Operating tehnology Services to Ensure CyberSecurity

Attack is the secret of defense/defense is the planning of an attack

SUN TZU

www.mi-line.com

Introduction:

The merging of OT and IT networks leverages various pre-existing approaches that can impact effective security measures to protect critical points in the process environment.
The following challenges also arise:

- Overview of network elements
- Connections between individual elements
- Network access administration and individual elements
- Security issues with legacy protocols
- Software update

95% of attacks happen due to human error. In the first half of 2020 alone, the growth of cyber attacks was 35% and rising…

The purpose of the services is to ensure the smooth running of critical processes in ICS / SCADA industrial control systems, by ensuring secure and efficient data acquisition, analysis, transmission, visibility, and management, as well as monitoring with multiple detection tools.

With traditional risk assessment procedures, it is impossible to:

- Make regular security inspections
- Perform multiple inspections instead of annual ones, which are not enough
- Constantly ensure the visibility of risks
- Record process changes

www.mi-line.com

With our solution, we offer ICS / SCADA end-to-end solutions, on one integrated detection device.

By setting up an anomaly detection system and with data collected.

We build:

- OT inventory of all components in the network and monitoring services
- MSSP (Management Solution Provider) Adding an OT environment to the SOC (Security Operations Center) to provide remote security services
- Preparation of risk assessment - one-time / periodically
- Based on IEC 62443 standard perform consulting and report preparation compliance

IEC 62443:

- is a series of standards that enable a systematic and practical approach to the protection of industrial automation and control systems (IACS).
- The standard covers every phase and aspect of industrial ongoing operations
- The system is divided into several categories that describe the technical process levels of industrial cyber security and their improvements.

www.mi-line.com

CIARA

Platform for Automated Risk Analysis and Risk Assessment of OT Networks Based on IEC 62443

Functions:

- Inventory of assets (retrieval via iSID gateway)
- Vulnerability detection and evaluation
- Virtual penetration test (MITER-ICS simulations)
- User and system behavior analysis
- Historical data of previous scoring
- Change detection

Purpose:

- Improving the security of the OT environment
- Planning security upgrades to reduce risks
- Network compliance with IEC 62443
- Automatic and data-driven risk analysis

CIARA, using a fully automated data-driven risk assesment algorithm, to generate reports by zones and conduits, the result is a risk assessment report divided into groups, and proposed solutions to improve safety posture.

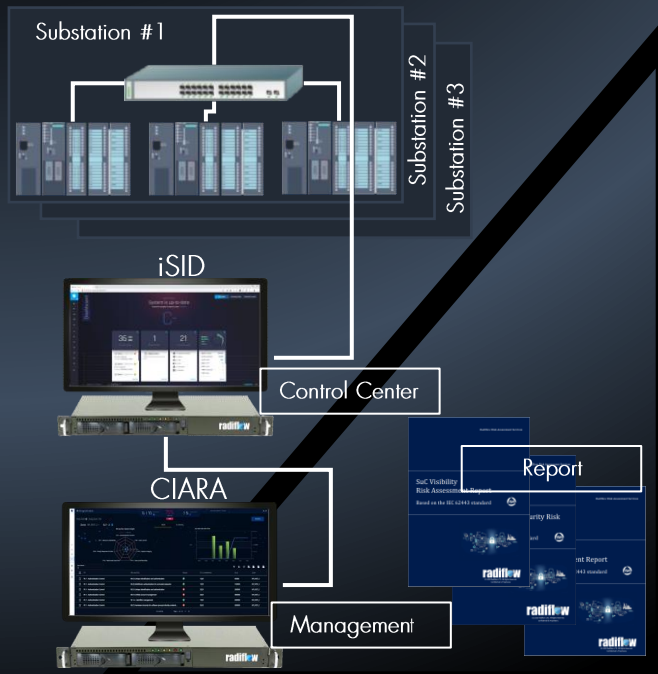
The risk assessment can be carried out monthly or periodically, without the need to rent the manufacturer`s equipment.

#1Network learning
Data acquisition via digital image

#2 Definition and initial risk assessment

#3 Security Requirements Analysis

#4 Risk reduction and introduction of security controls



www.mi-line.com

M

With the Radiflow solution we provide:

- Security check
- Services for a complete security solution
- An ecosystem with OT tools
- Compliance with IEC 624332

TECHNICAL EXPERTISE

Cybersecurity	OT
BeyondTrust, cisco, Cyber Israel, DELL EMC	BELDEN, GE, MEKOROT, RUGGEDCOM, SIEMENS

Technology partners

SIEM & CYBERSECURITY ANALYTICS	IDENTITY & ACCESS MANAGEMENT	NETWORK SECURITY	OT SECURITY & ASSET MANAGEMENT
ArcSight, Radar, RSA, splunk>	CYBERARK, RSA SecurID	paloalto, FORTINET, Gigamon, WATERFALL	Itsec Guardian, COPADATA, SIGA, ST Engineering

Awards and recognitions

FIRESTARTER Award for Radiflow's OT MSSP Partner Program	Global Customer Value Leader in Smart Buildings	SC 2020 awards Shortlisted for Best SCADA Security Solution	NCCoE NIST SP1800-7 Technology Partner
Gartner Representative Vendor in OT Security Market Guide	Cyber Security Excellence Award 2020 for iSID	CISS Blue Team in iTRUST CISS SWaT Challenge	CSA SINGAPORE Innovation Grant for Dynamic ICS Risk Scoring

www.mi-line.com