

Schedule 5: Security Services

1. INTERPRETATION

- 1.1 Except as defined in this Schedule 5, capitalised terms shall have the meanings given to them in the DEFINITIONS SCHEDULE.
- 1.2 To the extent applicable to the supply of Goods, in the event of conflict with the terms of this Schedule 5 and the Agreement, the provisions in this Schedule 5 shall take precedence and in the event of a conflict with the terms of this Schedule 5 and Order Form, the provisions of Order Form shall take precedence over this Schedule 5.

2. FOURNET SECURITY OPERATIONS CENTRE

- 2.1 FourNet's Security Operations Centre (SOC) provides a UK based managed service with security monitoring and incident response in order to provide protection to the Customer's infrastructure.
- 2.2 The included services from FourNet's SOC are detailed below as two different service offerings:

Service Description	FourNet SOC Lite	FourNet SOC
Honeypot Deployment	Included	Included
Threat Monitoring 24x7x365	Included	Included
Targeted Threat Insights	Included	Included
Monthly Security Reports	Included	Included
NMAP Scanning	Included	Included
UK Security Experts	Included	Included
DNS Email Record Checking	Included	Included
Dark Web Monitoring	Included	Included
Identity & Access Management	Not Included	Included
Expert Cybersecurity Training	Not Included	Included
SIEM Deployment & Integration	Not Included	Included
Threat Response 24x7x365	Not Included	Included
EDR & MDR Protection	Not Included	Included

2.3

3. SOC INCIDENT MANAGEMENT PROCESS

- 3.1 Following a cyber Incident being identified, a ticket is raised and categorised as follows:
 - 3.1.1 Unauthorised Access;
 - 3.1.2 Denial of Service;
 - 3.1.3 Malicious Code;

- 3.1.4 Scans or Probes;
 - 3.1.5 Attempted Access;
 - 3.1.6 Investigation; or
 - 3.1.7 Exercise.
- 3.2 If the incident is found to be Priority 1 or 2, then the SOC Manager and the Customer's official channels shall be informed. When informing the Customer, this is facilitated via a phone call. Any e-mail or CRM ticket communication will be kept vague and no sensitive information will be communicated through these routes. The secure details of the Incident will be stored within the ticket in the SIEM.
- 3.3 Following analysis of the Incident, actions shall be taken by FourNet to contain the Incident to avoid escalation or a spread of the issue to other systems.
- 3.4 When the Incident is resolved, the Incident will be closed. Incident closure means that the the vulnerability that led to the Incident have been closed and all Incident traces have been cleansed. The closure process includes testing systems to ensure that the eradication steps and controls were effective, and that the vectors used by the attack do not exist anymore or are ineffective. Any final information about the event will be added to the ticket in the SIEM.
- 3.5 All Incidents are managed 24 hours a day, 7 days per week.

4. INCIDENT PRIORITIES

4.1 The following table displays the Incident classifications:

Priority Level	Definition
Priority 1 (MI)	Critical Incident Total Loss of the supported service(s) affecting more than 30% of the supported service(s) across the customers estate.
Priority 2 (MI)	Major Incident Partial or Total Loss of the supported service(s) affecting between 5%-30% of the supported service(s) across the customers estate.
Priority 3	Minor Incident Partial or Total Loss of the supported service(s) or loss of functionality affecting less than 5% of the supported service(s) across the customers estate.
Priority 4	Request for Information Technical question or product support.
Priority 5	Moves, Adds, Changes, Deletions (MACD) Request to make a change on the customers system. Unless explicitly defined in the Order Form, these requests carry an additional charge.
Priority 6	Problem Case Root Cause or Trend Analysis required.

5. FOURNET SOC INCIDENT NOTIFICATION AND INVESTIGATION TIME

- 5.1 For the avoidance of doubt, the following paragraph 5 does not apply to Customers who have purchased FourNet SOC Lite.
- 5.2 When an Incident occurs, FourNet will communicate with the Customer and investigate the cause of the Incident. The following table sets out the Target Notification and Investigation Times for each Incident.

- 5.2.1 The Target Notification Time is the time elapsed between FourNet becoming aware of the Incident to providing the Customer with initial analysis of the event.
- 5.2.2 The Investigation Time is the total elapsed time that FourNet is expected to spend on the Incident before providing the Customer with an outcome.

Priority Level	Severity Description	Target Notification Time	Target Investigation Time
Priority 1	Critical	15 minutes	30 minutes
Priority 2	High	30 minutes	1 hour
Priority 3	Medium	1 hour	2 hours
Priority 4	Low	1 hour	3 hours

6. CHANGE MANAGEMENT

- 6.1 FourNet use Change Management to ensure that any changes made to the Customer's environment are considered, controlled and communicated. Following the submission of a Request for Change (RFC), The Change Advisory Board (CAB) must approve the change before the engineering team schedule work to be carried out. The Change is then sent to the Customer for review and presented to their own CAB. This CAB is responsible for reviewing and approving:
- 6.1.1 The change as a whole;
 - 6.1.2 The scope of the change;
 - 6.1.3 Necessary risk assessments;
 - 6.1.4 The technical scope of works for the change;
 - 6.1.5 The technical scope of works for backing out of a change;
 - 6.1.6 Post-change test and verification plan; and
 - 6.1.7 Time window for the change, the platform environment and any pre-defined milestones.
- 6.2 FourNet will attend and support the Customer CAB where required.
- 6.3 The following categories of Change are used:
- 6.3.1 Standard Change: this is a Change that is low risk, and utilises a pre-approved and documented procedure.
 - 6.3.2 Normal Change: this is a Change that is not pre-approved and requires a Request for Change to be submitted to the CAB.
 - 6.3.3 Emergency Change: this is a critical Change that required immediate implementation, and Emergency Change Advisory Board should be convened to review the Change in a timely manner.
- 6.4 A Change is defined as 'failed' when an Incident is created post Change; the Change has to be reverted; or the Change has been cancelled.
- 6.5 Following a failed Change, a Post Implementation Review will be conducted by FourNet to establish the Root Cause. The results of the Post Implementation Review will be shared with the Customer upon completion.

7. SERVICE CREDITS

- 7.1 Unless explicitly agreed in the Order Form, Service Credits are not applicable to Security Services.

8. EXCLUSIONS

- 8.1 Security Services will be delivered remotely, as such, on-site support visits are not included as part of the standard service offering. In the event that an Incident necessitates an on-site visit to resolve a service issue, such visits shall be considered outside the standard service scope and will be subject to additional charges.
- 8.2 Hardware maintenance is not included in this Service.