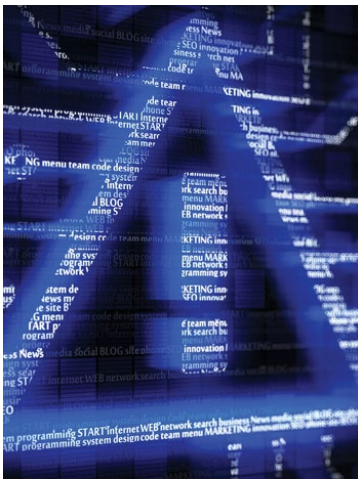
Product Datasheet

iRISK

Industrial Risk Analytics



HIGHLIGHTS

- Assessment of the actual business-related, as well as the health, environment and safety (HSE)-related impact of an industrial network's overall cyber-risk
- Significantly increase ROI with reduced overall cyber-risk as well as highly-effective, data-driven risk mitigation and asset management
- Contextual assessment of threat likelihood, based on analysis of historical data as well is IT & OT CVSS reports
- Automatically-generated risk analytics reports, based on up-to-date OT TI
- Support for IEC 62443 reporting

WHAT'S THE ACTUAL IMPACT OF CYBER-RISK ON YOUR NETWORK?

Each and every asset, protocol, port or other network element in an industrial network introduces an inherent amount of risk.

The amount of risk reflects the vulnerability of the asset to known threats and the criticality of the business process the asset belongs to, and is available in the form of a CVE (Common Vulnerabilities and Exposures) document.

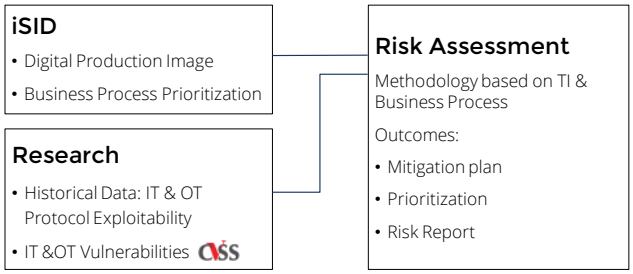
For operators seeking to further optimize their risk mitigation expenditure, Radiflow's iRISK Industrial Risk Analytics solution provides the actual business-related impact of the introduced risk, as well as its health, environment and safety (HSE) effects. Offered as a cloud service, the iRISK analytics process can be done either continually or on an ad-hoc basis, without the need for on-site permanent deployment.

Applying a unique quantitative (data-driven) approach enhanced by human expertise, iRISK weights the network's digital production (asset, protocols, etc.) image and business process prioritization from Radiflow's iSID, based on the likelihood of a risk materializing, on historical IT & OT protocol attack data (used as benchmarks for similar networks), and on IT & OT vulnerability data (CVSS).

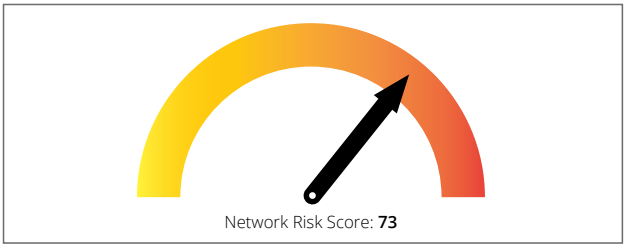
The weighted data is used to run network-wide attack simulations and inter-asset attack vectors. The ultimate result is a comprehensive real-world assessment report, as well as risk prioritization and recommendations for mitigation.

Cybersecurity Risk Matrix		Occurrence Likelihood Level			
		Low	Medium	High	Critical
Business Process Criticality (Impact)	Critical	1			1
	High		1	2	
	Medium		2		
	Low	3		1	

The actual impact of a cyber-risk accounts the criticality of the business process it's associated to (as defined in iSID) and the likelihood of an attack.



iRISK combines network and business process information from iSID with research data to provide an accurate, real-world risk assessment



iRISK provides an accurate risk score based on the real-world impact of an asset's vulnerabilities, factoring in the likelihood of attack.

radiflow

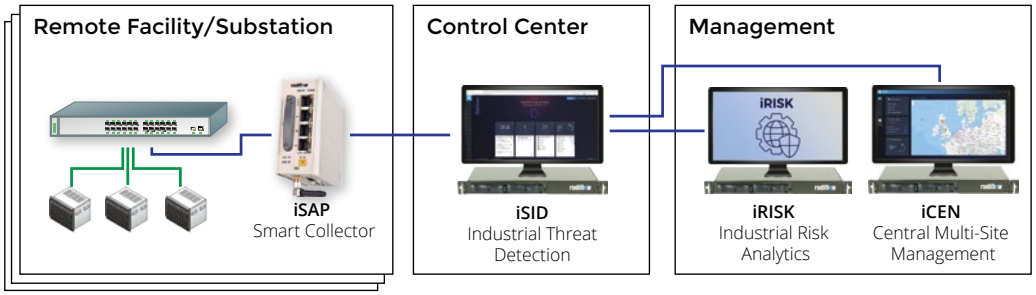
RISK VISIBILITY AND RECOMMENDATIONS

iRISK's automatically generates a full risk-status report, detailing network properties, overall risk score, extent of risk introduced by devices and protocols, likelihood of lateral threat movement between business processes, potential attack paths and more. The process is triggered automatically each time a change is detected on the network.

In addition, iRISK provides applicable remediation recommendations according to NIST guidelines, specifying which corrective actions improve network's security posture. For example, iRISK would recommend that the operator segment the network or allow only firewalled access to certain assets, which eliminate several attack vector exploits and improve the cyber risk score by a certain amount.

PART OF RADIFLOW'S FULL-STACK INDUSTRIAL CYBERSECURITY SOLUTION

- **iSAP**: Low-bandwidth Smart Collector
- **iSID**: Industrial Threat Detection & Network Visibility
- **iCEN**: Central management for multiple instances of iSID



COMPLIANCE WITH IEC 62443 CSMS

iRISK provides compliance with the relevant sections in IEC 42443 CSMS regarding risk assessment:

- 62443-2-1: *Define your Business Rationale (based on the nature and magnitude of financial, HSE, and other potential consequences should IACS cyber incidents occur.)*
- 62443-1-1 3.2.88: *Risk assessment process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources; quantifies loss exposures and consequences based on probability*
- 62443-2-1 A.2.3.3.2: Automated Risk and Vulnerability assessment report
- 62443-2-1 A.2.3.3.3.3: *Automated High level Risk Assessment report*
- 62243-2-1 4.2.3.12*: Conduct risk assessments throughout the lifecycle of the IACS*
- 62243-2-1 4.2.3.14*: Maintain vulnerability assessment records*
- *Mitigation Recommendation & Prioritization*

ABOUT RADIFLOW

Radiflow develops trusted Industrial Cyber-Security 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. Our intelligent Threat Detection and Analysis Platform for industrial cyber-security 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 cyber-security vendors.

Founded in 2009, Radiflow' solutions, are successfully deployed by major industrial enterprises and utilities protecting more than 3,000 critical facilities worldwide. 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