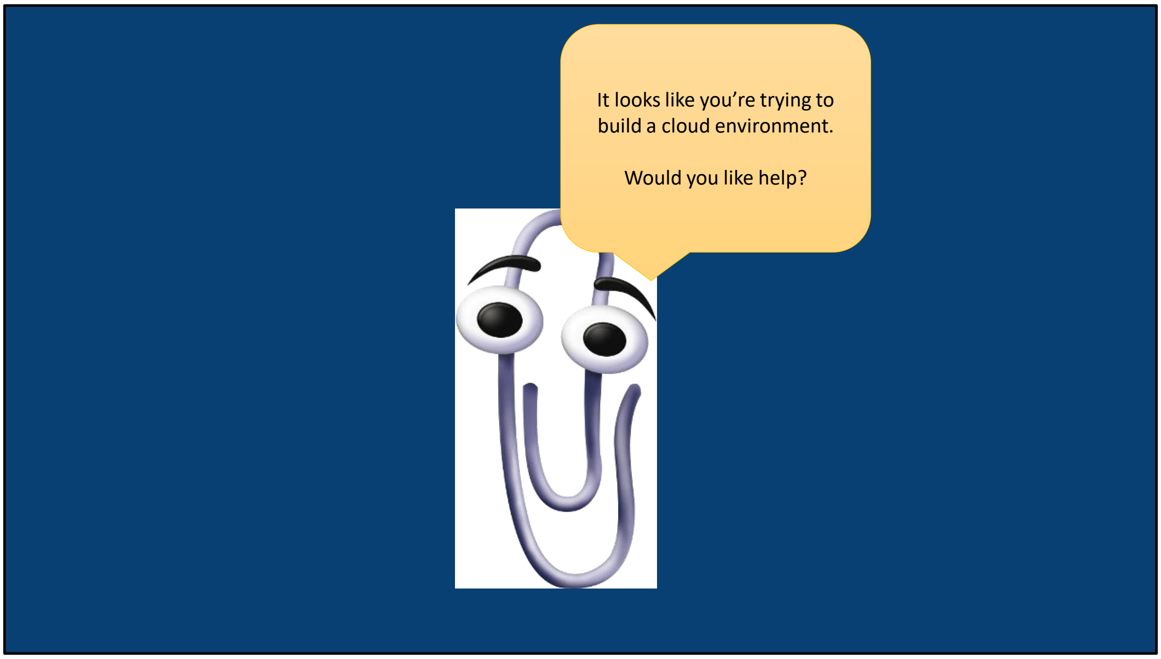
Electric Blue

Lessons from a Blue team securing Azure

Hi and Welcome to my presentation: Electric Blue – Lessons from a Blue team securing Azure

About Me

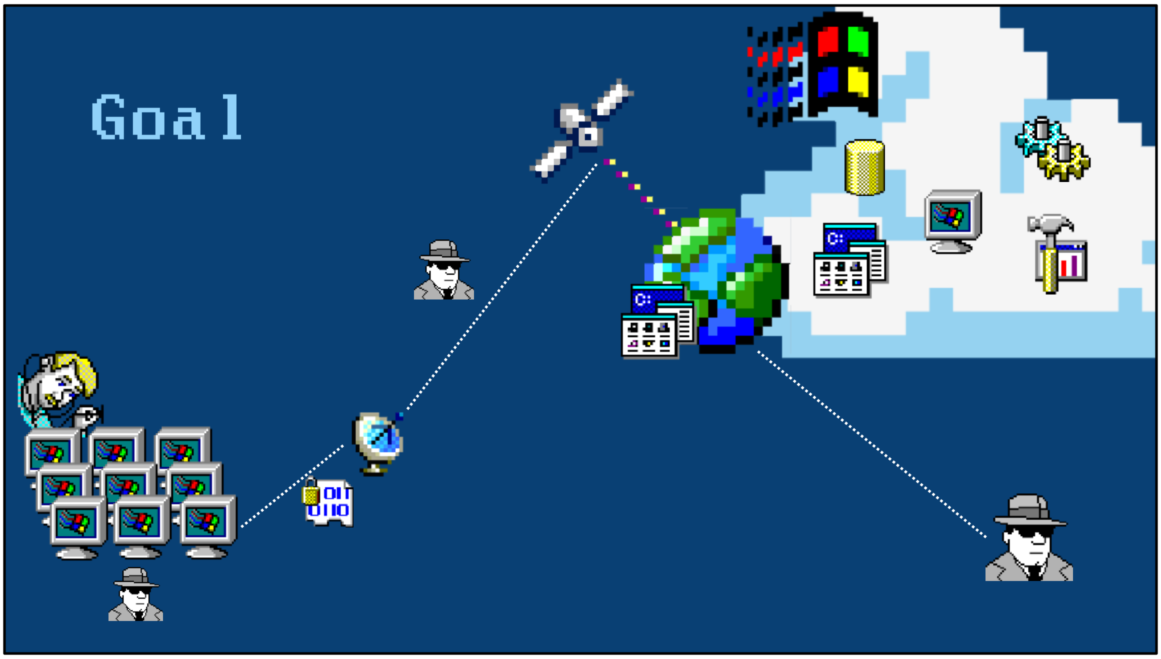
- I’m currently a Senior Security Analyst working in the SOC of a financial institution
- I’ve previously worked in IR, Red Teaming and Infrastructure Engineering for the Government
- All the opinions presented throughout this presentation are my own, and do not reflect any employer of mine, past or present.



It looks like you're trying to build a cloud environment.

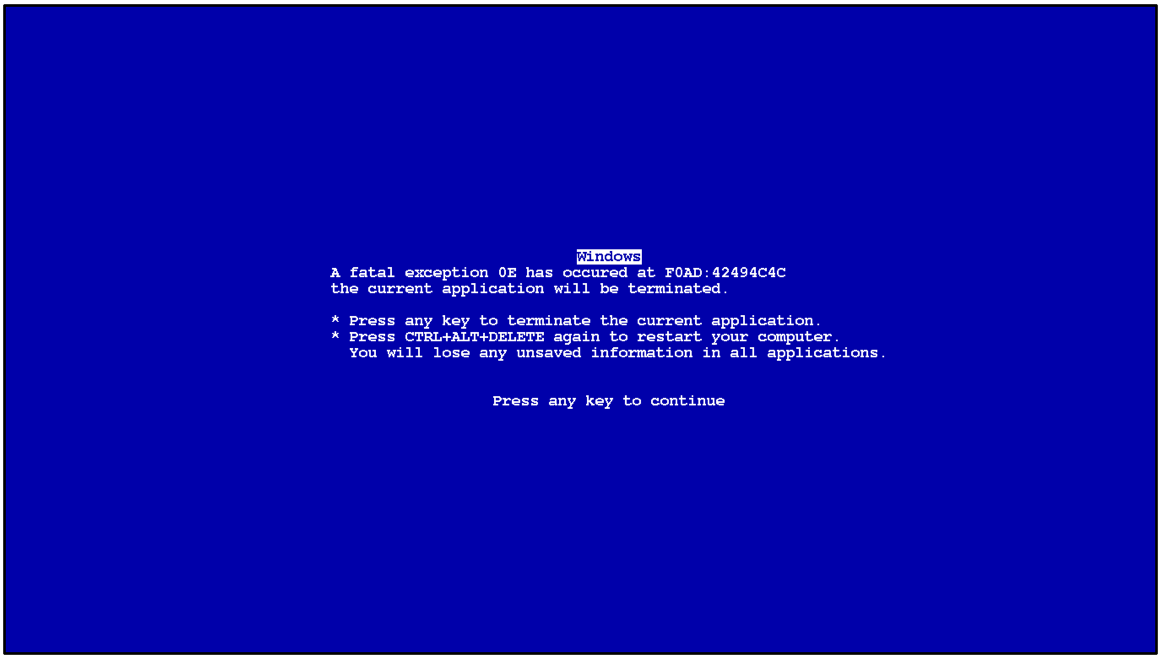
Would you like help?

- The aim of this talk is for those who are looking to build an Azure environment
    - Those that may already have one, may find some useful takeaways as well
- Going to cover some of the useful tips we wish we had of been told from the start
- Not going to be covering AAD and Office365 – lots of talks already cover these aspects



Goal

- A project was stood up to support a multi-cloud tenancy, there is a lot of reasons for this:
  - Redundancy
  - Regulation
  - Reducing Risk
  - Every cloud environment has their own advantages
- The question was asked of the SOC: what measures can we implement to ensure the platform is secure?
  - For staff users
  - For customers
  - For those managing the platform
- The SOC had its own requirements it wanted to fulfil
  - We didn’t want to have another portal we had to monitor – we wanted integration into our SIEM for active alerting
  - We wanted to set practices and conditions from the beginning to ensure good behaviour



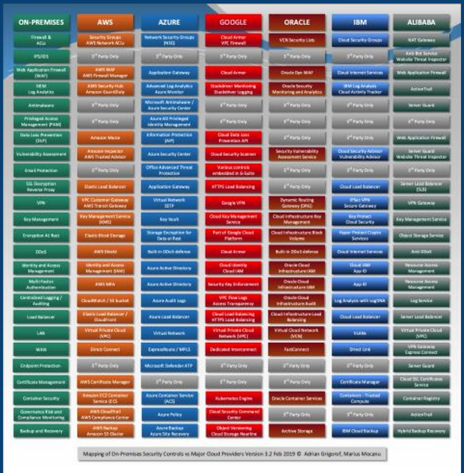
```
                          Windows
A fatal exception 0E has occured at F0AD:42494C4C
the current application will be terminated.

* Press any key to terminate the current application.
* Press CTRL+ALT+DELETE again to restart your computer.
  You will lose any unsaved information in all applications.


                 Press any key to continue
```

- The last thing we wanted was a situation where it all fell apart and ended up like this.

Terminology

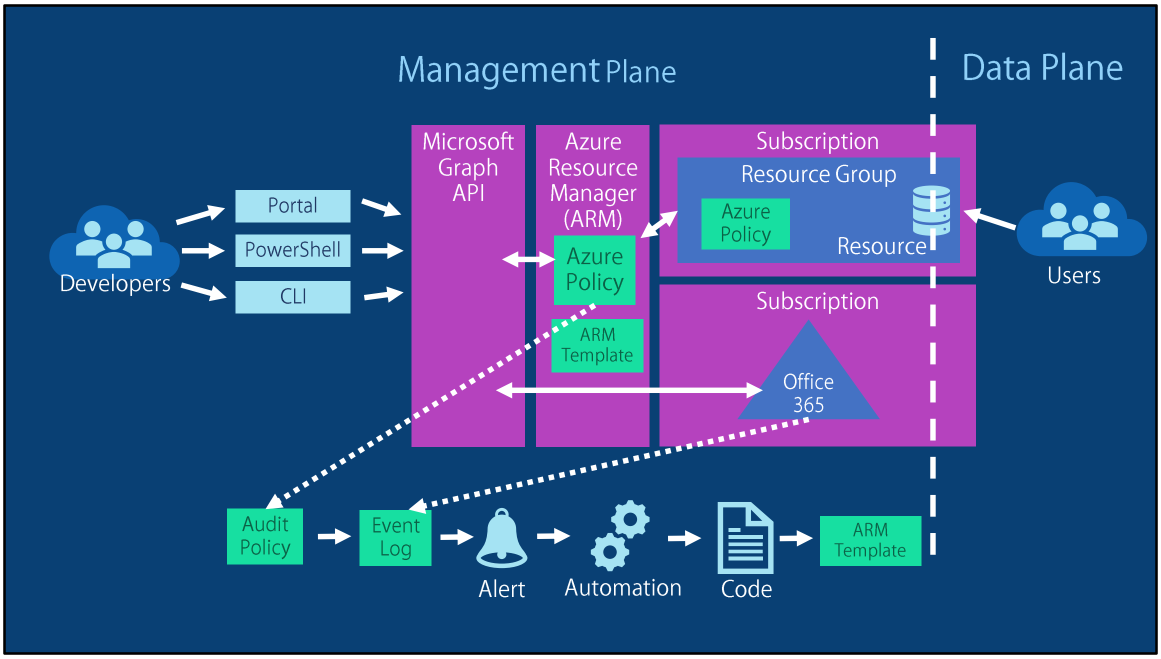


ON-PREMISES	AWS	AZURE	GOOGLE	ORACLE	IBM	ALIBABA
Firewall & ACLs	Security Groups AWS Network ACLs	Network Security Groups (NSG)	Cloud Armor VPC Firewall	VCN Security Lists	Cloud Security Groups	NAT Gateway
IPS/IDS	3rd Party Only	3rd Party Only	3rd Party Only	3rd Party Only	3rd Party Only	Anti-Bot Service Website Threat Inspector
Web Application Firewall (WAF)	AWS WAF AWS Firewall Manager	Application Gateway	Cloud Armor	Oracle Dyn WAF	Cloud Internet Services	Web Application Firewall
SIEM Log Analytics	AWS Security Hub Amazon GuardDuty	Advanced Log Analytics Azure Monitor	Stackdriver Monitoring Stackdriver Logging	Oracle Security Monitoring and Analytics	IBM Log Analysis Cloud Activity Tracker	ActionTrail
Antimalware	3rd Party Only	Microsoft Antimalware / Azure Security Center	3rd Party Only	3rd Party Only	3rd Party Only	Server Guard
Privileged Access Management (PAM)	3rd Party Only	Azure AD Privileged Identity Management	3rd Party Only	3rd Party Only	3rd Party Only	3rd Party Only
Data Loss Prevention (DLP)	Amazon Macie	Information Protection (AIP)	Cloud Data Loss Prevention API	3rd Party Only	3rd Party Only	Web Application Firewall
Vulnerability Assessment	Amazon Inspector AWS Trusted Advisor	Azure Security Center	Cloud Security Scanner	Security Vulnerability Assessment Service	Cloud Security Advisor Vulnerability Advisor	Server Guard Website Threat Inspector
Email Protection	3rd Party Only	Office Advanced Threat Protection	Various controls embedded in G-Suite	3rd Party Only	3rd Party Only	3rd Party Only
SSL Decryption Reverse Proxy	Elastic Load Balancer	Application Gateway	HTTPS Load Balancing	3rd Party Only	Cloud Load Balancer	Server Load Balancer (SLB)
VPN	VPC Customer Gateway AWS Transit Gateway	Virtual Network SSTP	Google VPN	Dynamic Routing Gateway (DRG)	IPSec VPN Secure Gateway	VPN Gateway
Key Management	Key Management Service (KMS)	Key Vault	Cloud Key Management Service	Cloud Infrastructure Key Management	Key Protect Cloud Security	Key Management Service
Encryption At Rest	Elastic Block Storage	Storage Encryption for Data at Rest	Part of Google Cloud Platform	Cloud Infrastructure Block Volume	Hyper Protect Crypto Services	Object Storage Service
DDoS	AWS Shield	Built-in DDoS defense	Cloud Armor	Built-in DDoS defense	Cloud Internet Services	Anti-DDoS
Identity and Access Management	Identity and Access Management (IAM)	Azure Active Directory	Cloud Identity Cloud IAM	Oracle Cloud Infrastructure IAM	Cloud IAM App ID	Resource Access Management
Multi-Factor Authentication	AWS MFA	Azure Active Directory	Security Key Enforcement	Oracle Cloud Infrastructure IAM	App ID	Resource Access Management
Centralized Logging / Auditing	CloudWatch / S3 bucket	Azure Audit Logs	VPC Flow Logs Access Transparency	Oracle Cloud Infrastructure Audit	Log Analysis with LogDNA	Log Service
Load Balancer	Elastic Load Balancer / CloudFront	Azure Load Balancer	Cloud Load Balancing HTTPS Load Balancing	Cloud Infrastructure Load Balancing	Cloud Load Balancer	Server Load Balancer
LAN	Virtual Private Cloud (VPC)	Virtual Network	Virtual Private Cloud Network (VPC)	Virtual Cloud Network (VCN)	VLANs	Virtual Private Cloud (VPC)
WAN	Direct Connect	ExpressRoute / MPLS	Dedicated Interconnect	FastConnect	Direct Link	VPN Gateway Express Connect
Endpoint Protection	3rd Party Only	Microsoft Defender ATP	3rd Party Only	3rd Party Only	3rd Party Only	Server Guard
Certificate Management	AWS Certificate Manager	3rd Party Only	3rd Party Only	3rd Party Only	Certificate Manager	Cloud SSL Certificates Service
Container Security	Amazon EC2 Container Service (ECS)	Azure Container Service (ACS)	Kubernetes Engine	Oracle Container Services	Containers - Trusted Compute	Container Registry
Governance Risk and Compliance Monitoring	AWS CloudTrail AWS Compliance Center	Azure Policy	Cloud Security Command Center	3rd Party Only	3rd Party Only	ActionTrail
Backup and Recovery	AWS Backup Amazon S3 Glacier	Azure Backup Azure Site Recovery	Object Versioning Cloud Storage Nearline	Archive Storage	IBM Cloud Backup	Hybrid Backup Recovery

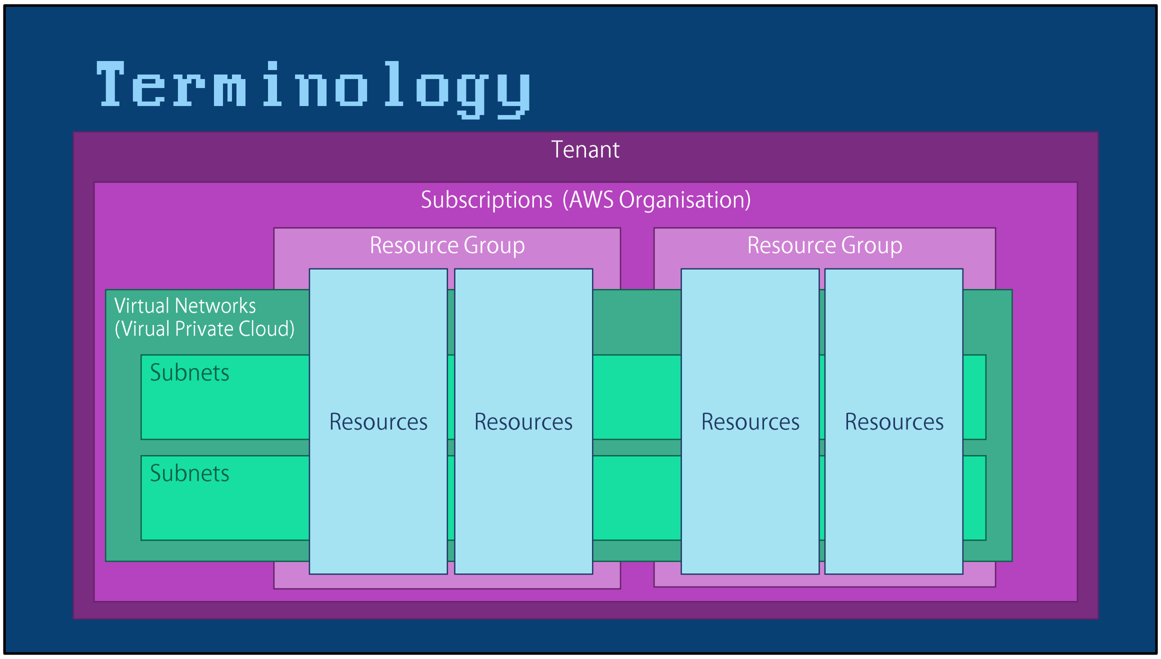
Mapping of On-Premises Security Controls vs Major Cloud Providers Version 3.2 Feb 2019 © Adrian Grigorof, Marius Mocanu

http://www.eventid.net/docs/onprem_to_cloud.asp

- For those of you that are new, or haven't seen it before, Adrian Grigorof and Marius Mocanu from EventID.net have a fantastic terminology mapper between platforms



- So what does the Azure cloud look like?
- You use either the portal, powershell or CLI to connect to the Microsoft Graph API
- The Microsoft Graph API authenticates you to Azure AD, and Office365
- Once authenticated, whichever action you undertake talks to Azure Resource Manager (ARM)
- The action you go to take compares against the current Global Azure policy to determine if you're permitted
- Azure Policy can also be applied at the Resource Group level
- If you try and do something that is against the Azure Policy it triggers the Audit Policy
- All actions that have defied the Azure Policy will automatically get logged to the event log
- All ALTER/DELETE/CREATE events are logged to the Event log by default
- You can then get this to trigger an alert, execute an azure automation, which in turn can execute some code, or deploy an ARM template.
- ARM Templates are a JSON representation of an Azure resource.
- This means you can deploy things like a Network Security Group (NSG – Azure Firewall) to a resource after an alert.



Terminology

Tenant

Subscriptions (AWS Organisation)

Resource Group

Resource Group

Virtual Networks
(Virual Private Cloud)

Subnets

Subnets

Resources

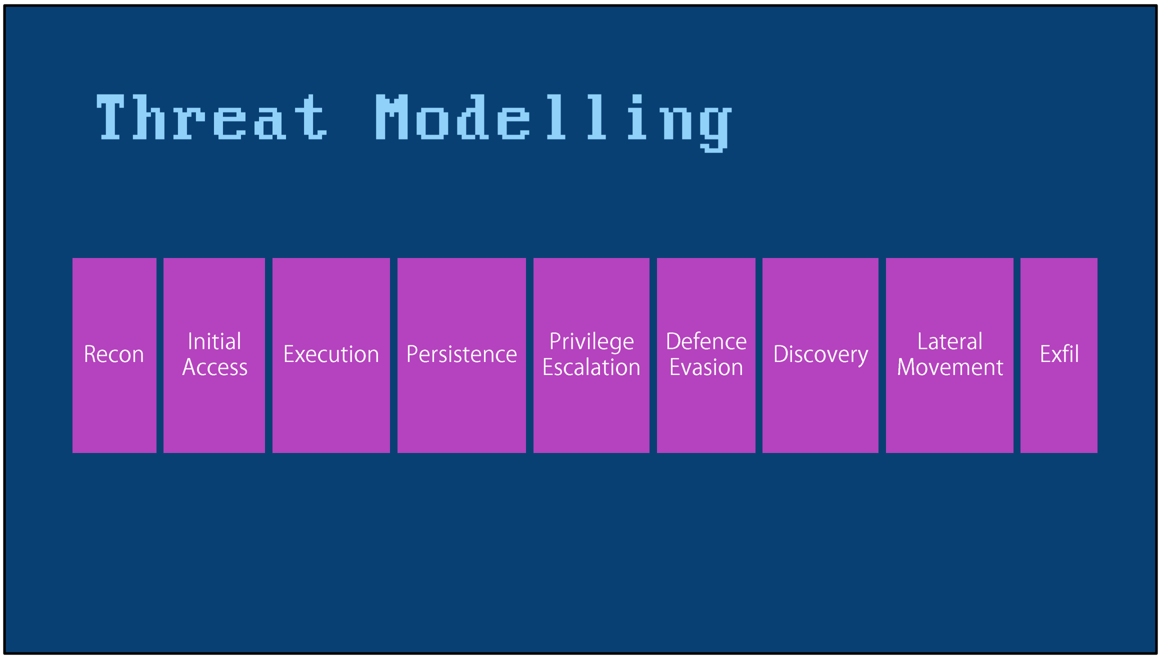
Resources

Resources

Resources

- Azure consists of Tenants, Subscriptions, Resource Groups and Resources
- I’ve put the equivalent AWS terms there for those more versed in that.
- Microsoft have a handy website that literally translates AWS terms to Azure
- A resource group is just a logical grouping of many resources
- Storage
  - Managed Disks
  - File/Blob/Queue/Table
  - DataPool
- Compute
  - Linux/Windows
  - PaaS Services – such as SQL
  - Azure Functions
  - LogicApps
- Logs
  - Azure Security Center
  - Azure Operations Management Suite
  - Azure Sentinel (NEW)
- Network
  - ExpressRoute – Virtual Private Networks

  - Vnets – Virtual Networks (typically one for a subscription, but can have more)
  - Subnets – Logical Addressing for Vnets (there’s no real concept of DHCP)
  - NetworkWatcher
- Plus a bunch of Machine Learning/AI/Containers/Azure DevOps/AAD/Hybrid Services



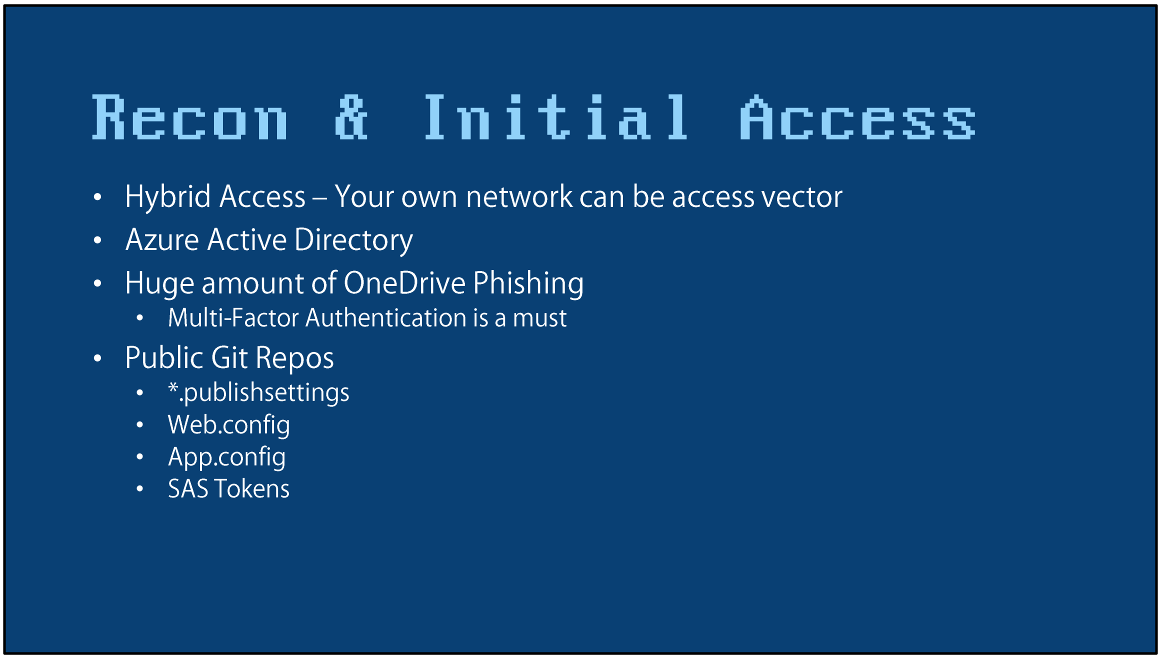
Threat Modelling

Recon | Initial Access | Execution | Persistence | Privilege Escalation | Defence Evasion | Discovery | Lateral Movement | Exfil

- Obviously, to understand some of the threats you need to undertake some threat modelling
- This means understanding how different parties are going to be using the cloud, and what resources they’ll use
- From this we can then focus on techniques, detections and controls
- Microsoft uses the STRIDE model (Spoofing, Tampering, Repudiation, Information Disclousure, Denial of Service and Elevation of Privileges)
- The MITRE ATT&CK model is more common in the industry
  - Not a one-to-one for cloud systems, so needed to understand what techniques are missing to fill in the gaps
- The important thing we learned is that these cloud systems are continuously evolving, which means we constantly need to threat model

Identity is King

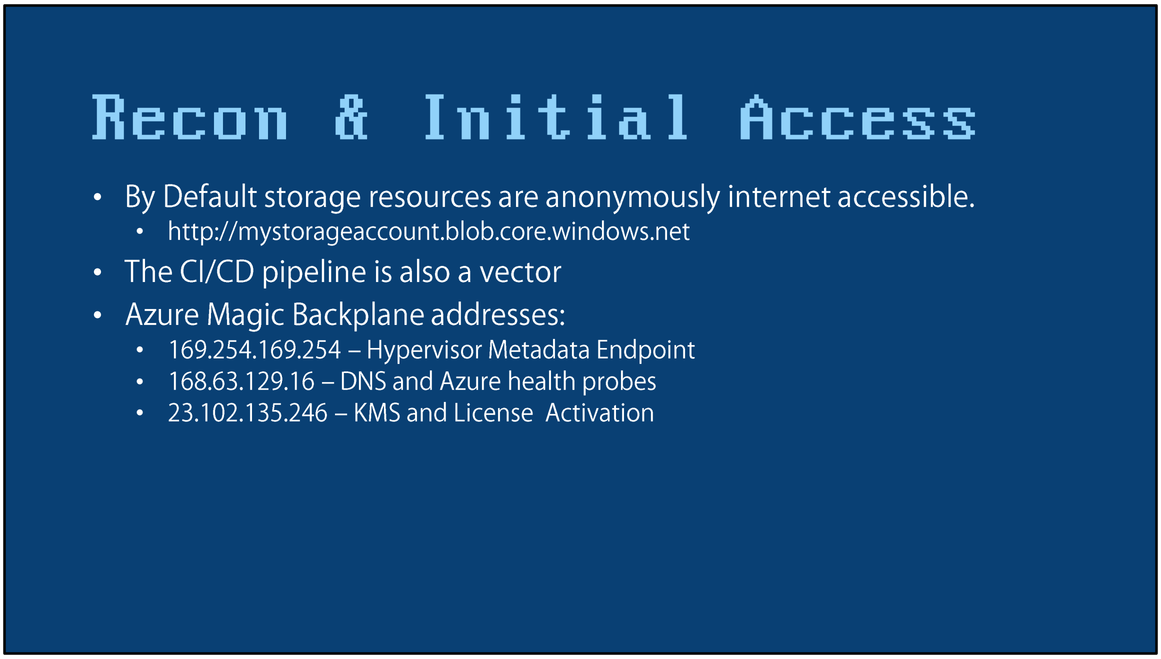
- If there's one thing to take away it's this
- As organisations mature they're transitioning to a identity aware security model
- It became obvious very quickly that there are a multitude of different ways to authenticate
- No matter the method, once a user has authenticated, they have the capabilities their permissions have let out.
- We have to remember we're not talking about normal users here, but a management plane with the ability to control potentially critical resources in a resource group
- ARM Details everything in Activity Logs – relating back to a user identifier
- But was there a way to determine if a user account has been compromised from their activity?
- From a Microsoft perspective, it was already game over when the credentials were obtained.
- This lead to the follow up question: what could an attacker do with a compromised account, and what can a defender do to protect against it?



Recon & Initial Access

- Hybrid Access – Your own network can be access vector
- Azure Active Directory
- Huge amount of OneDrive Phishing
  - Multi-Factor Authentication is a must
- Public Git Repos
  - *.publishsettings
  - Web.config
  - App.config
  - SAS Tokens

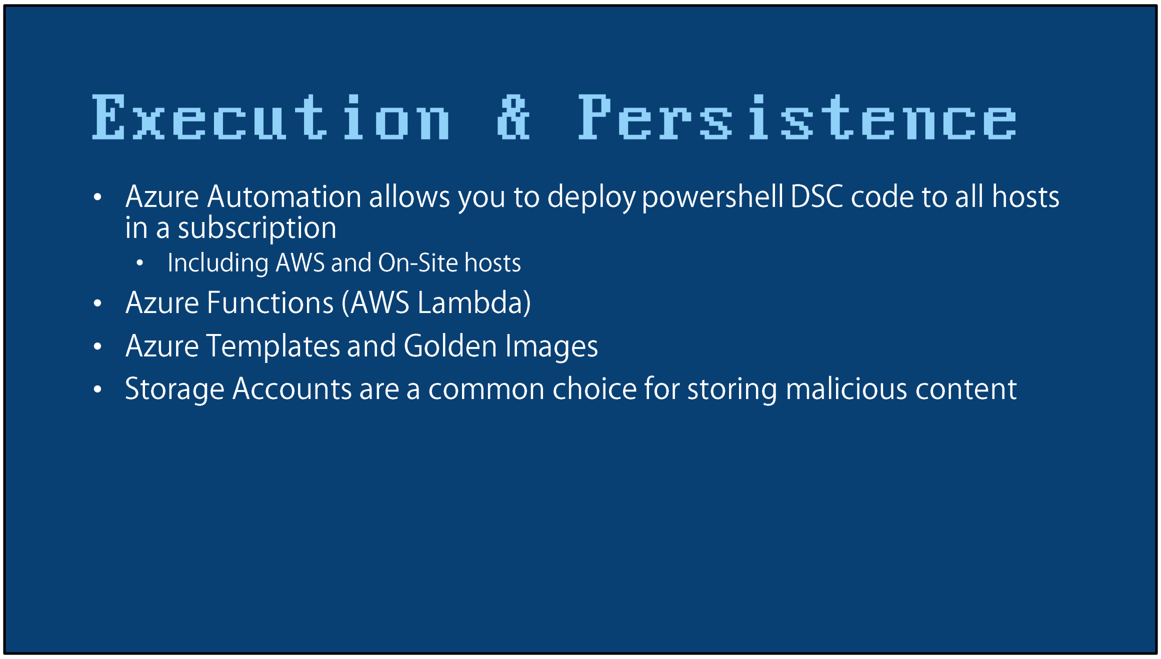
- No one can dispute that there are many ways to authenticate
  - Not as simple as just enabling multi-factor authentication – although would be foolish not to enable it!
  - SAS tokens, and different settings files all can contain keys that grant access
  - Comes back to securing your cloud environment is one small part of securing your CI/CD pipeline.
- Once you're authenticated, you're limited to the RBAC permissions that have been allocated – it's critical to ensure that these are as limited to the needs as possible.
- Do users legitimately need the permission to create/alter/delete every possible component?
- Huge amount of phishing around OneDrive/Office365 – all linked with AAD, which means possibility of pivoting in.
  - Be aware that if you've enabled MFA on an account, and they haven't logged in to set it up, then MFA isn't fully enabled.



Recon & Initial Access

- By Default storage resources are anonymously internet accessible.
  - http://mystorageaccount.blob.core.windows.net
- The CI/CD pipeline is also a vector
- Azure Magic Backplane addresses:
  - 169.254.169.254 – Hypervisor Metadata Endpoint
  - 168.63.129.16 – DNS and Azure health probes
  - 23.102.135.246 – KMS and License Activation

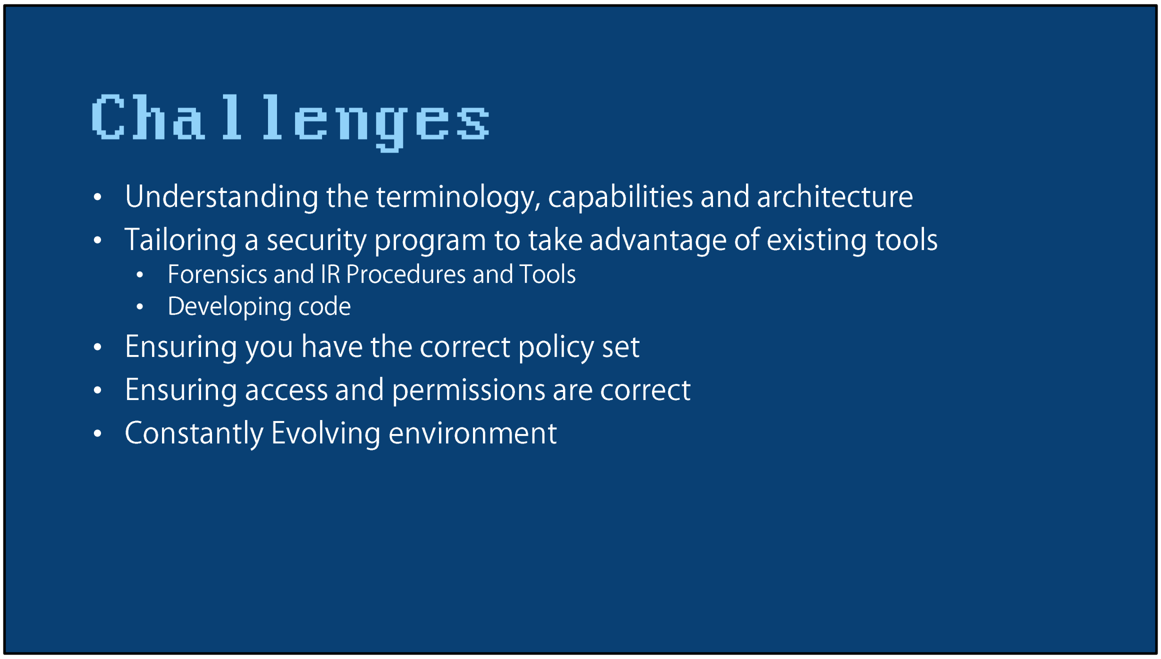
- Storage Accounts are anonymously accessible – great way to find information
- Storage Accounts have a minimum of 8 characters and maximum of 24 characters for a name
- Considering the code integration/code delivery pipeline is literally executing code, it’s a huge vector
- The azure magic backplane allows for querying/signalling to the Azure hypervisor
  - This includes letting Azure know the host is active
  - Querying the Azure DNS server (unless a custom DNS is specified)
  - Health probes to Azure Load Balancers



Execution & Persistence

- Azure Automation allows you to deploy powershell DSC code to all hosts in a subscription
  - Including AWS and On-Site hosts
- Azure Functions (AWS Lambda)
- Azure Templates and Golden Images
- Storage Accounts are a common choice for storing malicious content

- Azure ‘Run As Account’ – creates an Azure AD application with a service principal account,
- Azure automation allows you to run python or powershell scripts from a known repo
- But it’s very easy to add your own to this repo
- Assigned contributor role for the subscription (although this can be changed) – allows full access
- Azure Functions are the Azure equivalent to lambda
- There are existing templates and golden images, can create your own managed image
- Storage accounts can store content in 4 different ways – as blobs, files, tables and queues

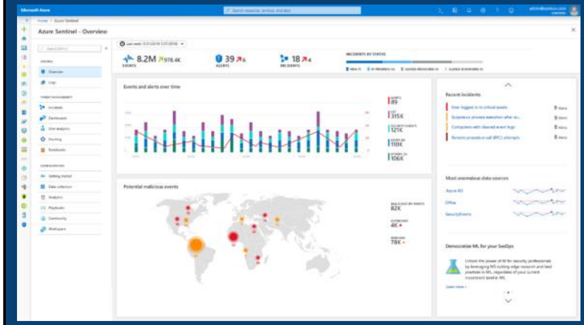


Challenges

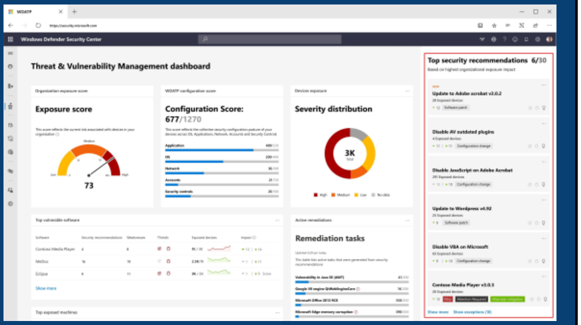
- Understanding the terminology, capabilities and architecture
- Tailoring a security program to take advantage of existing tools
    - Forensics and IR Procedures and Tools
    - Developing code
- Ensuring you have the correct policy set
- Ensuring access and permissions are correct
- Constantly Evolving environment

- There's a fair few challenges to be aware of before you begin
- Obviously you have existing tools, methods and procedures – need to integrate the Azure environment into what have
    - This means it's not too drastic a change to your existing methods
- Keep in mind that you may not have access to the console (especially in the case where it's serverless applications)
    - Microsoft can support you, but you need to understand what they can offer in the support contract
- IAM/RBAC is critical – need to make sure it's to your needs and identify key risk accounts
- The environment is constantly changing – hosts come up and down all the time, new code is deployed often, and Microsoft introduce features often.
- Different licenses will limit your features that you can use. E5 unlocks every feature, E3 loses access to a lot of security functionality.

Constantly Evolving

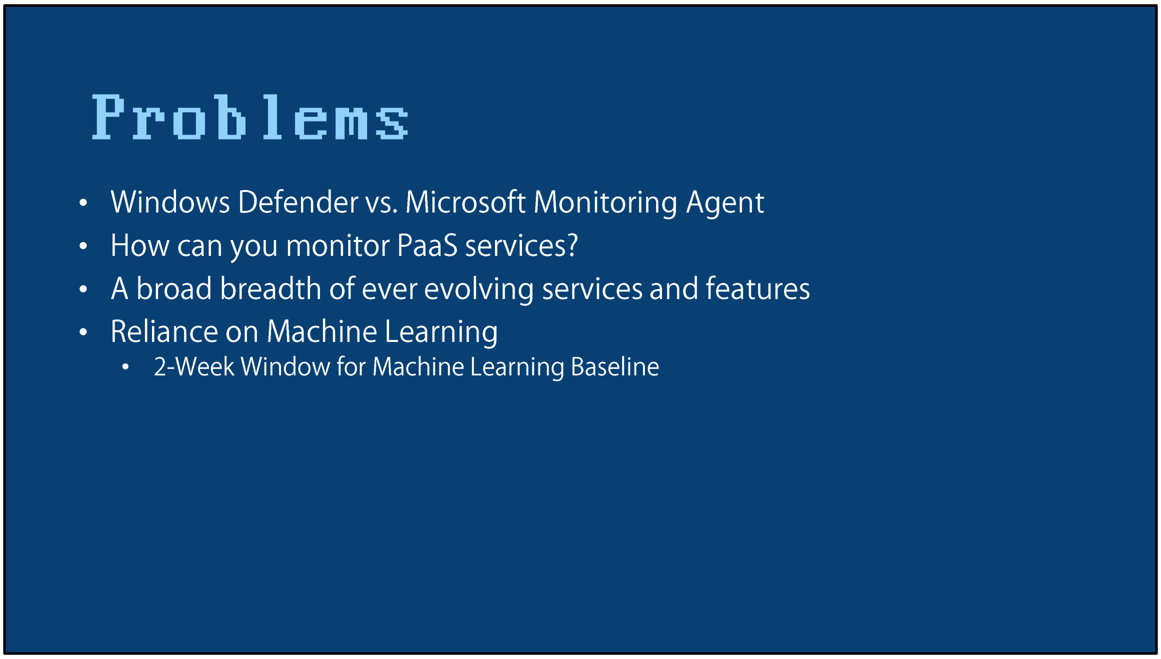

Azure Sentinel - Overview
8.2M
39
18
Events and alerts over time
Potential malicious events
Recent incidents

Azure Sentinel


Windows Defender Security Center
Threat & Vulnerability Management dashboard
Exposure score
73
Configuration Score:
677/1270
Severity distribution
3K
Top security recommendations 6/30
Remediation tasks

Azure ATP – Threat and Vulnerability

- Azure is a constantly evolving environment, there are large changes that take place often
- Above are two of the biggest announcements – Azure Sentinel and Threat and Vulnerability assessments for ATP
- This means you need to be constantly monitoring for changes
- This could introduce new avenues for exploitation, or better ways for current monitoring and protection
- There’s a huge battle in making sure that staff are kept up to date on the changes



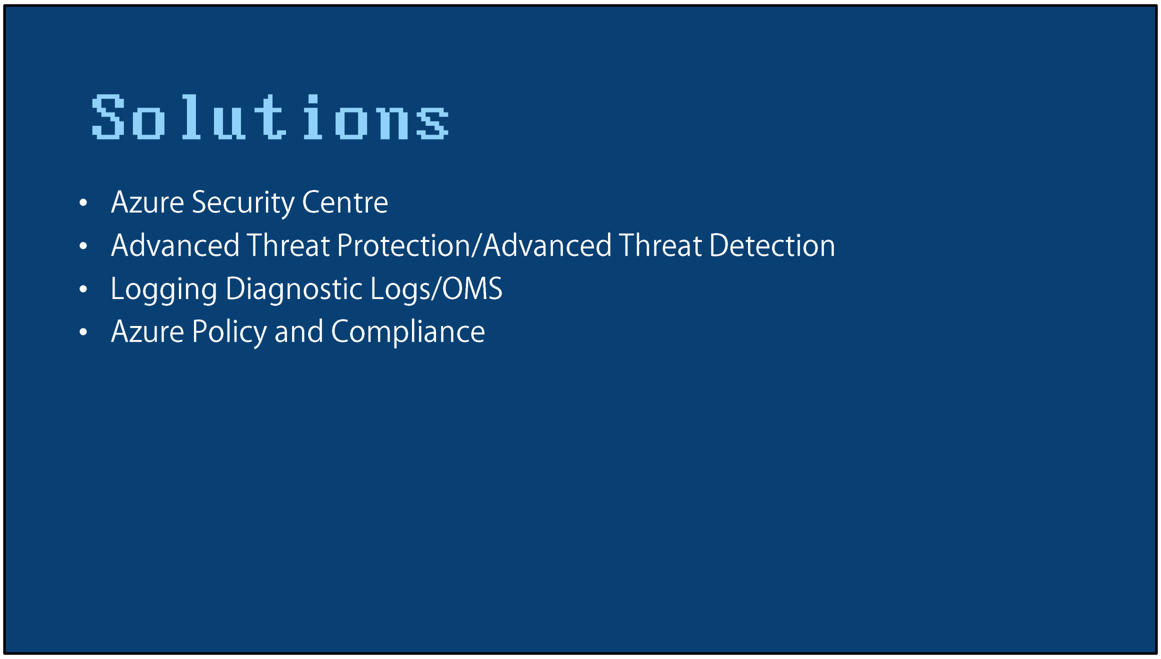
Problems

- Windows Defender vs. Microsoft Monitoring Agent
- How can you monitor PaaS services?
- A broad breadth of ever evolving services and features
- Reliance on Machine Learning
  - 2-Week Window for Machine Learning Baseline

- Like all things, there are gaps – it just means having further controls to overlap and cover them.
- At the end of the day we treat everything with zero trust – including the Microsoft Platform, and our users.
- Microsoft relies heavily on machine learning for all of it's alerts – there's no real signature based methods
  - This is the case with the Advanced Threat Protection agent, or the PaaS services protection
  - There's a two week window to build the baseline that's used
  - If this baseline includes malicious behaviour, it'll whitelist it automatically
- There's a priority for alerting as well. Microsoft Monitoring Agent is required to feed alerts from the system into Azure Security Centre
- Security alerts that occur on a host will go to Windows Defender, and windows System Centre Configuration Manager (SCCM) if configured from there.
- If this happens, it means that it won't feed into Microsoft Monitoring Agent and Azure Security Centre
- Any alerts that do make it past Windows Defender will make it to Azure

Security Centre, and will be low fidelity, and more than likely a false positive.

- Traditional EDR products won't work for Platform as a Service (PaaS), so you will need to think about what security measures can be introduced into the CI/CD lifecycle.
  - How can you ensure that the repos you use are legitimate (Artifactory/Private Repos)
  - How can you ensure that's being pushed is legitimate?
  - How can you ensure that the scripts to create resources haven't been altered maliciously?
  - Is your Jenkins server literally hosted on Azure?

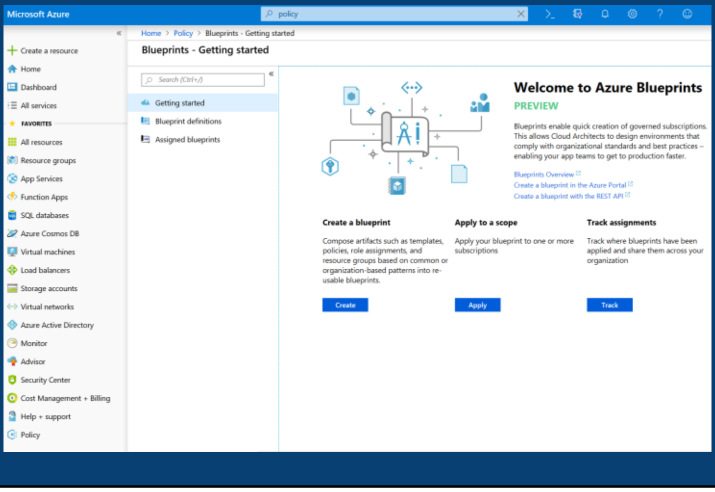


Solutions

- Azure Security Centre
- Advanced Threat Protection/Advanced Threat Detection
- Logging Diagnostic Logs/OMS
- Azure Policy and Compliance

- Azure Security Centre – Machine Learning based system, although it'll only be as good as the data it gets.
- Azure Security Centre is your first point for security incidents.
- May need to develop solutions to fill gaps
- Definitely need to consider your architecture when designing it.
- Need to update architecture constantly as things change.
- Lots of Opportunities to develop new security capabilities and experiment – including deception technologies.
- If you've purchased the E5 license, you can leverage even more features such as Just in Time computing, and Privileged Identity Management

Policy



Blueprints - Getting started

Welcome to Azure Blueprints

PREVIEW

Blueprints enable quick creation of governed subscriptions. This allows Cloud Architects to design environments that comply with organizational standards and best practices – enabling your app teams to get to production faster.

Create a blueprint

Compose artifacts such as templates, policies, role assignments, and resource groups based on common or organization-based patterns into re-usable blueprints.

Apply to a scope

Apply your blueprint to one or more subscriptions

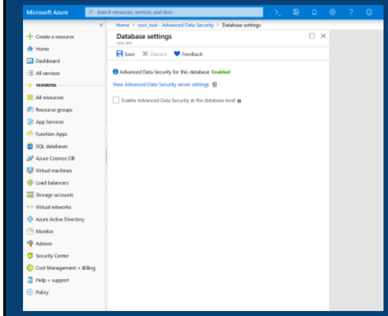
Track assignments

Track where blueprints have been applied and share them across your organization

- I haven’t really covered policy so far, but it’s critical to Azure
- It’s like group policy for Azure
- A policy definition checks what to evaluate, and what action to undertake
- It can be applied to a multitude of resources
- An initiative is a collection of policies
- Just because a new policy has been created doesn’t mean it has been applied.
- Compliance reflects how many resources have currently implemented a policy.
- You may need to redeploy a resource for the policy to be applied
- Blueprints make deployment of all of this incredibly easy

ATP/ATD

- Advanced Threat Protection/Advanced Threat Detection for PaaS



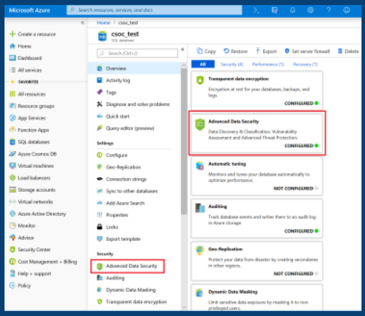
Database settings

csoc_test

Advanced Data Security for this database: Enabled

View Advanced Data Security server settings

□ Enable Advanced Data Security at the database level



csoc_test

SQL database

Transparent data encryption
Encryption at rest for your databases, backups, and logs.
CONFIGURED ●

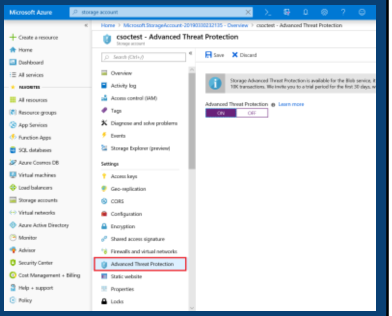
Advanced Data Security
Data Discovery & Classification, Vulnerability Assessment and Advanced Threat Protection.
CONFIGURED ●

Automatic tuning
Monitors and tunes your database automatically to optimize performance.
NOT CONFIGURED ○

Auditing
Track database events and writes them to an audit log in Azure storage.
CONFIGURED ●

Geo Replication
Protect your data from disaster by creating secondaries in other regions.
NOT CONFIGURED ○

Dynamic Data Masking
Limit sensitive data exposure by masking it to non-privileged users.



csoctest - Advanced Threat Protection

Storage account

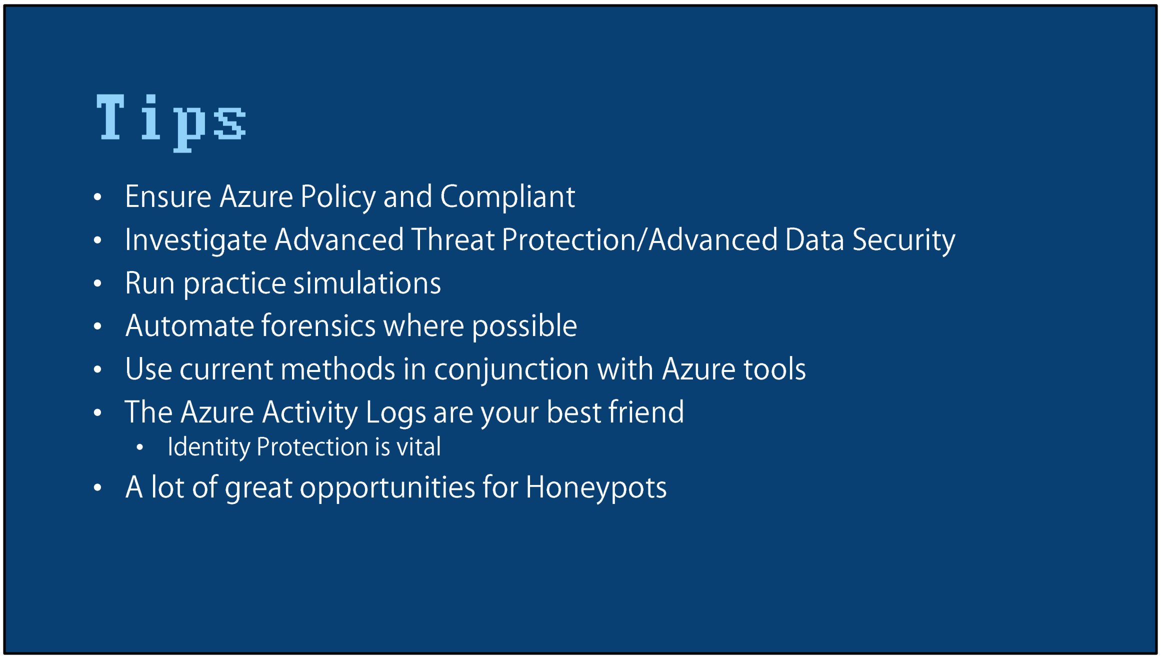
Storage Advanced Threat Protection is available for the Blob service, i
10K transactions. We invite you to a trial period for the first 30 days, w

Advanced Threat Protection Learn more

[✓ ON] OFF

- The naming convention is an utter confusion. Currently everything has been labelled Advanced Threat Prevention
- Advanced Threat Prevention refers to a Microsoft Developed EDR solution that solely uses machine learning
- Some of the PaaS services are switching to Advanced Threat Detection to differentiate between the endpoint agent and the security options, but not all have gotten there yet, so you may see references to Advanced Threat Prevention.
- Advanced Threat Detection (PaaS services) – feeds into Azure Security Centre, but needs to be enabled
- It’s currently only available to SQL PaaS services and blob component of storage accounts
    - For SQL PaaS services it alerts on SQL injection attempts (the SQL databases are directly internet accessible remember)
    - The Blob Storage alerts relate to suspicious access to the storage blob (such as unusual access attempts), not the storage of malicious files.
- Has a minimum two week window to establish the benchmark.
- Also has a small cost to them – be aware of this

- The Advanced Threat Prevention EDR agent can only be deployed if you have an E5 license
- Check out the tab in the menu.



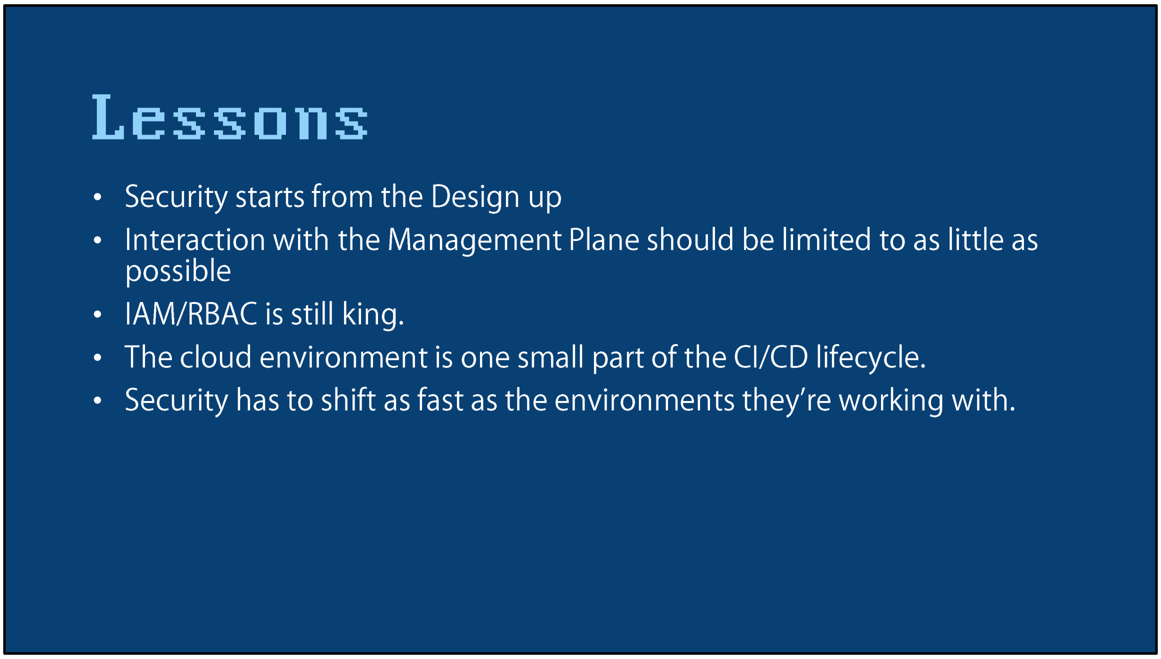
Tips

- Ensure Azure Policy and Compliant
- Investigate Advanced Threat Protection/Advanced Data Security
- Run practice simulations
- Automate forensics where possible
- Use current methods in conjunction with Azure tools
- The Azure Activity Logs are your best friend
  - Identity Protection is vital
- A lot of great opportunities for Honeypots

- Some general tips and recommendations for you all
- Don’t just create Azure Policy, ensure all your resources are compliant and that it’s being applied.
- Policy changes all the time, make sure it’s still meeting your needs
- For PaaS services Microsoft are deploying Advanced Threat Protection or Advanced Data Security – they have a cost, but they can generate alerts into Azure Security Centre
- Run drills, ensure that your current methods are applicable
- This includes calling Microsoft Support to ensure that what their capabilities are, and their timeframes are well known
- Some forensic techniques may be against terms and conditions (procdumping memory for instance)
- Develop code to make life easier for yourself
- Make use of what you currently have in your environment, but leverage Azure tools where it assists.
- The Azure activity logs are for all control plane events. They will give you information about every resource created, modified, or deleted by a user (no read though)
- Azure AD logs will give great information about logins as well – including location,

MFA and more.

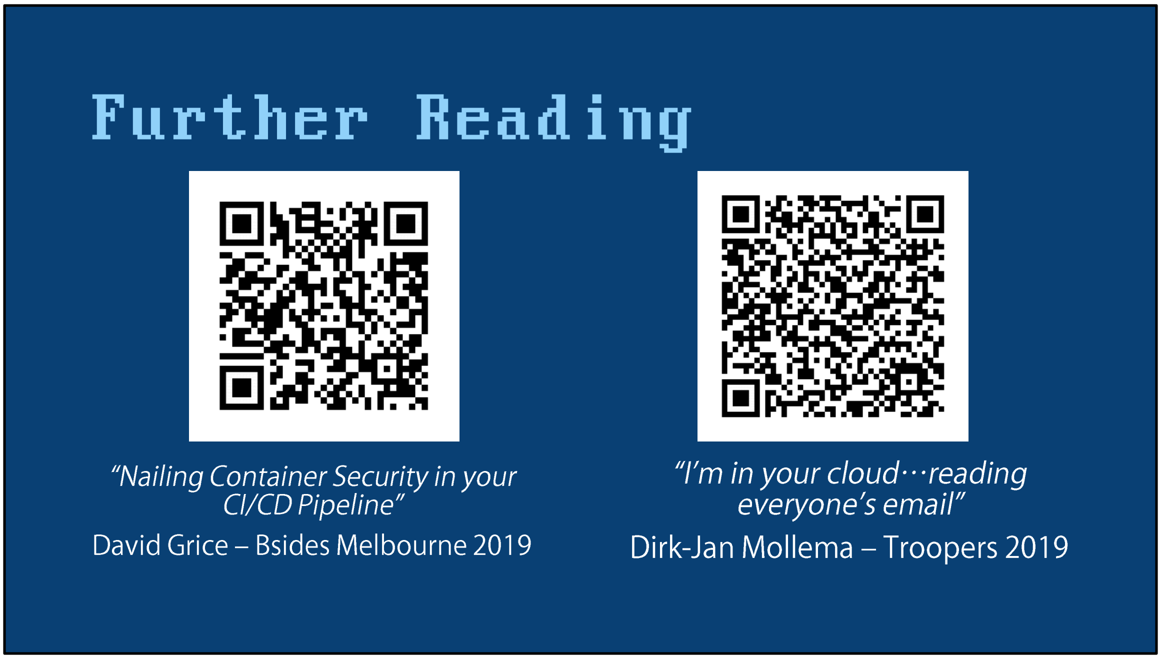
- The environment is perfect for someone wanting to set up honeytraps.



Lessons

- Security starts from the Design up
- Interaction with the Management Plane should be limited to as little as possible
- IAM/RBAC is still king.
- The cloud environment is one small part of the CI/CD lifecycle.
- Security has to shift as fast as the environments they're working with.

- Security needs to be designed from the ground up, the architecture is critical to limiting the scope and ensuring that only the required resources are accessible.
- Remember this is a management interface, literally to control infrastructure in your network.
- Security needs to learn to start implementing some of the DevOps/Agile practices to move as fast as the environment they're trying to secure.



Further Reading

"Nailing Container Security in your CI/CD Pipeline"

David Grice – Bsides Melbourne 2019

"I'm in your cloud…reading everyone's email"

Dirk-Jan Mollema – Troopers 2019

Some amazing talks that have covered different parts of Cloud environments. The Microsoft document is a labyrinth of great information – but it's hidden in there.

Questions

I just want to give a shout out to others who’ve presented at other cons, you’ve paved the way and made it look easy