# SOC & SIEM

VODAFONE BUSINESS SECURITY ENHANCED

BUSINESS
SECURITY
ENHANCED

BUSINESS
SECURITY
ENHANCED

Together we can
vodafone
business

# SOC & SIEM

## Service Definition

### VODAFONE BUSINESS SECURITY ENHANCED (VBSE)

As a dedicated cyber security partner, we offer comprehensive solutions to give customers a clear path forward, connecting and helping to protect their data, networks and the cloud from breaches or attacks. Based in dedicated secure locations and staffed by security cleared personnel from the account management team through to design, installation, and operations you can be sure your organisation is protected.

We combine our expert people, processes, and technologies to help support and defend the UK's critical national infrastructure, the public sector, government, defence, and large corporate enterprises.

### CYBER SECURITY MONITORING, ALERTING & REPORTING

The VBSE managed SOC & SIEM service is a set of sub-services that form part of our managed detection and response capability that uses a combination of techniques to detect anomalous behaviour on Monitored Assets. Our 24x7 managed SOC & SIEM service receives security event logs from your equipment. These events will be assessed via our Security Information and Event Management (SIEM) platform, with any events flagged as potential security incidents assessed by our Cyber Security Analysts within our Security Operations Centre (SOC) and, by pre agreed playbooks how they are responded to.

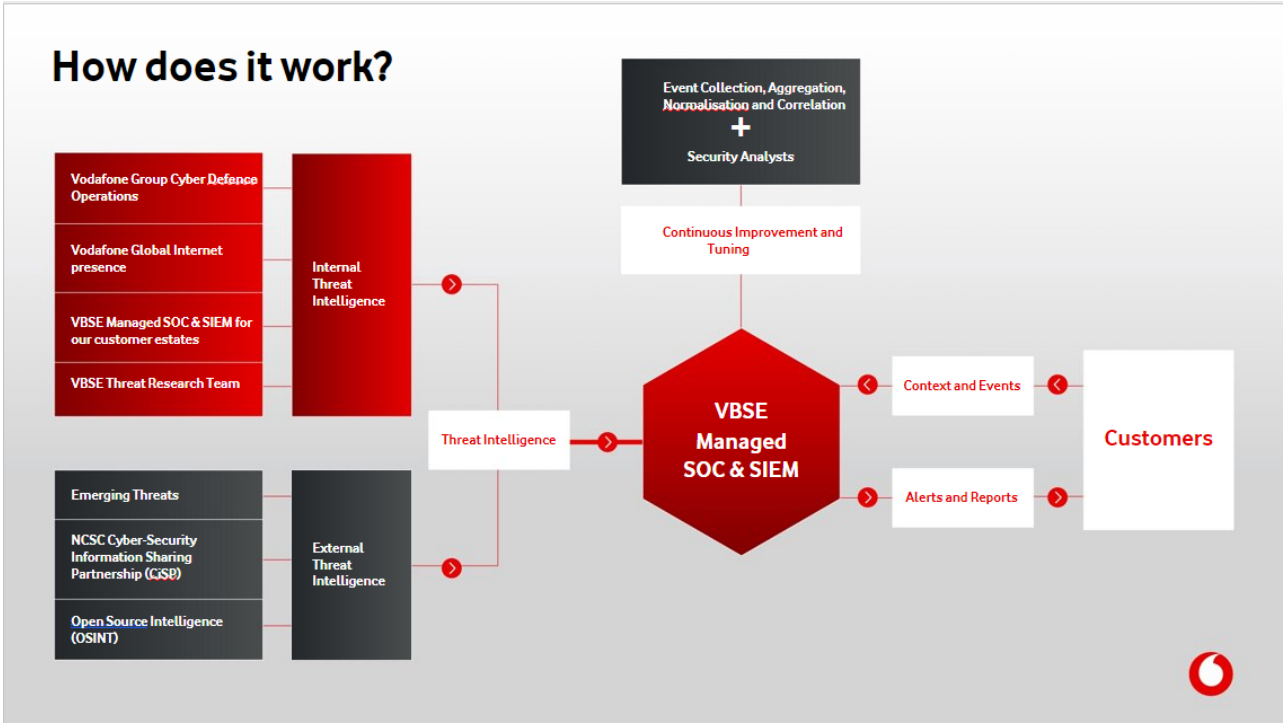
The service includes security incident alerts and monthly security reports.

### Service Overview

As a first step, establish a clear understanding of risk posture and the key issues that the customer faces or is likely to face based on threat intelligence including emerging threats. We will then have the context required to make specific recommendations relating to the monitoring and response options available to you.

During this phase we will discuss business objectives and operating processes to understand the:

- Business strategy and goals as well as expectations for future cyber security maturity
- Technology requirements that support the strategy
- Current and future security requirements
- Identify key risk management approach and agree on risk evaluation criteria (e.g. impact, probability, severity)
- Through design agree the events per second (EPS) to be sent
- Agree the response
- Define the scope of the project
- Identify the high-level data (information) assets owned, managed and utilised
- Identify critical systems and services (supporting assets) owned, managed and utilised




## SECURE MANAGEMENT

Our management systems and staff are housed in highly secure environments that have NCSC Tailored Assurance (CTAS).

Our service benefits from proven good practice security across the physical, personnel, procedural and technical domains. Vodafone business is also a corporate member of the UK Cyber Security Council.

## RELIABLE

Our geo-resilient Security Operations Centre (SOC) monitors the service 24 x 7 x 365 ensuring rapid notifications to incidents and threats.

## DESIGNED, DELIVERED AND MANAGED BY VODAFONE SECURE SECTOR

- Security cleared staff
- Verified by NCSC verified CHECK security testers
- Certified professionals
- Secure locations
- Secure systems & processes

## KEY FEATURES

- Log collection
- Log storage in a specialist database (SIEM)
- Analysis of logs to identify Events of Interest (EOI)
- Behavioural alerts based on single or multiple EOI
- Incident detection, investigation and notification
- Continuous analysis to produce incident reports
- Validated technology from trusted suppliers
- UK Sovereign on-premise
- Managed by UK Security Cleared experts

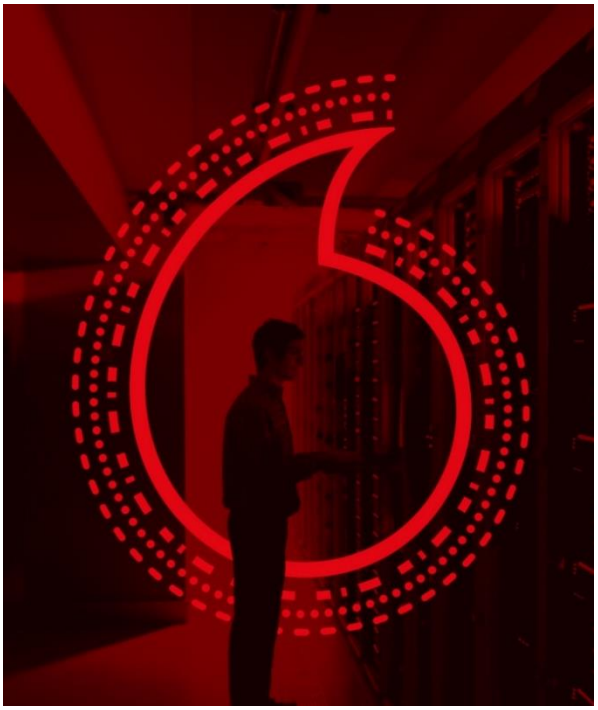
## SERVICE SUPPORT

We provide a fully managed service that is proactively monitored and maintained 24x7x365 by the VBSE SOC. Key features of the service support include:

- Aligned to NCSC & MITRE best practices
- Monthly routine security reporting
- Aligned to ITIL and ISO 20000 standards
- Our management systems and staff are housed in highly secure environments that have NCSC accreditation

## BENEFITS

- Vodafone can meet your security requirements
- Flexible to ensure the right solution is deployed
- Threat intelligence from multiple sources
- Proactive monitoring and 24 x 7 x 365 fault management
- Customised reports and support for systems and applications
- Service level availability guarantees to ensure uptime
- Customised service offering providing extra flexibility



## SERVICE LEVEL MANAGEMENT

We have a tailored support model for Service Level Management delivering:

- KPI and SLA performance reporting
- Regular operational service reviews
- Continual service improvement
- Problem and trend analysis
- Service development
- Customer satisfaction surveys
- Optional regularly meetings with assigned SOC Analyst
- Options to purchase additional complementary services such as Retained Incident Response (RIR) under a separate agreement, where our experts will work with you to respond to any breach and get your business back up and operating as normal.

## TARGET SERVICE LEVELS AVAILABILITY

| FIX TIMES | | |
|---|---|---|
| Sev 1 | Critical | 4 Hours |
| Sev 2 | Significant | 8 Hours |
| Sev 3 | Minor | 48 Hours |
| Sev 4 | No Service Impact | 72 Hours |

| AVAILABILITY | |
|---|---|
| 99.99% | Resilient Log Collection Environment |
| 99.97% | Non Resilient Log Collection Environment |

# Why Vodafone

Benefit from ongoing threat detection and response 24/7/365, with all work carried out by our security cleared experts who understand the current threat landscape

We work with some of the Gartner MQ Leaders for Network Firewalls, including Fortinet and Palo Alto

https://www.fortinet.com/solutions/gartner-network-firewalls

24x7 monitoring and incident reporting providing near real-time threat analysis across your network

25+ years securing Critical National Infrastructure organisations, intelligence agencies, government departments, defence contractors and transport and utility companies

UK CYBER SECURITY COUNCIL
CORPORATE MEMBER 2024-25

Vodafone named a Leader in the 2023 Gartner® Magic Quadrant™ for Network Services, Global

https://www.vodafone.com/business/news-and-insights/analyst-views/vodafone-named-a-leader-in-the-2023-gartner-magic-quadrant-for-network-services-global

vodafone
business

Together we can