Radiflow

CIARA

Cyber Industrial Automated Risk Analysis

Radiflow CIARA is the first-of-its-kind data-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 optimizing cybersecurity expenditure.

CIARA employs a fully-automated, data-driven Breach & Attack Simulation (OT-BAS)engine, which calculates the success likelihood of different attacker techniques and effectiveness of risk-mitigation measures, 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 cybersecurity ROI.

Data Driven Risk Management

CIARA enables data-driven optimization of OT-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 a breach & attack simulation engine, for simulating thousands of breach scenarios against proposed and existing security measures. The result is a prioritized mitigation plan based on each proposed mitigation measure's contribution to reducing overall risk.

By following CIARA's plain-language mitigation roadmap, users are able to effectively plan their multi-year OT-security expenditure to maximize their cybersecurity posture and control level over attack groups that are most relevant to their region and sector, and achieve the most cybersecurity ROI.

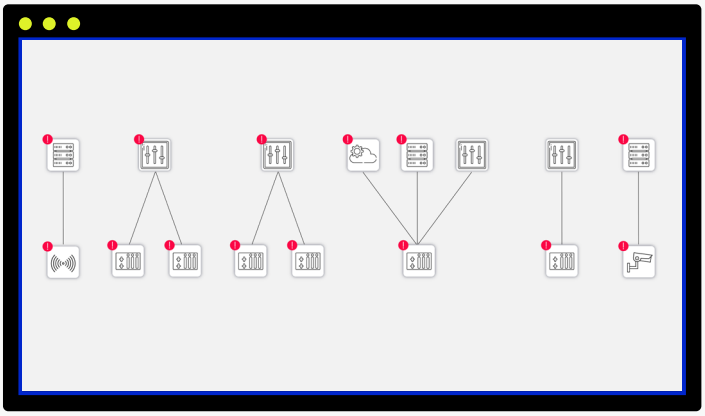
Top attack scenarios for different business processes, detailing the likelihood, impact and risk factor for each

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 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:

- **OT Network** inventory mapping including all assets & asset property, protocols & vulnerabilities*
- Vulnerability mapping (CVSS/CVEs)
- Virtual penetration testing (based on MITRE-ICS simulations & Radiflow Labs research)
- User and system behavior analysis
- Historical data on previous incident scoring
- Adversary threat intelligence (including MITRE ATT&CK TM)
- Change management detection



** OT network information may source from Radiflow iSID, 3rd party IDS or offline data collection*

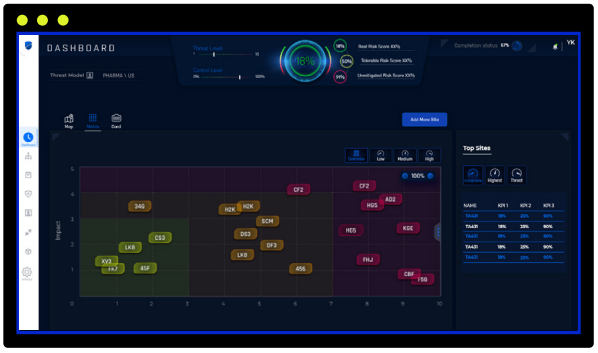
The Ciara Risk Management Process

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:

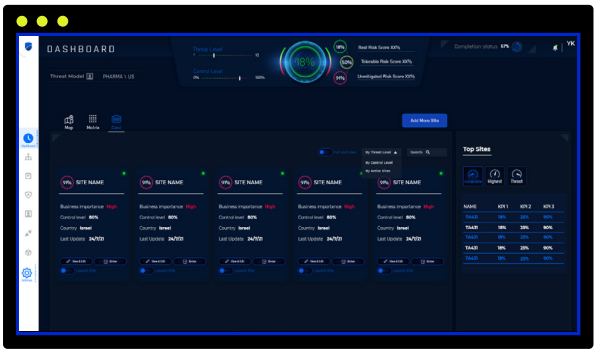
Step 1 (ZCR #1): Learning The Network

Network information is obtained from a digital image (model) of the network, produced by Radiflow iSID, 3rd party IDS systems or offline collection.

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



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



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

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.

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

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

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.

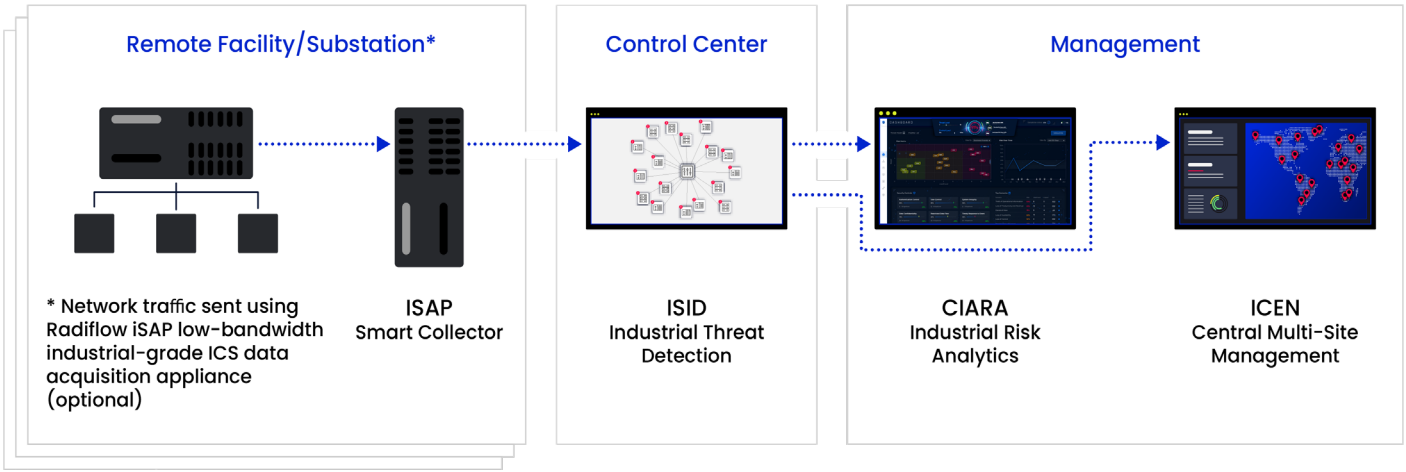
CIARA for OT-MSSP SOCs

In recent years, managed security services providers (MSSPs) have become a viable option for small-to-medium size OT organizations 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 unique OT network security and long-term risk management solutions for critical infrastructure and other ICS-based operations. The company works directly with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 6,000 sites around the globe.

Radiflow | For more info: **radiflow.com**