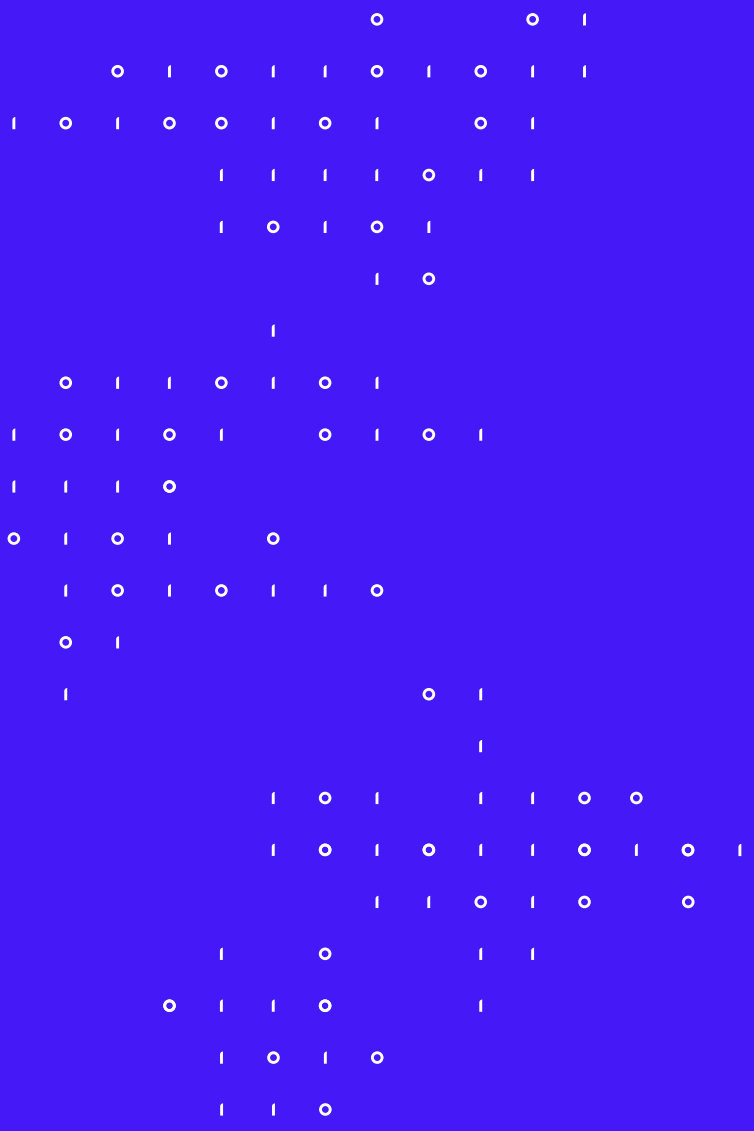
ISECO



ISECO Toolset

v1. 2020

The ISECO Toolset for IBM QRadar SIEM is a set of QRadar applications which extend the core functionality of IBM QRadar to meet specific client needs for security monitoring.

It utilizes the IBM QRadar SDK and provides additional functionality in a native and fully supported way.

All applications are available as perpetual licences or yearly subscriptions. Maintenance is carried out to provide support and perform new updates/upgrades.

IBM Gold Business Partner™

Expert

Digital Trust

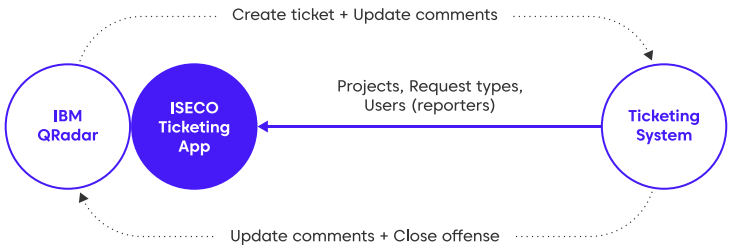
Threat Management

Ticketing

Extends native QRadar investigation workflow with 3rd party ticketing system integrations. Manual or automatic incident /ticket creation using a 3rd party system, two-way sync for comments and closing actions. Detailed automatic rules can be used to pre-fill values for the resulting tickets.

Features

- Create multiple templates for resulting tickets
- Manual ticket creation from an offense view – simply select template and create ticket
- Define automatic rules to determine what template will be used and/or what values will be pre-filled
- Automatic rules can be defined based on the offense for rule name, IP address, username
- Modular architecture to support multiple ticketing systems
- Two-way sync for offense/ticket comments
- Automatic offense closure after ticket is resolved (and vice versa)

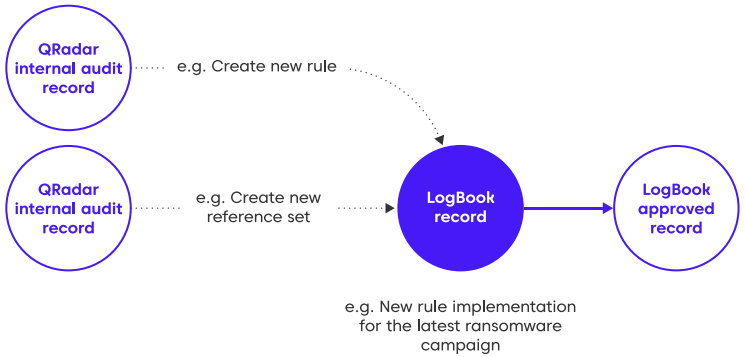


LogBook

LogBook helps you keep track of administrator or user activities in QRadar by pairing and grouping native QRadar audit messages with human readable records.

Features

- Automatically search for native QRadar audit records connected with user activity
- Create logbook record and pair it with native QRadar audit messages
- Workflow approval for logbook records included (user with admin privileges has to approve logbook records)
- Unchangeable approved records

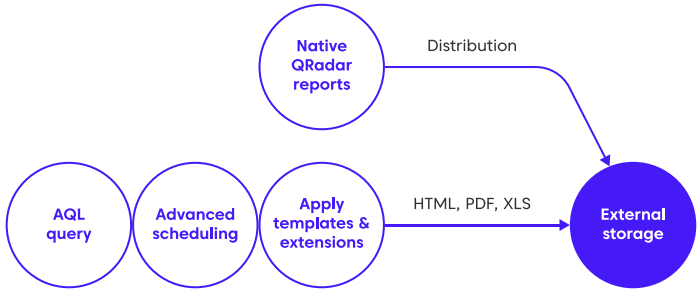


Advanced Reporting

Extends native QRadar reporting capabilities, allows for the distribution of native reports to external/remote storage, creates parametrized AQL reports and builds advanced Excel reports.

Features

- Distributes native QRadar reports to remote/external storage
- Can distribute non-empty reports only
- Send aggregated email notifications (report summaries)
- Configuration for email/report distribution based on QRadar user roles/security profiles
- Create AQL queries with specified parameters and run parametrized reports
- Create advanced AQL reports with custom scheduling and export the results as an Excel worksheet



Advanced Backup

Backup app extends native QRadar backup functionality and allows for the automatic distribution of QRadar backup to remote/external storage, monitoring of all operations (backup creation, distribution to remote/external storage) using standard logging to QRadar and specific correlation rules.

The application also enables the creation of a custom backup of any folder on QRadar deployment (distributed/HA deployments are also supported).

Features

- Distribute QRadar native backup archives to remote/external storage (SMB, NFS, SFTP)
- Create custom backup of any folder in QRadar systems to remote/external storage
- Maintain backup archives (retention)
- Advanced scheduling included
- Multiple backup sources and destinations supported
- Monitor all operations using native QRadar logging and Custom DSM, set of correlation rules included
- Support for distributed/HA deployment
- Native QRadar SDK app (ready for AppHost), QRadar 7.3.2+ required

Incident Report

Incident Report generates a specific report from QRadar offense for authorities such as superior CSIRT/CERT.

Features

- Fully integrated in QRadar offense user interface
- Generates report in machine-readable format suitable for automatic processing (XML, JSON)
- Output formats can be customized for your specific needs

Whitelist

Whitelist extension helps create a specific whitelist with multiple values which can be used in your correlation rules.

Features

- Whitelist values can be imported from an external source and updated on a regular basis
- Whitelisting condition can be based on several parameters – it opens up the possibility to create a time-limited whitelist, dynamic whitelist based on real-time values etc.

Log Enhancer

Log Enhancer enriches incoming audit messages with external information.

Features

- Add important information missing from the original message (for example DNS name where only IP address is provided, translate employee number to username etc.)
- Use it for standard correlations and/or custom propertes
- Two modes of enrichment available – direct enrichment (only the enriched message is stored) or forwarded enrichment (both the original and enriched message are stored)

Custom Agents

The development of custom agents was based on various experiences from IBM QRadar SIEM deployments and allows for events to be collected from non-supported or challenging systems.

IBM iSeries (AS400)

Custom agent for IBM iSeries (AJEMON–Audit Journal Entry Monitor) reads audit journal entries, formats them and sends them to QRadar as syslog messages. The agent was specifically built for the IBM iSeries with a deep understanding of the iSeries audit subsystem and is fully configurable with various filtering options.

Support for message queue events is available as an extension of the standard audit journal monitor.

MSSQL audit agent

MSSQL audit agent includes a specific set of configurable components and techniques for a safer reading of native MSSQL audit messages.

The agent resolves issues with badly designed MSSQL native audit systems, such as audit files rotating, locking audit files and disc space running low on the SQL server.

Tailor-made agent/connector

If you are looking for specific system integration, rough log format parsing or any other unsupported platform integration, we can assist you – our team has long-term experience with QRadar SIEM integration. Get in touch – we are ready to help!

Licensing, pricing & maintenance

License models

- Perpetual license and yearly maintenance
- Yearly subscription (maintenance included)

Maintenance

- Regular updates and application upgrades
- Technical support in case of application issues with 8x5 CET availability and NBD response

Pricing

ISECO Tool	Perpetual licence[1]	Yearly subscription
Ticketing	2 900 EUR	1 200 EUR
LogBook	2 400 EUR	1 000 EUR
Advanced Reporting	2 400 EUR	1 000 EUR
Advanced Backup	2 400 EUR	1 000 EUR
Incident Report	1 900 EUR	800 EUR
Log Enhancer	1 900 EUR	800 EUR
Whitelist	1 900 EUR	800 EUR
Custom Agents	On demand	On demand

[1] *First year of maintenance included in license price. Second and following years are at 25 % of the license price.*

Your notes

Contact

Are you interested in our ISECO Toolset applications? Great! Let's discuss how we can help.

Website

www.iseco.global

Phone

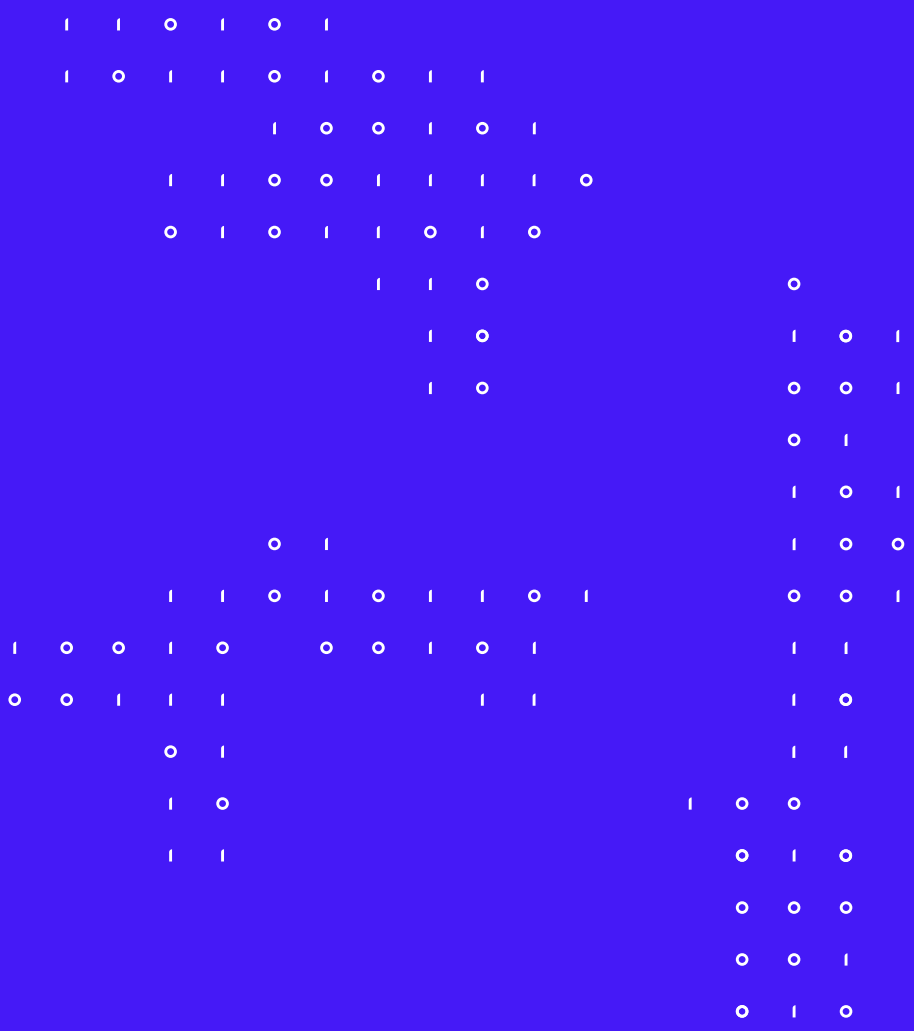
+420 234 760 570

E-mail

info@iseco.global

Adress

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



Securing insecurity