iSEC
Cybersecurity Assessment Service

WHY RADIFLOW?

Radiflow is a recognized leader in industrial cybersecurity, offering dedicated solutions designed to meet the unique requirements of industrial infrastructures:

EXPERIENCE

Over 10 years' experience discovering and analyzing advanced persistent threats and targeted attacks, including attacks on critical and industrial infrastructure

UNIQUE METHODOLOGY

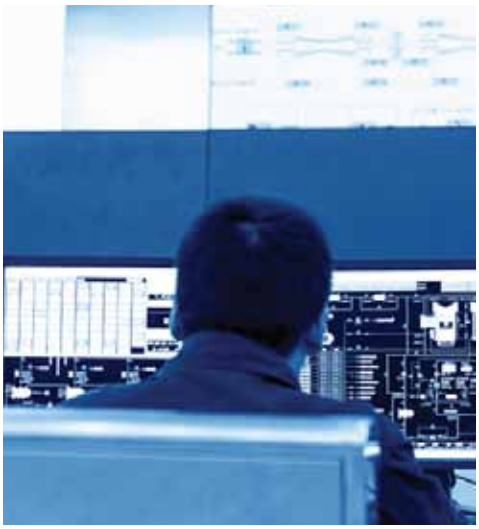
Radiflow offers a unique scan methodology to detect industrial attack vectors that can cause downtime.

EXPERTISE

Dedicated team of industrial cybersecurity experts who understand the colliding worlds of automation and security.

END-TO-END PORTFOLIO

Radiflow offers a holistic portfolio of services and technologies, including SCADA gateways, routers and firewalls, industrial network IDS and many more.



- Performed by Radiflow's dedicated team of ICS/SCADA Security experts
- Non-intrusive network traffic recording, with no interruption to ongoing operations
- Complete visualization of your OT network topology and all connected assets
- Detection of all known SCADA-specific CVEs (common vulnerabilities and exposures, logical changes in PLCs & open remote SSH sessions
- Structured, standards-based process, e.g. ISA/IEC-62443 (Formerly ISA-99)
- Detailed threat and vulnerability report and mitigation roadmap

How Secure is Your ICS Network?

Critical Infrastructure Protection (CIP) has in recent years become a national priority in terms of funding, regulation and general awareness, following a series of cyberattacks on critical infrastructure installations worldwide.

Today, companies in a wide range of industries realize the need for a cyber-protection plan that's economically viable, simple to operate and able to adapt ever-evolving attackers and methods.

Devising an ICS protection plan can be a daunting task. There's no one-size-fits-all solution, and in many cases operators have incomplete visibility into their networks.

An effective ICS/SCADA protection plan requires comprehensive identification and mapping of all devices, connections, ports and other network assets. Only then will you be able to detect vulnerabilities and exposures and assess them in terms of severity and potential impact if compromised.

The next phase is to generate an implementable mitigation and contingency plan, based entirely on facts and expert analysis, to ensure the effectiveness and efficiency of the project.

radiflow
Secure Your Assets

The iSEC Security Assessment Process

Radiflow's security assessment is a structured, standards-based (e.g. ISA/IEC-62443) process executed by experienced professionals.

1. Pre-Assessment

a. **Preparation and coordination**: pre-assessment review of self-reported network topology, SCADA equipment vendors, and other relevant information.

b. **On-site visit and meeting with key stakeholders**: review network structure and components, delineate known problems, and define a test plan and workflow. During this time our team will record samples of your network traffic for topology mapping and analysis.

2. Analysis

An operational activity baseline is created based on the analyzed network traffic, to detect vulnerabilities and possible attack vectors. This phase typically lasts 2-4 weeks, during which the Radiflow team will:

a. Identify and map all network devices, operating systems, applications and connections, down to the deep IT & OT protocols and components

b. Analyze the current security measures to determine whether attackers can extract sensitive information from network traffic, and verify network segmentation between controllers, servers and workstations

c. Evaluate the resiliency of the data-link layer security, to identify weaknesses that may expose your LAN

d. Analyze all management interfaces to PLCs, managed switches and routers

e. Verify separation between engineering workstations and servers

f. Examine the security of communication ports

g. Verify accessibility of the ICS via wireless and remote access technologies

h. Review the ICS' interaction with external systems

i. Examine the Internet connectivity of all ICS components

j. Check the use of undeclared protocols

k. Inspect security cabinets and telecom equipment

l. Confirm the exclusive use industrial-grade equipment: routers, switches, firewalls, converters, media, etc.

m. Discover network and device vulnerabilities, as well as possible exposures

n. Discovery of access control weaknesses, such as confidential information stored on poorly-protected file servers and inadequate or missing firewall protection

o. Analyze password usage to find information that is may be derived from a password (NTLM, MD5 hash, etc.). This will be used to generate a passive password list and a dictionary of common passwords

p. Test attackers' ability to burrow into the network and gain unauthorized access to critical ICS components

q. Review asset compliance with security standards, e.g. ISO/IEC 27001 and ISA-99

3. Report and Secure

An extensive report is submitted to the operator, and actions are taken to eliminate found threats and vulnerabilities.

The report includes an executive summary dashboard-style presentation of our conclusions and recommendations meant for senior management, as well as a comprehensive technical report that includes:

a. A clearly-presented description and drill-down of all data collected

b. A full list of found vulnerabilities ranked in order of severity and likelihood of use, along with a description of the consequences of a hacker exploiting each

c. A threat model detailing the practical impact on your organization in the event that hackers were to exploit the most critical vulnerabilities found

d. A programmatic mitigation plan with recommendations for addressing vulnerabilities and bridging security gaps. This includes suggested changes to equipment configurations and settings, use of detection/protection mechanisms, installation of necessary software updates on devices (PLCs, RTUs, HMIs, etc) and changes to policies, procedures, and processes.

Why are industrial environments uniquely vulnerable?

Modern industrial control systems (ICS) are vulnerable to cyberattacks for a number of unique reasons.

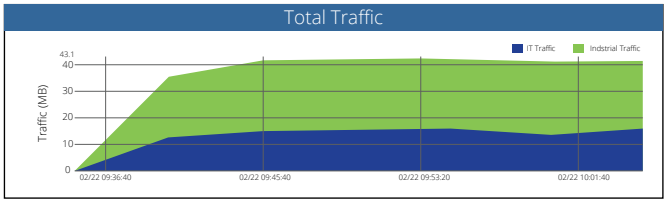
First, they often combine networked technologies with legacy systems, and it is not unusual for organizations to leave critical vulnerabilities un-patched rather than interrupting a process—something cyber-criminals are keenly aware of.

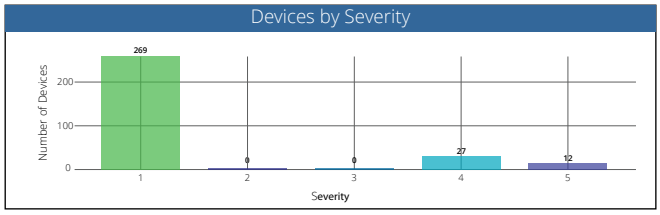
Second, inadequate controls over access rights, as well as the use of default settings, usage rules and policies—all in the name of operational continuity—add to the overall risk.

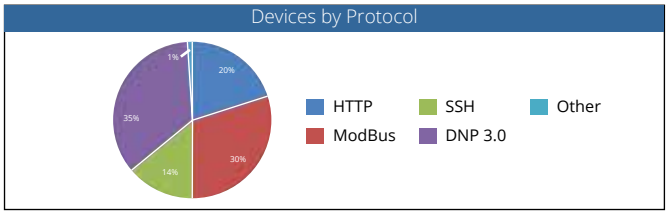
Some vulnerabilities unique to industrial-specific software, such as hard-coded passwords and insecure protocols are holdovers from a past where ICSs were not connected to the network and the concept of 'software vulnerabilities' barely existed.

Top Known Threats Detected

Event	Event Time	Port	Severity	Src Device Name	Src IP	Dst Device Name	Dst IP	Number of Events
Restart Communications Option	2/22/2017 10:13	Modbus	5	[NAME]	123.456.0.1	[NAME]	123.456.0.1	1
Report Server Information	2/22/2017 10:13	Modbus	5	[NAME]	234.567.0.2	[NAME]	234.567.0.2	2
Read Device Information	2/22/2017 10:13	Modbus	5	[NAME]	345.678.0.3	[NAME]	345.678.0.3	3







Some of the tables and charts included in the iSEC Assessment Report submitted to ICS operators

radiflow
Secure Your Assets

Performed by Top Professionals

We offer our security assessment service based on our vast experience, renowned expertise and product portfolio.

The assessment procedure is performed by Radiflow's top security experts. It employs the most up-to-date methodologies and is based on the company's portfolio of dedicated ICS/SCADA products.

Upon completion of the assessment, the customer is presented with a detailed report that includes all the information collected and logged, the findings resulting from the analysis, and a comprehensive cybersecurity plan of the organization. You are free to choose how and with whom to execute the plan.

Call for immediate action

To better understand Radiflow's security assessment and initiate the assessment process, please contact us at:

US and Canada:

Tel: +1 (302) 547-6839

sales_NA@radiflow.com

EMEA:

Tel: +972 (77) 501-2702

sales@radiflow.com

UK:

Tel: +44 (0) 800 2461963

sales_UK@radiflow.com

or visit us at www.radiflow.com

Radiflow is a leading provider of cybersecurity solutions for critical infrastructure networks (i.e. SCADA), such as power utilities, oil & gas, water and others.

Radiflow's security toolset validates the behavior of both M2M applications and H2M (Human to Machine) sessions in distributed operational networks. Radiflow's security solutions are available both as in-line gateways for remote sites and as a non-intrusive IDS (Intrusion Detection System) that can be deployed per-site or centrally.

Radiflow's solutions are sold either integrated within a global automation vendor's end-to-end solution, or by local channel partners, as a standalone security solution.

radiflow
Secure Your Assets