COMPANY OVERVIEW

TABLE OF CONTENTS

ABOUT Q-SEC

Born from the Network and Security Operations Centre of a holding group of 5 companies, the team have over 15 years of experience on the front line of cyber security - tackling the most complex of targeted attacks and spearheading compliance programmes ranging from GDPR preparation all the way through ISO implementation to sector-specific requirements in various geographies.

With all processes built around globally recognised standards in service operations and a world class consulting team of specialists, Q-Sec are focused on providing the best of both worlds - services tailored to unique requirements, while ensuring regulatory documentation and processes of the highest levels of maturity.

The key objective of Q-Sec is to provide a trusted, loyal, and business-aware cyber security partner to our clients - one that is acutely aware of the realities of their various industries and can best support them in their goals without increasing risk or compromising of the security of their data.

ECSO EUROPEAN CYBER SECURITY ORGANISATION · PCI DSS COMPLIANT · ITIL® · CISSP Certified Information Systems Security Professional · C|EH Certified Ethical Hacker®

MISSION AND VISION

What do we at Q-Sec stand for?

Mission

To help businesses achieve their objectives while not compromising on security and ensuring compliance to both the necessary and the beneficial standards.

Vision

To empower organisations of all sizes with cutting-edge cybersecurity solutions by seamlessly integrating best-in-breed tools, mature processes, and expert-managed services. We envision a safer world driven by continuous learning, collaboration, and fostering trust.

CYBER LANDSCAPE

75% of C-Suite executives put cyber as the biggest concern for risk management strategies (PwC Pulse 2025)

As the complexity of attacks and defence mechanisms is on the rise, companies are struggling to maintain a scalable risk management strategy - and a single error can cause costs to spiral. On average, enterprise organisations use 53 different security solutions, which only exacerbates the problems of resource availability.

By trying to maintain current strategies, businesses are often trapped in a cycle of compliance and impulse purchasing - with many opting for highly reactionary strategies which invariably increase risk. This is most prominent in the SME space, where resources are much more scarce and each decision can have a major impact on the implementation of business objectives.

KEY POINTS

For organisations to best tackle the winding road of the threat landscape without compromising on business objectives, cybersecurity needs to be seen and understood as a tool for enabling growth securely.

Knowledge

Organisations often have limited real knowledge of their threat exposure, meaning discussions around cybersecurity relate only to compliance or to abstract risk. Knowing your security posture is key to making informed decisions.

Understanding

When the data is available to make informed decisions, it is key to relate them to business risk and objectives. Ensuring cybersecurity is tackled as a business priority can shift the paradigm from reactive, to an enablement strategy.

Governance

As business adopt their strategies, ensuring they take into account the shifting nature of tactical objectives and moulding the cybersecurity strategy to retain compliance while enabling business becomes the key focus of governance

Q-SEC PATH TO SECURITY

Consult & Advise
CISOaaS
Audits
Penetration Testing
Build Reviews
Phishing Tests
Cyber Awareness
Incident Response

Design & Architect
Architecture
Segmentation
HLD/LLD Design
Process Overhaul

Deliver & Implement
Engineering
Installation
Configuration
SOAR builds

Monitor & Manage
SOCaaS
MDR
Managed Services
Response Retainer
Threat Hunting

Govern & Improve
Service Management
CISOaaS
CIP
Compliance

At Q-Sec, we aim to provide a tailored service built around the specific requirements of our clients. Whether at the beginning of their journey to implementing their cybersecurity strategy, or looking for the next level of secure operations through trusted partnerships - our offering is designed to tackle all of the issues our clients can face.

Our management consulting team is supplemented by the SOC to ensure validation of all technical findings, and our customers have constant direct access to our expert teams across the EU.

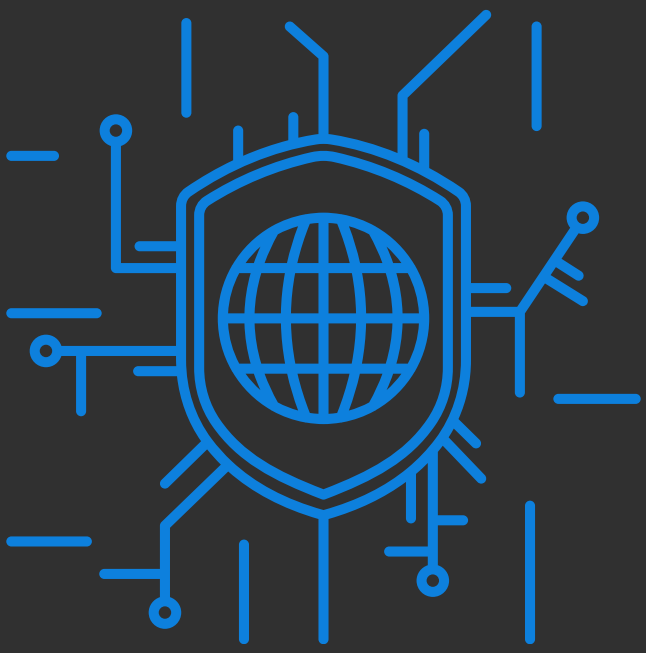
All services are fundamentally constructed with the objective of reducing risk while achieving business objectives - whether on grounds of compliance, maturity, or competitive edge.

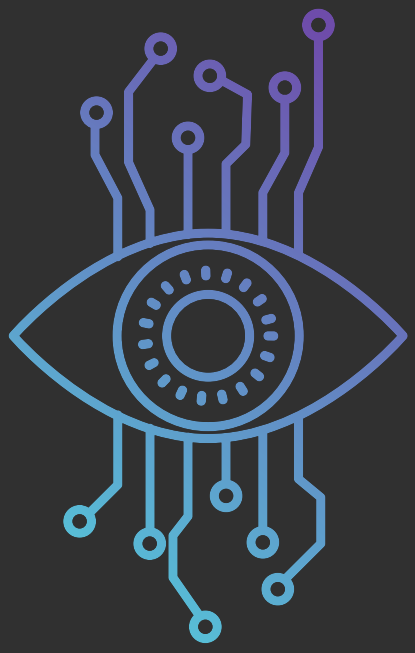
CONSULTING & ADVISORY SERVICES

In the current business environment, all organisations need the insights provided by cybersecurity experts. However, such resource is often difficult to find, budget, and give the necessary support to. The Q-Sec consulting team is here to provide that vital knowledge and advice, supported by a 24*7 Security Operations Centre team for data validation and technical insights.

Assessments

Whether its Penetration Testing, interviews with staff, Threat Hunting, OSINT investigations, Darkweb crawling, or Phishing simulations - the Q-Sec team has both the knowledge and tools to provide a full picture of the current security posture of any organisation. After any such engagement the client receives a full report of findings, including tactical and strategic recommendations for improvements - prioritised based on compliance requirements, risk, and business objectives.



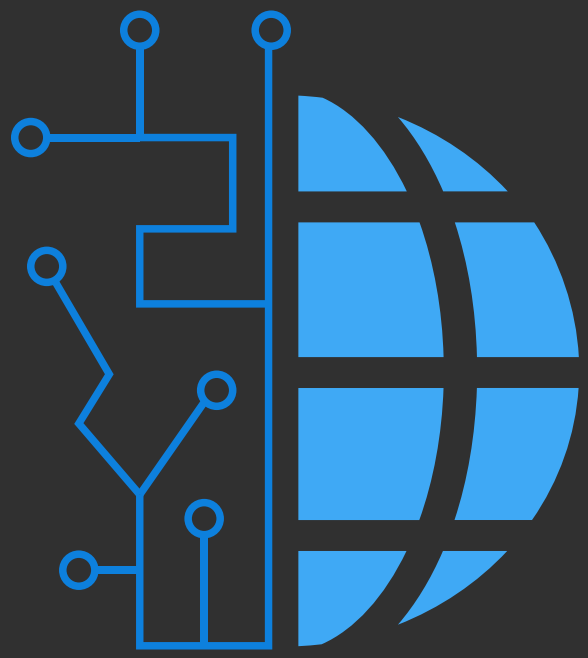


Awareness

At the heart of any organisation are its people. That also makes them the number one target and weakness in relation to cybersecurity. Through an engaging and mature cybersecurity awareness programme, companies can dramatically reduce their risk - as staff will be better equipped to identify threats or attacks. Often supported by phishing simulations and social engineering engagements, these services focus on improving the maturity of any client's teams to ensure cybersecurity is not considered an afterthought.

CONSULTING & ADVISORY SERVICES

Incident Response



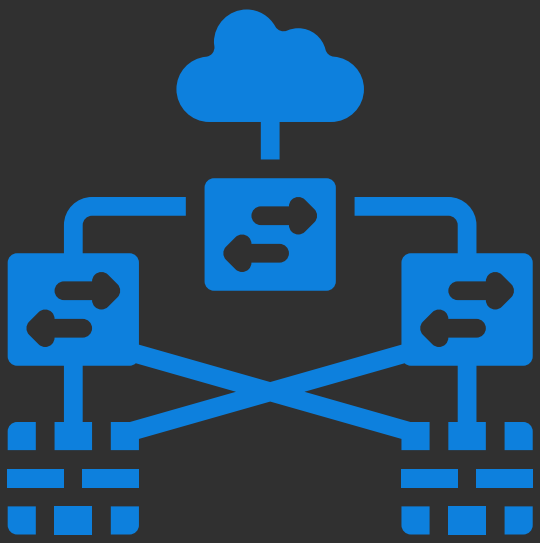
Often, in dire circumstances, a business may become the target of an attack that succeeds in causing damage or forces the invocation of remedial actions. If such a company doesn't have internal resource to tackle the scenario, Q-Sec Incident Response team can assist. This includes support in remediation, crisis communications, restoration of data (if possible), post-incident reporting, and creating any necessary summaries based on client and regulatory requirements. Whether as an on-call 'retainer' service, or an emergency call-out - the Q-Sec team is available to anyone facing an attack.

CISOaaS

For companies that need that vital expert resource to help design, document, and govern their cybersecurity strategy - but cannot justify expanding the permanent internal team - this service is that specialist pair of eyes. Working with business leadership, the detailed strategy is drawn up and aligned to the goals of the organisation. It is focused on building trust in the cyber team, while at the same team enabling the client to operate securely and in line with regulatory standards in their region.

DESIGN & ARCHITECT

This is a critical part of any service delivered by Q-Sec, as without accurate and documented architecture a project may fall far short of the objectives. From visual architecture of networks, through process design using global standards in incident management and response, all the way to network redesign programmes - Q-Sec have the entire breadth of skills necessary to design a solution specific to the needs of our clients.

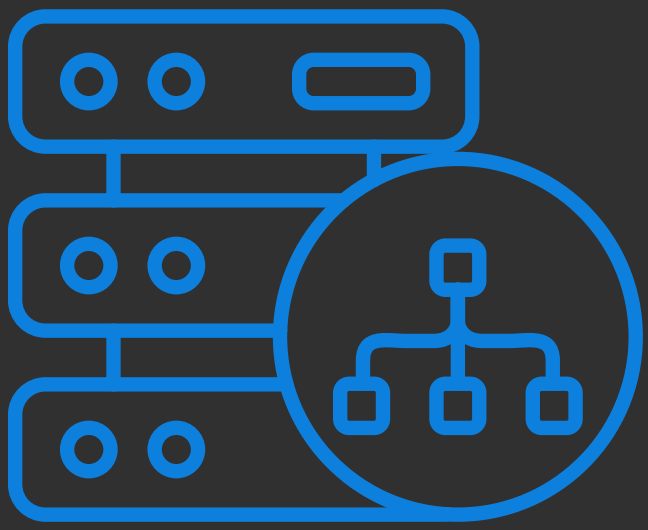


As part of service

All implementation plans from Q-Sec detail the relationship between any monitoring and response tools and the client's infrastructure. This not only provides absolute clarity prior to deployment, but it also resides at the heart of accountability for the delivery of the service. Both for compliance and peace of mind, we ensure complete transparency.

Standalone

As organisations grow organically and through M&A activities, the complexities of networks grow exponentially. Our specialist understanding of countless underlying deployment fabrics allows for the unique service of creating network maps and re-design strategies - with clarity and security in mind. This includes insights into shadow IT, legacy networking, and optimal network segmentation.



DELIVERY & IMPLEMENTATION

Installation and configuration lie at the heart of any IT provider, and at Q-Sec we are no exception. With a wide range of technological partnerships, we are able to support our clients with hands-on skills and optimal solutions.

TECH
PARTNER
LOGOS

Strategic Partnerships

Built over the years, our close partnerships allow for specialist support to be deployed whenever needed when setting up environments for our clients. any solution deployed is chosen based on not only immediate fit, but also with the future in mind - making sure businesses can focus on what matters, in the knowledge that the infrastructure will support it for years to come.

Strategic skills

Over years of experience, our senior consultants have built a wide range of specialisations across all our strategic solution partners. This is to build that vital confidence not only in front of our clients, but to highlight the close relationship we have with our technologies.

CERT
LOGOS

MONITORING & MANAGEMENT

As the requirement to be able to identify and respond to threats is greater than ever, the various solutions have to be able to cater to unique operation models. With that in mind, the Q-Sec team has built a series of delivery models that can all be further customised to tackle the objectives of our clients.

Tier 1: Monitor & Alert

For organisations wishing to take that first step into gaining visibility into activities in their network, Q-Sec provide an initial system of alerting on suspicious activities. By gaining insight into what is taking place not just at the network perimeter but also at its core, our clients can better gauge the need for more advanced services. With human-understandable and plain-English descriptions of events and possible incidents, such a service is a natural first step towards improving the security posture of your business.

- Technical nodes deployed to gain insight into traffic and activities
- Strategic devices and network segments chosen to ensure highest value
- False-positive alerts filtered out by Q-Sec analysts, increasing accuracy of service
- Alerts on possible incidents sent to client via email or phone, depending on severity
- Limited triage done by Q-Sec team

Tier 2: SOCaaS

The majority of organisations require many, if not all, of the functions of a SOC (Security Operations Centre). However, with human resource being difficult to secure and retain, the management overheads as well as costs often lead to businesses accepting the risk of lacking such a service. As this strategy is not sustainable, SOC-as-a-Service is the best solution both for security and economy. With a fully staffed SOC, Q-Sec are able to provide the triage, corroboration, and behaviour analysis vital to any business.

MONITORING & MANAGEMENT
Tier 2: SOCaaS Components

Event Monitoring

All devices and services that are connected to the Q-Sec SOC are monitored 24*7 using a purpose built blend of home-written rules in monitoring engines, behaviour analytics, and identifiable indicators of compromise. These are stored based on individual client and regulatory standards requirements. Q-Sec work closely with the client to identify the most valuable data sources.

Triangulation

Events that trigger certain thresholds, or indicate suspicious and/or abnormal behaviour are investigated by senior analysts and may be escalated to an incident. These are classified based on the Low/Medium/High/Critical categories, and follow-up activities are triggered depending on the incident. Depending on the incident, basic Threat Hunting activities may be included to maximise the accuracy of any incident data.

Notification and Support

The client is contacted based on the agreed communication strategy, with all necessary information allowing for initial remediation/containment activities. All activities are tracked using Incident Management tools, and the client receives constant support from the Q-Sec team during remediation actions - up to and including incident closure. This support, however, remains remote and is primarily advisory - as Response activities are the key aspect of MDR services, not SOCaaS.

Reporting and CIP

As part of ITIL-certified Service Management, the client receives a full incident summary monthly or quarterly, depending on the agreed requirement. This is followed up by timely Service Review meetings, during which opportunities for optimisation of the monitoring are discussed, any service issues are raised, and any CIPs (Continuous Improvement Plans) are tracked.

MONITORING & MANAGEMENT
Tier 3: MDR

Tier 3: Managed Detection & Response

When needing a true partnership, with the capability to dramatically increase cybersecurity through immediate incident response and proactive monitoring, the MDR service is the ideal solution. Going far beyond information and support, MDR allows for Q-Sec to perform traffic filtering, ongoing research into the threat exposure of the client, initiate remediation actions instantly, and have pro-active process management.

- Access to SOC Analysts
- Cyberthreat monitoring 24*7
- Threat Intelligence and Threat Hunting led by senior consultants
- Security Incident Reports
- Threat Containment and Response
- Service Management and Service Reporting
- Incident Response

Tier 3: Managed Detection & Response additional components

Threat Intelligence & Threat Hunting

The Q-Sec strategic partnerships provide ongoing and real-time threat intelligence which supplements the updates driven by investigations. This is further enhanced by activities looking for persistence mechanisms, suspicious application usage/network activity or the tactics and techniques and procedures ("TTPs") of threat actors. When a threat is detected, a security analyst will create a security incident and notify the client

Threat containment & response

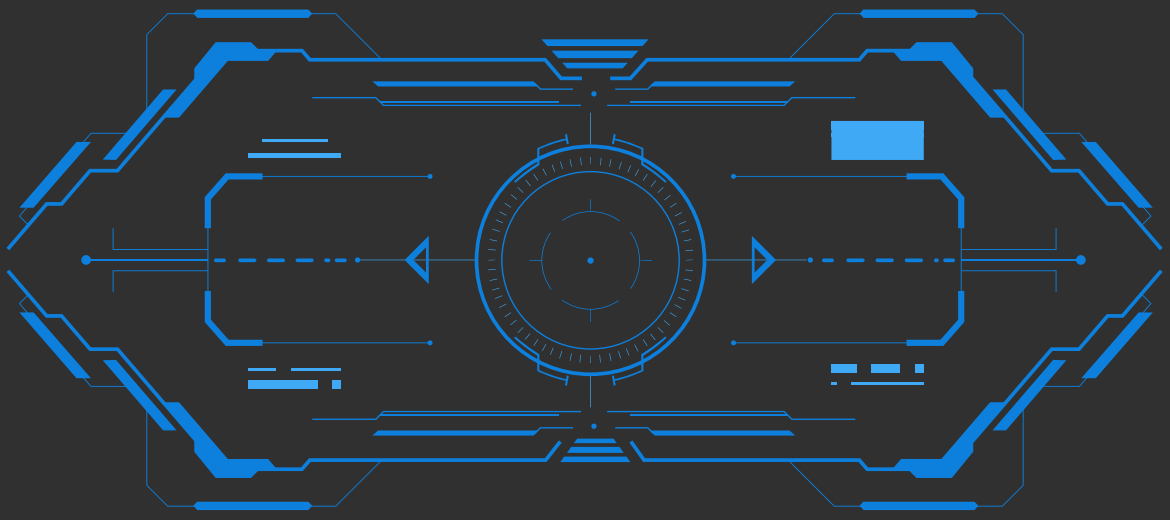
In the event where Q-Sec have access to various immediate response mechanisms, these are used according to agreed processes to contain and remediate against any malicious activities. In most cases, this requires constant communication with the client to provide any support necessary, such as manual device disconnection or local access.

MONITORING & MANAGEMENT
Tier 3: MDR

Incident response

When an incident is identified, an investigation takes to confirm the severity and nature of any threat. This uses relevant telemetry data, and evidence data, threat intelligence, as well as any other data and information sources available to the leading analyst. Using this information and appropriate automation capabilities of the deployment, the analyst then determines the nature and extent of any compromise which may have occurred. Depending on the nature of the potential threat, activities conducted during the process of the investigation may include:

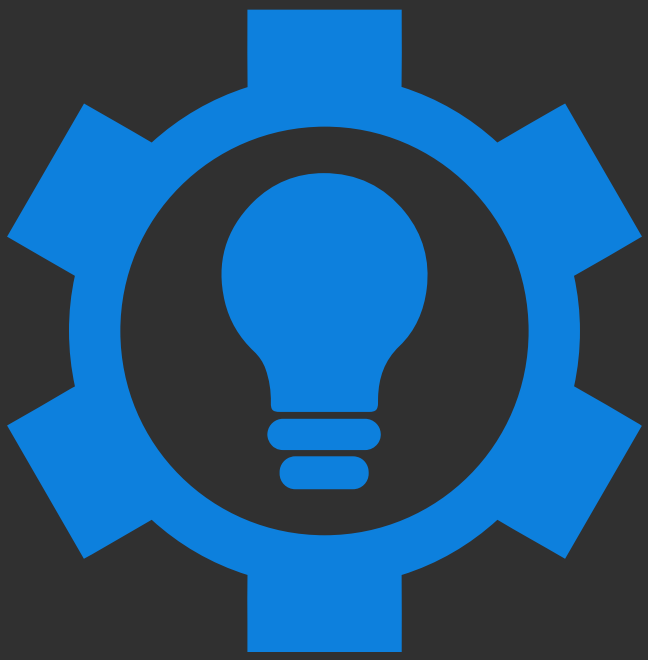
- Threat analysis
- Threat hunting
- Risk assessment of the events taking place
- Contextualisation of threats based on factors such as industry vertical and geopolitical context
- Categorisation according to industry best practice frameworks including MITRE ATT&CK
- Forensic analysis
- Malware analysis; and
- Recommendation to the Client of a suggested response covering suggested next steps

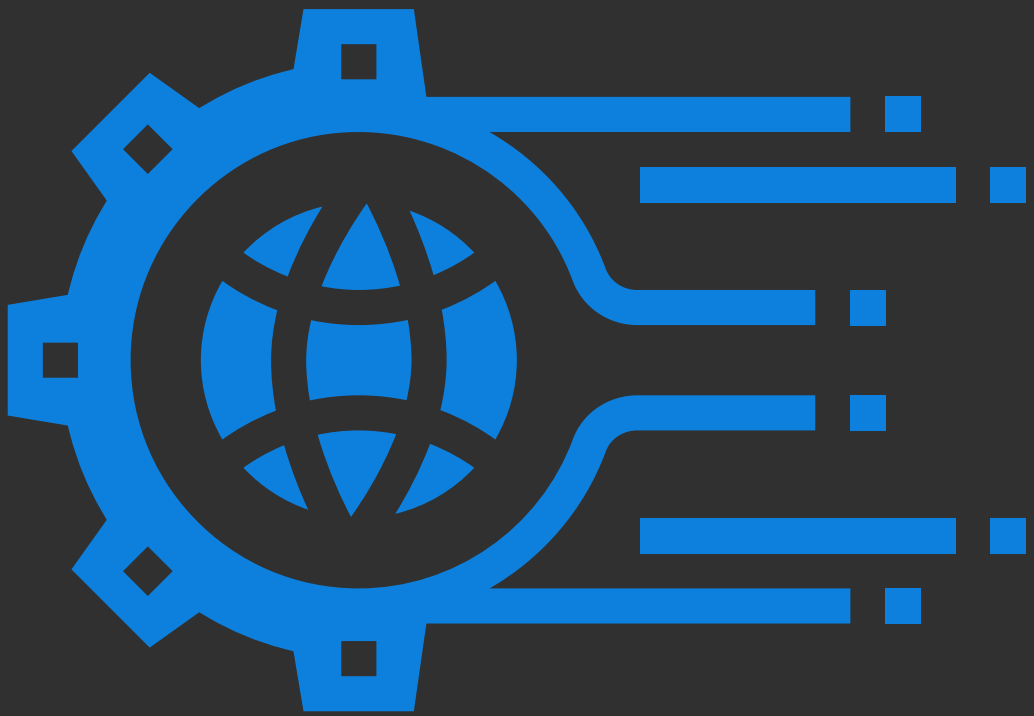


MONITORING & MANAGEMENT

Specialist Services

At Q-Sec, we are aware that there are many very unique circumstances that may require support which cannot be classified in general datasheets. From the management of only specific aspects of a security estate, through HVA (High-Value-Asset) protection using honeypots and web crawling, to the darkweb monitoring for threats against the organisation. Should something specific be needed, it is always worth discussing and depending on the structure of the engagement, solutions may be built to fit the circumstances - such as the creation of a sector-specific L3 SOC team focused on supporting only in the event of Critical threats or complex attack vectors.





GOVERNANCE

Service Value

Co-creating value through strategic partnerships is the most mature and sustainable way to ensure secure business growth and alignment to objectives. Through the ITIL Service Value System, Q-Sec ensure that any and all operations take into account iterative improvements and building on past success. To ensure all continuous improvement processes, all services take into account the need for open and clear communication channels with all parties involved. This is done in a number of ways.

Timely Communication

In the event of high-importance communication, Q-Sec will directly reach out in real time. Otherwise, regular Service Reviews, Quarterly Reviews, and internal Reviews are held to ensure highest quality of value co-creation.

Operational Synergy

All services effecting various business units must have established an understanding of the needs and objectives of the business unit. As these shift and evolve, modifications are implemented and enacted without delay.

Realtime Metrics

All governance is built on accuracy of data and KPI's. Ensuring responsibility and accountability through SLA's, Q-Sec are able to support all governance activities with data.

Economic Governance

Predictability of costs, and the necessity to optimise, are critical to any partnership - both due to economic needs, and the establishment of trust. Through clear cost analysis, Q-Sec ensure lasting and sustainable relationships.

Q-SEC

For inquiries, contact us.

www.q-sec.eu
sales@q-sec.eu