Schedule document

N4Threat detect

PUBLIC
Node4 limited
07/07/2021

Schedule document

N4Threat detect

Additional terms, Service Description & Service Level Agreement for N4Threat Detect SIEM Services.

1. Service description

"N4Threat Detect" offers Monitoring and Scanning services for a selection of security devices, applications and systems listed as an Asset. The different service features of N4Threat Detect are described below.

Information discovered by the service will be critical to the security integrity of the client. It is important that the information from the service is escalated to the appropriate areas within the client's organisation that mitigating actions can be taken by the clients IT department.

2. Definitions

"Additional Terms" means this Schedule forming which describes the Products and Services to be provided and the relevant service levels.

"***Asset"*** A device, appliance, software application or a system which is monitored by Node4's Managed Security Services.

"Charges" means charges as described in this Schedule and where relevant set out in the Order Form, and shall be payable by the Customer in accordance with Clause 7 of Node4 Terms and Conditions;

"Customer Responsible Incident" means in the event that a Service Affecting or Non-Service Affecting Incident is identified as being attributable to Customer Provided Equipment, Premises, Customer power supplies, or the action of the Customer, employees or agents of the Customer, the Incident shall be deemed the responsibility of the Customer. Any downtime shall not be included in service availability measurements and does not qualify for compensation.

"Exploit" A method to use a Vulnerability to gain unauthorised access to functions, data, or privileges with malicious intent. An exploit can include a script, virus, Trojan, or a worm. The exploit is mainly defined by the way it replicates and spreads. An attack is the use of an Exploit.

- A script refers to a document with steps to manually find and exploit vulnerabilities. A script is replicated by publishing it.
- A virus refers to malicious software attached to a medium (e.g., files, removable media, and documents). A virus replicates using this medium.
- A Trojan refers to malicious software embedded in applications. The Trojan will not replicate itself; it spreads with the application.
- A worm refers to a self-contained program (or set of programs) that spreads copies to other computers. A worm can spread through network connections and e-mails in a matter of hours.

"HIDS" Host Intrusion Detection System. A software agent installed on a server providing security related information to the SIEM for use with Intrusion detection.

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

"Installation Charge" means charges payable by the Customer for the installation of Firewall Services as provided in 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,

"Non-Service Affecting Incident" means an Incident or condition which is not a Service Affecting Incident.

"Penetration Test" Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

"Planned Outage" means proactive work required to maintain the service provided, Node4 may with reasonable notice require a temporary outage in service. Wherever possible Node4 will agree the

outage with the Customer in advance of the required work. 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 in accordance with Clause 3 below;

"SEIM" Security Event and Incident Management – Software used by Node4 to process log data and events from Assets. Its functions include:

- Normalisation – converting entries in logs and individual alerts into generalized Events independent of the device and its brand or version.
- Classification – giving Events a first classification, using Node4 proprietary Event Classification Policy Language, filtering out false positives or Events related to vulnerabilities absent in the targeted environment.
- Pattern matching – recognising patterns pointing to reconnaissance scans, infections or attacks.
- Statistics – calculating averages to discover trends and anomalies, and to allow comparisons.
- Workflow management – recording the activities for an Incident.
- Information management – managing the information needed to examine, evaluate, and classify Incidents.
- User management – defining the views and authorisation levels of users

"Service Availability" means the time for which a Node4 service is usable, expressed as a percentage of the total time in a given Service Measurement Period, excluding to the extent that the N4Threat Detect service is unavailable due to a Customer Responsible Incident or during a Planned Outage.

"Service Desk" means the single point of entry for all Service Tickets and Service Requests which can be accessed over the phone, by email or via our portal.

"Service Levels" means as set out at clause 7.3 of this document.

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

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

"Service Ticket" means the tickets which are raised in relation to Incident or Service Request

"Security Dashboard" Customer portal where customers can have a near real time view on the events/incidents being processed, and where they can view the company's security posture and effectiveness.

"Threat" A (suspected) use of an Exploit, or the (suspected) presence of a Vulnerability in the configuration, platform, of application code. A Threat can be an infection by a worm or virus, or it can be a targeted attack. Exploits can also combine into Blended Threats, exploiting multiple security weaknesses or defects

"Threat Signature" Code used to recognise a Threat by its pattern. A Threat Signature may contain algorithms to detect dynamically changed malicious behaviour, combat obfuscation, or impersonation.

"Vulnerability" A weakness or defect that can be exploited to gain access to data, functions, or privileges violating the intended authorisation. Vulnerabilities can range from defects in application or system software (e.g. bugs), in the user administration (e.g. non-protected user accounts), in the configuration (e.g. unintended network or file access), in the policy and rule set definition (e.g. unrestricted open ports or exposed IP-addresses), etc. The combination of all vulnerabilities of a given system or infrastructure is the exposure.

3. Specific terms

The following terms and conditions shall apply when Node4 provides N4 Threat Detect Services to the Customer.

3.1 Minimum commitment

The service is subject to a minimum contract term as defined on the Order Form. For termination of the services, there is a minimum notice period of 90 days written notice the earliest of which can be given at the end of the Initial Term.

3.2 Assumption of risk

N4Threat Detect involves the use of network scanning and testing technology that has inherent risks, including, but not limited to, the loss, disruption, or performance degradation of a Customer's or a third party's business processes, telecommunications, computer products, utilities, or data (the "Scanning and Penetration Tests Risks"). The Customer authorises Node4 to perform the network scanning and assumes all risk for adverse consequences resulting from associated with such component of N4 Treat Detect. Node4 shall take reasonable steps to mitigate these Scanning Risks; however, the Customer understands that these Scanning Risks are inherent in the provision of certain computer security services and the use of certain computer security products and cannot be eliminated.

3.3 Security service advisor

The Services contain allocated time per month for a Security Service Advisor to consult with the Customer. This time cannot be transferred or rolled over to earlier or later months.

3.4 Warranty

Node4 does not warrant that N4Threat Detect will detect and prevent all possible threats and vulnerabilities or that such services will render the Customer's network and systems invulnerable to all security breaches and vulnerabilities.

The Customer hereby assumes the sole responsibility for the accuracy of the IP addresses and domains provided to Node4, and the Customer will be liable for all costs and expenses from any third party claims of loss, damage (including reasonable attorneys' fees) and liability of any kind that may be incurred as a result of the inaccuracy of accuracy of the IP addresses and domains provided to Node4 by the Customer.

3.5 Suspension of service

Node4 shall be entitled to suspend the service:

- In a life or property threatening emergency
- If required to do so by any governmental or regulatory authority; or
- Where the customer is in breach of this Agreement or terms and condition.

3.6 Termination of service

Upon the termination or cessation of these N4Threat Detect Services the Customer is obligated to remove all N4Threat Detect licences from devices and infrastructure within 1 month of the end of such date.

4. Fees

Charges may comprise any or all of the following Charges including an Installation Charge and a "Monthly Service Charge" as agreed by the Parties.

4.1 Set-up charges

Any applicable set-up charges for the implementation of the support service shall be detailed on the purchase order.

4.2 Monthly service charges

Monthly Service Charges are paid either monthly or annually in advance based on the support provided and any other related service, as identified on the Order Form.

Monthly Service Charges are applied as and when the service is made available.

4.3 Additional professional services

A full range of Professional Services are available to the customer in addition to what is provided as part of the support contract. The Professional Service Charges include but are not limited to:

- Installation and configuration
- Remote services
- Management

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.

All incremental expenses incurred during these Professional Services will be passed directly to the Customer (as per the Node4 Expenses Policy). Provisioning costs such as cabling will be discussed and agreed with the Customer in the purchase order.

Additional tasks undertaken at the request of the customer by Node4 personnel from a Node4 location, will be charged at the hourly rates shown below.

Time support required:	Per hour
Mon – Fri 07.00 – 19.00	£80.00 per hour
All other times	£120.00 per hour

Time is charged by the hour. These rates are for a support / provisioning engineer and are subject to an annual review by Node4. For advanced engineers with MCSE or CCIE status or for on-site services please contact Node4 for pricing.

Contact Node4 relating to pricing for additional tasks requested by the Customer to be undertaken by Node4 personnel on a Customer Site.

5. Customer responsibilities

Customer shall provide Node4 with a Secure VPN connection to the SIEM system located on the Customer premises.

Customer must complete a RFIS within 15 Business Days of the Deployment meeting or Node4 may terminate Customer's order for N4Threat Detect service. If Customer fails to approve the project plan, or fails to provide any necessary information to implement the project plan, and such delay causes any activity on the critical path of the project plan to be delayed by more than 25 Business Days, Node4 may terminate Customer's order for N4Threat Detect service. Upon termination of an order for N4Threat Detect service, Node4 may charge Customer for any expenses incurred by Node4 (including labour fees) up to the date of termination, and shall immediately return to the Customer any amounts paid in respect of Services not provided or to be provided after the effective date of such termination.

6. Service provision

Prior to commencement of N4Threat Detect, Node4 will schedule a Deployment meeting to introduce the N4Threat Detect service delivery team, identify the appropriate contacts for Customer, discuss the scope of the N4Threat Detect service and its business impacts, and obtain a completed Request for Information Schedule (RFIS) from the Customer.

Upon receipt of completed RFIS, Node4 shall create a proposed project plan with key milestones, Phase Checkpoint Reviews and time-scales. N4Threat Detect will only be provisioned after the Customer has approved the project plan. During the implementation of the N4Threat Detect, the Customer may propose changes to the project plan or the N4Threat Detect service. Node4 will assess the Customer's proposal and may require the Customer to submit a new Service Order or Amendment to reflect the approved changes.

6.1 Service features

N4Threat Detect is available at three levels of protection;

- Essential is the entry level service
- Enhanced is the medium level of service
- Elite is the highest level of service

Further details are provided in the table below:

	Essential	Enhanced	Elite
Network Threat Alerts	*YES*	*YES*	*YES*
Host Threat Alerts	*No*	*YES*	*YES*
Custom Threat Alerts	*No*	*No*	*YES*
Vulnerability Scanning	*No*	*YES*	*YES*
Security Advisor	*1 hour pcm*	*3 hours pcm*	*5 hours pcm*
Reports	*5*	*10*	*15*
Web Pen Testing	*No*	*No*	*YES*
Live Dashboard	*YES*	*YES*	*YES*

6.2 Network threat alerting

Node4 will provide Network Threat Alerting. Network Threat Alerting will also cover the Endpoint

devices listed in the deployment scope. Threat alerting policies are, amongst others, based on a behaviour based, multi-factor correlation capability processed through the SEIM that evaluates and correlates reputational and behavioural patterns and characteristics in addition to signature-based detection methods. Node4 correlates and aggregates related events into Security Incidents automatically through its threat detection policies. Node4 has a wide variety of methods to detect Security Incidents. Events may appear harmless when they are detected in isolation; however, when they are combined with information from other events or from information in the Service Context, a more harmful pattern may appear. Events will be compared with Customer's Service Context and output obtained from network vulnerability scans. The Security and Compliance Dashboard provides a range of reporting functions.

6.3 Custom threat alerting

Node4 will implement custom threats which the Customer can define. Examples such as application login failures.

6.4 Notification of threats

The Customer will be notified of L4 and L5 Incident Classification, described below, in accordance with the Customer's notification and escalation details on a 24x7 basis. It is the Customer's responsibility to act on the notifications. Node4 will not be responsible for non-receipt of notification or failure of the Customer to act upon notification. False Positives may trigger L4 and L5 notifications. Node4 will not log on to an asset unless instructed as part of a Post Attack Forensic service.

Incident Classification	Risk Levels	Conditions
System Compromise	L5	Observed indicators of a compromised system.
Exploitation and installation	L4	Observed indicators of successful exploit of a vulnerability or a remote access Trojan or backdoor being installed on the system.
Delivery and Attack	L3	Observed behaviour indicating an attempted delivery of an exploit. This can include detection of malicious email attachments, network-based detection of known attack payloads or analysis-based detection of known attack strategies such as SQL Injection.
Reconnaissance and Probing	L2	Observed behaviour indicating an actor attempting to discover information about your organization. This is broad-based, including everything from port scans to social engineering to open-source intelligence.
Environmental Awareness	L1	Observed behaviour and status about the environment being monitored. This includes information about services running, behaviour of users in the environment, and the configuration of the systems.

6.5 Host threat alerting

Node4 will require HIDS agents to be installed on server Assets the detect Host threats and Internal Vulnerability Scanning. Customer acknowledges that without HIDS agents Node4 will not be able to maintain optimum secure posture and as a result there may be an increased risk of false-positives being generated and Node4 will not be able to assess accurately the impact of Incidents on the Customer's environment

6.6 External vulnerability scanning

Node4 will perform scans on the Customer's Internet facing Assets as part of the service schedule. The scan data will be used to classify and assign risk scores to Incidents Classification and related events. The goal of External Vulnerability Scanning is to identify as many vulnerabilities that are exposed to externally. The scans will be executed at times to cause a little disruption to the Customer's system as possible, but the Customer accepts the inherent risks associated with all types of scanning methodologies. Node4 utilise a third party tool to eliminate the possibility of the scan being launched internally. The scan may trigger alarms and create false positives

6.7 Executive reports

Monthly reports will be prepared. Such reports will contain an overview of security related incidents over the last reporting period. These reports will be sent to the Customer via e-mail.

The report contains an overview of Security Incident handling and provides recommendations for continuous improvement on how to resolve specific security issues. This service includes the following reporting types and summaries:

- Alarms
- Security Events
- Security Operations

6.8 App penetration testing

Authorisation to conduct the Penetration Testing is granted by the customer to appropriate members of Node4's information security team to conduct penetration tests against this organisation's assets. The Application Penetration Testing Scope shall be used to control who may perform these tasks. The Penetration Testing Scope is defined as part of the Service Schedule.

Undertaking a series of penetration tests will help test some of your security arrangements and identify improvements, but it is not a panacea for all ills. For example, a penetration test:

- Covers just the target application, infrastructure or environment that has been selected
- Focuses on the exposures in technical infrastructure, so is not intended to cover all ways in which critical or sensitive information could leak out of your organisation
- Is only a snapshot of a system at a point in time
- Can be limited by legal or commercial considerations, limiting the breadth or depth of a test
- May not uncover all security weaknesses, for example due to a restricted scope or inadequate testing
- Provides results that are often technical nature and need to be interpreted in a business context.
- Vulnerabilities may not be exploited depending on the level of risk to the system

Bearing in mind these testing constraints, penetration testing should not be assumed to find all vulnerabilities of a given system. The law of diminishing returns often applies in that the most obvious vulnerabilities will be discovered first, with further time yielding more and more obscure issues.

6.9 Post attack forensics

In the event of a system compromise the Customer may request additional services from Node4. These services are not included as part of the N4Threat Detect service and will be costed on a per incident basis.

7. Incident management

This section refers to Incidents and management pertaining exclusively to the service portal for the N4Threat Detect service and does not include any Customer systems or Customer infrastructure.

7.1 Incident handling

Incidents are handled as outlined in the Incident Management schedule Document.

7.2 Hours of support

The following table details the different Support Hours relating to the support hours defined on the Order Form (if nothing included on the Order Form Gold support is included for N4Threat Detect services).

Support Hours	
Bronze	Standard business hours support 9am to 5.30pm week days, excluding bank and national holidays
Silver	Support hours between 7am and 7pm weekdays, excluding bank and national holidays
Silver Plus	Priority 1 and 2 - Support hours between 7am and 7pm 7-days a week, including bank and national holidays, excluding Christmas day, Boxing day and new year's day Priority 3,4 and Service Request - Support hours between 7am and 7pm weekdays, excluding bank and national holidays
Gold	Priority 1 and 2 - Support hours 24/7 Priority 3,4 and Service Request - Support hours between 7am and 7pm weekdays, excluding bank and national holidays

7.3 Time to resolve

Node4 aims to respond, update and resolve Incidents in relation to the N4 Threat Detect service within the following times

Priority	P1	P2	P3	P4	Service Request
Faults & Technical Queries Acknowledge-ment*	30 Mins	30 Mins	1 Hour	2 Hours	1 Day
Remedial Engineer Actions Commence	1 Hour	2 Hours	4 Hours	12 Hours	N/A
Time to Resolve Fault	5 Hours	8 Hours	12 Hours	36 Hours	60 Hours

Resolution times in the table above do not apply where there is a Customer Responsible Incident, a Third Party Attributable Incidents or events outside Node4's reasonable control, any incidents including these aspects will be excluded from reporting provided.

All category 1 & 2 faults should be raised via the Service Desk system by a phone call. Should a priority 1 or 2 incident be raised via the portal or e-mail, the Customer is required to follow this up with a corresponding phone call to enable work to commence immediately on the issue.

** Acknowledgement refers to an automated service which generates a response and alerts engineers of a service failure; or where there is dialogue between the client and the engineer.*

**** Service Requests outside of the support contract, or Service Request implemented outside normal business hours these will be dealt with as chargeable projects.*

7.4 Incident duration

All Incidents recorded by the monitoring system will be reconciled against the corresponding Service Ticket raised by the Service Desk. The exact Incident duration will be calculated as the elapsed time between the Service Ticket being opened and the time when Service is restored.

7.5 Maintenance window

Where Node4 plans to perform essential works on the portal, Node4 will perform such works during low traffic periods and will give the Customer at least five (5) days prior notice. In the event of an emergency or Service-affecting fault such notice may be less than 24 hours. Exclusions

Node4 does not provide onsite installation, architectural and policy design services under N4Threat Detect service. N4Threat Detect service also does not include policy and configuration reviews, initial setup or maintenance of configuration on Subordinate Devices or migrations from management stations located on the Customer's premises to management stations hosted the SMC or from third-party owned management stations to management stations either located on the Customer's premises or hosted in the SMC. All of these excluded services, however, can be conducted by Node4 under a separate agreement.

8. Service credits

Node4 will provide the Customer with "Service Credits", as set out below.

8.1 Availability

The Service is "Available" when the N4Threat Detect SIEM system receiving logs is able to deliver alerts.

The following equation will be used to calculate Service Availability. References to minutes are to the number of minutes in the applicable Monthly Review Period:

((Total minutes – Total minutes Unavailable)/Total minutes) x 100

Service Availability during Monthly Review Period (Switch Service)	Service Credits as % of Monthly Service Charge for SEIM services
<99.9%	10%
<99.0%	15%
<98%	25%

8.2 Calculation of service credits

Where a Monthly Review Period incorporates part of a month, any Service Credit will apply to a pro-rated Monthly Charge.

Service Credits will be calculated monthly, aggregated and credited to the Customer on a quarterly basis.

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

The Customer must claim any Service Credit due to a failure to meet the Service levels, in writing, within twenty one (21) Business Days of the date at which the Customer could reasonably be expected to become aware that such Service Credit had accrued. The Customer shall not be entitled to any Service Credits in respect of a claim unless and until Node4 has received notice of the claim in writing in accordance with the above. Should Node4 require additional information from the Customer, the Customer shall provide its reasonable assistance to Node4.

8.3 Exclusions to payment of service credits

Service credits will not be payable by Node4 to the Customer in relation to the Service Availability for Incidents or disruptions to the Service caused by any of the following:

- The Incident, action or negligence of the Customer, its employees, agents or contractors;
- The Customer failing to comply with Node4 Terms and Conditions;
- An Incident in, or any other problem associated with, Customer's equipment or connection;
- Any event described in Force Majeure of Node4 Terms and Conditions;
- A failure by the Customer to give Node4 access to any equipment after being requested to do so by Node4; or
- Maintenance during any Planned Outage

Service credits are not applicable for more than one breach of any targets outlined in this document arising from the same occurrence.

The provision of Service credits shall be the sole and exclusive remedy for the failure to meet targets for the N4 Treat Detect Service. Node4 shall have no additional liability to the Customer.