Radiflow

iSID 6.2
RELEASE NOTES

TABLE OF CONTENTS

RELEASE CONTENT

SOFTWARE PACKAGE

THE ISID VERSION IS RELEASED AS A SINGLE RPM BASED ON CENTOS MINIMAL OPERATION SYSTEM, INSTALLED ON PHYSICAL BARE-METAL INSTALLATION OR VIRTUAL (VMWARE BASED) INSTALLATIONS USING RADIFLOW'S INSTALLATION MANGER (RIM)

DOCUMENTATION SCOPE

THE DOCUMENT STATES THE CHANGES FROM THE PREVIOUS ISID GA VERSION 6.0 TO THE CURRENT ISID GA 6.2 VERSION.

NEW FEATURES

The new iSID Version – 6.2 – Industrial Threat Detection System by Radiflow. The following describes all new features and changes made on the system that are significant and important to the everyday user.

ASSET VISIBILITY & OPERATIONS

PROCESS VALUES INFRASTRUCTURE

- Process values from OT protocols can be presented as part of "Asset management"
- Threshold values setup and alerting
- Values presentation – current, last hour and 24 hours
- Export as PDF, CSV report
- Support for Johnson Control N1 values – analog and digital

NEW/UPDATED SUPPORTED PROTOCOLS

- Johnson Controls
  - DPI for N2 protocol and improved DPI for N1
- IEC 61850
  - GOOSE parsing improvements
- Visibility for additional L2 Ethernet types – EtherCat, CC-Link, Powerlink, QNX, SERCOSIII, MRP.
- Improvement of ports/protocols association (MOXA, OPC, Yokogawa)

ASSET ATTRIBUTES

- Configuration of global attributes for OT assets – name and value
- Option for updating existing assets with these attributes and values

MONITORING ADDITIONAL OT NETWORK FROM SAME ISID INTERFACE

- Option to configure and view additional OT network from same ISID UI client
- Configuration of "Primary" and "Secondary" ISID and setting names
- Option for VLAN filtering for traffic monitoring

SERVICENOW OT CENTER INTEGRATION

- Automatic synchronization of assets from iSID to ServiceNow OT Manufacturing Center
- Setting up the integration and defining the synchronization policy is done from iSID UI

CYBER SECURITY

ASSET VULNERABILITY MANAGEMENT

- Updating vulnerability management module to new NVD API
- Capability to change Operating System for Windows and Linux machine
- Capability to add Service Pack level for Windows OS
- Updated MAC-vendor database

CERVELLO INTEGRATION

- Integration with Cervello Railway signaling security platform
  - Collect and analyze alerts sent by Cervello following suspicious patterns detection
  - System wide support (alerts screen, risk calculation)
  - Setting up the integration is done completely from iSID UI

CISCO ISE INTEGRATION

- Integration with Cisco ISE Network access control platform
  - Certificate-based mutual authentication between ISID and ISE
  - Automatically synchronization of assets information to ISE platform
  - Capability to invoke Adaptive Network Control (ANC) policy from Alerts screen following ISID threat and anomaly detection
  - Setting up the integration is done completely from iSID UI

SECURITY REPORT

- Adding "Zone" data to "Devices"
- Fixing bugs in "Subnet" and "Subnet direction" sheets
- Fixing bugs in protocols pie chart
- Improving error handling during report production
- Improving presentation of "Asset characteristics" sheet
- Add new user-defined info to "network visibility-devices" sheet
- Fixing bugs in "Router-Switch" sheet
- Additional improvements and fixes

SYSTEM

UI & USABILITY

- New Process Values (asset management) tab
- UI workflows for creating new integrations (ServiceNow OT, Cisco ISE, Cervello)
- Multiple renewed screens
- Removing "GOOSE", "Profinet" tabs from "Network Visibility-External data" tab

SNMP MONITORING

- Monitoring of ISID CPU and RAM via SNMPv3

PERFORMANCE

- Performance improvement in alerts management and analysis module

BACKUP AND RESTORE

- Fixing bugs in backup and restore functionality
- Improved robustness and error handling

NTP AND TIME SYNCHRONIZATION

- Fixing bugs in NTP Server configuration
- Improved robustness and error handling

SYSTEM SECURITY

- Third-party software versions update

PRODUCT COMPATABILITY

COMPATABILITY MATRIX

- iSID version 6.2 is compatible with:
  - iCEN V 6.2, V 6.0
  - iSAP
    - Rule based configuration – iSAP V 4.5.03.17 or higher
    - Transparent mode – all iSAP versions
  - CIARA TBD
- Upgrade procedure is supported from iSID version 5.7.7

FIXED ISSUES

KNOWN LIMITATIONS	
ISID-4542	Remote DB – needs to be configured as part of the installation process and only in "from scratch" mode (meaning the DB wasn't configured as remote DB for different iSID before)
ISID-4634	Blocked user can be released by changing only the username
ISID-5624	Authentication using Active Directory – can't map more than one AD group to specific iSID role

APPLICABLE DOCUMENTS

- iSID V6.0 user manual
- iSID quick installation guide
- iSID upgrade procedure
- iSAP configuration guide

THIS CONTROLLED DOCUMENT IS THE PROPERTY OF RADIFLOW LTD.

**THIS DOCUMENT CONTAINS PROPRIETARY INFORMATION.
ANY DUPLICATION, REPRODUCTION OR TRANSMISSION
TO UNAUTHORIZED PARTIES WITHOUT PRIOR
PERMISSION OF RADIFLOW IS STRICTLY PROHIBITED.**

STATEMENT OF CONDITIONS