MXDR FOR MICROSOFT SENTINEL SERVICE

SERVICE DESCRIPTION SD177

DOCUMENT CONTROL

Version	Completed by	Date
1.5	Theo Jarvis	30 July 2025
1.6	George Dunning	29 September 2025
2.0	George Dunning	3 December 2025

The version history has been recorded and archived and is available upon request should these be required.

PREPARED BY

Name	Job title
George Dunning	Service Development Product Manager

CONTENTS

1. SERVICE OVERVIEW

All bold and capitalised Terms throughout this Service Description are described in the Glossary and definition of Terms.

1.1 SERVICE SUMMARY

The Service provides Customers with a Managed Sentinel Service from Softcat's UK based 24x7x365 Security Operations Centre.

The Service comprises:

- 24x7x365 access to log Support Cases **("Softcat Support")**
- Deployment of the Microsoft Sentinel workspace and applicable core Components within the Microsoft Defender portal **("Sentinel Environment Deployment")**
- Access to Softcat's library of detection rules **("Detection Rules")**
- Validation of security Events and Alarms, identification of false positives and continuous tuning and calibration of the Security Information and Event Management application **("SIEM")**
- Integrated threat intelligence feed **("Threat Intelligence Feeds")**
- Incident response where malicious activity is suspected **("Security Incident Response")**
- Management of high impacting events that affect a large number of users, depriving the business of one or more critical services **("Major Case Management")**
- Standardised methods, processes and procedures which are used for all changes **("Change Management")**
- Providing a named Service Delivery Manager, service reviews and service reporting **("Service Delivery Manager")**
- Providing response actions through endpoint detection and response Platform(s) for investigating and responding to Cases **("Response Actions")**

Optional Add-Ons are chargeable extras and, where required, will be quoted, and confirmed on the Work Order:

- Providing a point-in-time look at Customer's cyber security posture in comparison with industry best practice **("Security Baseline Assessment") (Optional Add-On)**

Together, the above comprise the "Managed XDR for Microsoft Sentinel Service", referred to as the "Service" within this document.

Security Incident Response is provided in partnership with Check Point and managed by Softcat using the Major Case Management process which is described in this Service Description.

The Service is delivered in accordance with the following ISO standards:

- ISO 20000
- ISO 27001
- ISO 9001
- ISO 22301

Unless otherwise stated in the Work Order, and in addition to any Terms set out in this Service Description, the following applies to the delivery of the Service set out in this Service Description:

- Softcat Terms and Conditions: T&Cs
- The Data Processing Agreement: DPA
- Check Point Incident Response: SLA refer to Section 7.3

1.2 SERVICE FEATURE TABLE

Managed XDR for Microsoft Sentinel Service	
Softcat Support	
Log Support Cases 24x7x365 [1]	✓
Online Support portal to track and log calls	✓
A minimum of two (2) authorised contacts	✓
P1 response Service Level target	✓
Sentinel Environment Deployment	
Microsoft Sentinel workspace	✓
Log Analytics workspace	✓
Microsoft Sentinel Data Lake	✓
Deployment of Log Collection infrastructure [2]	✓
Security log onboarding	✓
Detection Rules	
Access to Softcat's library of detection rules	✓
Creation of custom detection rules	✓
Security Information and Event Management	
Determination and notification of true security Events and Alarms	✓
Ongoing tuning and optimisation of the Sentinel workspace	✓
Weekly reporting of P4 Cases	✓
Threat Intelligence	
Threat intelligence feed integration	✓
Security Incident Response	
Security Incident Response	✓
Purchase of additional Security Incident Response hours	✓
Flexible use of Security Incident Response hours	✓
Major Case Management	
Major Case Management process applies	✓
P1 notifications	✓
Change Management	
Standard Change Requests	✓
Normal Change Requests	✓
Retrospective Change Requests	✓

Emergency Change Requests	✓
Customer performed maintenance	✓
Service Delivery Manager	
Named Service Delivery Manager	✓
Service reports and reviews [3]	✓
Response actions [4]	
Manual response actions	✓
Isolation of endpoints	✓
Collection of investigation package	✓
Restrict app execution	✓
Run antivirus scan	✓
Stop and quarantine a file	✓
Security Baseline Assessment (Optional Add-On) [5]	
Access to the controls assessment portal and automated reporting	✓
Annual assessment and review workshop [6]	✓
Get-Well recommendations	✓

[1] Requests are acted upon within contracted coverage hours, as confirmed in the Work Order. Support for this Service is only provided for the Service and deployed Sentinel Resources. It does not include Support for the Customer's wider Azure cloud environment.

[2] Softcat will provide guidance to the Customer, in line with best practice on the deployment of Log Collection infrastructure. Where required, the Customer may request Softcat to complete the deployment on their behalf for an additional Fee. This will be identified as part of the initial scoping activity and confirmed on the Work Order.

[3] These service reports and service reviews are provided upon a Customer's request; these requests are limited to up to a maximum of once a month only.

[4] For the latest Supported endpoint detection and response ("EDR") Platforms the Customer should speak to their Account Manager for more information. Available actions will differ by Platform, licencing and Operating System ("OS").

[5] "Optional" and "Optional Add-On" means a chargeable extra. Where a chargeable extra is chosen by a Customer, this is confirmed on the Work Order.

[6] The Softcat consultant will agree the delivery method (by phone or in person) and attendees with the Customer prior to its delivery.

2. SERVICE DETAIL

2.1 SOFTCAT SUPPORT

Authorised Customer Contacts have access to Softcat Support around the clock and on any day of the year ("24x7x365") [7].

Customer Contacts should raise a Case primarily via the Support portal, where the Case type will be assessed, defined and communicated and the priority level will be agreed with the Customer. Where Service Levels apply to the management of a Case, these will be confirmed on the Work Order. For any Case which the Customer believes to be urgent, the Customer Contact must report to Softcat by telephone.

[7] Support is only provided for the Service and deployed Sentinel Resources. It does not include Support for the Customers wider Azure cloud environment.

2.2 SENTINEL ENVIRONMENT DEPLOYMENT

As part of the onboarding, Softcat will deploy the required environment into an empty Subscription for the Service which consists of three core Components listed below. The deployment and the continued integration are achieved through the CI/CD ("Continuous Integration, Continuous Delivery or Continuous Deployment") process.

The environment deployment consists of:

- Microsoft Sentinel will be deployed following Microsoft best practice using a distributed deployment model. The Sentinel workspace will be configured for ingestion, detection and retention of log source Events. This will be managed and monitored as part of the Service.
- Log Analytics workspace provides the database where all log source telemetry is ingested and retained for a specified retention period. By default this is ninety (90) days. Microsoft Sentinel is deployed as part of the Microsoft Defender portal, with an associated Log Analytics workspace automatically provisioned to store Events and analytics data. Detection and analytics are performed using the full functionality of Microsoft Sentinel against telemetry ingested and stored in tables in a defined schema.
- Data Lake provides cost-effective long-term storage of logs. Data Lake will mirror the data in Log Analytics, meaning that when data is sent to the high-performance analytics tier, a copy is automatically replicated to the most cost effective Data Lake tier. This ensures long-term storage and availability for future analysis. Softcat can also send data directly into the Data Lake tier, which allows noisy data sources that don't have immediate analytical benefits to remain stored. This can be referred to in the event of a serious cyber incident for threat hunting, or for any potential audit requirements. Softcat will agree with the Customer their requirements for long-term storage prior to deployment taking place.

2.2.1 DEPLOYMENT OF LOG COLLECTION INFRASTRUCTURE

Softcat will provide guidance to the Customer, in line with best practice on the deployment of Log Collection infrastructure. Where required, the Customer may request Softcat to complete the deployment on their behalf for an additional Fee. This will be identified as part of the initial scoping activity and confirmed on the Work Order.

2.2.2 SECURITY LOG ONBOARDING

To ensure only the correct log sources and logging level of each log source is onboarded into the Customer's Sentinel workspace, an initial assessment will have been performed with the Customer to understand what is to be monitored in their environment.

2.2.3 ENVIRONMENT ACCESS AND SECURITY

During onboarding and ongoing delivery, Softcat will require a certain level of access to be provided in the Customer's Azure environment. The type of access and permissions that must be configured are outlined below:

- **Microsoft Entra multi-tenant app registrations** - each Customer will have a unique set of app registrations that they will need to accept, this is required for the connectivity between the Customer's Sentinel instance and the Softcat incident response system. Optionally, additional app registrations may be required for enhanced threat intelligence feeds into Sentinel.
- **Azure Lighthouse ("ALH") offer** - each Customer will need to accept an Azure Lighthouse offer into their tenant, with permission delegation at the Subscription level. The offer contains pre-defined user groups and delegated permissions relevant to each group. This is to ensure the relevant access is available to the Softcat staff who provide the Service. The groups and delegated permissions are listed below.
- **Granular delegated admin privileges ("GDAP") relationship** - To enable Softcat's SOC Analysts to review and investigate active cases in Microsoft Defender, a GDAP relationship must be established and accepted by the Customer into their tenant. This setup requires assigning the 'Security Reader' and 'Security Administrator' roles within the tenant where Microsoft Sentinel is deployed, to ensure appropriate access to Microsoft Defender.
- **Owner login account** – each Customer will need to provide Softcat with a login account that holds owner permission to the Subscription and security administrator permissions to the Tenant where Sentinel is going to be deployed. This is required to ensure full deployment and configuration can take place.

User/Group	Delegated Permission	Access Type	Max Duration	MFA	Approvers
ALH - Managed Security L1 Analyst	Log Analytics Reader	Permanent	-	-	-
ALH - Managed Security L1 Analyst	Microsoft Sentinel Responder	Permanent	-	-	-
ALH - Managed Security L2 Analyst	Log Analytics Reader	Permanent	-	-	-
ALH - Managed Security L2 Analyst	Microsoft Sentinel Responder	Permanent	-	-	-

User/Group	Delegated Permission	Access Type	Max Duration	MFA	Approvers
ALH - Managed Security L3 Analyst	Log Analytics Reader	Permanent	-	-	-
ALH - Managed Security L3 Analyst	Microsoft Sentinel Responder	Permanent	-	-	-
ALH - Managed Security Security Engineer	Log Analytics Reader	Permanent	-	-	-
ALH - Managed Security Security Engineer	Microsoft Sentinel Contributor	Permanent	-	-	-
ALH - Managed Security Security Engineer	Managed Services Registration Assignment Delete Role	Permanent	-	-	-
ALH - Managed Security Security Engineer	Contributor	Eligible	4 hours	Azure	PIM - Managed Security (Approvers)

2.3 DETECTION RULES

The Customer will have access to Softcat's library of detection rules. These will initially be applied based on the log sources onboarded, through careful selection of the detection rules batched into groups known as baseline use case sets, mapped to the log sources by technology.

An initial assessment to identify the Customer's threat landscape and critical assets will be performed. This assessment will ascertain the required security monitoring coverage of the Customer's environment prior to the deployment of the baseline use case sets. Additional analytic detection rules outside of the baseline set will then be deployed (this is dependent on the Customer onboarding the required Event logs): the roadmap for this will be agreed during onboarding workshops.

Based on the Customer's threat landscape during the life of the Service there will be use cases that require custom content to be created, such as detection rules or custom log onboarding. As part of the Service, the creation of custom content is available to the Customer; upon request Softcat will agree with the Customer the timelines based on complexity. Where an item is deemed to be high complexity this may be subject to an additional charge which will be quoted separately and detailed in the Work Order.

Examples of what could be deemed high complexity are noted below:

- Application programming interface ("API")-based log sources
- Log Parsers / custom data collection rules ("DCRs")
- Custom connectors
- New development of Swimlane (SOAR) automations
- External enrichment sources

2.4 SECURITY INFORMATION AND EVENT MANAGEMENT

Softcat triages security Events and Alarms to determine false positives from true security Incidents. During the Onboarding Period and throughout the Contract Term, Softcat's Security Engineers will tune and calibrate the Sentinel workspace based on intelligence learnt through the analysis of the Customer's security Events and Alarms in relation to the Customer's Operating environment.

When a true security Alarm is discovered, Softcat will alert the Customer so that the Customer can take corrective action to mitigate any associated security risks, and, where appropriate, Softcat will engage Security Incident Response. See also "Security Incident Response" section 2.6.

2.5 THREAT INTELLIGENCE FEEDS

As part of the Service, Softcat integrate a threat intelligence feed into Sentinel utilising Open Threat Exchange ("OTX"). OTX delivers community-generated threat data, enables collaborative research, and automates the process of updating the security infrastructure with threat data from any source. This includes a wide range of Indicator of Compromises ("IOC") that can be used to detect threats including IP addresses, hostnames (subdomains), email and URLs.

2.6 SECURITY INCIDENT RESPONSE

Security Incident Response is provided by Softcat's IT Partner, Check Point, and managed by Softcat using the Major Case Management process.

Customers receive twenty (20) hours of Security Event Management as part of the Service. Where Softcat believes an incident would require Security incident Response, the Customer is notified of the recommendation and is asked to confirm their authority to invoke it.

If the Customer has used their twenty (20) hours, additional time can be purchased during the Contract Term. Any additional hours purchased will be confirmed on a Work Order. The Customer is to contact their Softcat Account Manager for more information.

Customers can use their Security incident Response hours for additional Security incident related services from Check Point, such as forensics and threat intelligence.

2.7 MAJOR CASE MANAGEMENT

When a P1 occurs, Softcat will manage communication with the Customer Contact(s) throughout the Case's lifecycle, in accordance with the communication plan described in the Softcat Services Welcome Pack document. This document is sent to the Customer during the Onboarding Period of the service.

In addition to communications, Softcat will follow its major Case management process to resolve the issue or find a workaround that is agreeable to the Customer.

2.8 CHANGE MANAGEMENT

When Softcat makes a recommendation for a critical security patch, a Fix, a best practice upgrade or any other recommended change, Softcat and the Customer will follow the Change Management process to implement these changes.

Change Requests, including changes to configuration, will be managed under the Softcat Change Management process with the Customer approving all changes that impact data ingestion or retention within the security Platform. During the Service onboarding process, the Customer will nominate named Customer Contacts who have the authority to approve these changes. The Customer can also initiate a change e.g. a requirement to make a configuration change.

2.8.1 PRE-APPROVED CHANGES

Pre-approved changes will be agreed in advance of the service going live with the Customer. These will be captured during the onboarding period. Any pre-approved changes will not require any additional Customer or Change Management approval.

2.8.2 STANDARD CHANGES

Standard changes are pre-approved changes that are determined as carrying extremely low risk. These changes have defined roll out, back out and test plans associated with them. Standard changes will complete within one Working Day of the request being logged unless the customer specifies a later date.

2.8.3 NORMAL CHANGES

Normal changes are not pre-approved and will require a Softcat technician to complete a roll out, back out and test plan. Under the Change Management process, these plans will be approved by the Customer, and Change Management approval. If the change is expected to be actioned on a repeated basis, Softcat and the Customer can mutually agree that it is recorded as a standard change.

2.8.4 RETROSPECTIVE CHANGES

Retrospective changes are only permitted if the change was implemented to resolve or immediately prevent an outage on a business-critical system. For a retrospective change to be actioned, the Customer and Softcat Change Management approval will be tracked against the Case of the related issue.

2.8.5 EMERGENCY CHANGES

Emergency changes are raised when the implementation window is required in a time prior to the next available Change Advisory Board meeting ("CAB"). If a Customer requests an emergency change, then it is implemented entirely at their own risk. If the change is not successful, it will be rolled back, if possible. No ad-hoc trouble shooting will be completed.

2.8.6 CUSTOMER PERFORMED MAINTENANCE

These changes are designed to allow Softcat Support to record when a Customer or a Customer's supplier advises that they are performing maintenance work. These changes will automatically progress through to an 'open' and then a 'closed' state when the scheduled window begins and expires.

2.9 SERVICE DELIVERY MANAGER

Customers will be assigned an aligned Service Delivery Manager who will serve as the primary point of contact and escalation for service-related matters during UK Working Hours. The Service Delivery Manager will be responsible for producing comprehensive service reports and conducting service reviews as agreed. During these reviews, they will analyse trends and provide recommendations tailored to the Customer's specific service needs. The reports will detail performance against predefined KPIs and Service Level targets.

Additionally, the Service Delivery Manager will collaborate with internal stakeholders, partners, and Customer Contacts to ensure that the Service operates smoothly. This includes assisting with service onboarding activities as well as proactively suggest service improvements where they arise to continually enhance the service experience.

2.10 RESPONSE ACTIONS

Where the Customer has opted for Response Actions to be included as part of the Service, Softcat will leverage the capabilities of the Customer's existing EDR platform via integration to the Service to utilise the available actions as part of the investigation process and to assist with responding to Cases.

An example of available actions may include: isolate device, run antivirus scan, restrict app execution, or collect information package.

The available actions will differ depending on the EDR platform being utilised, the licencing, and the operating system of the endpoints the Customer currently has in place. Softcat will confirm with the Customer the availability of actions during scoping. For example, the licence requirements for Microsoft Defender for Endpoint can be found on the following link, https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts.

Additional actions or features may become available during the life of the Service. Where this happens these will be communicated to the Customer as part of their monthly Service Review.

2.11 SECURITY BASELINE ASSESSMENT (OPTIONAL ADD-ON)

When purchased as part of the Managed Sentinel Service, Softcat will run an annual assessment of the Customer's existing internal controls, while externally assessing the posture of the Customer's organisation. This allows the Softcat consultants to understand the Customer's organisation's current exposure to cyber risk and suggest routes for improvement.

Softcat will identify internal and external risk profiles, provide a tailored report through the assessment portal with simple steps to help the Customer improve security maturity, and build a plan which is tailored to their organisation and aligned with their business objectives. The Customer will be able to view the results and scoring on a single, easy-to-use dashboard, to quickly understand their current levels of security.

2.11.1 CONTROLS ASSESSMENT PORTAL

Customers are provided access to the Softcat Cyber Controls Assessment portal through which they complete and submit the service questionnaire. This is completed remotely with a Softcat consultant.

A Softcat consultant will guide the Customer through the assessment, using the information that the Customer provides. The Softcat consultant will create a report which scores the Customer's security controls against the critical cyber security controls recommended by the Center for Internet Security ("CIS").

2.11.2 ASSESSMENT REPORT

Softcat will aggregate the results of the Customer's assessment(s) that are deemed in scope to produce an executive overview and report on the Customer's security posture. The report will be available to the Customer via the Softcat Cyber Controls Assessment portal. This will be followed by a review workshop with the Customer which will cover a high level summary of findings and Get-Well recommendations.

Whilst Softcat can Support Customers to implement their Get-Well plan through technology, Professional Services and advisory services, these would form a separate project and be chargeable as extra work. Customers of the Service should contact their Account Manager and/or Service Delivery Manager with any queries.

3. SERVICE LEVELS

3.1 SECURITY INFORMATION AND EVENT MANAGEMENT

The Service Level targets for Cases, security alarms and Requests are shown in the table below.

The Service Level target column is the percentage of requests responded to within the response metric, for example: 95% of Cases logged as a P1 are responded to within fifteen (15) minutes.

Priority	Description	Service coverage hours	Response metric	Notification method	Service Level target
Priority 1 (P1)	Business impacted or imminent impact expected within four (4) hours; for example, severe cyber event or SIEM Platform full outage.	24/7	< 15 minutes	Phone call and email	95%
Priority (P2)	Customer cannot perform business critical functions; loss of revenue; risk of severe reputational damage; all End-Users unable to perform business critical roles. Highly likely to require security incident response.	24/7	< 30 minutes	Phone call and email	95%
Priority (P3)	Moderate to high impact cyber event or partial SIEM Platform outage.	24/7	< 4 hours	Email	95%
Priority (P4)	Risk to revenue generation; multiple End-Users unable to perform business critical roles. May require security incident response.	24/7	1 week	Weekly report	95%

Category type	Description	Service coverage hours	Response metric	Fulfilment target	Service Level target
Request [8]	Low to moderate impact cyber event. Unlikely to require security incident response. Request – Working Hours only	M-F 09:00 – 18:00 (ex. Bank Holidays)	< 4 Hours	5 Working Days	95%

[8] Unless specified otherwise, any requests are subject to the above metrics.

3.2 MAJOR CASE MANAGEMENT

As part of the major Case process, initial P1 email communications are sent to the Customer Contact list, within fifteen (15) minutes of receiving the escalation.

Updates will be communicated hourly, unless there is a specific reason for a delay (e.g. a restore job is running and is expected to take two (2) hours). In such circumstances, the Customer's expectation will be set in the previous communication.

When Softcat has determined that the impact of the P1 Case on the Customer has been mitigated, the P1 Case will be 'resolved'.

Following the resolution of the Case, if the Customer is still running at a loss of redundancy, or at a reduced but acceptable capacity, then the Case will be reassessed, and priority determined and reflected accordingly.

Upon resolution a report will be compiled and provided to the Customer.

If the reason for the outage has not been established, a problem record will be raised and managed by Softcat.

3.3 CHANGE MANAGEMENT

The Service Level is determined by the type of change. The Service Level starts from when the Customer supplies Softcat with all of the information that is required by Softcat for the completion of the work. Any time spent determining the Customer's expectations or requirements will not be included in the Service Level.

Category type	Description	Service coverage hours	Response metric	Fulfilment target	Service Level target
Pre-approved change	A set of changes agreed during on boarding that are pre-approved and don't require any further Customer or Change Management approval.	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	1 Working Day	95%
Standard Change	A pre-defined procedural change with minimum risk and impact to service. [9]	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	1 Working Day	95%
Normal Change	A change, which requires authorisation, is complex and / or requires down time for a related service.	M-F 09:00 – 18:00 (ex. Bank Holidays)	<4 Hours	5 Working Days [10]	95%
Emergency Change [11]	A change required to restore service or protect / mitigate a threat to the environment where it is not acceptable to restore under the related Case.	Applied in line with a major Case (Priority 1)			

[9] This is dependent on all required information being received to complete the request. Some changes may cause a negative effect, i.e. the Fix of Events may lead to an undesired and unforeseen outcome occurring. Therefore, success is measured by the absence in reoccurrence of a given condition.

[10] Dependent on complexity, impact, and approved design.

[11] Softcat reserve the right to disable users, services, or devices which are found to present an immediate threat to the Customer's or Softcat's environment without authorisation.

4. CUSTOMER RESPONSIBILITIES

4.1 MANAGED SENTINEL SERVICE

The Customer acknowledges and agrees that Softcat's ability to deliver the Service is contingent upon the Customer ensuring timely payment of all associated Azure subscription and consumption charges. Should Customer fail to meet their financial obligations to Microsoft, resulting in suspension, interruption, or termination of Azure services or Subscriptions. Softcat shall have no obligation to deliver the Service, nor shall Softcat be liable for any breach of Service Levels or warranties during such suspension or termination period. Softcat's performance commitments and associated service level agreements (SLAs) under this Agreement shall resume only when Microsoft services have been fully restored, and the Customer's Azure Subscription is once again in good standing.

For the Customer to utilise the Service, they are required to have a suitable Agreement in place such as Cloud Solution Provider ("CSP") or an Enterprise Agreement ("EA") / Microsoft Customer Agreement ("MCA").

This will enable Softcat to act on the Customer's behalf and raise the necessary Support Cases where applicable on the Customer's behalf to Microsoft. Where this is not the case and there is a related issue, the level of Support that will be available from Softcat will be restricted to advice only until the issue is resolved by the Customer.

4.2 SOFTCAT SUPPORT

a. The Customer should ensure that Customer Contacts are skilled in or knowledgeable of the Customer's Operating Environment, have sufficient access rights and are of a sufficient proficiency to apply the recommendations that are provided as part of this Service.
b. Prior to Service commencement the Customer should provide:
    i. The Customer's admin on Softcat's ticketing platform must maintain at least two (2) Customer Contacts for the purposes of Support and continuity; and
    ii. Any relevant Key Information e.g. models, serials, tenancy, Subscription.
c. When raising a Case, the Customer Contact should provide, when requested by Softcat:
    i. Valid and applicable serial numbers for the affected Supported Product(s).
    ii. Reasonable visibility of system logs, configuration files and error messages.
    iii. Details of Software versions and configuration.
    iv. A description of the symptoms and other devices or services impacted.
    v. Confirmation of when the issue first occurred and if it has occurred before (where possible provide previous Case references).
    vi. Details of any recent changes or projects implemented prior to the issue being raised.
    vii. Details of all Fixes, configuration amendments and updates performed already to attempt to resolve prior to raising the Case.
    viii. To what extent the issue is affecting operation of the Customer's business.
    ix. The number of End-Users impacted and their location.
    x. Contact details of the Customer Contact.
    xi. Details of any trouble-shooting steps already undertaken.
d. Implementation of best practice recommendations advised by Softcat.

e. Direct Support for End-Users. Customers should ensure the Customer's staff are trained to refer all Cases to the Customer Contact in the first instance, and not permit persons other than a Customer Contact to approach Softcat to register Cases.
f. Provide thirty (30) days' notice to Softcat of any requested addition(s) to the Supported Product list.
g. Use the Service only for the business purposes of the Customer and keep all access credentials and certificates, which Softcat may provide to allow access to the service, safe and secure, and not share them with any Third Party without Softcat's prior written consent.
h. Not use or attempt to use or misuse the Services in any way that is criminal or otherwise unlawful in any relevant jurisdiction.

4.3 SENTINEL ENVIRONMENT DEPLOYMENT

a. Complete and return all pre-requisite onboarding documents.
b. Provide Softcat with their unique tenant hostname from the *.onmicrosoft.com domain.
c. Provide Softcat with the Customer tenant ID for where the Sentinel deployment will take place.
d. Provide Softcat with an empty subscription for where the Sentinel deployment will take place.
e. Ensure the subscription ID they are providing is empty and that they are able to apply the required permissions as requested by Softcat.
f. Provide Softcat with their Azure region for deployment of resources.
g. Provide Softcat a login account that has owner permission to the subscription where Sentinel will be deployed.
h. Accept the required Lighthouse offering and App Registration requests.
i. Accept the required GDAP relationship into the Customer's tenant.

4.4 SECURITY INFORMATION AND EVENT MANAGEMENT

a. Provide Softcat with requested information to Support troubleshooting.
b. Provide Softcat with a list of the names, numbers and email addresses of Customer Contacts who should be notified of a security Event or Alarm. The Customer should maintain this list and ensure that it is accurate during the Contract term.

4.5 MAJOR CASE MANAGEMENT

Ensure that their Customer Contacts is maintained accurately.

4.6 CHANGE MANAGEMENT

Ensure that their Authorised Contact List is maintained accurately. This determines who is a change approver, escalation contact(s) and commercial approver.

4.7 SERVICE DELIVERY MANAGER

a. Provide email distribution list for any service reports or communication.
b. Keep Customer Contacts up to date in ticketing platform (ServiceNow) to allow Service Delivery Managers to provide the Service effectively.
c. Provide advanced notification to Softcat Support of any planned maintenance that could have an impact on any hardware or Software that Softcat provide Services for.

d. Provide advanced notification to Softcat Support of any planned decommissioning of Softcat-related equipment or Software.

4.8 SECURITY LOG ONBOARDING

a. Notify Softcat before changing or adding any log sources.
b. In the event that logs are not received from an expected source or in an expected format (during set up and throughout the life of the Contract), Softcat will alert the Customer so that the Customer can identify and rectify the cause of the issue. Where required, Customers can request advice on how to do this through their Softcat Account Manager or named Service Delivery Manager.
c. Ensure that all logs do not contain Personally Identifiable Information ("PII") and payment information.

4.9 RESPONSE ACTIONS

Ensure where applicable that they have an active and appropriate licencing for their nominated EDR platform.

4.10 SECURITY BASELINE ASSESSMENT (OPTIONAL ADD-ON)

a. Comple the Cyber Controls Assessment questionnaire.
b. Provide information as requested by Softcat, such as:
    i. Customer users who should be given access to the Platform and necessary security access information;
    ii. the Customer's business, Customer's core business objectives and the existing Security Controls (technical, organisational and physical).

5. NOTABLE EXCLUSIONS

5.1 SOFTCAT SUPPORT

a. At an additional cost the Customer can request project and design work, including Professional Services by contacting their Account Manager for a quote.
b. Support is only provided for the Service and deployed Sentinel Resources. It does not include Support for the Customer's wider Azure cloud environment.

5.2 SENTINEL ENVIRONMENT DEPLOYMENT

The deployment of the required environment for the Service cannot be integrated into a Customer's Existing infrastructure as code ("IaC") delivery and will only be deployed from Softcat's IaC CI/CD pipelines.

5.3 SECURITY INFORMATION AND EVENT MANAGEMENT

a. Storage and management of credit or debit card data.
b. Notification of vendor patch releases and the management of vulnerabilities.

5.4 SERVICE DELIVERY MANAGER

a. Any bespoke reporting or service reviews. [12]
b. Service Delivery Managers will not act as a project manager or in any other capacity outside of the activities described in this Service Description.

[12] This is available, but subject to an additional charge. Customers can request a quote by contacting their Softcat Account Manager.

5.5 RESPONSE ACTIONS

Support of third party EDR Platform(s). Support is only provided for the Service and deployed Sentinel Resources. It does not include Support for the Customer's wider Azure cloud environment.

5.6 SECURITY BASELINE ASSESSMENT (OPTIONAL ADD-ON)

a. The Service does not include the remediation of identified security risks or issues, nor does it include the implementation of Get-Well recommendations that arise from the Security Baseline Assessment. However, if the recommendation aligns with the Service, Softcat will collaborate with the Customer to address the recommendation.
b. For recommendations outside the scope of the Service, Softcat can Support remediation activity but this would form a separate project and be chargeable as additional work. The Customer is to contact their Softcat Account Manager for more information.
c. Independent verification of Customer-provided information.

6. SERVICE ACCEPTANCE AND ONBOARDING

Following receipt of a Customer purchase order, Softcat will confirm the Contract by sending a Work Order, which is usually undertaken online via DocuSign.

Following the acceptance of the Contract, the Onboarding Period will begin. This is the period in which any pre-requisite dependencies for the Service are completed, for example the collation of the Key Information. If there is a requirement for any additional assessment of the Customer's Operating Environment following Softcat's receipt of the Key Information, this will be undertaken during the Onboarding Period.

At the end of the Onboarding Period, the Customer will be provided with an Acceptance into Service (AIS) document which is required to be signed by the Customer within five (5) days of receipt. The Activation Date for the Service will be the day on which the Onboarding Period ends and is signed off as complete by the Customer or, in the event of no response, five (5) days after the Onboarding Period has completed and the AIS document has been provided (whichever is the sooner). Where any Key Information requested by Softcat is outstanding at the Activation Date, Softcat's obligation to deliver the Service shall be subject to reasonable endeavours.

Shortly after the Work Order is sent, the Customer will receive a "Softcat Services Welcome Pack" document, which includes key contact details for Softcat, an overview of the escalation process, and other useful information.

7. SERVICE BILLING AND CONTRACT TERM

The billing frequency, and the Initial Term will be agreed with the Customer and confirmed in the Work Order.

Unless it is stated on the Work Order that the Service will not Auto-Renew[13], or written notice is given by either Party to the other of its intention not to renew the Contract at least ninety (90) Working Days before the expiry of the Initial Term or any subsequent Renewal Term, the Service at the expiry of the Initial Term or any subsequent Renewal Term will be renewed automatically for a further term of twelve (12) months on the same Terms and Conditions as detailed within the Contract.

[13] The state of Auto-Renew will be reflected in the 'service specific section' of the Work Order.

7.1 SECURITY BASELINE ASSESSMENT (OPTIONAL ADD-ON)

If a Customer chooses to give Notice not to renew the Service, access to the controls assessment portal will be available for ninety (90) days following the lapse of the Service end date.

8. TERMS AND CONDITIONS

8.1 OVERVIEW OF TERMS AND CONDITIONS

The delivery of the Service to the Customer shall be governed by Softcat's Terms and conditions, this Service Description and the Work Order, and the other Agreements listed below.

- Softcat terms and conditions: https://www.softcat.com/terms-and-conditions-uk/
- Check Point Incident Response SLA: https://www.softcat.com/documents/incident-response.pdf

Capitalised terms in this document shall have the meaning set out here: https://www.softcat.com/documents/glossary-and-definition-of-terms.pdf, unless they are defined in the Terms and Conditions. In the Event of any discrepancy or conflict between the Softcat T&Cs, this Service Description and the Work Order, the Work Order shall take precedence to the extent of any discrepancy or conflict.

For the purposes of the relevant Work Order and this Service Description, the Term "Service" shall be interpreted as an "Annuity Service".

8.2 DATA PROCESSING AGREEMENT AND ACCEPTANCE OF THE CONTRACT

By signing the Work Order, the Customer agrees to the Data Processing Agreement (DPA), available here: https://www.softcat.com/documents/Softcat-Services-DPA2019.pdf

The DPA shall be a separate Agreement to the Contract (and no liability shall arise (i) under this Contract in respect of the Processing, or (ii) under the Processing Agreement in respect of the remaining aspects of providing or using the Annuity Services).

If, in the absence of a signed Work Order but following receipt of this Service Description, the Customer provides a PO for the Services and/or instructs Softcat to provide the Services, the Customer shall be deemed to have accepted the terms and conditions of the Contract, including the Service Description and the DPA.

8.3 ADDITIONAL TERMS

8.3.1 SENTINEL ENVIRONMENT DEPLOYMENT

The Customer is provided with a Service only. The licenses and Agents required to deliver the Service are not sold to or passed to the Customer as a Component. The Customer is aware of the technology however is not able to choose the manner in which that technology is deployed or used by Softcat to deliver the Service. Any EULA is used for the Customer to grant access to a third party to deploy into the Customer environment only. If the Customer stops taking the Softcat Service, the technology is removed as part of transition.

8.3.2 SECURITY INCIDENT RESPONSE

Softcat plc (Softcat) has agreed to arrange the supply to the Customer (as named in the signature block below) certain managed or ongoing services ("Managed Services"), subject to the Softcat Terms and Conditions (current version available at https://www.softcat.com/terms-and-conditions-uk/ and on request,

and capitalised Terms in this document which are not defined here shall be interpreted in line with the Terms and Conditions).

Softcat has sub-contracted the provision of the Supplies to its subcontractor (IT Partner), who has provided details of the Service by way of a Service Description (https://www.softcat.com/documents/incident-response.pdf).

Pursuant to this document, the Check Point Incident Response Service Level Agreement shall be considered part of the Agreement between Softcat and the Customer.

In the Service Description noted in the Security Incident Response section, if there is reference to Softcat as the party the IT Partner is delivering to, this shall be interpreted as referring to the Customer and, correspondingly, where in that document there is reference to the IT Partner, this shall be interpreted as referring to Softcat, so that the effect is that Softcat and the Customer have the same rights, entitlement, duties and obligations to each other under the Agreement as would be the case between the IT Partner and Softcat (respectively) under the Service Description.

By signing the Work Order, Softcat and the Customer agree to the above and the contents of the Service Description.

8.4 ISO STANDARDS

The Service is fully compliant with the following ISO standards, ensuring the highest levels of quality, security and continuity:

- **ISO 20000** – Focuses on IT service management, ensuring that service are aligned with business needs and adhere to best practices. By following ISO 20000, the Service guarantees that the IT service management processes are efficient, effective, and continually improving to meet Customer evolving demands.
- **ISO 27001** – Dedicated to information security management systems. It helps organisations protect data and manage security risks systematically. Compliance with ISO 27001 ensures that robust security measures are in place to safeguard sensitive information, mitigate risks and respond promptly to security Incidents.
- **ISO 9001** – Addresses quality management systems. It ensures that the Service consistently meets Customer requirements and strives for continuous improvement. By adhering to ISO 9001, the Service demonstrates commitment to delivering high-quality services that enhance Customer satisfaction and operational excellence.
- **ISO 22301** – For business continuity management systems, helping organisations prepare for a respond to disruptive Incidents. Compliance with ISO 22301 ensures that the Service has comprehensive plans and procedures in place to maintain business operations during unforeseen events, thereby minimising downtime and ensuring service continuity.

SOFTCAT PLC, FIELDHOUSE LANE, MARLOW, BUCKS, SL7 1LW