

# iSIM

## Industrial Service Management Tool

### WHY RADIFLOW?

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

### EXPERIENCE

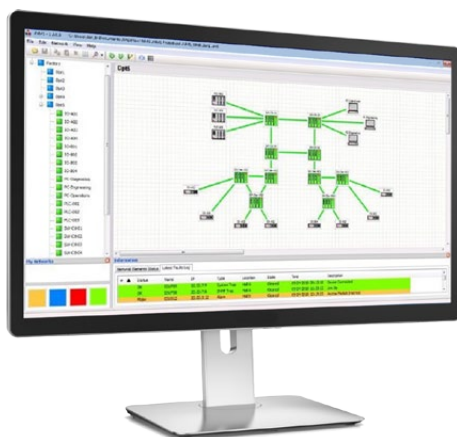
Over 10 years of experience discovering and analyzing advanced persistent threats and targeted attacks, including attacks on critical and industrial infrastructure.

### 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 SCADA gateways, routers and firewalls, industrial network IDS and more.



- ▶ Cross-network maintenance for device groups
- ▶ Security violation alerting
- ▶ User-access logging and reporting
- ▶ Automatic database backup
- ▶ Network performance analysis
- ▶ Management of Authentication Proxies

## Central Management for Multiple On-Site Gateways

iSIM is an intuitive network management tool for Radiflow's secure gateways. It provides a real-time view of all network devices and allows combining devices on disparate networks into a single group for simple and intuitive cross-network maintenance.

### Cross-network OS version upgrading

iSIM significantly simplifies OS upgrading by creating device groups and allowing for group batch operations. Prior to the upgrade, iSIM verifies each device's connectivity, to enable uploading the new OS version to all device group members. Upon completion, a detailed report is issued.

### Database Export/Import

iSIM periodically backs up device configurations to the server. This backup can be used to restore the configuration of devices that had been misconfigured due to human error, or should a physical replacement of a device be needed.

Continued...

## SECURITY

Radiflow's devices offer advanced security features such as a distributed firewall and task-based validation of human-to-machine (H2M) sessions. This enables granting access to only specific end-devices without exposing the entire network. All user access and activities are fully logged.

### Network access management

Radiflow's distributed firewall enables enforcing security profiles across the network according to predetermined policies. iSIM translates the security profiles into firewall rules, which are automatically uploaded to the secure gateways across the network. This ensures that the same profiles are used across the network.

When service maintenance is needed but granting access to the entire network is not acceptable, Radiflow's APA (Authentication Proxy Agent) allows setting a time window for accessing a specific device via the distributed firewall.

iSIM enables selecting specific Radiflow devices on the network and creating custom firewall rules for each device. This in effect creates, during the allotted time window, a direct tunnel from the technician's PC to the specific SCADA device (PLC, IED, RTU, etc.) without exposing the entire network.

At the end of the access window a detailed log file is generated with all of the technician's operations.

## DIAGNOSTICS

iSIM provides a map view of the network topology, divided into sub-networks, indicating each edge device (by Radiflow or otherwise) such as PLCs, RTUs etc. Events reported to iSIM by Radiflow's networked devices are presents in an aggregate view.

Operational alerts are prioritized and color-coded, and presented graphically as map links. The user is able to filter alerts by severity, protocol and more.

iSIM also contains traffic analysis tools, which provide:

- ▶ Log files with all violations
- ▶ Log files for the maintenance process
- ▶ Traffic statistics of links in the network
- ▶ Performance-over-time graphs for selected links

## SPECIFICATIONS

### Functionality

- ▶ Map topology management
- ▶ Network elements auto-discovery
- ▶ Network administration tools
- ▶ Security rules planning per service group
- ▶ Security violations log
- ▶ Aggregate log for network alarms
- ▶ Performance monitoring tools

### System Administration

- ▶ Client-Server architecture
- ▶ User-authorization levels