Radiflow

CIARA Data-Driven OT Risk Assessment and Management

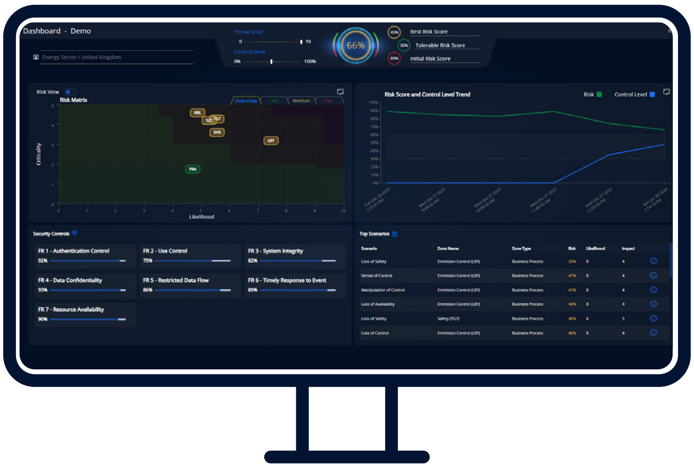
Prompt, automatic, accurate, and compliant risk assessments for CNI and ICS Operators and their MSSPs, Auditors, and Consultants

In the transforming Cyber Physical System (CPS) environment and escalating threat landscape, CNI and industrial operators struggle to produce accurate risk assessments that tie back to key assets and processes that they can justify and act upon in a cost-effective and timely manner.

To manage today's cyber risk, a proactive, continuous, automated, and data-driven Risk Assessment and Management platform is essential.

HIGHLIGHTS

- Frequent, automated risk assessments chart cyber progress at much lower cost and far more accuracy than traditional manual methods
- Measures the gap between current security controls and compliance with standards and industry best practices
- Delivers a comprehensive roadmap – per site and overall – prioritized by each mitigation control's contribution to risk reduction
- Optimizes cyber spend for maximum ROI


Dashboard - Demo
Energy Sector / United Kingdom
Threat level
0
10
Control level
0%
100%
66%
45%
Best Risk Score
30%
Tolerable Risk Score
89%
Initial Risk Score
Risk View
Risk Matrix
Overview
Low
Medium
High
Criticality
Likelihood
KRL
SZ1
TG7
SHS
L8Y
FRA
Risk Score and Control Level Trend
Risk
Control Level
100%
0%
Tue Dec 26 2023 7:27:01 PM
Wed Dec 27 2023 9:44:42 AM
Wed Dec 27 2023 10:08:58 AM
Wed Dec 27 2023 11:48:56 AM
Wed Dec 27 2023 12:39:26 PM
Sun Jan 28 2024 7:14:18 PM

Security Controls

FR 1 - Authentication Control 92%

FR 2 - Use Control 75%

FR 3 - System Integrity 82%

FR 4 - Data Confidentiality 93%

FR 5 - Restricted Data Flow 86%

FR 6 - Timely Response to Event 89%

FR 7 - Resource Availability 90%

Top Scenarios

Scenario	Zone Name	Zone Type	Risk	Likelihood	Impact
Loss of Safety	Emmision Control (L8Y)	Business Process	50%	8	4
Denial of Control	Emmision Control (L8Y)	Business Process	47%	8	4
Manipulation of Control	Emmision Control (L8Y)	Business Process	47%	8	4
Loss of Availability	Emmision Control (L8Y)	Business Process	46%	8	4
Loss of Safety	Safety (TG7)	Business Process	46%	6	5
Loss of Control	Emmision Control (L8Y)	Business Process	46%	8	4

EFFECTIVE RISK MANAGEMENT FOR TODAY'S CPS ENVIRONMENT

CIARA, Radiflow's Risk Assessment and Management platform for OT organizations, automatically discovers and learns key risk indicators and accurately evaluates per-site and overall security posture and risk. It determines how to direct the OT security budget to maximize the effectiveness of threat-mitigation controls based on cybersecurity regulations, standards, and frameworks like NIS2, IEC 62443, and NIST CSF.

AUTOMATED RISK ASSESSMENTS

The complexity and scale of modern industrial networks make evaluations by traditional risk assessment procedures problematic. The cumbersome spreadsheet and eyeball methods no longer work nor are they acceptable to the cyber authorities.

Data-driven CIARA slashes assessment and audit time, as well as required resources. It automatically ingests relevant data from the network and operations, and assesses risk accurately, rapidly, and unobtrusively. CISOs, MSSPs, auditors, and consultants can run complete and safe risk assessments as frequently as desired to measure security posture and track cyber progress.

FREQUENT RISK EVALUATIONS PER SITE AND OVERALL

Highly scalable CIARA's calculations, outputs, and displays are applied cross-enterprise as well as to each industrial site individually. Security personnel can quickly view overall risk scores and drill down to each region, site, and network for finer granularity. Flexible and customizable dashboards and reports simplify understanding and presentation to stakeholders.

OPTIMIZED SECURITY ROADMAP AND CYBER SPEND

CIARA's risk-mitigation planner helps security stakeholders prioritize controls to meet risk goals taking into consideration budgetary constraints. By following CIARA's mitigation roadmap, operators are able to divert expenditure from mitigations which marginally reduce risk – given actual threats to networks, assets, and operations – to those that produce the greatest cybersecurity ROI. When a new attack tactic or vulnerability is published, CIARA can check the potential impact on the network and direct the security team to effective defense tactics.

GUIDING THE COMPLIANCE JOURNEY AND CLOSING THE GAPS

CIARA's value increases over time. As it delivers historical and long-term perspectives, CIARA reveals compliance improvements, deteriorations, and trends.

The outcomes of CIARA's risk assessments include key indicators for risk, threat, and control levels. CIARA produces a wide variety of rich and granular OT security reports as well as a comprehensive hardening plan (ISA/IEC 62443-compliant), prioritized by each mitigation control's contribution to achieving risk management goals.

NIS2 DIRECTIVE

Going into effect in October 2024, Article 21 of the NIS2 Directive requires that essential and important entities undertake "policies and procedures to assess the effectiveness of cybersecurity risk-management measures." CIARA delivers these capabilities, boosting compliance with the new, stringent directive.

UNDERSTANDING THE NETWORK

CIARA provides network visibility tables and reports, displaying all network segments, zones, conduits, assets, asset properties, protocols, links, and vulnerabilities. As the environment changes, data-driven CIARA automatically updates its knowledgebase.

Gartner®

CIARA is included in Gartner's Hype Cycle for Cyber Risk Management 2023.

Radiflow

NON-INTRUSIVE BREACH AND ATTACK SIMULATIONS

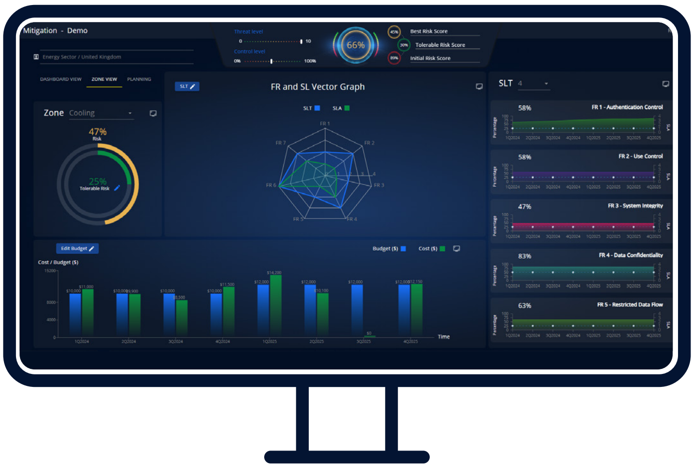
CIARA employs a Machine Learning-driven, virtual breach-and-attack simulation (VBAS) for assessing risk based on the latest threat intelligence and vulnerabilities. Using multitudes of current data points for network, asset, locale, industry, adversary capabilities, and attack tactics, CIARA builds a digital twin and simulates a wide array of security controls against relevant known threats, factored against a host of common OT risk scenarios such as loss of availability, loss of control, and loss of data. It calculates the likelihood of attacks and the effectiveness of corresponding risk-mitigation measures – both installed and proposed – per asset and zone.

Analysts can control attack vectors such as source or destination and they can create adversary and loss scenarios. CIARA determines and displays top insights, attack routes, techniques used, and exploitable CVEs.

CIARA VBAS answers questions like:

- How can a specific Advanced Persistent Threat (APT) take control over this engineering station?
- What is the likely kill chain of an adversary who would attempt to impair safety in the cooling zone?
- What are the potential threats and vectors from LockBit ransomware?
- What is the likelihood of losing control of a PLC?

Security analysts can propose and analyze specific mitigations and their contribution to reducing risk.



DATA SOURCES AND INTEGRATIONS

CIARA continuously ingests and enriches data from a broad range of sources through integrations with a variety of platforms, systems, and solutions:

- Radiflow iSID Threat Detection platform
- Other intrusion detection/prevention systems
- Asset management systems
- Vulnerability management systems
- OT management systems
- Popular firewalls
- Popular SIEMs
- Zero Trust solutions
- IAM solutions
- Common Vulnerabilities and Exposures (CVE) database
- User and system behavior analysis
- Historical data on earlier incident scoring
- Adversary threat intelligence including MITRE ATT&CK™

CIARA FOR MSSPS, AUDITORS, AND CONSULTANTS

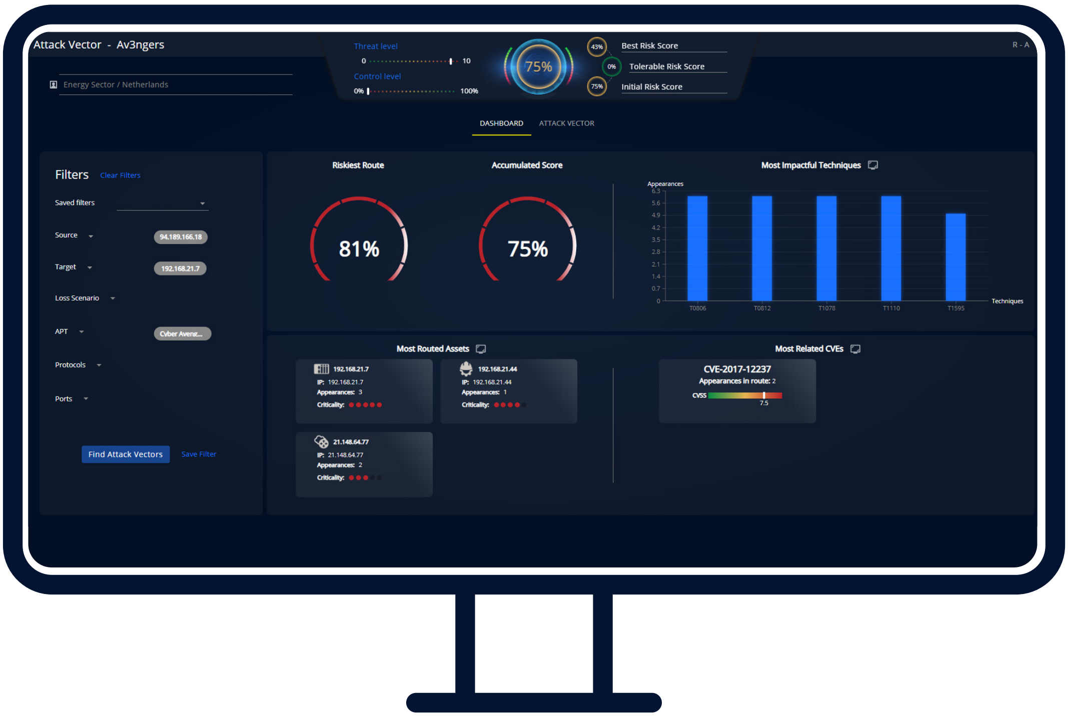
By deploying CIARA, Managed Security Service Providers (OT-MSSPs) can offer their industrial and CNI customers effective ROI-driven risk assessment and management services with less time and effort while boosting delivered value.

For auditors, CIARA's quick installation, speed, and short time-to-value expedite the audit process, including mock and compliance audits.

For security consultants, CIARA creates automated compliance and security reports for presentation to senior management, technical management, auditors, and regulators, delivering information-rich, quantified risk scores by asset, site, and overall. CIARA also makes valuable recommendations for security improvements.

GETTING STARTED WITH CIARA

Organizations prepared to undertake their OT Risk Management program can implement the CIARA solution, integrate it with Radiflow's iSID Threat Detection solution and/or their own data sources (or have Radiflow do the integration), and execute accurate CIARA risk assessments as frequently as desired.



Saved filters

Source: 94.189.166.18

Target: 192.168.21.7

Loss Scenario

APT: Cyber Aveng...

Protocols

Ports

192.168.21.7
IP: 192.168.21.7
Appearances: 3
Criticality: ●●●●●

192.168.21.44
IP: 192.168.21.44
Appearances: 1
Criticality: ●●●●

21.148.64.77
IP: 21.148.64.77
Appearances: 2
Criticality: ●●●

CVE-2017-12237
Appearances in route: 2
CVSS 7.5

Radiflow

www.radiflow.com

info@radiflow.com

Radiflow is a leading, global provider of OT Security and Risk Management solutions and services for critical infrastructure and industrial automation. We enable operators to continuously safeguard their operations while they manage risk, optimize their security budget, and comply with standards, regulations, and industry best practices. Locally or centrally deployed, Radiflow solutions integrate with leading technology and partner platforms. Now part of the Sabanci Group, Radiflow protects over 8,000 sites worldwide.