RedShield Cloud
Managed Application Security Service

INCIDENT REPORT

CASE # 48170

Purpose of this Document

This document contains analysis and follow up relating to a severity 1 incident tracked in multiple RedShield support cases.

Version Control

Version:	Created by:	Date:	Description:
0.1	Daya Rajaratnam	12 June 2020	Initial Draft
1.0	Sam Pickles	12 June 2020	Review

Confidentiality

This document must be treated as Commercial in Confidence, and distribution is restricted to RedShield and its direct customers.

Disclaimers as to the Information

The information contained in this document is for general information purposes only. RedShield assumes no responsibility for the information provided by its third-parties, technologies and tools used to arrive at the information presented.

Review and Approval

Name:	Details:
Sam Pickles	CTO, RedShield Security Ltd 79 Boulcott Street, 12th Floor, Wellington, NZ 6011 sam@redshield.co
Graeme Neilson	CISO, RedShield Security Ltd. 79 Boulcott Street, 12th Floor, Wellington, NZ 6011 graeme@redshield.co

Contact

All enquiries relating to this document should be referred to:

Name:	Details:
Daya Rajaratnam	Manager Infrastructure, RedShield Security Ltd 79 Boulcott Street, 12th Floor, Wellington, NZ 6011 daya@redshield.co

Table of Contents

1. Management Summary

A widespread service outage was caused by our cloud service provider IBM which caused some customer applications to fail between 22:00 to 00:15 UTC.

Incident Ticket:	48170
Severity:	High
Services Impacted:	All RedShield customer applications, which have both primary and backup datacenters provided by IBM
Service Impact Period:	June 10th 22:00 to June 11th 00:15 UTC
Application Impacted:	Customer hosted applications via IBM datacenter
Incident Cause:	One of IBM's third party network providers advertised routes which resulted in IBM datacenter traffic becoming severely impeded globally.
Incident Resolution	IBM Network specialists made adjustments to route policies to restore network access.
Outcomes	Services to IBM datacenters were restored and services returned to normal.

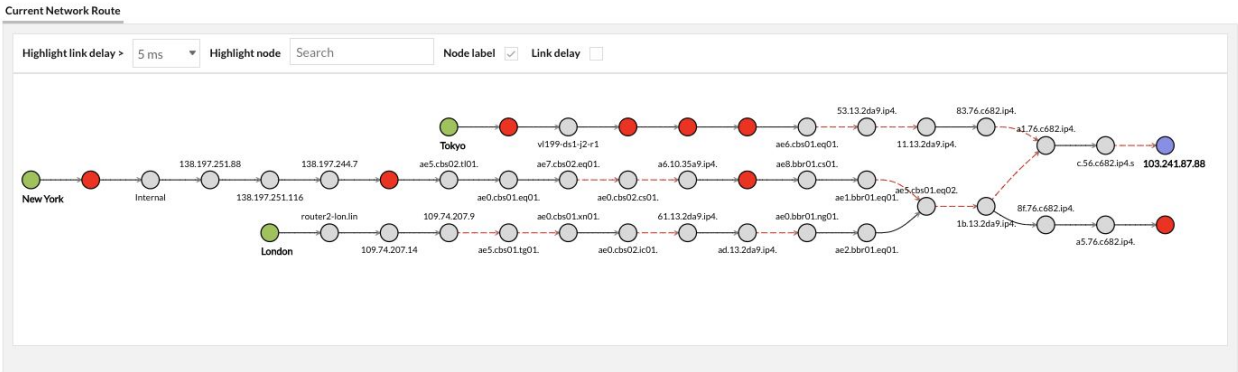
2. Root Cause Analysis

Timeline (shown in NZ time):

10:00 - Monitor failures were detected by RedShield monitoring systems.
10:06 - Support staff was notified via a 3rd party Slack notice - IBM related issue.
10:10 - Internal comms posted within RedShield of the anomaly.
10:10 - Confirmed IBM network and support portal were unavailable.
10:14 - Confirmation of the impact and verified the issue to be IBM related.
10:18 - Phone escalation to IBM (approx 1 hr response time to answer)
10:34 - War room established with RedShield internal teams coordinating on Hangouts.
10:40 - Support staff manually migrated traffic away from degraded connections, for all customers configured with non-IBM datacenter options available.
10:43 - Service announcement posted via RedShield Service Announcements.

As shown below, network traces for one of our monitor probes taken at 10:02 AM NZT show mostly failures, from multiple locations globally:

Location	Reason	Resolved IP
Fremont-CA	-	-
London	DNS Server could not resolve (timeout)	-
New York	DNS Server could not resolve (timeout)	-
Sydney	-	-
Auckland	DNS Server could not resolve (timeout)	-
Tokyo	DNS Server could not resolve (timeout)	-



Similar failures were detected around this time for virtually all IBM hosted services globally.

IBM have advised RedShield via a support ticket:

“A 3rd party network provider was advertising routes which resulted in our WW traffic becoming severely impeded. This led to IBM Cloud clients being unable to log-in to their accounts, greatly limited internet/DC connectivity and other significant network route related impacts. Network Specialists have made adjustments to route policies to restore network access, and alleviate the impacts.“

3. Resolution and Recovery

10:40 - Support staff manually migrated traffic away from degraded connections, for all customers configured with non-IBM datacenter options available.
10:55 - IBM call center was able to answer the support call and confirm the issue and advised no ETA on resolution.
12:07 - Services restored, according to RedShield monitoring systems.
13:57 - IBM confirmed all services are back to normal operation.

4. Corrective and Preventive Measures

RedShield have reconsidered the risk associated with the dependency on IBM cloud as a single provider to some customers. This is not a single point of failure as such; since every datacenter is itself highly redundant in carrier connectivity, and network and server provisioning; and all applications are configured to use at least two RedShield datacenters. The issue here relates to customers for whom both datacenters are provided by IBM. We had not previously considered a complete global failure of all IBM cloud datacenters, to be a realistic possibility.

RedShield already operates multiple non-IBM datacenters in NZ and USA. We have expedited existing plans to build an additional non-IBM datacenter for Australia, and substantially upgrade capacity in our non-IBM datacenters in NZ and USA.

This will deliver the capability to deploy all customers to a mix of both IBM and non-IBM datacenters, in all key markets.