ISECO

IBM QRadar Services

Expert

Security Operations
& Response

www.iseco.global info@iseco.global

Service & Support

Service and support proposed using SLA:

- 10x5 CET or 24x7 support availability
- Next business day response time for non-critical issues
- 2h response time for critical incidents
- Best-effort for critical incidents including outside of the specified availability times
- The SLA can be adjusted based on the client's needs

Our services cover the following:

- Full SIEM deployment support, including customization
- Regular updates and upgrades (e.g. to the latest version) of QRadar
- Analysis of reported issues using remote access (VPN)
- Resolving reported issues, communicating with IBM support on the client's behalf, submitting PMRs and RFEs
- Resolving implementation issues (rules, reports, extensions, etc.)
- Integration with ISECO QRadar software health monitoring service
- Proactive resolutions – when an issue is detected by another client, ISECO will inform the client and resolve the issue
- Q&A for QRadar functionality and deployment
- Remote session with the client if necessary i.e. for issue identification
- Service is completely remote (VPN, Remote session)

Consultancy

Our consultancy services operate on the basis of pre-paid man-days (MD).

The client can enlist our consultancy services for the following tasks:

- User training conducted remotely or on-site
- Analysis of system or application logging
- Log source integration and log source connector set-up
- Creation of reports based on the client's needs
- Fine-tuning offences and correlation rules
- Integration of external systems and services
- Remote offence analysis and consultancy
- Functionality upgrades of custom tools
- Development of custom tools
- General implementation tasks
- Other SIEM consultancy and services

Consultancy MDs are calculated by the full hour and the client will receive a periodic report of the MDs used. A detailed, up-to-date report is also available on the helpdesk portal.

The number of required MDs is always calculated upon request and the client must always confirm the calculation prior to billing.

Our consultancy services are conducted by experienced consultants with 4+ years' experience with QRadar SIEM projects.

After a consultancy request has been submitted to the support portal, ISECO will then notify the client with an estimate of the number of MDs required.

Consultancy can be conducted both on-site and remotely based on the client's requirements and legal restrictions (for non-EU markets).

Security Monitoring

Regular security operations using SIEM output processing are essential for effective security monitoring.

Security operations can be realized:

A) Continuously 24x7 (full SOC)

B) Continuously 10x5 with a tolerance for critical incidents outside of working hours

C) Regularly in defined time slots

An assessment is conducted prior to the commencement of service.

Option B) includes:

- Integration of QRadar offences with the ISECO portal
- L1 and L2 offence analysis performed by ISECO experts via remote access (response time based on the client's requirements (15min-2h))
- Analysis of the offences to identify:
  - False positives
  - Potential incidents (the client's staff must conduct further investigation)
  - Incidents (the client is notified immediately)
- Search and evaluation of all available information in QRadar SIEM and other provided information sources to identify the threat, assess the potential impact and define the remediation steps
- Contact with the client based on the agreed-upon requirements and criticality: SMS notifications, e-mail, scheduled calls
- Consultancy during the analysis process conducted remotely
- Recommendations for fine-tuning rules and reports