THREAT EXPOSURE MANAGEMENT SERVICE

SERVICE DESCRIPTION SD197

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

DOCUMENT CONTROL

Version	Completed by	Date
1.0	Theo Jarvis	06 March 2024
1.1	Theo Jarvis	07 August 2024
1.2	Theo Jarvis	05 November 2024
1.3	Theo Jarvis	04 April 2025
1.4	Theo Jarvis	30 July 2025

PREPARED BY

Name	Job title
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

The Threat Exposure Management ("TEM") Service provides Customers with access to the Picus Platform supported by Softcat. Softcat's in-house Cyber Security Assessors utilise the Platform to validate the security effectiveness across the Customer's environments using real-world attack simulations. The on-going output is reviewed with the Customer as part of a monthly workshop with one of Softcat's in-house Cyber Security Assessors.

The TEM Service offers a range of different features that the Customer can choose from to ensure the Service meets their needs. To be able to deliver the Service effectively the Customer must select at least 1 (one) of the Optional Add-On features outlined within the Service Description. All selected features will be confirmed on the Customer's Work Order.

The Service comprises:

- Deployment and on-going Support of the Picus Platform **("Picus Platform")** [1]
- Access to dashboards providing trending stats on simulation outcomes, security scoring and monthly review sessions **("Reporting And Dashboards")** [2]
- A point of contact and escalation **("Service Delivery Associate")**

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

- Access to updated threat libraries, scheduled attack simulations, validation for network security tools, and integration with the MITRE ATT&CK framework, along with Threat Intelligence Mapping **("Security Control Validation" (Optional Add-On))**
- Integration with SIEM ("Security Information and Event Management") / EDR ("Endpoint Detection and Response") platforms providing insights into which stage an attack has been prevented at **("Detection Analytics") (Optional Add-On))**
- Attack path mapping; a library of real-life attack actions, customisable assessment options and agentless deployment **("Attack Path Validation" (Optional Add-On))**
- Insights on Customer's existing deployed rules, including threat coverage and opportunities for improvements **("Detection Rule Validation" (Optional Add-On))**
- Risk-based visualisation and prioritisation of assets and vulnerabilities for effective threat exposure management **("Attack Surface Validation" (Optional Add-On))**
- Insights around identifying common cloud misconfigurations and overly permissive IAM ("Identity And Access Management") policies. **("Cloud Security Validation" (Optional Add-on))**

[1] Not available to the Customer where only Attack Path Validation has been selected.

[2] Access to live dashboards is not available for Attack Path Validation feature. All reporting for Attack Path Validation will be delivered by a Security Assessor.

Together, the above comprise the "Threat Exposure Management Service", referred to as the "Service" within this document.

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 apply to the delivery of the Service set out in this Service Description:

- Softcat Terms and Conditions: T&Cs
- The Data Processing Agreement: DPA

1.2 SERVICE FEATURE TABLE

	Threat Exposure Management Service
Picus Platform	
Access to the deployed Platform[1]	✓
Provide configured Agents	✓
Reporting & Dashboards	
Access to live dashboards and insights[2]	✓
Recurring workshops & reporting in line with chosen package	✓
Security score overtime[2]	✓
Attack module breakdown (overall score)	✓
Service Delivery Associate	
Contact and escalation	✓
Security Control Validation (Optional Add-On)[3]	
Extensive library of threats updated daily[4]	✓
Simulation of attacks on a predefined schedule	✓
Threat builder (customised attack scenarios)	✓
Validation of network security, SIEM and EDR Platforms[5]	✓
Mapping of results to MITRE ATT&CK framework	✓
Threat intelligence mapping	✓
Detection Analytics (Optional Add-On)[3]	
Integration with SIEM and EDR Platforms[5]	✓
Prevented attacks analytics	✓
Attack Path Validation (Optional Add-On)[3]	
A total of 3 (three) simulations per year	✓
Attack path mapping	✓
Library of real-life attack actions	✓
Customisable assessment options	✓
Agentless deployment option	✓
Detection Rule Validation (Optional Add-On)[3]	
Provision of insights on improvement points and positive points for detection rule baseline	✓
Ability to prioritise rules that need improvement	✓
Mapping of results to MITRE ATT&CK framework	✓

Measurement of the threat coverage of rules and analysis deficiencies	✓
Attack Surface Validation (Optional Add-On)[3]	
Automated asset discovery	✓
Identification of related security and policy gaps	✓
Asset Vulnerability prioritisation	✓
Cloud Security Validation (Optional Add-On)[3]	
Identification of common cloud misconfigurations	✓
Identification of overly permissive IAM policies	✓
Actionable insights	✓

[1] Not available to the Customer where only Attack Path Validation has been selected.

[2] Access to live dashboards is not available for Attack Path Validation feature.

[3] "Optional" and "Optional Add-On" means a chargeable extra. Where an optional extra and/or Optional Add-ons are chosen by a Customer, this is confirmed on the Work Order.

[4] Softcat is not responsible for the maintenance of this library. Picus own and manage all features and elements of the threat library.

[5] Current integrations available for the Platform can be found here.

2. SERVICE DETAIL

2.1 PICUS PLATFORM

Softcat will deploy and configure the Picus Platform as part of a remote engagement. The Customer will be granted access to the Platform as part of the Service for viewing purposes.

Softcat will determine the scope of the Customer's implementation, based on the selected modules, integrations and reporting frequency. From this a list of prerequisites will be identified and worked through with the Customer. Where an Agent is required, Softcat will provide details to install a pre-configured Agent that the Customer will deploy within their environment.

2.2 REPORTING & DASHBOARDS

2.2.1 SECURITY CONTROL VALIDATION

As part of Security Control Validation, the Platform has the capability to produce automated reporting and custom dashboards. This enables the Customer to stay on top of their security posture and keep Stakeholders across their business informed.

Activity throughout the month is rolled up into a monthly workshop where one of Softcat's aligned Cyber Security Assessors will discuss what has occurred in the month, provide insights and agree any amendments to the scheduled assessments for the coming months.

2.2.2 ATTACK PATH VALIDATION

As part of Attack Path Validation, following the successful completion of a simulation the Customer will be provided with 2 (two) reports; an executive summary and a technical report. The technical report will be run through by the assessor focusing on the technical remediation guidance for addressing the gaps that have been identified.

The technical report will provide a detailed breakdown of simulated attack paths and exploited vulnerabilities, along with step-by-step analysis of privilege escalation and lateral movement techniques. It will also include MITRE ATT&CK mapping for threat intelligence correlation and technical remediation guidance for addressing identified gaps.

The executive summary report will provide a high-level overview of the attack simulation results, including a business impact assessment of identified vulnerabilities. It will also offer clear risk prioritisation, potential financial and reputational consequences, and strategic recommendations for improving security posture.

If the customer has only opted for APV and no additional modules, such as Security Control Validation ("SCV") then the Customer will not have access directly to the Platform for custom dashboards or ad hoc reporting.

2.3 SERVICE DELIVERY ASSOCIATE

The Service Delivery Management team is a point of contact and escalation for any services detailed within the Work Order. The Service Delivery Management Team is available during standard UK Working Hours.

A named Service Delivery Manager, service report and service reviews are available for an additional charge. Customers can request this by contacting their Softcat Account Manager. This will then be detailed in the Work Order.

2.4 SECURITY CONTROL VALIDATION (OPTIONAL ADD-ON)

With access to the Picus threat library which is updated daily by security experts, Softcat can test Customers' defences against current and emerging attack techniques. The output from these tests are mapped to the MITRE ATT&CK framework[4], enabling the Customer to visualise threat coverage and prioritise the mitigation of gaps.

Softcat identifies weaknesses in threat prevention and detection controls a Customer may have by continually assessing the effectiveness of their security tools, both on an ongoing scheduled basis and on-demand when required. Supplying real-time metrics, including an overall security score for the Customer's organisation, Softcat can help Customers measure performance and demonstrate the value of their existing controls.

Via the Platform, Customers will have the ability to compare their security scores with industry peers, regional counterparts, and other Picus Platform users. Softcat will provide insights into the most simulated threats, threat templates, and popular ATT&CK tactics within the Customer's region, industry, and Picus community. This enables the Customer to better understand the prevalent threats and helps them prioritise their security efforts accordingly.

As part of the Security Control Validation, the Customer is recommended to leverage their standard organisational Gold Images to deploy an environment, Workload or VM, so that the test environment will be identical to the current production systems.

[4] https://attack.mitre.org

2.5 DETECTION ANALYTICS (OPTIONAL ADD-ON)

Softcat will provide insights into attacks that are missed by the Customer's prevention and detection controls, identifying blind spots and enabling the Customer to focus on threats which could pose a risk if mitigation action is not taken. Softcat can validate existing rulesets, providing further insights so the Customer can respond to threats earlier in the kill chain journey, by optimising these rules and ensuring the controls are effective and generate prompt alerts.

Using correlation rules available through the Picus Platform, Softcat can help reduce false positives by ensuring the detection content the Customer uses is effective and reliable. All assessment results are mapped to the MITRE ATT&CK framework, enabling the Customer to visualise their threat coverage and prioritise mitigation of gaps.

To use the detection and analytics module, the Customer will need to install the integration Agent on a specified Linux distribution that is supported. Once the system with the specified requirements is ready, make sure the VM has internet access and any security controls do not affect the communications efforts of the Agent and the management Platform. Below is a list of Linux distributions that can host the integration Agent. The Linux "Operating System (OS)" will require internet access over port 443 (HTTPS).

- CentOS 7 – 8 – 9

- RedHat 7 – 8 – 9
- Ubuntu 22.04

2.6 ATTACK PATH VALIDATION (OPTIONAL ADD-ON)

Using the Attack Path Validation ("APV") module, Softcat can automatically discover and visualise the steps an evasive attacker could take to compromise servers, workstations, and users. Powered by Picus' Intelligent Adversary Decision Engine, it will simulate real-world adversary actions to identify high-risk attack paths and supply actionable insights for the Customer to use to remediate them.

To verify attack paths that pose an actual rather than a theoretical risk, Softcat validates them utilising the platform by simulating adversarial actions such as credential harvesting, kerberoasting, and lateral movement.

APV focuses on 2 (two) simulation objectives, simulating ransomware behaviour and/or obtaining domain admin privileges. Softcat tailor the simulations to the Customer's requirements by defining a scope and by selecting the type of discovery, stager and credential access that can be leveraged by the decision engine to achieve an objective.

2.6.1 AVAILABLE STAGERS COMPARISON TABLE

Stager	Execution technique	Implant process	File type	Tested EDRs
Honeybadger stager	DLL side loading + APC injection	Remote	EXE, DLL	CrowdStrike Falcon, Sophos EDR, Trend Micro XDR, Microsoft Defender for Endpoint ATD, Trellix Mvision XDR
Mole stager	DLL side loading + callback function	Self hosting	EXE, DLL	Sophos EDR, Trend Micro XDR, Microsoft Defender for Endpoint ATD
Raccoon stager	APC injection	Remote	EXE	Sophos EDR, SentinelOne, Microsoft Defender for Endpoint ATD
Eagle stager	Callback function	Self hosting	EXE	Sophos EDR, Sentinel One, Microsoft Defender for Endpoint ATD

APV is delivered to the Customer in two parts, the initial assessment which will run the simulation, followed by a written report which will be delivered by an assessor, guiding the Customer through the recommendations found.

The simulations are limited to a total of 3 (three) per year with a gap of at least 3 (three) months between each simulation. Where the Customer requests for additional simulations this will be subject to an additional charge which will be quoted separately and detailed in the Work Order.

Within 45 (forty-five) days of the original simulation being run, Softcat will re-run the successful attack paths the simulation took to achieve any objectives, this is to help validate any remediation action the Customer has taken.

The follow up simulation must be completed within 45 (forty-five) days of the original simulation being run and cannot be extended. The assessor will confirm this window as part of the report delivery.

2.7 DETECTION RULE VALIDATION (OPTIONAL ADD-ON)

Where the Customer has opted for the Detection Rule Validation module, Softcat will review rules that are deployed in the Customer's environment through integration with their SIEM tooling. The available SIEM solution integrations are constantly updated, and the latest known available integrations can be found .

The integration enables Softcat to validate rules to identify quality and performance issues, highlight the detection coverage based on real world threats that matter to the Customer, and provides strong benefits to SOC ("Security Operations Centre") teams such as process automation, rule development, and correct log Resource management.

After the initial assessment is run against the detection rules, Softcat will work to best practice and examine the results with the Customer to prioritise the improvement insights in the rules according to the insight categories, aiming to see the improvements made in the next assessment and to then repeat the cycle.

Where an integration has taken place, Customers may incur additional costs related to ingestion and log storage according to their existing Agreements. It is important to note that any additional costs generated using the Service are the responsibility of the Customer and not included as part of this Service. For example, any costs related to ingestion and log storage which could occur with the integration of a SIEM platform and running simulations.

2.8 ATTACK SURFACE VALIDATION (OPTIONAL ADD-ON)

Attack Surface Validation ("ASV") is a module available to support attack surface management. ASV manages and automates the discovery, classification, and risk assessment of a Customer's internal and external cyber assets. It aggregates and normalises asset and vulnerability data from a range of sources, enhancing visibility and supplying insights to prioritise the security of users, hosts, Applications, and assets. ASV supports with the following use cases:

- Obtain a unified view of asset inventory – get all digital assets within a single view, including devices, users, Software, policies, and Vulnerabilities.
- Improve endpoint security hygiene - identify and manage endpoint security Agents that may be absent, non-operational, unregistered, or not complying with prescribed security policies.
- Discover and prioritise Vulnerabilities - pinpoint vulnerabilities across all assets, including devices, Software, users, and policies.

2.9 CLOUD SECURITY VALIDATION (OPTIONAL ADD-ON)

The Cloud Security Validation module helps support with cloud security posture management by identifying common cloud misconfigurations and overly permissive IAM ("Identity And Access

Management") policies, which are the two primary causes of cloud data breaches. This is achieved by using real-world cloud-specific attacks to uncover excessive user permissions that could enable attackers to compromise critical services. This information can then be shared along with actionable insights as part of the monthly workshops.

3. SERVICE LEVELS

3.1 PICUS PLATFORM

Picus Security is dedicated to providing its users with a reliable, uninterrupted experience. With the exception of any planned outage due to maintenance, Picus Security does its best to maintain a minimum uptime of 99.5% for users logging in and utilising the dashboard metrics.

Description	Metric	Target
Picus Platform availability	Uptime per month	99.5%

3.2 REPORTING & DASHBOARDS

Softcat will use reasonable endeavours to send the Assessment Report within ten (10) Working Days of the completion of any assessment and/or workshop (as applicable).

4. CUSTOMER RESPONSIBILITIES

4.1 THREAT EXPOSURE MANAGEMENT

When utilising the Service, Customers with existing Platforms may incur additional costs related to ingestion and log storage as per their existing Agreements. It is important to note that any additional costs generated using the Service are the responsibility of the Customer.

4.2 PICUS PLATFORM

a. Completing any pre-requisite documentation/actions provided ahead of the Service commencing.
b. Providing a list of all current deployed security tooling within the Customer's environment. This is required ahead of the Service commencing.
c. Provide Softcat with details for new users that require access. This includes ensuring that where relevant the required level of access is included.
d. Update Softcat on any changes in relevant personnel that are linked to the Service, including leavers.
e. Deployment of any Agents required into the Customer's environment.
f. A full system backup must be taken ahead of the engagement.

4.3 REPORTING & DASHBOARDS

a. The Customer must ensure the right stakeholders from their organisation attend the agreed workshops.
b. The Customer must participate in agenda setting for any of the monthly workshops so that Softcat can deliver the content and outcomes the Customer requires.

4.4 SERVICE DELIVERY ASSOCIATE

a. Keep authorised contact list up to date to allow Service Delivery Associates to provide the Service effectively.
b. 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.
c. Provide advanced notification to Softcat Support of any planned decommissioning of Softcat-related equipment or Software.

4.5 ATTACK PATH VALIDATION (OPTIONAL ADD-ON)

a. Before a simulation is run the Customer will be required to add SHA1 hashes to any endpoint protection on the device. These will be provided to the Customer in advance of the simulation taking place.
b. The Customer will be responsible for downloading and executing the provided simulation files. These will be provided in a secure manner to the customer in advance of the Simulation taking place.
c. Before a simulation is run the Customer will be required to ensure that any firewall in place is not blocking communication between the stager and relevant platform.
d. The Customer must ensure the initial access point being used for the simulation is on a computer that is joined to Microsoft Active Directory.
e. The Customer must ensure the simulation is run with a domain user, not a local user.

4.6 SECURITY CONTROL VALIDATION (OPTIONAL ADD-ON)

a. The Customer is responsible for deploying Agents (portable or installable), where these are used, in accordance with the simulations agreed.
b. The Customer is responsible for the on-going maintenance and patching for any additional infrastructure deployed to support agents, including any VMs.

4.7 DETECTION ANALYTICS (OPTIONAL ADD-ON)

Where additional Resources have been deployed within the Customer's environment, these Resources are the responsibility of the Customer, for example the updating and patching of any VMs ("Virtual Machines").

4.8 DETECTION RULE VALIDATION (OPTIONAL ADD-ON)

The Customer must complete any additional pre-requisites required to allow integration with their nominated Platform.

5. NOTABLE EXCLUSIONS

5.1 CONTINUOUS THREAT EXPOSURE MANAGEMENT

a. The Service does not include remediation of security risks or issues identified, or implementation of Get-Well recommendations following the monthly reports and/or workshops.
b. Softcat can Support remediation activity, but this would form a separate project and would be chargeable as additional work. Customers of the Service should contact their Softcat Account Manager and/or Service Delivery Manager with any queries.

5.2 SECURITY CONTROL VALIDATION (OPTIONAL ADD-ON)

Each Microsoft Windows Platform can only run a single Picus Windows Agent instance.

5.3 DETECTION RULE VALIDATION (OPTIONAL ADD-ON)

a. The creation of custom integrations. The available integrations can be found here.
b. The integration agent is not supported for use on SELinux ("Security-Enhanced Linux").

5.4 CLOUD SECURITY VALIDATION (OPTIONAL ADD-ON)

Only the following public cloud providers are supported:

- Amazon Web Services (AWS)
- Microsoft Azure (Azure)
- Google Cloud Platform (GCP)

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.

The Activation Date for the Service will be the day on which the Onboarding Period ends. 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, Contract Start Date 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, 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.

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 and 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/

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 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).

If, in the absence of a signed Work Order but following receipt of this Service Description, the Customer provides a purchase order 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 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