Business Services

PUBLICATION 1 SERVICE DESCRIPTION FOR NETWORK DETECTION & RESPONSE

1.1 Definitions

As used in this Service Description, the following capitalized terms will have the meanings given to such terms.

"**Alarm**" means a state event sent by a component on the platform.

"**Alert Management Level**" means the activities done by Orange when managing a Security Incident.

"**Business Days**" means normal working days 8.00 AM-5.00 PM, Monday to Friday.

"**Incident**" means a Security Incident or a Platform Incident.

"**Level of Service**" means the different level of service in response to an Incident provided by Orange on top of the Platform.

"**NDR**" means 'Network Detection and Response'.

"**NTA**" means 'Network Traffic Analysis'.

"**Platform Incident**" means an alarm leading to a disruption (with or without an impact) of the Service. Platform Incident has a predefined management process.

"**Platform**" means the solution hardware or software provided by Orange's third party vendor (Vectra) which is the base of the Service.

"**Security Incident**" means a security detection identified by the Platform triggering analysis, reporting, and response by Orange.

"**Service Request Form**" or "**SRF**" means the form that details Customer's specific Service requirements.

"**Service**" means the managed threat detection with option network detection and response, as described in this Service Description.

"**Signature-less Detection**" means a detection engine that detects suspicious behavior ((low – medium – high – critical) based on artificial intelligence technology.

"**Vectra Devices**" means Vectra's physical brain and/or sensor devices.

1.2 Service Overview

This Service is a fully managed service that primarily supervises, analyzes, and detects security anomalies on Customer's network (and, optionally corrects them).

The Service is operated from a NTA platform built on Vectra technology. It monitors the activity on the Customer's network by examining all traffic flows and analyzing it to match, detect, and identify any suspicious behavior within the traffic flows. Detection of suspicious behavior is based on a signature-less artificial intelligence engine. Such engine increases the probability of (a) detection as the engine is inspecting and collecting traffic in east-west communication and (b) detecting zero day attacks as the platform is collecting and building attack behavior using AI and machine learning.

The Service is fully installed, supervised, and maintained by Orange and consists of the three co-dependent layers:

- Base layer: Platform
- Second layer: Level of Service
- Third layer: Alert Management Level

1.3 Platform

The Platform is the Vectra 'Detect solution' which is a NTA used to analyze Customer's traffic and match, detect and identify suspicious behaviors.

1.3.1 Main components

1.3.1.1 Sensors

This is the component where the distill functions are made which are extracting metadata from all network traffic collected. Sensors are distributed over the whole Customer's network in carefully studied design by Orange, allowing it to collect all types of traffic profiles needed for efficient operation of the Platform. The below traffic profiles are recommended for optimum performance:

- User to internet traffic.
- User to datacenter traffic.
- User to user traffic.
- User to authentication servers traffic.
- DHCP traffic.

Sensors can be hardware or virtual. During the design phase, Orange will recommend the best option for the Customer.

1.3.1.2 Brain

The brain is a physical device that applies data science and machine learning algorithms to distilled metadata.

Customer can order an extra spare brain (optional): which will be in cold standby backup mode for the main brain. It will receive backup from the main brain and can be manually enabled to replace the main brain in case of any failure.

1.3.2 Platform Methodology

The Platform allows Customer to have complete visibility on network threats through Signature-less Detection engine that helps identify attacks and malicious activities based on learning and identifying attacker behaviors.

The attacker models and behaviors in the Platform are built based on the below approaches and features:

- For command and control communications, the Platform looks at how the control connection is being used. It doesn't matter what the specific tool used by attacker is or whether the traffic is encrypted or not.
- Learning about the network which the attacker is targeting by network scans and sweeps, as well as more advanced techniques like active directory (AD) recon to learn about admin groups and credential privileges.
- Moving laterally whether through stolen accounts, exploits, or by triggering backdoors previously installed on a compromised system. For every host in the network, the Platform maps which credentials the host uses to access which services and which other hosts it administers via which protocols. The Platform also identifies how the host uses remote procedure code (RPC) for remote code execution and how it uses remote desktop protocol (RDP). For example when a stolen credential is used to try to move laterally, this behavior will trigger one or more of these attacker models which is in the Platform.
- The Platform detects data exfiltration. This happens by looking at how data is gathered, staged, and moved out of the Customer's network. As well as methods like tunneling. The Platform does not function like DLP (which only finds accidental leakage); it works independent of (a) encryption, (b) chunking or other obfuscation techniques, and (c) the protocol used.

1.4 Level of Service

This represents the level of effort to be delivered by Orange for the Incidents. This component varies between the two (2) following levels of service:

1.4.1 Core Level of Service

- Brain and Sensor: hardware, VM management, maintenance.
- Operating System (OS) maintenance.
- Provision 24x7 of hardware, OS monitoring.
- Change management: pre-defined number of change requests (simple and/or complex).
- Core service includes the below activities and features:
  - Triaging based on Customer request (change requests).
  - Customer will have read-only access to the Platform to monitor detections.
  - Automated emails are sent from the Platform for critical and high detections.
  - On-Demand analysis of alerts and detections are done based on Customer's request as detailed in Section 1.5.1.
  - Reports of on-demand activity are sent by email.

Additional charges may be applied if the limit of the above points is exceeded.

1.4.2 Extended Level of Service

- Brain and Sensor: hardware, VM management, maintenance.
- Operating System (OS) maintenance.
- Provision 24x7 of hardware, OS monitoring.
- Change management: pre-defined number of change requests (simple and/or complex).
- Extended service includes the below activities and features:
  - Triaging based on Customer's request (change requests).
  - Customer will have read only access to the Platform to monitor detections.
  - On-Demand analysis of alerts and detections are done based on Customer's request as detailed in Section 1.5.1.
  - Real time analysis based on Standard or Premium levels as detailed at Section 1.5.2 and Section 1.5.3.
  - Alerts and reports are sent by email and on the Orange portal.
  - Automated emails are sent from the Platform for critical and high detections.
  - Proactively check false/true positive by analyzing detections then propose or recommend needed changes and triage rules.
  - Only when Customer has dedicated SIEM platform-as-a-service: correlation with other security tools on SIEM platform.
  - Share monthly reports with Customer.
  - Monthly Customer review call with Orange security manager or SOC point of contact.

1.5 Alert Management Level

Orange provides the level of expertise and organizational resources when a security alert of suspicious behavior is notified by the Platform. There are different alert management levels for responding to alerts:

- On-Demand;
- Standard; or
- Premium.

1.5.1 On-Demand

- Analysis based on Customer request only.
- Reports generated from the Platform.

1.5.2 Standard

The Standard alert management level can be chosen only with the extended service Level:

- On-Demand alert management level.
- Real time analysis of host alerts (high and critical).
- Real time analysis of attack campaigns.
- Service is on 8x5 or 24x7 model.
- Standard reporting.

1.5.3 Premium

The Premium alert management level can be chosen only with extended service level:

- On-Demand alert management level.
- Real time analysis of host alerts (high and critical).
- Real time analysis of attack campaigns.
- Real time analysis of all alerts on hosts marked as key assets.
- Service is on 8x5 or 24x7 model.
- Premium reporting.

1.6 Service Features

1.6.1 Platform's Software Maintenance

Under Orange's responsibility, the Platform's software will be maintained and updated automatically without Service disruption through the cloud connectivity between the brain appliance and the third-party vendor cloud. This process doesn't violate or share any Customer information or detections to the third-party vendor.

Orange ensures that the software version on the Platform is fully supported by the third-party vendor.

1.6.2 Hardware Maintenance

Orange is responsible for maintaining the third-party vendor hardware provided with the Service.

Delivery of new hardware is as follows:

- Next Business Day delivery available in all 50 states of the USA.
- 3 Business Day delivery available in the remainder of the Americas (subject to international shipping availability).
- 3 Business Day delivery available in Europe, including the United Kingdom and Ireland.
- Shipping to other countries available on-demand.

Maintenance also covers hardware replacement service in case of failure.

For hardware hosted at Customer's premises, maintenance is subject to Orange's local presence. The Customer must provide Orange up-to-date contacts of employees who can give access to Customer's premises. Orange will perform validation tests with the Customer's help on all replaced hardware. Upon positive validation tests, Orange leaves with the defective hardware.

If Customer cannot accept the delivery delays above: we recommend that a spare brain device is included in the order.

1.6.3 Technical Integration

Orange will work with Customer to determine the level of effort needed for Orange to integrate and setup the Service into the Customer's IT infrastructure. Depending on the level of effort and the scope of the Service implementation project, Orange may either provide Customer with a project plan that outlines the steps and activities that the Parties will undertake to implement the Service, or send to Customer's technical contact or administrator an e-mail to explain the necessary technical changes that Customer needs to make to its IT infrastructure in order to implement and use the Service.

Customer will supply Orange with all technical data and all other information that Orange may reasonably request to allow Orange to supply the Service.

1.6.4 Service Developments

Orange may modify and update the features and functionality of the Service. These updates may include any subsequent release or version of the Service containing functional enhancements, extensions, error corrections, or fixes.

Updates will not automatically include new features which may or may not require additional cost.

Any third party vendor's available update is subject to Orange's sole decision to implement it on the Service.

1.6.5 Optional Services

As optional features of the Service, Customer may order the below list of optional services. These optional features may be subject to additional charges and are not provided as stand-alone offers.

1.6.5.1 Account Lock Down

Orange can integrate Customer's active directory with the Platform to automatically or manually lock down a host identified in a detection as a response action.

1.6.5.2 Essential Threat Hunting

Threat hunting activity can be done on Platform.

- **Option 1:** 8 hours per month.
- **Option 2:** 16 hours per month.

1.6.6 Overview of the Composition of Service & Available Options

It is mandatory that Customer chooses one level of service and one alert management level.

Reference	Features	Details
0	Platform	Build by Orange. Run by Orange.
1	Level of Service	Choose one or more from the below list: ▪ Core service. ▪ Extended service.
2	Alert management level	Choose one from the below list: ▪ On-Demand. ▪ Standard (only with Extended service level). ▪ Premium (only with Extended service level).
3	Spare Brain (Optional)	As illustrated in Section 1.3.1.2.
4	Threat hunting (Optional)	As illustrated in Section 1.6.5.2.
5	Account lock down (Optional)	As illustrated in Section 1.6.5.1.

1.7 Customer Responsibilities

1.7.1 Customer Requirements

Prior to commencement of the ordered Service, the Parties will complete the applicable SRF(s). Customer shall provide all relevant technical specifications and documentation regarding its existing network (IT infrastructure). Orange will reasonably assist Customer in completion of the SRF(s). Customer shall ensure that all information contained in the completed SRF(s) is accurate.

Customer, through its network engineer, is responsible for sending a copy of the network traffic to the Platform to be analyzed. This copy is either done through network TAP or through mirror ports on Customer's infrastructure.

1.7.2 Customer Security Contacts

- Customer will identify and designate two (2) primary security contacts:
  - One (1) security architect/analyst or someone who can provide clarifying information to Orange about any network component like a server or subnet in order to better decide about the Security Incident if it is true or false detection. This individual will receive periodic reports from Orange.
  - One (1) network engineer.
- Customer will ensure that primary contacts are available and can be contacted by Orange 24 hours a day, 7 days a week.
- Primary contacts can open tickets in relation to (a) the malfunctioning of Service, (b) for analysis / changes / hardware issues.
- Orange will respond only to Incidents and Service requests issued by a primary contact by telephone or via the Orange portal.
- Customer will notify Orange of any changes to the primary security contact in writing, on Customer's letterhead, and such notification must be signed by a senior manager in the Customer's organization.

The primary security contacts identified in the SRF will ensure that:

- All security contact information is maintained and current.
- Orange is notified before and after any planned outages or configuration changes to Customer's network or network services.
- All planned outages or configuration changes to customer network or network devices are scheduled at least 5 Business Days in advance.

1.7.3 Acceptance Testing

Upon completion of the installation of the Service, Orange will commence acceptance testing, which will confirm that all aspects of the Service are operational in accordance with the terms set forth in this Service Description and the parameters set forth in the SRF.

Upon completion of the acceptance testing, Orange will provide to Customer a "Service Acceptance Form" for Customer's execution, which form will identify the acceptance tests performed by Orange.

Customer will be deemed to have accepted the Service on the date on which Orange issues the Service Acceptance Form, unless Customer notifies Orange in writing of a material fault in the Service within 5 Business Days of receipt of the Service Acceptance Form. In such event, the above acceptance process will be repeated.

1.8 Support

1.8.1 Change Management

The change management supplied by Orange enables the Customer to submit and monitor change requests on Platform software.

Changes made in project mode are monitored regularly during meetings between the Customer and Orange.

Changes are two main types:

- Changes following Orange's analyst recommendation for a Security Incident.
- Changes requested by Customer. The Customer changes are limited to a pre-defined number as specified in the order. Those changes may be in relation to the Service and/or related to a Security Incident. The change request is either simple or complex. In the event Customer requires additional changes, Orange will charge the Customer for changes (simple or complex) exceeding the predefined change count agreed in the order.

1.8.2 Incident Management

The Incident management supplied by Orange enables the Customer to open, follow up, and close Incidents.

1.8.3 Service Desk

Orange provides a service desk for the Customer to support the Service. The service desk is provided in French or English and is used to:

- Register proactive ticket openings (supervision of the Service);
- Register reactive ticket openings (following a call from the Customer);
- Qualify each ticket in terms of severity (which determines the processing speed);
- Follow up each ticket.

1.8.4 Customer Service Manager (CSM)

For a large project, a Customer Service Manager (CSM) is named. Except when a team or person is dedicated to a specific customer for example, the CSM is shared with other customers. However, Orange restricts the activity of its CSMs to a limited number of customers in order to ensure maximum knowledge of the Customer.

When a CSM is named, the CSM is operationally accountable for the execution of the Services. The CSM is globally responsible for the interface between the customers and Orange. The CSM may also provide consulting mission to the customer. The CSM:

- Coordinates the operating of Customer solution.
- Drives potential escalations.
- Ensures evolutions and changes follow up.
- Diffuses information on preventive maintenance.
- Configures and comments online reporting in the Customer Care Service.
- Provides Customer, a monthly dashboard commented including values for indicators of availability and capacity of the solution.
- Organizes meetings with Customer after each delivery dashboard to make a full point on the solution. A meeting report is always written by the Customer Service Manager and distributed to Customer.
- Ensures follow up and analysis of the quality of service in accordance with commitments under the Contract, of any problems and initiates corrective actions necessary and the implementation of appropriate preventive measures to improve the performance of the solution. These actions are recorded and followed in personalized action plan.

1.8.5 Security Manager (SM)

The Security Manager (SM) is part of the Orange's team. The SM is in charge to make the follow-up of security activity (security policy, reporting, incidents follow up). Consequently, the SM is the escalation point of contact for any security purpose.

The SM is present for all the duration of the project, from the start of the build and for the entire duration of the run.

Orange restricts the activity of its SMs to a limited number of customers in order to ensure maximum knowledge of the Customer and thereby offer an analysis and consulting service that matches the Customer context as much as possible.

1.9 Service Level Objective

1.9.1 Service Time

The matrix below shows service times to build and run the Service for the levels of service.

Type	Calendar Days	Service Time
Core service - On-Demand	Working Days	8 AM- 5 PM CET and CEST
Extended service - Standard 8x5	Working Days	8 AM- 5 PM CET and CEST
Extended service - Standard 24x7	Daily	24x7
Extended service - Premium 8x5	Working Days	8 AM- 5 PM CET and CEST
Extended service - Premium 27x7	Daily	24x7

1.9.2 Notification Times & Methods

Notification times are calculated from the time the Incident is classified until notification to the Customer is started. Complete Incident documentation may take longer to compile, depending on how the Incident develops and its nature.

Priority	1 – Critical	2 – High	3 – Medium	4 - Low
Notification time (within Service time)	30 min	2 hours	8 hours	24 hours
Telephone contact	Yes			
Email Incident Notification	Yes	Yes	Yes	
Portal information	Yes	Yes	Yes	Yes
Incident documentation	Yes	Yes	Yes	Yes
Advice and support by telephone	Yes	Yes	Yes	Yes
Recommended action	Yes	Yes		

1.9.3 Report Interval

Customer will receive reports within following schedule:

Type	Interval	Report Day
Monthly Security Report	Monthly	10th working day following month

1.9.4 Conditions & Exclusions

The Service Level Objectives are subject to the following conditions and exclusions:

- The Service Level Objectives apply only to the Service infrastructure and do not apply to or include the Internet, the local browser, or User's link to the Internet.
- The Service Level Objectives will apply from the first full month following the Date of Acceptance of the Service at the relevant Location, unless specified otherwise.
- Unless otherwise specified, the measurement period for all Service Level Objectives commences on the first day of the month and ends on the last day of the month.
- The Service Level Objectives are targets only, and there are no remedies, financial or otherwise, associated with non-achievement of any Service Level Objective for the Active Prevention Service.
- The Service Level Objective for Hardware Maintenance is subject to the specific country service availability listing (as provided by Orange upon Customer's request and as may be amended from time to time), and on-site field engineer and Customer contact availability, which will be defined on a case-by-case basis.

1.10 Order

1.10.1 Minimum Order, Pricing & Billing

The order for the Service shall be (a) for a minimum 12-month term (the 'Minimum Term') and (b) a Platform sized to manage at least 500 IP addresses.

One-time charges apply as well as monthly recurring charges and both are defined subject to:

- Total number of ordered hosts (any machine with IP address).
- The selected level of service and alert management level.

Additional Charges shall apply if optional features are ordered by Customer.

1.10.2 Early Service Termination

Notwithstanding anything to the contrary set forth in the Agreement, if Customer terminates the Service Term for convenience before the end of the Service Term, then it must give Orange at least 90 days' written notice using the Orange-prescribed Order termination form and pay Orange the following early termination Charges:

- If the Service Term (as indicated on the Order) is 12 months, then Customer will pay Orange:
  - All unpaid Charges for the Service that Orange provided up to the actual disconnection of the Service.
  - All Charges associated with the unused portion of the Service Term.
- If the Service Term (as indicated on the Order) is more than 12 months, Customer terminates the Service Term before the end of the Service Term, then Customer will pay to Orange.
  - All unpaid Charges for the Service that Orange provided up to the actual disconnection of the Service.
  - All Charges associated with the unused portion of the first 12-month period of the Service Term.
  - 50% of all Charges associated with the remaining portion of the Service Term.
- All charges and fees that Orange may be liable to pay to any third party.

1.10.3 Customer's Order Change

- **Level of service upgrade:** changing Customer's monthly running price following to the newly selected level of service:
  - *Upgrade can be done with one (1) month notice or as agreed between Parties.
  - **Downgrade can be done with three (3) months' notice or as agreed between Parties.
- **Level of service downgrade:** changing Customer's monthly running price following to the newly selected level of service:
  - *Upgrade can be done with one (1) month notice or as agreed between Parties.
  - **Downgrade can be done with three (3) months' notice or as agreed between Parties.
- **Increase the number of IP addresses (hosts):** this will include addition one-time price to increase license with third party vendor and will include increase in the monthly running price following the assumption that more IP addresses will increase the number of detection and will result in an increase in the level of effort.
- **Decrease the number of IP addresses (hosts):**
  - For an order with a Minimum Term of 12 months: this request cannot be done and not applicable.
  - For an Order with a Minimum Term of 12 months and more: this request can be done from the beginning of second year from the order date. It will include a reduction in the monthly running price as of this second year. It is understood such request shall not entitle Customer to any reduction of the one-time price paid by the Customer at the beginning of the Service and Orange shall not refund the one time price. Any and all charges and fees Orange may be liable to pay to any third party vendor for this reduction in license shall be paid by the Customer.

END OF SERVICE DESCRIPTION FOR NETWORK DETECTION & RESPONSE