CIARA

Cyber Industrial Automated Risk Analysis

Radiflow CIARA is the first-of-its-kind ROI-driven risk assessment & management platform for industrial organizations.

Serving as a stakeholder decision-support tool, CIARA empowers CISOs and owners of complex ICS environments to increase the effectiveness of their risk-mitigation measures throughout the entire system lifecycle, while significantly reducing cybersecurity expenditure.

CIARA employs a fully-automated, data-driven risk assessment algorithm, which calculates the actual monetary/HSE impact of each risk-mitigation measure, using thousands of data points for network, asset, locale, industry, adversary capabilities and attack tactics.

The result is a comprehensive mitigation roadmap (fully ISA/IEC 62443-compliant), prioritized by each mitigation control's contribution to overall risk reduction, thus maximizing the impact of cybersecurity expenditure.

radiflow

ROI-BASED RISK MANAGEMENT

CIARA enables ROI-based optimization of cybersecurity expenditure to ensure the effectiveness of threat-mitigation measures in relation to the adversaries and attack tactics relevant to the specific industrial network.

CIARA's unique risk assessment algorithm combines the likelihood of attacks on networked assets with their quantitative real-world impact (e.g. monetary loss or non-compliance with governing regulations), and prioritizes mitigation measures based on their contribution to reducing overall risk.

By following CIARA's plain-language mitigation roadmap, users are able to divert expenditure from mitigations which marginally reduce risk (given the actual threats the network faces) to those that produce the most cybersecurity ROI.

Top Scenarios

Scenario	BP ID	BP Name	Risk	Likelihood	Impact	
Denial of Control	OKB	HIGH_VOLTAGE_Backup	85%	8.6	5.0	i
Loss of Availability	OKB	HIGH_VOLTAGE_Backup	85%	8.6	5.0	i
Loss of Control	OKB	HIGH_VOLTAGE_Backup	85%	8.6	5.0	i
Loss of Safety	KDB	STATION_A	86%	8.6	5.0	i
Loss of Safety	31M	STATION_B	86%	8.6	5.0	i
Loss of Safety	LTD	DIST_2	86%	8.6	5.0	i
Loss of Safety	OKB	HIGH_VOLTAGE_Backup	86%	8.6	5.0	i
Manipulation of Control	OKB	HIGH_VOLTAGE_Backup	86%	8.6	5.0	i
Loss of Safety	OKB	HIGH_VOLTAGE	74%	8.6	5.0	i

Top attack scenarios for different business processes, detailing the likelihood, impact and risk factor for each

AUTOMATED, DATA-DRIVEN ASSESSMENT

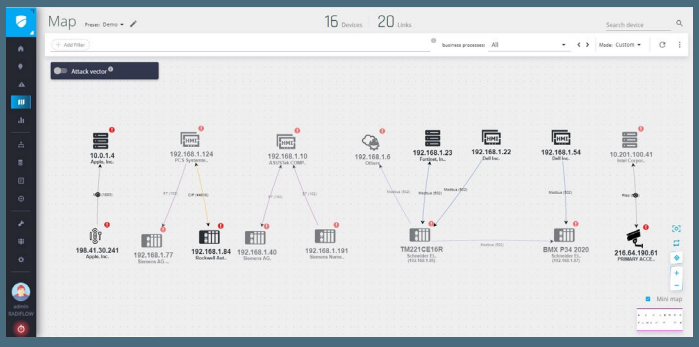
Understanding OT network risk is a key factor in devising an effective cybersecurity plan. However, the complexity and the scale of modern ICS networks (due to the digital transformation of industry 4.0) render risk evaluation by traditional risk assessment procedures practically impossible. You simply can no longer "eyeball" risk.

Moreover, ad-hoc or annual risk reviews are no longer sufficient. Adequate protection requires continuous risk monitoring that instantly accounts for each and every change on the network, throughout the OT cybersecurity life-cycle.

CIARA simulates hundreds of commonly-used security controls against relevant known threats, factored against common OT risk scenarios (loss of availability, loss of control, damage to property, etc). This is done using indicators from a variety of sources to model network vulnerabilities, defences, possible attackers and attack methods:

- Inventory mapping (provided by Radiflow iSID*)
- Vulnerability mapping (CVSS/CVEs)
- Virtual penetration testing (based on MITRE-ICS simulations & Radiflow Lab research)
- User and system behaviour analysis
- Historical data on previous incident scoring
- Adversary threat intelligence (including MITRE ATT&CK™)
- Change management detection

* Optional network data acquisition from flat file or PCAP file



CIARA's analysis uses a "digital image" of the OT network, including all assets & asset property, protocols & vulnerabilities, generated by Radiflow iSID

THE CIARA RISK MANAGEMENT PROCESS

Compliant with the ISA/IEC 62443 standard, CIARA helps customers that are new to OT Cybersecurity to achieve compliance and optimize their cybersecurity expenditure. CIARA's risk assessment & mitigation planning process utilizes ZCRs (zone & conduit requirements) as specified in the standard:

STEP 1 (ZCR #1): LEARNING THE NETWORK

Network information is obtained from a digital image (model) of the network, produced by Radiflow iSID.

Deliverable: full network visibility report displaying all assets, protocols, and links.

STEP 2 (ZCR #2-4): NETWORK DEFINITION & INITIAL RISK ANALYSIS

Zones (operational units) and Conduits (between zones) are defined and each is assigned a monetary impact or HSE value.

Industry & geo-location characteristics are used to assess the relevance of adversaries (using the MITRE ATT&CK database). Attack scenarios are simulated.

Deliverable: Zone and SL-T table (CIARA will out-of-the-box add IEC-62443 SL-Ts to zones)

STEP 3 (ZCR #5): ANALYSIS OF EACH ZONE'S FOUNDATIONAL & SECURITY REQUIREMENTS

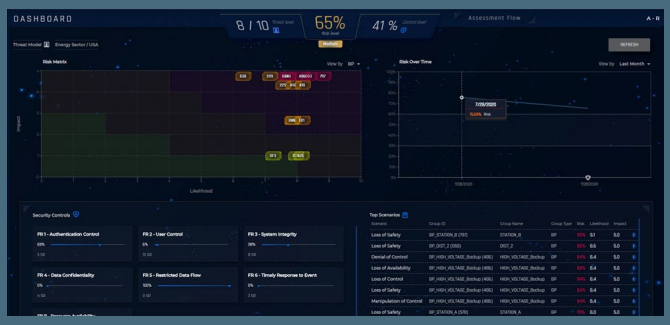
CIARA compares between each zone's current and required security level, and presents the user with the controls (mitigation measures) needed to achieve each zone's target (SL-T). Controls are prioritized by their contribution to reducing overall network risk. Expert input is used as needed.

Deliverable: Detailed Risk Report, including all threats, vulnerabilities, zone impact, unmitigated & target risk levels, existing countermeasures, likelihood of impact, residual vs. tolerable risk, and additional cybersecurity countermeasures.

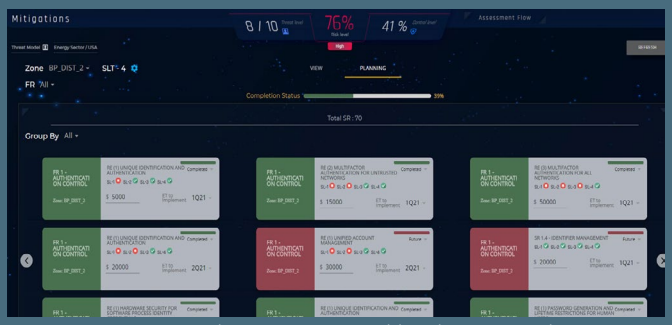
STEP 4 (ZCR #6-7): FINALIZING MITIGATION PLAN AND APPLYING SECURITY CONTROLS

Upon implementation of each prescribed Control measure, CIARA will re-calculate the network's overall risk score as well as the security position of each zone.

Deliverable: ongoing documentation of the cybersecurity requirements, assumptions and constraints needed to achieve the SL-T, as well as ownership and accountability for implementing controls.



The CIARA dashboard: detected Zones are displayed in a color-coded risk level array



Mitigation Controls are prioritized by their contribution to reduction of overall network risk

Gap-comparison between each zone's achieved (SL-A) and target (SL-T) security levels ("spider" graph, top left); controls checklist with dynamic risk scoring (bottom)

Region & industry information is used to assess the relevance of adversaries and attack tactics

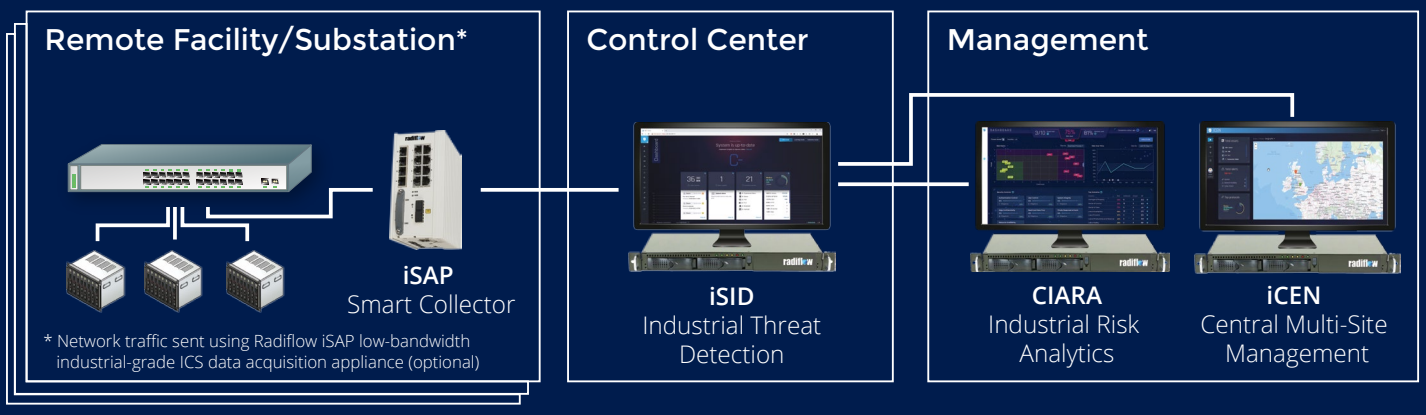
RADIFLOW CIARA FOR OT-MSSP SOCs

In recent years, managed security services providers (MSSPs) have become a viable option for small-to-medium size OT organisations seeking enterprise-level security without setting up a full-fledged network security operation.

With CIARA, OT-MSSPs are now able to offer their ICS-based users risk assessment and management services (periodic or ongoing monitoring), in tandem with Radiflow's award-winning iSID Industrial Threat Detection Platform. MSSP users will benefit from overall lower cybersecurity expenditure thanks to CIARA's ROI-driven mitigation roadmap.

PART OF THE RADIFLOW SOLUTION SUITE

CIARA is part of Radiflow's innovative solution suite for industrial organizations. Designed for industrial organizations of all sizes, CIARA is an integral part of Radiflow's multi-tier OT detection & prevention toolset, which includes the award-winning iSID industrial threat detection platform, the iSAP low-bandwidth smart collector for distributed networks, and the iCEN central multi-site management tool for corporate or OT-MSSP SOCs.



ABOUT RADIFLOW

Radiflow develops trusted Industrial Cybersecurity Solutions for Critical Business Operations. Our portfolio of game-changing solutions for ISC/SCADA networks empowers users to maintain visibility and control of their OT networks while increasing overall security expenditure ROI. Our intelligent Threat Detection and Analysis Platform for industrial cybersecurity minimizes potential business interruptions and loss within your OT environment.

Radiflow's team consists of professionals from diverse backgrounds, from cyber-experts from elite military units and automation experts from global cybersecurity vendors.

Founded in 2009, Radiflow's solutions are successfully deployed by major industrial enterprises and utilities protecting more than 4,000 critical facilities worldwide, and endorsed by Tier-1 customers & external labs. More at www.radiflow.com.

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) 800 246-1963
sales_UK@radiflow.com

France:
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

DACH:
Tel: +49 (160) 109 75 65
sales_DACH@radiflow.com

www.radiflow.com | info@radiflow.com