CYBER CONNEXION

22 MARCH 2024

CAPSTONE PROJECT PRESENTATION

AGENDA

CYBER
CONNEXION

ABOUT US

MEET OUR TEAM

ANDREW COLINET

Security Operations Centre (SOC) Analyst

CATHERINE DUCHARME

Cloud Security Specialist

JAVARIA NAUMAN

Cybersecurity Practitioner

GALO F. GINOCCHIO

Cybersecurity Consultant

tpl: toronto public library

100+

Library branches

26+

Million item collection

#1

North American circulation

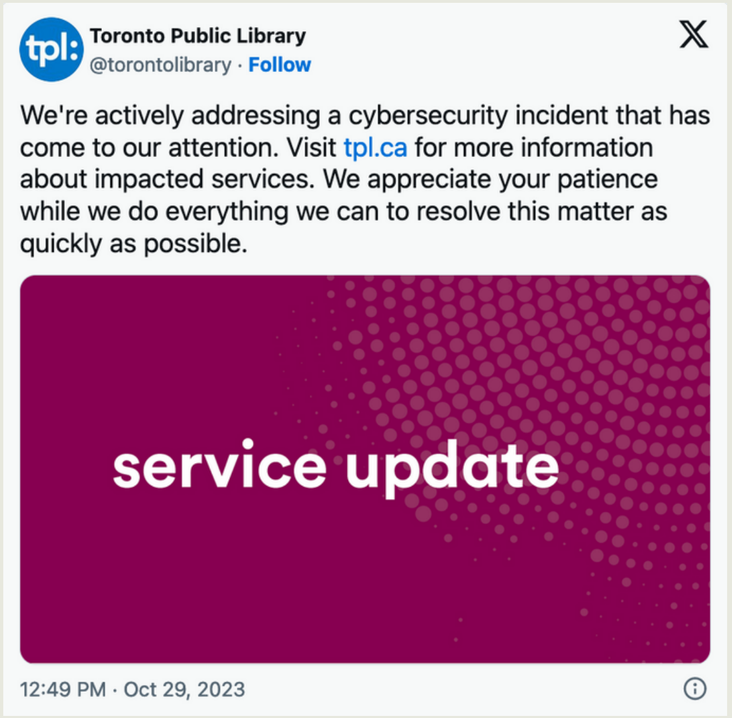
#1

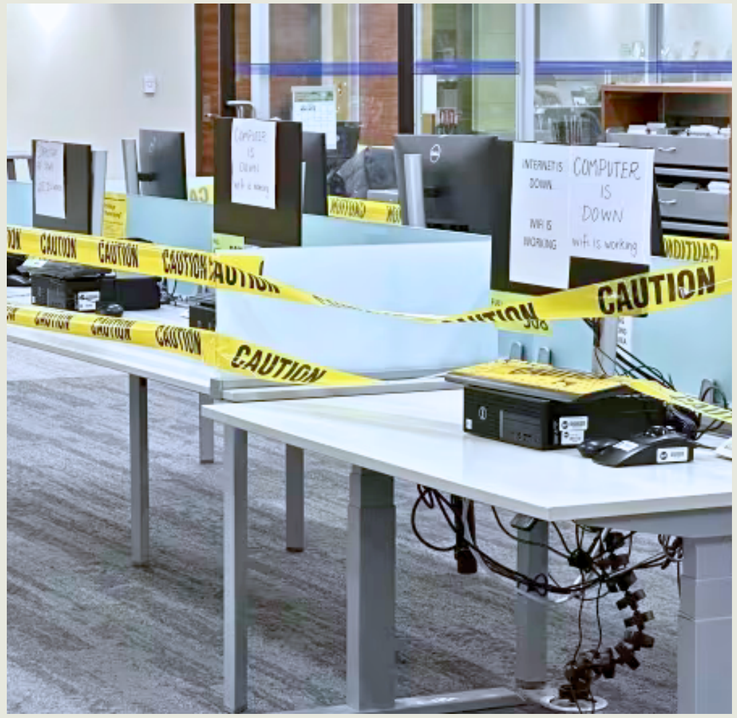
Largest neighbourhood based system

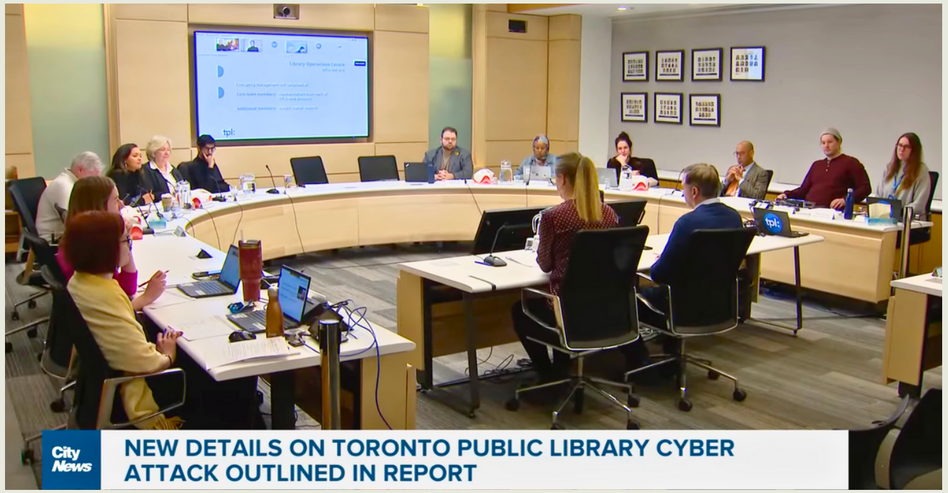
OCTOBER 28

2023

TIMELINE: 120 DAYS







October 29 2023

CYBERSECURITY INCIDENT:
TORONTO PUBLIC LIBRARY SHUT DOWN!

→

November 15 2023

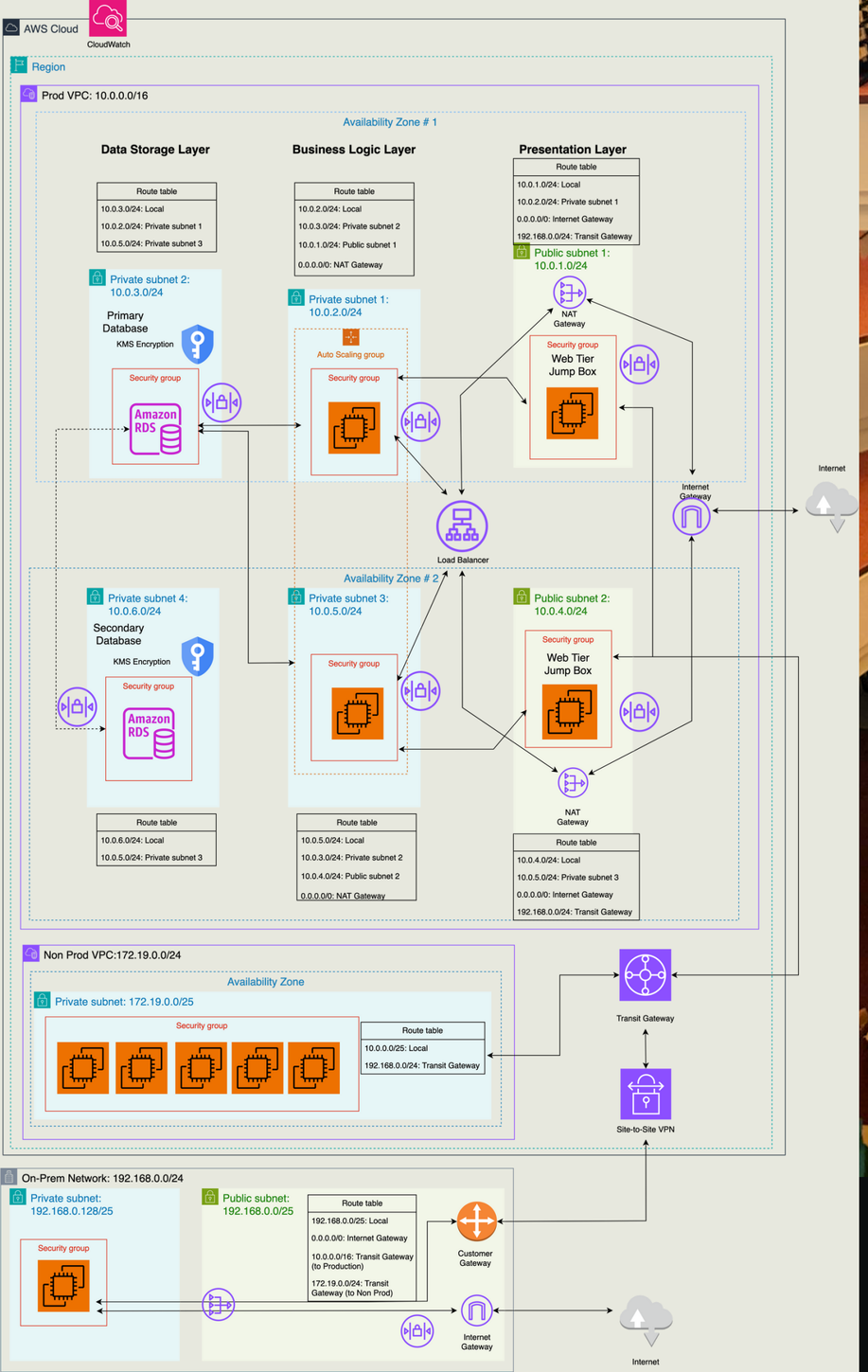
DETAILED ANNOUNCEMENT:
RETURN TO SERVICE PLANNED!

→

February 26 2024

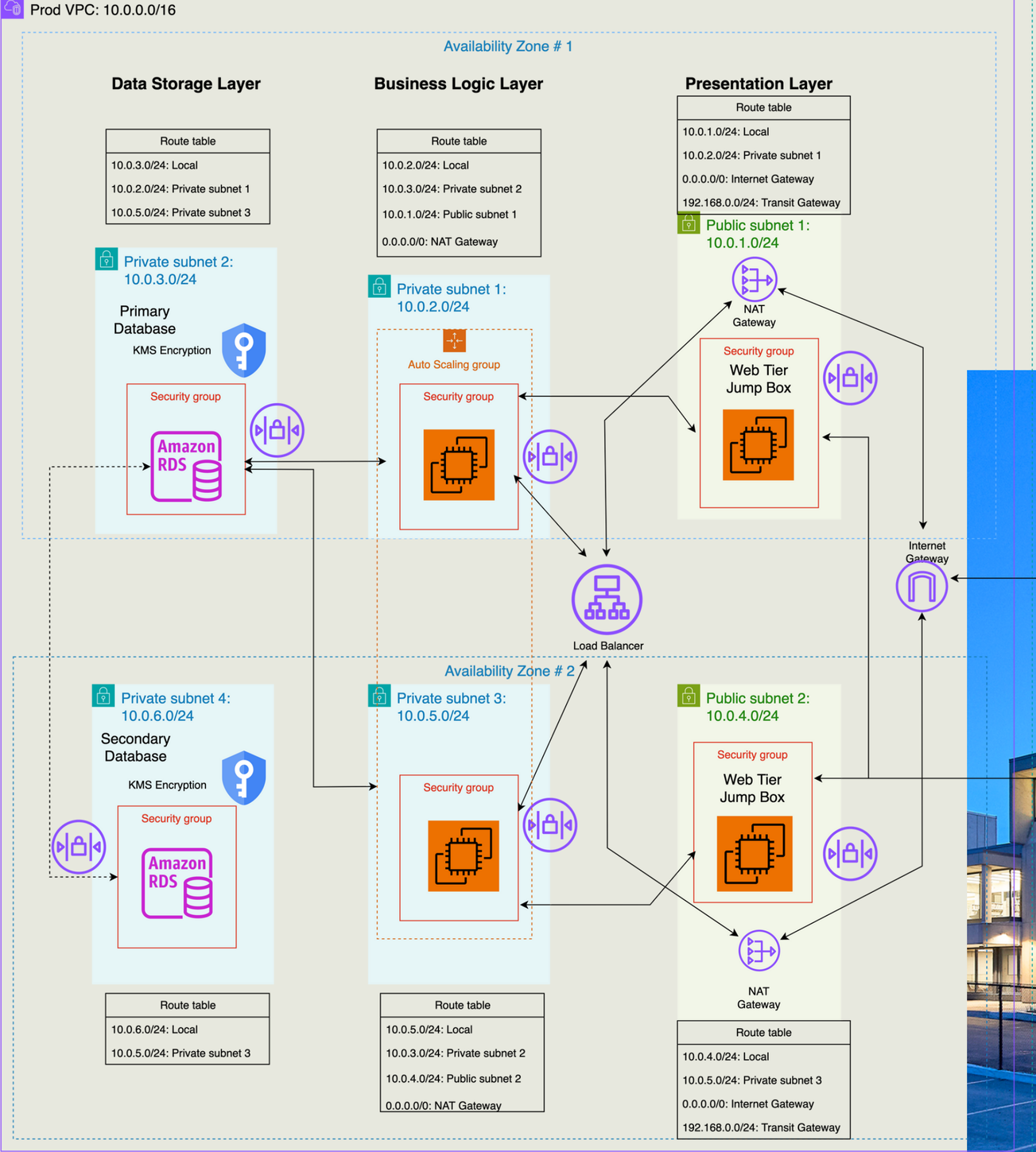
FINAL REPORT:
TORONTO PUBLIC LIBRARY RETURNS TO SERVICE!

→



TORONTO PUBLIC LIBRARY

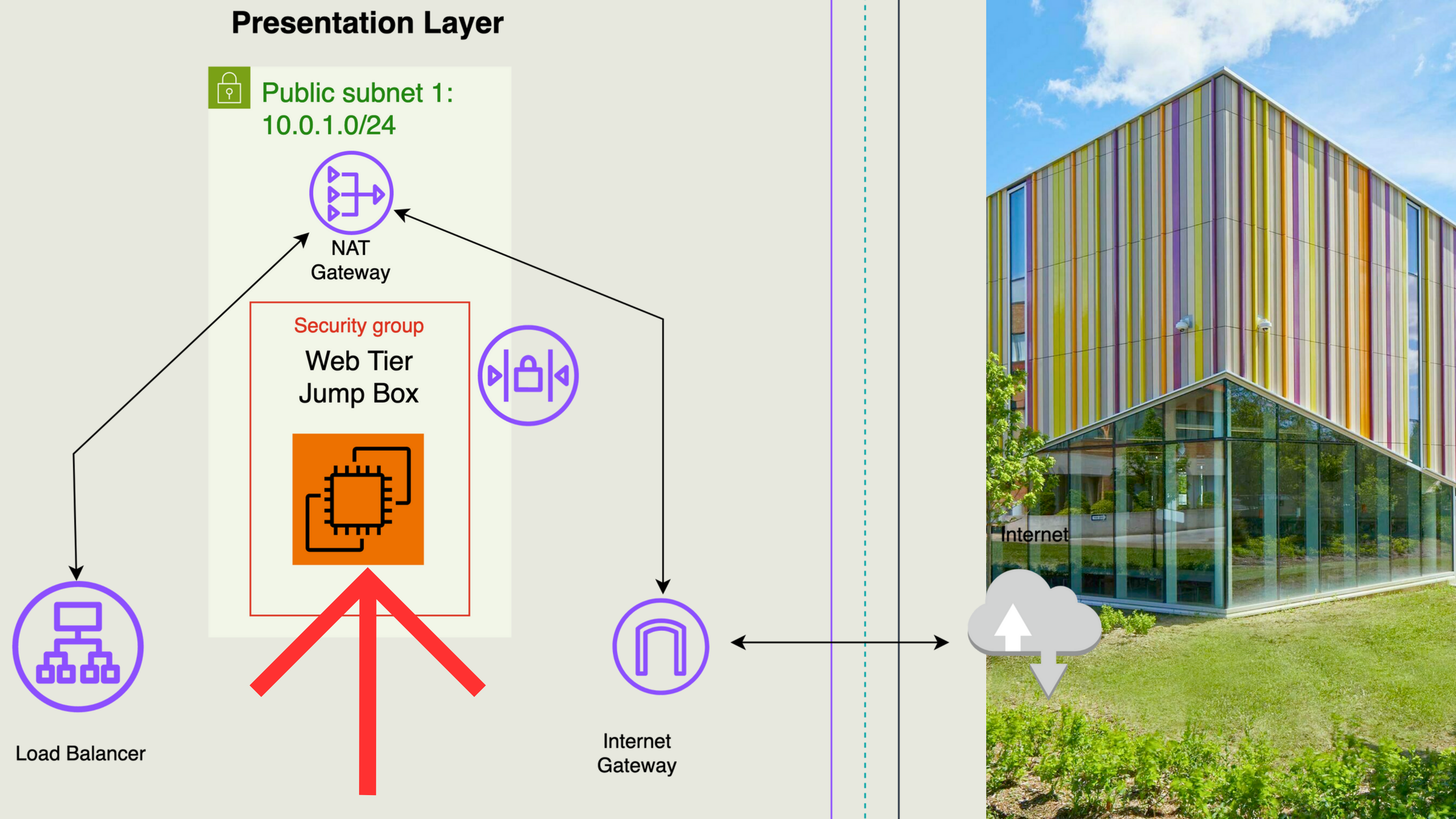
AWS ARCHITECTURE ON DRAW.IO



WHAT WE DID

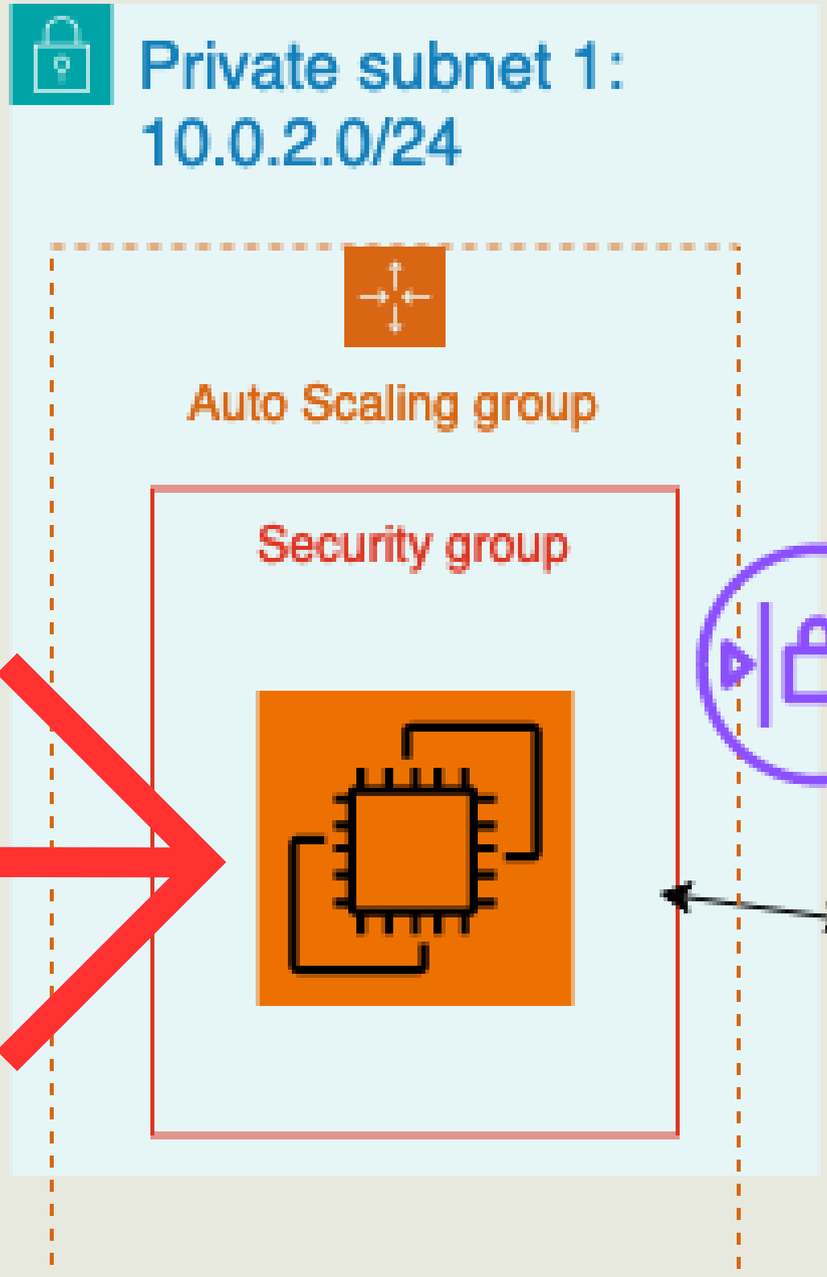
AWS ARCHITECTURE ON DRAW.IO

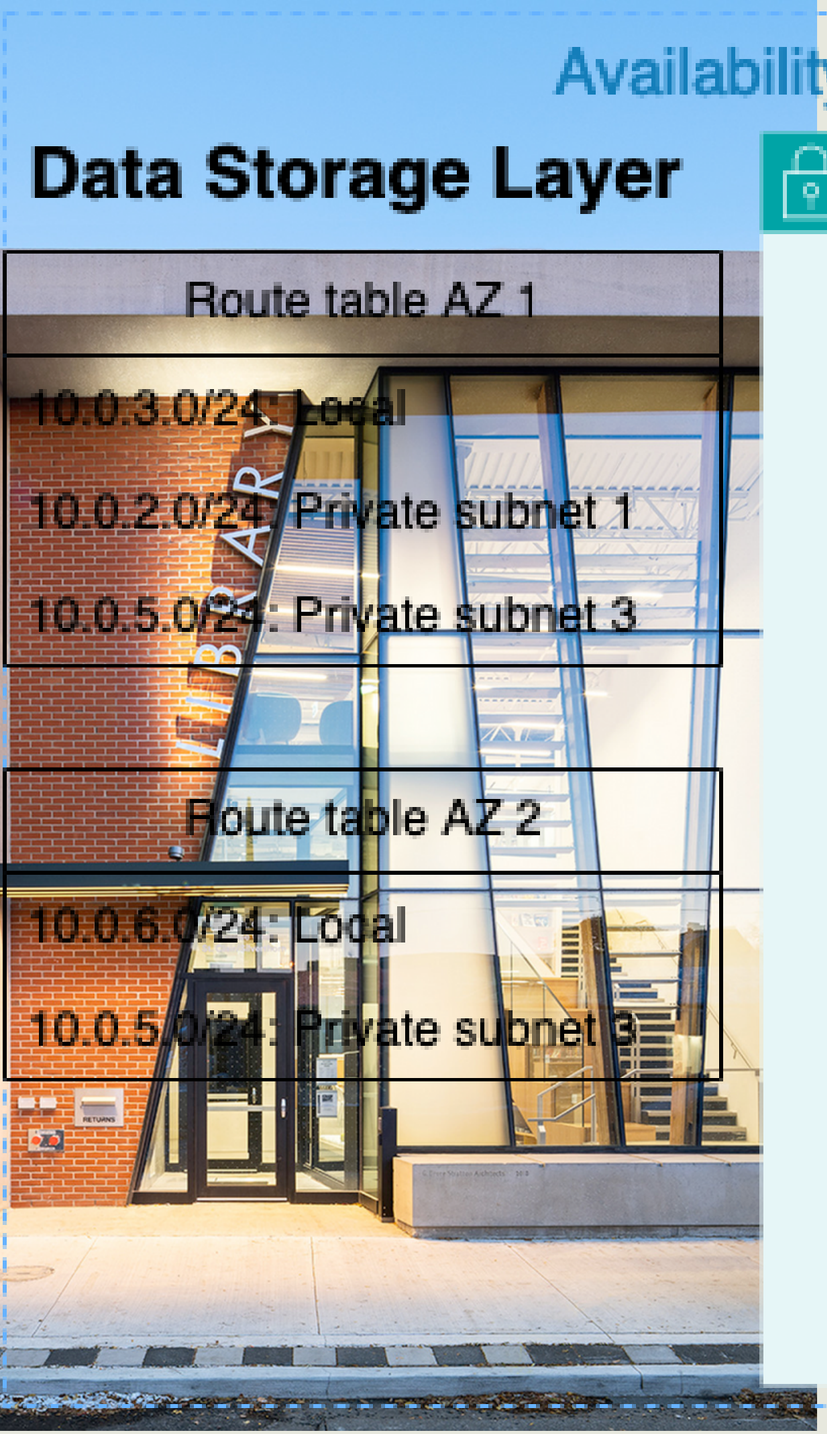
PROD VPC


Presentation Layer
Public subnet 1:
10.0.1.0/24
NAT
Gateway
Security group
Web Tier
Jump Box
Load Balancer
Internet
Gateway
Internet

Business Logic Layer

Route table
10.0.2.0/24: Local
10.0.3.0/24: Private subnet 2
10.0.1.0/24: Public subnet 1
0.0.0.0/0: NAT Gateway





Availability Zone # 1

Private subnet 2:
10.0.3.0/24

Primary
Database

KMS Encryption

Security group

Amazon
RDS

Availability Zone # 2

Private subnet 4:
10.0.6.0/24

Secondary
Database

KMS Encryption

Security group

Amazon
RDS

```
colineta@DESKTOP-RKJPQQ7:~/.ssh$ ssh -A ec2-user@54.221.56.28
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Thu Mar 21 20:23:56 2024 from 99.226.227.43
[ec2-user@ip-10-0-1-76 ~]$ ssh ec2-user@10.0.2.93
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Thu Mar 21 20:24:56 2024 from 10.0.1.76
[ec2-user@ip-10-0-2-93 ~]$
```

JUMP TIER TO APP TIER

NON PROD VPC

AWS ARCHITECTURE ON DRAW.IO

WHAT WE DID

Non Prod VPC:172.19.0.0/24

Availability Zone

Private subnet: 172.19.0.0/25

Security group

Route table
10.0.0.0/25: Local
192.168.0.0/24: Transit Gateway

Transit Gateway

Site-to-Site VPN

ON PREM

WHAT WE DID

AWS ARCHITECTURE ON DRAW.IO

On-Prem Network: 192.168.0.0/24

Private subnet:
192.168.0.128/25

Security group

Public subnet:
192.168.0.0/25

Route table
192.168.0.0/25: Local
0.0.0.0/0: Internet Gateway
10.0.0.0/16: Transit Gateway (to Production)
172.19.0.0/24: Transit Gateway (to Non Prod)

Customer Gateway

Internet Gateway

Internet

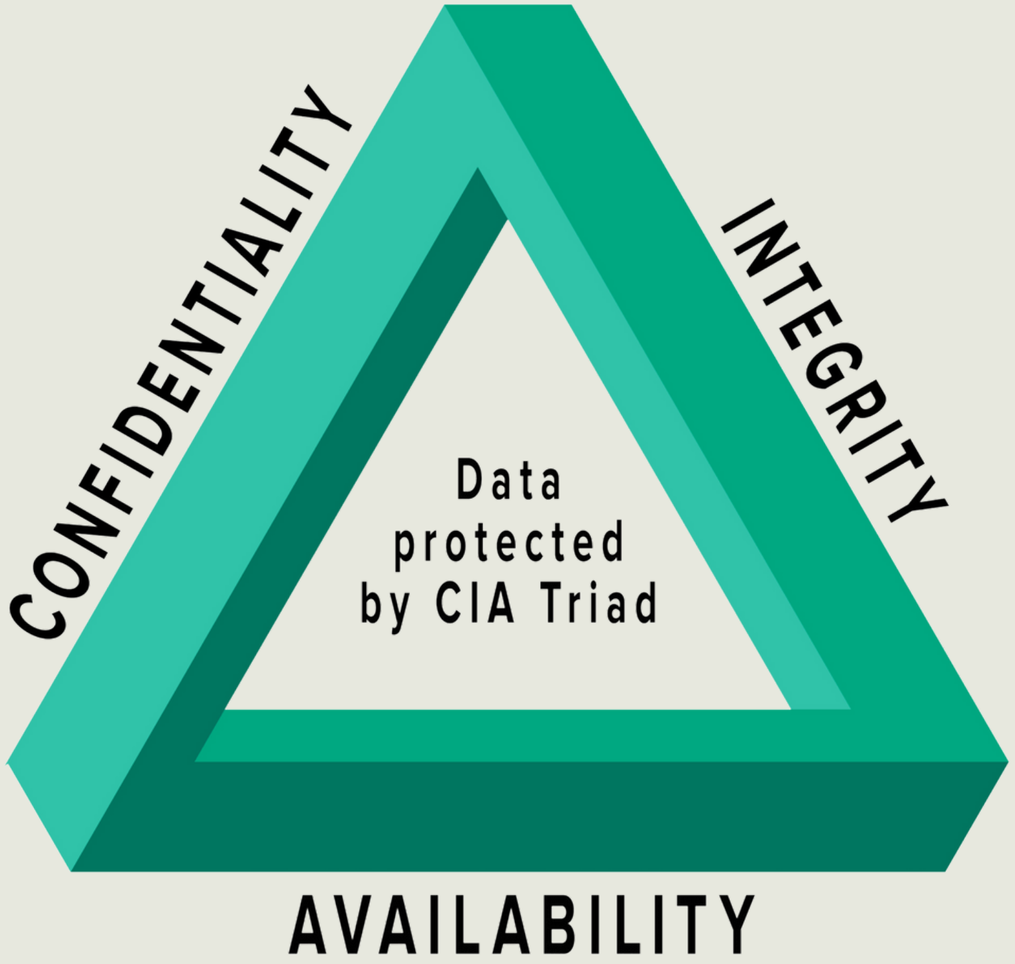
GUIDING PRINCIPLES

01 CIA

02 Defense in Depth

03 Zero Trust

04 NIST


CONFIDENTIALITY
INTEGRITY
Data
protected
by CIA Triad
AVAILABILITY

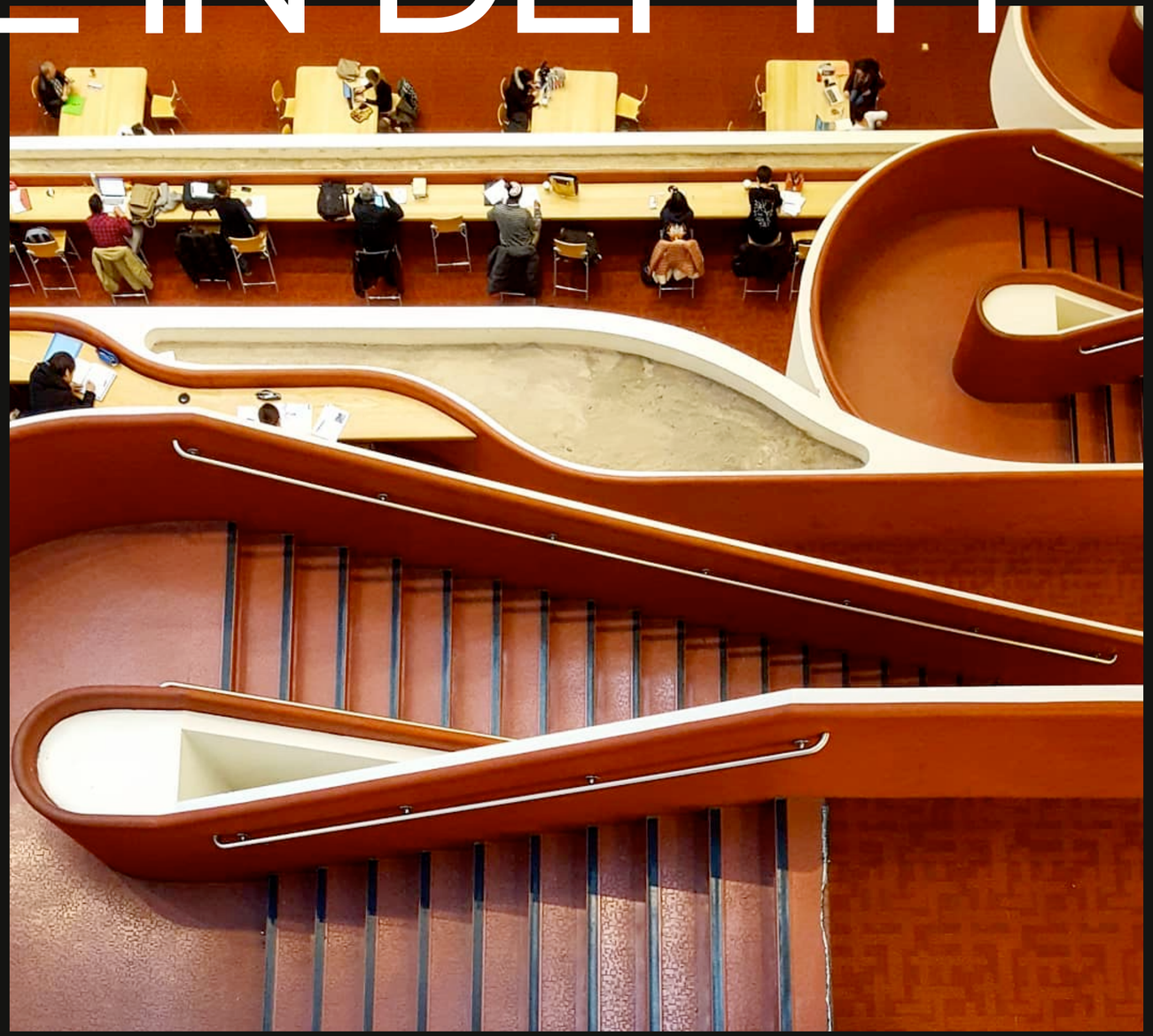
DEFENCE IN DEPTH

PHYSICAL CONTROLS

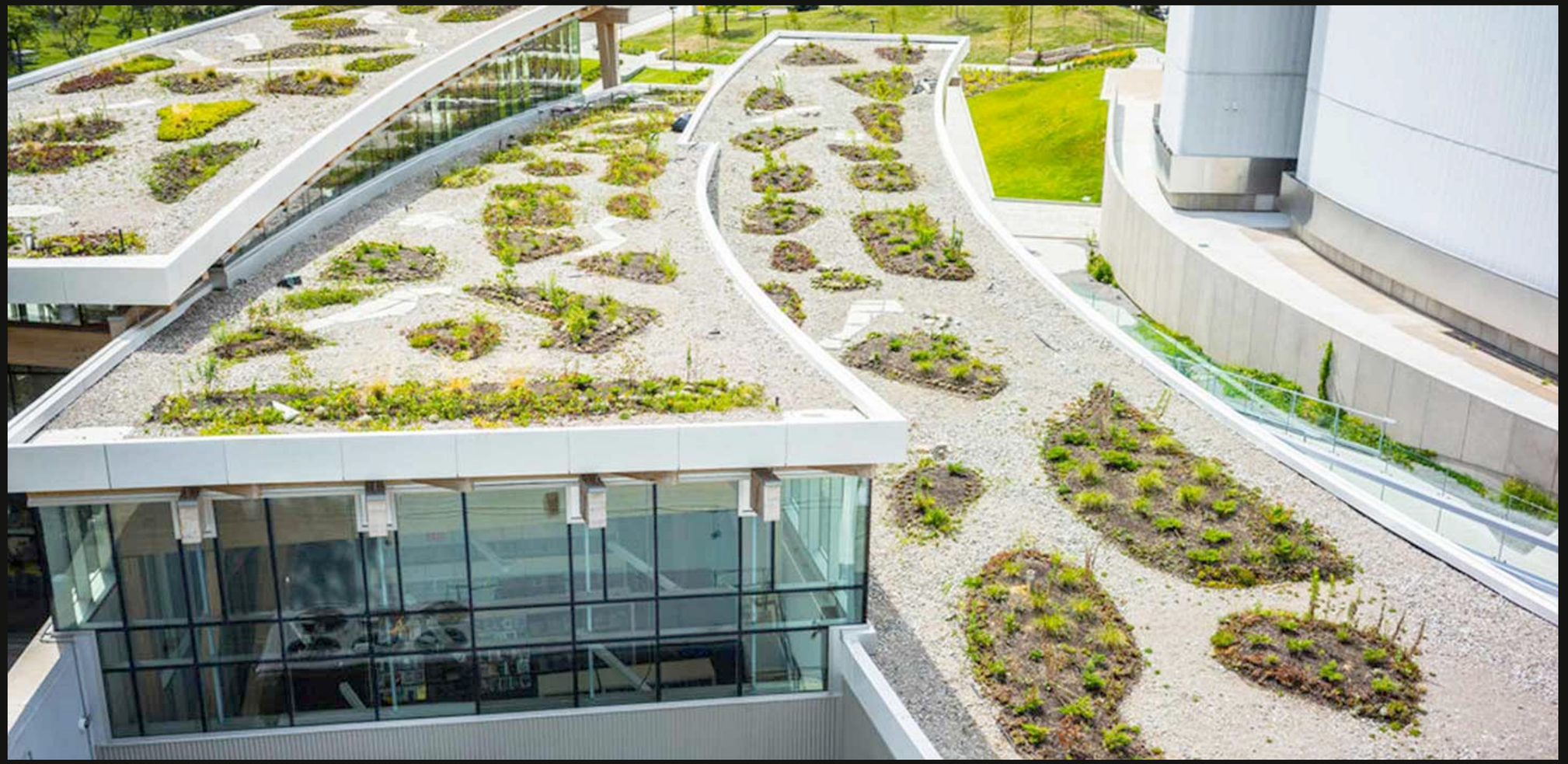
NETWORK SECURITY CONTROLS

ADMINISTRATIVE CONTROLS

ANTIVIRUS



ZERO TRUST



ZERO TRUST

LEAST PRIVILEGE

ALWAYS VERIFY

ASSUME BREACH

NIST COMPLIANCE

IDENTIFY

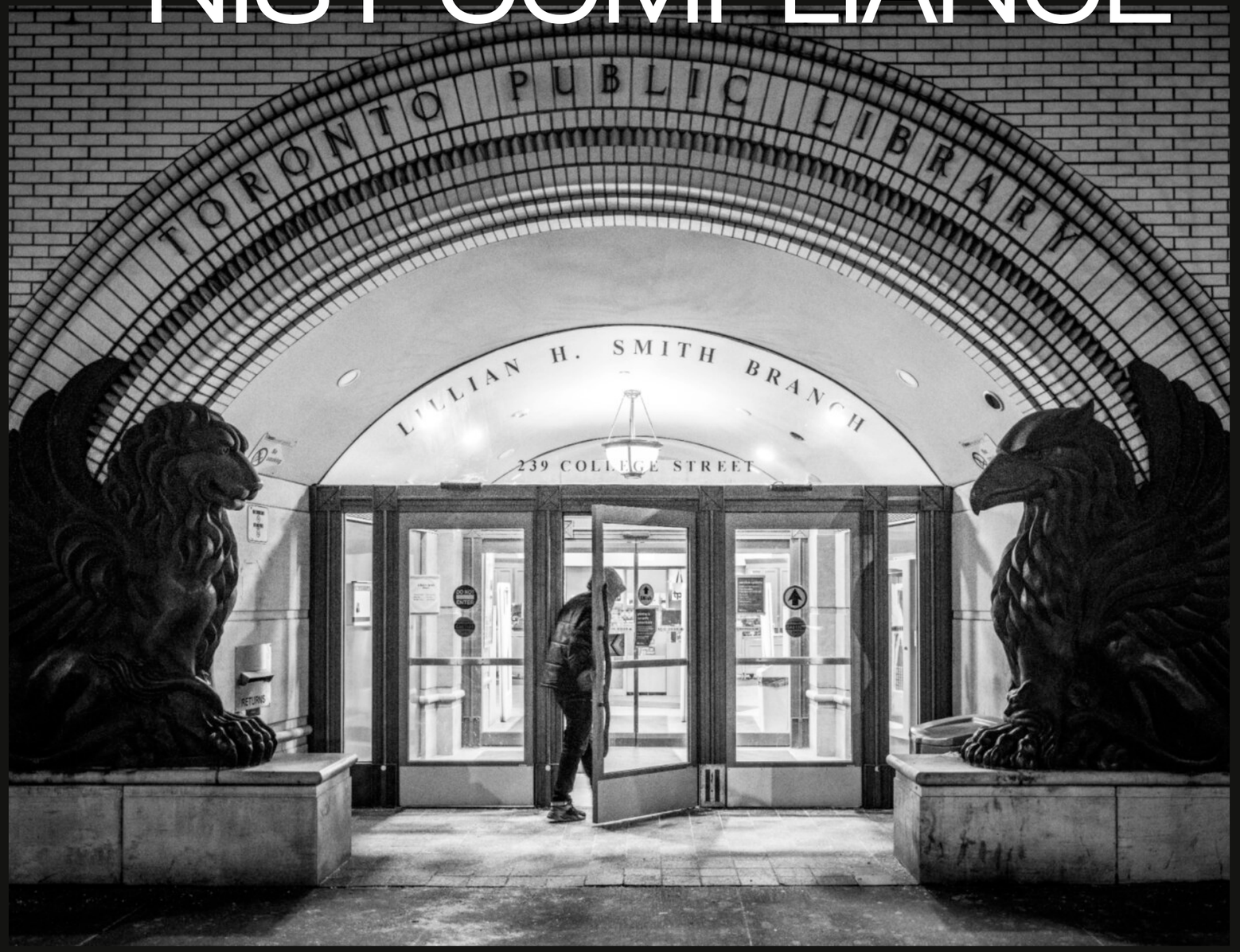
PROTECT

DETECT

RESPOND

RECOVER

GOVERN



HashiCorp

Terraform

AWS CLOUDFORMATION

Amazon CloudWatch

Viewing Dashboard for : NorthMedicaidUser

Select User : NorthMed

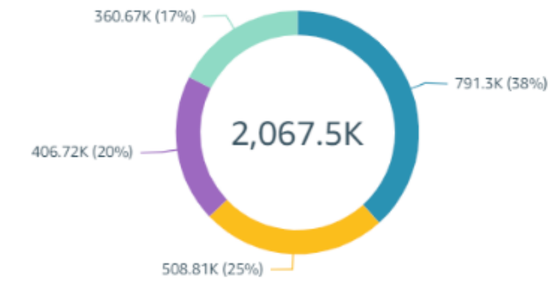
venue is forecasted to be
64 for Feb 2020

Revenue by Admit Date

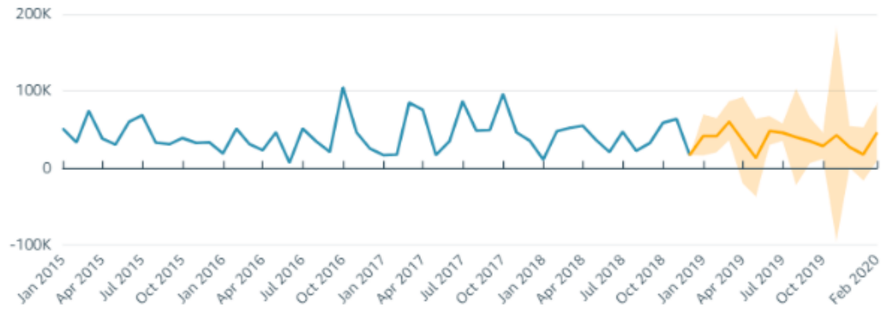
2017
$611K

-$145K ↓

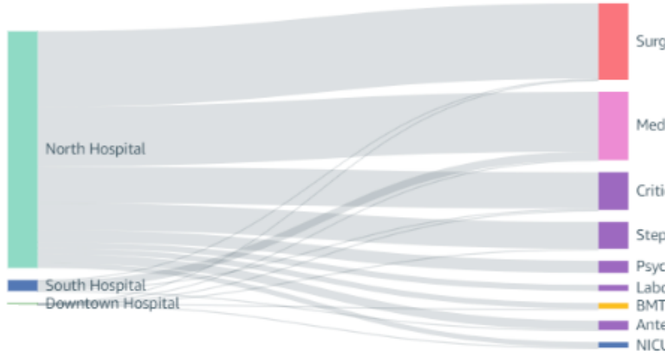
Sum of Revenue by Payor Segment



Sum of Revenue by Admit Date



Sum of Revenue by Hospital and Category



Revenue by Hospital, Payor Segment, and Physician

al	Payor Segment	physician	revenue
Hospital	Corporate Insurance	ANDERSON	6,350.43
Hospital	Medicaid	ANDERSON	18,714.51
Hospital	Medicare	ANDERSON	11,291.64
Hospital	Personal Cost	ANDERSON	1,345.79
Hospital	Corporate Insurance	BROWN	17,169.76
Hospital	Medicare	BROWN	71,693.25
Hospital	Personal Cost	BROWN	8,184.89
Hospital	Corporate Insurance	Barnett	11,889.54
Hospital	Medicaid	Barnett	20,951.05
Hospital	Corporate Insurance	Bradley	19,415.82
Hospital	Medicaid	Bradley	25,843.93
Hospital	Medicare	Bradley	827.76
Hospital	Corporate Insurance	Bray	5,050.9
Hospital	Medicaid	Bray	8,874.1
Hospital	Personal Cost	Bray	11,971.04
Hospital	Corporate Insurance	Cement	36,309.21
Hospital	Medicaid	Cement	33,602.97
Hospital	Medicare	Cement	2,748.66

amazon QuickSight

Revenue

693.37K 0.09K

ue by Payor Segment, Hospital, and State

nt	hospital	state	revenue
Insurance			508,809.74
	Downtown ...	New York	9,629.51
	North Hospital	Connecticut	128,642.92
		Delaware	123,783.02
		Mass	198,702.69
		New Jersey	157,625.92
		New York	80,471.1
	South Hospital	New York	92,445.81
Medicare			406,719.94
Personal Cost			360,671.22

21.

toronto public library

STAFF REPORT
INFORMATION ONLY

Cybersecurity Report

Date: February 26, 2024

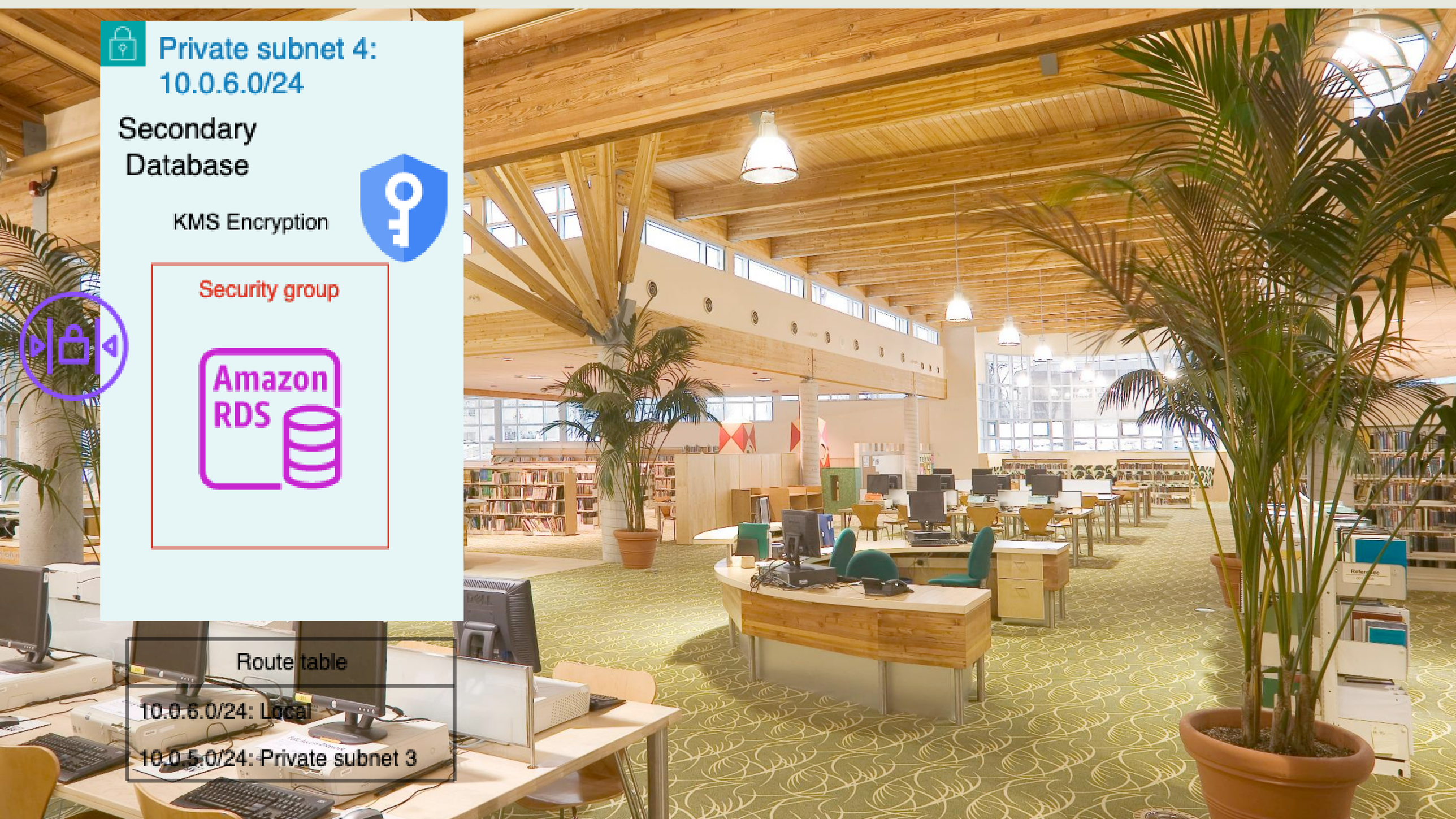
To: Toronto Public Library Board

From: City Librarian

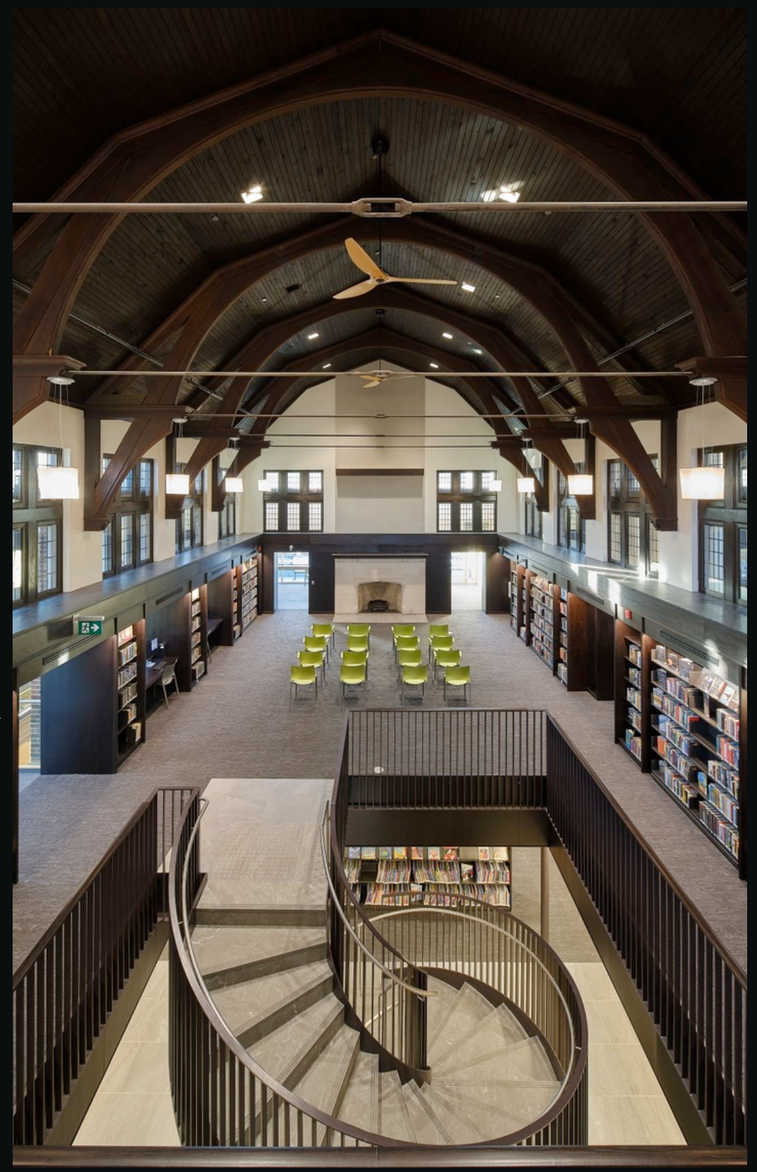
SUMMARY

The purpose of this report is to provide the Toronto Public Library Board with a final report on the investigation into the Toronto Public Library's (TPL's) cybersecurity attack.

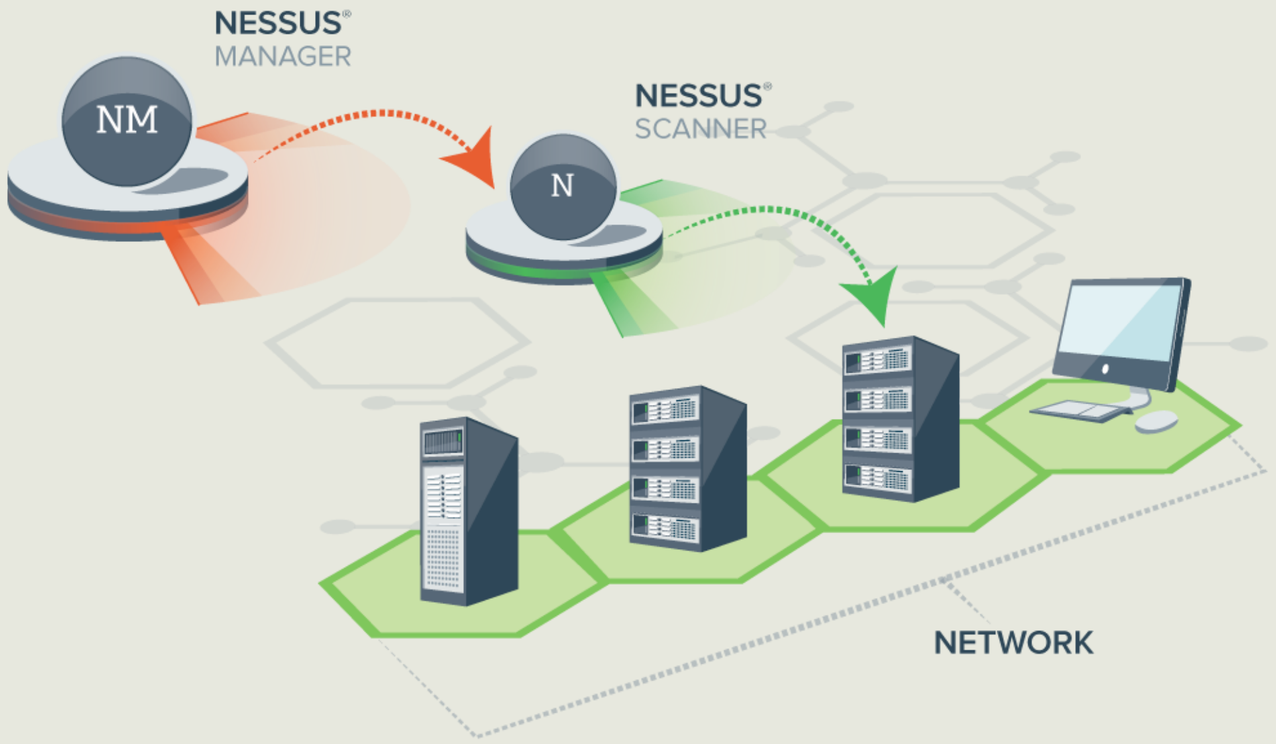
When TPL became aware of a cybersecurity incident on October 28, 2023, staff immediately initiated measures to mitigate potential impacts by shutting down the technical environment including all internal and external networks and systems. Third-party legal counsel with expertise in cybersecurity were engaged to collaborate with third-party cybersecurity technical experts to advise on containment, conduct forensics, and assess the impact. In addition, the cybersecurity experts supported staff's planning for and implementation of additional proactive measures to safeguard TPL's data and information systems. The privileged and confidential report from legal counsel, including its appended technical input from the third-party cybersecurity experts, outline the support the experts provided in response to the incident, their forensic analysis of the cyberattack, and the privileged and confidential input given to support TPL in rebuilding its technical environment for optimum security.


Private subnet 4:
10.0.6.0/24
Secondary
Database
KMS Encryption
Security group
Amazon
RDS
Route table
10.0.6.0/24: Local
10.0.5.0/24: Private subnet 3

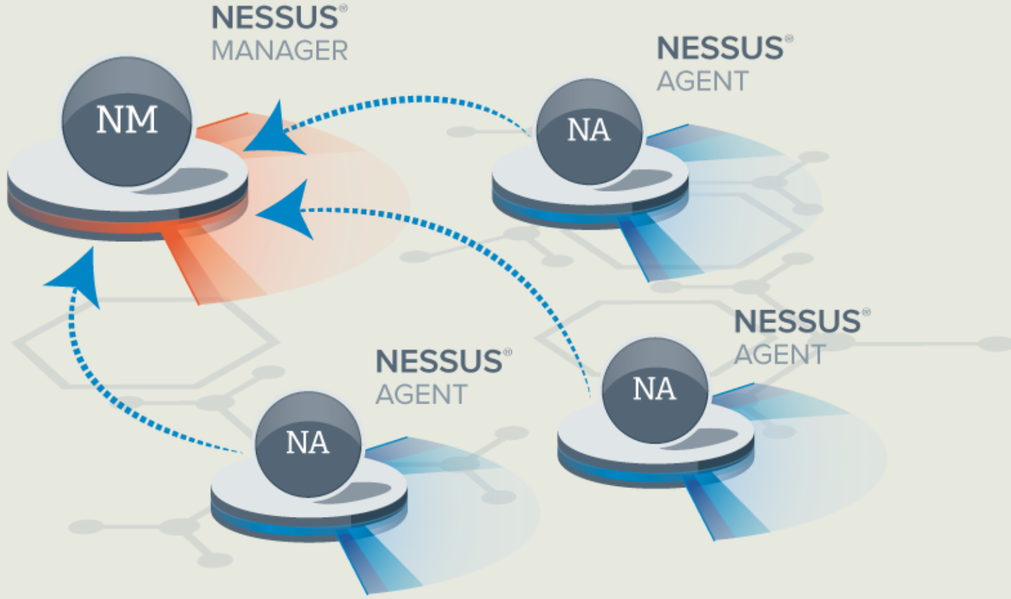
VULNERABILITY MANAGEMENT



Traditional Scanning



Agent-based Scanning



tenable network security

NESSUS AGENT SCAN

Summary

Critical	High	Medium	Low	Info	Total
0	4	4	0	37	45

Details

Severity	Plugin Id	Name
High	190943	Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6653-1)
High	183116	Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM : ZeroMQ vulnerabilities (USN-4920-1)
High	183123	Ubuntu 18.04 ESM / 20.04 ESM : libmysofa vulnerability (USN-5184-1)
High	172614	Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : FFmpeg vulnerabilities (USN-5958-1)
Medium	183568	Ubuntu 20.04 ESM / 22.04 ESM : Python vulnerabilities (USN-5342-2)
Medium	183778	Ubuntu 18.04 ESM / 20.04 ESM / 22.04 ESM : FFmpeg vulnerabilities (USN-6449-1)
Medium	182982	Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM : FFmpeg vulnerabilities (USN-6430-1)
Medium	185568	Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Traceroute vulnerability (USN-6478-1)
Info	170170	Enumerate the Network Interface configuration via SSH

NESSUS AGENT SCAN

NAME	IPV4 ADDRESS	VULNERABILITIES	VULNERABILI...	CRITICAL	HIGH
agent-name	10.0.5.170		18	0	0
agent-name	10.0.2.181		18	0	0
agent-name	10.0.5.162		18	0	0
agent-name	10.0.2.79		18	0	0
agent-name	10.0.4.29		18	0	0
agent-name	10.0.1.240		18	0	0

SEVERITY	NAME	FAMILY	INSTANCES
Info	OS Identification	General	6
Info	Host Fully Qualified Domain Name (FQDN) Resolution	General	6
Info	Authenticated Check : OS Name and Installed Package Enumeration	Settings	6
Info	Netstat Portscanner (SSH)	Port scanners	6
Info	Nessus Scan Information	Settings	6
Info	Enumerate IPv6 Interfaces via SSH	General	6
Info	Enumerate IPv4 Interfaces via SSH	General	6
Info	Remote listeners enumeration (Linux / AIX)	Service detection	6
Info	BIOS Info (SSH)	General	6
Info	Common Platform Enumeration (CPE)	General	6
Info	Device Hostname	General	6
Info	Time of Last System Startup	General	6
Info	Netstat Connection Information	General	6
Info	Ethernet MAC Addresses	General	6
Info	OS Identification and Installed Software Enumeration over SSH v2 (...	Misc.	6
Info	OS Security Patch Assessment Not Available	Settings	6
Info	Unix Software Discovery Commands Available	Settings	6
Info	Enumerate the Network Interface configuration via SSH	General	6

0 CRITICAL VULNERABILITIES

0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES

0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	03/20/2024 at 4:46 PM
TEMPLATE	Basic Agent Scan

Agent Details

REPORTED
6 of 6

GROUPS
PriusAgents

EXTERNAL SCAN

NAME ↑	IPV4 ADDRESS	VULNERABILITIES	VULNERABILI...	CRITICAL	HIGH
ec2-44-200-2...	44.200.225.1...		26	0	0

SEVERITY	NAME	FAMILY	INSTANCES
Info	RPC Services Enumeration	Service detection	2
Info	ICMP Timestamp Request Remote Date Disclosure	General	1
Info	RPC portmapper Service Detection	RPC	1
Info	SSH Server Type and Version Information	Service detection	1
Info	SSH Protocol Versions Supported	General	1
Info	Remote Desktop Protocol Service Detection	Service detection	1
Info	Nessus SYN scanner	Port scanners	1
Info	OS Identification	General	1
Info	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
Info	Nessus Scan Information	Settings	1
Info	Service Detection	Service detection	1
Info	TCP/IP Timestamps Supported	General	1
Info	Backported Security Patch Detection (SSH)	General	1
Info	Common Platform Enumeration (CPE)	General	1
Info	RPC portmapper (TCP)	RPC	1
Info	Device Type	General	1
Info	Patch Report	General	1
Info	SSH Algorithms and Languages Supported	Misc.	1
Low	SSH Server CBC Mode Ciphers Enabled	Misc.	1
Info	Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
Info	OS Security Patch Assessment Not Available	Settings	1
Info	SSH SHA-1 HMAC Algorithms Enabled	Misc.	1
Low	SSH Weak Key Exchange Algorithms Enabled	Misc.	1
Info	OpenSSH Detection	Misc.	1
Medium	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	Misc.	1

0 CRITICAL VULNERABILITIES

0 HIGH VULNERABILITIES

1 MEDIUM VULNERABILITIES

2 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	03/22/2024 at 8:58 AM
TEMPLATE	Advanced Network Scan
SCANNER	US East Cloud Scanners

TARGETS

44.200.225.118

SCANNER GROUPS

US East Cloud Scanners

FUTURE RECOMMENDATIONS

Regular Data Backups

Patch Management

Endpoint Protection

Access Controls

Monitoring


TEENS
tpl
toronto
public library

tpl toronto public library

THANK YOU

Cyber Connexion

— Powered by —
The Fields Institute