Managed Threat Detection and Response

Service Definition

boxxe

making
technology
human

Service Definition

making technology ***human***

boxxe makes the global workplace habitable from a technological and human perspective. One does not overrule the other. They function efficiently and effectively together.

We believe in reciprocal adaptation: adapting technology to people and people to technology.

We aim to make organisations the best they can be through technology and by giving every person, wherever they are in the world, the confidence to use that technology to drive efficiency and effectiveness in every aspect of their working lives.

How can we help to make you the best you can be?

Please conserve energy
do not print this document

About Our Service

Service Overview

Managed Threat Detection and Response (MTDR) is a managed security service that provides security monitoring, threat intelligence, incident analysis, incident response and threat hunting.

Based on IBM QRadar and IBM Cloud Pak for Security (CP4S), MTDR will collect data from pre-agreed sources, be that the customers own infrastructure (servers, systems, applications), public cloud providers (AWS, Azure etc) & Private Cloud instances via remote log collection agents and Digital Risk and Endpoints via 3rd Party Vendors Digital Shadows and Sophos.

Any abnormalities are raised by an alarm where trained security analysts and engineers of the boxxe cyber security team, as well as AI-assisted technologies from our vendors, triage and qualify the threat.

Security events are then reported on and managed via the boxxe cyber security team depending on the level of service taken by the customer

- Threat Monitoring and Alerting – boxxe will alert the customer to the issue and support them, through investigations, evidence and information gathering, linking the event to global threats, and resolution advice, if they are at risk. This service will not include any automated response or remediation work.
- Threat Response - As above but with the addition of remediation work. boxxe will act swiftly to mitigate the impact of the attack. This will include automated responses and manual interventions such as threat containment to stop the attack spreading, approved, and agreed security countermeasures (e.g. taking systems offline), implementation of agreed procedures and co-ordination and management of the response. The service will not include remediation of any damage done by the attack on the customer, however support and advice will be provided on how to prevent further attacks
- Proactive Security Management (Threat Hunting) – the customer gets the above 2 reactive services but in addition boxxe will include threat hunting, intelligence gathering and malware analysis to identify zero-day cyber threats that may be lurking undetected on the customer network.

Benefits

The key benefits of the service are:

- Complete Threat Detection across the IT Stack – Provides 24/7 monitoring tailored to the customers network by our expert SOC engineers as the customer can choose what they want monitoring and to what extent.
- Improved Speed and Efficiency – Increases efficiency of incident handling and IT compliance with centralised log collection, analysis, and retention
- Access to a broader range of skills and experience - Just one in four businesses (24%) reported that any of their staff in cyber roles had undertaken training in the last year. Meanwhile around 408,000 businesses (30%) have more advanced skills gaps in areas such as penetration testing, forensic analysis, and security architecture, while over a quarter (27%) have a skills gap around incident response and don’t outsource it (DCMS). Boxxe cab help the customer avoid this skill gap with our team of highly trained, security cleared analysts.
- Greater value from detection technology - A recent survey of security analysts revealed that the average enterprise SOC experiences more than 10,000 daily alerts, with almost third experiencing as many as 1,000,000 per day. This highlights the level of pressure organisations are under, with many underestimating the time it takes to configure and optimise the cyber security technology they buy out of the box. Moving to MTDR negates all those issues as boxxe have done the hard work for the customer fine tuning the technology to get the best results
- Cost Efficiency – Removes the need for a large CAPEX investment for an in-house SOC - Research by the Ponemon Institute suggests that it costs an average of £2.5 million a year to run a SOC. By moving to MTDR the customer can avoid recruitment of hard to find and costly cyber security expertise, therefore reducing costs This is with no loss is security measures as the customers cybersecurity will be even more manageable and cost-effective.

Service Features

Design, Install and Configuration

Design and Install

boxxe will set up the customer on QRadar and will work with the customer to define the correct security policies and implement the config and rule set as outline in the table above.

Once setup is complete boxxe's consultants will notify the customer they are entering a fine-tuning period. boxxe will monitor the incoming logs and data to ensure they are coming through at the correct level and ensure the customer is getting an acceptable level of alerts coming through.

System Integration and Support

No matter the use-case, there is a way to securely monitor it, even if it is an application, or an aging application.

Threat Modelling

The design phase will also include an element of Threat Modelling where we will understand where the customers threats are likely to be before monitoring them.

Playbook Design

boxxe will create Incident Response plans for the customer, including the use of fully automated, or human approved actions

Service Maintenance & Support

24x7 SOC Team

The customer will be given access to our 24/7/365 York based, Security-Cleared and Highly Trained Analysts who will provide the monitoring and management of the service. The team will be available to handle any queries you may have.

24 X 7 Service Desk Portal

The customer will be given access to our Online Customer Service Portal. The Portal will be available for logging incidents 24 x 7 x 365 (subject to downtime for scheduled or emergency maintenance).

Business Hours Service Desk

In all situations, a unique ticket will be raised, a priority level will be allocated, and managed through to completion and acceptance within the Service Desk management system.

Standard operational hours are 08:30 to 17:30, Monday to Friday, excluding UK national bank holidays and the period between Christmas Day and New Year's Day.

Incidents will only be worked on within standard operational hours.

The service desk will be available for:

- Adding or deleting devices on the network
- Adding new rules
- Changing existing alert rule and thresholds
- Ad-hoc requests as required

Quarterly Service Report

boxxe will schedule Service Review meetings every quarter with the customer to discuss Service performance, expected enhancements or extensions, any recommended improvements, and any other applicable requirements.

boxxe will also email the customer with a report showing a breakdown of support requests per category and status, every quarter.

Systems Management

Platform Administration

boxxe will host and manage the monitoring platform (IBM QRadar + CP4S) and ingest the customers logs through remote collection. The boxxe SIEM has an unlimited EPS for customers, however if the customer has made an existing investment (e.g. in Sentinel or their own QRadar) boxxe are also able to look after that SIEM platform for them meaning there is no need for them to sacrifice their existing investment. Boxxe will accept the feeds into CP4S and run using the processes outlined in this service description

Log And Inventory Management.

We ensure that the data we collect is maintained, it is relevant and accurate to your purposes. In the event we lose visibility, we will look to reconnect the device, or onboard it to the service.

Log Retention

boxxe will retain all ingested logs for 6 months for forensic retrieval and to assist in the unlikely event that disaster recovery is required. After 6 months of retention, this data will be overwritten.

Backup & Archiving

Backup and archiving of configuration, log and app data is performed daily to ensure that QRadar may be restored in the event of a fault or catastrophe.

Detection Rule Development

boxxe will perform regular workshops where we engineer rules for the latest threats. The lifecycle involves testing and proving effectiveness before implementing for all customers.

Incident Management & Response

Threat Detection

We will detect qualified and attempted attacks on systems, applications, and related business services. This is achieved through our trained security analysts and engineers for qualification and identification of incidents as well as AI-assisted technologies from our vendors.

Incident Qualification

boxxe will conduct investigations to qualify threats posed and their impact raised by triggered alerts. When an Event arrives in the queue to triage, an analysts will qualify the threat for its legitimacy and in the process, understand the true severity of the Alert.

We will then run the threat through our Qualification process to consider the potential threat of the event against several factors:

- Progress against the Cyber Kill Chain
- MITRE ATT&CK Tactics observed
- Attribution against a known actor (APT)
- Potential Impact against % of users

Incident Alerting and Management.

We then consider that an Event becomes an Incident when there is some remediation work to be carried out by the customer to halt the attack or prevent any residual risk, at that point we will assign a threat category level, CAT 1 (Minor) through 5 (Major).

Depending on the threat category level boxxe will manage the incident in the best way for the threat. The individual alert will be specific to the customer, but an example of the management methods is below

Alert Level	Description & Example	Notification Method

Critical	A critical level alert is a worst-case scenario, defined between P1 to P2 – there is an issue that requires immediate attention. A critical cyber security incident we view as an active threat actor being identified within your environment. We also view any critical system disruption events that prevent us from being able to perform fundamental identification and qualification of threats. In this case, we will notify you of the disruption, but you may not be required to resolve.	Phone Call, Customer Service Portal, and Incident Room.
Medium	A medium level alert conveys that that identified security event on the surface is less of an impactful risk to you but should be looked to be resolved in good time. We also take the view that should any critical log sources stop sending logs to us this impacts our ability to proactively monitor your critical devices.	Email, Customer Service Portal, Analyst Calls, and Daily and Weekly Reports.
Low	We view the least severe events as items that are worthy of note but do not cause any disruption or severe risk, these are meaningful for reporting of ongoing system faults or compliance findings. Should there be many of these in large volumes however, this could cause reason for concern meaning we raise the bulk of events as a medium on qualification of an underlying problem.	Customer Service Portal, Daily and Weekly Reports and Analyst Calls.

Incident Response

24/7 threat containment and triage with incident management and orchestration powered by IBM QRadar & CP4S.

boxxe will act swiftly to mitigate the impact of the attack. This will include automated responses and manual interventions such as threat containment to stop the attack spreading, approved, and agreed security countermeasures (e.g. taking systems offline), implementation of agreed procedures and co-ordination and management of the response. The service will not include remediation of any damage done by the attack on the customer, however support and advice will be provided on how to prevent further attacks

Threat Intelligence & Hunting

Threat Intelligence Feeds

Premium Threat Intelligence Feeds are included in this service, which will provide intelligence of the most relevant early warning indications of threats to the customers operation and sector. As a result boxxe will spot, and report on highly relevant threat actors.

Boxxe will use the following threat feeds (subject to change)

- QRadar X Force
- Open Threat Exchange
- NCSC
- SANS

Threat Hunting

Threat hunting is included in the service, Analysts will proactively perform Threat Hunts for zero-day threats as they break, to find malicious actors in the customers environment that have slipped past any initial endpoint security defences.

Threat Modelling

boxxe will work to identify, communicate, and understand threats and mitigations within the context of the customers infrastructure. The modelling process will include:

- Description of the subject to be modelled
- Assumptions that can be checked or challenged in the future as the threat landscape changes
- Potential threats to the system
- Actions that can be taken to mitigate each threat
- A way of validating the model and threats, and verification of success of actions taken

Threat Awareness

boxxe will provide regular reporting and communication of threats of significance and trending data.

Service Tiers

The customer will be able to choose levels as service from the below:

Area	Feature	Threat Detection	Threat Detection and Response	Threat Hunting
Design, Install and Configuration	Design and Installation	✓	✓	✓
	System and Integration and Support	✓	✓	✓
	Threat Modelling	✓	✓	✓
	Response Playbook Design		✓	
Service Maintenance & Support	24X7 SOC Team	✓	✓	✓
	24 X 7 Service Desk Portal	✓	✓	✓
	Business Hours Service Desk	✓	✓	✓
	Quarterly Service Report	✓	✓	✓
Systems Management	Platform Administration	✓	✓	
	Log And Inventory Management	✓	✓	
	Log Retention	✓	✓	
	Backup & Archiving	✓	✓	
	Detection Rule Development	✓	✓	
Incident Management & Response	Threat Detection	✓	✓	
	Incident Qualification	✓	✓	
	Incident Alerting and Management	✓	✓	
	Incident Response		✓	
Threat Intelligence &	Threat Intelligence Feeds	✓	✓	✓

Hunting	Threat Awareness			✓
	Threat Modelling			✓
	Threat Hunting			✓

Your Support

This chapter identifies and describes the high-level components that make-up the service.

Pre-Requisites

No specific pre-requisites for this service to be offered or delivered, however a full assessment and implementation design must take place for boxxe to be able to accept a service into live.

Service Hours

Standard Operating Hours are 08:30 to 17:30, Monday to Friday, excluding UK national bank holidays and the period between Christmas Day and New Year's Day.

Incidents will only be worked on within Standard Operating Hours unless otherwise agreed. boxxe can provide OOH or 24 x 7 support under certain circumstances, but these are not regular terms and need to be agreed separately in writing.

Additional support agreements can be made to cover exceptional periods such as Christmas, but these are not regular terms and need to be agreed separately in writing.

Pricing Terms

For all service variations the customer is charged based what parts of the customer infrastructure will be monitored. Pricing will also factor in the level of cover the customer requires, duration of cover and SLAs required.

Onboarding

boxxe will follow a standard onboarding process to set up your MTDR environment.

Upon go-live boxxe will provide Early Life Support. Early Life Support is a period of "hyper-care" immediately following transition of the managed service to boxxe. This period is used to closely monitor the service and provide increased resources to address post-transition issues, blockers, or bottlenecks with the aim of rapid remediation, mitigation, or implementation of a workaround whilst a longer-term solution is identified.

After Sales Support

Service Review Meetings

boxxe will schedule regular Service Review meetings to discuss Service performance, expected enhancements or extensions, any recommended improvements, and any other applicable requirements.

Your allocated boxxe Service Manager will be the primary point of contact for all management issues relating to the Managed Service provided by boxxe.

The Service Delivery Manager will provide:

- SLA Management
- Vendor and Third-Party Management
- Continual Improvement and Service Improvement Plans (if required)
- Major Incident reports including interim reports and subsequent Root Cause Analysis
- Service Review Reports

The Service Manger will also arrange, chair and minute regular Service Review meetings. The primary purpose of these meetings will be to review the performance of the managed service against the SLA.

Reporting

boxxe is dedicated to the delivery of quality products and services. All calls and emails to the boxxe Service Desk are categorised, reported, and reviewed each month by the Service Manager. boxxe uses this information to measure the quantity and priority of outstanding incidents, and the quality of service. Our processes are continuously reviewed to ensure they are effective and efficient in their delivery.

Service Management

Service Desk

The boxxe Service Desk will provide a first line point of contact for the management of IT incidents and requests.

The boxxe Service Desk operates within the ITIL best practice framework.

The Service Desk can be accessed by the Online Customer Service Portal or via telephone or email. The Customer Service Portal will be available for logging incidents and requests 24 x 7 x 365.

The Service Desks key functions will be to:

- Receive inbound incidents and requests from authorised personnel
- Record details of incidents and requests within the ITSM tool
- Resolve the incident or request at First Contact where possible
- Allocate the call to the correct Resolver Team where a First Time Resolution is not possible
- Provide regular updates to the caller or other authorised parties as appropriate
- Notify the customer when the incident or request has been resolved
- Monitor progress of incidents and requests to ensure they are being progressed to resolution

Incident Management

The primary goal of Incident Management is to restore normal service operation as quickly as possible and to minimise the adverse impact on business operations; thereby ensuring that the best possible levels of service quality and Availability are maintained

In all situations, a unique ticket will be raised, a priority level will be allocated and managed through to completion and acceptance within the ITSM tool.

Standard Operational Hours are 08:00 to 18:00, Monday to Friday, excluding UK national bank holidays and the period between Christmas Day and New Year's Day.

Incident Management Process

Incident Identification

Incidents can be reported to the Service Desk in several different ways:

- Customer email – servicedesk@boxxe.com
- Telephone – 01904 809 820

- ServiceNow Portal – https://service.boxxe.com/csm

Incident logging

All Incidents will be logged into the boxxe Incident Management System (IMS).

Each incident will include the following information as a minimum:

- Unique Reference Number (System Generated)
- Customer Contact Details
- Incident Category (See Incident Categorisation)
- Incident Priority (See Incident Prioritisation)
- Incident Description
- Incident Status
- Incident Resolution Description

Incident Diagnosis

Resolver Groups will investigate and diagnose incidents and will record details of actions taken in the IMS.

In the first instance, the Service Desk Analyst will carry out initial diagnosis to determine the cause of the issue.

Should the analyst not be able to resolve the incident within they will pass this to another Resolver Group for Resolution. Where incidents need to be escalated to the vendor, boxxe will put the incident on hold whilst the vendor investigates a resolution.

Incident Resolution

Once a potential resolution or workaround has been identified it is applied and tested. The Incident record will be updated with the relevant information, detailing what investigation work was undertaken, what resolution and testing was done and whether this was successful. Where a workaround is in place without a root cause, the incident will be closed, and a Problem ticket will be raised.

Incidents in a Resolved state can be reopened if the issue has not been resolved correctly. However, if an Incident is left in a Resolved state for more than 5 days, this Incident will be automatically closed. A Closed Incident cannot be reopened, and a new Incident will need to be logged.

Incident Closure

The Service Desk will check that the incident is fully resolved and that the users are satisfied and willing to agree the incident can be closed. At this stage the Service Desk will close the ticket and an email will be sent to the user confirming the status of the ticket. The ticket can no longer be reopened.

Problem Management

Problems are defined as the unknown underlying cause of one or more incidents. A problem will become a known error when the root cause or workaround is known, and the temporary or permanent alternative has been identified.

boxxe will employee Problem Management to minimise the effect on users of defects in services and within the infrastructure. The Problem Management process shall be instigated in all cases of recurring Incidents and in cases where a temporary work around has been applied to close an incident and a permanent fix is required.

Problem tickets will be categorised and prioritised according to their impact.

The boxxe Problem Manager will be responsible for coordinating activities to diagnose and investigate the root cause. Where a workaround is available, this will be documented within the Known Error database.

Once a Solution has been identified it will be tested and implemented via the Change Management process.

Change Management

Changes to systems are an inevitable consequence of their running and development. The purpose of the Change Management Process is to minimise the risk associated with such Changes. It also enables all parties to keep track of Changes that have been made to systems and to assure all implications, interdependencies and back out processes have been considered before any change is implemented.

boxxe Change Manager

The boxxe Change Manager will manage the Change Management Process covering all changes raised by boxxe and customer. The boxxe Change Manager will:

- Record all received change requests from the customer and boxxe
- Maintain these records with the status of changes as they are processed through the change management process

- Organise and chair the Change Advisory Board
- Maintain a forward schedule of change
- Maintain timely communications with the customer

Types of Changes

Normal

A Normal change is one that is submitted, fully documented, approved, and has an implementation date that allows discussion at the next regularly scheduled CAB meeting. Normal Changes must be submitted to CAB at least 5 working days before the scheduled implementation date.

Standard

These have a low risk for which a known procedure exists, has been documented and has a predictable outcome may be pre-approved. The business objective for a Standard, Pre-approved change is to ensure that Standard changes receive an appropriate level of review while also minimizing restrictions. The criteria for standard, pre-approved changes are, as follows:

- The change must be a repetitive, standard activity
- The change’s calculated risk level must be Low
- The change must meet lead time requirements
- The change must initially be represented in CAB – before being approved to be a standard change

Pre-approved changes will not require the same level of scrutiny as other changes but must be presented at CAB for approval to convert a change to Standard.

Emergency Change

This is to be used for Emergency Changes that are required to repair a failure (ASAP) in an IT service that has a large negative impact on customers. Emergency changes are usually approved by an emergency meeting of the CAB (ECAB). This action should only be taken in situations where there is a loss of critical functionality. A Change Review is held to determine the reasons for the Emergency change.

Note: An emergency change is not a change that is raised late, due to poor management. late changes, which cannot be categorised as an emergency, will be rescheduled to meet the correct lead times

Change Approval

The Customer must approve each Planned and Emergency change before a Change is reviewed at CAB. Approval must be received either via email or via ServiceNow

Change Advisory Board (CAB)

The Change Advisory board (CAB) delivers support to the Change Management team by approving requested changes and assisting in the assessment and prioritization of changes.

A CAB will take place at a pre-agreed time. CAB meetings will provide a formal review and authorisation of changes, a review of outstanding Changes, a discussion of impending changes and closure of completed changes.

The CAB will consist of IT management and attendees who are relevant to the RFCs being considered.

Changes may be rejected by the CAB if a Change is not represented at the CAB, lacks appropriate approvals, lacks appropriate documentation, or if issues / concerns are raised during the CAB.

Change Schedules

The boxxe Change Manager will compile and maintain a Forward Schedule of Changes, covering changes authorised by the CAB. This schedule will be updated weekly after the CAB and issued to your Service Delivery Manager.

Customer Complaints

All customers can send compliments and complaints to the customerservices@boxxe.com inbox. Any compliments and complaints received by boxxe will be categorised and escalated in accordance with our Compliments and Complaints process. If you have any questions about this process, please contact boxxe's Customer Services team.

Where the complaint is related to a service provided by a third-party vendor, boxxe will act as a mediator. boxxe will record the complaint with the vendor, check in regularly while it is being managed by the vendor's internal complaints procedure, and report back for final resolution.

Customisation

Boxxe have a standard AVD service, this can be customised to include specific customer design criteria which will be determined during customer workshops and

Service levels

Availability Management

Contractually agreed availability service levels that will be provided within the services

KPIs and Service Credits

To be defined after Early Life Support

Termination

If the agreement is terminated early in accordance with the T&Cs (for example because of your material breach or if you suffer an Insolvency Event), in addition to the amounts set out in the T&Cs, the customer will pay boxxe any charges reasonably incurred by us from a supplier or vendor of related products because of the early termination.