

Welcome to



Microsoft Security USER GROUP



Who we are and what we do

Sanna Diana Tomren



Marius Sandbu



Linda Andersen



Haflidi Fridthjofsson



Craig Forshaw



Purpose of this community

- Have fun
- Build network
- Share knowledge
- Learn from each other
- Giving power to the community
- Develop technology for a secure and sustainable future

Microsoft Security, where to start?

Microsoft Cybersecurity Reference Architectures (MCRA)

Capabilities

What cybersecurity capabilities does Microsoft have?



Build Slide

Azure Native Controls

What native security is available?



Multi-Cloud & Cross-Platform
What clouds & platforms does Microsoft protect?

Attack Chain Coverage

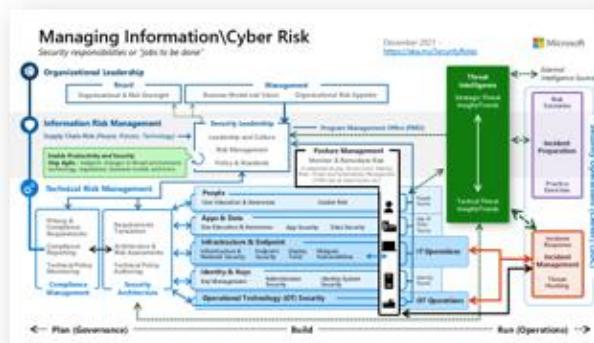
How does this map to insider and external attacks?



Build Slide

People

How are roles & responsibilities evolving with cloud and zero trust?



Zero Trust User Access

How to validate trust of user/devices for all resources?



Security Operations

How to enable rapid incident response?



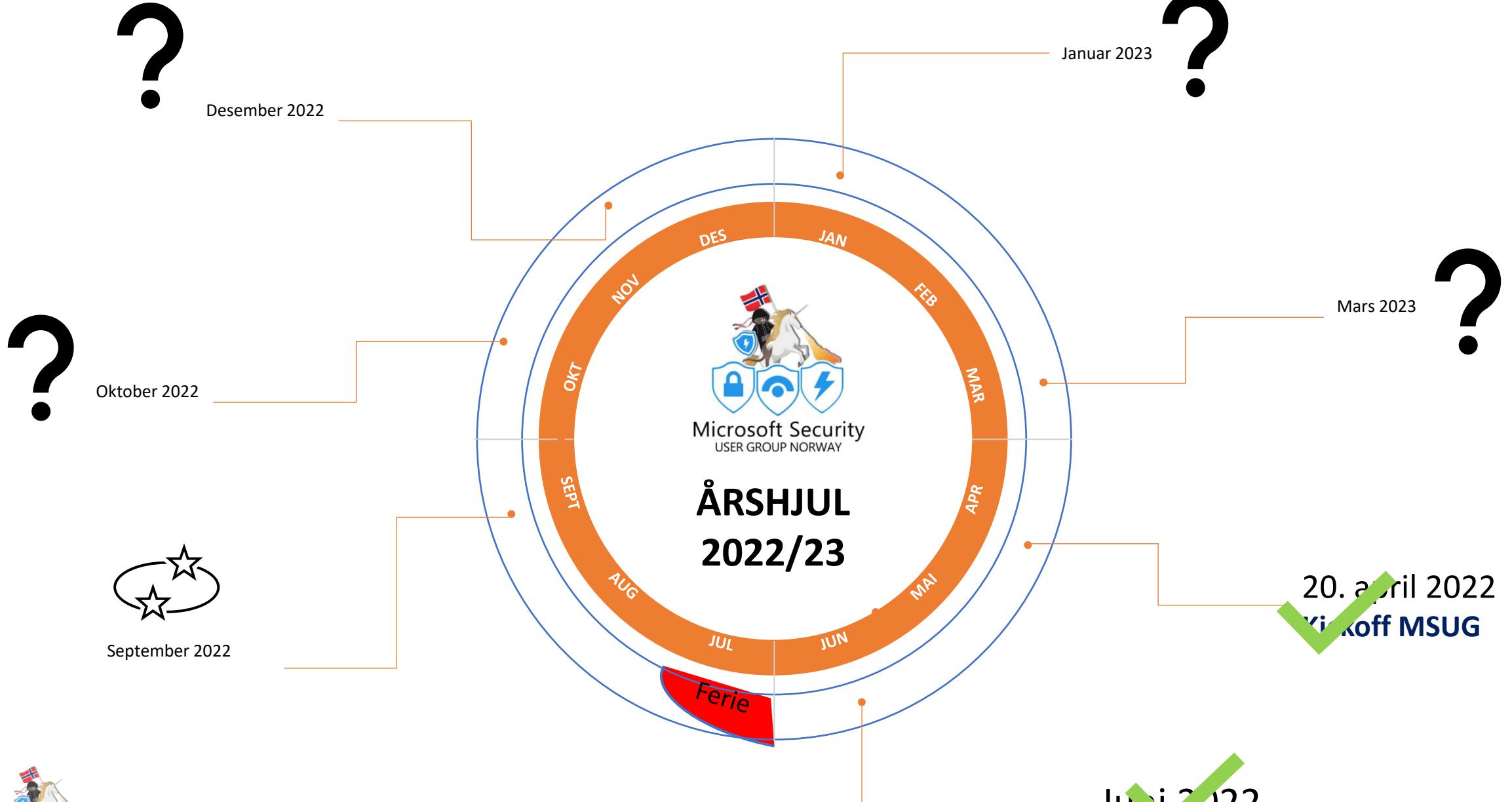
Secure Access Service Edge (SASE)
What is it? How does it compare to Zero Trust?

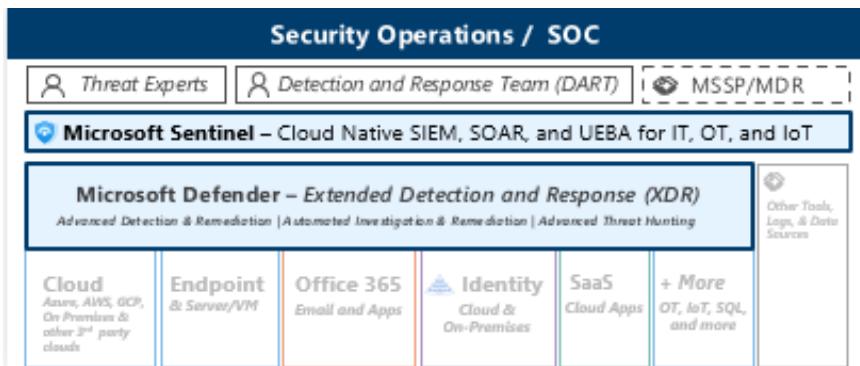


Operational Technology

How to enable Zero Trust Security for OT?







Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

December 2021 – <https://aka.ms/MCRA>

This is interactive!

Security Guidance

1. Present Slide
 2. Hover for Description
 3. Click for more information
- 1. [Security Documentation](#)
 - 2. [Microsoft Best Practices](#)
 - 3. [Azure Security Top 10 | Benchmarks | CAF | WAF](#)

SaaS

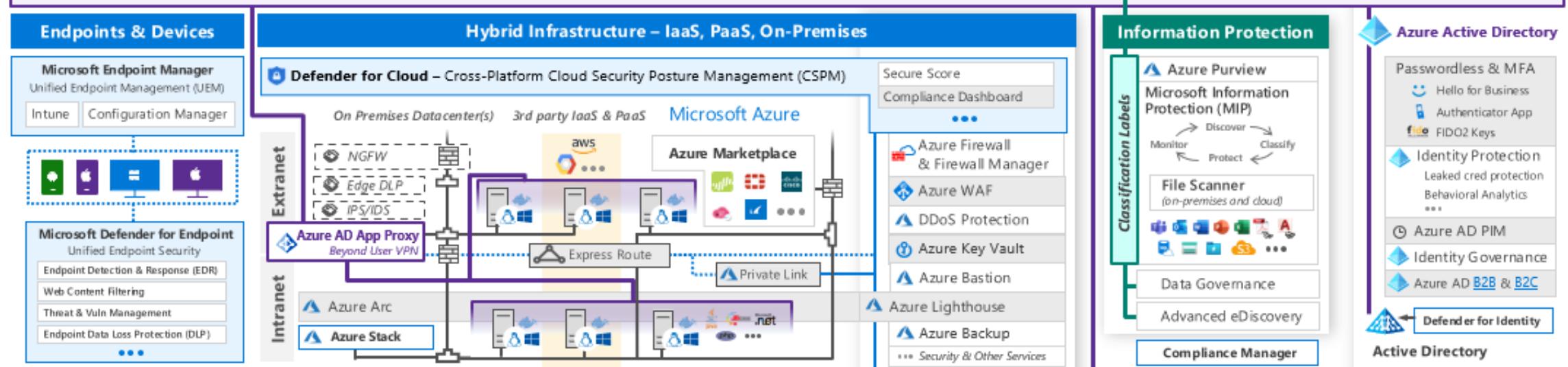


- App Discovery & Risk Scoring (Shadow IT)
- Threat Detection & Response
- Policy Audit & Enforcement
- Session monitoring & control
- Information Protection & Data Loss Prevention (DLP)



Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity



Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance

Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls



Defender for Cloud – Cross-Platform, Cross-Cloud XDR
Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS). Proactive Threat defenses

People Security

Attack Simulator | Insider Risk Management | Communication Compliance

Github Advanced Security – Secure development and software supply chain

Threat Intelligence – 8+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

Thanks to our sponsors



Go to www.menti.com and use the code 4642 6287



What topic would you want to hear about in our next Meetups ?



Microsoft Security
USER GROUP



A recap from the latest Microsoft Defender updates



Who am I?



Marius Sandbu

Cloud Evangelist @ Sopra Steria



[@msandbu](https://twitter.com/msandbu)



[Linkedin.com/msandbu](https://linkedin.com/msandbu)



msandbu.org



Trusselsky



CLOUDFIRST

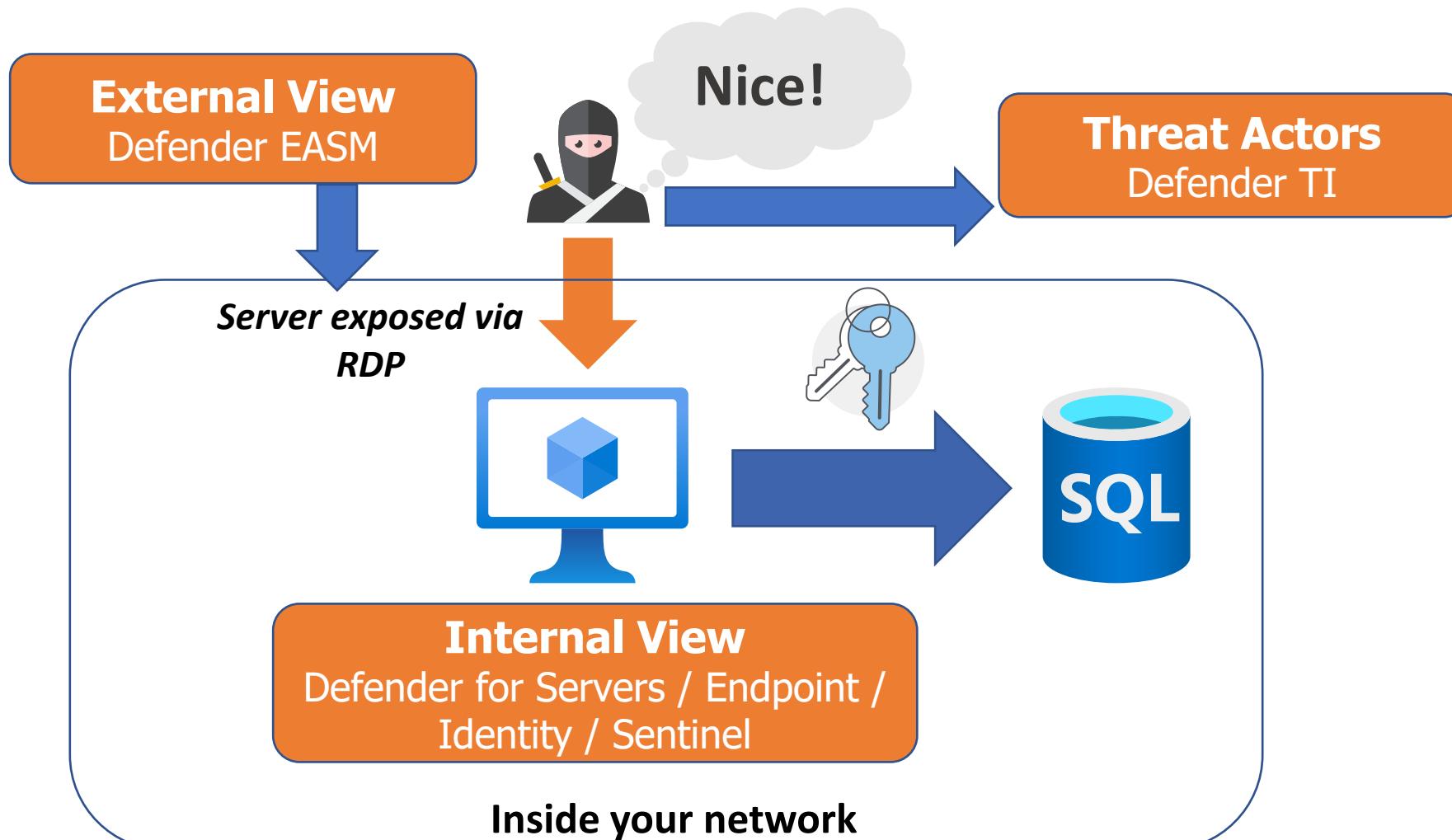
Agenda

- Defender **Threat Intelligence** (TI)
- Defender **External Attack Surface Management** (EASM)
- Defender for Cloud updates
- Defender for Servers updates
- Other updates (if > time)



Automatic Generated Picture from Midjourney (fun fun!)

Why do we need to have all these security services?!



What is Microsoft Threat Intelligence?



Microsoft Defender Product Family



Defender Threat Intelligence

Microsoft Defender Threat Intelligence is a threat intelligence (TI) solution, that helps customers with insights—context, indicators, implications, and strategies—about threat actors and adversary-threat infrastructure. Defender Threat Intelligence aggregates observations and provides curated open-source intelligence (OSINT), along with threat research articles, advanced proprietary threat indicators, and vulnerability intelligence for exploits found in the wild.

Select license quantity

Select billing frequency

€3,513.80 license/month
Pay monthly, annual commitment

€42,165.60 license/year
Pay yearly, annual commitment

Subtotal before applicable taxes
€3,513.80

[Buy](#) [Start free trial](#)

Compare details

There are no details to display.

One-month free trial via Admin Portal

What is Microsoft Threat Intelligence?

```
3 AZFWNatRule  
4 | summarize count() by SourceIp
```

Results Chart

SourceIp ↑↓	count_
> 107.178.200.234	2
> 107.178.231.249	1
> 107.178.232.185	2
> 107.178.232.247	1
> 107.178.232.252	2
> 107.178.232.253	2
> 107.178.236.1	2
> 107.178.236.19	2
> 107.178.236.21	1
> 107.178.236.23	2
> 128.14.134.170	1
> 128.14.137.178	1

🇺🇸 128.14.134.170

◆ Malicious (Score : 100) First Seen: 2018-04-09 | Last Seen: 2021-06-01 | Netblock: 128.14.128.0/21 | ASN: AS21859 - ZEN-ECN | Organization: Zenlayer Inc

Summary Data

Reputation : ◆ Malicious (Score : 100)

Severity	Rule	Description
◆	Third Party Blocklist (dataplane_sipquery)	Threat Type: SCANNER

🇨🇦 142.44.137.77

■ Suspicious (Score : 68) First Seen: 2017-12-24 | Last Seen: 2022-09-13 | Netblock: 142.44.128.0/17 | ASN: AS16276 - OVH | Organization: OVH SAS | 0

Summary Data

Reputation : ■ Suspicious (Score : 68)

Severity	Rule	Description
■	Web components observed	The set of web components observed is frequently associated with suspicious behavior

Microsoft Threat Intelligence API Access

```
$headers = @{
    Authorization="Bearer AzureADACCESSTOKEN
}

import-csv '.\query_data (1).csv' | ForEach-Object {
    Invoke-WebRequest -Uri
    https://ti.defender.microsoft.com/api/reputation?query=$
    ($_.SourceIp) -Method Get -Headers $headers -
    UseBasicParsing -ContentType "application/json".Content
    | ConvertFrom-Json
}
```



Microsoft Threat Intelligence API Access

```
score classification rules
-----
 2 UNKNOWN          {}
74 SUSPICIOUS      {@{name=ASN; description=Infrastructure hosted by this ASN frequently exhibits suspicious}
 0 UNKNOWN          {}
100 MALICIOUS       {@{name=Third Party Blocklist (dataplane_sshclient); description=Threat Type: SCANNER; sev}
66 SUSPICIOUS      {@{name=ASN; description=Infrastructure hosted by this ASN frequently exhibits suspicious}
 9 UNKNOWN          {}
 2 UNKNOWN          {}
 1 UNKNOWN          {}
66 SUSPICIOUS      {@{name=ASN; description=Infrastructure hosted by this ASN frequently exhibits suspicious}
73 SUSPICIOUS      {@{name=ASN; description=Infrastructure hosted by this ASN frequently exhibits suspicious}
 0 UNKNOWN          {}
 0 UNKNOWN          {}
```

[Microsoft Defender Threat Intelligence \(Defender TI\)](#)
[Reputation Scoring | Microsoft Docs](#)



Microsoft Threat Intelligence

Access to free tier via
ti.defender.microsoft.com

Limited integration options
with Microsoft Security

One Analytics rules that uses
the dataset → (DNS from DC)

More Analytics Rule to come!

(Preview) Microsoft Threat Intelligence Analytics

Medium Severity	Gallery Content Content source	Threat Intelligence Rule Type
-----------------	--------------------------------	-------------------------------

Description
This rule generates an alert when a Microsoft Threat Intelligence Indicator gets matched with your event logs. The alerts are very high fidelity.

Note : It is advised to turn off any custom alert rules which match the threat intelligence indicators with the same event logs matched by this analytics to prevent duplicate alerts.

Data sources

- Common Event Format (CEF)
- CommonSecurityLog --
- DnsEvents --
- Syslog

Tactics and techniques

- Lateral Movement (0)
- Persistence (0)

Microsoft Threat Intelligence – Free vs Paid

Features	Defender TI Free	Defender TI Premium
Articles	<input checked="" type="checkbox"/> New articles first in Premium	<input checked="" type="checkbox"/> Directly available
Articles description	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Articles Public indicators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Articles Defender TI indicators	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Reputation	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Analytics insights	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Data: Historical data	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Data: Whois information	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Data: Whois historical information	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Data: Cookies	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Data: Components	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Demo of Microsoft Threat Intelligence



Microsoft Defender External Attack Surface Management

Some of the features



SHODAN



+ Preview features



Microsoft

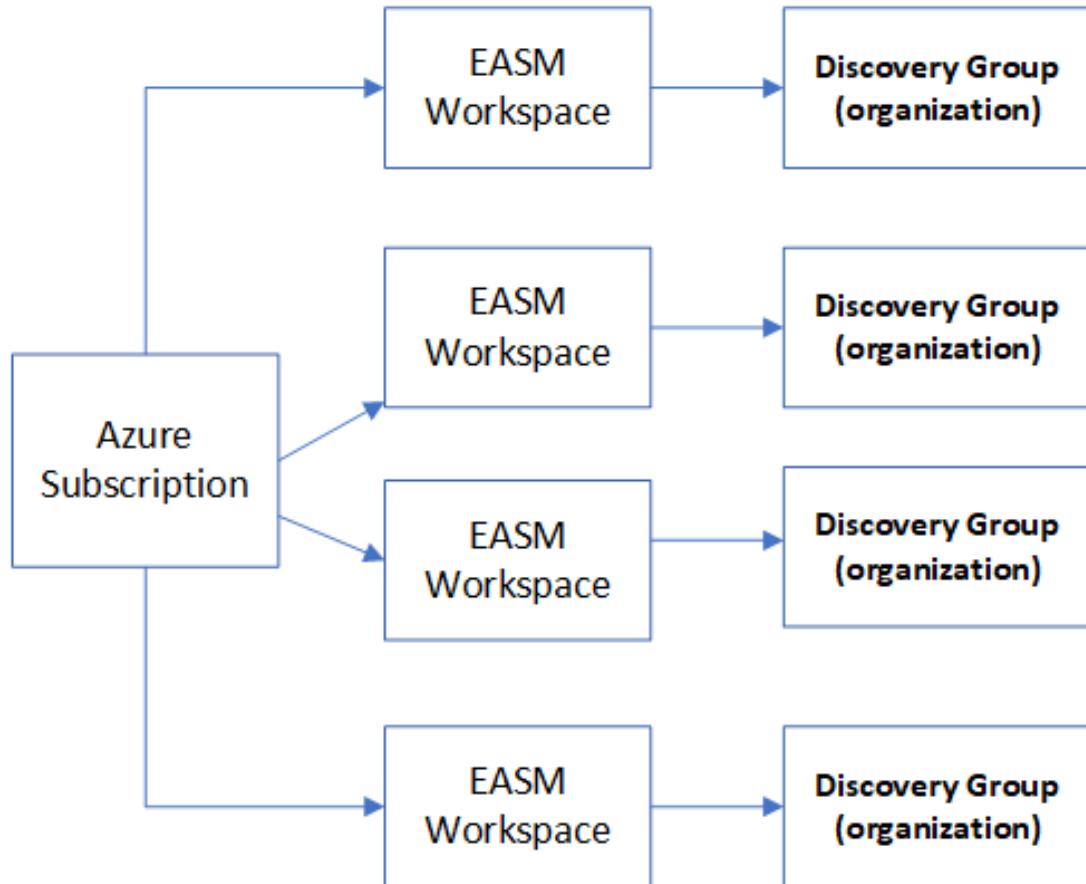


Defender
EASM

Terraform AzAPI Example

```
resource "azapi_resource" "easm" {
    type = "Microsoft.Easm/workspaces@2022-04-01-
preview"
    name = "easmdemo"
    parent_id = azurerm_resource_group.aksrg.id
    location = "swedencentral"
    schema_validation_enabled = false
}
```

Microsoft Defender External Attack Surface Management



One Workspace can have
multiple Discovery Groups

One Discovery Group can
contain multiple seeds

Seeds:

- Domains
- IP Blocks
- Hosts
- Email Contacts
- ASNs
- Certificate Common Names
- Whois Organizations

So what do we get?

Mapping of our infrastructure from
an «outside» view

Assets – External Services –
Vulnerability mapping

CVE Exposure – IP Reputation –
SSL Configuration

Customize which seeds should be
monitored

Dashboards!

1
High Severity Observations

Found from 1 of 84 Insights

Top Observations

Vulnerability Description	Count
CVE-2016-2569 - Squid Proxy Denial of Service Vulnerability	1
CVE-2019-17638 Jenkins Server Vulnerability May Lead to Sensitive Data Leak	0
CVE-2022-23277 Microsoft Exchange Server Remote Code Execution Vulnerability	0
CVE-2020-4448 IBM WebSphere Application Server Remote Code Execution Vulnerability	0
Microsoft Patches Four 0-Day Remote Code Execution Vulnerabilities in Exchange Server (Patch)	0

All 84 Insights

Important to note

Currently not integrated with
Security Graph API

Not available in most regions yet
(Sweden Central closest)

Cost is per Asset = 0.104,- per
day

Example: 100 Assets = 320,-
per month (30-day trial)

Assets by state

Total assets

■ 8.3M

Total Cost of Assets for
Netflix Inc

= **863.000,- per day**

Demo of Microsoft EASM

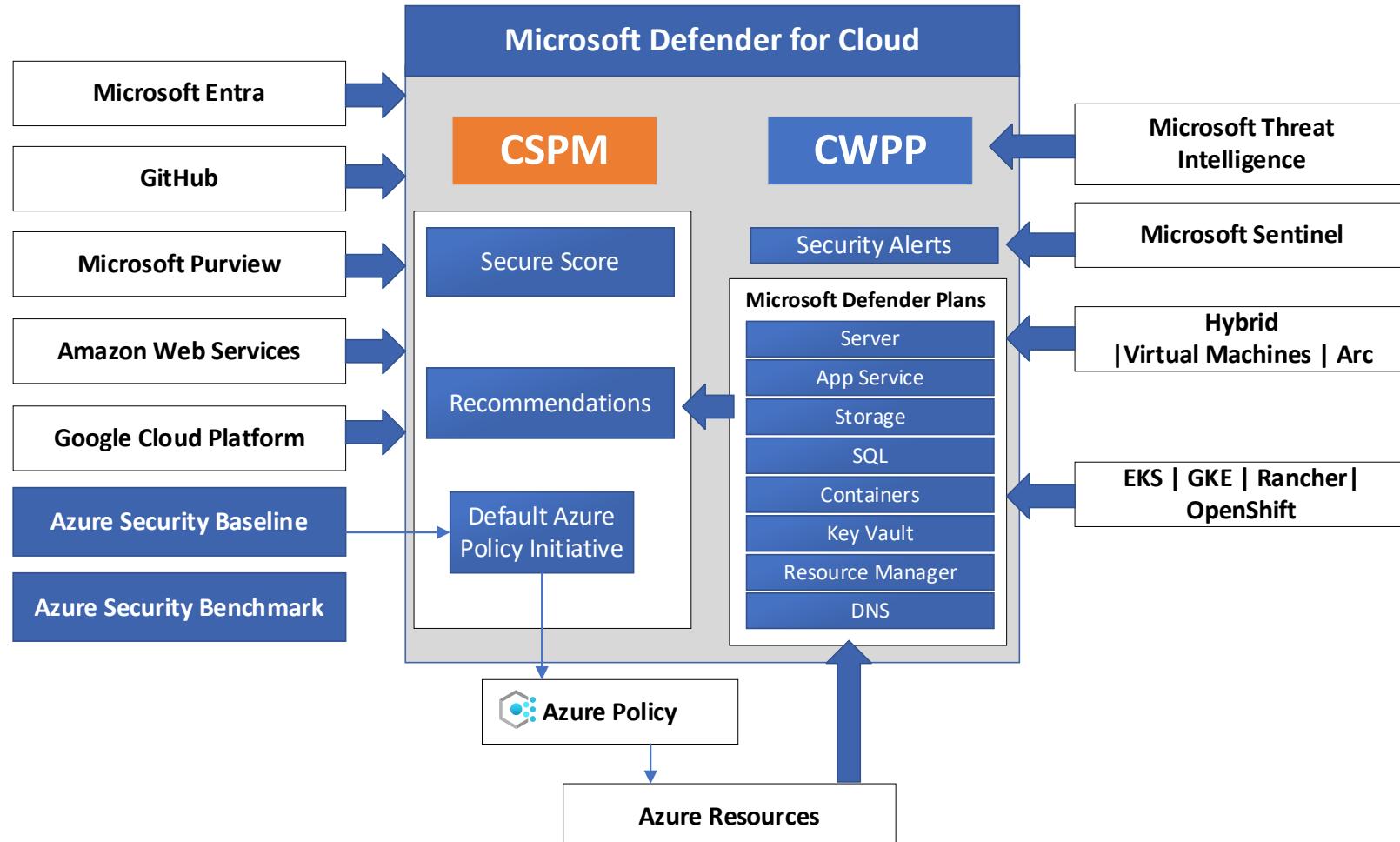


Microsoft Security
User Group Norway
C2 Restricted

©2022 Microsoft Security User Group Norway All Rights Reserved

@MsSecUGNorway
#MSUGN

Defender for Cloud what is it?



CSPM = Cloud Security Posture Management

How secure is your Cloud Platform setup?

CWPP = Cloud Workload Protection Platform

How secure is your actual workload?

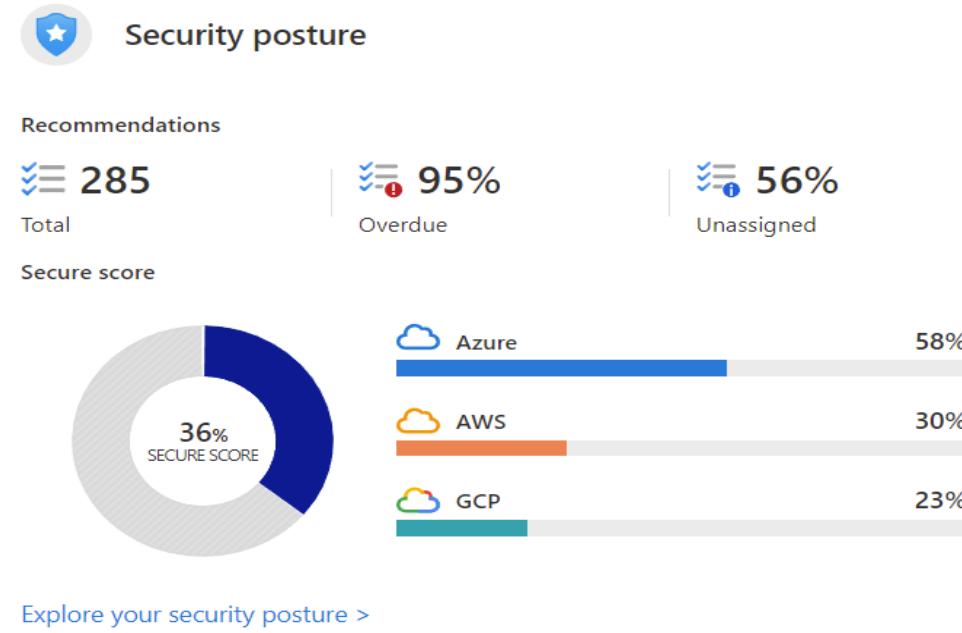
Updates for Defender for Cloud

Governance Rules

Support for Azure Monitor Agent
<https://portal.azure.com/?feature.includePreviewTemplates=true> (workbook)

Defender for Containers

Not directly related...
New firewall log schema for Azure Firewall logging



Azure Monitor Agent

- DCR rules
- Multihoming
- Single Agent
- A bunch of features in Public Preview

[Supported features in Azure Monitor vs Log Analytics Services](#)

Updates for Defender for Cloud

Auto-provisioning for Endpoint
Unified Solution

Defender for Cosmos DB & ARM

Integration with Entra Permissions
Management

JIT Access for VMs in AWS EC2

A lot of features in Private Preview
coming soon!



Permission Creep Index for an Azure
Environment – **Showing service account with
high amount of privileges**

Updates for Defender for Server

Attack Surface Reduction Rules reporting in Defender

Network and Web Protection for Linux and MacOS

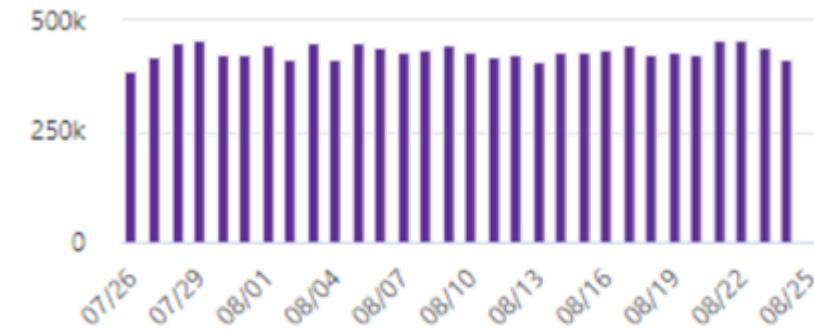
Block vulnerable applications
(Currently for Windows Client OS)

Contain Devices from the Network
(Windows 10 + 2019)

12995.9k detections blocked

Last 4 weeks

Attack surface reduction (ASR) rules stop threats by blocking various attack techniques.



Screenshot of the Microsoft Defender for Server interface. It shows a summary of device status: 3 total devices, 0 high risk, and 0 high exposure. On the right, a context menu for a specific device is open, with the 'Contain device' option highlighted with a red box. Other menu items include 'Open device page', 'Device value', 'Manage tags', 'Ask Defender Experts', 'Action center', and 'Exclude'.

Updates for Defender for Server

Two plans (1 or 2)
50,- or 150,- per month

Plan 1 does not include
vulnerability scanning from Qualys
(only from Microsoft)

Plan 1 does not include EDR
capabilities

Dashboard > Microsoft Defender for Cloud > A vulnerability assessment solution should be enabled on your virtual machines >
A vulnerability assessment solution should be enabled on your virtual machines ...
Remediating 1 resource

Choose a vulnerability assessment solution:

- Threat and vulnerability management by Microsoft Defender for Endpoint (included with Microsoft Defender for servers)
- Deploy the integrated vulnerability scanner powered by Qualys (included with Microsoft Defender for servers)
- Deploy your configured third-party vulnerability scanner (BYOL - requires a separate license)
- Configure a new third-party vulnerability scanner (BYOL - requires a separate license)

Demo of Microsoft Defender



@MsSecUGNorway
#MSUGN

New stuff from Azure AD the last year (if time..)

Group Write Back in Azure AD

FIDO2 Azure MFA Verification

Nested Group membership

Continous Access Evaluation GA

Custom Attributes Based Access

Cloud Trust (Preview)

Microsoft decided to change all names to Entra...

Entra Permissions Management
(Cloudknox)

Improved Identity Flow with Logic App and Entitlement Management

Removing of legacy authentication in October

TOTP MFA for Azure AD B2C

Possibility to adjust Access token lifetime

On-prem provisioning (LDAP and SQL)

Workload Identity

Cross tenant federation

Secure authentication with temporary pass

Certificate basert authentication

Automatic removal of guest accounts based upon access review

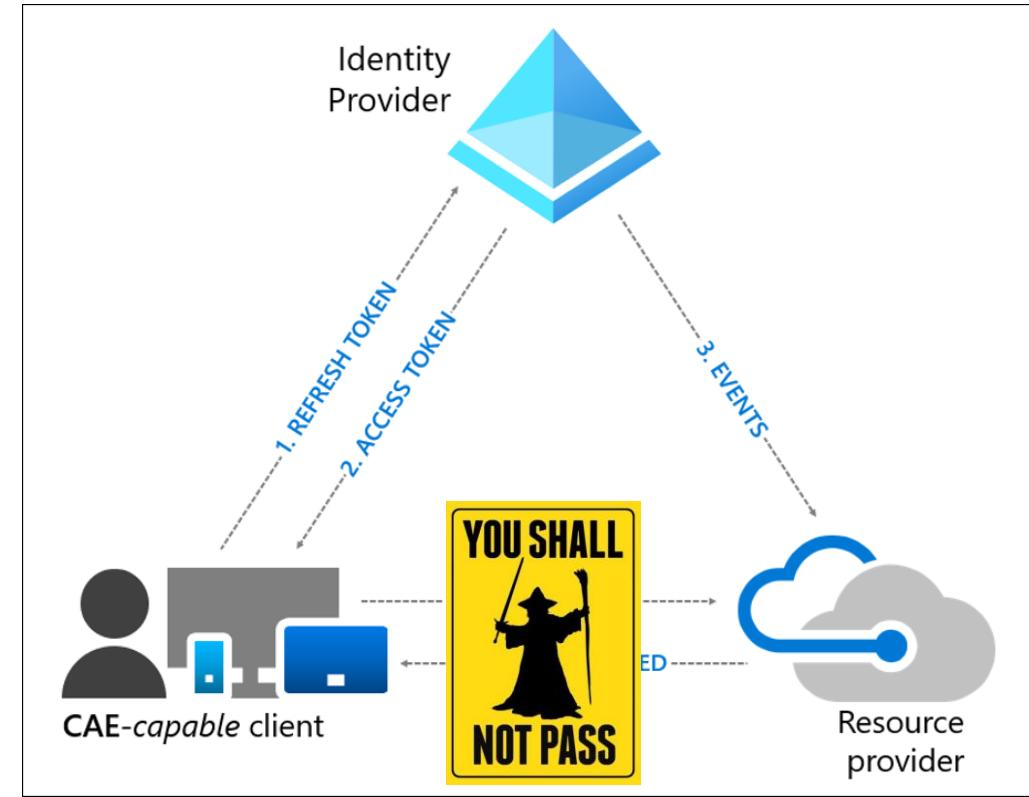
Azure AD basert Kerberos

Lifecycle Workflows

[What's new? Release notes - Azure Active Directory - Microsoft Entra | Microsoft Docs](#)

Continuous Access Evaluation (CAE)

- Activities that trigger a new evaluation
 - Accounts deleted or deactivated
 - Password changed or reset
 - MFA enabled for account
 - High-risk detection in PIM
 - Administrator revokes token
- At the moment only support in Microsoft Office
- If no CAE used the token is alive for 1 hour



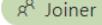
Lifecycle Workflows

- Workflow Jobs

- Can be triggered manually or automagically
- Based upon user attributes
- Can be defined on Azure AD account or via Sync Engine
- Customed workflow via Logic Apps
- Based upon the attribute **NewEmployeeHireDate**

Choose a workflow

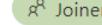
Choose a workflow template to start creating your custom workflow. [Learn more](#)

 Joiner

Onboard pre-hire employee

Configure pre-hire tasks for onboarding employees before their first day

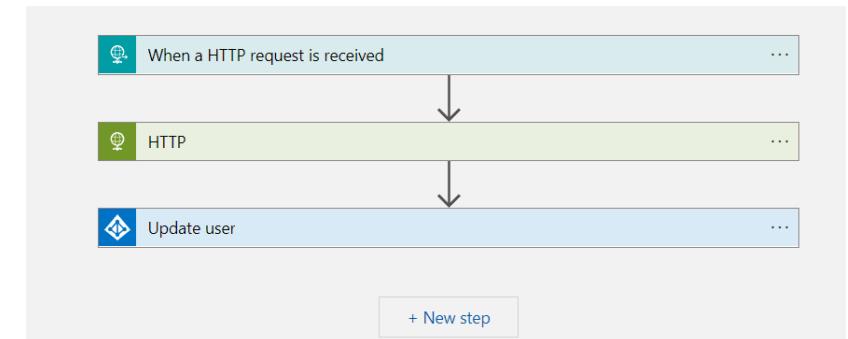
[Select](#) | [Details](#)

 Joiner

Onboard new hire employee

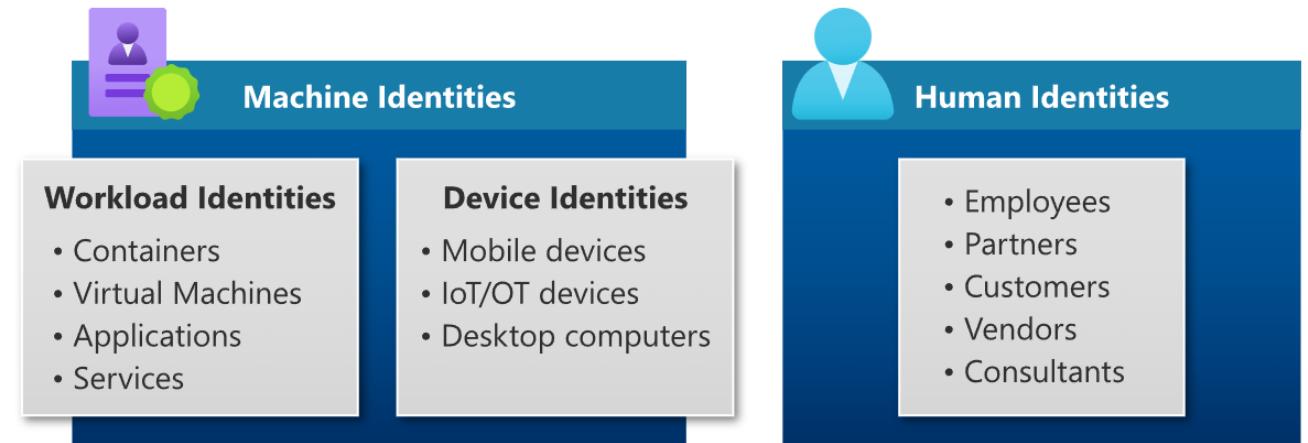
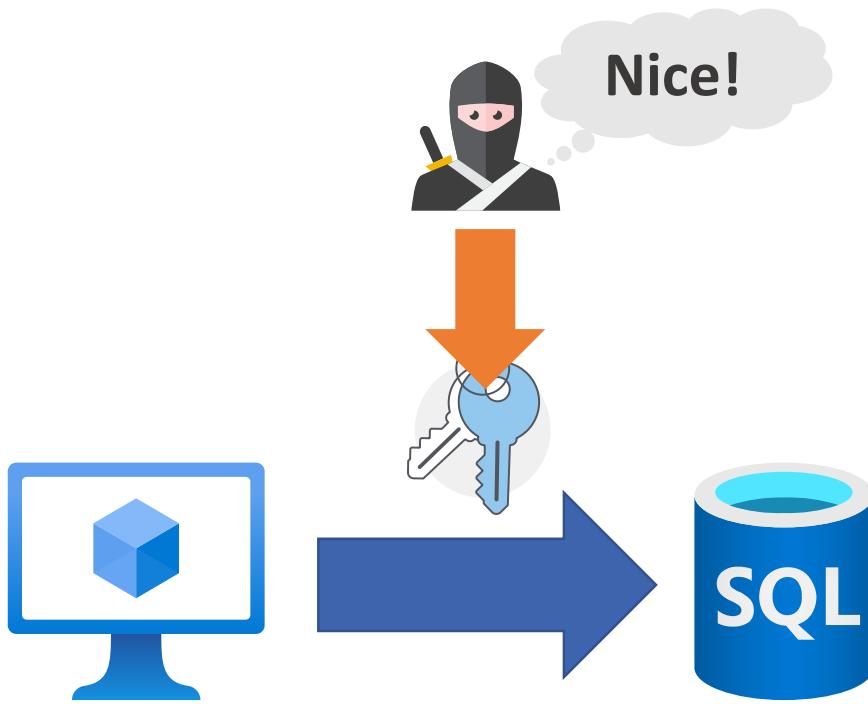
Configure new hire tasks for onboarding employees on their first day

[Select](#) | [Details](#)



Logic Apps

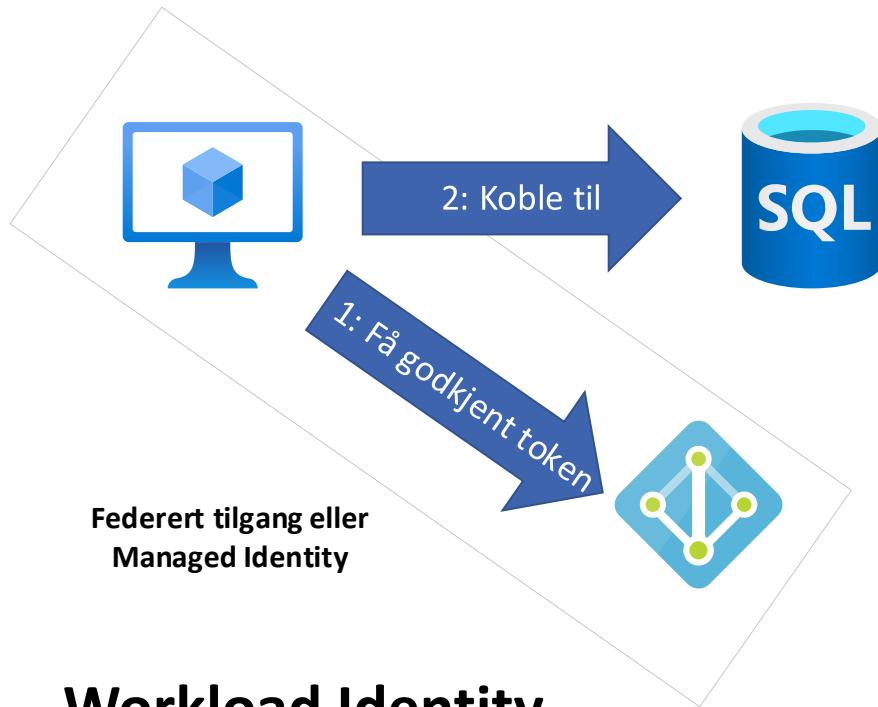
Workload Identity



How to solve service authentication...

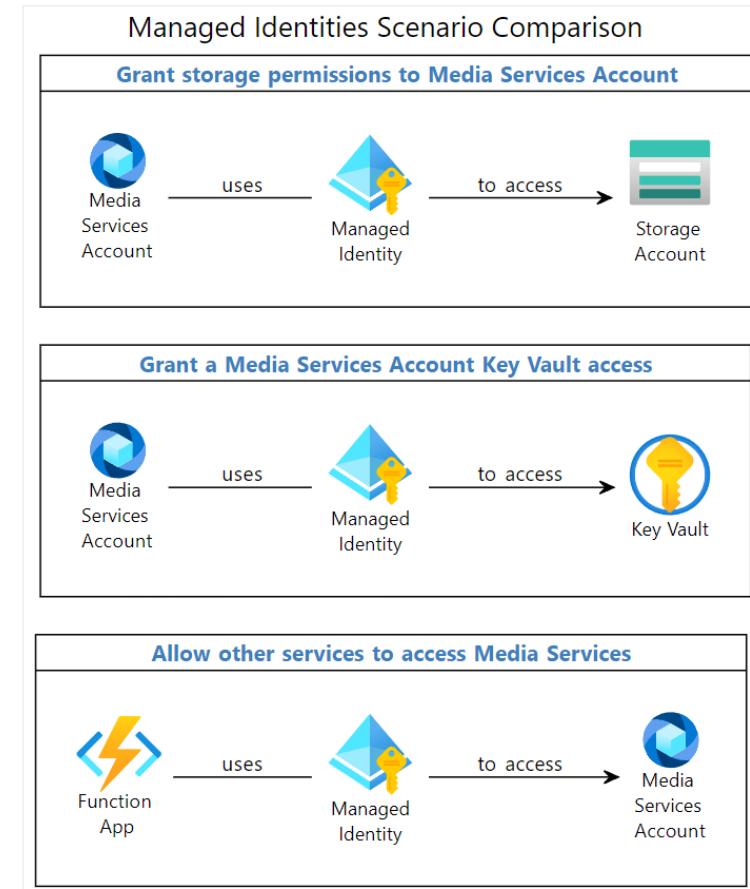
- Username and password?
- Certificate?
- Active directory?

Workload Identity or Managed Identity



Workload Identity

- Conditional Access
- Workload Federation support for
 - Github Actions
 - Google Cloud
 - Kubernetes tjenester
 - Egenutviklet applikasjoner



Token lifetime Configuration

Tokens in Azure and expiration

- Access Tokens (60 – 90 minutes)
- SAML Tokens (60 minutes)
- Refresh Tokens (24 hours / 90 days)
- Session token (24 hours or 180 days)
- Primary Refresh Token (14 days)

- Conditional Access Sign-in frequency can override **90 day refresh token**

```
$policy = New-AzureADPolicy -  
Definition  
@('{"TokenLifetimePolicy": {"Versi  
on": 1, "AccessTokenLifetime": "02:  
0:00"} }') -DisplayName  
"WebPolicyScenario" -  
IsOrganizationDefault $false -  
Type "TokenLifetimePolicy"
```

Login for the first time

- Access token
- ID token
- Refresh Token
- PRT (if Azure AD maskin)

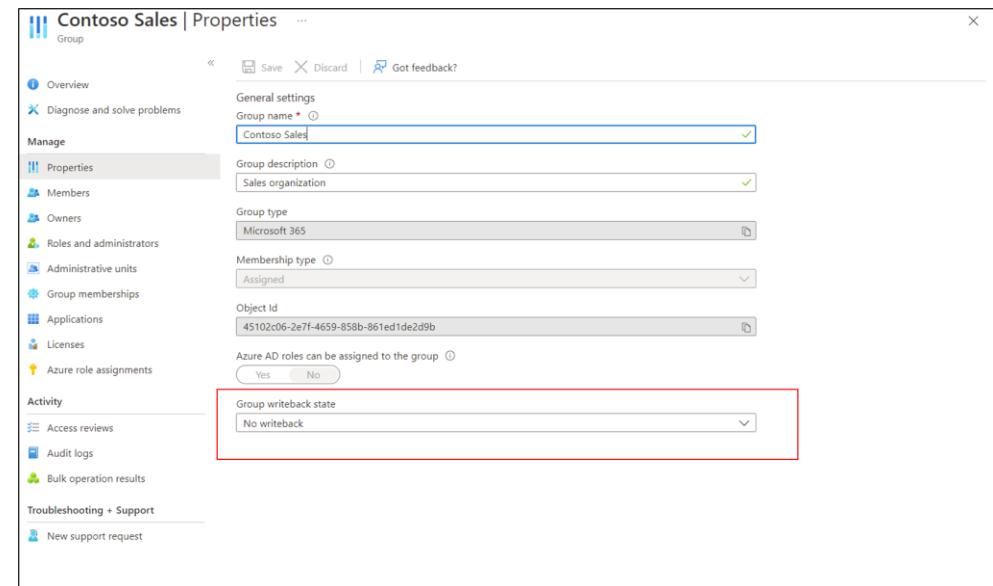
Refresh Token sent
to Azure AD

Application gets a
new access token

Group Writeback in Azure AD

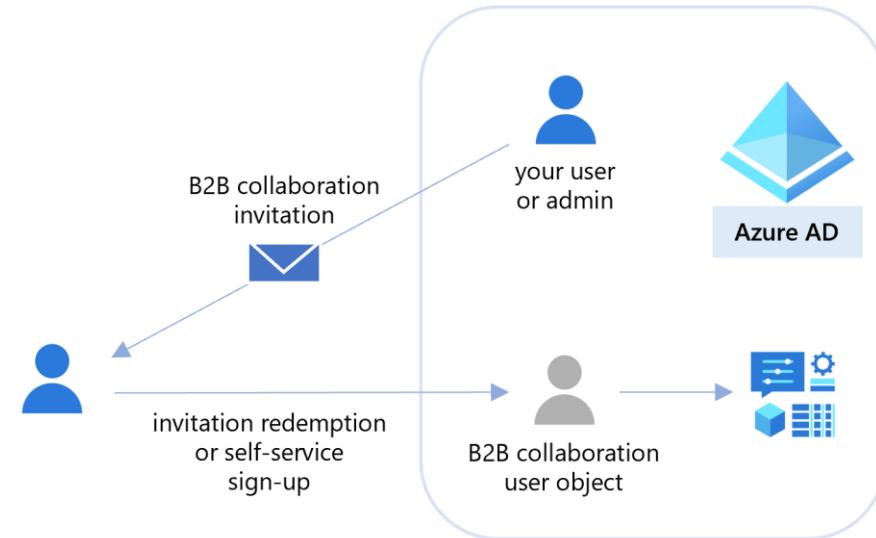
To features currently available

- GA - Microsoft 365 Groups to distribution groups
- Preview (Writing back as security groups)
- Can be combined with PIM and Entitlement Management
- Means that the source of authority for groups are in Azure AD and not the other way around
- Cannot force ownership on existing synchronized groups



Cross-tenant access

- **B2B Collaboration in Azure AD**
 - User A becomes guest in tenant B
 - Typically by inviting members to a Team Channel
 - Challenges with MFA, Device Health and Conditional Access
- **B2B Direct Connect**
 - To use Shared Channels in Microsoft Teams
 - Directly federation between organizations
 - Can define trust other organizations security settings



- Trust multifactor authentication from Azure AD tenants
- Trust compliant devices
- Trust hybrid Azure AD joined devices



[Say goodbye to unmanaged Azure AD accounts for B2B collaboration - Microsoft Tech Community](#)

LDAP, SQL and SCIM provisioning

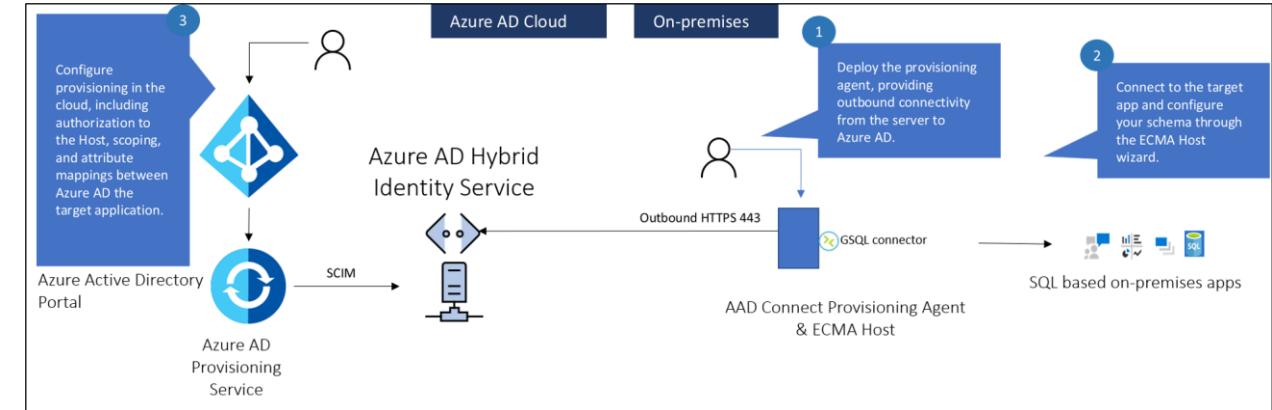
- LDAP

- AD LDS
- OpenLDAP
- Apache LDAP
- Oracle
- IBM Tivoli

- SQL Server

- Supporterte SQL Server
- Microsoft SQL Server
- IBM DB2
- Oracle
- MySQL

- Azure AD already supports a bunch of other SaaS services



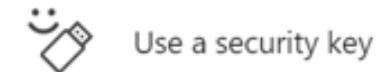
It is only the old
MIM / FIM Engine in
disguise....

Certificate based authentication (Preview)

- SmartCard login supported on the latest version of Windows 11 insider
- Free feature in Azure AD (belive it or not!)
- Built-in support already for most Microsoft applications on mobile devices
- Must used a UPN based certificate
- Cannot use public PKI service
- Can be used as a single factor or combined multifactor authentication



Choose a way to sign in



Use a security key



Use my password



Sign in with a certificate

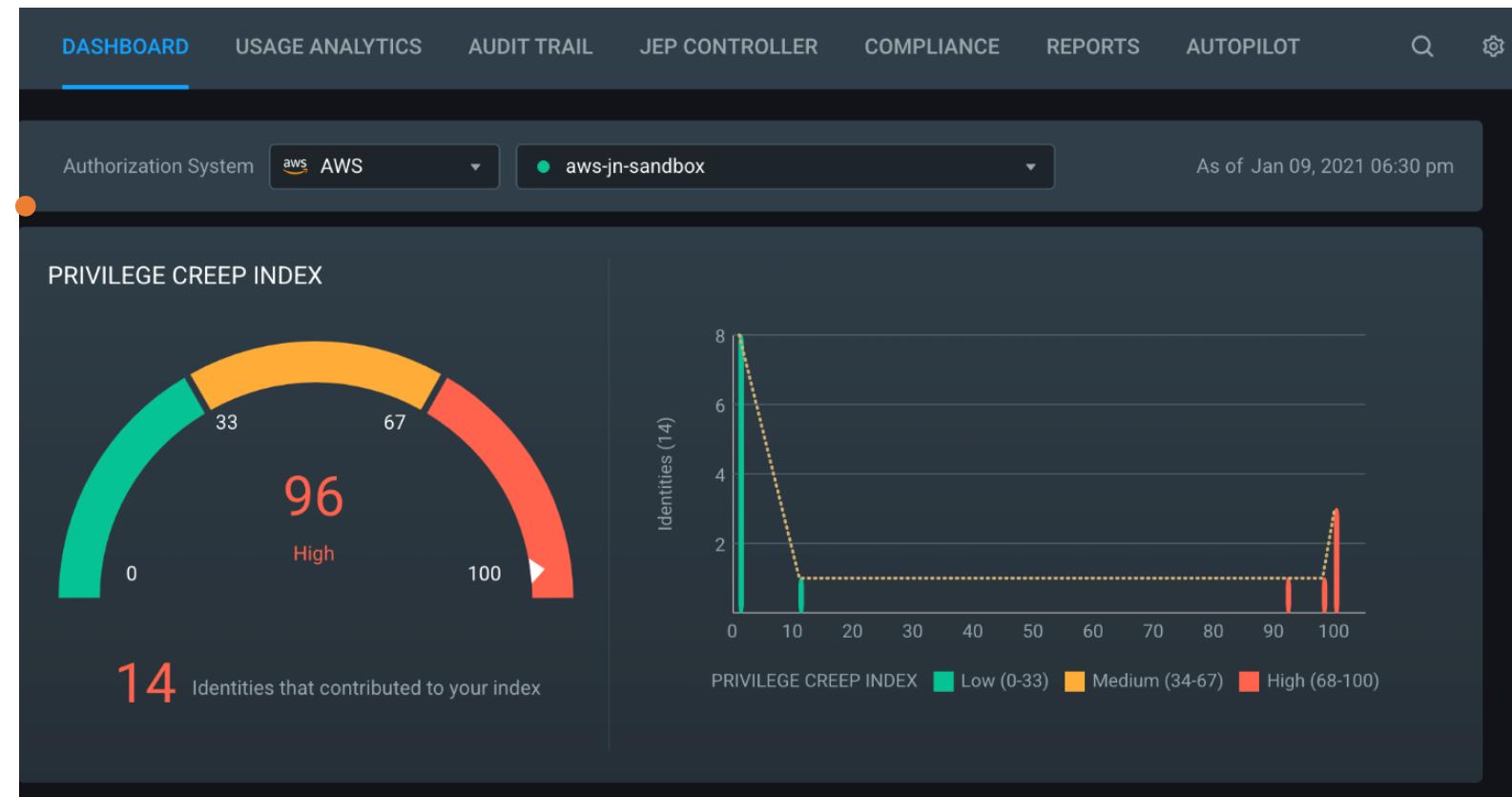
Back

Cloudknox (Entra Permission Management)

Are you sure
you are
running with
least-privilege?

Google Cloud
Amazon Web Services
Microsoft Azure

Keys
Access Keys
Service Principles
Managed Identities
Roles



Go to www.menti.com and use the code 4642 6287



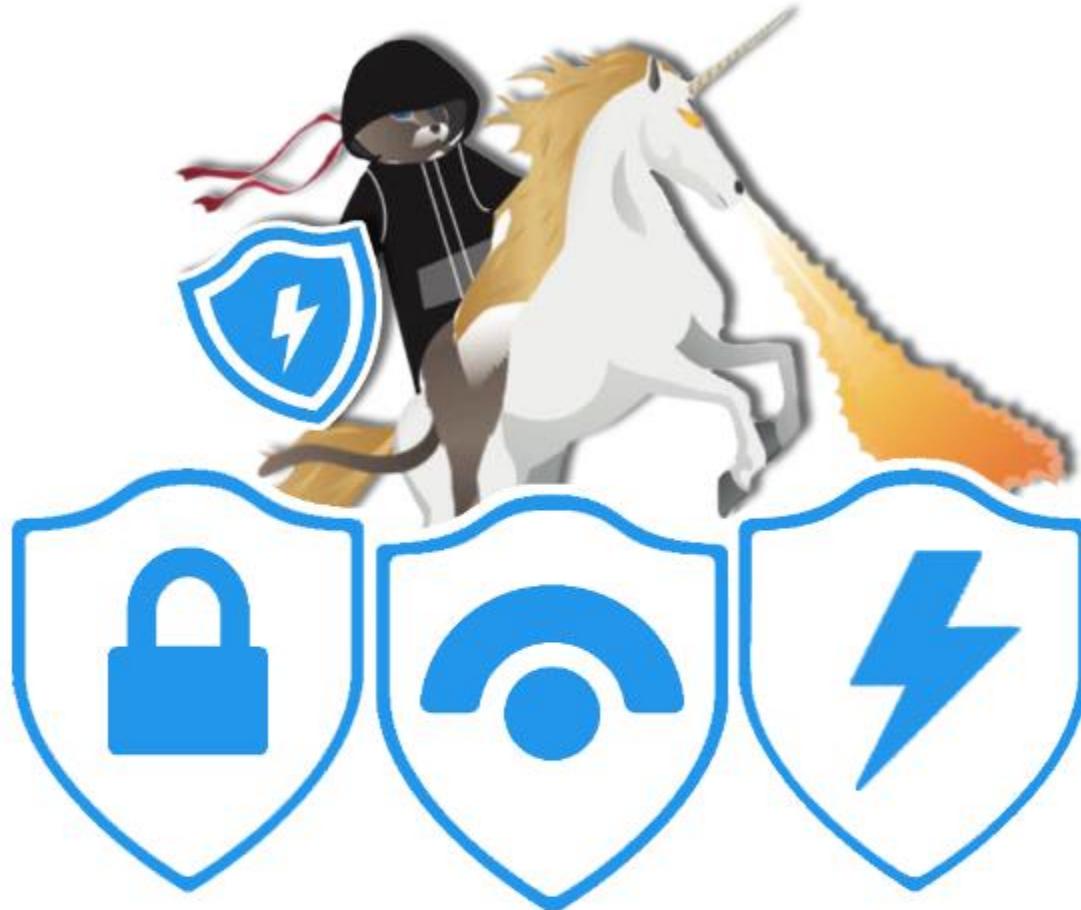
What topic would you want to hear about in our next Meetups ?



Microsoft Security
USER GROUP



15 Min
Break



Microsoft Security

USER GROUP



Ready, set, log ?

Part 1
Microsoft Security User Group



whoami

Kim Ytredal

- Information security industry for 13 years
 - Worked as a security analyst and security advisor
 - I love creating smart security solutions
 - Have multiple certifications

Hobbies

Breaking things, security, boating, politics, economics, bacon and beer



This session

- What does data logging mean?
- Which logs and metrics should we keep
- Some sources to consider
- How long should we keep logs
- When logs containing personal data
- Get data to log analytics (sentinel)
- Scenario 1 – Linux Agentless
- Scenario 2 – OMS gateway
- Scenario 3 – compliance
- Scenario 4 – The way ?
- Table, column, row, value
- Standard preliminary processing
- Log Health

What Does Data Logging Mean?

Data logging is the process of collecting and storing data over a period of time in order to analyze specific trends or record the data-based events/actions of a system, network or IT environment. It enables the tracking of all interactions through which data, files or applications are stored, accessed or modified on a storage device or application.



Which logs and metrics should we keep

- Planing

- What is the purpose and what is my mandate

Example:

We want to collect logs to uncover if someone is trying to steal our intellectual property

Which value chains and systems support ours intellectual property

Which logs can we retrieve from these systems

Is it sufficient to be able to detect leakage

- Forensics logs
- Analytics (detection) logs

Do we need more technology?

- Design

- Design your solution in accordance with legislation and internal controls

More on this on this later*

- Security and operations
 - Flexibility and robustness
 - Access Control
 - Timestamp unification across sources

Some sources to consider

Cloud solution activity logs

DNS

DHCP

Command line logs

PowerShell transactions

File auditing

File integrity changes

File name changes

Login failures

Malware attacks seen by IDS or other evidence

Malware detection

Modified registry values

New login events
New processes started or running processes stopped

New service installation

New user accounts

Password changes

Scans on your firewalls open and closed ports

Shared access events

Lateral network connections

Unauthorized logins

Etc.

How long should we keep logs

- It takes on average 212 days to identify a breach
 - In many cases, it is because we are notified by a third party
 - Cost of breach depends on
 - Business's size
 - Complexity
 - And most importantly, the threat actor's objective
- My recommendation is to store for at least a year



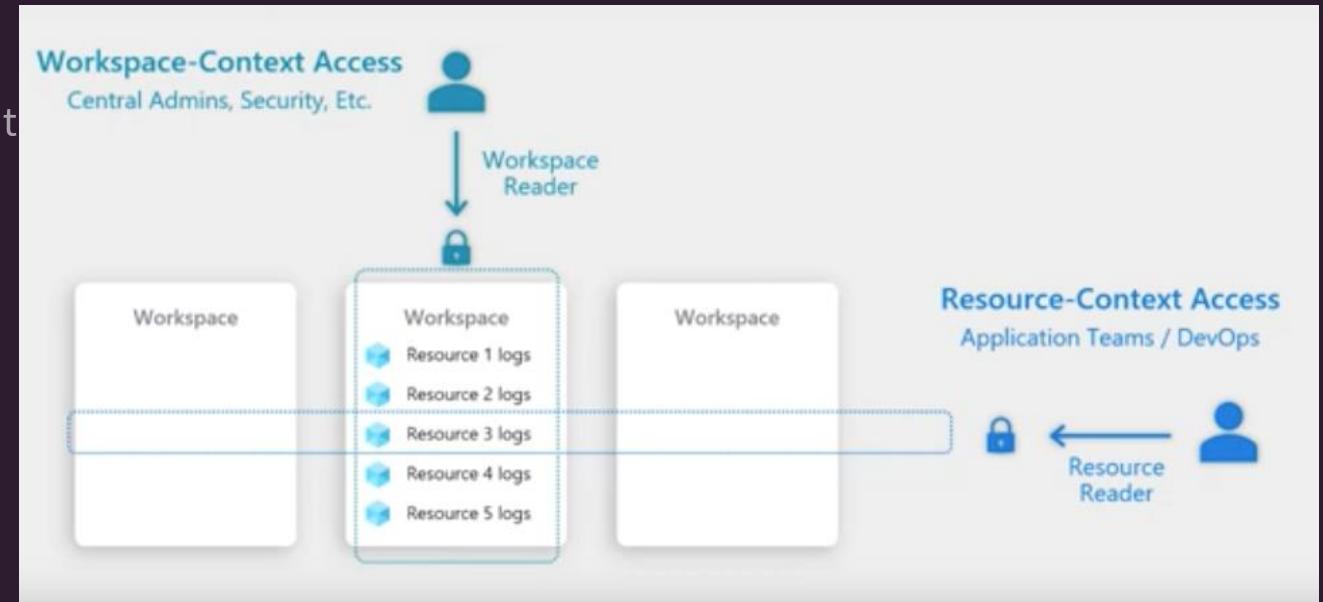
Small demo

- Set workspace retention
- Archive periode

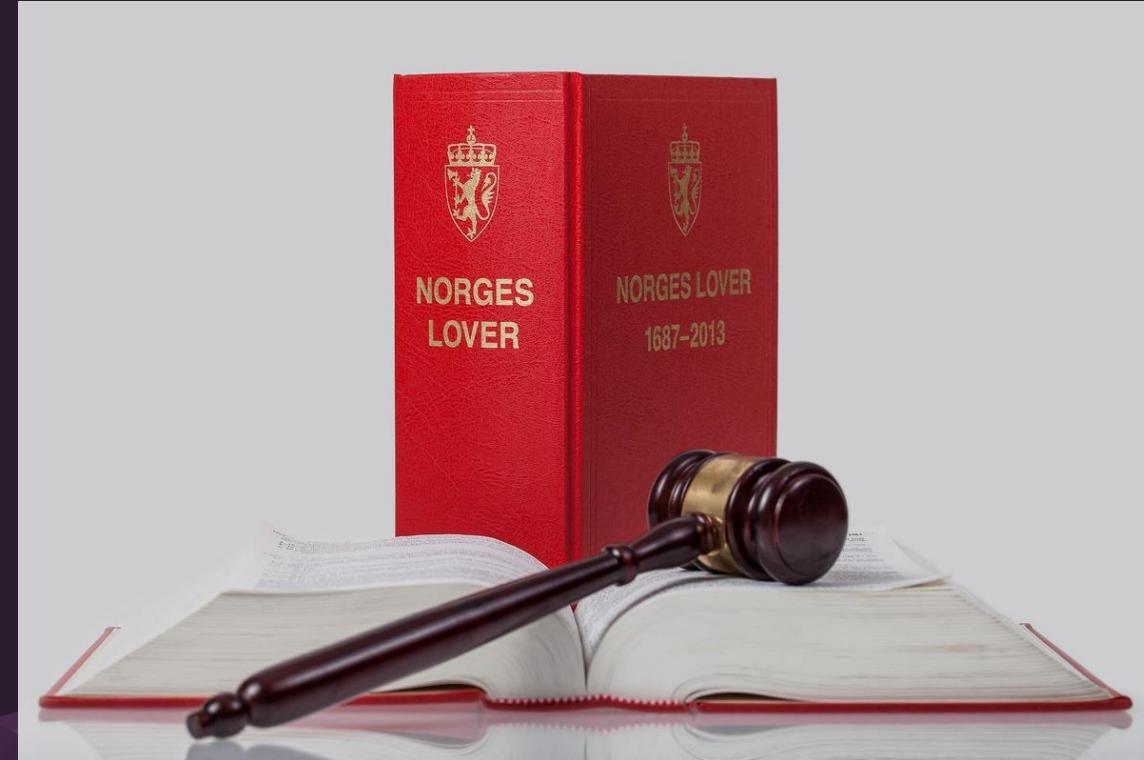


When logs containing personal data

- General Data Protection Regulation (GDPR)
 - Update or create data processing activities document “Behandlingsprotokoll”
 - Reflect what is processed and why
 - Data minimization of personal data
 - How long can we store with privacy in mind
 - Access control
 - Who watched what when (for log analytics this is LAQueryLogs)



Please note that there may be special legislation
that apply to you or your customer



Small demo

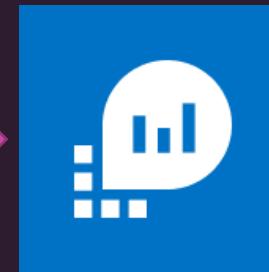
- Check log analytics access policy
- Activate LAQueryLogs



Collect security data from sources

- Office 365 and Azure
 - Security alerts, activity logs
- Collectors
 - Syslog, CEF, Windows, Linux
- Threat intel
 - MS Graph and Taxii
- API
 - Custom logs

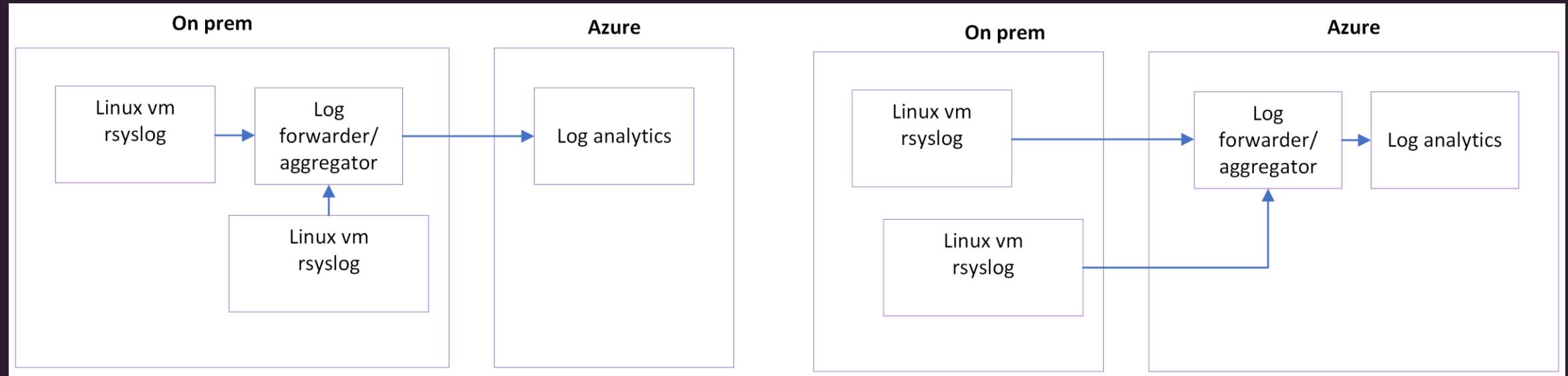
Log analytics



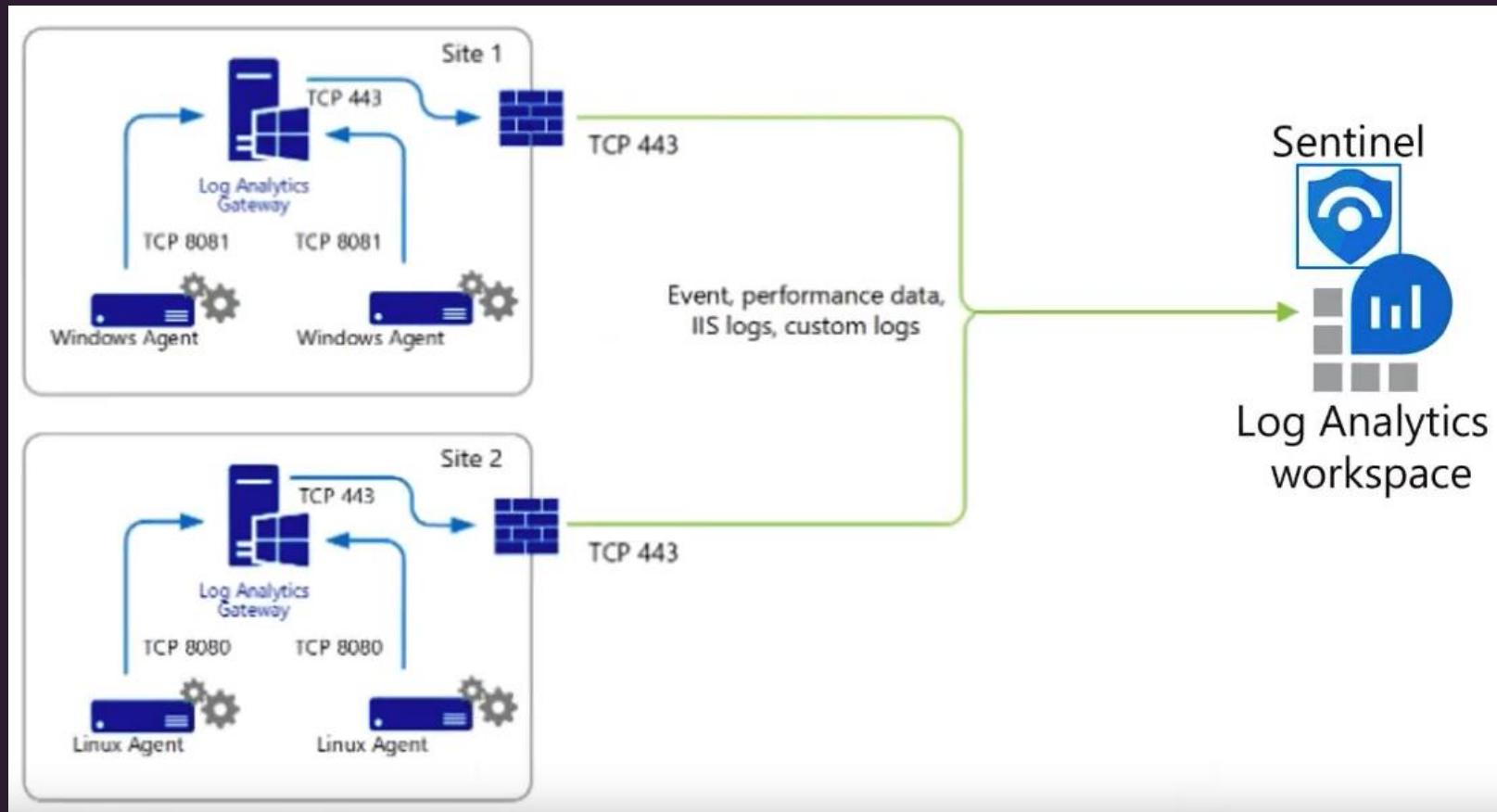
Get data to log analytics (sentinel)

Scenario	Solution
Filtered, transformed og aggregated	* Logstash * Other solutions
Filtered	* Logstash * Other solutions * AMA (Azure Monitoring Agent + data collection rules)
Agentless	* Syslog collection with upstream solution (logstash) * Windows (was on roadmap)
System without direct internet access	* OMS gateway * Other intermediate solutions (like logstash)
Multiple log analytics – Security and operations	* MMA (Microsoft Monitoring Agent) (Switch to AMA if possible) * AMA (Azure Monitoring Agent + data collection rules) -With multiple destinations
Custom logs	* Logstash * Other solutions
Office 365, Microsoft 365 Defender, etc	Data connectors in sentinel

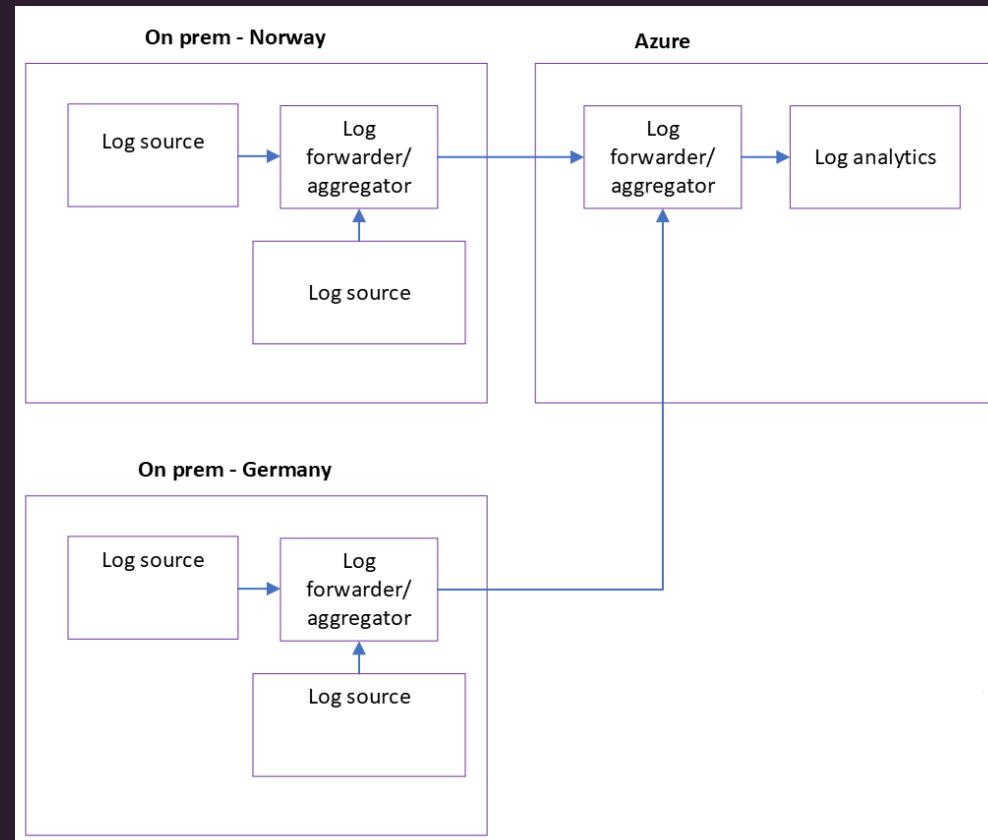
Scenario 1 – Linux Agentless



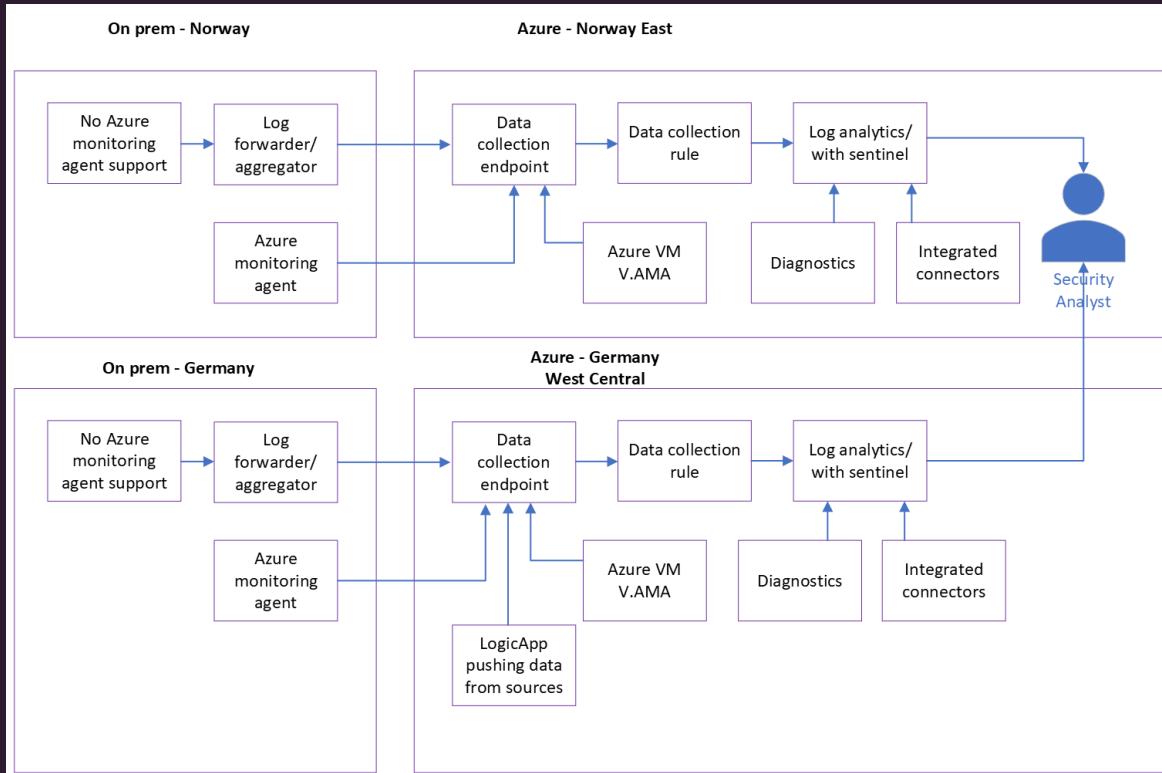
Scenario 2 – OMS gateway



Scenario 3 – Compliance



Scenario 4 - The way ?



- * Helpful with multi tenant
- * works with lighthouse

Screenshot of the Microsoft Sentinel portal showing a search view for the "log-sentinel-demo-eno-01" resource group. The interface includes:

- Header: Microsoft Sentinel, forsec (forsec.no)
- Toolbar: Create, Manage view, Refresh, Export to CSV, Open query, View incidents
- Filter bar: Filter for any field..., Subscription equals all, Resource group equals all, Location equals all, Add filter
- Search results table:
 - Name: log-sentinel-demo-eno-01 (selected)
 - Resource group: rg-sentinel-demo-eno (selected)

Table, column, row, value

Table

Row

Column

TimeGenerated[UTC]	Col 2	Col 3	Col 4
Value			



Standard preliminary processing

Action	What	Why
Filtering	Columns Values Row	<ul style="list-style-type: none">• Remove sensitive data• Only relevant data• Cost reduction
Transformation	Values	<ul style="list-style-type: none">• Masking sensitive data
Aggregation	statistics over -values	<ul style="list-style-type: none">• Cost reduction• Faster querying
Table unification - (A)SIM	Normalized schema - Column names	<ul style="list-style-type: none">• Easier to query across tables• Easier to document and learn

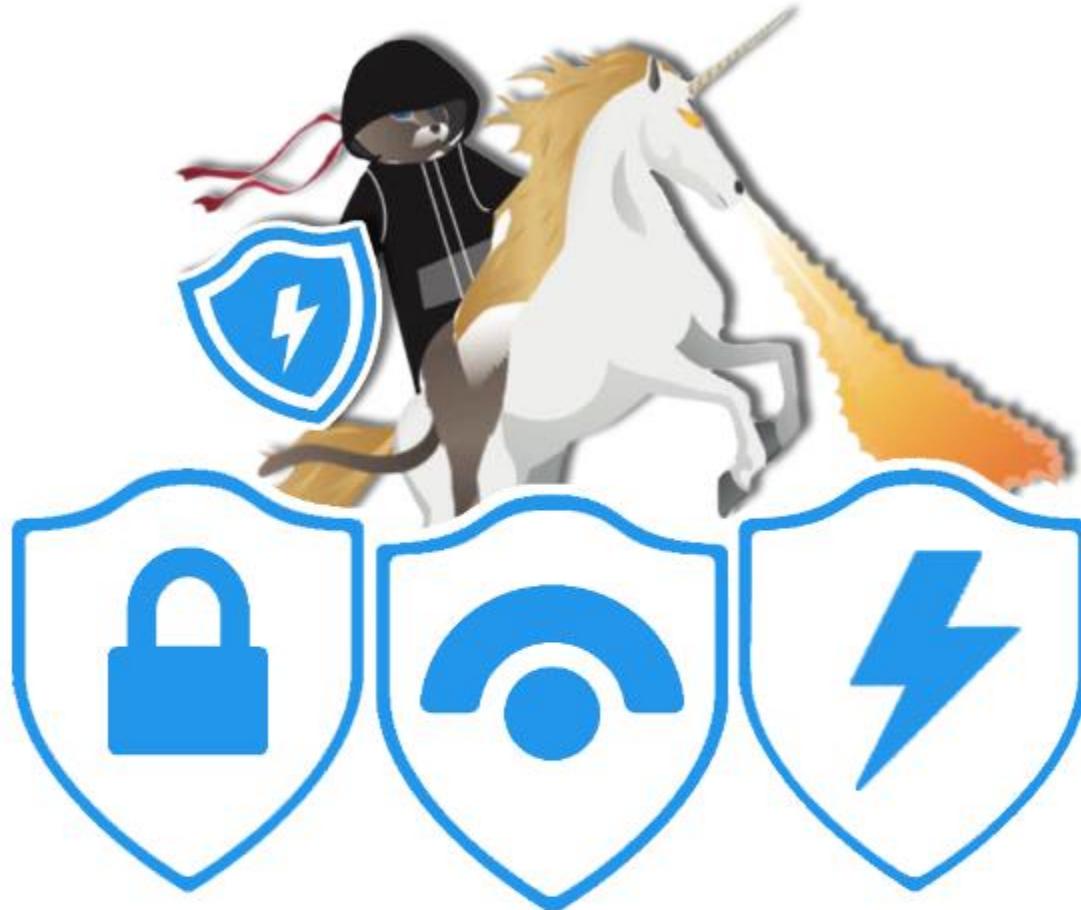
Log Health

- Log ingestion
 - Drop
 - Decrease
 - Increase
 - Missing endpoints
- System upgrades can change column names
- Column errors



The end of part 1





Microsoft Security

USER GROUP

