Cloudreach Managed Security Services

Service Specification

Service Specification

Service Name:	Managed Security Services
Service Level Hours:	Refer to section 1.1
Unit of Charge:	Monthly Fee
Prerequisites:	Refer to Deployment Documents Infrastructure Reliability
Supported Cloud Platforms:	AWS, Azure and GCP
Product Codes:	CPA-AL-LICAL-PRO (Alert Logic Threat Management - Professional Licences), CO-THREAT&VULN-FUNDAMENTALS, CO-THREAT&VULN-ESSENTIALS, CO-THREAT&VULN-FUND-ENTERPRISE
Version Number:	1.0
Status:	Live
Published Date:	February 2020

The Small Print

This document has been prepared solely for Cloudreach's customers. It is provided to the Customer on a confidential basis. Any reproduction or distribution of this document, in whole or in part, or the disclosure of its content, without the prior written approval of Cloudreach is not permitted. By accepting, opening or reviewing this document, Customer acknowledges the confidential nature of the information contained in this document and agrees not to reproduce or distribute this document or any information contained in this document.

Definitions

The definitions for all capitalised terms used throughout this Service Specification are set out in the Cloud Operations Service Definitions document which forms a part of this Service Specification and the Cloudreach Order Form to which this Service Specification relates.

Table of Contents

1.0 Security Services Overview

Cloudreach Managed Security Services provide a proactive approach for customers that need advanced threat intelligence and security expertise to provide continuous security monitoring and operational administration of managed devices to safeguard environments and meet compliance needs in AWS, Azure and GCP, cloud environments.

Cloudreach Security Solutions:

- Cloudreach Security Fundamentals
- Cloudreach Security Essentials
- Cloudreach Security Enterprise

Features	Cloudreach Security Fundamentals	Cloudreach Security Essentials	Cloudreach Security Enterprise
Install, Configure, Maintain Threat & Vulnerability Software	✔	✔	✔
Automated Vulnerability Reports	✔	✔	✔
Review & Recommendations	Quarterly	Monthly	Monthly
Active Vulnerability Remediation	✘	✔	✔
24*7 Incident, Threat Management & Remediation	✘	✘	✔

1.1 Service Levels

Services	Service Level Hours
Cloudreach Security Fundamentals	Business Hours (9x5) (*PDT time zone if the Customer is based in NA and GMT time zone if the Customer is based in EEA & UK*)
Cloudreach Security Essentials	Business Hours (9x5) (*PDT time zone if the Customer is based in NA and GMT time zone if the Customer is based in EEA & UK*)
Cloudreach Security Enterprise	24x7

2.0 Cloudreach Security Fundamentals

This service tier provides a fundamental level of security operations support. Cloudreach will install, configure & maintain tooling that provides customers the ability to view vulnerabilities & recommendations, enabling the customers security team to action..

Install, Configure & Maintain Threat & Vulnerability software - Cloudreach will deploy the security software in a customers environment and configure it to ensure it is working as expected.

Automated Vulnerability Reports - Cloudreach will create such reports on behalf of the customer and schedule them to be delivered at the frequency desired.

Review & Recommendations - Cloudreach will provide guidance as to priority actions which should be remediated for specific vulnerabilities. This will be completed on a quarterly basis.

Cloudreach will also be responsible for ensuring the security software is operational as well as support any changes required to reports and configuration where the effort is <3 hours per month.

3.0 Cloudreach Security Essentials

This service tier is inclusive of everything in Cloudreach Security Fundamentals offering. In addition, Cloudreach will also be responsible for reporting on vulnerabilities as well as remediating those vulnerabilities in collaboration with the customer.

Reviews & Recommendations - Monthly

Active Vulnerability Remediation - Cloudreach shall monitor the vulnerabilities generated and report any such vulnerabilities and configuration issues on a monthly basis as part of monthly reporting. In response to identified vulnerabilities and/or configuration issues, Cloudreach shall implement mutually agreed actions to the Customer's Cloud Platform where these actions are within the overall scope of this Service Specification and purchased by the Customer. Where the actions fall outside of the overall scope of this Service Specification, Cloudreach shall inform the Customer in writing.

4.0 Cloudreach Security Enterprise

A fully managed security service which includes everything in Cloudreach Fundamentals & Essentials offerings but in addition has 24x7 incident, threat management & remediation support.

4.1 Threat Management

As part of Threat Management, Cloudreach shall:

1. Respond to the intrusion types generated by a Intrusion Detection System (IDS) monitoring and log collections, as defined in the table below, by raising an Incident via the Cloudreach Incident Management Process;

2. In response to identified Incidents, Cloudreach shall implement mutually agreed actions to the Customer's Cloud Platform where these actions are within the overall scope of this Service Specification and purchased by the Customer. Where actions are outside the overall scope of this Service Specification, Cloudreach shall notify the Customer in writing and no action will be taken at the time until Customer provides it's consent;

Intrusion Type	Description
Brute force	This Incident identifies repeated authentication attempts and related activities. Alert Logic triggers a brute force incident when sufficient events indicate attempts to systematically compromise a system by brute-force guessing valid username and password combinations.
Information leak	This Incident identifies generally successful reconnaissance attempts. Alert Logic creates an information leak incident when events indicate attempts at reconnaissance activities such as port scans used to identify open and closed ports, or obtaining information from a secure system.
Log policy	This Incident uses the Log Management log correlation policies to identify potential issues. Log Management can create a log policy incident automatically based on selected correlated log messages and specifically defined conditions.
Misconfiguration	This Incident identifies a possible system misconfiguration. Alert Logic triggers a misconfiguration incident when events indicate that a system is incorrectly configured. Attackers can utilize the misconfiguration to compromise the system.
Policy violation	This Incident identifies activities that violate the acceptable use policies of most companies. These activities include viewing inappropriate material, peer-to-peer activity, and firewall policy changes.
Recon	This Incident identifies attempts to evaluate a target. Alert Logic creates a recon incident when events indicate reconnaissance activities against a network or set of hosts. The activities that trigger this Incident include gathering information about a server operating system, software versions, or the existence of debugging or demonstration scripts.
Suspicious activity	This Incident identifies activity not included in another category as set out in this table, and that requires further research. Alert Logic creates a suspicious activity incident when anomalous activities, which could indicate a compromise, occur.
Trojan activity	This Incident identifies activity that indicates a host is infected by a Trojan horse or other backdoor malware. Alert Logic creates a Trojan activity incident when events indicate a Trojan in the network. This type of malware acts as a legitimate program, but steals information or harms the system.
Worm activity	This Incident identifies hosts that display signs of worm infection. Alert Logic creates a worm activity incident when events indicate the traversing of a network worm.
Application attack	This Incident identifies attacks that target application-specific vulnerabilities. Alert Logic creates an application attack incident when an attacker attempts to compromise an application with a buffer overflow, race condition, directory traversal, SQL injection, cross-site scripting, /usr/bin/perl or other UNIX command attempts. This feature can also be set in Blocking mode and is only available as part of Alert Logic Threat Management - Enterprise. This an additional chargeable licence in addition to the Professional licence.

Cloudreach shall respond to the Intrusions Types in accordance with the service levels outlined in the section 6.0.

Cloudreach will not provide resolution times as part of Threat Management due to the varied nature of threats and the potential complexity of threat resolution. Cloudreach does provide target resolution times specified in 6.1.4

5.0 Metrics

Cloudreach will use the following metrics to assess a customer's environment for the services defined above.

- **Center of Internet Security (CIS) Compliance**
  - Cloudreach will benchmark the compliance status of a customers environment relative to the CIS framework.
  - Upon the initial meeting between Cloudreach and the customer, some checks may be removed from the Metrics in the event of mitigating circumstances or non-requirements.

- **Vulnerable Configuration**
  - Cloudreach will determine if any configuration issues are a risk to the security posture of the environment(s).
  - Examples of vulnerable configuration includes but is not limited to:
    - SSH inbound (port 22) from 0.0.0.0/0
    - RDP inbound (port 3389) from 0.0.0.0/0
    - Plain-text credentials within the environment
    - Poorly configured certificate/key storage

- **Common Vulnerabilities and Exposures (CVEs)**
  - Cloudreach will evaluate all CVEs discovered and determine if they must be remediated before onboarding into Managed Services. Examples of CVEs, but not limited to:
    - Any CVE within the customer environment(s) which is older than 60 days.
    - Any public-facing host which contains a CVE over criticality level 4.0. All other CVEs under this score will be assessed based on the risk level to the environment(s).
    - Any OpenSSH, CVEs should not be configured to allow external connections from unverified IP addresses.

6.0 Services Management Support

Cloudreach will provide maintenance, troubleshooting, support and service management to ensure the availability and accessibility of the Customer's environment(s) in the Public Cloud. This section covers the service management Cloudreach will provide to the Customers as part of Infrastructure Reliability.

6.1 Incident Management Process

6.1.1 Incident Management Guidelines

Cloudreach and Customer shall adhere to the following guidelines as part of the Incident Management Process:

- All Incidents raised by Customer will be logged with Cloudreach and will be categorised as per the Priority table (see “Incident Prioritisation” table below) in the manner described below:

Priority	CSD Access Level	Log incident by email support@cloudreach.com	Log incident through webportal**	Log incident by telephone*
P1	24X7	❌	❌	✔
P2	24X7	✔	✔	✔
P3	24x5	✔	✔	✔
P4	24x5	✔	✔	✔
P5	24x5	✔	✔	❌

*[UK] 0800 612 2966, [Overseas] +44 207 183 3991 or [US/Canada] (212) 335-0700
**webportal can be found at support.cloudreach.com using login details provided by Cloudreach during the onboarding process

    - The CSD can be accessed on a 24/7 basis to assist with P1 and P2 Incidents in the manner set out below. An Incident can be logged by the Customer or Cloudreach either through:
        - (i) emailing Cloudreach at support@cloudreach.com;
        - (ii) calling [UK] 0800 612 2966, [Overseas] +44 207 183 3991 or [US/Canada] (212) 335-0700;
        - (iii) the web by logging in to support.cloudreach.com using login details provided by Cloudreach during the onboarding process; or
        - (iv) mutually agreed automated event process.

    - For P1 Incidents specifically, the CSD can be accessed on a 24/7 basis only by telephone through the numbers as set out above. For the avoidance of doubt, P1 Incidents cannot be raised by email or through the CSD web portal.

- Customer can access CSD only by a designated Customer employee ("Support Engineer") raising an Incident.
- Cloudreach is under no obligation to respond to Incidents made in a manner which does not comply with this section. CSD will use reasonable endeavours to find a work-around or solution to the Incident.
- When logging an Incident, Customer will provide to Cloudreach the following diagnostic information:
    - Detailed description of the issue
    - Customer Incident number
    - If available and reproducible, step by step instructions to reproduce the reported Incident
    - If available, date and time (and timezone) when Incident occurred
- Following the logging of an Incident, Customer shall be available via email or

telephone to answer questions and assist the CSD as appropriate.

- Customer shall provide telephone or email access to the End User to facilitate troubleshooting Incidents.
- Customer shall provide access to End User support tools or permit Cloudreach to use their support tools to facilitate troubleshooting Incidents.
- Customer shall, within 5 working days of a request from Cloudreach, provide CSD staff access to all required Customer systems in order to enable Cloudreach.

6.1.2 Incident Prioritization

The following tables outline the prioritization of Incidents and the description of each Priority Level.

Priority Level	Type of issue
P1 - Critical Impact	Total loss of service, no workaround available.
P2 - High Impact	Functional but degraded critical service or total loss for a service which supports a critical service. No work around available.
P3 - Medium Impact	Non critical service which is partially impacted and not functioning as intended.
P4 - Low Impact	Minor issue contained to a small group. A work around or alternative service is available.
P5 - Very Low	Impact and urgency are negligible and do not need to be resolved to improve or restore service, or general technical guidance.

6.1.3 Incident Prioritization for Threat Management

The following table outlines the prioritization of Incidents and the description of each Priority Level for Threat Management.

Threat Level	Examples	Incident Priority
Critical	Successful data leakage; worm propagation; requires immediate remediation, or other post-compromise activity.	P1
High	Aggressive penetration tests, large scale or long duration brute force attacks.	P2
Medium	Brute-force or dictionary attacks; reconnaissance; failed web attack such as SQL injection, Apache Struts.	P3
Low	No threat, policy violation, authorised scans.	P4
Very Low	Informational Events which do not generate an incident.	P5

6.1.4 Incident Response and Resolution Times

The table below shows the response and resolution times for each Incident Priority. For the purpose of this clause:

- "Response" is defined as Cloudreach acknowledging the Incident by (i) providing a Cloudreach reference number either electronically or verbally to the Customer and (ii) assigning a priority to the Incident.
- "Resolution" is defined as Cloudreach providing a reasonable workaround or solution to the Incident.
- The time for Resolution starts at the same time as the Response time.
- SLA for Response and Resolution times start ticking when an Incident is logged by a Customer (either by phone, email or through the CSD web portal) or when Cloudreach is alerted of a service impact via its monitoring system.

Priority	Target Response Time	Target Resolution Time
P1	15 mins (24x7)	4 hours (24x7)
P2	30 mins (24x7)	8 hours (24x7)
P3	1 hour (24x5)	24 hours (24x5)
P4	4 hours (24x5)	3 Business Days (24x5)
P5	1 Business Day	Reasonable endeavours