MANAGED SIEM SERVICE

SERVICE DESCRIPTION SD098

DOCUMENT CONTROL

Version	Completed by	Date
2.9 (Archived)	Theo Jarvis	05 September 2022
3.0	Theo Jarvis	08 March 2023
3.1	Theo Jarvis	10 July 2023
3.2	Theo Jarvis	05 November 2024
3.3	Theo Jarvis	30 July 2025

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

PREPARED BY

Name	Job title
Diane Fawkes	Services Development Product Manager
Prakash Lad	Services Development Programme Manager
Natasha Sagar	Services Development CSI Manager
Amanda Mason	Service Development Team Lead
Theo Jarvis	Service Development Programme Manager

CONTENTS

1. SERVICE OVERVIEW

All bold and capitalised terms used throughout this Service Description are described in the Glossary and definition of terms

1.1 SERVICE SUMMARY

Softcat's Managed Security Information and Event Management (SIEM) service provides Customers with a Softcat managed SIEM technology Platform in which Customer system logs are captured and managed with real-time analysis alerting and management of security alerts.

The service comprises:

- 24x7x365 access to log Support Cases **("Softcat Support")**
- Parsing, management, and storage of logs received into a SIEM application **("Security Log Management")**
- Validation of security Events and Alarms, identification of false positives and continuous tuning and calibration of the SIEM application **("Security Information and Event Management")**
- 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")**

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

- Softcat to set up the log sending **("Security Log Sending Set Up" (Optional Add-On))**
- Retrieval of stored logs **("Security Log Retrieval" (Optional Add-On))**
- Providing a point-in-time look at your organisation's cyber security posture in comparison with industry best practice **("Security Baseline Assessment") (Optional Add-On)).**

Together, the above comprise the "Managed SIEM 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 8.3.

1.2 SERVICE FEATURE TABLE

Managed SIEM Service	
Softcat Support	
Log Support Cases 24x7x365 [1]	✓
Online Support portal to track and log calls	✓
A minimum of two (2) Customer Contacts	✓
P1 response Service Level	✓
Security Log Management	
Set up of Log Collection	✓
Parsing of logs into searchable format	✓
Advice on Log Sending	✓
Flexible log storage options	✓
Security Information and Event Management	
Determination and notification of true security Events and Alarms	✓
Ongoing calibration and tuning of SIEM application	✓
Weekly reporting of P4 Cases	✓
Read only access to security portal	✓
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 [2]	✓
Security Log Sending Set Up (Optional Add-On) [3]	

Set up of Log Sending	✓
Security Log Retrieval (Optional Add-On) [3]	
Retrieval of archived logs during Contract Term	✓
Security Baseline Assessment (Optional Add-On) [3]	
Access to the controls assessment portal and automated reporting	✓
Annual assessment and review workshop [4]	✓
Get-Well recommendations	✓

[1] Requests are acted upon within contracted coverage hours, as confirmed in the Work Order.

[2] Service reports are provided on a monthly basis only, and the frequency of the service review is at the Customer's request.

[3] "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.

[4] The 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") [1].

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.

[1] Requests are acted upon within contracted coverage hours, as confirmed in the Work Order.

2.2 SECURITY LOG MANAGEMENT

2.2.1 SET UP

Softcat offers a consumption-based model for system log storage and will work with the Customer to size and price an appropriate level of storage for the Security Log Management. The agreed storage will be confirmed on the Work Order. During the Contract Term, the Customer may add to the level of storage required and the additional charge will be pro-rated for the remainder of the Term. Log storage cannot be removed during a Contract Term or lowered for any Renewal Term.

Softcat will work with the Customer to identify log types and log sources in accordance with Softcat's security guidelines. The security guidelines will enable the Customer to send and store logs.

Following the setup of the Log Collection into the Supported Product and throughout the life of the Contract, Softcat will assist the Customer to identify additional log sources (e.g. as the Customer's Operating Environment changes) to allow the Customer to send and store additional logs.

2.2.2 LOG PARSING, STORAGE, AND ARCHIVING

During the Onboarding Period, Softcat will ask the Customer for all log sources ("Key Information") that need to be stored. Softcat will identify any log sources that are incompatible with the Security Log Management service and will add these to the Service Product backlog for review and management.

Softcat will Parse all compatible received logs into a searchable format. Logs will be stored for either thirty (30) days or ninety (90) days, after which time they will be archived for the contract length. Storage options will be discussed with the Customer and the chosen option will be confirmed on the Work Order.

If the Customer's subscription expires and they decide not to renew, The SIEM Platform instance will be decommissioned fourteen (14) days after the expiration. All data, including asset information, orchestration rules, user credentials, events and vulnerabilities (hot storage), and raw logs (cold storage), will be destroyed.

The retained data is not accessible without an active subscription and will be deleted following the fourteen (14) days.

2.3 SECURITY INFORMATION AND EVENT MANAGEMENT

Softcat triages security Events and Alarms to determine false positives from true security events. During the Onboarding Period and throughout the Contract Term, Softcat's Security Analysts will tune and calibrate the SIEM Platform 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, engage Security Incident Response. See also "Security Incident Response".

2.3.1 ACCESS TO SECURITY PORTAL

As part of the Service (and from the completion of the Onboarding Period) the Customer has read only access to a security portal, through which they can:

- View a dashboard of their open security events.
- Review reporting.

2.4 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.

2.5 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.

2.6 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.

2.6.1 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.

2.6.2 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.

2.6.3 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.

2.6.4 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.

2.6.5 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.

2.6.6 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 they will automatically progress through to an 'Open' and then a 'Closed' state when the scheduled window begins and expires.

2.7 SERVICE DELIVERY MANAGER

Customers will be assigned a named Service Delivery Manager who will act as a point of contact and escalation for the Service during standard UK Working Hours.

The aligned Service Delivery Manager will produce service reports and deliver service reviews as agreed. As part of the service review, they will run through the report in more detail and discuss and capture any other Service-relevant actions.

Reporting provided will detail performance against pre-defined KPIs and Service Level targets, with various Case details.

2.8 SECURITY LOG SENDING SET-UP (OPTIONAL ADD-ON)

The Customer is responsible for setting up Log Sending. Where required, the Customer may request assistance with this by contacting their Account Manager or Service Delivery Manager for a Professional Services quote: this is available as a chargeable option.

2.9 SECURITY LOG RETRIEVAL (OPTIONAL ADD-ON)

Archived logs can be retrieved for the Customer for an additional charge and for as long as they remain available in the Platform.

2.10 SECURITY BASELINE ASSESSMENT (OPTIONAL ADD-ON)

When purchased as part of the Managed SIEM Service, Softcat will run an assessment annually 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 organisations 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 that's tailored to the organisation, 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.

2.10.1 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").

2.10.2 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 of 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	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 [5]	Low to moderate impact cyber event. Unlikely to require Security Incident Response.	M-F 09:00 – 18:00 (ex. Bank Holidays)	< 4 Hours	5 Working Days	95%

	Request – Working Hours only				

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

3.2 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 Customers' 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. [6]	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 [7]	95%
Emergency Change [8]	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)			

[6] This is dependent on all required information being received to complete the request. Some changes are a negative effect, i.e. the Fix prevents an undesired outcome occurring, so success is measured by the *absence* in reoccurrence of a given condition.

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

[8] Softcat reserve the right to disable users, services, or devices, which are found to present an immediate threat to the Customer or Softcat environment without authorisation. This also excludes project related tasks where scope has deviated from agreed design.

3.3 MAJOR CASE MANAGEMENT

As part of the major Case process, initial P1 email communication 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 issue, 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.

4. CUSTOMER RESPONSIBILITIES

4.1 SECURITY LOG MANAGEMENT

a. Sending of logs in a format that has been requested by Softcat to Softcat's log management Platform.
b. Send details of log sources for the Customer's Operating Environment to Softcat prior to the Onboarding Period so that Softcat can identify to the Customer any incompatibilities with the log management service.
c. Provide accurate information to Softcat on log sizing requirements and contextual information (such as network topologies, key users and services, operational policies, technologies, etc.) regarding the Customer's Operating Environment to allow Softcat to set up and maintain the Service effectively.
d. Provide and maintain security credentials if requested by Softcat to allow logs to be received and Parsed.
e. Test log sending and recovery if requested by Softcat.
f. Notify Softcat before changing or adding any log sources.
g. Complete and return all pre-requisite onboarding documents.
h. Provide Softcat with requested information to Support troubleshooting.
i. The Customer is responsible for setting up Log Sending. Where required, the Customer may request assistance with this by contacting their Account Manager or Service Manager for a Professional Services quote: this is available as a chargeable option.
j. 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.
k. Ensure that all logs do not contain Personally Identifiable Information ("PII") and payment information.

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 be 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 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.
i. Follow the information in the Softcat Services Welcome Pack.

4.3 SECURITY INFORMATION AND EVENT MANAGEMENT

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.

4.4 MAJOR CASE MANAGEMENT

Customer has a responsibility to ensure that their Customer Contacts is maintained accurately.

4.5 CHANGE MANAGEMENT

Customer has a responsibility to ensure that their Customer Contacts is maintained accurately. This determines who is a change approver, escalation contact(s) and who is a commercial approver.

4.6 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.

4.7 SECURITY BASELINE ASSESSMENT (OPTIONAL ADD-ON)

a. Completing 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

At an additional cost the Customer can request project and design work, including Professional Services by contacting their Account Manager for a quote.

5.2 SECURITY INFORMATION AND EVENT MANAGEMENT

a. Storage and management of credit or debit card data.
b. The Customer may request Softcat completes the Log Sending as a chargeable Professional Services engagement.
c. Notification of vendor patch releases and the management of vulnerabilities.

5.3 SECURITY LOG MANAGEMENT

a. If the Customer's subscription expires and they decide not to renew, The SIEM Platform instance will be decommissioned fourteen (14) days after the expiration. All data, including asset information, orchestration rules, user credentials, events and vulnerabilities (hot storage), and raw logs (cold storage), will be destroyed.
b. The retained data is not accessible without an active subscription and will be deleted following the fourteen (14) days.

5.4 SERVICE DELIVERY MANAGER

a. Any bespoke reporting or service reviews. [9]
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.

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

5.5 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[10], 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.

[10] 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 this Service Description, the Work Order, Softcat's Terms and conditions 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 Terms and conditions and this Service Description, this Service Description shall take precedence.

For the purposes of the Terms and Conditions and the relevant Work Order, the term "Managed SIEM Service" as used herein, shall be interpreted as a "Managed Service" for the purposes of those other documents.

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

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).

8.3 ADDITIONAL TERMS

8.3.1 SECURITY INFORMATION AND EVENT MANAGEMENT

The Customer is provided with a Service only. 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 technology however is not able to choose the manner in which that technology is deployed or used by Softcat to deliver the Service but only in the way Softcat uses the tool regardless of the tool's actual capability. 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, 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 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.