Managed Detection and Response

SERVICE DEFINITION

BUSINESS
SECURITY
ENHANCED

BUSINESS
SECURITY
ENHANCED

Together we can
vodafone
business

Managed Detection & Response (MDR)

Service Overview

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 including government agencies, defence, energy, healthcare and large corporate enterprises.

MANAGED DETECTION AND RESPONSE (MDR)

The VBSE MDR service comprises of our protective monitoring SOC & SIEM service, enhanced with SOAR and UEBA functionality. We use a combination of techniques to detect anomalous behaviour on Monitored Assets then report incidents and take automated actions according to customised playbooks across your environment from our 24x7x365 managed SOC.

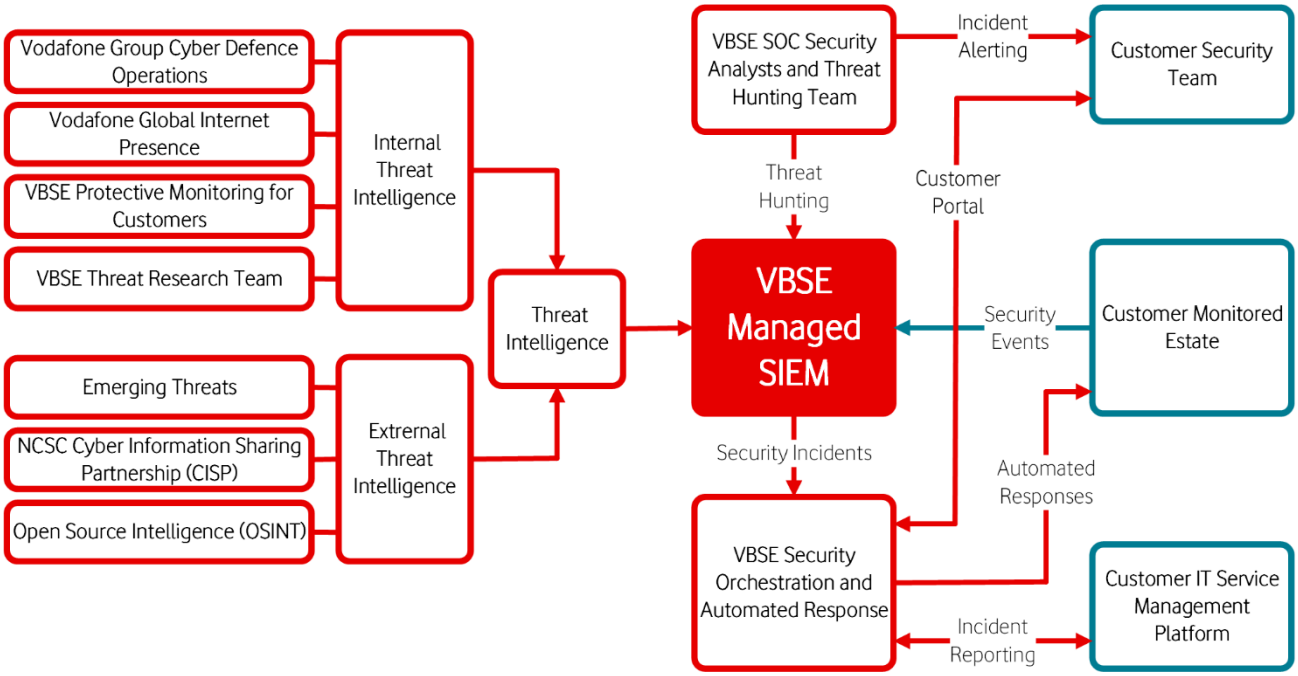
Security events from your Monitored Assets will be ingested, correlated, and analysed by our Security Information and Event Management (SIEM) platform, with any events flagged as potential security incidents investigated by our Cyber Security Analysts within our Security Operations Centre (SOC) and, according to pre-agreed playbooks, alert your security teams and/or carry out automated responses via our Security Orchestration and Automated Response (SOAR) platform.

Our MDR service includes security incident alerting, automated responses, monthly reporting, ITSM integration and access to our customer facing portal, which enables your security teams to view real-time incidents.

Our UK sovereign 24x7x365 SOC, staffed with SC and DV cleared analysts, will work with your technical and security teams to on-board your Monitored Assets into our platform, create baseline traffic patterns, configure use-cases and craft customer specific playbooks, which detail actions for us to take upon detecting security incidents via our SOAR tool.

Our Gartner top-right quadrant SIEM ingests a range of industry standard Threat Intelligence (TI) feeds, further supplemented with data gathered from across our global internet presence infrastructure. This feed allows our SOC to hunt and identify Indicators of Compromise (IOCs) present in traffic routed across Vodafone's Autonomous System (AS), which accounts for 20% of global internet traffic.

At VBSE we strive to forge strong partnerships between our organisation and customers, working closely with your security team to develop a sophisticated and mature MDR service, which enables us to help protect your Monitored Assets.



KEY SERVICE FEATURES

- UK sovereign, fully on-premise platform delivered from secure locations
- 24x7x365 UK based security cleared (SC & DV) SOC staff
- SOC Analysts and our Threat Hunting team carry out IoC detection, incident investigation and alerting
- Remote incident support following incident detection
- SIEM provides real-time event enrichment, analysis, correlation and detection of security threats
- SOAR functionality automates responses and integrates with your ITSM
- Customer facing portal for viewing real-time incident details
- UEBA functionality enhances incident detection
- Service priced using Events Per Second (EPS) and number of devices to be on-boarded
- Ability to ingest security feeds from any device producing Syslog or WEF events
- Ability to ingest security event feeds from devices hosted in public cloud environments
- ISO 27001:2022 accredited
- Cyber Essentials Plus compliant
- Aligned with NCSC best practice guidelines
- Solution verified by NCSC accredited CHECK security testers
- TI feeds from multiple industry standard sources supplemented with data from Vodafone's global internet presence
- Use-cases and incidents aligned with MITRE ATT&CK framework
- Security events retained for 6 months by default (including 1-month hot storage)
- Monthly service and security reporting by default

Managed Detection and Response (MDR) Delivery Phases:

Build Tasks	Onboarding	Baselining	In-Life
Procurement of any software (e.g. virtual firewalls) Building of Virtual Machines (VMs), and customer partition within the SIEM, including reporting set up	Adding assets to be monitored, parsing logs and ingesting logs to the SIEM Creating use case definitions, required reports configuring them in the SIEM, and creating playbook	Refining alert triggers to filter out false positives Improving parsing, use case definition and reports, and updating playbook based on result of monitoring your network	Continuous improvement and any changes via Change Requests

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 to the highest levels
- Continual Service Improvement
- Problem and Trend analysis
- Service development
- Customer satisfaction surveys
- Optional regularly meetings with assigned SOC Analyst
- Options to purchase additional complimentary services such as Retained Incident Response (RIR), where our experts will work with you to respond to any breach and help get your business back up and operating as normal.

SERVICE LEVEL MANAGEMENT

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

- KPI and SLA performance reporting
- Regular operational service reviews

The Support Service is available as shown below:

Support Service	Service Cover Period
Service Incident Management for Severity Level 1 & 2 Service Incidents	24/7
Service Incident Management for Severity Level 3 & 4 Service Incidents	Working Hours
Service Request Fulfilment	Working Hours

The following severity level classifications apply to the Service:

Severity Level	Severity Level Description	Severity Level Definitions
1	Critical	A total loss of the Service. E.g. The Vodafone SOC is unable to process or receive Security Event Logs.
2	Significant	Partial loss of the Service which has a significant detrimental effect on Vodafone's ability to perform normal operations but which does not represent a total loss of the Service. E.g. SIEM persistently fails to connect to Security Event Log aggregator server or does not receive Security Events from Security Event Log aggregator server within the expected period.
3	Minor	Degradation of Service, such as loss of resilience, including a severity Level 1 or 2 Service Incident where Vodafone has been denied access to a Customer Site or Managed Asset or where Vodafone has been unable to agree a period of maintenance activity (for reasons outside Vodafone's reasonable control) to restore normal service.
4	No service impact	Any Service Incident not classified as severity level 1, 2 or 3.

The Target Time to Restore for each severity level is as follows:

Severity Level	Target Time to Restore
1	4 Hours
2	8 Hours
3	24 Hours
4	72 Hours

vodafone
business

Together we can