Check Point
SOFTWARE TECHNOLOGIES LTD

ONE STEP AHEAD

CRITICAL INFRASTRUCTURE

ICS and SCADA Security Solutions for Ultimate Cyber Defense

Industrial Control Systems (ICS) have emerged over the years as being under protected and highly vulnerable to breaches and hacks. These systems are comprised of aging legacy hardware, special communication protocols (group of protocols also known as SCADA protocols) and older software and Operating Systems' (OS) that are typically not updated or patched frequently. Infrequent updates and patches of ICS systems create a long window of exposure (may take several years to patch), leaving these system open to known attacks.

When Securing Your SCADA/ICS Environment, Consider the Following:

Secure Both OT and IT Environments

Network Segmentation is arguably the most important step to secure Industrial Control Systems. IT (used for administrative purposes) infrastructure and OT, Operational Technology, used to manage industrial operations, each have specific security requirements and should be segregated completely. IT systems such as email and Windows file servers are regularly patched, updated, and rebooted. OT systems are required to run 24/7 and cannot be rebooted for patch or code upgrades. These systems are often legacy systems that weren't originally designed with security controls and run unsecure protocols that can be hacked.

Secure Multi SCADA Vendor Environments

Critical infrastructure that spans across industries such as energy, oil and gas, mining, manufacturing and defense continue to be major targets. These environments use proprietary, mission critical, and sensitive ICS/SCADA networks and devices, bringing a host of new challenges to traditional IT security management solutions. Industrial sites also require remote access by vendors to provide timely support to their systems, introducing additional complexities in maintaining the security of the Operational Technology (OT) environment. The best way to manage a multi-vendor environment is with a solution that is vendor agnostic.

OT Network Visibility

Large networks consisting of hundreds or even thousands of devices are a complex task. Remote central management of security policies and effective situational visibility are necessary to optimally secure the infrastructure. Security is comprised of many layers and it's important to have a single view of all incidents in one place. Unifying security solutions can allow use of expertise already present in the environment and provide a full-spectrum view of the security posture across ICS security devices and the networks.

Secure Against a Wide Variety of Attack Vectors

Be sure to implement specific protection to segment and isolate connectivity to and between facilities and production areas, following the ISA-99 zones and conduits model. Ensure the security of the SCADA network devices perimeter and interface points. It's also important that all endpoints and portable equipment used for management is secured with port control protection and freefrom malware.

The Importance of Virtual Patching

Patching is crucial to a company's security posture because it protects against vulnerabilities. Without it, attackers will continue to exploit these vulnerabilities. However, the standard patch management process can be overwhelming because of cost and complexity. Many of these concerns for SCADA system PLC's, RTU's, and HMI's can be addressed by virtual patching, which can offer immediate protection for any system or application in use.

Secure the Control Systems Workstations

Threats such as malware, viruses, worms and bots change constantly and are becoming a serious problem for ICS environments. End-users are often the targets of phishing emails that may contain links to websites infected with malware. To prevent employees from being targeted, security teams need to defend end-user systems against zero-day threats, bot communications with Command and Control servers. Anti-Malware and Application Control further help to prevent malware with a single scan and make sure only approved programs are in use.

Comply to Security Regulations

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) presents clear security guidelines for network security managers, such as Electronic Security Perimeters (CIP-005) and System Security Requirements (CIP-007) among others. In addition, Configuration Change Management (CIP-010) requires firms "to prevent and detect unauthorized changes to systems by specifying configuration change management requirements." Be able to validate policy and configuration changes in real-time, security managers can identify issues before policies are implemented.

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

US Headquarters | 59 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com/ics