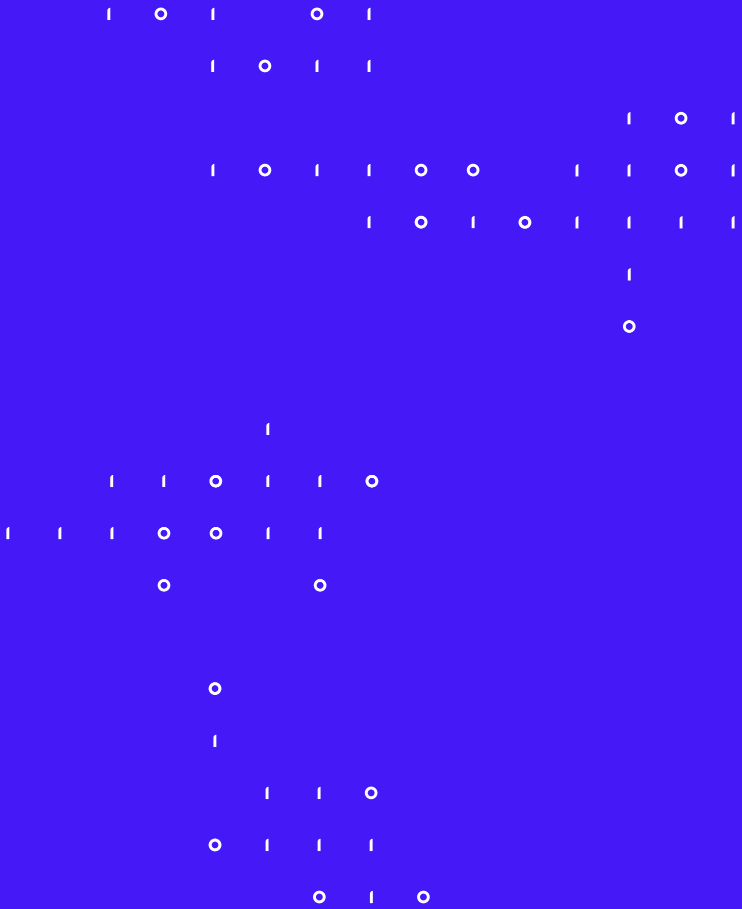


ISECO
Security Monitor

v1. 2017

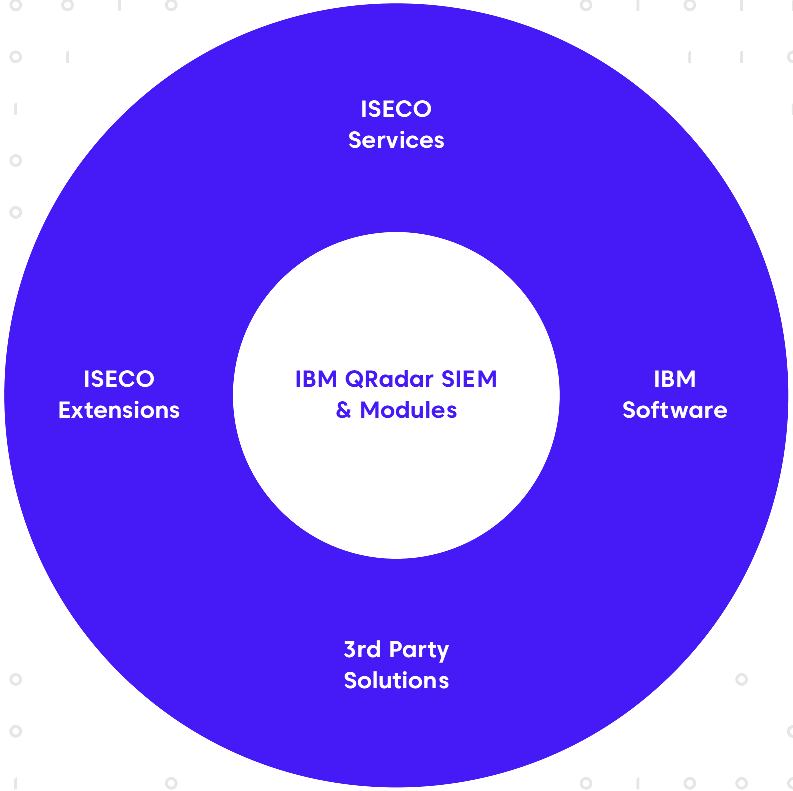
ISECO Security Monitor solution based on the IBM QRadar platform is an integrated system combining full IBM QRadar SIEM with an ISECO Toolset, extending the functionalities and professional services to meet all of your security monitoring needs.

💡 The solution can be delivered as a standard license or as a service.

IBM
Gold
Business Partner

Expert

Security Operations
& Response



An integrated system combining full IBM QRadar SIEM with ISECO Toolset.

Overview

IBM QRadar SIEM is a one of the leading SIEM solutions on the market with a broad range of functionalities and relatively simple basic implementation and operations.

Nevertheless, not all security monitoring needs can be met by the QRadar SIEM software alone or via basic implementation.

This is why the ISECO Security Monitor was introduced. To extend the QRadar SIEM potential and to provide additional functionalities and professional services with unique know-how.

- ✓ First-class IBM QRadar SIEM with all of the extensions like Vulnerability Management and UBA
- ✓ ISECO professional implementation, service support and security monitoring services
- ✓ ISECO toolset applications utilize QRadar SDK & API and provide advanced functions for security monitoring operations and support
- ✓ IBM & third party extensions to meet your special security monitoring needs

Features

01

IBM QRadar SIEM

- Security intelligence platform – SIEM 2.0
- Top ranking in Gartner Magic Quadrant and Forrester Wave in the SIEM domain
- Extensive security-based data collection, correlation and secure storage
- Tool for security correlations, detection of incidents and investigation support
- Single console tool

IBM
QRadar

02

ISECO Toolset

- Log enhancing
- Identity Awareness to fully track user history
- Blacklist consolidation and efficient evaluation
- Advanced ticketing integration with manual and automatic ticket creation and assignment options
- Enhanced reporting based on AQL
- Logbook for operator activity audits
- Custom connectors for MS Exchange, AS400 or MS SQL auditing
- And many more

For more information about the ISECO Toolset, download ISECO Toolset leaflet.

03

ISECO Services

Implementation

- Solution implementation
- Consultation of security monitoring use cases and implementation
- Customer integration and custom development

Operation

- Advanced proactive service support
- Ongoing consulting for advancement, integration of custom applications etc.
- Security monitoring as a service - ISECO SOC for outsourcing the security monitoring agenda

For more information about ISECO Services, download ISECO Services leaflet.

Optional

IBM & third party solutions

- IBM Security Guardium – advanced database monitoring
- IBM Security Appscan – tool for assessing application vulnerabilities
- FlowMon – probes and collectors for NetFlow/IPFIX processing with advanced NBA
- Rapid7 Nexpose – advanced vulnerability management
- AgileSI SAP Monitoring – security monitoring of SAP environment

Solution editions

Features	Standard	Enterprise	Toolset
IBM QRadar	●	●	—
ISECO Support App	●	●	○
ISECO Logbook	●	●	○
ISECO Ticketing	○	●	○
ISECO Incident Report	○	●	○
ISECO Custom Agents (Exchange, MSSQL)	○	●	○
ISECO Log Enhancer	○	●	○
ISECO Identity Awareness	○	●	○
ISECO Process Monitor	○	●	○
ISECO Advanced Reporting	○	●	○
ISECO Whitelist	○	●	○
ISECO Blackhammer	○	●	○
ISECO AJEMON for AS400	○	○	○

● Included ○ Optional — Not included

Deployment options

A

On-premise

Traditional license model and annual maintenance.

- License deployable as virtual or HW appliance
- Maintenance including updates & upgrades and support paid on an annual basis

Additional services

- Implementation
- Advanced service support and consulting
- Security monitoring as a service

B

SaaS deployment

Service model with monthly/annually calculated fee. Virtual appliances hosted in client infrastructure or HW appliances hosted in client infrastructure or full SaaS in cloud. Advanced support always included.

Additional services:

- Implementation
- Consulting
- Security monitoring as a service

Appliances, sizing, licence & pricing

Appliances

ISECO Security Monitor can be delivered upon request with two default appliance types based on incoming data rate and client performance requirements.

ISM Appliance Standard

- 16 Core, 64 GB RAM, 10 TB, 2U
- Up to 5000 EPS as all-in-one

ISM Appliance Plus

- 28 core, 128 GB RAM, 48 TB, 2U
- Up to 15 000 EPS as all-in-one

Upon the client's request, the appliance sizing can be modified, for example storage size.

Solution sizing

Each ISECO Security Monitor deployment is individually prepared based on the client's requirements and infrastructure. The following have to be taken into consideration:

- Client's security monitoring requirements
- Number and type of systems in infrastructure
- Infrastructure complexity
- Incoming data load – events and flows to estimate event per second rate (EPS) and flow per minute rates (FPM)

The sizing deployment is usually prepared after a short evaluation with the client.

Licensing & pricing

ISECO Security Monitor is licensed and the price for both deployment options is calculated based on solution sizing:

- Edition
- Events per second rate (EPS)
- Flows per minute rate (FPM)
- Optional appliances
- Optional additional QRadar SIEM modules and ISECO modules
- Optional IBM or third party solutions

The price is available upon request, provided that the above-listed basic sizing parameters are specified.

Contact

Are you interested in our Security Monitor solution? Great! Let’s discuss how we can help you.

Website

www.iseco.global

Phone

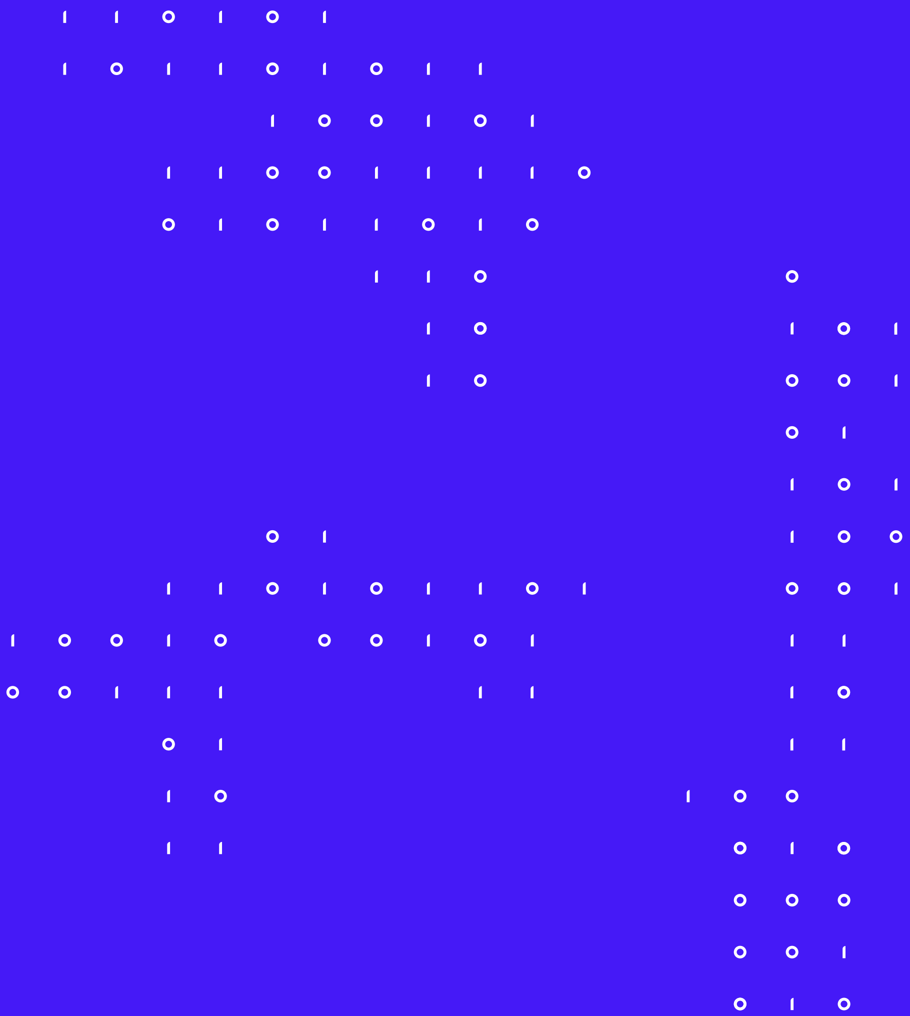
+420 234 760 570

E-mail

info@iseco.global

Adress

ISECO.CZ s.r.o.
Bartůňkova 2349/3a, Chodov
149 00 Praha 4
Czech Republic



Securing insecurity