Service Attachment (SA) for Network Detection and Response Services

SA-NDR V1.2 REVISED 8/31/2021

This Service Attachment for Network Detection and Response Services ("SA-NDR") is between Centre Technologies, Inc. a Texas corporation (sometimes referred to as "we," "us," "our," OR "Provider"), and the Customer found on the applicable Quote (sometimes referred to as "you," "your," OR "Customer"). Collectively, these two entities are "the Parties". The MSA, together with the Quote and relevant Service Attachments, forms the Agreement between the Parties.

The Parties further agree as follows:

1. SCOPE – SA-NDR SERVICES

Service Description

In connection with the Services listed in detail in your Quote for Network Detection and Response ("NDR") Services, Customers are entitled to the use of all services to be performed within the scope of this Service Attachment.

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

a. Remote Telephone Support shall be available 24 x 7 x 365.

b. Remote Email Support shall be available 24 x 7 x 365.

Centre will undertake problem management as soon as we become aware of an incident. All activity related to a given incident will be formally documented by Centre staff within Centre's Service/Ticket Management system. This will include all updates during the troubleshooting process up to final resolution. If a root cause can be determined it will be documented in the service ticket as well.

NDR is a managed service that provides real-time monitoring of potential threats to Customer systems, with the following standard services capabilities and modules (the "NDR Services"):

Intrusion Detection and Prevention. This capability facilitates the identification and mitigation of specific dangerous TCP traffic.

a. **Full Packet Capture and Playback.** This capability allows for forensic analysis of suspicious activity after the fact.

b. **ExecutionerTM.** This module that prevents "drive-by downloads" of malicious executables through domain white-listing technology.

c. **Asset Manager Protect ("AMP").** This module protects Customer's assets against threats known to the SOC using a global IP blacklist updated in near real-time by the SOC. The blacklist is updated each time a new threat or vector of infection is identified on any network monitored by the SOC.

Sensors. Upon the Parties executing a Quote for the NDR Services, Centre will provide at least one (1) physical and/or virtual security appliance (a "Sensor") for each location that is to receive the NDR Services as detailed on the applicable Quote. Sensors will be sized according to traffic volumes and storage requirements and identified on the applicable Quote. Monitoring of Small Office Home Office ("SOHO") Sensors will be restricted to internal network traffic only.

Sensor(s) will be deployed with one or more SPAN(s) to analyze network traffic flows of the following types:

a. External Network (Internet) to Internal Network.

b. Internal Network to External Network (Internet).

c. Other data segments depending on the volume of data to be monitored and capacity of the implemented Sensor (VPN, DMZ, VoIP, Market Data, etc.).

d. For SOHO Sensor Only: Home network user traffic should be segregated from business user traffic. Non-business users should not have access to the Centre SOHO solution.

e. For SOHO Sensor Only: Sensor deployment on the local network needs to support Ethernet (IEEE 802.3x) standards and throughputs.

f. WAN/Internet (site-site VPN) needs to support typical consumer broadband services available from major network operations (e.g., Cable, DSL, FTTx, WiMax, etc.).

The Sensor(s) will analyze the network traffic to watch for:

a. Reconnaissance attempts through scanning of Customer networks by unauthorized individuals.

b. Specific attack attempts by unauthorized individuals using hacking tools.

c. Traffic generated by infected systems (Customer computers compromised by specific viruses or worms).

d. Misconfigured internal systems (Customer computers generating inappropriate traffic).

e. Security Policy/Acceptable Use Violations (Employees using the network for inappropriate uses).

Centre will configure and remotely manage the Sensor and its embedded software as part of the NDR Services. Customer may only access the configuration of such Sensor with Centre's prior written authorization. Centre shall only access the configuration of other network devices connected to the Sensor with Customer's authorization and shall do so through an encrypted and secure means.

Service Level Objectives

Scope

Each Sensor has ongoing 24x7x365 monitoring with an objective twenty (20) minutes or less initial response time for human threat assessment and Customer alert. The following describes the alerting policy and escalation matrix followed by Centre:

Any dispatch within, or outside of, the Standard Coverage Area requires mutual approval between Centre and Customer and is billable to the Customer unless NDR Services are sold with Secure Managed Services.

Customer Point of Contact ("POC")

Customer shall assign a technical Point of Contact ("POC"), which shall be the primary interface with Centre and/or partner resources responsible for service delivery.

Response Time
Response time can be impacted by the distance from the affected site to the nearest available field technician with the proper skills to resolve the problem.

The Response Time Goals set forth in this document for Global On-Site Dispatch are aspirational in nature and Centre does not promise or guarantee service within such time frames. Under no circumstances shall the aforementioned goals form the basis for any claim or breach of the Agreement.

Centre and Customer establish the following response time goals:

Severity Priority	Alert Category	Notification & Escalation
Low (P4)	Minor activity is recorded but not alerted.	None
Medium (P3)	Acceptable Use Policy violations. Includes SSH/RDP/FTP connections, P2P activity, Proxy Usage, TeamViewer, LogMein, Skype or Teams usage.	Automated email notification within 120 minutes of reception of the policy violation event on the Centre platform.
High (P2)	Threat activity that does not require immediate attention. If left unchecked, these events may lead to more severe security incidents.	Email notification within 40 minutes of determination of the security event by the SOC.
Critical (P1)	Threat activity that requires immediate attention. These items may indicate that a severe security incident is underway or is imminent. This category also includes issues that indicate a disruption in the Provider's service.	Email notification within 20 minutes of determination of the security event by the SOC. Phone call escalation from the SOC if a customer acknowledgement is not received for the initial email notification.

Customer Responsibilities. Customer is responsible for:

a. any and all data and systems which Customer grants access to for receipt of the NDR Services;

b. obtaining all necessary licenses, permissions and consents to enable Centre to access the Customer's network and servers in order to provide the NDR Services;

c. designating a Project Coordinator to work directly with and serve as the primary Customer contact with Centre for the duration of Customer's receipt of the NDR Services;

d. providing Centre a complete copy of its security (including privacy) policies, as available. Customer is solely responsible for creating, maintaining and enforcing its security policies to protect the security of Customer Data and Systems;

e. its choice of equipment, systems, software and online content;

f. providing the necessary resources, information, documentation and access to personnel, equipment and systems, as reasonably required by Centre, to allow Centre to perform the NDR Services;

g. providing a current network topology diagram to ensure capturing the correct traffic and correct configuration of the NDR Services;

h. notifying Centre in advance of any network changes that will affect Customer's network topology and /configuration so that all relevant traffic is being captured within the Sensor; and

i. communicating all network infrastructure changes to Centre. Effective monitoring requires that ability to SPAN an interface on any applicable segment.

In event Customer fails to perform its obligations in the time and manner specified or contemplated above, or should any assumption outlined herein with respect to the NDR Services fail to be valid or accurate, then Centre will not be responsible for any related delay or damages. In the event that Customer fails to notify Centre of network changes as contemplated above, then Centre shall be released from any and all obligations to monitor the Customer's network until Customer has notified Centre of such change.

Maintenance Windows

Hardware firmware upgrades are performed only where necessary to resolve a specific issue or to address a critical vulnerability.

Service Provider reserves the right to deploy out of band emergency patches outside of established maintenance windows, with no advance notice, if deemed necessary and appropriate. If out of band patches are applied Centre will notify Customer as soon as possible.

Safety and Security Recommendations

Provider may make recommendations regarding safety and security related to Customer's network and practices. If Customer fails to adopt or implement the recommended protocols, Customer is responsible for any and all damages related to regulatory, security, privacy, or data protection, including but not limited to fines, data breach notification, malware or ransomware costs, restoration, forensic investigation, restoring backups, or any other costs or damages related to Customer's refusal to implement the recommended protocols.

2. NETWORK CHANGE COORDINATION

Significant Changes to Customer's Network

You will notify us via email of all significant proposed network changes and will provide us with at least thirty (30) days advance notice to provide opportunity to comment and follow-up regarding proposed changes.

Research Regarding Network Changes

Evaluation of network change requests sometimes will require significant research, design, and testing by Provider. These types of requests are not covered by this Service Attachment and will be billed at our then-current rates for time and materials.

3. SUITABILITY OF EXISTING ENVIRONMENT

Minimum Standards Required for Services

Customer represents, warrants and agrees that its existing environment meets the following requirements or will obtain upgrades to its existing environment to meet the following requirements:

Customer equipment must be maintained under manufacturer's warranty or maintenance contract or is in proper working order. Provider is not responsible for Customer equipment that is not maintained under manufacturer's warranty or maintenance contract or that is otherwise out of order. All fees, warranties, and liabilities against Provider assume equipment is under manufactures warranty or maintenance contracts or is in working order.

Provider in its reasonable opinion and supported by manufacturer information, may designate certain equipment or software as obsolete, defective or end of life (EOL) and therefore exclude it from coverage and performance metrics under this Agreement. This includes, but is not limited to, specific operating system builds/versions that are end of life and no longer supported by the manufacturer as shown below:

1. All servers with Operating Systems must be running current versions and have all of the latest Critical Updates installed and be patched within 30 days of the last patch.

2. All desktop PC's and notebooks/laptops with Operating Systems must be running current versions of software, and have all of the latest Critical Updates installed and be patched within 30 days of the last patch.
3. All server and desktop software must be genuine, licensed and vendor supported.
4. The environment must have a currently licensed, vendor-supported hardware firewall between the internal network and the internet.
5. There must be an outside IP address assigned to a network device, allowing VPN access.

Costs required to bring Customer's environment up to these Minimum Standards are not included in this Agreement and shall be incurred and paid by Customer.

4. EXCLUSIONS

We are not responsible for failures to provide Services that are caused by the existence of any of the following conditions or otherwise that occur during any period of time in which any of the following conditions exist:

Customer Actions or Criminal Activity

Problems resulting from your actions or inactions that were contrary to our reasonable recommendations are covered in the MSA in Section 12.

Customer Responsibilities

Problems resulting from your failure to fulfill any responsibilities or obligations under our agreements.

Customer Resolution
Provider's ability to resolve problems due to Customer re-prioritizing Provider's recommendations.

Factors Beyond Provider's Control
Delays or downtime due to any factor outside of Provider's reasonable control.

Internet Connectivity Loss or Loss of Power
Loss of Internet connectivity or power at your location for any reason.

5. TERM, RENEWAL, AND TERMINATION

This Service Attachment is effective on the Service Start Date identified in the Quote. Unless properly terminated by either party, this Service Attachment will remain in effect through the end of the term specified on the Quote (the "Initial Term"). The definitions of Term, Renewal, and Termination are defined in the MSA and are hereby incorporated in this SA-NDR.

The remainder of this page is intentionally left blank.