



Storebrand

Invester i fremtiden



Who am I

**Lead Security Architect @
Storebrand**

Education

Master of Science in
Information Security

Consultant

10+ Years as
consultant

MSUG

Part of Microsoft
Security User Group
Organizers

Hobbies

Gaming in winter and
disc golf during
summer

Security MVP





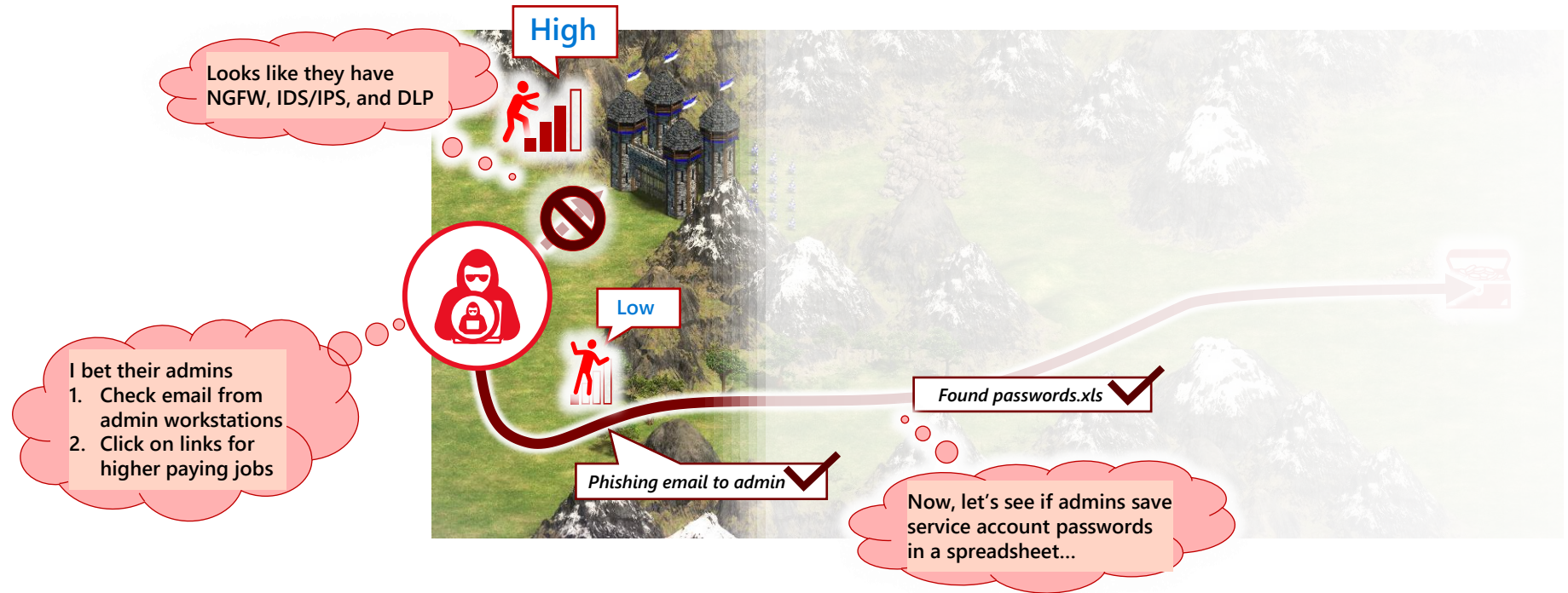
Agenda

- Misconceptions and anti patterns.
- Skillsets in cybersecurity space
- Demo – MFA
- Demo – Azure Apps/Resources
- Infrastructure as code
- Demo – IAC (if time)
- Questions and Answers



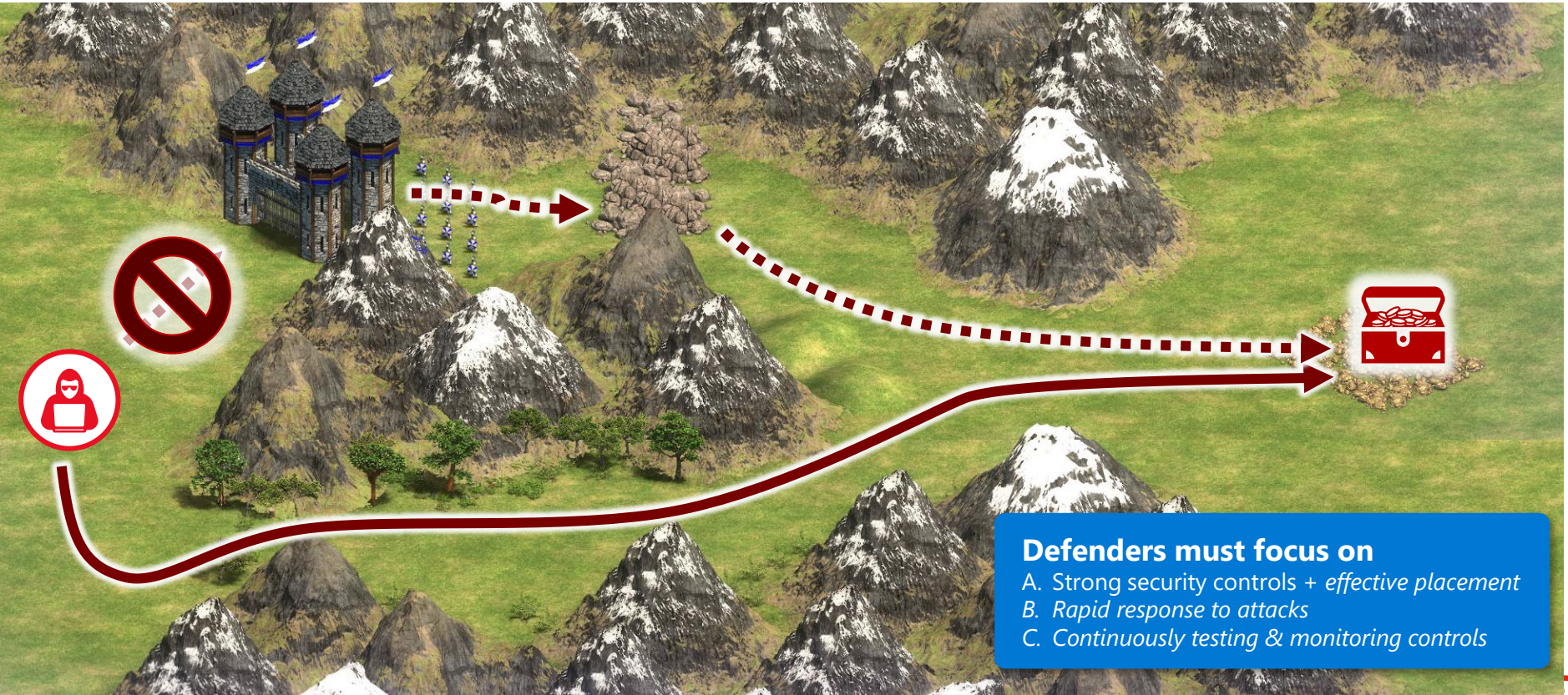
Attacker Perspective: shaped by experience & 'fog of war'

Attackers use what they see, know, and can guess



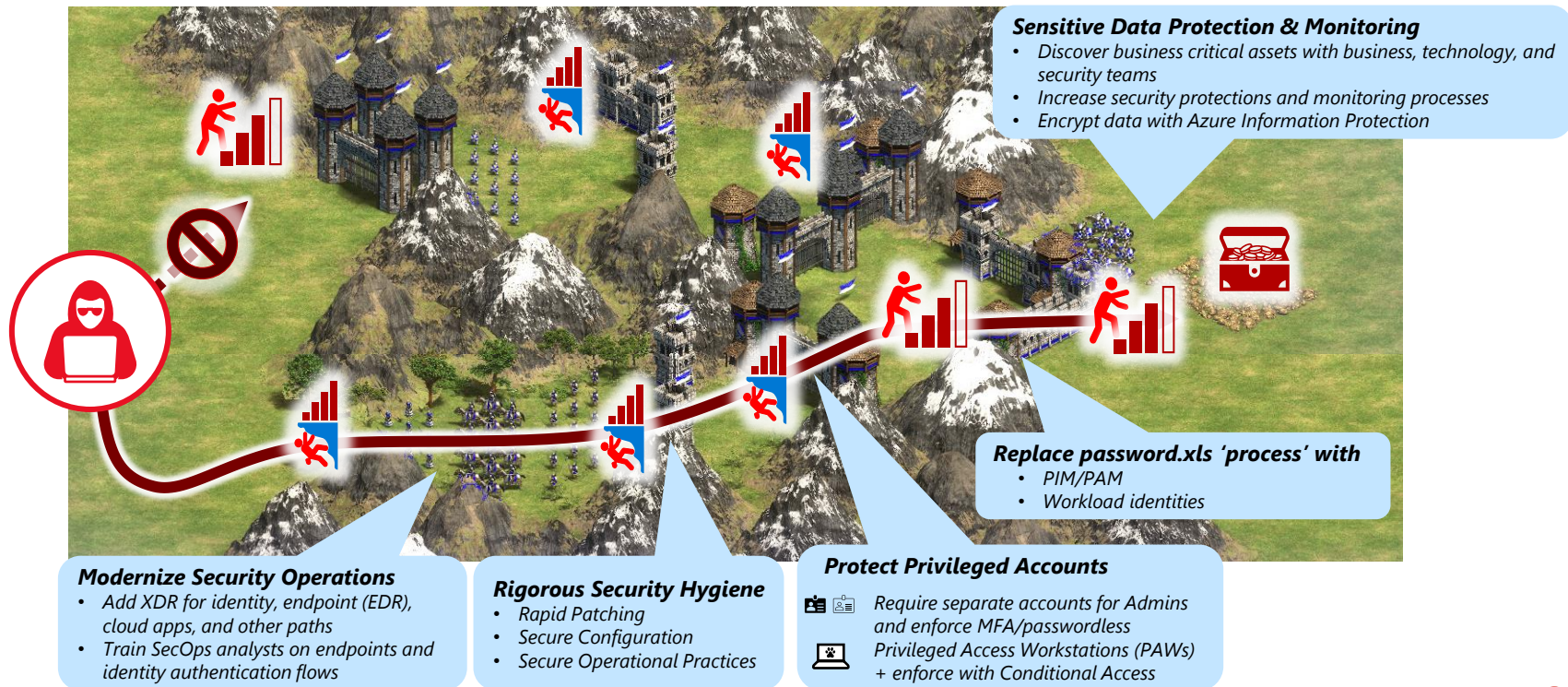
Attackers choose the path of least cost/resistance

Antipattern: Believing attackers will follow the planned path

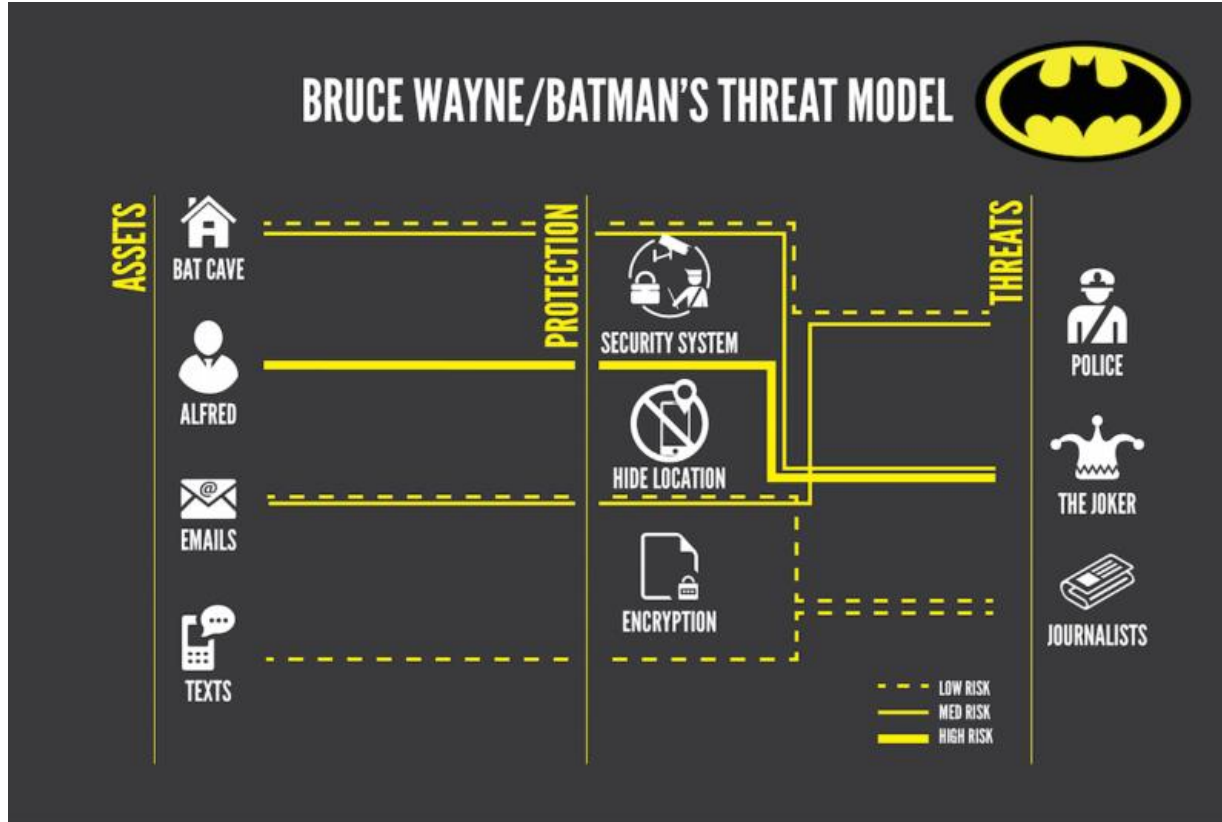


Strategically position security investments

Raise cost and friction on attacker's easiest and highest impact paths



Threat modelling



Storebrand-dagen 2024

Drikkebonger



Storebrand

Vorspiel - kl. 16.00 - 18.00

Gjelder en enhet mineralvann/øl/cider

Frist for å bruke bongen: 01:00

Lysaker

DENNE ER BRUKT

2024-09-06 15:59:44 +0200

Storebrand

Festbong - kl. 16.00 - 00.30

Gjelder en enhet mineralvann/øl/vin

Frist for å bruke bongen: 01:00

Lysaker

DENNE ER UTLØPT

Storebrand

Festbong - kl. 16.00 - 00.30

Gjelder en enhet mineralvann/øl/vin

Frist for å bruke bongen: 01:00

Lysaker

DENNE ER BRUKT

2024-09-06 16:26:59 +0200

Storebrand dagen: 3 drinks limit

Program:

Kl. 16:00: Vorspiel for alle i Bakhagen! Det er meldt strålende ☀️☀️☀️ !

Vår egen DJ Morten Vee lager god stemning 🎵

Kl. 18:00: Servering av mat fra ulike food stands og egen pizza-ovn i bakhagen

Her finner du noe for enhver smak og eventuelle allergier

Kl. 20:00: Martes party-quiz med fine premier 🎁

Kl. 20:15: Modig veiviser-prisen deles ut 🏆

Kl. 21:00: Mini-konsert med Lavrans

Kl. 21:30: Dagny inviterer til en magisk konsertopplevelse

Need Music med DJ skaper klubb-stemning og dancing under vår legendariske disco-kule utover kvelden. 🎵🎵🎵



Anders Kristiansen

Lysaker

DENNE ER BRUKT

2024-09-05 17:16:05 +0200

Storebrand

Festbong - kl. 16.00 - 00.30

Gjelder en enhet mineralvann/øl/vin

Lysaker

DENNE ER BRUKT

2024-09-05 17:21:13 +0200

Storebrand

Festbong - kl. 16.00 - 00.30

Gjelder en enhet mineralvann/øl/vin

Lysaker

Bekreft

Avbryt

Free drinks
for everyone?

Goal: Zero Assumed Trust

Reduce risk by finding and removing implicit assumptions of trust

False Assumptions

of implicit or explicit trust

Security is the opposite of productivity

All attacks can be prevented

Network security perimeter will keep attackers out

Passwords are strong enough

IT Admins are safe

IT Infrastructure is safe

Developers always write secure code

The software and components we use are secure

Zero Trust Mitigation

Systematically Build & Measure Trust

Business Enablement

Align security to the organization's mission, priorities, risks, and processes

Assume Compromise

Continuously reduce blast radius and attack surface through prevention and detection/response/recovery

Shift to Asset-Centric Security Strategy

Revisit how to do access control, security operations, infrastructure and development security, and more

Explicitly Validate Account Security

Require MFA and analyze all user sessions with behavior analytics, threat intelligence, and more

Plan and Execute Privileged Access Strategy

Establish security of accounts, workstations, and other privileged entities ([aka.ms/spa](#))

Validate Infrastructure Integrity

Explicitly validate trust of operating systems, applications, services accounts, and more

Integrate security into development process

Security education, issue detection and mitigation, response, and more

Supply chain security

Validate the integrity of software and hardware components from open source, vendors, and others



Important skills of a cybersecurity professional

Foundational Technical Knowledge

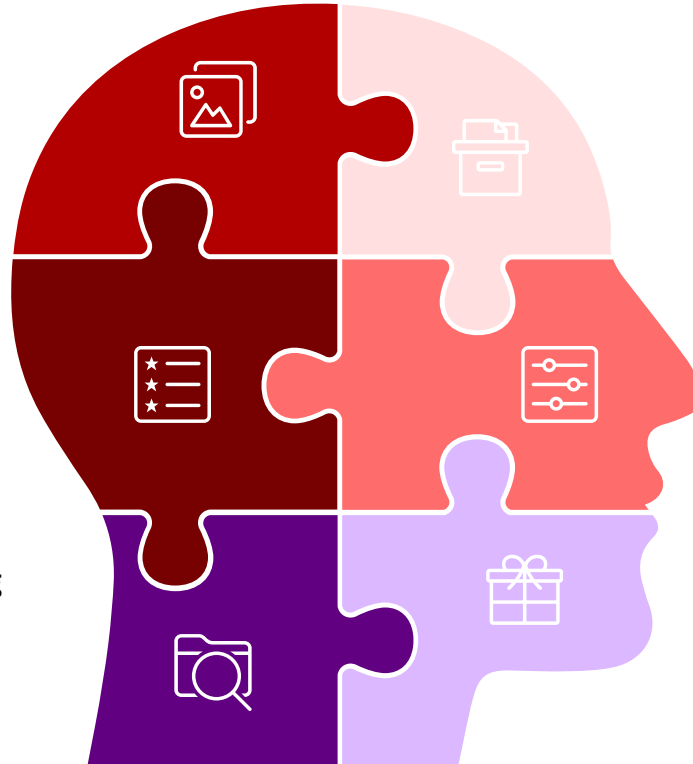
Understanding how networks function, identity and tooling works is critical for being successful

Programming and Scripting

Being able to automate tasks, analyze vulnerabilities, build with IAC require coding understanding

Ethical Hacking and Penetration Testing

Learning how to think like an attacker helps in identifying and addressing system vulnerabilities and run threat modelling



Problem-Solving and Analytical Thinking

Staying updated on the latest threats and understanding how to analyze and respond to them is vital.

Communication and Collaboration

Effective communication skills are essential for explaining complex security issues to non-technical stakeholders and working with different departments

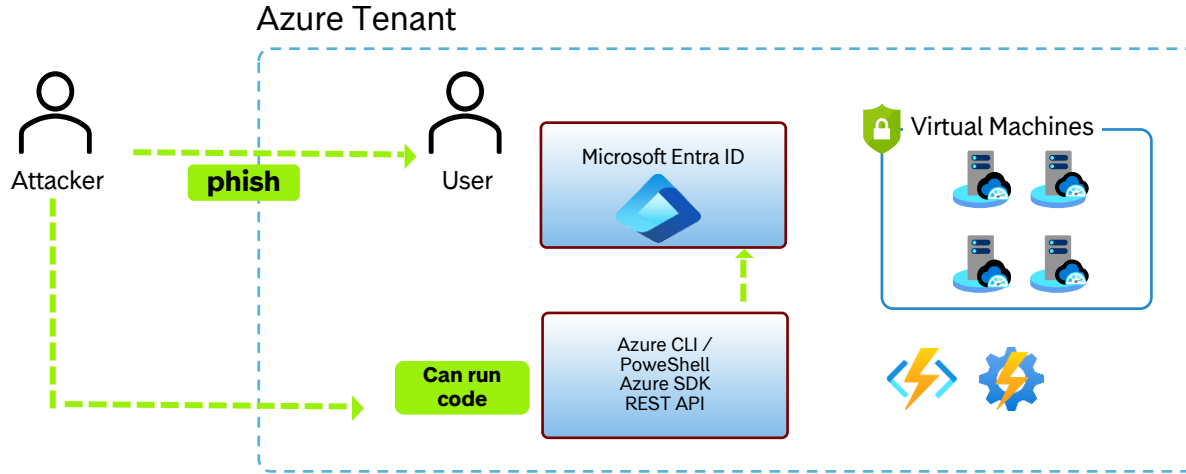
Cloud Security

Most business have some kind of cloud deployment. Understanding and securing cloud is essential.



Attack path MFA - Reconnaissance

Passwords are strong enough



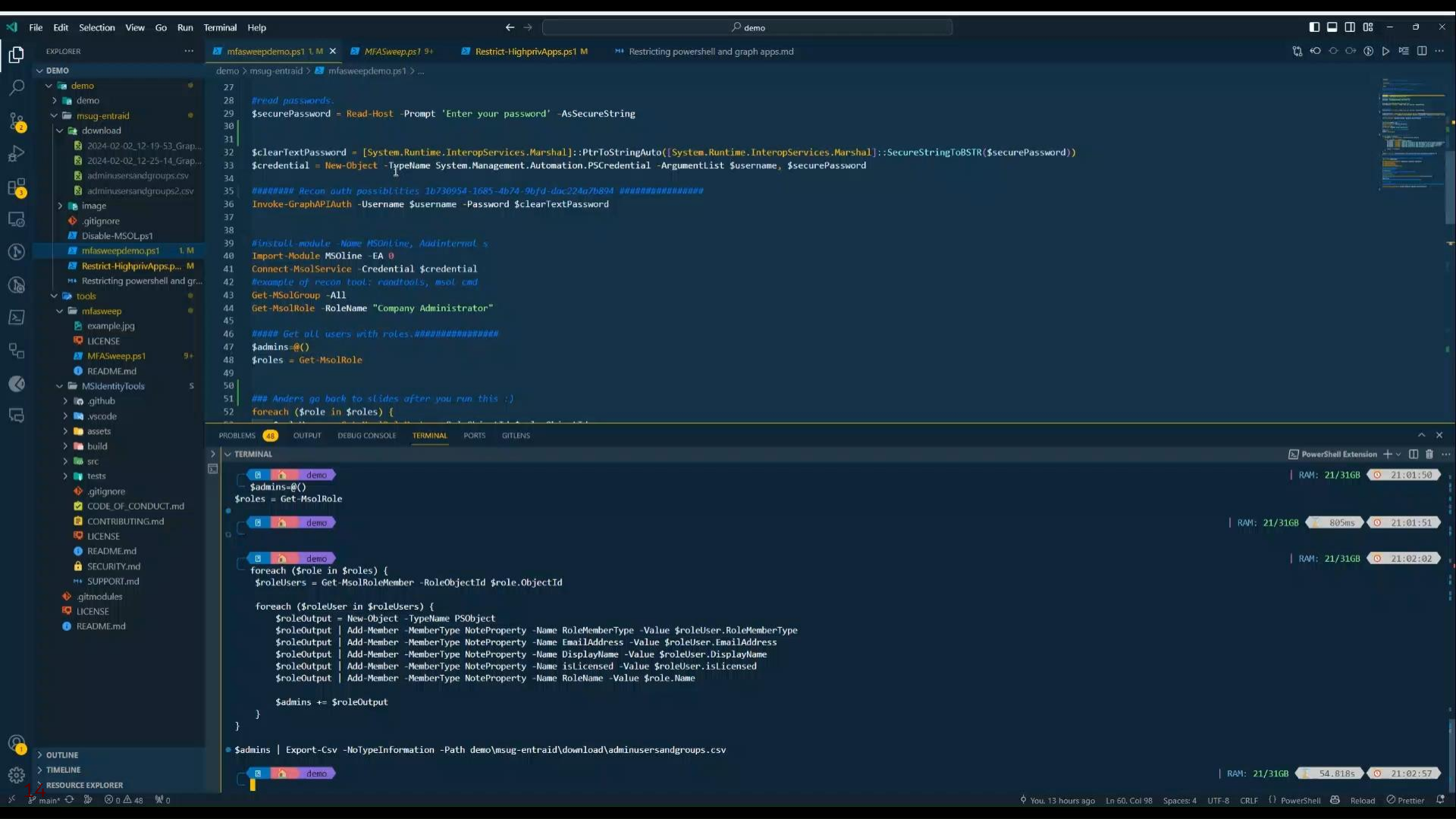
```
----- Microsoft Graph API -----  
[*] Authenticating to Microsoft Graph API...  
[*] SUCCESS! AllanD@M365x62188674.OnMicrosoft.com was able to authenticate to the Microsoft Graph API  
[***] NOTE: The "MSOnline" PowerShell module should work here.
```



MFA Sweep

MFASweep is a PowerShell script that attempts to log in to various Microsoft services using a provided set of credentials and will attempt to identify if MFA is enabled. Depending on how conditional access policies and other multi-factor authentication settings are configured some protocols may end up being left single factor.





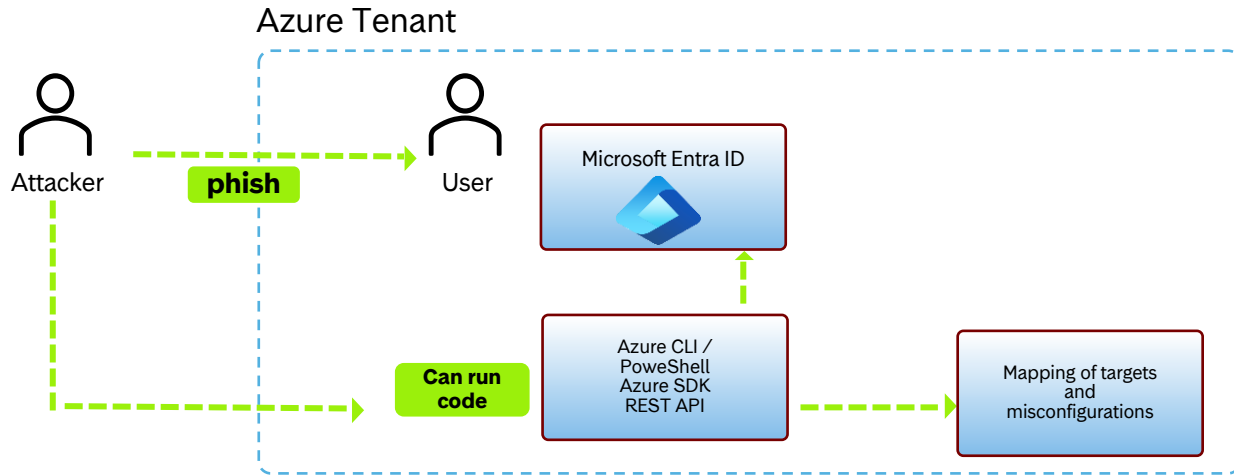
WHO CARES ABOUT MFA?



I NEED TO LOGIN NOW

Attack path MFA - Recap

Passwords are strong enough



Logging and detection

Home >

Sign-in events

Download

Export Data Settings

Troubleshoot

Refresh

Columns

Got feedback?

This view will be soon replaced with a view that includes refresh tokens and application sign-ins. Try out our new sign-ins preview.

Date: Last 24 hours

Show dates as: Local

Add filters

Date	Request ID	User	Application	Status
1/25/2024, 10:35:52 AM	e4143297-787a-495b-92b0-1...	anderskristi	Microsoft Azure PowerShell	Interrupted
1/25/2024, 8:48:42 AM	3ea46598-f14b-4ac0-9782-e3...	anderskristi	Microsoft Graph Command Li...	Success
1/25/2024, 8:48:31 AM	739c572d-8721-4dfb-8f6e-f4e...	anderskristi	Azure Portal	Success
1/25/2024, 8:48:16 AM	3263d2dc-1ca3-4af9-87ad-0e...	anderskristi	Microsoft Graph Command Li...	Success
1/25/2024, 8:48:13 AM	b867b39b-cf87-408a-bc4e-04...	anderskristi	Microsoft Graph Command Li...	Interrupted
1/24/2024, 2:31:27 PM	caf8f310-08ef-45b4-a3de-513...	anderskristi	Azure Active Directory PowerS...	Success
1/24/2024, 2:29:47 PM	f3e21173-19fd-4bc2-8fe3-09a...	anderskristi	Azure Active Directory PowerS...	Success
1/24/2024, 2:29:40 PM	2c55f1eb-9e8f-4b0e-82dd-bc...	anderskristi	Microsoft Azure PowerShell	Interrupted
1/24/2024, 2:29:37 PM	8065b10c-7ee1-4d5e-bd2e-9...	anderskristi	Azure Active Directory PowerS...	Success
1/24/2024, 2:29:33 PM	6dd461b2-3684-437c-a77a-b...	anderskristi	Azure Active Directory PowerS...	Success
1/24/2024, 2:29:05 PM	badd1ada-0e9d-4693-afcb-a3...	anderskristi	Microsoft Graph Command Li...	Success
1/24/2024, 2:29:02 PM	31f4d146-c7f7-4afe-b95d-1ba...	anderskristi	Microsoft Graph Command Li...	Interrupted
1/24/2024, 2:26:46 PM	f94e527a-40bf-45a1-89de-80...	anderskristi	Microsoft Graph Command Li...	Success
1/24/2024, 2:26:42 PM	5d1aacb0-fd79-4685-ad1a-28...	anderskristi	Microsoft Graph Command Li...	Interrupted
1/24/2024, 2:23:49 PM	306aa36f-cae6-4670-a2e9-04...	anderskristi	Microsoft Graph Command Li...	Success
1/24/2024, 2:21:29 PM	2fe09f43-e130-4cfe-94ae-3d5...	anderskristi	Microsoft Graph Command Li...	Failure
1/24/2024, 2:20:43 PM	896cc804-4c60-4133-9215-7e...	anderskristi	Microsoft Graph Command Li...	Failure
1/24/2024, 2:09:24 PM	3ea46598-f14b-4ac0-9782-e3...	anderskristi	Microsoft Graph Command Li...	Success

Activity Details: Sign-ins

Basic info

Location

Device info

Authentication Details

Conditional Access

Report-only

Date

1/25/2024, 8:48:42 AM

Request ID

3ea46598-f14b-4ac0-9782-e3670a32f800

Correlation ID

35397f31-346a-4ad0-a0ef-0ad35e5df4dc

Authentication requirement

Single-factor authentication

Status

Success

Continuous access evaluation

No

Additional Details

MFA requirement satisfied by claim in the token

Follow these steps:

Troubleshoot Event

Launch the Sign-in Diagnostic.

1. Review the diagnosis and act on suggested fixes.

User

anderskristi

Username

anders@anderskristiansen.com

User ID

8ffa280c-f1db-4284-84a1-53dc4f6409c5

Sign-in identifier

User type

Member

Cross tenant access type

None

Application

Microsoft Graph Command Line Tools

Application ID

14d82eec-204b-4c2f-b7e8-296a70dab67e

Resource

Microsoft Graph

Resource ID

00000003-0000-0000-c000-000000000000

Resource tenant ID

07d87066-942e-4072-8596-36dd123efc1b

Home tenant ID

07d87066-942e-4072-8596-36dd123efc1b



Protecting 1st party apps

- Conditional Access Policy Example
- The Application ID is always the same when on Microsoft managed applications

Require MFA for Graph CLI

Conditional Access policy

 Delete  View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more](#)

Name *

Require MFA for Graph CLI

Assignments

Users ⓘ

[All users](#)

Target resources ⓘ

1 app included

Network NEW ⓘ

[Not configured](#)

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Control access based on all or specific network access traffic, cloud apps or actions.
[Learn more](#)

Select what this policy applies to

Cloud apps

Include Exclude


- ☐ None
- ☐ All cloud apps
- ☒ Select apps

Edit filter

[None](#)

Select

[Microsoft Graph Command Line Tools](#)

 Microsoft Graph Command Li...
14d82eec-204b-4c2f-b7e8-296a70dab67e



Entra ID Applications

1st party apps

- Developed by Microsoft and are designed to work seamlessly with the Microsoft Ecosystem
- These apps tend to be forgotten but can have a quite large attack surface.
- These apps don't always result in a service principal being created in your tenant. This can lead to confusion.

Own applications

- Developed or created by the organization
- Typical misconfiguration issues with broad access (owners)
- Poor credential management
- Conditional Access
- Lack of monitoring of these apps

3rd party apps

- Managing access can be more complex than 1st party.
- Supply chain review of 3rd party apps is rarely conducted. (NSM Report)
- Conditional Access policy misconfigurations.
- Too broad access
- Lack of risk detection and monitoring

Application type == Microsoft Applications X



APPS EVERYWHERE



**DO YOU HAVE ANY
QUESTIONS?**



Demo Azure Resource plane + apps



Sentinel - An end-to-end solution for security operations



Powered by community + backed by Microsoft's security experts



Collect



Visibility

Detect



Analytics



Hunting



Intelligence

Investigate



Incidents

Respond



Automation





Tenant



Subscription



Resource Group



Workspace



Microsoft Sentinel

What is infrastructure as code (IaC)?

Declarative

Define what you want,
version based, no
config drift



Consistency

Ensures standards and
compliance, things are
done similar. (LZ,
logging etc)



Self-Service

Teams can deploy
what they need

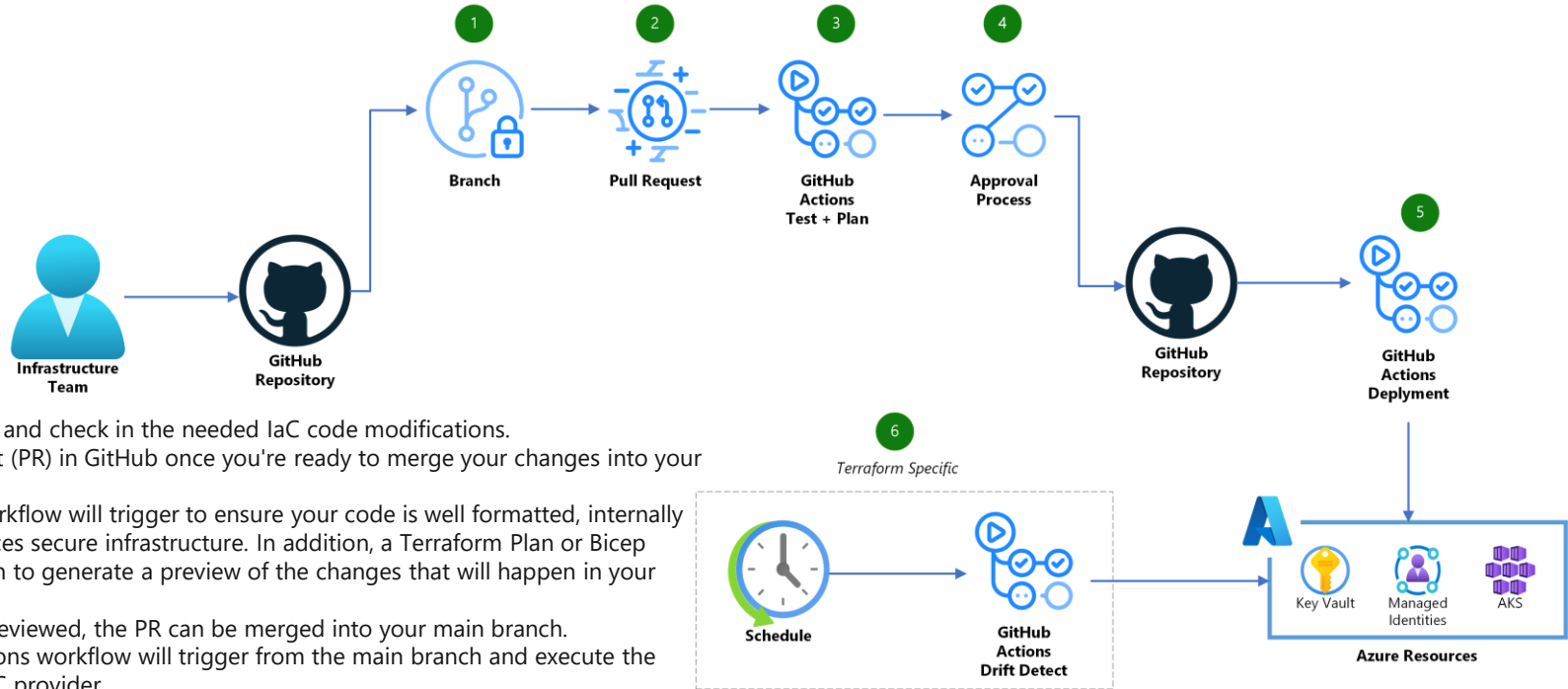


Security

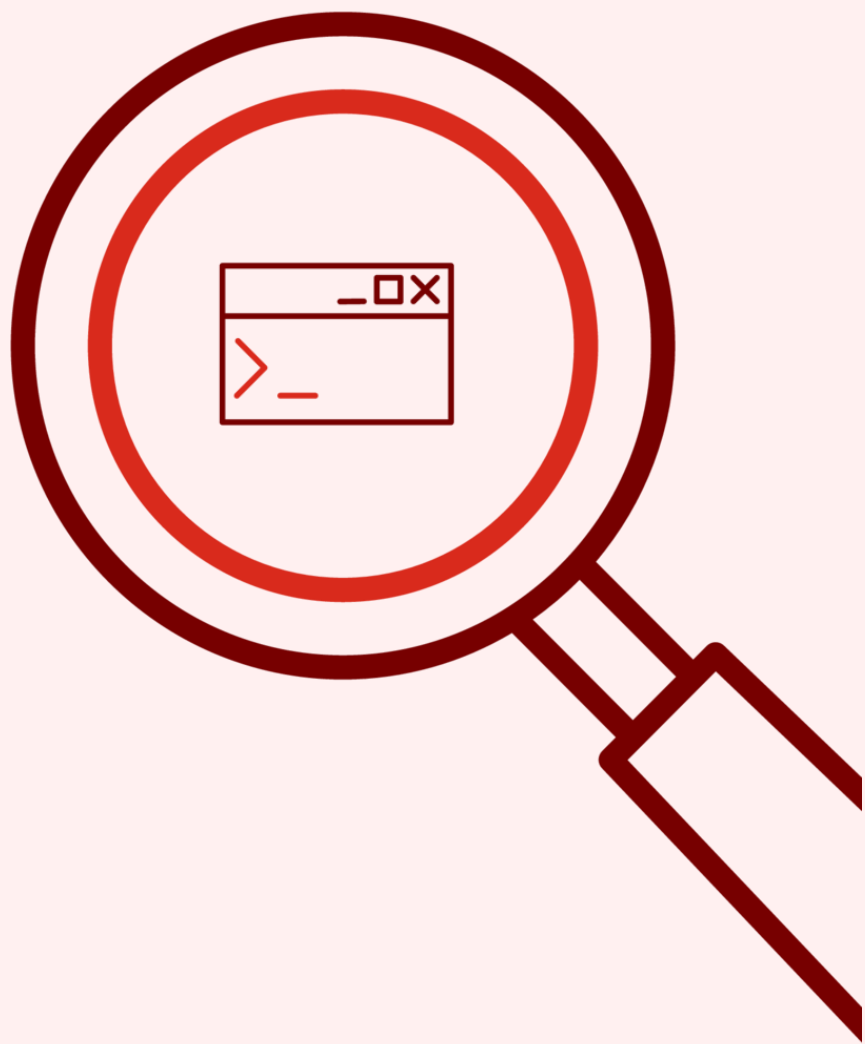
Transparent, security
standards in template,
pipeline



Infrastructure as code – Example flow



Demo Sentinel IAC



Recap

- Play around and have fun
- Troubleshooting is only through hands on
- Ask for help, consult others
- Create a lab, fail fast and learn fast concept.

Microsoft Sentinel free trial activated

The free trial is active on this workspace from 10/9/2024 to 11/9/2024 at 11:59:59 PM UTC.

During the trial, up to 10 GB/day are free for **both Microsoft Sentinel and Log Analytics**. Data beyond the 10 GB/day included quantity will be billed.[Learn more.](#)

OK





References

#

<https://github.com/dafthack/MFASweep>

#

[GitHub - Azure/bicep-registry-modules: Bicep registry modules](#)

#

[Deploy to Azure with IaC and GitHub Actions - Azure DevOps | Microsoft Learn](#)

#

[Security Adoption Resources](#)

#

<https://azure.microsoft.com/en-us/free/students>



`/?'ACCESSKEY='X'ONCLICK='ALERT("THAT'S ALL FOLKS!")`

