Manage Your Risk Through Cyber Resiliency

Resiliency, Situational Awareness & Preparedness for Critical Infrastructure

Cyber Vulnerability Assessment

Problem	Cause	Solution	Benefit
• Constant flow of newly discovered vulnerabilities • Configuration changes or evolutions introduce new weaknesses	• Malicious parties attempting to gain unapproved access • Software coding errors • Regulatory requirements • Gaps in coordination and awareness	• Vulnerability scans to identify potential vulnerabilities and threats • System patching • OT Testing and device hardening	• Identifies patching priority based on criticality • Identification of known vulnerabilities • Enhanced security across the network

Scope of supply: The activities below are conducted and documented:

- Based on either NIST, NERC CIP, IEC 62443 -3-3 & -2-2, ISO 27001, other
- Identification of Electronic Security Parameter (ESP) / Secure Zones & Conduits
- Identification of all ports and services
- Identification of security weaknesses in the target systems
- Entire network and port scans including internal routers, firewalls and switches
- Review of the remote access paths and configuration.
- Ranking of each detected vulnerability to Critical, High, Medium, and Low impact category.
- Assessments of access management, account configurations
- Identification of vulnerabilities or potential threats
- Detailed Cyber Vulnerability Assessment (CVA) documentation of results and assessed systems

Hardening Services

Problem	Cause	Solution	Benefit
• Devices and endpoints are often configured using manufacture default configurations which tend to be insecure • Unhardened endpoints are easy attack vectors • Need to align with best practices and customer security policy • Antivirus is not part of the standard build	• Common misconfigurations or not optimal security configurations with defaults • IT department is focused on operations vs. security	• Configure settings on endpoints and other systems using “secure hardening standards” (configuring system firewall, AV, MAC address filtering, application whitelisting, etc.)	• Common misconfigurations are unable to be exploited • Attack surface reduction (limiting available and open services and ports running) • Overall security within the environment is substantially increased • Helps meet various cyber standards (e.g. ISO, etc.)….

Examples of hardening measures:

- Enable password complexity requirements (where applicable)
- Enable port monitoring
- Enable MAC filtering on utilized physical ports
- Enable scripted hardening tasks
- Verify logon banner exists
- Disable non-critical OS user accounts

- Setup of **System and Network Logging** (optional)
- **Hardened firewall rules** and the access control lists (optional)
- Activation of the **Application Whitelisting** feature (optional)
- Evaluation of **secure backup and recovery** systems and procedures (optional)
- **Security Patch and Anti-Malware updates** application (optional)
- Application of **system security policies and procedures** (optional)
- **Disabling unutilized ports** and services (Physical and Virtual) (optional)
- **Encryption** of required communication ports (optional)
- **Password enforcement** on all systems where technically feasible (optional)

Your Critical Infrastructure Cybersecurity Contacts -

Matt Morris
Managing Director
1898 & Co. Critical Infrastructure Cybersecurity
matt.morris@1898andCo.com
770.557.6205 (cell)

Jason Vigh
Section Manager
1898 & Co. Critical Infrastructure Cybersecurity
jason.vigh@1898andCo.com
220.666.9080 (cell)

1898 & CO SM

PART OF BURNS McDONNELL