Radiflow and Sixgill

Advanced Dynamic Risk Modeling for ICS Environments

WHY RADIFLOW?

Radiflow is a recognized leader in industrial cybersecurity, offering dedicated solutions designed to meet the unique requirements of industrial infrastructures:

EXPERIENCE

Over 10 years' experience discovering and analyzing advanced persistent threats and targeted attacks, including attacks on critical and industrial infrastructure

EXPERTISE

Dedicated team of industrial cybersecurity experts who understand the colliding worlds of automation and security.

END-TO-END PORTFOLIO

Radiflow offers a holistic portfolio of services and technologies, including secure gateways, Industrial IDS and many more.

- Risk-driven dynamics and proactive risk monitoring for critical infrastructures
- Go beyond CVEs with vulnerability intelligence from both open and dark-web sources, for proactive protection against emerging and fringe threats
- Integration via Radiflow's iSID detection and monitoring platform for ICSs
- Alerts for contextual business relevance and production impact

The Problem:

Risk modeling in critical industrial infrastructure (CII) environments requires a dynamic and comprehensive approach to risk.

The current methodology for threat detection in Industrial Control Systems (ICS) relies on passive risk modeling, using generic threat intelligence feeds such as Common Vulnerability Reports (CVEs).

While commonly used, generic threat intelligence feeds may not cover emerging threats that have not been yet materialized, or fringe threats that apply only to certain locales or sectors. Consequently, current ICS exploitability modeling tools and threat posture assessments may be not only ineffective—they may actually produce dangerously misleading results.

To achieve a comprehensive risk model, relevant to your cyber management systems and mitigation procedures, multiple risk vectors and operational factors need to be taken into account:

- Network and system topology, mitigation and security controls
- The importance of a specific asset to a business process (business impact)
- Current attack tools "in the wild" that can be used against your network
- Reported breaches in your industry or/and region
- Threat actors interested in breaching your organization
- Relevant breach techniques and tactics applicable to your industry

Risk-driven dynamics and proactive risk monitoring in CII are the cornerstones for establishing an efficient and cost-effective cyber security policy.

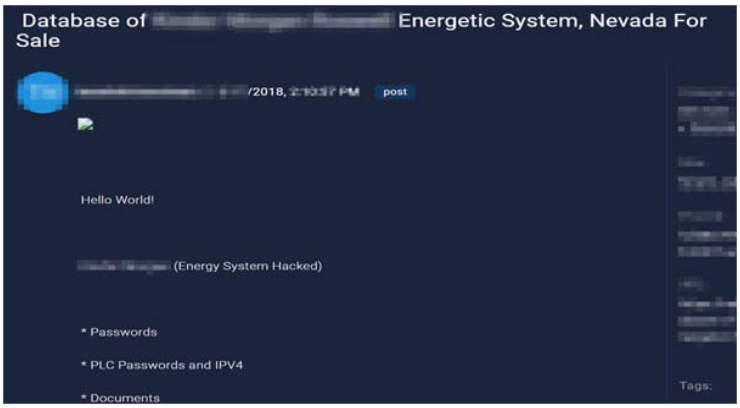
Continued...

The Solution:

Radiflow's threat detection and monitoring platform (iSID) delivers threat and risk modeling to your ICS environment, by monitoring the ever-changing threat landscape.

By incorporating Sixgill's proactive threat intelligence services, Radiflow is now able to dynamically deliver contextual cyber-relevance (e.g. cyber-resiliency posture, industry, location) to your production process, based on both open and Dark Web sources. This includes impact to business/production, threat actors that utilize breach techniques applicable to your network, and much more.

This screenshot displays ICS-specific threat intelligence information, including network and device password, retrieved from Dark Web intelligence sources. Had this type of information been applicable to the security of your network and assets, it would surely bring you to change your risk posture and incident response prioritization.



Radiflow's iSID detection and monitoring platform for ICSs, in tandem with Sixgill's threat Intelligence services, will map your threat landscape and cyber-attack surface, deliver alerts for contextual business relevance and production impact, and provide risk modeling and incident response prioritization—all efficiently managed through a single platform.

About Radiflow

Radiflow is a leading provider of cyber security solutions for critical infrastructure networks. SCADA networks often extend across multiple remote sites, allowing automation devices to be controlled from the control center. Radiflow's security tool-set validates the behavior of both M2M applications and H2M (Human to Machine) sessions in distributed operational networks. Radiflow's security solutions are available both as in-line gateways for remote sites and as a non-intrusive IDS (Intrusion Detection System) that can be deployed per site or centrally. Radiflow was founded in 2009 as part of the RAD group, a family of ICT vendors with over $1Bn annual revenues.

Radiflow solutions were launched at the end of 2011, validated by leading research labs and successfully deployed by major utilities worldwide. More information can be found at www.radiflow.com.

About Sixgill

Sixgill is a worldwide leading cyber intelligence vendor. Cyber intelligence is the critical missing link in today's cybersecurity environment, providing organizations with a threat intelligence picture that allows them to focus their resources on preventing attacks, discover those already perpetrated and mitigating the damage caused by cyber-crime.

Established in 2014, the Company already has a wide range of customers from leading Fortune 500 companies as well as Federal Agencies. Utilizing artificial intelligence and machine learning, Sixgill automates the production cycle of cyber intelligence from monitoring, to extraction to production, uniquely focusing on relevant threat actors by mapping the Dark Web as a Social network where significant amounts of cyber-crime takes place. Providing prioritized and automated real-time alerts when threats are detected and then providing a comprehensive threat intelligence picture through advanced data mining and behavioral analytics of the threat actors, the time from alert to receipt of automated actionable intelligence is the fastest on the market. For more information: www.cybersixgill.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 2461963
sales_UK@radiflow.com

radiflow
Secure Your Assets