SCHEDULE DOCUMENT

N4SECURE

PUBLIC

NODE4 LIMITED

28/07/2017

SCHEDULE DOCUMENT

N4SECURE SERVICES

This schedule contains additional terms and conditions and service description applicable to the N4Secure Services and should be viewed with associated Order Form, Node4's General Terms and Conditions and the Acceptable Use Policy.

1. OVERVIEW

N4Secure offers Monitoring and Scanning services for a selection of security devices, applications and systems listed as an Asset. The different service features of N4Secure are described below.

N4Secure 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

All levels are as described in *Table 1 (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 hr per calendar month	3 hrs per calendar month	5 hrs per calendar month
Reports	5	10	15
Web Pen Testing	No	No	YES
Live Dashboard	YES	YES	YES

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

"***Asset"*** means a device, appliance, software application or a system which is monitored by Node4's Managed security services

"Customer Responsible Faults" means in the event that a Service Affecting or Non-Service Affecting Fault is identified as being attributable to customer Provided Equipment, Premises, customer power supplies, or the action of customer, employees or agents of the customer, the fault 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" means 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.

"RFIS" *means the* request for information schedule

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

"Monthly Review Period" means the calendar monthly periods commencing on the 1st of each month during the Term, over which Service performance measurements are calculated, provided that the first Monthly Review Period will commence on Ready for Service Notification;

"Network Management System" means Node4's network integrated fault management system;

"Node4 Network" means the network wholly owned and managed by Node4;

"Non-Service Affecting Fault" means a fault or condition which is not a Service Affecting Fault.

"Penetration Test" or "Pen Testing" *Penetration* testing is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

"Security Dashboard" *means* 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.

"SEIM" *means* 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 Monthly Review Period. The Node4 service shall be deemed available for the purposes of calculating Service Availability if it is not usable due to an event outside our reasonable control, a Customer Responsible Fault, a Third Party Attributable Fault or is due to a Planned Outage.

"SSA" means the Node4 resource assigned to the Customer

"Standard MAC" means a change to one device which can be completed within 30 minutes by a technical support engineer between 7am and 7pm Monday to Friday.

"Technical Support Centre" means Node4's fault management centre, which operates the Node4 Network Management System;

"Threat" means 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" *means* 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" *means* 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 N4Secure Services to the Customer.

3.1 INSTALLATION AND SET-UP

Customer must complete a RFIS within 15 Business Days of the Deployment meeting or Node4 may terminate Customer's order for N4Secure 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 N4Secure service. Upon termination of an order for N4Secure service, Node4 may charge Customer for any expenses incurred by Node4 (including labour fees) up to the date of termination.

3.2 TERMINATION OF SERVICE

Upon the termination or cessation of the service the customer is obligated to remove all N4Secure licences from devices and infrastructure within 1 month of the end of service date.

3.3 THIRD PARTIES

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

The customer shall indemnify and defend Node4 for all costs and expenses related to a third party's claim of loss, damages and liabilities (including legal expenses and the expenses of other professionals) incurred by Node4, resulting directly or indirectly from any claim attributable to or arising out of Node4's use of network scanning technology (each, a "Scanning Claim"), including, without limitation, the use by Node4 of network scanning technology to analyse assets that are not controlled directly by the customer, including, without limitation, servers hosted by third parties. This obligation of the customer in connection with a Scanning Claim shall not apply if Node4's gross negligence or wilful misconduct gave rise to such Scanning Claim.

3.4 WARRANTY

No warranty is provided by Node4 that N4Secure Service 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.

4. FEES

Fees will commence when Ready For Service Notification is provided by Node4, this is following activation of the supporting network connection. Fees may comprise any or all of the following aspects.

4.1 INSTALLATION AND SET-UP FEES

Any applicable installation or set-up Fees as detailed on the Order Form.

4.2 SERVICE FEES

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

4.3 PROFESSIONAL SERVICE FEES

Additional tasks undertaken by Node4 at the request of the customer or activities undertaken by the customer which require the remote support of Node4 personnel will be charged at the hourly rates shown below.

Time support required:	Per hour	Per day
Mon – Fri business hours	£60.00 per hour	£480.00
Mon – Fri other times	£100.00 per hour	POA
Saturday	£100.00 per hour	POA
Sunday	£100.00 per hour	POA

Time is charged by the hour. These rates are for a trained technician 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.

5. CUSTOMER RESPONSIBILITIES

5.1 THREATS

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

5.2 ASSUMPTION OF RISK

N4Secure 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 or associated with such component of N4Secure. 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.

6. PROVISION OF SERVICES

6.1 SERVICE INSTALLATION AND PROVISIONING

Prior to commencement of N4Secure, Node4 will schedule a Deployment meeting to introduce the N4Secure service delivery team, identify the appropriate contacts for Customer, discuss the scope of the N4Secure 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. N4Secure will only be provisioned after the customer has approved the project plan. During the implementation of the N4Secure, the customer may propose changes to the project plan or the N4Secure service. Node4 will assess the customer's proposal and may require the customer to submit a new Order Form or amendment to reflect the approved changes.

6.2 INCIDENT CLASSIFICATION

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.

6.3 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 Dashboard provides a range of reporting functions.

6.4 NOTIFICATION OF THREATS

The Customer will be notified of L4 and L5 incident classification, in accordance with the Customer's notification and escalation details on a 24x7 basis. False Positives may trigger L4 and L5 notifications

Customer will be notified of L1, L2 and L3 incident Classification in accordance with the Customer's notification and escalation details during Business Hours.

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 CUSTOM THREAT ALERTING

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

6.7 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 incident 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

6.8 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 application 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 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.

The customer is assigned a SSA who will host a quarterly service review meeting. The SSA is assigned to multiple N4Secure customer accounts and is not dedicated to the customer. The SSA assists with the following items:

- Training on Security Dashboard
- Manages the customer communication and Security Advisories
- Provides assistance in scheduling a quarterly external network scan
- Manages service issues and Service Credit requests
- Security Incident handling summary of Incidents and Events.
- Asset review
- Monthly strategic review on Incidents to provide broader trends on Incidents.
- Security Digest review: include a summary with highlights and recaps of items of interest

The SSA is the Customer escalation point for issues regarding the amount of incident tickets allocated to a service request, inquiries about the scope of the services, and quality of the N4Secure service and the SLA.

The SSA will make recommendations to improve the customer's security and risk posture, analysing the Asset capacity lifecycle, providing the customer specific and industry specific risk advisories, assisting the customer with critical asset identification and internal/external vulnerability scanning and scan data uploads to improve Threat Analysis and Security Incident Handling, and training the Customer on the use and features of the Security Dashboard

6.10 EXECUTIVE REPORTS

Weekly and/or monthly reports will be prepared. Such reports will contain an overview of security related incidents over the last reporting period. Customers may request to review these reports with the SSA in the quarterly service review. These reports will be made available through the Dashboard and will be sent to the customer via e-mail.

A monthly reporting summary review. 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

6.11 LIVE DASHBOARD

The Live Dashboard is configurable and extensible dashboard for creating custom views of threat, compliance, and operational data.

Where Node4 plans to perform essential works on the Live Dashboard, Node4 will endeavour to perform such works during low traffic periods and will endeavour to 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.

6.12 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 N4Secure service and will be costed on a per incident basis.

Node4 will not log on to an asset unless instructed as part of a Post Attack Forensic service.

6.13 PROFESSIONAL SERVICES

A full range of Professional Services are available to the customer including but are not limited to:

- Installation and configuration
- Ad-hoc support

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. Provisioning costs such as cabling will be discussed and agreed with the customer in the Order Form.

6.14 CHANGES

Moves, Adds & Changes (MAC) are not provided as part of the standard service. If "Full Management" is taken and included on the Order Form an unlimited number of Standard MACs are included (fair use policy applies), Node4 will endeavour to complete Standard MACs within 3 Business Days.

Change requests conducted outside of the support contract, or change request implemented outside

normal business hours will be dealt with as chargeable projects and subject to the Support and Professional Services Fess in 4.4.

7. SERVICE CREDITS

Service credits are not available for N4Secure Services.

8. EXCLUSIONS

N4Secure Service does not provide

- onsite installation,
- architectural and policy design.
- policy and configuration reviews,
- initial setup or maintenance of configuration on Subordinate Devices
- migrations from management stations located on the customer's premises to management stations hosted the SMC
- Migrations 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, can be provided by Node4 under a separate agreement.