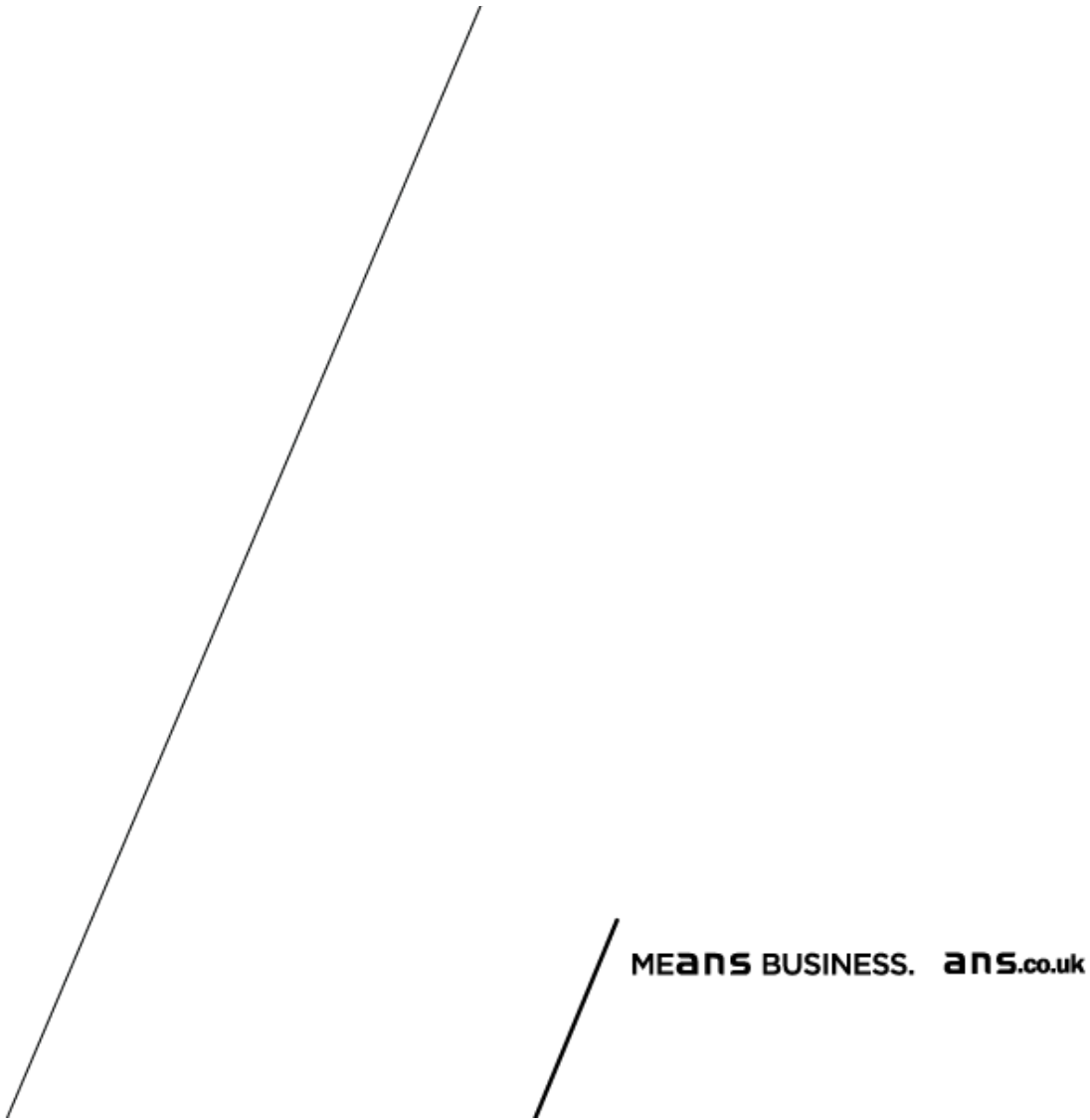
Service Definition

Threat Management | As A Service



MEans BUSINESS. ans.co.uk

1. Operational Services

1.1 Service Description

Normal Business Hours = 9:00 -17:30, Monday to Friday
(excluding bank holidays)
Working Day – 8.5 Normal Business Hours
24x7 = 24 hours a day, 7 days a week

1.1.1 ANS Service

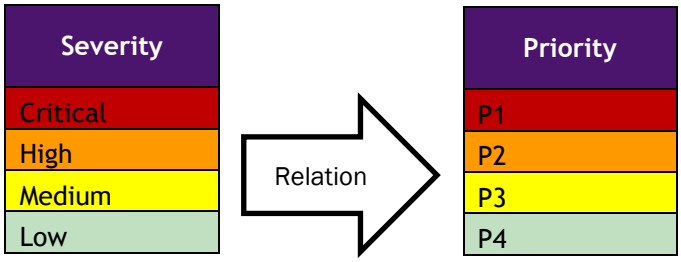
Service	Service Description	Service Hours
Incident Response	Provide data, interpretation, and remediation advice for Customer Incident response for P2, P3, P4 Security Incidents	Normal Business Hours
Incident Response	Provide data, interpretation, and remediation advice for Customer Incident response for P1 Security Incidents	24 x 7
Incident Remediation Advice	Provide advice on how to contain and remediate a P2, P3 or P4 Security Incident	Normal Business Hours
Incident Remediation Advice	Provide advice on how to contain and remediate a P1 Security Incident	24 x 7
Security Intelligence	Identify high priority security issues through advanced technology and expertise from aggregating security events and cross-correlating security data	24 x 7
Network Threat Detection	Real-Time Network Monitoring and Proactive Incident Identification	24 x 7
Log Analytics	Sources of Log Data are collected, aggregated, analysed and normalized to identify suspicious activity that may indicate a security risk	24 x 7
Vulnerability Management	Continuously monitor the environment for vulnerabilities, gain visibility into the environment, and improve the security and compliance posture with actionable intelligence	24 x 7
Configuration Assessment	Service, Policy and Instance configurations against Cloud security best practices	24 x 7
Web App Attack Detection	The combination of signature-based detection and an embedded learning engine provide protection by detecting both known attacks and deviations from expected application behaviour	24 x 7
Enterprise Reporting	Provides an overview of several security aspects, such as incidents, events, and vulnerabilities, for your enterprise. This report provides the Executive Summary information for several report categories.	Normal Business Hours

Vulnerability Scanning	Configurable scheduled Vulnerability Scans - PCI, Internal and External Scanning with output reports sent to the Customer automatically	Normal Business Hours

1.2 Incident Management

Incident is a pattern of potentially malicious activity that implies an identified threat to an information system, violates acceptable use policies, or circumvents standard security practices. The Supplier classifies incidents into four threat severity ratings: Critical, High, Medium, and Low.

1.2.1 Threat Severity Ratings:



1.2.2 Incident Response and Escalation Table:

Incident Priority	Threat Severity Rating	Response SLA	Escalation Notification	Notification Type
P1	Critical	30 Minutes	Immediate	Telephone Call
P2	High	1 Hour	None	Telephone Call
P3	Medium	4 Hours	None	Email/GLASS
P4	Low	1 Day	None	N/A
P5	Question Query	2 Days	None	N/A

For an Incident "Response" is the time from when the ticket is first logged within the Supplier ITSM Tool to the time that the Supplier responds with a suitably qualified Employed person whether via an email, GLASS Portal update, telephone call (dependant on Priority). For detailed process flow see the current Managed Services Handbook.

From the time of Response until resolution, updates shall be provided to the Named Contacts and/or Escalation Contacts by email or GLASS Portal updates at such frequencies as set out in the table above.

Incident Resolution is handled by the Change Authority of the Supported Asset under investigation.

1.3 Change Management

Remediation steps are shared with the Customer by the Supplier. Resolution of and carrying out remedial steps is the responsibility of the Change Authority of the Supported Asset under investigation.

If the Supported Asset is under a Managed contract with the Supplier then the Service Levels of that contract will comply and the Supplier will remediate via the Suppliers Change Management Process.

Where the Customer is the Change Authority then the Incident will be functionally escalated (assigned) to the Customer to deliver any required remedial actions via Change Management.

2. Service Levels, Key Performance Indicators and Service Credits

Category	Service Level Target
P1 Incidents	100% of incidents responded to within 30 minutes – 24x7 Service Hours.
P2 Incidents	100% of incidents responded to within 1 Normal Business Hour.
P3 Incidents	100% of incidents responded to within 4 Normal Business Hours.
P4 Incidents	100% of incidents responded to within 1 Working Day.
P5 Incidents	100% of incidents responded to within 2 Working Days.

3. Exclusions

The following are listed as exclusions, but this list shall not be considered complete or exhaustive and the Terms and Conditions should be consulted.

a. End User or 1st Line support
b. Advice to any persons not listed as a Named Contact
c. Failure to meet Service Levels due to local environmental factors such as power and cooling
d. Change Requests for remediation are not included unless the Supported Asset is covered under a Managed contract with the Supplier
e. Critical security notifications that come to the Supplier in email format will be treated as Medium (Telephone will be treated as Critical)
f. High security notifications that come to the Supplier in email format will be treated as Medium (Telephone will be treated as High)

4. Customer Responsibilities

Including but not limited to:

a. Where required the Customer shall make available appropriately skilled Employed persons while an Incident is being managed
b. The Customer shall provide full administrative access to the Supplier to all the services outlined in the Impact Assessment and any subsequently identified services or provide persons with adequate access to allow investigations to proceed
c. The Customer is required to ensure that all Customer Supported Assets are appropriately licenced and have Supplier recommended hardware and vendor support in place.
d. The Customer shall ensure that all relevant Customer employees have access to and have read the Supplier's Managed Services Handbook
e. The Customer shall ensure an on-going availability of suitable Internet connection (if not provided by the Supplier)
f. The Customer shall ensure 24x7x365 availability of a suitable Escalation Contact should the Supplier need to gain approval for an Emergency Change or to engage other aspects of the Customer's support functions
g. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the Customer Supported Assets including environmental changes. Failure to do so may result in Additional Service Charges.
h. Cloud Defender onboarding will require Customer participation to ensure that the Supplier receives the right level of Customer feedback and activity to ensure a successful deployment.
i. Customers are responsible for installing agents, configuring appropriate firewall access to enable agent communication, and notifying The Supplier when installation of agents is complete. Customers are responsible for configuring appropriate access to enable appliance communication.
j. Customers are responsible for racking and installing the physical appliance(s) (if applicable), and/or loading and installing the virtual appliance image. Customers are responsible for providing network access to the appliance(s) for The Supplier personnel, configuring appropriate firewall access to enable appliance communication, and notifying The Supplier when installation of the appliance(s) is complete.
k. Customers are responsible for completing service activation questionnaires and participating in kickoff meetings to agree to the scope of the onboarding process, confirm the minimum deployment configuration and timeline of activities, and provide appropriate technical and security contacts to receive alerts, notifications and escalations. Customers are also responsible for participating in efforts to tune the Cloud Defender to best fit Customer needs.
l. Customers are responsible for identifying key stakeholders to participate in The Supplier sessions for introduction and handover to service, and to complete the available self-guided training.
m. Service continuity will require Customer participation to ensure that The Supplier receives relevant data for analysis and has the appropriate escalation contacts.
n. Customers are responsible for identifying target systems/networks and AWS environments/assets to include within the Cloud Defender service and ensuring that Cloud Defender technologies are installed appropriately for the desired scope of service and properly configured:
    a. to access all monitored networks including any necessary changes to on premise equipment such as firewalls and switches.
    b. for the desired level of log collection in their audit log settings.
o. Customers who have configured and implemented log collection black-out periods (for example, cache log data on local machine during business hours for single upload after business hours) should recognize that this collection configuration will delay log ingestion, aggregation, and normalization by the Cloud Defender service.
p. Customers must ensure that collection for target source log data and networks are properly installed in Cloud Defender and validate log and event data is being sent back to The Supplier for storage and analysis.
q. Customers are responsible for confirming the actual IP addresses, domains, or address ranges are specifically allocated to Customers prior to initiating any scans.

r. Cloud Defender capabilities depend upon a reliable connection between the the Supplier service assets, the protected network, and the Security Operations Centre. If the source network is unavailable for any reason, then event collection and correlation will be impeded. The Supplier will not be responsible for the service level commitments for that period.
s. Cloud Defender depends upon a reliable connection between the The Supplier hosted scan technologies and Customer target networks / systems. If a reliable connection is unavailable for any reason, The Supplier will not be responsible for the service level commitments for that period.
t. Customers are responsible to ensure that there is no "Scan Interference" as defined in PCI SSC's "ASV Program Guide" during the PCI Scans.
u. Cloud Defender depends upon reliable log, event, and scan data from Customer networks. Systems that are off-line, in error, or otherwise in a state that degrades the collection of log and event data inhibit service delivery. Customers are responsible for ensuring that Customer-owned networks, systems, and applications within the scope of the Cloud Defender service are maintained and functioning properly.
v. Customers are responsible for participating in ongoing service optimization activities such as performing agreed upon network or application changes and changes to Customer information.
w. Customers are responsible for communicating all relevant changes to Customer environments that may impact the scope of log and event collection/correlation or vulnerability scanning.
x. Customers are responsible for configuring escalation alerting and notification options in the The Supplier portal with accurate and updated information. Customers should include both security and technical contacts when they configure notifications so that the appropriate parties may be quickly reached and notified of a given condition.

5. Assumptions

a. All Customer Supported Assets within the Demarcation Zone within this Contract are covered by a valid software maintenance and support agreement in line with this Contract Service Levels
b. All Customer Supported Assets are in a Valid Supported Configuration at the point of contract start date
c. All Customer specific pre-requisites have been completed before contract commencement
d. The Customer will provide a suitable specification platform, operating system for the collector server