ResBaz
RESEARCH BAZAAR

Cloud Security

An Introduction to Cloud Security for Researchers

Dr Thomas Laurenson

tom.laurenson@auckland.ac.nz

June 2025

What is our goal?

- Discuss ***security best practices***
- Discover ***methods*** to improve cloud security
- Change ***thought patterns*** about security

OPENNESS
USABILITY
COLLABORATION
SECURITY
imgflip.com

Research vs Security

Research Systems	Secure Systems
Academic mindset	Corporate mindset
Collaborative	Restrictive
Open source	Closed source
Low risk (perceived)	High risk
Lacking best practices	Process heavy

Research Compute

- **Option 1: Laptop**
  - Logical first option
- **Option 2: HPC**
  - Got some serious data to crunch?
- **Option 3: Cloud**
  - Want more flexibility?

ResBaz
RESEARCH BAZAAR

Cloud Computing in a Slide

- Normal compute
- More compute
- And way more stuff!
- AWS, Azure and GCP all have 200+ services

aws

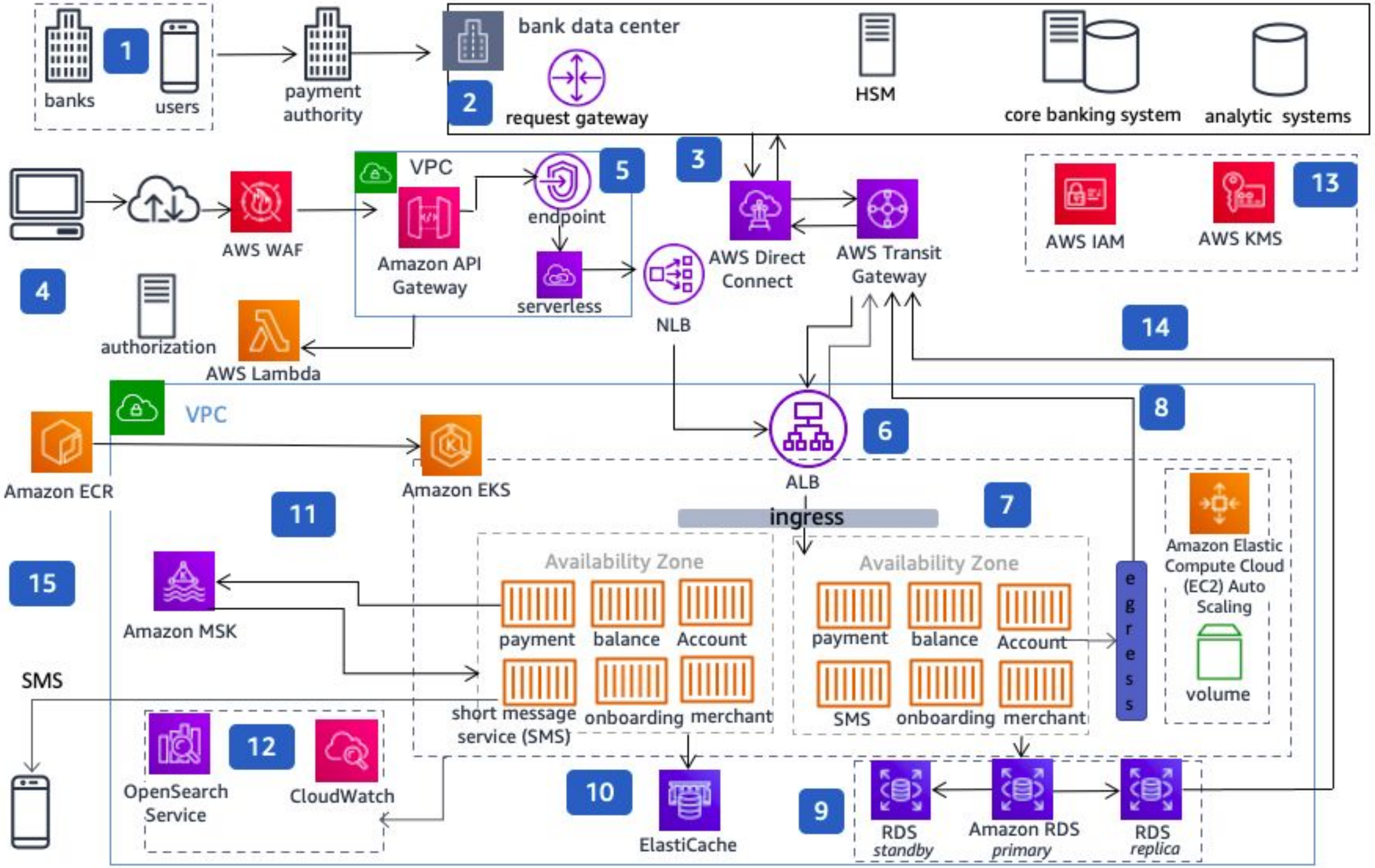
Azure

Google Cloud

ARDC Nectar Research Cloud

https://aws.amazon.com/products/compute/

All the services!



https://docs.aws.amazon.com/architecture-diagrams/latest/payment-system-interface-modernization/payment-system-interface-modernization.html

ResBaz RESEARCH BAZAAR

Cloud Security is Hard

- Multiple platforms
- Multiple systems
- Self-managed
- Not secure by default
- Information overload
- Difficult terminology

The cybersecurity reality…

- EDUCAUSE
  - Ranks cybersecurity as #1 competency in 2024
  - 116 successful cyberattacks against universities in 2023
  - Average cost of $6 million (NZD) per data breach

- Data Breach Investigations Report (DBIR)
  - ~2000 security incidents
  - 86% confirmed data disclosure
  - Threat actor:
    - 68% external
    - 32% internal

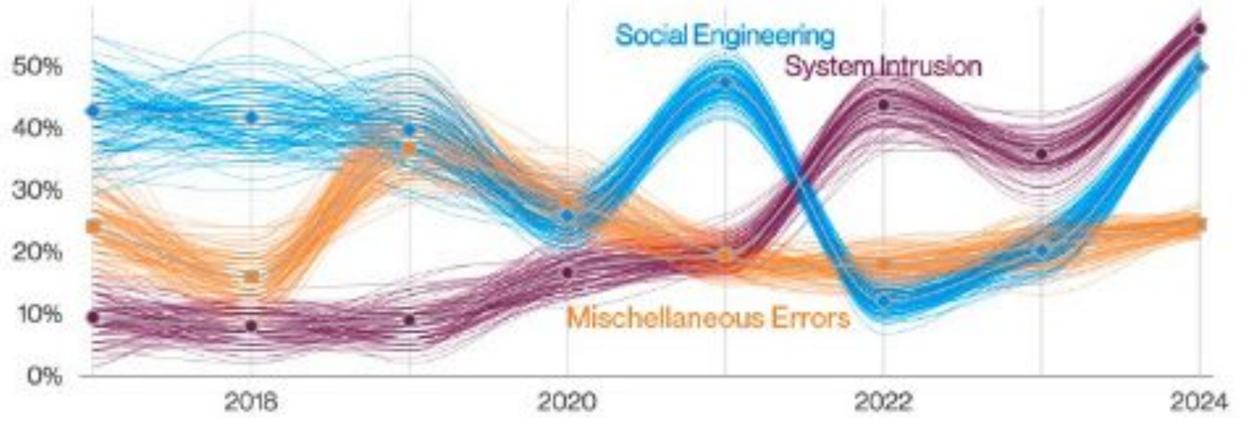


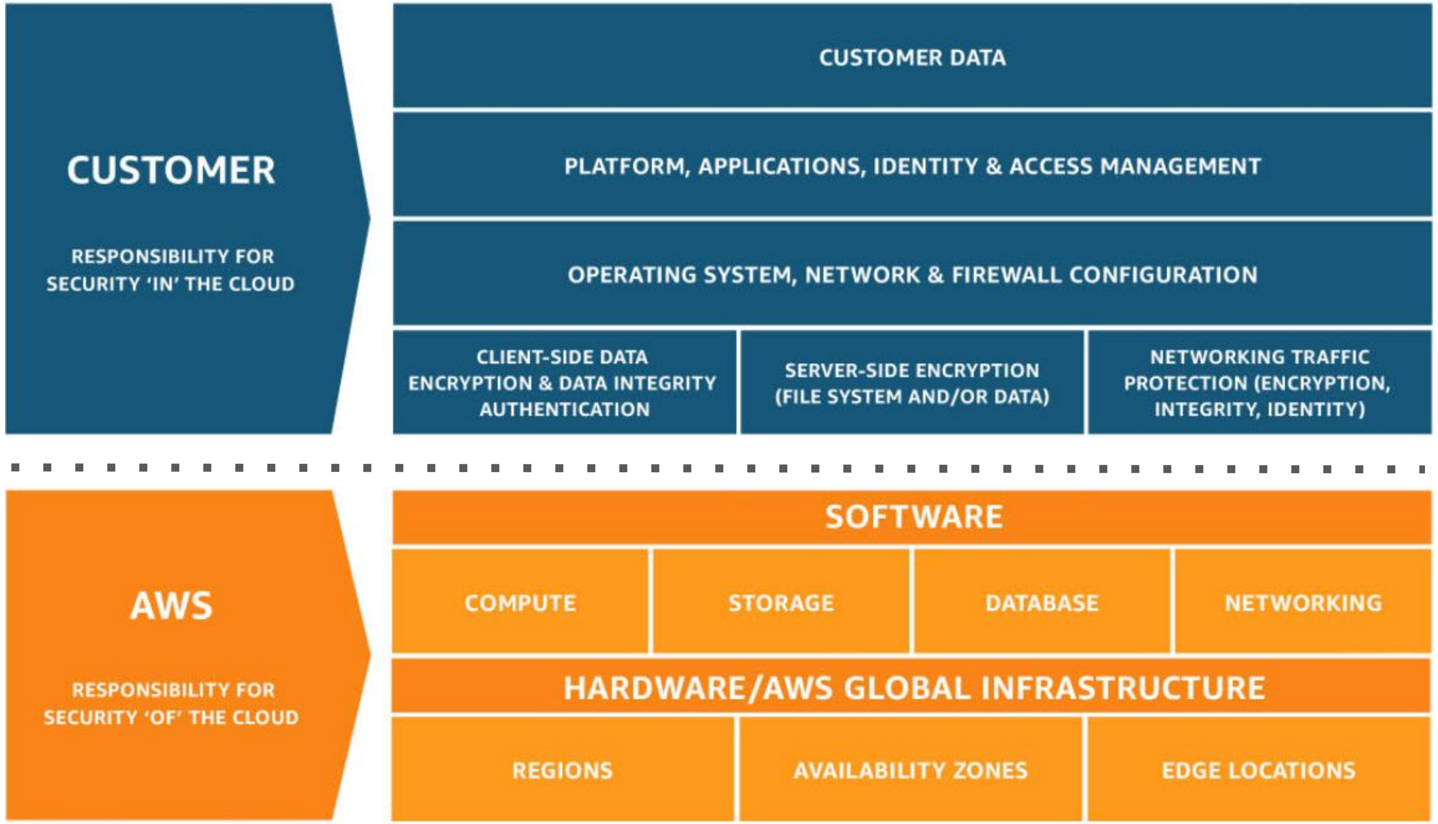
Figure 59. Top patterns in Educational Services industry breaches

https://www.verizon.com/business/resources/reports/dbir/
https://library.educause.edu/resources/2023/5/2023-educause-horizon-report-teaching-and-learning-edition

Shared Responsibility

- *“Security in the Cloud”*
- Mainly application and OS level
- Patching software, firewalls

- *“Security of the Cloud”*
- AWS, Azure, Nectar etc.
- Mainly infrastructure level



CUSTOMER

RESPONSIBILITY FOR SECURITY ‘IN’ THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY ‘OF’ THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

https://aws.amazon.com/compliance/shared-responsibility-model/

What are we doing?

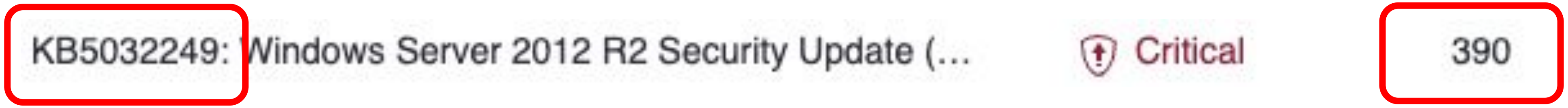
- **Central**
  - Training and awareness
  - Security scanning
  - Security focussed roles

- **Centre of eResearch**
  - Extending range of managed services (MVMS, SRE)
  - Security improvements for Nectar Cloud
  - Maturing security processes

ResBaz
RESEARCH BAZAAR

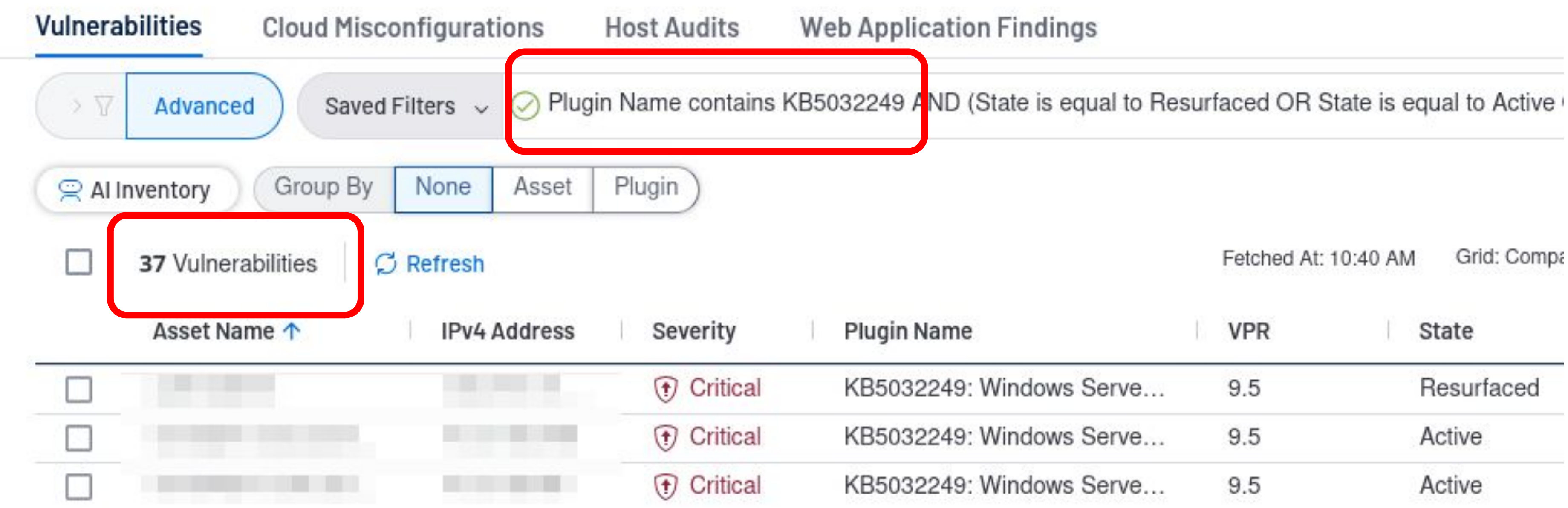
Progress...

2024



KB5032249: Windows Server 2012 R2 Security Update (… Critical 390

2025



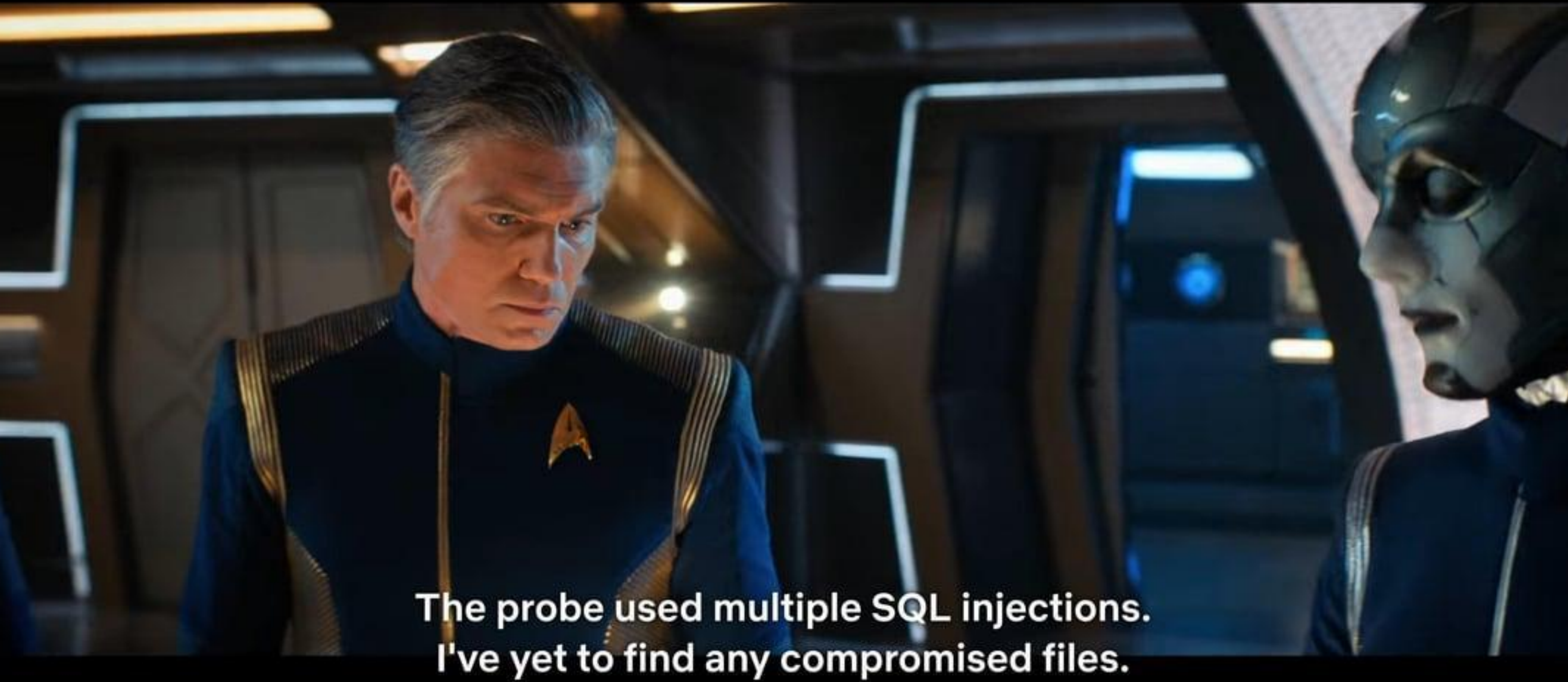
Plugin Name contains KB5032249 AND (State is equal to Resurfaced OR State is equal to Active

□ 37 Vulnerabilities

Fetched At: 10:40 AM Grid: Compa

□	Asset Name ↑	IPv4 Address	Severity	Plugin Name	VPR	State
□	[redacted]	[redacted]	Critical	KB5032249: Windows Serve…	9.5	Resurfaced
□	[redacted]	[redacted]	Critical	KB5032249: Windows Serve…	9.5	Active
□	[redacted]	[redacted]	Critical	KB5032249: Windows Serve…	9.5	Active

ResBaz RESEARCH BAZAAR



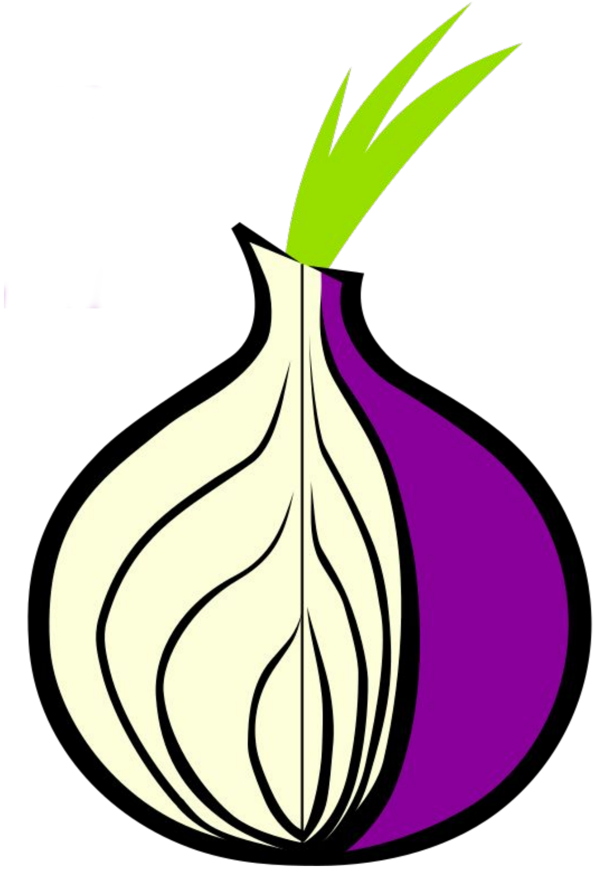
The probe used multiple SQL injections.
I've yet to find any compromised files.

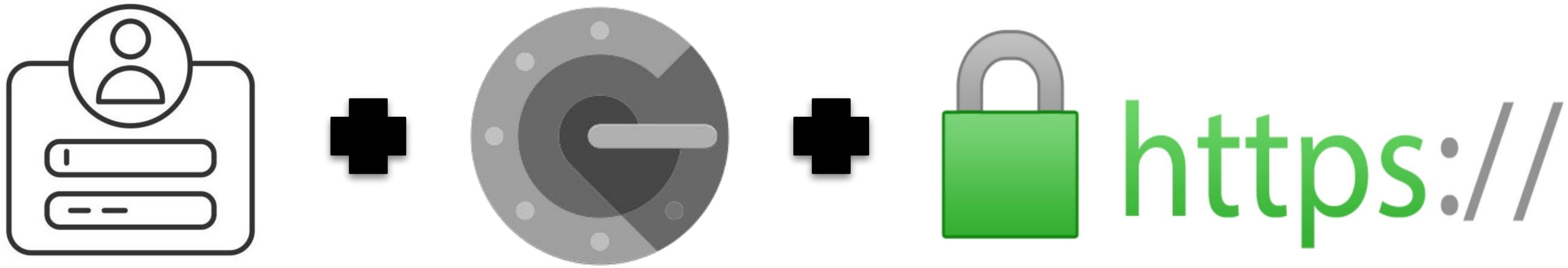
Today's Top 5

1. **Layers** are essential
2. Let someone else **manage** it
3. **Upgrade** as much as possible
4. **Expose** only essential services
5. **Harden** what is left

1 Layered Security

- *Defence in depth*
- Security is like onions 😭
- Layered approach…
- No one single solution is enough





ResBaz
RESEARCH BAZAAR

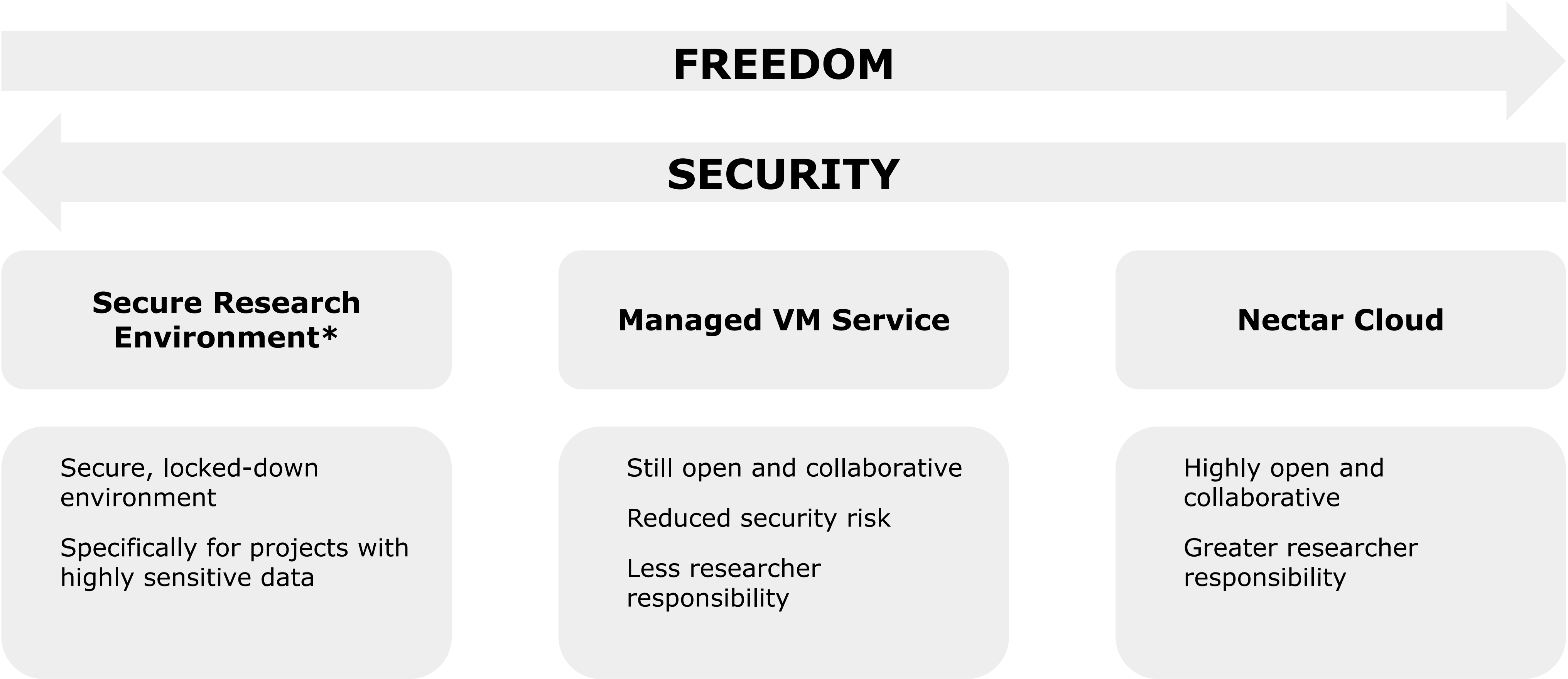
2 Third Party Management

- Use a ***university-managed*** service
  - Managed Virtual Machine Service (MVMS)
  - Nectar Cloud managed service
  - For example: Database, R Studio instance

- Use ***vendor-managed*** service
  - For example: AWS Managed Services
  - Where AWS performs security hardening and backups

https://research-hub.auckland.ac.nz/research-software-and-computing/advanced-compute/research-virtual-machines
https://aws.amazon.com/managed-services/

Tiered Access Model



FREEDOM

SECURITY

Secure Research Environment*

Secure, locked-down environment

Specifically for projects with highly sensitive data

Managed VM Service

Still open and collaborative

Reduced security risk

Less researcher responsibility

Nectar Cloud

Highly open and collaborative

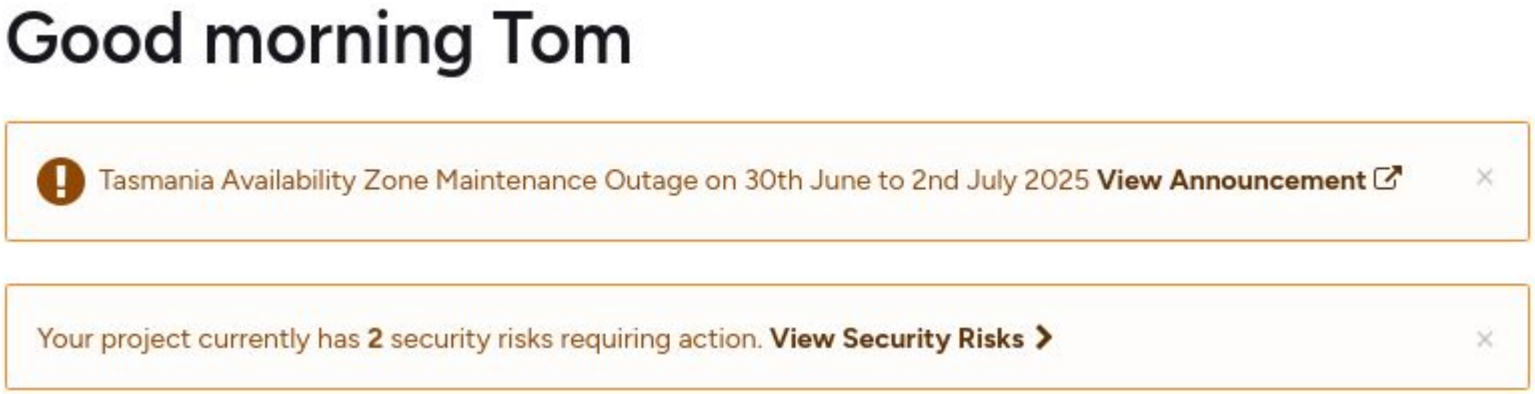
Greater researcher responsibility

https://research-hub.auckland.ac.nz/research-software-and-computing/advanced-compute/research-virtual-machines

ResBaz RESEARCH BAZAAR

Hardening Nectar Cloud

- Automatic security updates (Linux only)
- Pre-installed fail2ban (Linux only)
- Hardened RDP
- SSH connection using CAs (Linux only)
- Default security scanning “agents”
- New “security alerts”



Good morning Tom

Tasmania Availability Zone Maintenance Outage on 30th June to 2nd July 2025 **View Announcement**

Your project currently has **2** security risks requiring action. **View Security Risks**

3 Upgrading

- Keeping your **operating system** up-to-date
- Keeping your **installed software** up-to-date
- Aspects can be automated

```
sudo apt upgrade

sudo dnf upgrade

sudo yum update
```

4 Expose Only Essential Services

- Cloud computing and the Internet are inherently linked
- Provides Internet-accessible "resources"

Best Practices:

- Only expose what needs to be on the Internet
- Restrict access using "Security Groups"
- Remove access by "Network Segmentation"

5 Hardening

- Configuring system/software to be more secure
- Follow best practices

Examples:

- Set HTTPS on your web server, disable HTTP
- Set SSH to only allow key authentication, disable password login
- Set RDP connections to only accept from specific IP addresses
- Install intrusion prevention software (e.g., fail2ban)

5 Hardening – How?

- CIS Benchmarks
  - https://www.cisecurity.org/cis-benchmarks
  - AWS CIS Foundations Benchmark
  - CIS compliance with Ubuntu LTS

- AWS Best Practices
  - https://aws.amazon.com/getting-started/aws-security-essentials/
  - https://docs.aws.amazon.com/security/

- Nectar Knowledge Base
  - https://support.ehelp.edu.au/support/solutions

Revisiting Today's Top 5

1. **Layers** are essential
2. Let someone else **manage** it
3. **Upgrade** much as possible
4. **Expose** only essential services
5. **Harden** what is left

Future of Security

> *eResearch solutions become so secure…*
> *that nobody can use them*

- Primary goal is always to **support research** and researchers
- Retain **highly open and collaborative** systems
- Prioritise balance between **security and freedom** in tiers
- Set and maintain **sensible defaults**
- Raise **awareness** and provide **educational material**

ResBaz
RESEARCH BAZAAR

Thank you!
Any Questions?

Dr Thomas Laurenson

tom.laurenson@auckland.ac.nz

June 2025