Azure Security Faux Pas

What To Do Before You Get Penetration Tested

Name: Blaise St-Laurent
Title: Architecture & Cloud Lead
Date: March 2021

Who am I?

- Architecture & Cloud Lead
- 22 years in the security field
- Came from a network security background
- Cloud agnostic, but primarily Azure and AWS focused

ZX Security

- Organisation structure:
  - 28 staff
  - 7 years in business
  - 2018 Deloitte Fast 50
  - CREST Certified

CREST. PEN TEST

Deloitte FAST 50

ZX Security

- What we do:
  - Web based security testing (API, website etc)
  - Internal and external penetration testing
  - Specialist work (hardware, red team, physical access)
  - Security design and architecture reviews
  - vCISO, SLT security advice and consulting
  - And of course, cloud security reviews

ZXSECURITY.CO.NZ

The basics

- Microsoft Cloud (One Cloud)
  - Azure
  - Microsoft 365
  - Power Platform
- All 3 underpinned by common security technology (Azure Active Directory)
- Most customers are going from on-premises to Cloud based

Azure security – broad trends

- Every customer examined has an on-prem Active Directory
- Azure is seen as very much a cloud extension of more traditional infrastructure
- Microsoft 365 drives users into Azure, but it's not an easy migration
- DevOps is driving a lot of excitement
    - The basics aren't necessarily done well though!
- Serverless is sexy but scary, still being digested as a concept
- Proliferation of portals and technologies makes for a difficult and unclear implementation of Microsoft Cloud.

Azure security – broad trends

- Many customers are multi-cloud:
  - Azure for Infrastructure / Internal apps
  - AWS for external, customer facing apps
- Very few use B2B tenants or other separation of users; lots of guest accounts and external entities exist in "Customer's" Azure AD
- Monitoring and log retention is suddenly much more complicated and potentially expensive vs traditional on-prem

ZX SECURITY

ZXSECURITY.CO.NZ

How ZX assesses Azure security

- Mostly manual testing:
  - Automated tooling is in its infancy compared to AWS
  - Security Center is key and covers most of the findings, yet customers routinely ignore it
  - Deep dive on some specific issues based on understanding of the customer / application
- Also examine any source code, externally-facing resources that are exposed

Azure security – the data

- Customer breakdown:
  - Public sector – 10 reports
  - Private – 22 (Note: same company responsible for 7 reports)
- Most of the reports are combined with other assessments:
  - Azure + M365
  - Azure + Web App / API tests

The data

- ZX uses normalised findings for many common issues so we can compare across customers
- Issues' impacts and likelihood change depending on context
- Access granted to consultant biases which findings will be discovered (ex: Reader at Subscription level vs Global Reader)
- Note we are looking primarily at how common they are, this can be for a few reasons:
  - Easy to pick up programmatically (ex: reported in Security Center)
  - Not a default setting
  - Requirements for NZISM

Evolution of data

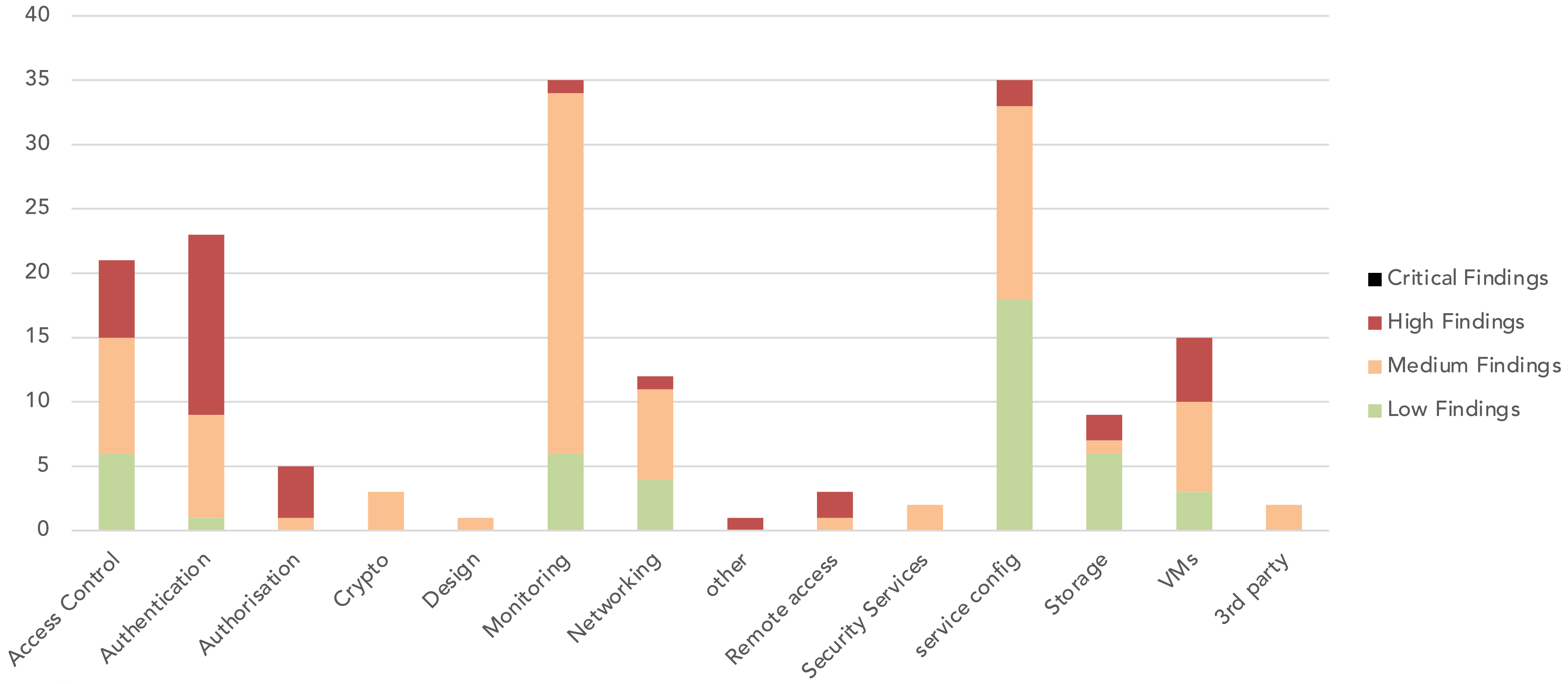
- There are definite historical trends on the data at hand:
  - As our customers' Azure use evolved and matured, so too did our testing
  - Under-representation of new services that are now fairly common (App Services, Bastion)
  - Kubernetes – different type of engagement
  - New security features are also under-represented
    - JIT – Just In Time access
    - PIM – Privileged Identity Management

Being first is not always best…

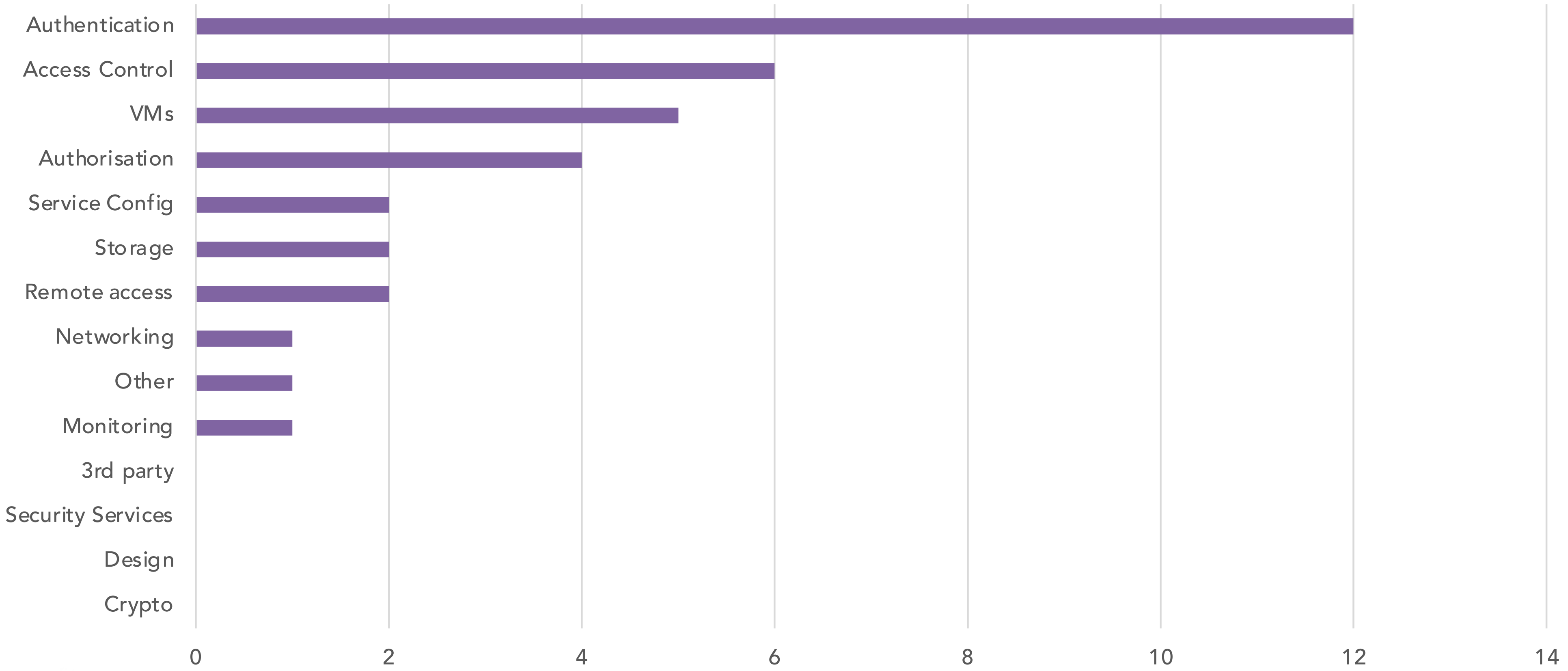
MS has had the benefit of watching and learning AWS for a first past the post mistakes

- Storage Accounts are harder to misconfigure
- Metadata Server issues are much less prevalent
- API Keys more difficult to leave lying around.
  - Depends on framework.
  - MS Tooling handles secrets better by default
- Azure RBAC is much simpler to configure
- Security Center gives tremendous visibility

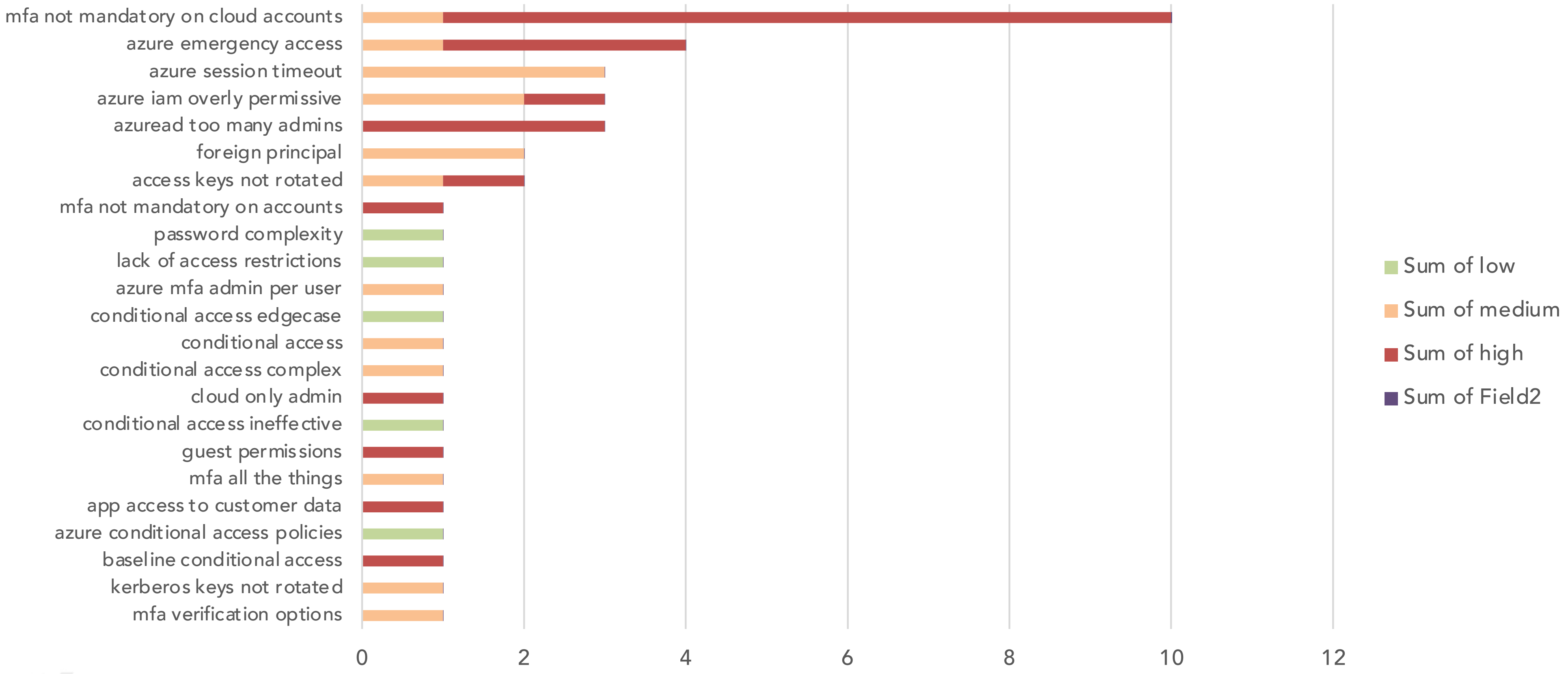
Broad trends



Breakdown of high findings



AAA major issues



Identity is the new perimeter

- AAA (authentication, authorization, access control) misconfigurations make up 22 of the 36 high findings:
  - MFA not mandatory on cloud accounts on 9 different customers.
  - Too many people have too much power in the Tenant – exists on-prem but impact is multiplied in cloud.
  - People are starting to use Conditional Access Policies but fail to protect against the unexpected

Conditional Access (a detour)

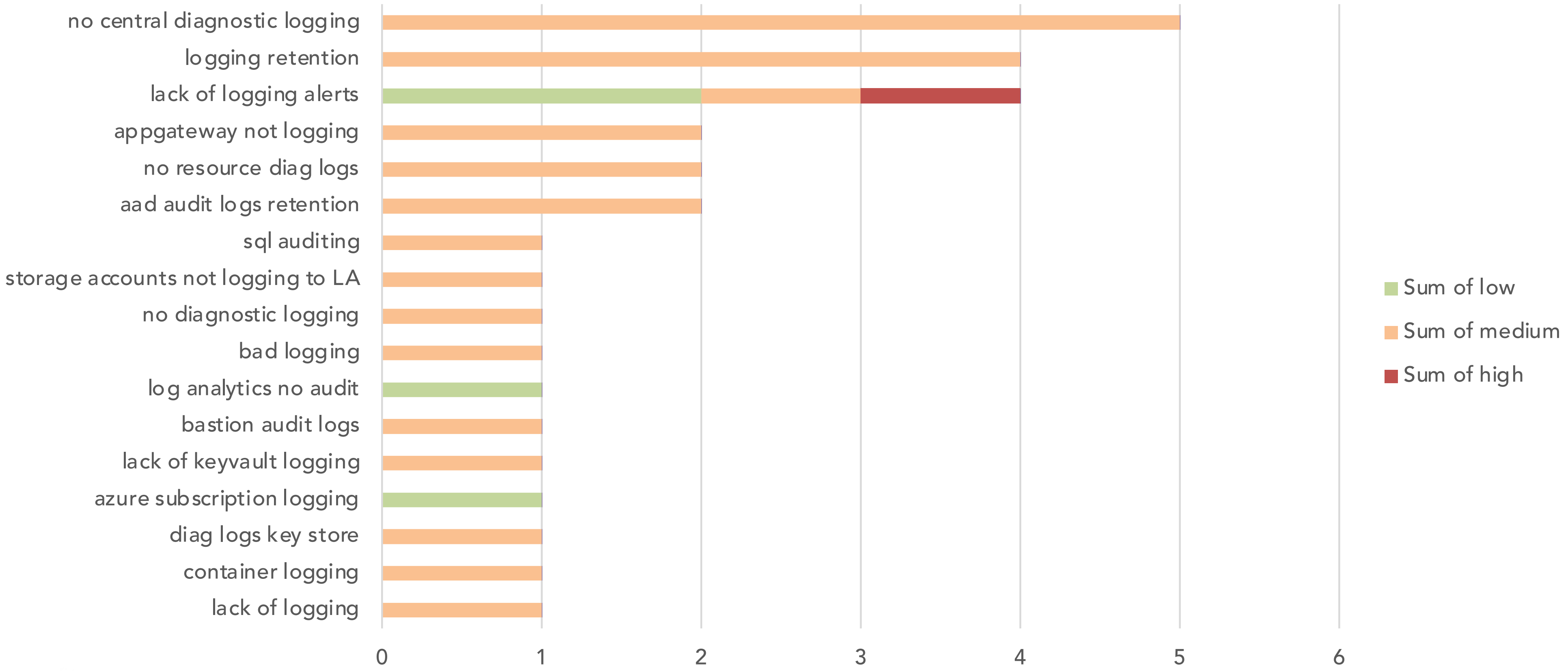
- Conditional access is:
  - Very powerful
  - Not default deny!
  - Very difficult to audit using the GUI
  - Lacking tools to help automate / audit
  - Very prone to edge cases going undetected

Why is this so important?

Customers’ biggest weakness is often their On-Premises Active Directory, which is happily syncing into Azure.

- Getting Domain Administrator access on-prem is a very common occurrence for our Internal Pen Test team
- Pivoting from on-prem to Azure once you’ve got DA is simple if there are no additional verifications (such as MFA)
- Often customers will exclude their on-prem from Conditional Access

Monitoring deep dive



Monitoring takeaways

- Default is to not log security events (no diagnostic logs)
- Retention is 30 days unless steps are taken to increase this (comes at a cost)
- Alerting must be thought through and configured
- Many services have additional security logging not enabled using the Subscription-level Diagnostic Settings

Other important findings

- Applying access control at different levels (done on the objects rather than within IAM):
  - Tenancy
  - Management Groups
  - Subscription
  - Resource Group
  - Resource
- More flexibility to split Dev / Test and Prod

Remote access

- Zero reason to expose management protocols to the internet.
- Numerous options (in order of preference)
  1. Bastion
  2. Just In Time Networking
  3. Site to Site VPN
- At the very least, limit the firewall configuration to known source Ips!

Up and coming findings…

Some new findings that, though limited in our stats, are on our radar:

- OAuth related misconfigurations allowing users to grant permissions to 3rd party apps (configurable in either M365 or Azure)
- Azure AD Sync federation abuse (made popular by Holiday Bear / "Solar Winds")
- Managed Identity / System identities
- Recommending Private Endpoint use (instead of public access)
- Kubernetes / Container host and container security issues

Azure Security Center

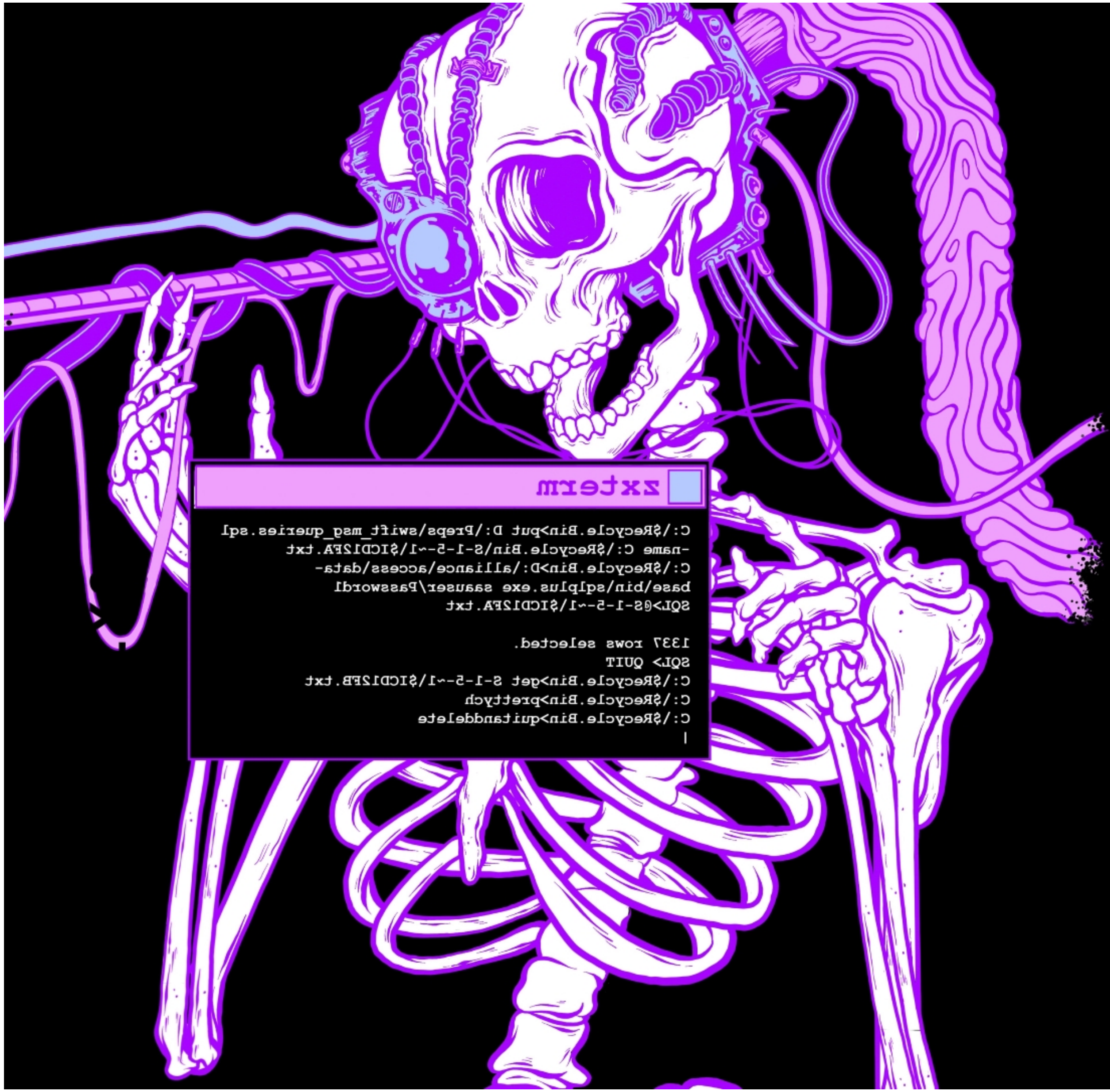
- Microsoft is currently suffering from a proliferation of admin portals.
- For Azure, the key Security portal is built into the Azure Portal, Security Center
- Why pay us to tell you what's already displayed in your tenant?
- Security Center pay as you go – you can enable Azure Defender for the subscription and not any of the resources

Free Tools

- GitHub - DanielChronlund/DCToolbox: Tools for Microsoft cloud fans – Handle Conditional Access as code, powershell scripts
- https://github.com/hausec/PowerZure - PowerShell project created to assess and exploit resources within Microsoft's cloud platform
- https://posts.specterops.io/introducing-bloodhound-4-0-the-azure-update-9b2b26c5e350 - Bloodhound, but for Azure!
- https://github.com/azure/stormspotter - graphical representation of azure environments with an eye on security

Security resources

- Azure Security Benchmarks (now up to v2, with baselines!) (MS)
  - Now has Azure Policy to automate testing
- Azure Security Best Practices and patterns (MS)
- Azure Security Podcast
- Microsoft Azure Well-Architected Framework - Security Pillar (MS)
- CIS Benchmarks
  - Azure Foundations
  - Microsoft 365 Foundations



```
C:/$Recycle.Bin>put D:/Preps/swift_msg_queries.sql
-name C:/$Recycle.Bin/S-1-5-~1/$ICD12FA.txt
C:/$Recycle.Bin>D:/alliance/access/data-
base/bin/sqlplus.exe saauser/Password1
SQL>@S-1-5-~1/$ICD12FA.txt

1337 rows selected.
SQL> QUIT
C:/$Recycle.Bin>get S-1-5-~1/$ICD12EB.txt
C:/$Recycle.Bin>prettych
C:/$Recycle.Bin>quitanddelete
|
```

LinkedIn: Blaise St-Laurent
Email: Blaise@zxsecurity.co.nz
Website: zxsecurity.co.nz