SMC™

OUR KNOWLEDGE IS YOUR POWER

VULNERABILITY DISCOVERY SERVICE

We'll help you face the increasingly common and costly cybersecurity threats in industrial infrastructure.

ASK YOURSELF:

- Do you understand what assets are connected to your critical applications?
- Do you know what your most significant cybersecurity threats are and have you addressed them?
- Are you vulnerable to third-party applications hosted on your network?
- Does your company have a disaster recovery plan after a cyberattack occurs?

WE HAVE THE EXPERIENCE TO HELP

The first step to securing critical protection and coverage against cyberattacks is a Vulnerability Discovery Service. This service can be delivered by SMC's Cybersecurity experts.

A Vulnerability Discovery Service is designed for customer ease of use. This service will provide visibility into your industrial network assets with no additional hardware, no configuration, and no risk of disruption. The results will provide information to **assess and prioritize** your OT network security risks through asset inventory, vulnerability details, and a risk assessment report.

BENEFITS

- Proactively discover your **vulnerabilities, misconfigurations, and unsecured network connections**
- **Reduce cyber risk** in your industrial infrastructure
- **Identification and classification** of assets across your ICS network
- **Actionable plan for remediation** of your hidden threats

Rockwell Automation

For more information, please visit smcelectric.com

CHALLENGES YOU FACE

SKILLS GAP

- Lack of qualified personnel
- Achieving productivity goals
- Lack of staffing to expand operations

INFLEXIBILITY

- Low adoption of risk management processes
- Shadow/Stealth IT
- Lack of tools to manage infrastructure
- Too much data, lack of actionable information

VULNERABILITY

- Security is an afterthought and standards are evolving
- Aging industrial control systems and protocols
- Lack of proper policies and procedures

IT/OT CONVERGENCE

- Lack of comprehensive asset inventory
- Integrate customer demand supply chain and industrial processes
- Integration of new technologies

WHAT TO EXPECT:

1. **Vulnerability Discovery Service preparation**
   a. The process begins with a pre-site kickoff call with an SMC cybersecurity expert.
2. **On-site data collection process**
   a. The SMC Specialist will run a lightweight executable on your plant network to perform the data collection.
3. **Remote data review**
   a. The captured data is returned to SMC for processing and analyzed through the Claroty Threat Detection Software.
4. **Study delivery**
   a. The Risk Assessment Report is created from analyzed data providing you with an overall health check that you can use to understand all the assets on the plant network along with any Common Vulnerabilities and Exposures (CVEs) that may affect those assets.

   i. The report will provide the following:
   - Full Asset Identification of the Environment
   - Visibility into IT/OT/IOT assets
   - Vulnerability information for assets (e.g. CVEs)
   - Vulnerability information for assets (e.g. CVEs)
   - Risk identified for assets (e.g. misconfigurations)

For more information, please visit smcelectric.com