Service Schedule

Threat Detect Managed SIEM

08/05/2025 Node4 Limited PUBLIC

Introduction

This schedule contains additional terms and conditions, service description and service levels applicable to the Threat Detect service and should be viewed with associated Order Form, Node4's General Terms and Conditions and the Acceptable Use Policy

1 Overview

The Threat Detect service offers a managed Security Incident and Event Management (SIEM) solution, based on Microsoft Azure Sentinel. The service features of Threat Detect are described below.

Incidents and events identified by the service may be critical to the security integrity of the Client or minimise the potential impact. It is imperative that the Client ensures any contact information and escalation path is up to date and includes appropriate representatives that can respond and remediate.

2 Definitions

"Asset" means a device, appliance, software application, or system monitored by Node4's Security Operations Team.

"Breach" means an incident that results in the confirmed disclosure, alteration, or unauthorised use of sensitive information or system access by an entity not authorised to do so.

"Charges" means charges as described in this Schedule and, where relevant, set out on the Order Form, and shall be payable by the Client in accordance with Node4's Terms and Conditions.

"Client Responsible Incident" means that if a Service Affecting Incident is identified as being attributable to the Clients, such as Client provided equipment, premises, power supplies, the actions of the Client, or the actions of its employees or agents, then the Incident shall be deemed the responsibility of the Client. Any downtime shall not be included in service availability measurements and does not qualify for compensation.

"Custom Data Connector" means a user-defined or third-party defined integration or data interface that enables data ingestion into the Azure Sentinel SIEM from sources that do not have a native connector.

"Incident" means an unplanned interruption to a service or a reduction in service quality.

"Installation Charge" means charges payable by the Client for the installation of the service, by way of a Technical Onboarding process, as provided on the Order Form.

"Monthly Review Period" means the calendar monthly periods commencing on the 1st of each month during the Term, over which Service Levels and Service performance measurements are calculated.

"Planned Outage" means proactive work required to maintain the service. Node4 may, with reasonable notice, require a temporary outage. Wherever possible, Node4 will agree the outage with the Client in advance. Any planned downtime shall not be included in fault or Service Availability measurements.

"Professional Service Charges" means the professional service charges detailed on the Order Form or otherwise agreed in writing between the Parties.

"Recurring Service Charge" means the recurring fees payable by the Client for the provision of the service, as specified on the Order Form.

"Risk" means the potential for loss or damage to an organisation's assets, measured as the likelihood that a threat will exploit a vulnerability and the magnitude of the resulting impact.

"Security Incident" means a security event, real or suspected, that compromises the confidentiality, integrity, or availability of information assets, or that violates an organisation's security policies.

"***Security Incident Response***" means the coordinated process and set of procedures executed by the Client or its nominated third party to detect, analyse, contain, mitigate, and recover from security incidents that compromise the confidentiality, integrity, or availability of the Client's information systems or data. This process may include the execution of a pre-defined incident response plan, communication with relevant stakeholders, forensic analysis where necessary, and the implementation of corrective measures to prevent recurrence.

"Service Availability" means the time for which a Node4 service is usable, expressed as a percentage of the total time in each Service Measurement Period, excluding any periods during which the Threat Detect service is unavailable due to a Client Responsible Incident or a Planned Outage.

"Service Credits" means where specifically stated in a Schedule Document and/or Order Form, the credits due to the Client, which shall apply upon non-achievement of Service Levels.

"Service Desk" means the single point of entry for all service tickets and Service Requests, which can be accessed by telephone, email, or via the Node4 service portal.

"Service Levels" means any service levels applicable to the Services as set out in this Schedule Document.

"Service Measurement Period" means the calendar month for which the Service is measured.

"Service Request" means a request for a change or for information.

"SIEM" means Security Information and Event Management, the software used by Node4 to process log data and events from Assets.

"SOC" means Security Operations Centre, comprising Node4's Security Operations Team – a team of security professionals who

operate the service with the primary aim of identifying threats and incidents.

"SoW" means Statement of Work, a document that details the scope, activities, outcomes, and timescales for a project or piece of work.

"Standard Data Connector" means a prebuilt or out-of-the-box integration or data interface that Node4 has experience in implementing and supporting, which enables the ingestion of logs, alerts, and telemetry from various data sources into the Azure Sentinel SIEM.

"Technical Onboarding" means the set of technical activities scoped in the Statement of Work and agreed in a project plan, undertaken through interactive collaboration between the Parties to help ensure successful use of the service by the Client.

"Third Party Attributable Incident" means that if a Service Affecting Incident is identified as being attributable to a third-party of the Clients, such as third-party provided equipment, premises, power supplies, the actions of the third-party, or the actions of its employees or agents, then the Incident shall be deemed the responsibility of the Client. Any downtime shall not be included in service availability measurements and does not qualify for compensation.

"Threat" means any circumstance or event, whether intentional or unintentional, that has the potential to cause harm to an organisation's information systems, processes, or data.

3 Specific terms

The following specific terms and conditions shall apply when the Threat Detect service is provided to the Client.

3.1 Termination resulting from client delays

If the Client fails to approve the project plan agreed upon as part of Technical Onboarding or fails to provide the information necessary to implement that plan, and such failure or delay causes any activity on the plan's critical path to be delayed by more than twenty-five (25) Business Days, Node4 may terminate the Client's order for the Threat Detect service. In the event of such termination, Node4 may charge the Client for any expenses incurred (including labour fees) up to the date of termination.

3.2 Licence removal

Upon the termination or cessation of the Threat Detect service, the Client must remove all Threat Detect licences from its devices and infrastructure within one (1) month of the effective termination date.

3.3 Continuous data transmission

The Threat Detect service requires all relevant systems to remain available and continuously transmit data to the managed SIEM. The Client acknowledges that any disruption to this data feed may result in incomplete information retention and reduced alert or event visibility. In such circumstances, Node4 shall not be responsible or liable for any failure of data transmission from the Client's systems, or any resulting limitations on the service.

3.4 Client security responsibilities

The Client shall take reasonable steps to maintain a secure environment by following

industry best practices – such as applying timely updates and patches and using appropriate security settings. Should the Client fail to do so, resulting in an increased number of alerts, Node4 may charge additional fees based on the extra resources required to manage those alerts.

3.5 Fair usage

The Threat Detect Service is subject to a fair usage policy. The alert volume threshold is agreed on a per-client basis, taking into account the Client's specific environment and the number and type of data connectors deployed. If the alert volume exceeds this agreed threshold due to Client actions or conditions, Node4 reserves the right to charge additional fees on a pro rata basis at its standard rates. Node4 may periodically review and update these thresholds and will provide the Client with at least 1 months written notice of any such changes.

3.6 Intellectual property

All intellectual property rights, including but not limited to patents, copyrights, trade secrets, trademarks, and any other proprietary rights, in any materials, software, methodologies, documentation, deliverables, custom rule sets, custom analytics and any Custom Data Connectors provided by Node4 in connection with the Threat Detect service shall remain the exclusive property of Node4 or its licensors. Node4 hereby grants the Client a limited, non-exclusive, non-transferable, royalty-free licence to use such deliverables solely for the purpose of receiving the Threat Detect service during the term of this Agreement.

Any intellectual property provided under this Agreement is supplied on an "as-is" basis, without any express or implied warranty or guarantee of suitability for any particular purpose, including without limitation any warranties of merchantability, fitness for a particular purpose, or non-infringement.

The Client shall not copy, modify, reverse engineer, decompile, disassemble, or create derivative works from any deliverables, nor distribute or sublicense them except as expressly permitted in writing by Node4. Any feedback, suggestions, or recommendations provided by the Client shall be deemed non-confidential and may be used by Node4 without any obligation of compensation. The Client's use of any third-party software incorporated in the Threat Detect service shall be subject to the applicable third-party licence agreements. Except as expressly granted herein, all rights not specifically granted to the Client are hereby reserved by Node4.

3.7 Exclusion of third-party dependencies

The Client acknowledges that the Threat Detect service is dependent on Microsoft Azure Sentinel and other third-party products or services. Node4 shall have no liability for any service interruptions, modifications, or cancellations arising from actions taken by Microsoft or any third-party provider. In the event that Microsoft or any other third party modifies, suspends, or terminates the services upon which Threat Detect relies, Node4 shall not be held responsible for any resulting impacts on service performance or functionality. The Client agrees that such changes may affect the performance of the Threat Detect Service and that any necessary adjustments or additional costs resulting from these changes shall be borne by the Client.

3.8 Warranty disclaimer

Node4 does not warrant that the Threat Detect service, Microsoft Sentinel, or Microsoft threat intelligence will detect or prevent all possible threats or vulnerabilities,

nor does it guarantee that these services will render the Client's network and systems invulnerable to security Breaches or vulnerabilities. The Client accepts that the Threat Detect service cannot provide insight into every potential risk to the Client's IT systems and operations.

Additionally, the Client bears sole responsibility for the accuracy of any data or information it provides to Node4 and shall remain liable for all costs and expenses resulting from third-party claims of loss or damage (including reasonable legal fees) arising out of inaccuracies in such data or information.

4 Fees

Charges may include any or all the following: Installation Charges, Professional Service Charges, and Recurring Service Charges.

4.1 Installation charges

Installation Charges for implementing the service shall be detailed on the Order Form. Installation Charges shall be invoiced upon completion of the installation work.

4.2 Recurring service charges

Recurring Service Charges are determined based on the service option selected and any related services, as specified on the Order Form. These charges are payable monthly, quarterly, or annually in advance. Recurring Service Charges shall commence on the earlier of the date of service handover or the service kick-off meeting.

4.3 Connector removal

The Client may request, in writing via a Service Desk ticket, that individual connectors cease to be integrated into the service. However, the total number of connectors and associated fees will only be reassessed at the time of contract renewal.

4.4 Scoping of renewals

When renewing under a new agreement, the total number of connectors will be recalculated to determine the ongoing service fees. If the Client requires Node4 to remove connectors, this reduction may only be applied at the end of the initial term.

4.5 Additional professional services

A range of Professional Services are available to undertake tasks and management not included in this service. The Professional Service Charges include but are not limited to:

- Mitigation of the risks identified through use of the service.
- Management of mitigations for the client's networks - network appliances, servers and applications.
- Incident response through Node4's Security Incident Response partner.
- Data Retention and Storage Management services (to manage the cost-effective storage of logs).
- Completion of tasks or requests that require Node4 personnel to visit a client's site.
- Training and enablement activities
- Bespoke documentation and non-standard reports.
- Offboarding and termination support, such as data extraction or transfer assistance.

The Professional Services are subject to the price list below. Specific rates for large or repeat orders can be agreed on a case-by-case basis in writing.

Additional tasks undertaken at the request of the Client by Node4 personnel, will be charged at rates agreed between the parties in advance.

5 Client responsibilities

To onboard and deliver the service, Node4 requires the Client to:

- Work with Node4 to compile and agree on a Statement of Work (SoW) before placing an order.
- Ensure that all details captured in the SoW that are materially important to the successful delivery of the service are accurate.
- Include in the SoW a list of key contacts for the service, specifically designating contacts for alerts. This information is critical to effective service delivery, and the Client is responsible for promptly notifying the Security Operations team of any changes or updates to these contacts throughout the life of the service.
- Provide the required administrative access to the relevant subscription or resource group to enable Node4 to deploy and manage the Microsoft Sentinel instance and any additional required resources.
- Provide all technical prerequisites (e.g. network configurations, firewall rules, identity management, log forwarding) necessary for the successful deployment and integration of the SIEM system.
- Assume responsibility for all Microsoft Azure charges, including those relating to the ingestion and storage of logs within the environment.
- Retain all logs within Microsoft Azure for a minimum of 90 days, ensuring these are accessible to the SIEM system, and grant Node4 access to these logs to support the Threat Detect service.

6 Service provision

6.1 General

The Threat Detect service comprises two key phases: Technical Onboarding and Ongoing Service Management.

Prior to the commencement of Ongoing Service Management, Node4 will schedule a Technical Onboarding kick-off meeting to introduce the Threat Detect service delivery team, confirm the appropriate Client contacts, and discuss the scope and business impacts of the service.

Node4 shall prepare a project plan outlining key milestone, tasks (with assigned priorities), checkpoints, a timetable for progress reviews, and overall project timescales. The Client is required to approve this plan before any tasks specified in the Statement of Work (SoW) can commence.

The benefits of the Threat Detect service begin with the kick-off meeting at the start of the Technical Onboarding phase, with the full benefits realised only upon the successful completion of all activities detailed in the SoW.

Event and alert monitoring are available only for servers, applications, and assets that have been successfully onboarded into the service.

During both the formulation of the project plan and the Technical Onboarding process, the Client may propose changes to the project plan, or the Threat Detect service. Node4 will assess such proposals and may require the Client to sign a new Order Form to reflect the changes and any resulting impact to the service fees.

6.2 Service sizing

The sizing of the Threat Detect service is dependent on the following

- Quantity of standard connectors
- Quantity of customer connections
- Quantity of users
- Quantity of servers, firewalls and other assets integrating with the SIEM

A list of Standard Data Connectors can be shared during compilation of the Statement of Works.

Complexity based connectors are added to determine the service option, this is dependent on the number of firewalls, servers and users. The impact on the number of connectors is shown in the table below:

Item	Unit	Additional Connectors
Firewalls	Each 5	1
Servers	Each 50	1
Users	Each 1000	1

6.3 Data connectors

Data Connectors are included up to the number supported under the Threat Detect service option purchased, as specified on the Order Form. This total number comprises all Standard Data Connectors and any pre-agreed Custom Data Connectors.

Custom Data Connectors may be added to the Threat Detect service and are subject to additional fees unless otherwise stated on the Order Form or in the SoW. Where pre-agreed, development of Custom Data Connectors may be completed as part of the Technical Onboarding process.

Professional services for adding Custom Data Connectors that are not pre-agreed are subject to availability and will incur additional fees. The Client may not use the professional service days included in the Technical Onboarding for any subsequent service changes beyond twelve (12) months from the completion of Technical Onboarding.

Once a Custom Data Connector has been successfully onboarded, it is added to the total count of connectors managed under the Threat Detect service.

6.4 Deployment location

Microsoft Azure Sentinel can be deployed in various geographic regions. If the Client has commissioned Node4 to deploy a SIEM on its behalf and has specific requirements regarding data residency or compliance, these must be specified in advance by the Client and included in the SoW.

6.5 Modification of scope

Once the scope of Technical Onboarding has been agreed, no further changes may be made to that scope. However, additional services or additional Custom Data Connectors may be added subject to additional fees and an associated SoW.

7 Service features

The size of the Threat Detect service is determined by the complexity of the Client's IT estate and the number of data connectors required. There are three service options, as detailed below:

	Small (1-10 Connectors)	**Medium** (11-20 Connectors)	**Large** (21-30 Connectors)
Standard Connectors	Maximum of 10	Maximum of 20	Maximum of 30

Time Allocation included in Technical Onboarding for Custom Connectors	5 days	5 days	5 days
Network Threat Alerts	Yes	Yes	Yes
Custom Threat Alerts	Yes	Yes	Yes
Use Cases (Client Specific Threat Scenario Rules)	1 per year	3 per year	5 per year
Security Analyst	1 hour per calendar month	3 hours per calendar month	5 hours per calendar month
Frequency of Reports and Review Meetings	Monthly – 1 standard report	Monthly – 1 standard report	Monthly – 1 standard report
Live Dashboards	Yes – 1 additional may be added each month	Yes – 3 additional may be added each month	Yes – 5 additional may be added each month

7.1 Network threat alerting

Node4 will provide network threat alerting by ingesting firewall logs, including traffic logs, which are then matched against Node4's internal and external threat feeds. While individual events may appear harmless in isolation, the aggregation of multiple events or the inclusion of contextual data may reveal patterns indicative of harmful activity. These events will be evaluated in the context of the Client's environment to better assess risk. This feature will not be available if the Client fails to, or is unable to, forward logs from its firewalls to the SIEM.

7.2 Custom threat alerting

During Technical Onboarding, the Client shall define any custom alerts that are required to be monitored. These custom alert requirements will be incorporated into the Client's standard report. In subsequent monthly reviews, any new custom alert requirements identified by the Client will be considered for inclusion in the service. However, these may be subject to additional fees.

7.3 Client use cases

Node4 will work with the Client to map high-level business risk scenarios into actionable use cases. In this process, Node4 will group analytic rules, incidents, workbooks, playbooks, and hunting queries to address these scenarios. The resulting use cases are designed to detect threats, aggregate alerts, provide visual insights, and proactively search for potential threats, thereby enabling more targeted security management. Each use case is subject to a fair use limit of 2 days of development time. Where the creation of new rules is required as a result of a use case, such rules may be made available to all Clients subscribing to the Threat Detect service, where deemed appropriate by Node4.

7.4 Threat notifications

The Client will be notified in accordance with the contact details and escalation path provided to and agreed by Node4. It is the Client's responsibility to update Node4 promptly with any changes to these details. Node4 will make repeated attempts to notify the Client using the current contact information as described in the Service Management section of this schedule. Node4 shall not be held responsible where the Client fails to acknowledge notifications.

Furthermore, it is the Client's responsibility to act upon such notifications. Node4 will not log on to any asset unless specifically instructed to do so as part of a separately commissioned Incident Response or Post-Attack Forensic service, and only where authorised to do so and covered by a separate service, such as a Node4 managed infrastructure service.

7.5 Ongoing reporting and communications

Node4 will designate a named Security Operations Team analyst as the primary point of contact for the Client. Each month, the analyst will prepare a report documenting the alerts from the previous month, identifying areas for improvement, and providing integrated changes and recommendations. This monthly report will be emailed to the Client's designated contact as specified in the Statement of Work (SoW) or as updated by the Client thereafter. The report will include summaries of alarms, security events, and security metrics, as well as an overview of Security Incident handling with recommendations for continuous improvement.

Additionally, a monthly online review meeting will be scheduled, subject to mutual availability, during which the analyst may share industry insights or Node4-specific threat intelligence. Requests for edits to existing reports or for additional reporting items will be considered subject to the fair use policy.

Node4 reserves the right, at its sole discretion and without prior notice, to either temporarily appoint a substitute Security Operations Team analyst or permanently replace the designated analyst to cover the role for any reason, including, but not limited to, absence, unavailability, or termination of employment with Node4.

7.6 Security analyst resource

The Services include a monthly allocation of Security Analyst consultation time, as indicated on the Order Form. This allocation is non-transferable and cannot be carried forward to earlier or subsequent months.

8 Service management

This section pertains exclusively to the management of the SIEM instance used for the Threat Detect service and the handling of alerts, it does not cover any Client systems or Client infrastructure.

8.1 Service levels

The Threat Detect service offers the following Service Levels:

Service Level	Service Hours
Gold	Priority 1 and 2 - Support hours 24/7 Priority 3,4 and Service Request (P5) - Support hours between 7am and 7pm weekdays, excluding bank and national holidays

8.2 Response times

Node4 aims to respond to and update Incidents related to the availability of the Threat Detect service within the following timeframes:

	P1	P2	P3	P4	P5 (Service Request)
Faults & Technical Queries Acknowledgement*	30 Mins	30 Mins	1 Hour	2 Hours	1 Day
Investigation and Triage Actions Commence	1 Hour	2 Hours	4 Hours	12 Hours	N/A

Time is counted only during the service hours applicable to the selected service level, as detailed above and stated on the Order Form. These response times do not apply in cases of Client Responsible Incidents, Third-Party Attributable Incidents, or events beyond Node4's reasonable control, and such incidents will be excluded from reporting.

All Priority 1 and 2 faults must be raised via the Service Desk by telephone. If a Priority 1 or 2 incident is raised via the Service Desk portal or e-mail, the Client must follow up with a phone call to ensure immediate commencement of work.

Service Requests (P5) requiring implementation outside the applicable service level and associated hours of operation are subject to additional professional services fees.

8.3 Monitoring and detection

Node4 will maintain continuous monitoring of the Client's environment in line with the agreed service level. Where the monitoring platform classifies an event or alert as high risk, a Security Engineer will review it within thirty (30) minutes of that alert being raised.

8.4 Alert classification and notification

In addition to any Incidents impacting service delivery, Threat Detect includes a service level for notifying the Client of alerts or events that Node4 determine may evolve into a Priority 1 Incident.

When reviewing alerts and events from Threat Detect monitoring, the Security Engineer will assess the risk based on factors such as the frequency and number of alerts, their context within the Client's business, and the risk profile shared with Node4. The final determination of an incident's priority is based on the judgment of Node4's Security Operations team, informed by professional expertise, rulesets, machine learning, industry insights, experience, and prior knowledge of the Client's environment and risks.

Once assessed, the risk is mapped against impact priorities defined as follows:

Priority Level	Description
Priority 1 (P1)	Very high impact (e.g. suspicious data exfiltration, active ransomware, major data Breach, complete system outage)
Priority 2 (P2)	Significant impact (e.g. suspicious user activity, significant data loss, major security vulnerability)
Priority 3 (P3)	Priority 3 (P3): Moderate impact (e.g. indicators of compromise, malware on non-critical systems, unauthorised access attempts)
Priority 4 (P4)	Low impact (e.g. blocked phishing attempts, multiple failed login attempts, minor protocol issues)
Priority 5 (P5)	Incidents that do not have immediate impact but may require future attention (e.g. new login location alert within expected region)

8.5 Incident triage and investigation

For Priority 1 Security Incidents, Node4 will initiate investigation and triage promptly. Once a high-risk alert is identified, a Security Engineer will review it within thirty (30) minutes of that alert being raised. Following initial review, if the alert or event is confirmed as a credible threat, Node4 will notify the Client within one (1) hour of the alert being raised. From that point forward, the Client will receive regular updates on the incident status no later than every one (1) hour until the alert has been fully triaged or downgraded. An Incident Manager will be assigned to coordinate the investigation, ensure regular progress updates are provided to the Client, and collaborate with other Node4 teams as needed. This triage process does not constitute a comprehensive Security Incident Response service, which remains the Client's responsibility.

8.6 Incident response

Where Node4 acts as the Managed Service Provider for assets affected by a Security Incident, the incident will be escalated to the relevant Node4 Managed Services teams for technical remediation as directed by the Security Operations team. Once a Security Incident reaches an appropriate priority level, the Managed Services team will manage the incident per the Node4 Incident Management Schedule Document. However, the scope of this Incident Management does not extend to comprehensive Security Incident Response activities, such as full restoration, people/process management, public relations, or broader incident response measures.

For assets managed by the Client or their third parties, the Client will be advised and must arrange for technical remediation independently. If Security Incident Response is required, the Client is responsible for executing those measures separately.

8.7 Security incident handling

The Threat Detect service does not remediate Security Incidents that are detected and triaged through alerts and events highlighted by the service. However, although under no obligation to do so, Node4 reserves the right to take reasonable steps to intervene where it has legitimate access, to isolate systems and servers to contain a threat –particularly in circumstances where inaction may place the Client's data, other systems, other Node4 Clients, associated third parties, or the Node4 network at risk.

Where the Client has engaged services from Node4's Security Incident Response partner, the Incident Manager responding to the incident will alert this third party, providing updates regarding the incident and including their representative as part of the response team.

8.8 Unacknowledged notification andescalation

In the event Node4 is unable to obtain acknowledgement or response from the Client after the initial notification of a high risk alert or Priority 1 Security Incident, the Security Engineer will make repeated and escalating attempts to contact the Client.

At the first level of escalation (Level 1), the Engineer will attempt to reach the primary contact at least three (3) times. If those attempts fail, the Engineer will escalate to the second level of contact (Level 2) and make at least two (2) further attempts. If there is still no response, the Engineer will escalate to the third level of contact (Level 3) and make at least one (1) attempt.

Should the Client remain unresponsive after exhausting these escalation points, Node4 reserves the right to cease further contact attempts. Where the Client has provided fewer than three contact levels, the escalation process will end once the highest available contact level has been reached without success.

9 Exclusions

The Threat Detect service expressly excludes the following services and features:

- On-site installation, architectural design, and policy design services
- Policy or configuration reviews
- Development of cyber incident response plans or custom playbooks
- Technical remediation of Client devices or infrastructure
- Threat hunting
- Digital forensics
- Security Incident Response

These exclusions remain the responsibility of the Client or their third-party providers,

unless separately contracted with Node4 under a distinct service agreement.

10 Service credits

Node4 will provide the Client with Service Credits as set out below.

10.1 Service performance

Service performance is calculated as the percentage of closed Incidents during a month that were acknowledged and for which investigation commenced within the agreed Service Levels (Service Credits will only apply if a minimum of 10 closed Incidents are recorded during the month).

The applicable Service Credits are as follows:

Service performance during monthly review period	Service Credit as a percentage of monthly fees
90% or above	N/A
Less than 90% but 80% or above	5%
Less than 80%	10%

10.2 Service credit calculation

If a Monthly Review Period covers only part of a month, any Service Credit will be applied on a pro rata basis to the Monthly Charge.

Service Credits are calculated monthly, aggregated, and then credited to the Client on a quarterly basis.

If the service is cancelled during a Monthly Review Period, any applicable Service Credits will be calculated on a pro rata basis.

The Client must submit any claim for Service Credits in writing within twenty-one (21) Business Days from the date the Client could reasonably have become aware that such credits had accrued. No Service Credits will be granted unless Node4 receives written notice of the claim. If Node4 requires further information to process the claim, the Client shall provide its reasonable assistance.

10.3 Service credit exclusions

Service Credits will not be payable for any reduction in service availability or performance resulting from Incidents or disruptions caused by:

- The actions, negligence, or omissions of the Client, its employees, agents, or contractors
- The Client's failure to comply with Node4's Terms and Conditions
- Any Incident or issue associated with the Client's own equipment, infrastructure, or data connection
- Any event described in the Force Majeure clause of Node4's Terms and Conditions
- A failure by the Client to provide Node4 with any items specified in the Client Responsibilities section
- Excessive alert volume – defined as the alert volume exceeding any agreed levels by 20% or more for three consecutive months, or exceeding Node4's fair usage policy
- Planned or unplanned outages of the Microsoft Azure platform
- Maintenance during any Planned Outage

Service Credits shall apply only once per Breach of any target arising from the same occurrence.

The provision of Service Credits shall be the sole and exclusive remedy for any failure to meet the service targets for the Threat Detect Service. Node4 shall have no additional liability to the Client.