Radiflow ST Engineering

FEATURE DATASHEET

Ensure CCOP (Singapore) Compliance with Radiflow CIARA

Radiflow CIARA provides an automated, CCOP-compliant risk assessment platform for managing CII cybersecurity risks

General

In July 2022, Cyber Security Agency (CSA) of Singapore published the Cybersecurity Code of Practice version 2 (CCoP v2) to further strengthen the cybersecurity posture for the Critical Information Infrastructures.

Radiflow's CIARA risk assessment and management platform is now able to cross reference Singapore CCOP v2 to enable Singapore entities to manage their CII cybersecurity risk via an automated platform, to ensure CCOP compliance and optimize the ROI on OT security.

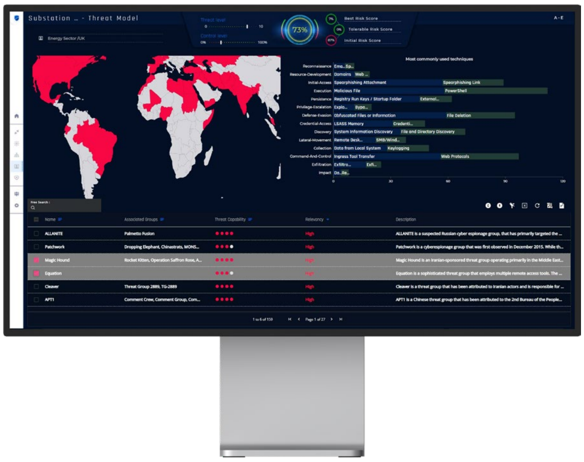
About Radiflow CIARA

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 ICS CISOs and owners to optimize their OT- security expenditure and ensure the effectiveness of threat-mitigation controls.

CIARA employs a threat intelligence-driven breach & attack simulation (OT-BAS) engine for assessing risk. Radiflow's OT-BAS algorithm calculates the per-zone likelihood of attacks and the effectiveness of corresponding risk-mitigation measures (installed and proposed), and accounts for the impact of attacks on different business processes. This is done using thousands of data points for network, asset, locale, industry, adversary capabilities and attack tactics.

The outcomes of CIARA's breach and attack simulations include key indicators for risk, threat and control levels; a variety of OT- security reports; and a comprehensive hardening plan, prioritized by each mitigation control's contribution to achieving the user's risk management goals.



Name	Associated Groups	Threat Capability	Relevancy	Description
ALLANITE	Palmetto Fusion	●●●●	High	ALLANITE is a suspected Russian cyber espionage group, that has primarily targeted the ...
Patchwork	Dropping Elephant, Chinastrats, MONS...	●●●○	High	Patchwork is a cyberespionage group that was first observed in December 2015. While th...
Magic Hound	Rocket Kitten, Operation Saffron Rose, A...	●●●●	High	Magic Hound is an Iranian-sponsored threat group operating primarily in the Middle East...
Equation		●●●○	High	Equation is a sophisticated threat group that employs multiple remote access tools. The ...
Cleaver	Threat Group 2889, TG-2889	●●●●	High	Cleaver is a threat group that has been attributed to Iranian actors and is responsible for ...
APT1	Comment Crew, Comment Group, Com...	●●●●	High	APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People...

1 to 6 of 159 Page 1 of 27

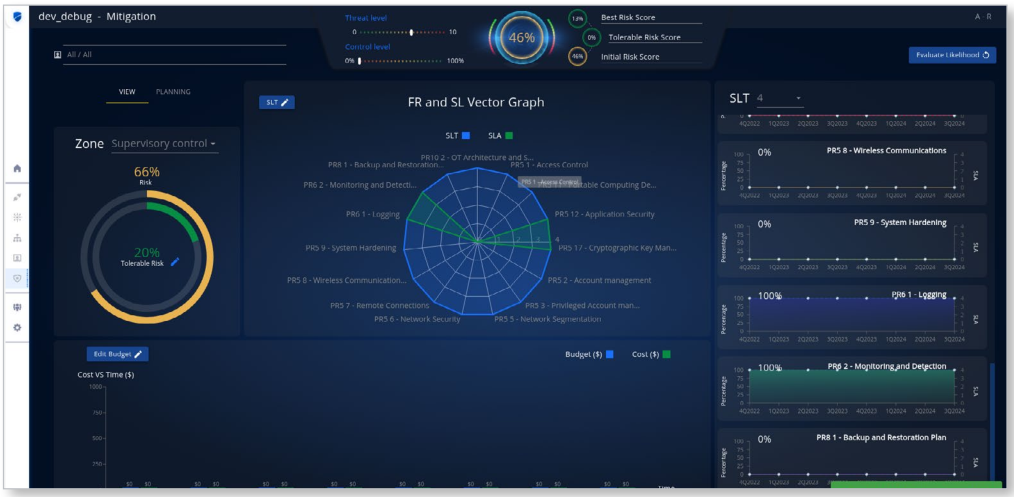
CIARA accounts for the sector and geo-location of the assessed OT network to prioritize and de-prioritize threats and corresponding mitigation measures

The CIARA Risk Assessment Platform for CCOP Compliance

- Identification of CII assets in the network (CCOP Chapter 4) to create an inventory connectivity map
- Assessment of mitigation controls (CCOP Chapter 5) for effectiveness in mitigating threat and reducing risk
- CIARA APT (Advanced Persistent Threat) uses the MITRE ATT&CK threat intelligence database. APTs are sorted according to relevance to Singapore's cyber-threat landscape and are evaluated, using virtual breach attack simulations (BAS) for likelihood of attack.
- Vulnerabilities derived from CVE databases are automatically indexed to the SuC and network exposure values are calculated
- Radiflow's OT IDS continuously monitors the network to detect attack and breach indications, with full-detail alerts sent to SIEMs/SOCs including event meta-data for actuary and risk calculations

Some Key Examples of CCOP mitigations assessed by CIARA:

- Account management
- Network Segmentation
- Remote Connection
- Wireless Communication
- System hardening
- Malware Protection
- Software upgrade and update
- Application Security
- Monitoring and Detection
- Data flow monitoring



CIARA's CCOP dashboard clearly presents the SuC's standing vis-à-vis the foundational requirements (FRs) stated in the CCOP standard, and generates a custom roadmap for optimizing OT security and ensuring compliance, based on the network's unique threat/risk landscape, mitigations installed and unique characteristics and vulnerabilities.

ABOUT RADIFLOW

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates 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 7000 sites around the globe.

ABOUT ST ENGINEERING

ST Engineering is a global technology, defence and engineering group with offices across Asia, Europe, the Middle East and the U.S., serving customers in more than 100 countries. The Group uses technology and innovation to solve real-world problems and improve lives through its diverse portfolio of businesses across the aerospace, smart city, defence and public security segments. An industry leader in cybersecurity with over two decades of experience, we deliver a holistic suite of trusted cybersecurity solutions to empower cyber resilience for government and ministries, critical infrastructures, and commercial enterprises.

Radiflow www.radiflow.com | info@radiflow.com ST Engineering www.stengg.com/cybersecurity | cybersecurity@stengg.com