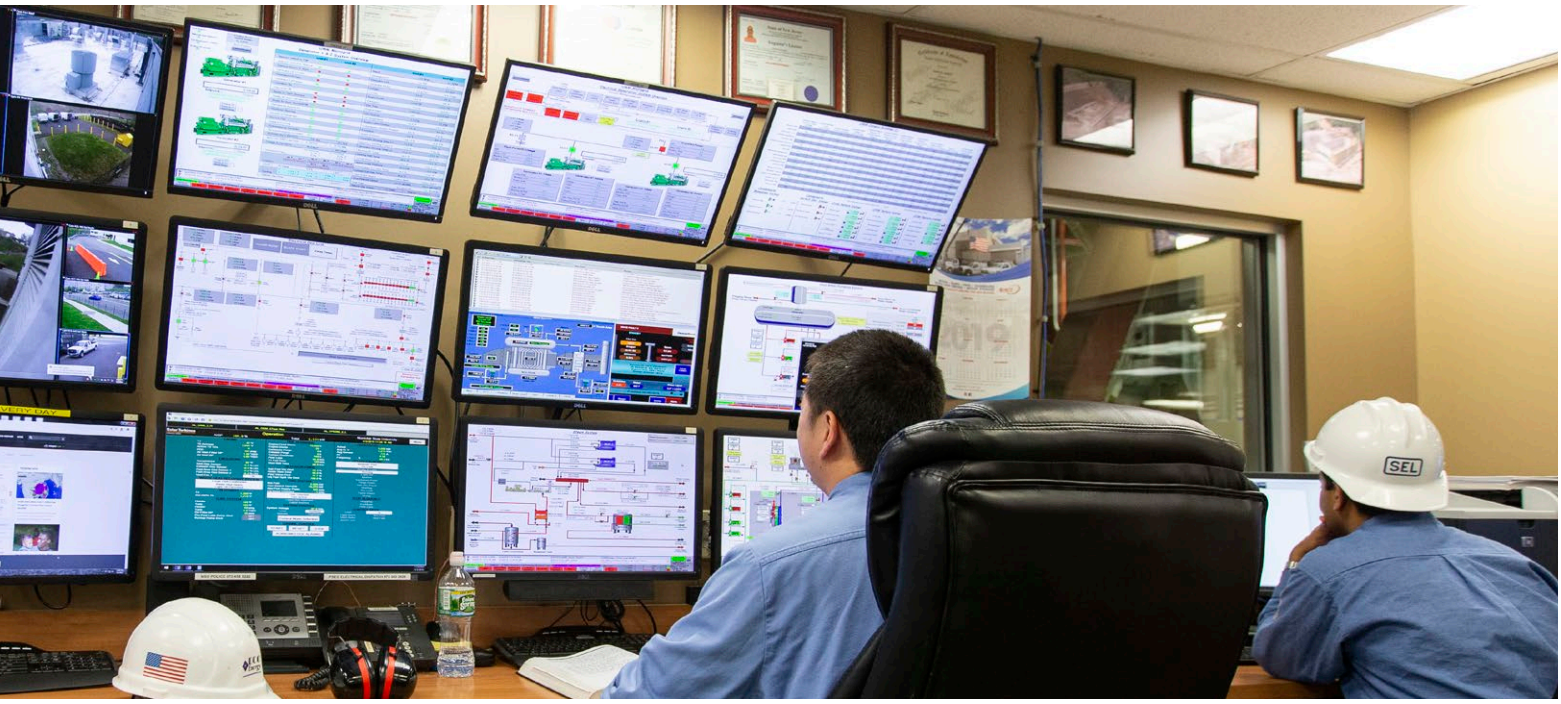
- Define incident handling and response based on scope of attack.
- Identify who has the authority to unplug from the internet.
- Prepare alternate, secure methods of communication in case regular methods become compromised or unavailable.
- Ensure team members have appropriate permissions.

Document Everything

- Documentation should answer: Who, What, When, Where, Why, and How.
- Documentation should be reviewed and approved regularly.

Implement Ongoing Training

- Conduct regular table-top exercises.
- Test recovery strategies and backups.



SEL CYBERSECURITY SERVICES

Our team provides solutions that improve cybersecurity, streamline asset management, and prepare your organization to respond to a cyber incident.

Initial Evaluation

SEL cyber experts provide onsite evaluation specific to the customer framework.

- Provide an overview of processes and recommendations (1–2 days).
- Perform in-depth analysis of highest priority targets (3–5 days).
- Review/create security policy framework.

Disaster Recovery Readiness Validation

SEL provides evaluation, recommendation, and confirmation of physical tools and backups to use during an incident.

- Confirmation and location of spare equipment, backups, etc.
- Validation of recovery backup procedures

Documentation and Communication Plan Creation

Creating and maintaining a plan specific to critical infrastructure environments provides efficiency during incident response and when restoring operations.

- Identify gaps in the plan.
- Review roles and assignees.

Vulnerability Assessments

Many attacks take advantage of existing vulnerabilities that could be patched. Identifying and addressing vulnerabilities now could prevent or mitigate later incidents.

- Test alerts triggered on network reconnaissance scans.
- Analyze vulnerability scan reports.
- Perform firewall configuration reviews.
- Review logs (e.g., SCADA, firewall, and Microsoft Active Directory).
- Ensure logs are available.
- Detect indicators of compromised systems.
- Analyze communications traffic.

Ongoing Training

Cyber awareness training keeps resources up to date, identifies gaps in readiness, and increases security knowledge for preventing incidents.

- Credential rotation
- Alerts on failed login attempts
- External email attachment awareness
- Manual operation readiness
- Table-top exercise

For more information, please contact SEL Infrastructure Defense at secure@selinc.com.

SEL CYBERSECURITY CERTIFICATIONS

Our team of security professionals holds several cybersecurity certifications from the Global Information Assurance Certification (GIAC) organization as well as the International Information System Security Certification Consortium (ISC)². These are globally recognized organizations known for leadership in cybersecurity training, certifications, and knowledge.

SEL cyber experts maintain the following certifications:

- GIAC Response and Industrial Defense (GRID)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Certified Incident Handler (GCIH)
- SANS Security Awareness Professional (SSAP)
- Certified Information Systems Security Professional (CISSP)

SEL SCHWEITZER ENGINEERING LABORATORIES

+1.509.332.1890 | info@selinc.com | selinc.com