Valcon
70 Gracechurch St,
London EC3V 0HR

valcon.com

Valcon G-Cloud Lot 3
Service Definition

SecOps Services

[Security Services | Security strategy, Security risk management, Security design, Security incident management, Security audit services, Security quality assurance (QA) and testing, Other]

Version 1.0

1. About Us

Valcon is a leading European consultancy specialising in AI and data-driven business transformation, with a growing and established presence in the UK. A trusted partner to major organisations including multiple UK Government departments and public sector agencies. Valcon connects strategy and operations, helping organisations create value in their transformation programmes.

With over 1,750 consultants across Europe, Valcon brings deep expertise across data, AI, technology and consulting. In the UK, Valcon works with clients across financial services, public sector, retail, industrials and infrastructure. Valcon is backed by private equity firm Rivean Capital.

2. Service Description

SecOps Services integrate security practices with IT operations to manage and enhance an organisation's security posture. In today's threat landscape, traditional security measures are insufficient to counter the evolving cyber threats. SecOps employs continuous monitoring, incident response, vulnerability management, threat intelligence, security automation, and compliance management to address security challenges.

Features

- Continuous monitoring of network traffic and system logs
- Incident response planning and execution
- Vulnerability management and patch prioritisation
- Threat intelligence gathering and analysis
- Security automation for process efficiency
- Compliance management with industry regulations
- Integration of security practices with IT operations
- Focus on real-time detection and response to security threats
- Emphasis on collaboration between security and operations teams
- Alignment of security efforts with business objectives

Benefits

- Enhanced security posture and resilience against cyber threats
- Real-time detection and response to security incidents
- Improved efficiency and effectiveness of security operations
- Reduction of security risks and vulnerabilities
- Alignment of security efforts with business objectives
- Compliance with industry regulations and standards
- Automation of routine security tasks for process efficiency
- Integration of security practices with IT operations
- Collaboration between security and operations teams for holistic security management
- Protection of assets and data against unauthorised access and breaches

3. Approach

Delivering SecOps services to a client typically follows a structured approach. Below are the phases commonly used, along with tasks under each phase.

Initiation Phase:

- Define project objectives, scope, and success criteria.
- Identify key stakeholders and establish communication channels.
- Conduct a kickoff meeting to align expectations and goals.
- Develop a project charter outlining roles, responsibilities, and timelines.

Assessment Phase:

- Conduct a comprehensive assessment of the client's existing security posture, including systems, applications, networks, and processes.
- Identify security risks, vulnerabilities, and compliance gaps through vulnerability assessments, penetration testing, and security audits.
- Analyse threat intelligence data to identify potential threats and attack vectors targeting the client's environment.

Strategy Development Phase:

- Develop a SecOps strategy tailored to the client's specific needs and objectives.
- Define security goals, objectives, and key performance indicators (KPIs) to measure the effectiveness of the SecOps program.
- Establish security policies, standards, and procedures aligned with industry best practices and regulatory requirements.
- Develop incident response and escalation procedures to ensure swift and effective response to security incidents.

Implementation Phase:

- Implement security controls, technologies, and tools to improve the client's security posture.
- Deploy security monitoring and detection systems, such as SIEM (Security Information and Event Management) and IDS/IPS (Intrusion Detection and Prevention Systems).
- Configure security policies and access controls to enforce least privilege and ensure data confidentiality, integrity, and availability.
- Implement security automation and orchestration to streamline security operations and response processes.

Training and Awareness Phase:

- Provide training and awareness programs to educate employees and stakeholders about security best practices, policies, and procedures.
- Conduct phishing simulations and security awareness training to help employees recognise and respond to security threats effectively.
- Promote a culture of security awareness and accountability throughout the organisation.

Monitoring and Response Phase:

- Continuously monitor the client's environment for security incidents and anomalies using automated tools and manual analysis.

- Investigate and respond to security incidents promptly, following established incident response procedures.
- Coordinate with internal teams and external stakeholders, such as law enforcement or regulatory agencies, as needed to address security incidents.

Continuous Improvement Phase:

- Conduct regular reviews and assessments of the SecOps program to identify areas for improvement and optimisation.
- Implement lessons learned from security incidents and audits to enhance security controls and procedures.
- Stay informed about emerging threats and technologies to adapt the SecOps program to evolving security challenges.

Reporting and Documentation Phase:

- Generate regular reports and dashboards to communicate security metrics, KPIs, and trends to stakeholders.
- Document security incidents, response activities, and lessons learned for post-incident analysis and compliance purposes.
- Provide recommendations and actionable insights to help the client improve their security posture and achieve their security goals.

By following this structured approach, organisations can effectively deliver SecOps services to clients, helping them enhance their security posture, mitigate risks, and protect against evolving cyber threats.

4. Effort and Cost

Effort will be determined collaboratively between the Valcon and the client based on the skills mix and scope required.
Please refer to the Pricing Document for current rates.

- Rate card prices are exclusive of VAT.
- Expenses are recharged at cost and supported by receipts.
- Expenses may include reasonable travel, accommodation, and subsistence costs.
- The payment schedule will follow milestone completions as agreed in the Statement of Work.

5. Assumptions

The successful delivery of the engagement depends on assumptions and dependencies jointly agreed between the Valcon and the client.

- These may include (but are not limited to):
- Access to required stakeholders, systems, or information
- Timely decisions and approvals
- Availability of resources and infrastructure
- Defined governance and communication processes

All assumptions and dependencies will be recorded and validated as part of the Statement of Work (SoW).