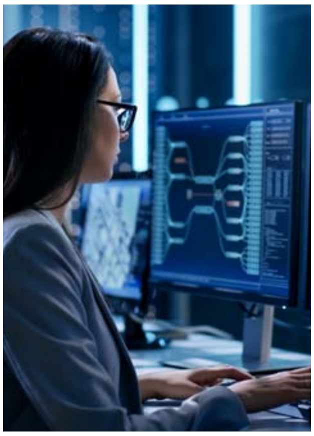
Radiflow for MSSPs

Radiflow's ICS/IIoT Security Solution for Managed Security Service Providers (MSSPs)



- Single-pane access to all tenants' iSID Industrial Threat Detection systems through the iCEN Central Provisioning & Alerting platform
- Cloud topology-enabled data analysis for ICS/IIoT intrusion detection
- Secure, low-bandwidth data collection and transfer using Radiflow's iSAP industrial-grade collector and compression engine
- Integration with leading industry CVE feeds for vulnerability database updates and alerts
- Pushing of Indications of Compromise (IOC) to select iSID systems
- Export of templated analysis reports for use in governance and compliance reports

A holistic, single-pane ICS/SCADA security suite for MSSPs

Radiflow's MSSP offering addresses the critical challenges facing ICS/IIoT security service providers: assuring secure and efficient data collection, analysis and transfer, as well as provisioning multiple detection engines, in a cloud environment.

With Radiflow's offering, MSSPs are able to offer their ICS/IIoT-based tenants a unified, end-to-end solution suite, designed from the ground up for industrial operations:

- **iSAP - data acquisition and transfer**: at the OT network level, the iSAP hardware-based industrial-grade collector conveys (via GRE tunnel) an encrypted, bandwidth-efficient mirrored data stream to the iSID Industrial Threat Detection system at the MSSP. iSAP can also act as an IIoT switch, accepting ICS protocols and securely sending northbound traffic.
- **iSID - threat and vulnerability detection**: installed per-MSSP tenant, iSID provides real-time alerting for threats and vulnerabilities detected in the OT network. It provides visibility and insight to OT Asset Discovery, with full attributes for type, vendor, project and middleware version, as well as ICS/IIoT protocol-based deep packet inspection.

  For cyber-reporting compliance, iSID exports compliant templated reports for visibility (including an inventory of all OT assets, network links, protocols, attack types and more), monitoring, and alert statistics.

  iSID integrates with leading industry CVE feeds. When a new vulnerability relevant to a tenant asset data base is published, the tenant will be notified via iCEN. If requested, additional threat intelligence services can be integrated to push IOCs (Indications of Compromise) to iSID.

Continued....

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

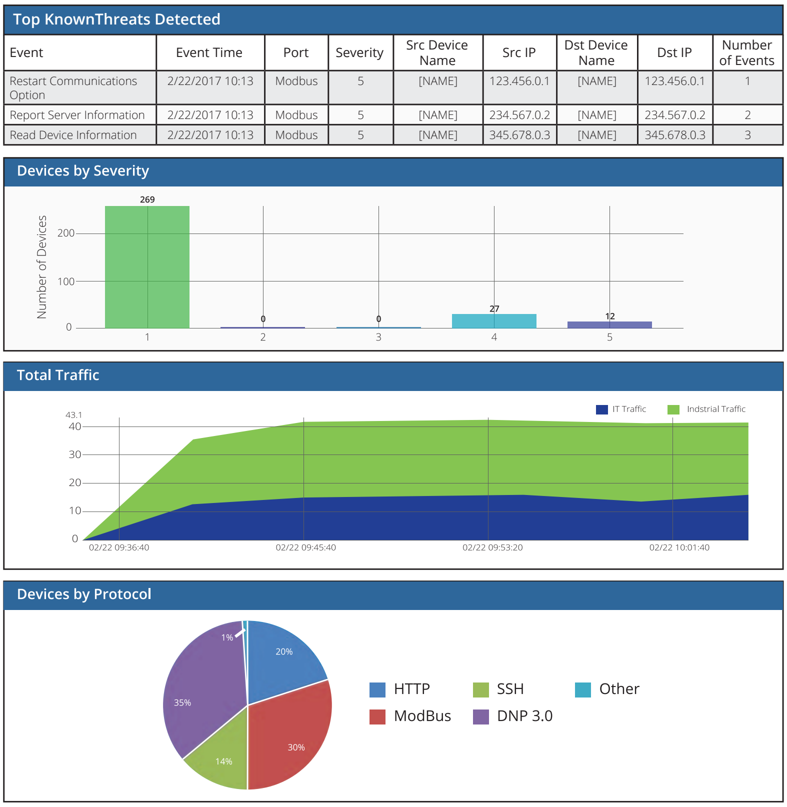
Dedicated team of industrial cybersecurity experts who understand the colliding worlds of automation and security.

END-TO-END PORTFOLIO

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

Continued...

- **iCEN - single-pane central alerting, monitoring and provisioning platform**: installed and operated by the MSSP, iCEN provides single-pane monitoring, alerting and provisioning for multiple tenants' iSID systems. iCEN is available for both Multi-VM and Multi-Stack tenant deployments, allowing tenants to optimize their shared monitoring costs. To assure tenant separation, Radiflow does not recommend shared network and shared application deployments.
    - **iCEN Alert Monitoring**: the single-pane iCEN cyber monitor module displays alerts triggered by all tenants' iSID systems. In addition, iSID can interface with leading SIEM vendor to monitor IT and OT environments.
    - **iCEN Management:** as a multiple iSID-management platform, iCEN enables system monitoring, health checks and provisioning of threat intelligence updates such as attack signatures. iCEN's single-pane dashboard will alert the MSSP for malfunctions or overloads at any iSID instance belonging to tenants.
- **Secure operation in Multi-VM or Multi-Stack environments**: to prevent data leakage from one tenant to the another via iCEN, a special tokenizing solution has been applied which sends only de-classified information to the shared monitoring application. MSSP Tier-1 SOCs will receive alert metadata to notify clients and proceed to incidend response. In certain scenarios Tier-2&3 SOCs will be able to log into the iSID on the relevant tenant for deeper incident investigation.



Top KnownThreats Detected

Event	Event Time	Port	Severity	Src Device Name	Src IP	Dst Device Name	Dst IP	Number of Events
Restart Communications Option	2/22/2017 10:13	Modbus	5	[NAME]	123.456.0.1	[NAME]	123.456.0.1	1
Report Server Information	2/22/2017 10:13	Modbus	5	[NAME]	234.567.0.2	[NAME]	234.567.0.2	2
Read Device Information	2/22/2017 10:13	Modbus	5	[NAME]	345.678.0.3	[NAME]	345.678.0.3	3

Sample reports generated by iSID

About Radiflow

Radiflow is a leading provider of cybersecurity solutions for critical infrastructure networks (i.e. SCADA), such as power utilities, oil & gas, water and others.

Radiflow's security toolset 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's solutions are sold either integrated within a global automation vendor's end-to-end solution, or by local channel partners, as a standalone security solution.