Microsoft Security

USER GROUP NORWAY

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Welcome to Microsoft Sentinel 1-2-3

By Sanna Diana

Sanna Diana Tomren

Assosiate Manager,
Cloud Security Lead Norway,
Accenture

Sanna Diana Tomren

@sanna_diana

sanna-diana.medium.com

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Microsoft Sentinel 1-2-3 Agenda

Security Operations and Challenges

Microsoft Sentinel and Log Analytics

Design and Architecture

Sentinel in context – Legacy vs. Cloud-native

Sentinel Deployment

AI, ML and Automation

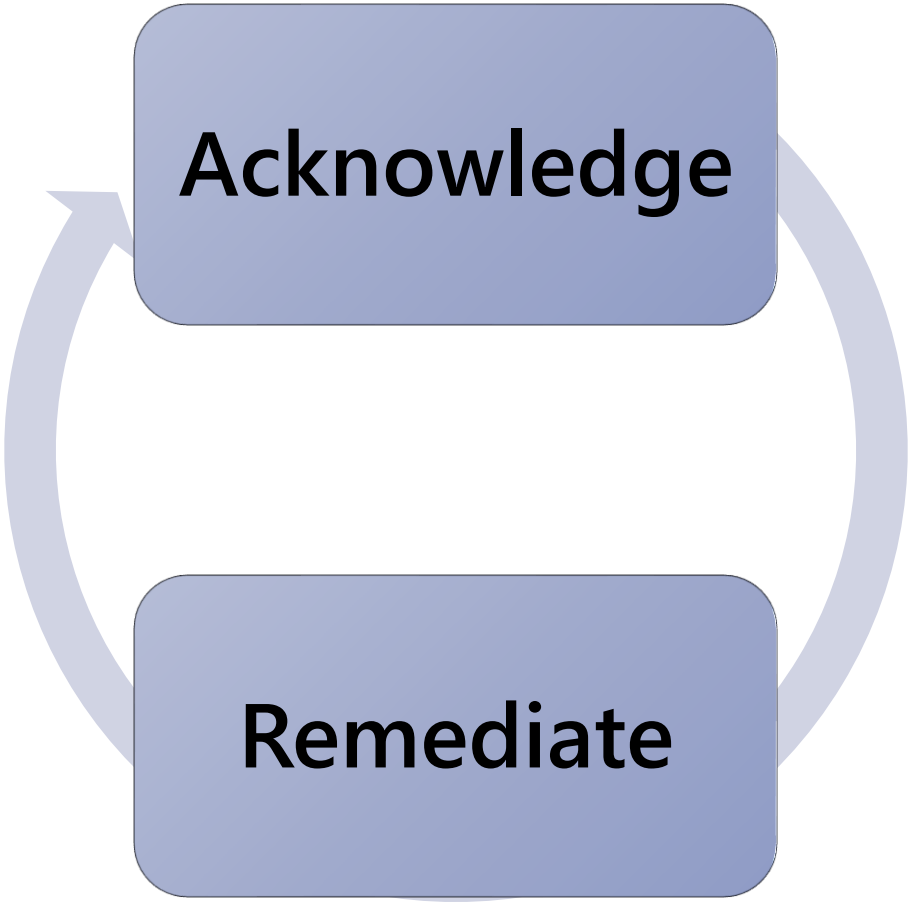
Investigation and Hunting

Technology, Processes and People

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Security Operations



Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Security operations challenges

Sophistication of threats

IT deployment and maintenance

76%
report increasing security data*

44%
of alerts are never investigated*

Too many disconnected products

3.5M
unfilled security jobs in 2021**

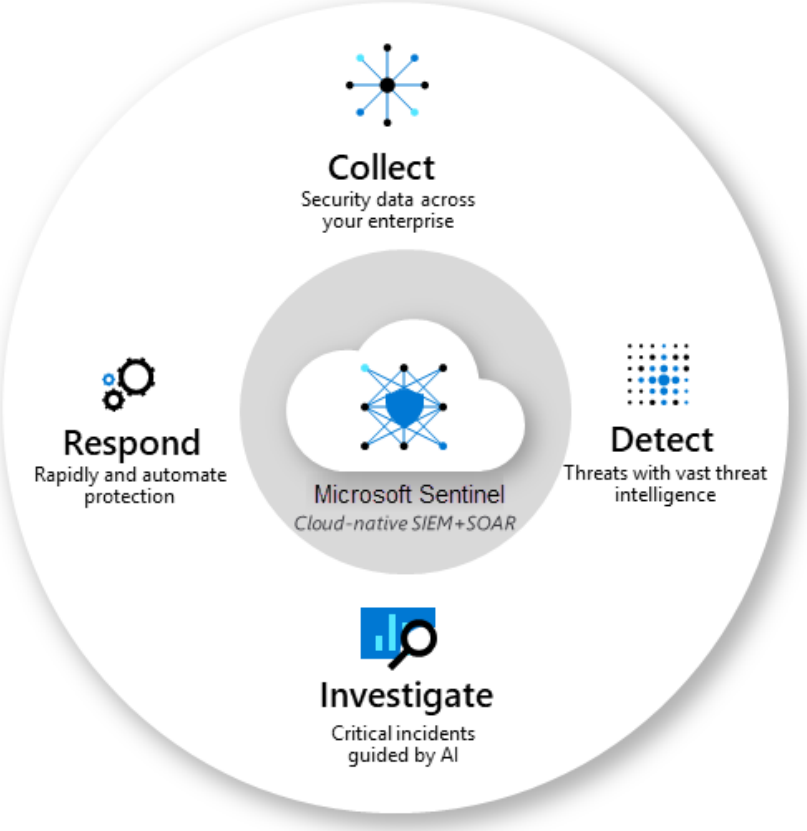
Lack of automation

*ESG: Security Analytics and Operations: Industry Trends in the Era of Cloud Computing 2019
**CSO Magazine

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

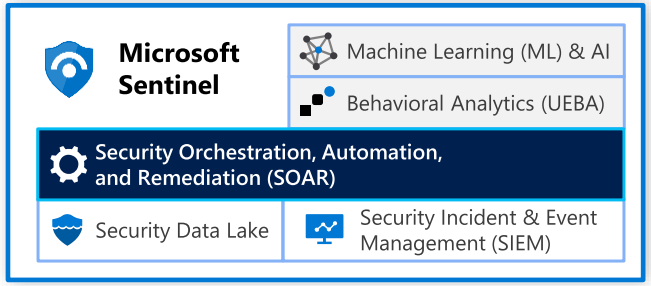
Microsoft Sentinel

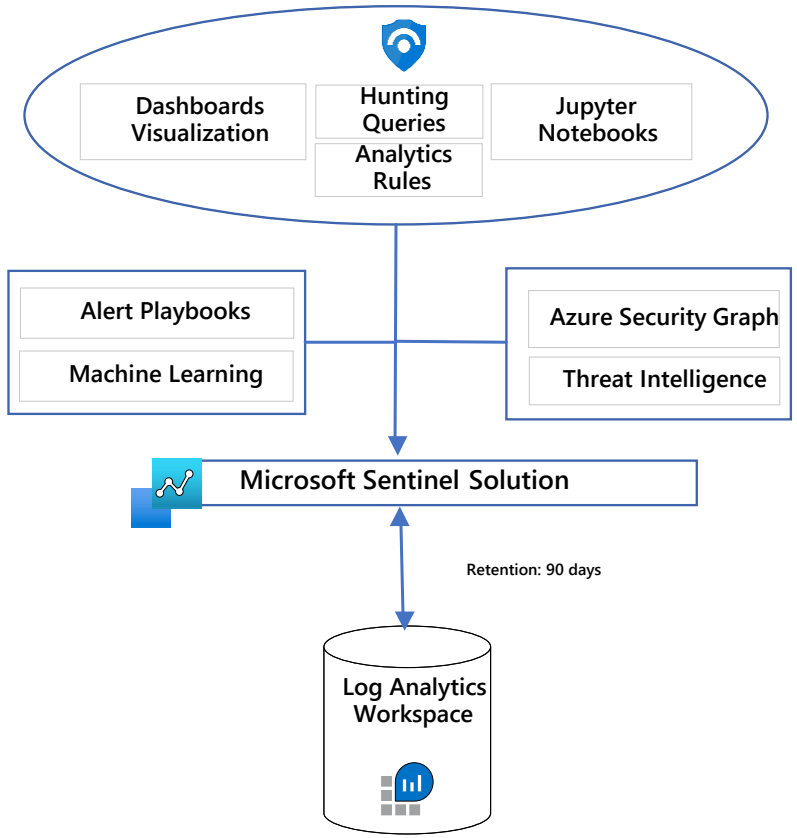


Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Sentinel & Log Analytics

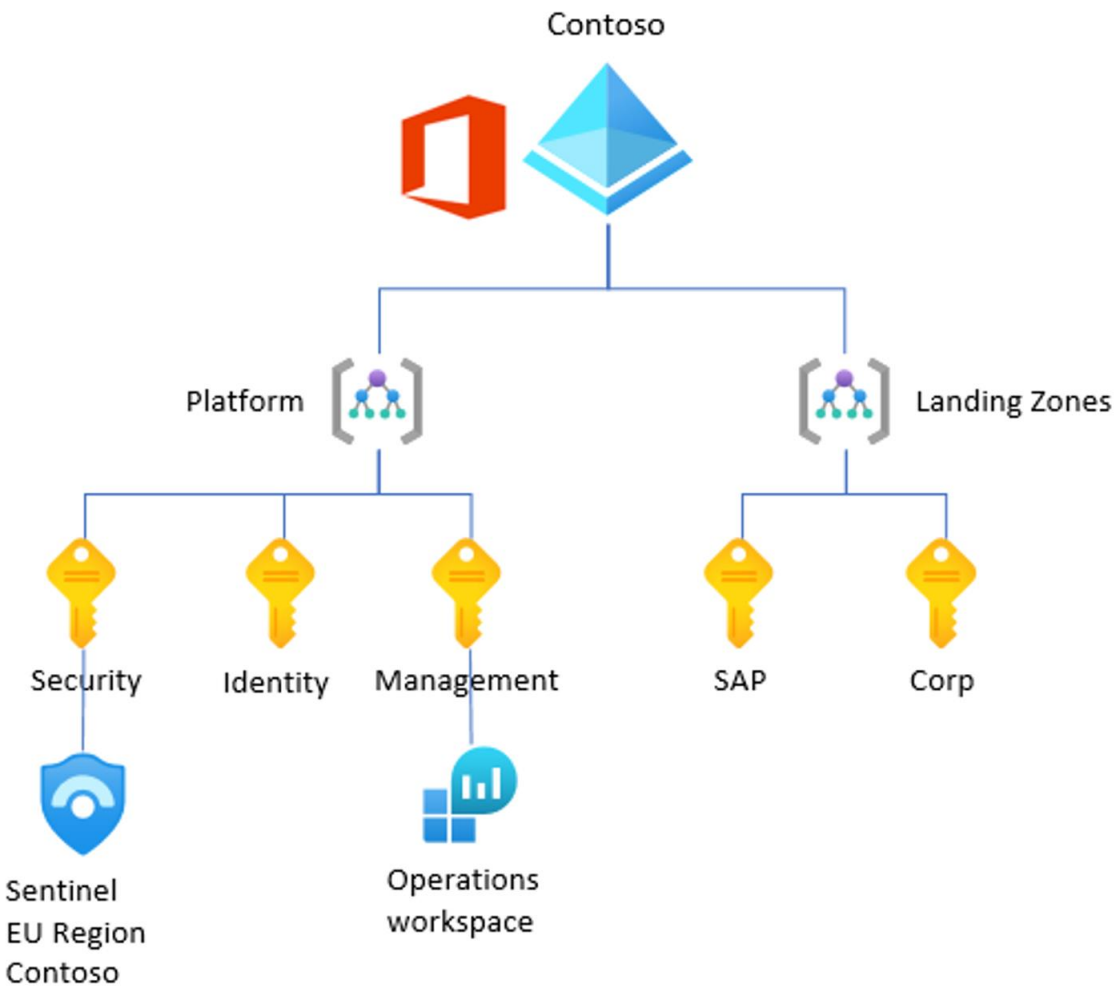


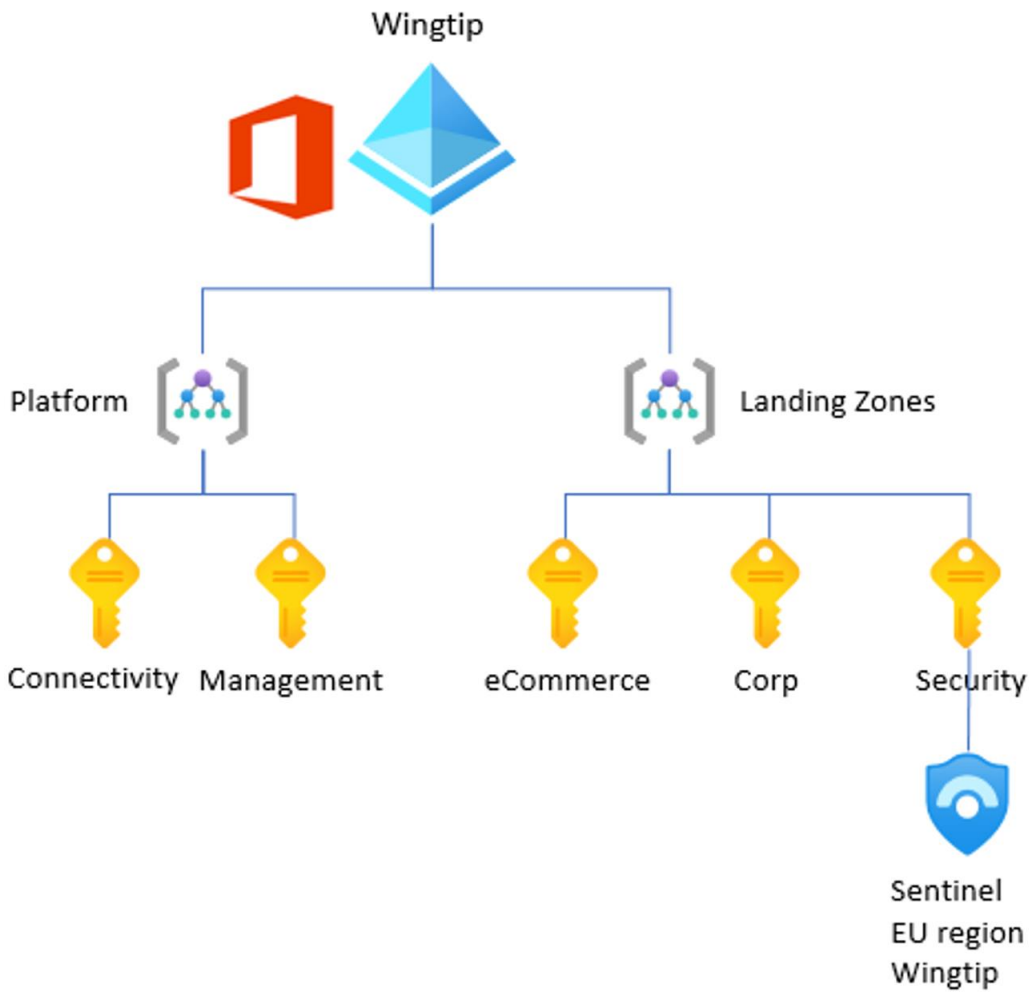


Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

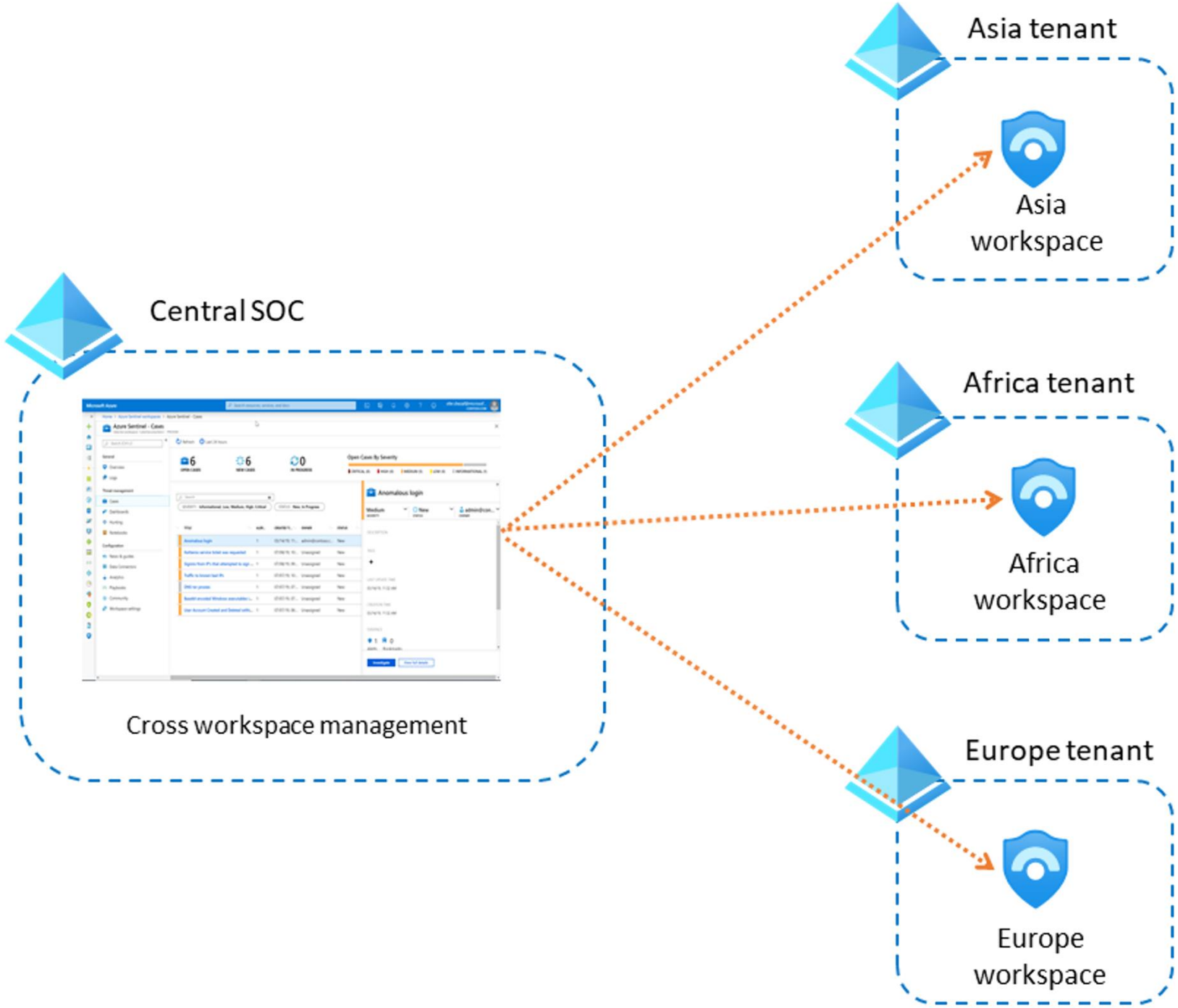
Design





Microsoft Security
USER GROUP NORWAY

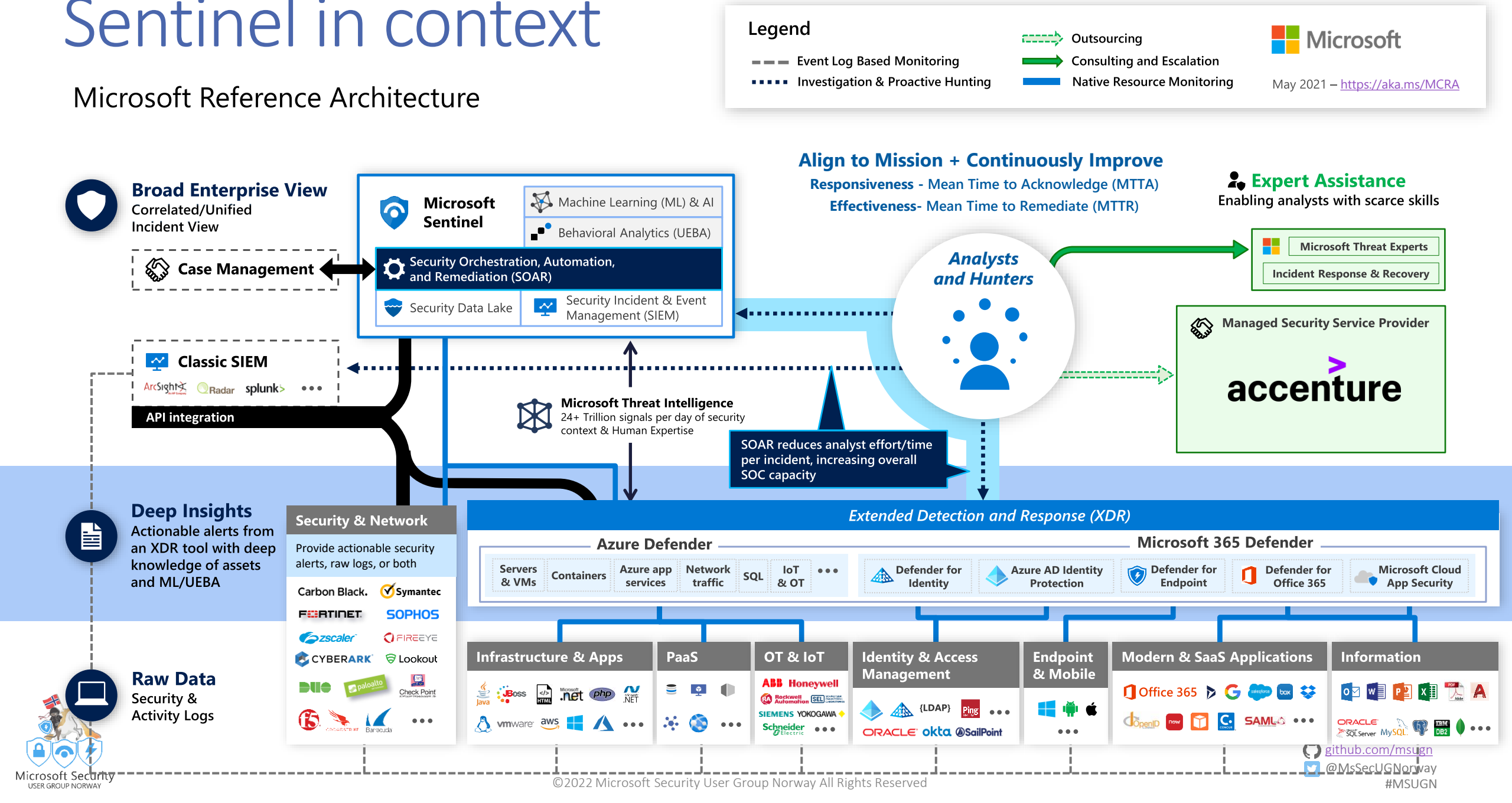
github.com/msugn
@MsSecUGNorway
#MSUGN



Microsoft Security
USER GROUP NORWAY

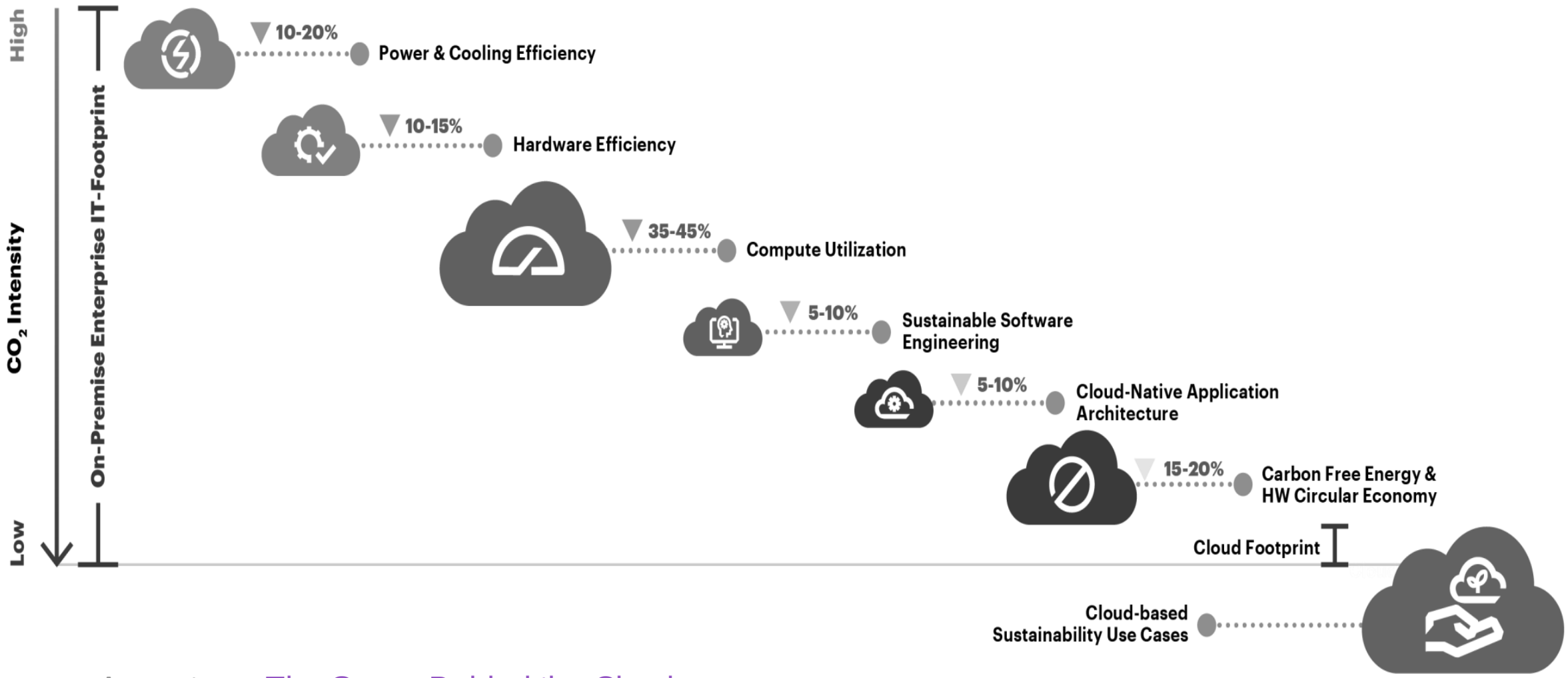
Sentinel in context

Microsoft Reference Architecture



Legacy vs. Cloud-native

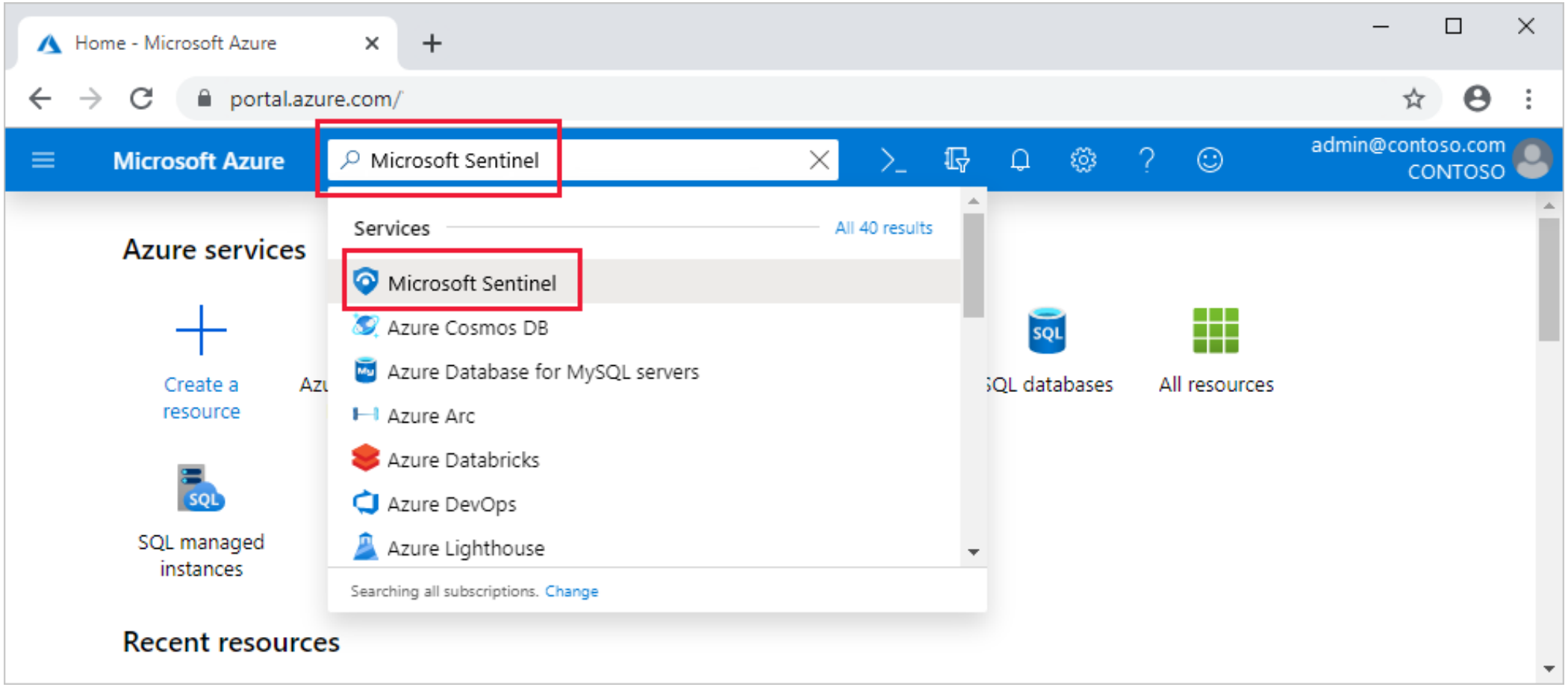
Legacy SIEM operation challenges	Cloud-native SIEM & SOAR capabilities
Good coverage of on-premises assets, on-premises architectures may have insufficient coverage for cloud assets	Can ingest data from both on-premises and cloud assets, ensuring coverage over the entire estate
Slow response to threats	Tuned and up to date environment
Scaling challenges	Collects data automatically and at scale
Manual analysis and response	Detects unknown threats, investigates threats with artificial intelligence, and responds to incidents rapidly with built-in automation
Complex and inefficient management	Continuously Improved



Accenture, The Green Behind the Cloud

Deployment

Deployment



Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Alternate deployment / management options:

1

Deploy Microsoft Sentinel via ARM template

2

Manage Microsoft Sentinel via API

3

Manage Microsoft Sentinel via PowerShell

Microsoft Security
USER GROUP NORWAY

Onboard Data

Microsoft Sentinel | Data connectors

Selected workspace: 'redmondsentineldemoenvironment'

Search (Ctrl+/)

Guides & Feedback Refresh

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics
- Watchlist (Preview)
- Playbooks
- Solutions (Preview)
- Community
- Settings

97 Connectors 15 Connected 0 Coming soon

Search by name or provider Providers : **All** Data Types : **All** Status : **All**

Status	Connector name
	Agari Phishing Defense and Brand Protection (Preview) Agari
	AI Analyst Darktrace (Preview) Darktrace
	AI Vectra Detect (Preview) Vectra AI
	Akamai Security Events (Preview) Akamai
	Alcide kAudit (Preview) Alcide
	Alsid for Active Directory (Preview) Alsid
	Amazon Web Services Amazon
	Apache HTTP Server (Preview) Apache

AI Vectra Detect (Preview)

Not connected	Vectra AI	--
Status	Provider	Last Log Received

Description

The AI Vectra Detect connector allows users to connect Vectra Detect logs with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation. This gives users more insight into their organization's network and improves their security operation capabilities.

Last data received

--

Author

Vectra AI

Supported by

Vectra AI

Version

1.0

Related content

1 Workbooks 4 Queries 0 Analytic rules templates

Open connector page

Azure Active Directory
PREVIEW

Azure Active Directory

Connected	Microsoft	11 minutes ago
STATUS	PROVIDER	LAST LOG RECEIVED

DESCRIPTION

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your SSPR usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

LAST DATA RECEIVED

07/03/19, 01:37 PM

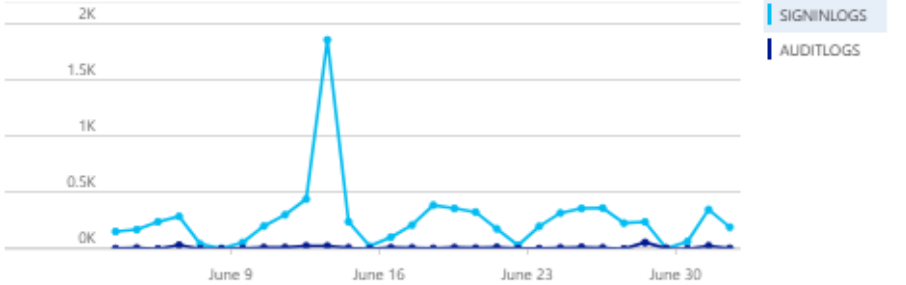
RELATED CONTENT

2 Dashboards

2 Queries

DATA RECEIVED

Go to log analytics



Total data received
7.99 K

Total data received
306

DATA TYPES

SigninLogs 07/03/19, 01:36 PM

AuditLogs 07/03/19, 01:37 PM

Instructions Next steps

Prerequisites

To integrate with Azure Active Directory make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Diagnostic Settings:** required read and write permissions to AAD diagnostic settings.
- ✓ **Resource provider registration:** your subscription '44e4eff8-1fcb-4a22-a7d6-992ac7286382' needs to be registered to resource provider 'Microsc
- 🔒 **Tenant Permissions:** required 'Global Admin' and 'Security Admin'.
- 🔒 **License:** required AAD P1/P2.

Configuration

Connect Azure Active Directory logs to Microsoft Sentinel
Select Azure Active Directory log types:

Azure Active Directory Sign-in logs Disconnect

Azure Active Directory Audit logs Disconnect

Microsoft Sentinel – Github

The following table summarizes permissions, licenses and permissions needed and related cost to enable each Data Connector:

Data Connector	License	Permissions	Cost
Azure Activity	None	Subscription Reader	Free
Azure Defender	ASC Standard	Security Reader	Free
Azure Active Directory	Any AAD license	Global Admin or Security Admin	Billed
Azure Active Directory Identity Protection	AAD Premium 2	Global Admin or Security Admin	Free
Office 365	None	Global Admin or Security Admin	Free
Microsoft Cloud App Security	MCAS	Global Admin or Security Admin	Free
Microsoft Defender for Identity	AATP	Global Admin or Security Admin	Free
Microsoft Defender for Endpoint	MDATP	Global Admin or Security Admin	Free
Threat Intelligence Platforms	None	Global Admin or Security Admin	Billed
Security Events	None	None	Billed
Linux Syslog	None	None	Billed
DNS (preview)	None	None	Billed
Windows Firewall	None	None	Billed

Microsoft 365 Defender connector is currently in **PREVIEW**

Incident integration

Bi-directional sync, also referred to as a two-way sync

Microsoft Sentinel's Microsoft 365 Defender incident integration allows you to stream all Microsoft 365 Defender incidents into Microsoft Sentinel and keep them synchronized between both portals.

Analytics

Home > Microsoft Sentinel workspaces > Microsoft Sentinel

Microsoft Sentinel | Analytics

Selected workspace: 'contoso77'

Search (Ctrl+/)

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks (Preview)
- Entity behavior analytics (Preview)

Configuration

- Data connectors
- Analytics
- Playbooks
- Community
- Settings

Create | Refresh | Enable | Disable | Delete

116 Active rules

Rules by severity

High (8) | Medium (64) | Low (41) | Informational (3)

Active rules | **Rule templates**

Search | Severity : All | Rule Type : All | Tactics : All | Data Sources : All

SEVERITY	NAME	RULE TYPE	DATA SOURCES	TACTICS
Medium	IN USE Cisco - firewall block but success logon to Azure AD	Scheduled	Cisco ASA +1	Initial Access
Medium	(Preview) TI map IP entity to AzureActivity	Scheduled	Threat Intelligence Platforms (Pr... +1	Impact
Medium	IN USE (Preview) TI map URL entity to PaloAlto data	Scheduled	Palo Alto Networks +1	Impact
Medium	(Preview) TI map Domain entity to PaloAlto	Scheduled	Palo Alto Networks +1	Impact
Medium	IN USE (Preview) TI map Email entity to SigninLogs	Scheduled	Threat Intelligence Platforms (Pr... +1	Impact
Medium	IN USE (Preview) TI map URL entity to SecurityAlert data	Scheduled	Microsoft Cloud App Security +2	Impact
Medium	(Preview) TI map File Hash to CommonSecurityLog Event	Scheduled	Palo Alto Networks +1	Impact
Medium	(Preview) TI map Email entity to SecurityAlert	Scheduled	Azure Security Center +1	Impact
Medium	IN USE (Preview) Anomalous SSH Login Detection	ML Behavior Analytics	Syslog	Initial Access
Medium	(Preview) TI map Email entity to CommonSecurityLog	Scheduled	Palo Alto Networks +1	Impact
Medium	(Preview) TI map File Hash to Security Event	Scheduled	Security Events +1	Impact
Medium	(Preview) TI map Domain entity to DnsEvent	Scheduled	DNS (Preview) +1	Impact
Medium	IN USE (Preview) TI map IP entity to AWSCloudTrail	Scheduled	Threat Intelligence Platforms (Pr... +1	Impact
Medium	IN USE (Preview) TI map URL entity to AuditLogs	Scheduled	Azure Active Directory +1	Impact

< Previous | 51 - 100 | Next >

(Preview) TI

Medium
Severity

Description
Identifies a match in D

Data sources
DNS (Preview)
DnsEvents 08/10/

Threat Intelligence Platf
ThreatIntelligenceIn

Tactics
Impact

Rule query

```
let dt_lookBac
let ioc_lookBa
//Create a lis
let list_tlds
```

Note:
- You haven't analytic rule
- One or more might limit t

Create rule

Microsoft Sentinel - Overview
Selected workspace: contoso

Search (Ctrl+/)

General
- Overview
- Logs
- News & guides

Threat management
- Incidents
- Workbooks
- Hunting
- Notebooks

Configuration
- Data connectors
- Analytics
- Playbooks
- Community
- Workspace settings

Refresh | Last 24 hours

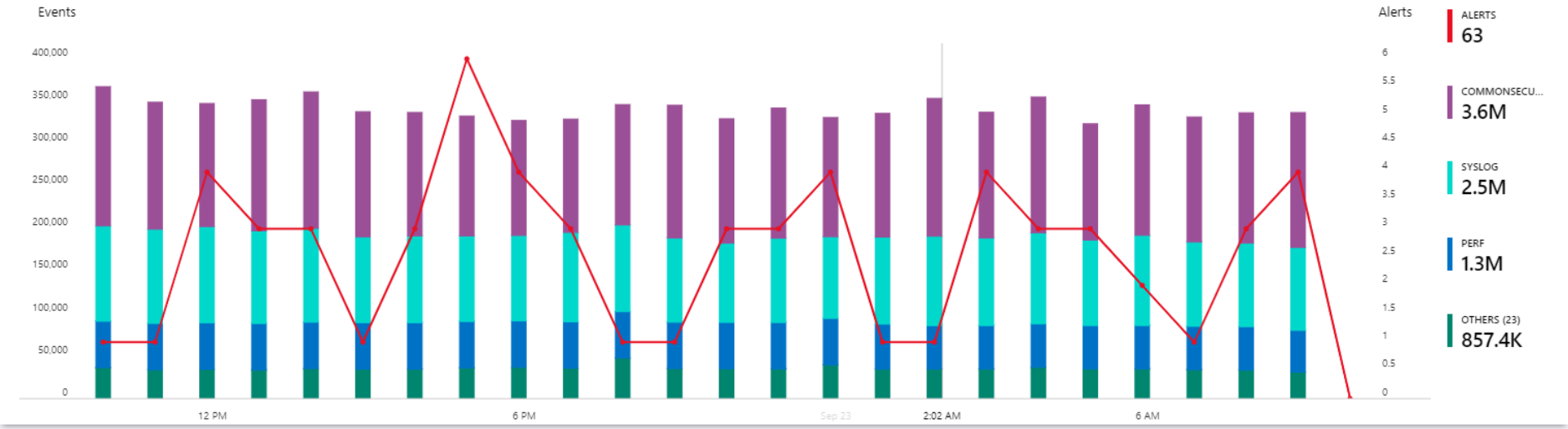
8.2M 7.9K
Events

63 1
Alerts

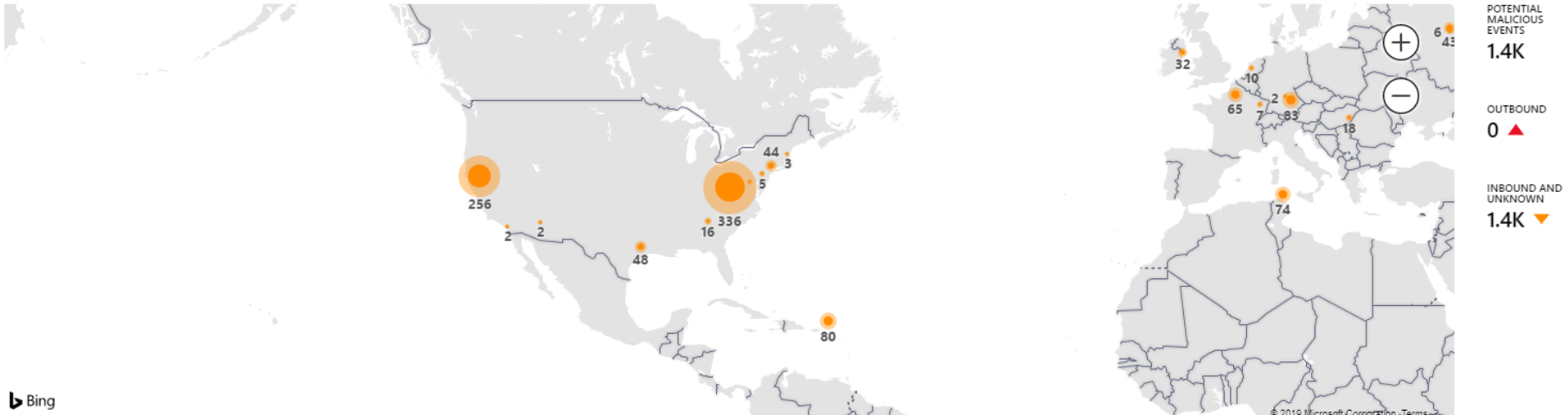
160 35
Incidents

INCIDENTS BY STATUS
NEW (158) IN PROGRESS (2) CLOSED (TRUE POSITIVE) (2) CLOSED (FALSE POSITIVE) (1)

Events and alerts over time



Potential malicious events



Recent incidents

- Alert
- Time Series Anomaly detection for T
- Investigation
- Time Series Anomaly detection
- Suspicious heartbeat events

Data source anomalies

AzureActivity

AzureDiagnostics

Democratize ML for your SecO

Unlock the power of AI for s
leveraging MS cutting edge
ML, regardless of your curre

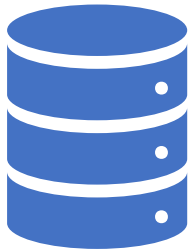
Learn More >

AI, ML & Automation

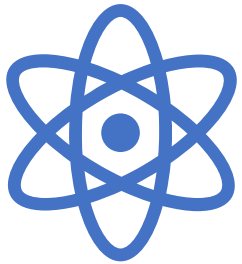
Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

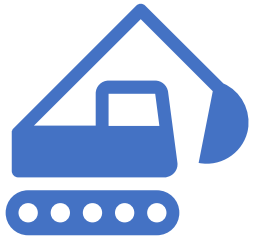
Reducing security alert fatigue using Machine Learning (ML) & AI



Built-in ML



Fusion



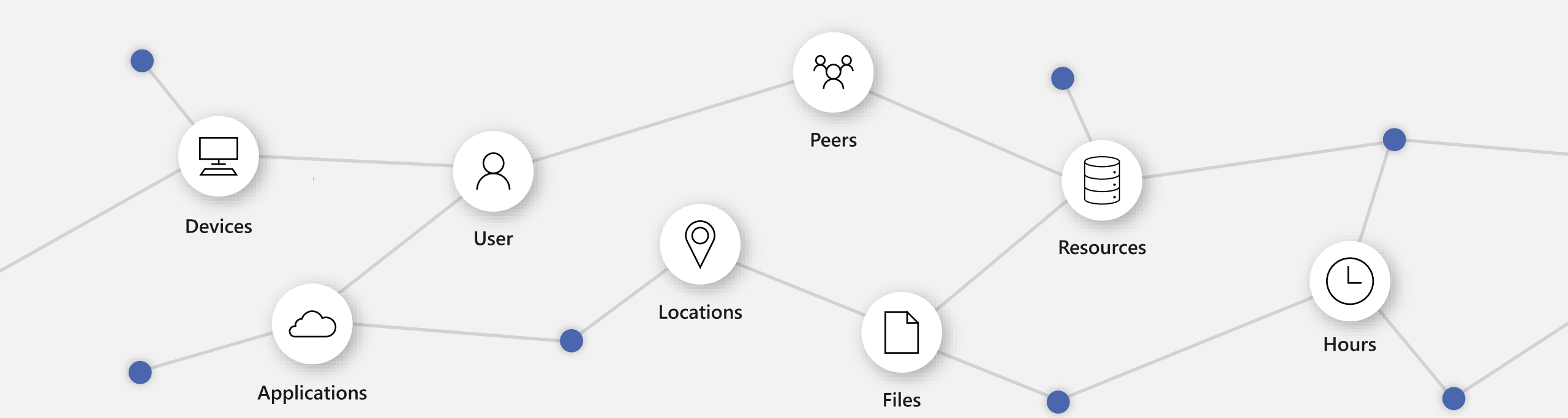
Build-your-own ML

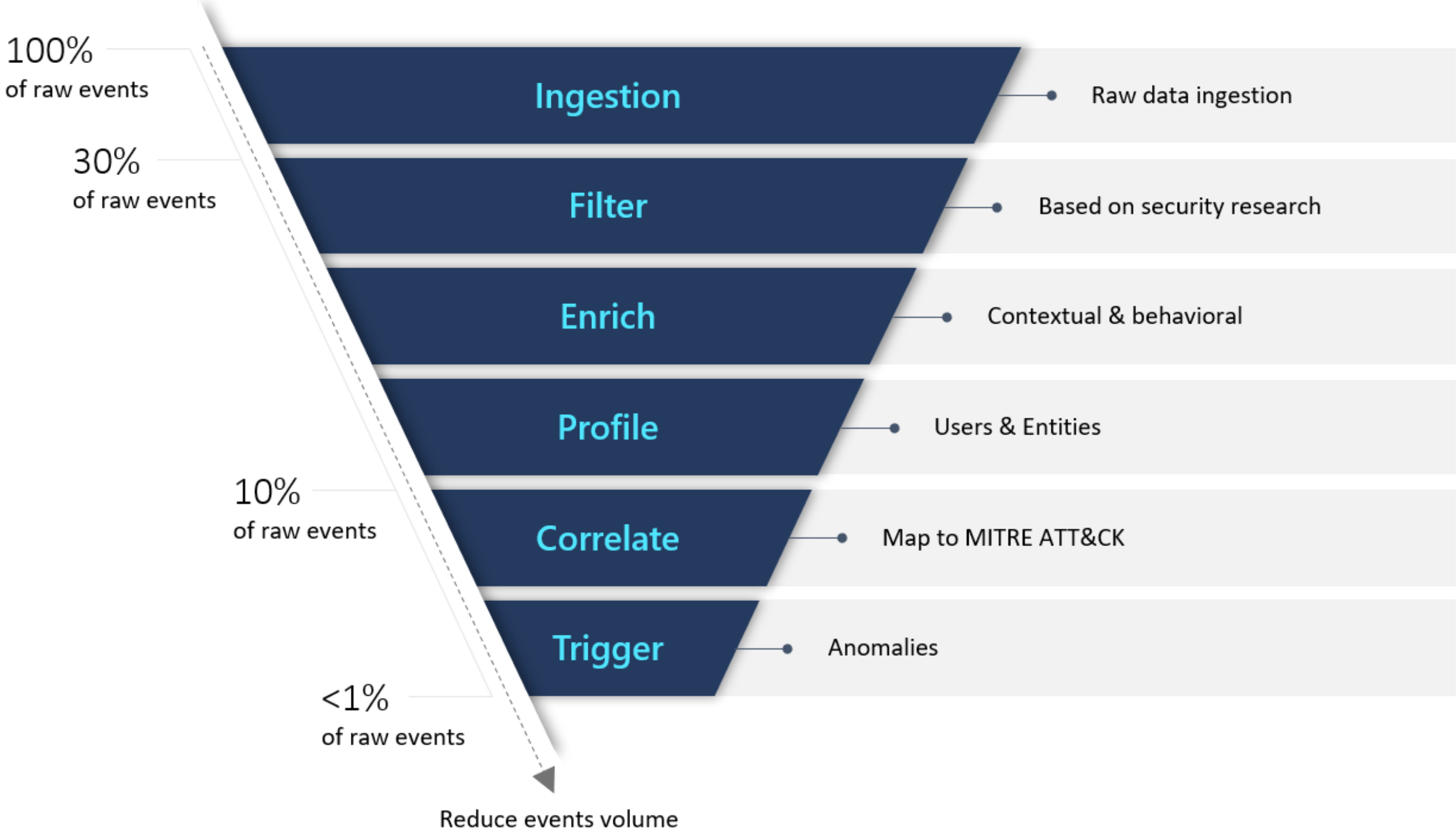
Microsoft Security
USER GROUP NORWAY

Built-in ML

User Entity Behavior Analytics (UEBA) solutions use analytics to **build the standard profiles** and behaviors of users and entities (hosts, applications, network traffic and data repositories) **across time and peer group horizons**. Activity that is anomalous to these standard baselines is presented as suspicious.

Gartner




100%
of raw events
30%
of raw events
10%
of raw events
<1%
of raw events
Ingestion
Filter
Enrich
Profile
Correlate
Trigger
Raw data ingestion
Based on security research
Contextual & behavioral
Users & Entities
Map to MITRE ATT&CK
Anomalies
Reduce events volume

Fusion

- Microsoft Sentinel uses the **Fusion correlation engine**
- Fusion is enabled by default in Azure Sentinel, as an analytics rule called ***Advanced multistage attack detection.***
- The Fusion engine can also correlate alerts produced by scheduled analytics rules with those from other systems
- Analytics rules must contain kill-chain (tactics) and entity mapping information in order to be used by Fusion.

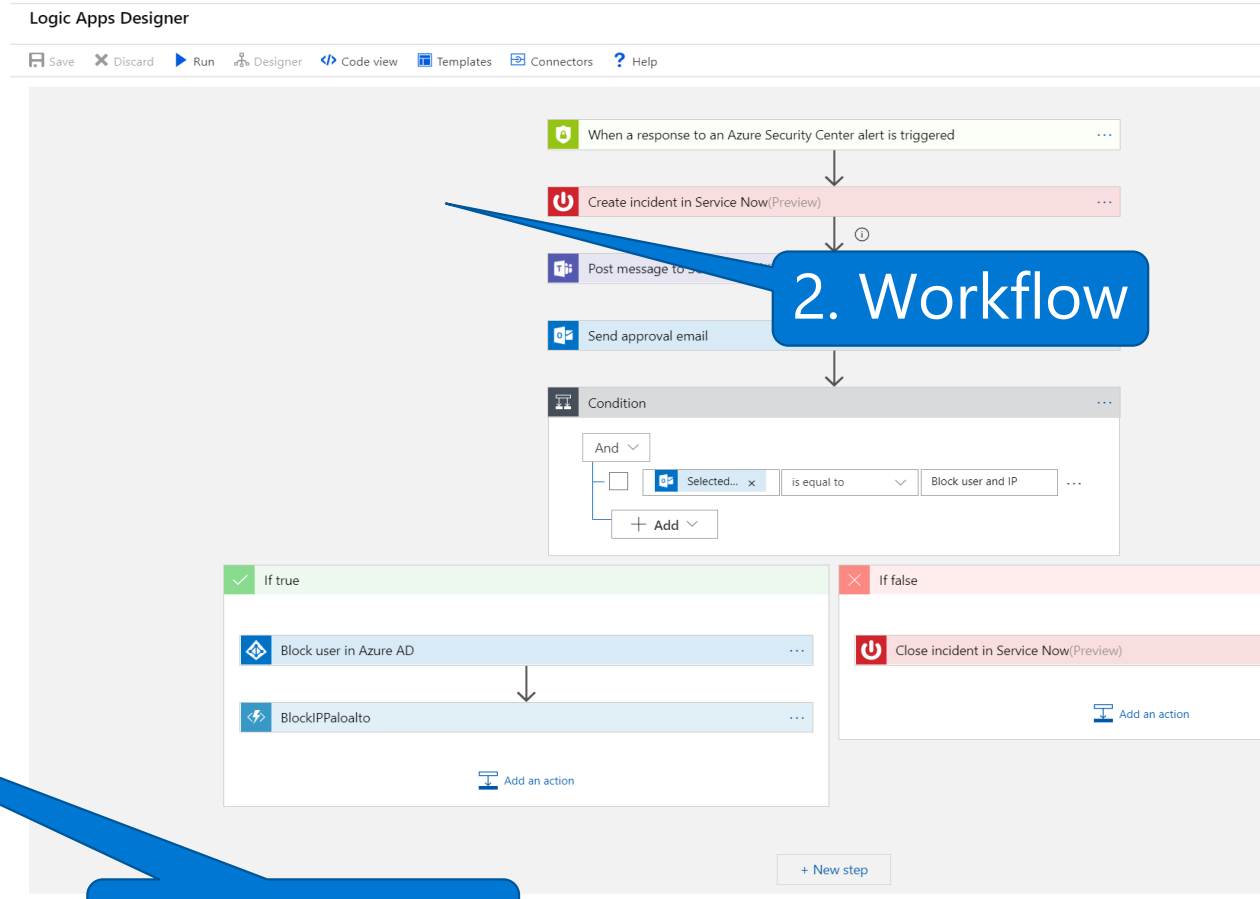
Build-your-own ML

- Microsoft Sentinel offers Databricks, Spark, and Jupyter Notebook and introduce seamless model management, model deployment, workflow scheduler, data versioning capabilities and specialized security analytics libraries.

Automation

Security Orchestration, Automation, and Remediation (SOAR)

1. Integration



2. Workflow

3. Response

Example playbooks

Incident Management

Assign an Incident to an Analyst

Open a Ticket (ServiceNow/Jira)

Keep Incident Status in Sync

Post in a Teams or Slack Channel

Enrichment + Investigation

Lookup Geo for an IP

Trigger Defender ATP Investigation

Send Validation Email to User

Remediation

Block an IP Address

Block User Access

Trigger Conditional Access

Isolate Machine

Investigation

Home > Microsoft Sentinel > Microsoft Sentinel > Incident

Investigation

Undo Redo

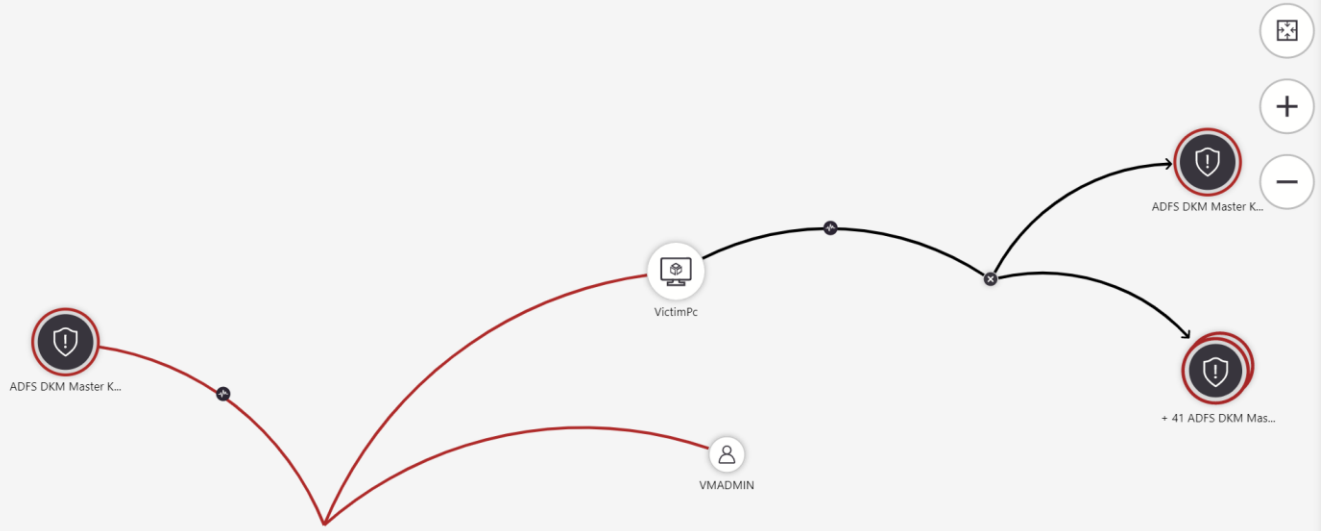
ADFS DKM Master Key Export
Incident

High
Severity

New
Status

Unassigned
Owner

5/3/2021, 12:14:42 PM
Last incident update time



Timeline

ADFS DKM Master Key Export
4/4/2021, 12:10:00 PM
Identifies an export of the ADFS DKM Mast...

ADFS DKM Master Key Export
5/2/2021, 12:10:01 PM
Identifies an export of the ADFS DKM Mast...

Timeline
Info
Entities
Insights
Help

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Hunting

Home > Microsoft Sentinel

Microsoft Sentinel | Hunting

Selected workspace: 'CyberSecuritySOC'

Search (Ctrl+/)

General
- Overview
- Logs
- News & guides

Threat management
- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence (Preview)

Configuration
- Data connectors
- Analytics
- Watchlist (Preview)
- Automation
- Community
- Settings

Refresh | Last 24 hours | New Query | Run all queries (Preview) | Columns

224 / 249 — Active / total queries
0 / 0 — Result count / queries run
0 — Livestream Results
0 — My bookmarks

LEARN MORE
About hunting

Queries | Livestream | Bookmarks

1	36	31	57	31	19	19	13	16	27	31	25	29	29
PreAttack	Initial Ac...	Execution	Persiste...	Privilege...	Defense ...	Credenti...	Discovery	Lateral ...	Collection	Exfiltrati...	Comma...	Impact	No Tactic

Search queries | Favorites : All | Provider : All | Data sources : All | Tactics : All | Techniques : All | More (2)

Query	Provider	Data Source	Results	Results delta (Pre...	Tactics	Techniques (Preview)
Changes made to AWS IAM policy	Microsoft	AWSCloudTrail	--	N/A		T1078 +1
Consent to Application discovery	Microsoft	AuditLogs +1	--	N/A	Persistence	T1136
Rare Audit activity initiated by App	Microsoft	AuditLogs +1	--	N/A		T1136
Rare Audit activity initiated by User	Microsoft	AuditLogs +1	--	N/A		T1136
Azure storage key enumeration	Microsoft	AzureActivity	--	N/A	Discovery	T1087
DNS lookups for commonly abused TLDs	Microsoft	DnsEvents	--	N/A		T1483 +2
DNS - domain anomalous lookup increase	Microsoft	DnsEvents	--	N/A		T1483 +2
DNS Full Name anomalous lookup increase	Microsoft	DnsEvents	--	N/A		T1483 +2
High reverse DNS count by host	Microsoft	DnsEvents	--	N/A	Discovery	T1046
Abnormally long DNS URI queries	Microsoft	DnsEvents	--	N/A		T1483 +2
DNS Domains linked to WannaCry ranso...	Microsoft	DnsEvents	--	N/A		T1035 +1
Cobalt Strike DNS Beaconing	Microsoft	DnsEvents +1	--	N/A	Command and Con...	T1483 +1
Failed service logon attempt by user acco...	Microsoft	AuditLogs +1	--	N/A	Credential Access	T1110
Failed Login Attempt by Expired account	Microsoft	SecurityEv... +1	--	N/A	Initial Access	T1078
Multiple Password Reset by user	Microsoft	AuditLogs +4	--	N/A		T1078 +1
Permutations on logon attempts by User...	Microsoft	OfficeActiv... +1	--	N/A	Credential Access	T1110
RareDNSLookupWithDataTransfer	Microsoft	CommonS... +3	--	N/A		T1043 +1
Rare domains seen in Cloud Logs	Microsoft	AuditLogs +2	--	N/A		T1190 +2
Tracking Privileged Account Rare Activity	Microsoft	SecurityAlert +5	--	N/A		T1078 +1

< Previous | 1 - 50 | Next >

Rare Audit activity initiated by User

Microsoft — Provider | -- — Results | AuditLogs, Update — Data sources

Description
Compares the current day to the last 14 days of audits to identify new audit activities by OperationName, InitiatedByUser, UserPrincipalName, PropertyName, newValue This can be useful when attempting to track down malicious activity related to additions of new users, additions to groups, removal from groups by specific users.

Created time
9/1/2019

Query
```
let current = 1d;
let auditLookback = 14d;
let propertyIgnoreList = dynamic(["TargetId.
UserType", "StsRefreshTokensValidFrom",
"LastDirSyncTime", "DeviceOSVersion",
"CloudDeviceOSVersion", "DeviceObjectVersion"]);
```
View query results >

Entities
Account | Host | IP

Tactics
Persistence — Persistence is any access, action, or configuration change to a system that gives an adversary a persistent presence on that system.
read more on attack.mitre.org

Lateral Movement — Lateral movement consists of techniques that enable an adversary to access and control remote systems on a network.
read more on attack.mitre.org

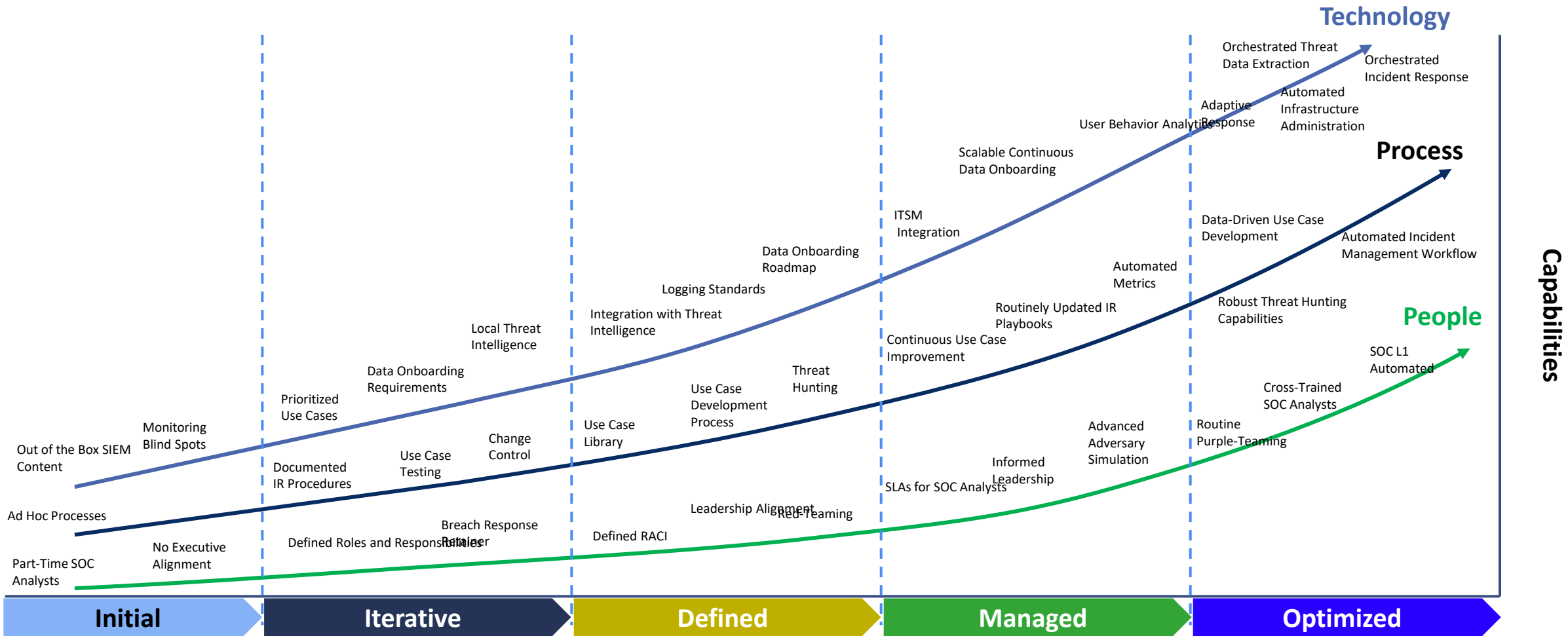
Techniques
T1136 — Create Account

Run Query | View Results

Technology, Processes and People

Microsoft Security
USER GROUP NORWAY

By Accenture



Maturity phases

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Microsoft Security Advantages

$ 4 billion annually investment in cybersecurity

+24 trillion signals proceeded daily

World class technologists and security experts on product development

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Thank You!

Sanna Diana Tomren

@sanna_diana

sanna-diana.medium.com

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Who am I

Anders Kristiansen
Azure Security Lead | @ Devoteam M-Cloud

@pelsner

Linkedin.com/In/andersK

Microsoft Security
USER GROUP NORWAY

Sentinel – Cloud native SIEM/SOAR

Hacker hacking vector created by catalyststuff - www.freepik.com

Slide Deck: github.com/msugn/events

Agenda

Building a scalable sentinel architecture

-logs and ingestion to sentinel

Various use cases we have seen that is key to monitor.

- Run as command
- PIM
- SPN Abuse

If time:

Sentinel Repos,etc.

Microsoft Security
USER GROUP NORWAY

Building a sentinel architecture

Microsoft Security
USER GROUP NORWAY

Design decisions considerations

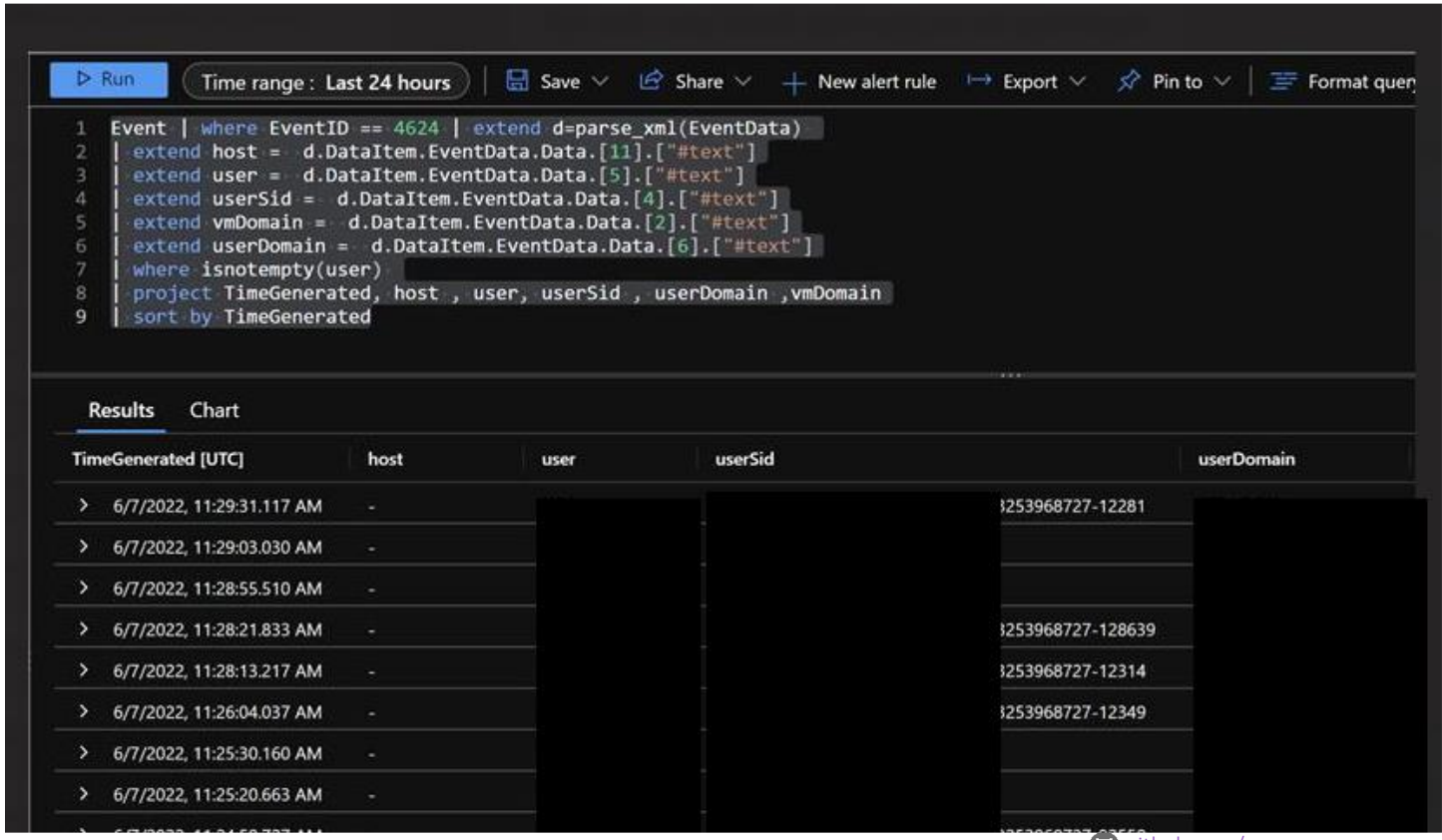
How are your organization (SOC) going to use sentinel?

Multitenant org? Side by side?

Region

Workspace design

1. Check out DD tree
2. Understand cost
3. Daily cap
4. Naming
5. AKS considerations
6. Plan your log ingestion



Microsoft Security
USER GROUP NORWAY

Logs types example

Platform logs

Azure Resources (diagnostics logs)

Activity log (Subscription Layer)

Azure Active Directory logs(Azure tenant)

Virtual machine logs

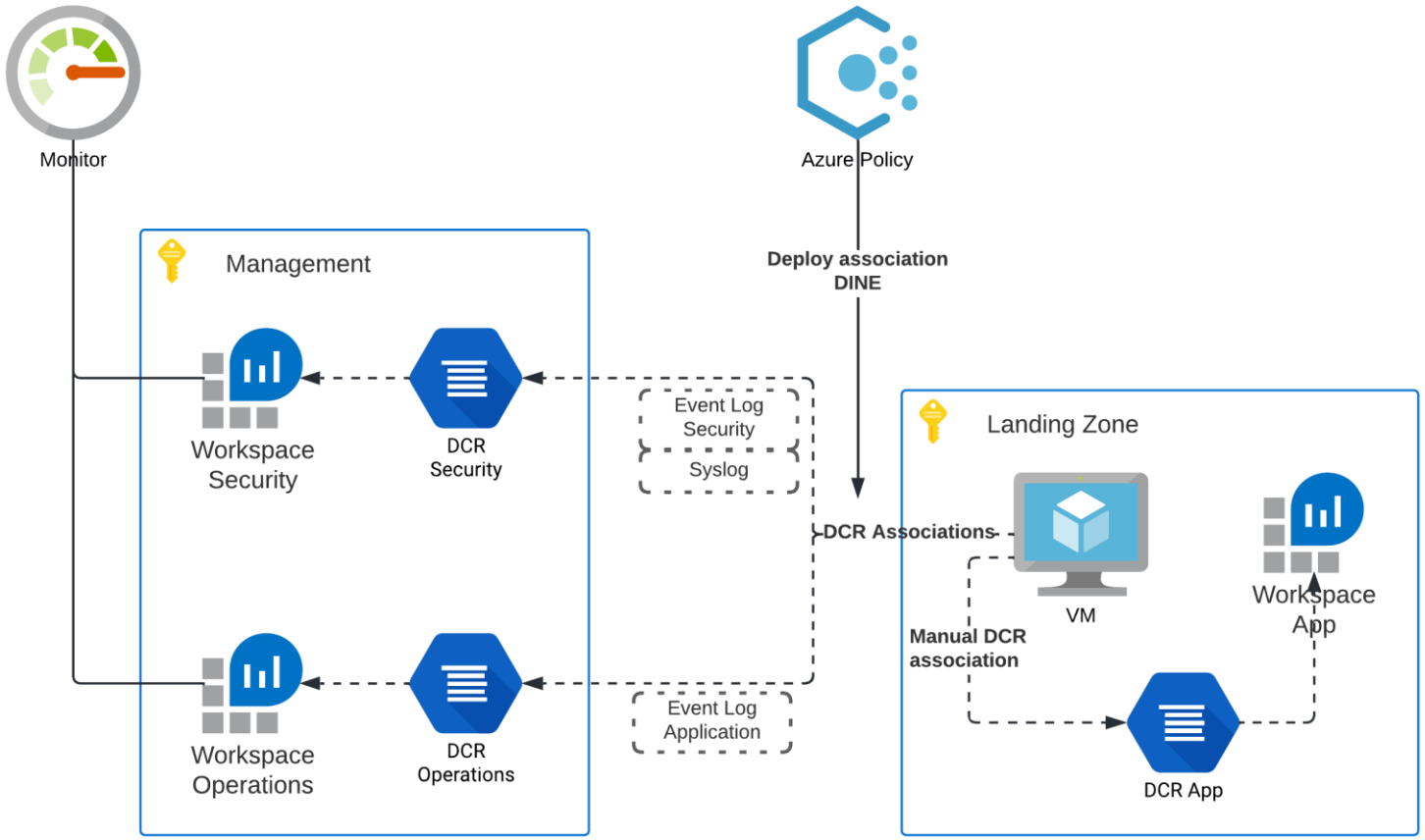
AMA Agent preferred.

VM Insight

Defender for cloud

Connectors

Microsoft Security
USER GROUP NORWAY



Zero Trust Rapid Modernization Plan (RaMP)

Modern Security Operations

1. **Streamline response** to common attacks with XDR for Endpoint/Email/Identity + Cloud (via M365 & Defender for Cloud)
2. **Unify Visibility** with modern Security Information and Event Management (SIEM via Microsoft Sentinel)
3. **Reduce manual effort** - using automated investigation/remediation (SOAR), enforcing alert quality, and threat hunting

Microsoft Security
USER GROUP NORWAY

DCR Example – AVD troubleshooting

```
    "windowsEventLogs": [
        {
            "streams": [
                "Microsoft-Event"
            ],
            "xPathQueries": [
                "Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational!*[System[(EventID=1149)]]",
                "Security!*[System[(EventID=4624 or EventID=4778)]] and *[EventData[Data[@Name='LogonType']='10']]",
                "Microsoft-Windows-TerminalServices-RDPClient/Operational*[System[(EventID=1102)]]!*"
            ],
            "name": "eventLogsDataSource"
        }
    ]
},
"destinations": {
    "logAnalytics": [
        {
            "workspaceResourceId": "[parameters('workspaces_t_opslogs_log_externalid')]",
            "name": "t-opslogs-log"
        },
        {
            "workspaceResourceId": "[parameters('workspaces_t_seclogs_log_externalid')]",
            "name": "la-1502734893"
        }
    ]
},
"dataFlows": [
    {
        "streams": [
            "Microsoft-Perf"
        ],
        "destinations": [
            "t-opslogs-log"
        ]
    },
    {
        "streams": [
            "Microsoft-Event"
        ],
        "destinations": [
            "la-1502734893"
        ]
```

Run | Time range : Last 24 hours | Save | Share | New alert rule | Export

```
Event | where EventID == 4624 | extend d=parse_xml(EventData)
| extend host =  d.DataItem.EventData.Data.[11].["#text"]
| extend user =  d.DataItem.EventData.Data.[5].["#text"]
| extend userSid =  d.DataItem.EventData.Data.[4].["#text"]
| extend vmDomain =  d.DataItem.EventData.Data.[2].["#text"]
|extend userDomain =  d.DataItem.EventData.Data.[6].["#text"]
| where isnotempty(user)
| project TimeGenerated, host , user, userSid , userDomain ,vmDomain
| sort by TimeGenerated
```

Results | Chart

TimeGenerated [UTC]	host	user	userSid
08/06/2022, 06:02:12.340	t-avd-C8D1	maarten.rosier[redacted]	S-1-12-1-1816938841-115
TimeGenerated [UTC]	2022-06-08T06:02:12.34Z		
host	t-avd-C8D1		
user	maarten.rosier@[redacted]		
userSid	[redacted]		
userDomain	[redacted]		
vmDomain	WORKGROUP		
08/06/2022, 06:02:12.340	t-avd-C8D1	maarten.rosier@[redacted]	S-1-12-1-1816938841-11
07/06/2022, 12:24:49.973	t-avd-C8D1	maarten.rosier@[redacted]	S-1-12-1-1816938841-11
07/06/2022, 12:24:49.973	t-avd-C8D1	maarten.rosier@[redacted]	S-1-12-1-1816938841-11
07/06/2022, 12:17:58.723	t-avd-C8D1	maarten.rosier@[redacted]	S-1-12-1-1816938841-11
07/06/2022, 12:17:58.723	t-avd-C8D1	maarten.rosier@[redacted]	S-1-12-1-1816938841-11

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Recap of Extensions and Run Commands

- **Runs also as context of local system account**
- **No way to remove the features**
- **Only permission needed is**
  - Microsoft.Compute/virtualMachines/runCommand/action
  - Accessible by Virtual Machine Contributer
- Requires Public IP access to Azure from VM
- Managed Run Commands in Preview
  - Parallel execution of multiple scripts
  - Support for long running scripts

PowerShell Script

```
1  whoami
```

Run

Output

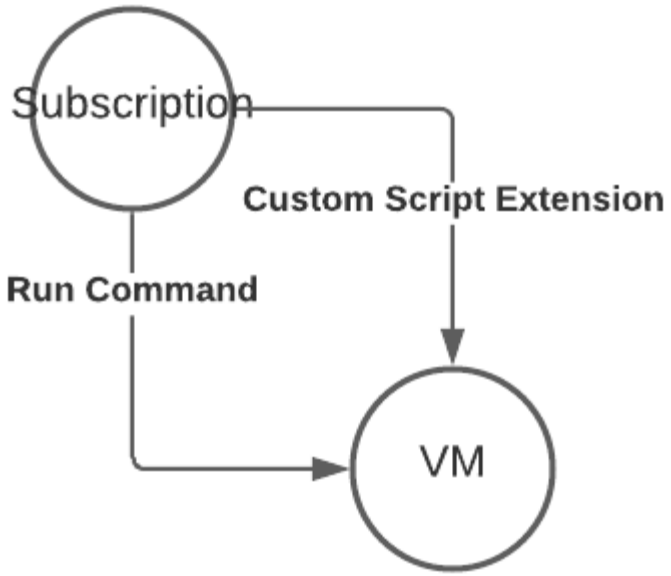
```
nt authority\system
```

Example: Set-ADAccountPassword -Identity user03 -NewPassword $NewPwd -Reset

Log path: C:\WindowsAzure\Logs\Plugins\Microsoft.CPlat.Core.RunCommandWindows

Microsoft Security
USER GROUP NORWAY

Attack path



Adding local user example

PowerShell Script

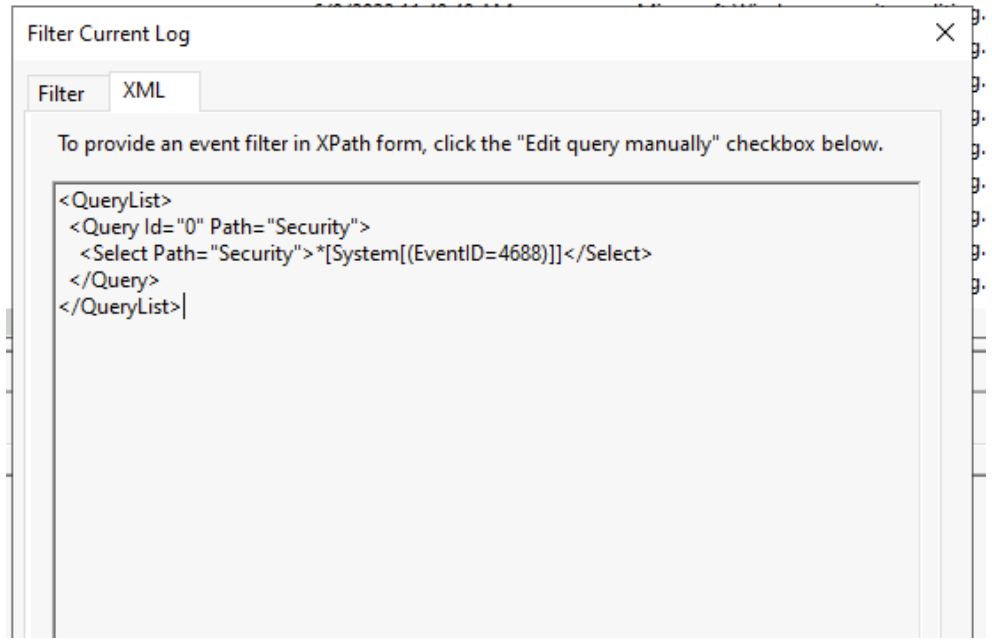
```
# Username and Password
$username = "msug"
$password = ConvertTo-SecureString "Passw0rd123!" -AsPlainText -Force  # Super strong plane text

# Creating the user
New-LocalUser -Name "$username" -Password $password -FullName "$username" -Description "msug"
```

Run

Output

```
Name Enabled Description
---- ------- -----------
msug True    msug
```



Microsoft Security
USER GROUP NORWAY

How to detect and alert

- Built-in query from azure.
- Used for lateral movement, gain persistence, troubleshooting, in-guest config.

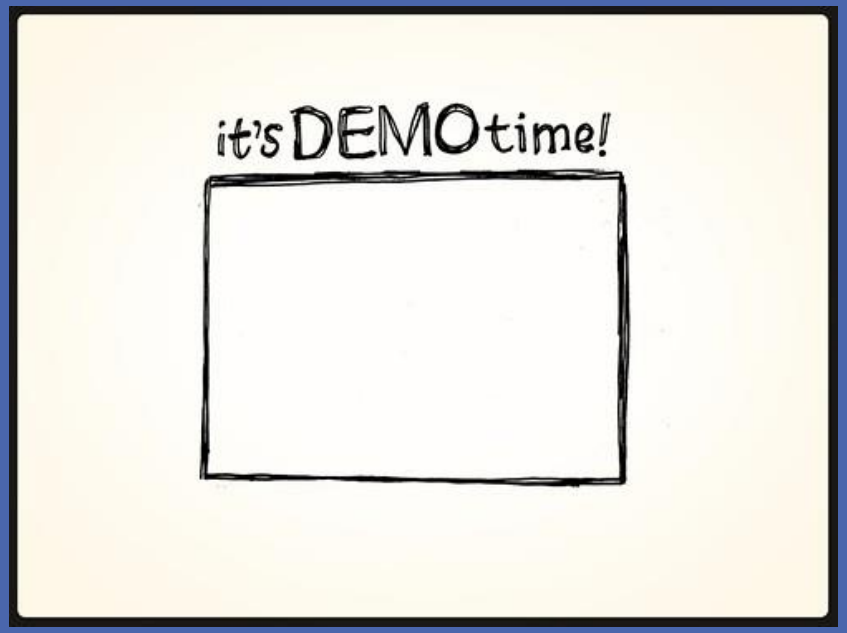
```
AzureActivity
| where CategoryValue == "Administrative"
| where OperationNameValue =~ "Microsoft.Compute/virtualMachines/runCommand/action"
| extend VMName = tostring(todynamic(Properties).resource)
| summarize make_list(ActivityStatusValue), TimeGenerated = max(TimeGenerated) by CorrelationId, CallerIpAddress, Caller, ResourceGroup, VMName
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	VMName	CorrelationId	CallerIpAddress	Caller	ResourceGroup	list_ActivityStatusValue
6/7/2022, 10:57:28.870 AM	t-msug1	e8ce526b-e2e0-4905-88ce-9f53aa18cd43	84.234.135.144	Anders.Kristiansen@Devoteam....	T-MSUG	["Start","Accept","Success"]

CorrelationId	e8ce526b-e2e0-4905-88ce-9f53aa18cd43
CallerIpAddress	84.234.135.144
Caller	Anders.Kristiansen@Devoteam.no
ResourceGroup	T-MSUG
VMName	t-msug1
list_ActivityStatusVal...	["Start","Accept","Success"]
0	Start
1	Accept
2	Success
TimeGenerated [UTC]	2022-06-07T10:57:28.87Z

Demo: built in rules, navigation



Microsoft Security
USER GROUP NORWAY

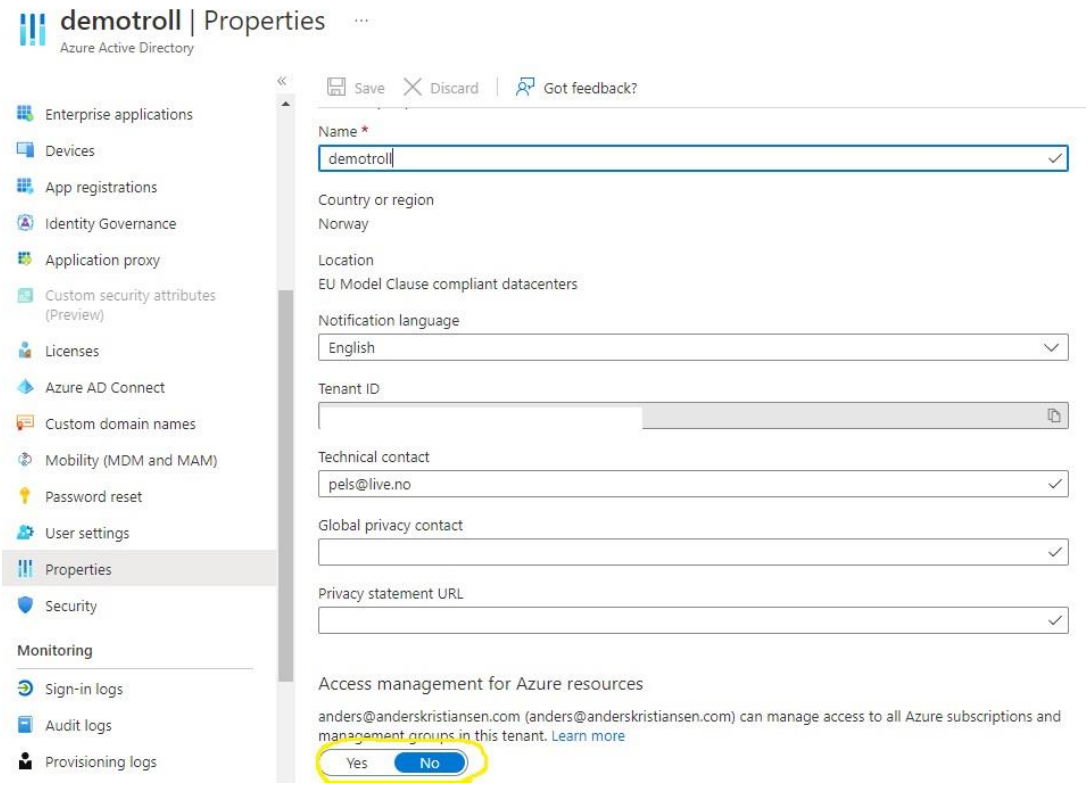
Privileged Identity Management

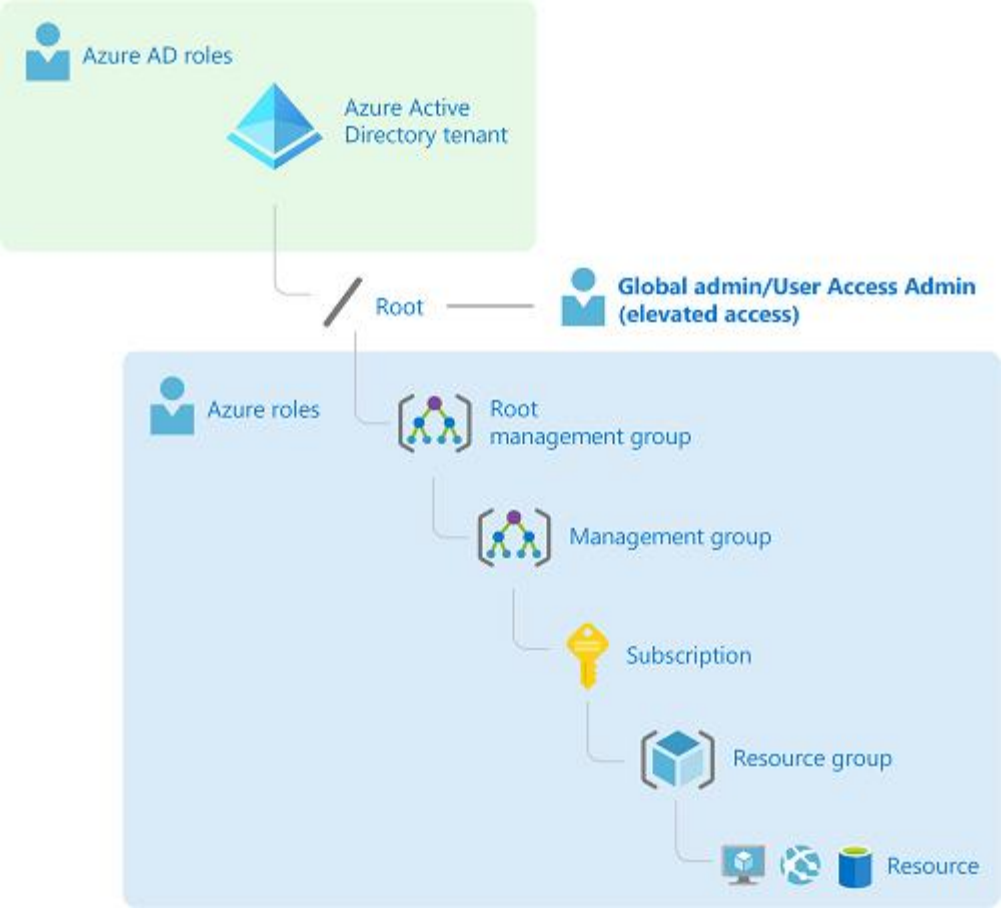
Detecting and alerting on high privileged actions

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

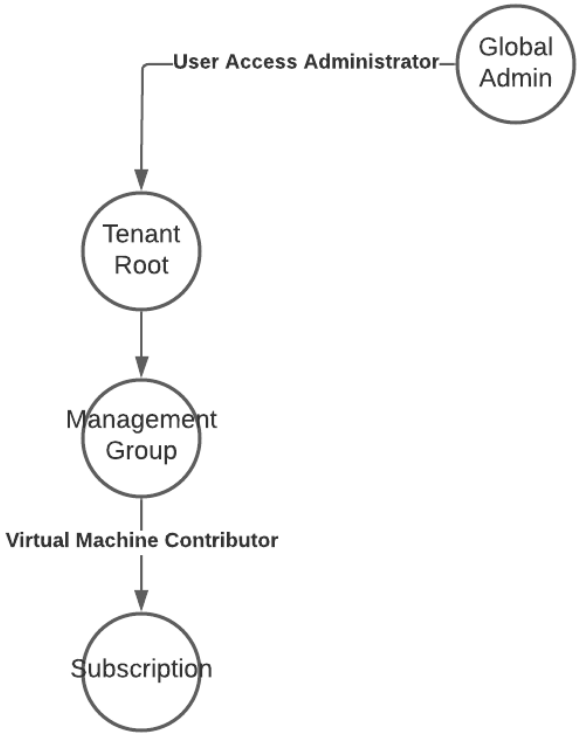
Recap Privileged Identity Management





https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin

Elevate Azure Subscription access



- Attacker or internal already have high privileges to tenant
- Enabling this to further extend persistence over environment.
- Do not show up in regular logs!

https://cloudbrothers.info/en/azure-dominance-paths/

Activity

Directory Activity

Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. Visit Log Analytics

Search

Timespan : **Last 6 hours** | Tenant Resource Provider : **None**

6 items.

Operation name	Status	Time	Time stamp	Subscription
Assigns the caller to User Access Administrator role	Succeeded	2 minutes a...	Sun Jun 05 ...	
Assigns the caller to User Access Administrator role	Started	2 minutes a...	Sun Jun 05 ...	
Create role assignment	Succeeded	37 minutes ...	Sun Jun 05 ...	
List Entities	Succeeded	37 minutes ...	Sun Jun 05 ...	
List Entities	Succeeded	37 minutes ...	Sun Jun 05 ...	
GetEntities	Succeeded	2 hours ago	Sun Jun 05 ...	

Summary JSON


```
    "correlationId": "25f34318-3b83-4fed-ba82-a91b7b0537cf",
    "description": "",
    "eventDataId": "2a9450d5-3b53-451c-b36c-2f66e502141c",
    "eventName": {
        "value": "BeginRequest",
        "localizedValue": "Begin request"
    },
    "category": {
        "value": "Administrative",
        "localizedValue": "Administrative"
    },
    "eventTimestamp": "2022-06-05T09:22:33.7195604Z",
    "id": "/providers/Microsoft.Authorization/events/2a9450d5-3b53-451c-b36c-2f66e502141c/ticks/637900177537195604",
    "level": "Informational",
    "operationId": "25f34318-3b83-4fed-ba82-a91b7b0537cf",
    "operationName": {
        "value": "Microsoft.Authorization/elevateAccess/action",
        "localizedValue": "Assigns the caller to User Access Administrator role"
    },
    "resourceProviderName": {
        "value": "Microsoft.Authorization",
        "localizedValue": "Microsoft.Authorization"
    },
    "resourceType": {
        "value": null,
        "localizedValue": ""
    },
    "resourceId": "/providers/Microsoft.Authorization",
    "status": {
        "value": "Started",
        "localizedValue": "Started"
    },
    "subStatus": {
        "value": "",
        "localizedValue": ""
    },
    "submissionTimestamp": "2022-06-05T09:24:00.1502945Z",
    "subscriptionId": "",
    "tenantId": "07d87066-942e-4072-8596-36dd123efc1b",
    "properties": {
        "requestbody": "{}",
        "eventCategory": "Administrative",
```


Logs is located under directory activity

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

Hunting

eate new

n query | Save | Share link

```
CloudAppEvents
| where Application == 'Microsoft Azure'
| where ActionType has 'ElevateAccess Microsoft.Authorization'
//| summarize  by ActionType  | sort by ActionType asc
```

g Started | Results

port

1 of 2 selected | Search

mestamp	ActionType	Application	ApplicationId	AppInstanceId	AccountObjectId	AccountId	Ac
un 5, 2022 11:48:21 AM	ElevateAccess Microsoft....	Microsoft Azure	12260	0	df211e71-92cb-4ed7...	df211e71-92cb-4ed7-ad...	Ar
un 5, 2022 11:48:19 AM	ElevateAccess Microsoft....	Microsoft Azure	12260	0	df211e71-92cb-4ed7...	df211e71-92cb-4ed7-ad...	Ar

Inspect record

armServiceRequestId	c5d277b9-d539-4ed7-84b7-2f3b4
GDSEnqueueTimeUtc	2022-06-05T09:49:29.0000000Z
PreciseTimeStamp	2022-06-05T09:48:19.0075429Z
resourceProvider	Microsoft.Authorization
EventEnvironment	diagnosticsprod
eventInstanceId	019fd1d9-c7b3-4a1a-8e09-22d91
ActivityId	3a1fc577-5c27-426b-b6b4-9381e
eventTimestamp	2022-06-05T09:48:19.0062627Z
subscriptionId	
ReleaseVersion	6.2022.21.4+6c99530.release_202
EventNamespace	csmNorwayERPF
AccountMoniker	MdsResourceStackRPFNorwayE
operationName	Microsoft.Authorization/elevateAc
authorization	{"scope":"/providers/Microsoft.Au
applicationId	c44b4083-3bb0-49c1-b47d-974e5
uniqueTokenId	xexYttNZIkm3aIE1bloSAA
correlationId	3a1fc577-5c27-426b-b6b4-9381e
principalPuid	10032000958102EF
RoleLocation	Norway East
ProviderGuid	6a309439-9c04-49f6-b5cf-9a8e78
EventVersion	Ver24v0
RoleInstance	FrontdoorWeb-vmss-fdweb_13

Event from CloudAppEvent in Defender 365.

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MSUGN

So how do we got this to sentinel?

Search by ID, title, tags, owner or product | Severity : All | Status : 2 selected | Product name : All | Owner : All

Auto-refresh incidents

Severity	Incident ID	Title	Alerts	Product names
Medium	5	Global Admin Elevated Access to Azure Root Management Group	1	Microsoft Sentinel
Medium	4	Global Admin Elevated Access to Azure Root Management Group	1	Microsoft Sentinel

Global Admin Elevated Access to Azure Root Manag...
Incident ID: 5

Unassigned — Owner | New — Status | Medium — Severity

Description
Detects activity when Global Admin elevates access to Azure Root Management Group as User Access Administrator where it's inherited to all subscriptions

Alert product names
- Microsoft Sentinel

Evidence
2 Events | 1 Alerts | 0 Bookmarks

Last update time
06/05/22, 12:09 PM

Creation time
06/05/22, 12:09 PM

Entities (2)
Anders Kristiansen
b507cd211c194747a...
View full details >

Tactics and techniques
Credential Access (1)
Privilege Escalation (1)

Incident workbook
Incident Overview

Analytics rule
Global Admin Elevated Access to Azure Root Management Group

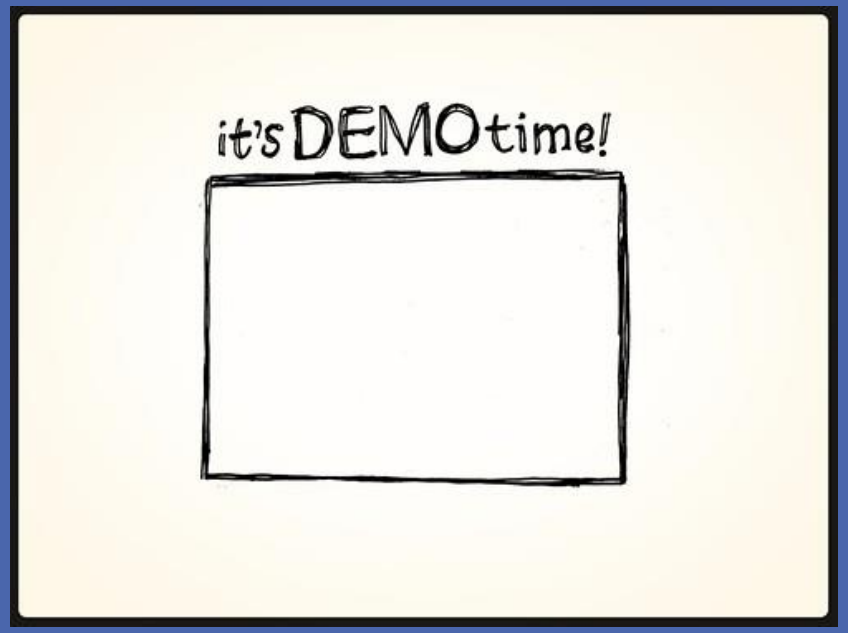
Tags

Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/...

Last comment (Total: 0)

Write a comment...

PermissionScope
/



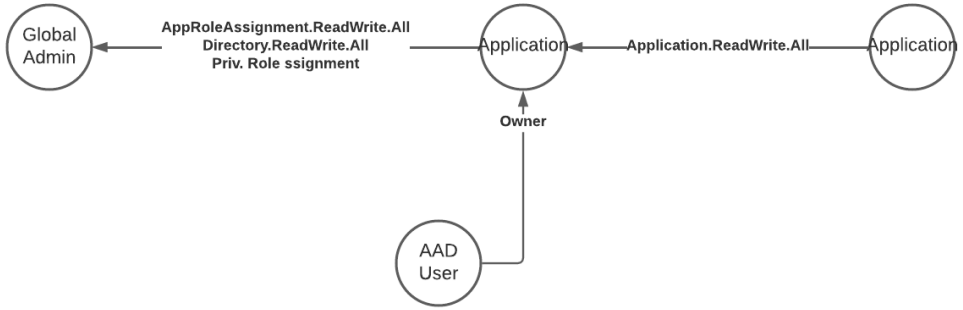
Microsoft Security
USER GROUP NORWAY

DEMO

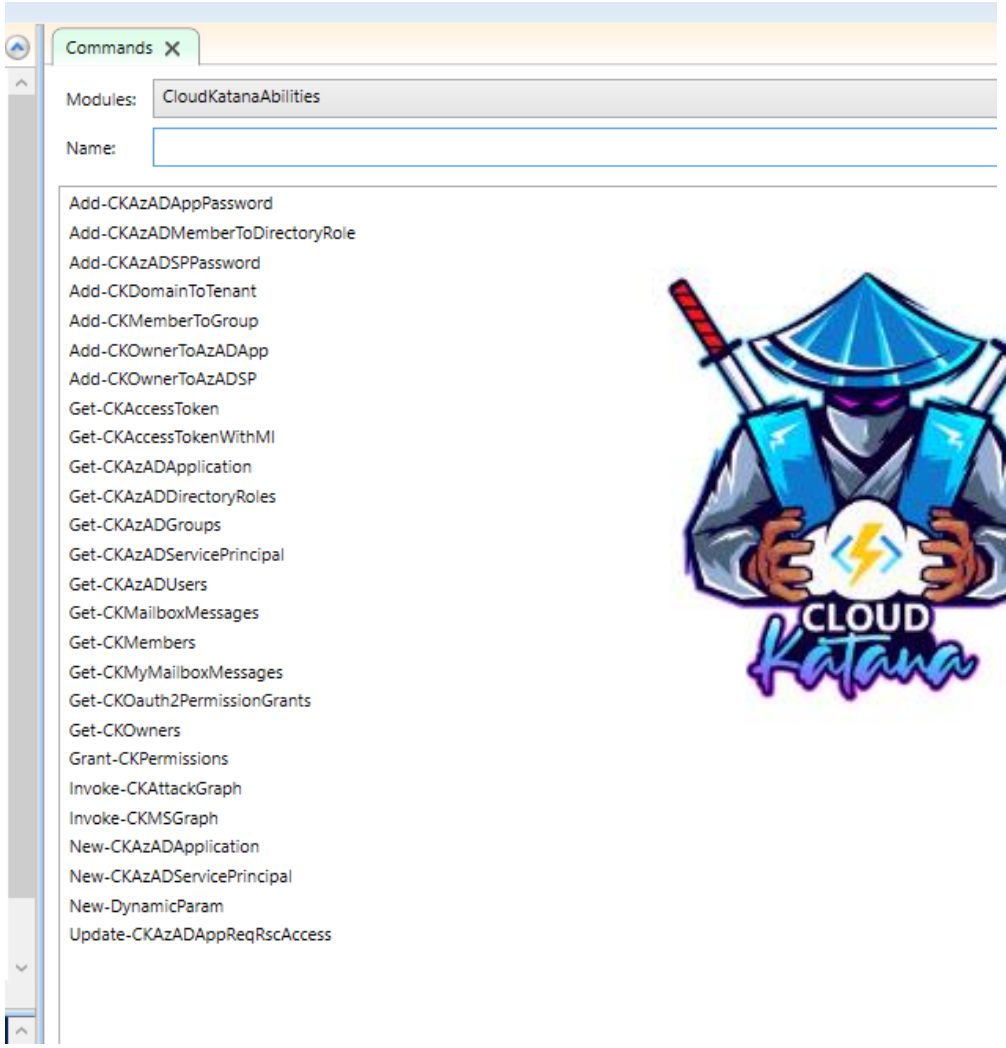
SPN abuse.

Setting the stage for this attack:

1. Recon of SPNs with high privilege SPNs.
2. GrantAppRoleAssignmentPermission
    - - AppRoleAssignment.ReadWrite.All
    - - Application.Read.All
3. AddPasswordToApp – add secret
4. GrantRoleMgmtPermission
    - RoleManagement.ReadWrite.Directory
5. AddServicePrincipalToGARole (Or whatever role)
    - - globalAdminTemplateRoleId: 62e90394-69f5-4237-9190-012177145e10



CloudKatana PS Module and function app




```yaml
    name: GrantAppRoleAssignmentPermission
    execution:
      type: ScriptModule
      platform: Azure
      executor: PowerShell
      module: ...
      parameters:
        spObjectId: variable(victimAppSPObjectId)
        resourceName: Microsoft Graph
        permissionType: Application
        permissions:
          - AppRoleAssignment.ReadWrite.All
          - Application.Read.All
  - number: 2
    name: AddPasswordToApp
    execution: ...
    wait: 120
  - number: 3
    name: GetAccessTokenOne
    dependsOn: ...
    execution:
      type: ScriptModule
      platform: Azure
      executor: PowerShell
      module: ...
      parameters: ...
  - number: 4
    name: GrantRoleMgmtPermission
    dependsOn:
      - 3
    execution:
      type: ScriptModule
      platform: Azure
      executor: PowerShell
      module: ...
      parameters:
        accessToken: reference(3).access_token
        spObjectId: victimAppSPObjectId
        resourceName: Microsoft Graph
        permissionType: Application
        permissions:
          - RoleManagement.ReadWrite.Directory
    wait: 120
  - number: 5
    name: GetAccessTokenTwo
    dependsOn: ...
    execution: ...
  - number: 6
    name: AddServicePrincipalToGARole
    dependsOn:
      - 5
    execution:
      type: ScriptModule
      platform: Azure
      executor: PowerShell
      module: ...
      parameters:
        accessToken: reference(5).access_token
        directoryRoleTemplateId: cloudAppAdminTemplateRoleId
        directoryObjectId: variable(victimAppSPObjectId)
```


https://www.powershellgallery.com/packages/CloudKatanaAbilities/1.0

Detection

In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, start a free trial.

Subscription: Microsoft Azure Sponsorship ([redacted])

Log Analytics workspace: loganalytics

- [x] NonInteractiveUserSignInLogs
- [x] ServicePrincipalSignInLogs
- [ ] Archive to a storage account

```
let timeframe = 90d;
AADServicePrincipalSignInLogs
| where TimeGenerated >= ago(timeframe)
//| where AppId == '<YourAppId>'
| summarize arg_max(ServicePrincipalName, *) by IPAddress
| project TimeGenerated, AppId, ServicePrincipalName, IPAddress, Location
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	AppId	ServicePrincipalName	IPAddress	Location
6/7/2022, 9:29:36.383 AM	4961cf70-9885-44fd-a649-3ebbbcc33dd4	az-sp-infra-cicd-sub-shared-nonprod	52.255.134.84	US
6/6/2022, 9:04:07.326 PM	05f96940-d4eb-4576-b609-63bdb19559e8	az-sp-core-cicd-sub-platform-prod	52.254.6.39	US
6/3/2022, 10:03:31.800 PM	05f96940-d4eb-4576-b609-63bdb19559e8	az-sp-core-cicd-sub-platform-prod	52.252.115.162	US
6/6/2022, 10:04:11.007 PM	05f96940-d4eb-4576-b609-63bdb19559e8	az-sp-core-cicd-sub-platform-prod	52.250.6.157	US
6/3/2022, 12:35:32.187 PM	8cec9d94-b0af-41d8-9909-7e3de8356efd	az-sp-sandbox-cicd-sub-shared-nonprod	52.186.143.98	US
6/3/2022, 12:30:45.265 PM	8cec9d94-b0af-41d8-9909-7e3de8356efd	az-sp-sandbox-cicd-sub-shared-nonprod	52.185.32.145	US
6/7/2022, 10:03:29.775 PM	05f96940-d4eb-4576-b609-63bdb19559e8	az-sp-core-cicd-sub-platform-prod	52.173.32.156	US

Audit Log Details

Activity | Target(s) | **Modified Properties**

Target	Property Name	Old Value	New Value
Microsoft ...	AppRole.Id		"1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9"
Microsoft ...	AppRole.Value		"Application.ReadWrite.All"
Microsoft ...	AppRole.Displa...		"Read and write all applications"
Microsoft ...	AppRoleAssign...		"2022-06-08T05:54:09.9532789Z"
Microsoft ...	AppRoleAssign...		"2022-06-08T05:54:09.9532789Z"
Microsoft ...	ServicePrincipal...		"c688916b-c93e-4667-bfba-d5419347b4e7"
Microsoft ...	ServicePrincipal...		"msug"

```
let DangerousPermissions =
dynamic(["AppRoleAssignment.ReadWrite.All","Application.ReadWrite.All","RoleManagement.ReadWrite.Directory"]);
AuditLogs
| where OperationName == "Add app role assignment to service principal"
| mv-expand TargetResources
| mv-expand TargetResources.modifiedProperties
| where TargetResources_modifiedProperties.displayName == "AppRole.Value"
| extend InitiatedByUserPrincipalName = InitiatedBy.user.userPrincipalName
| extend AddedPermission = replace_string(tostring(TargetResources_modifiedProperties.newValue),'"','')
| where AddedPermission in~ ( DangerousPermissions )
```

Homework from Andy Robbins

#1 Audit and remove rights that is not needed.

- GA, Privileged Authentication Administrator, Privileged Authentication Administrator
- **Check for SPN with MS graph roles:**
- RoleManagement.ReadWrite.Directory
- AppRoleAssignment.ReadWrite.All

#2 Audit Privileges Held by Other Principals

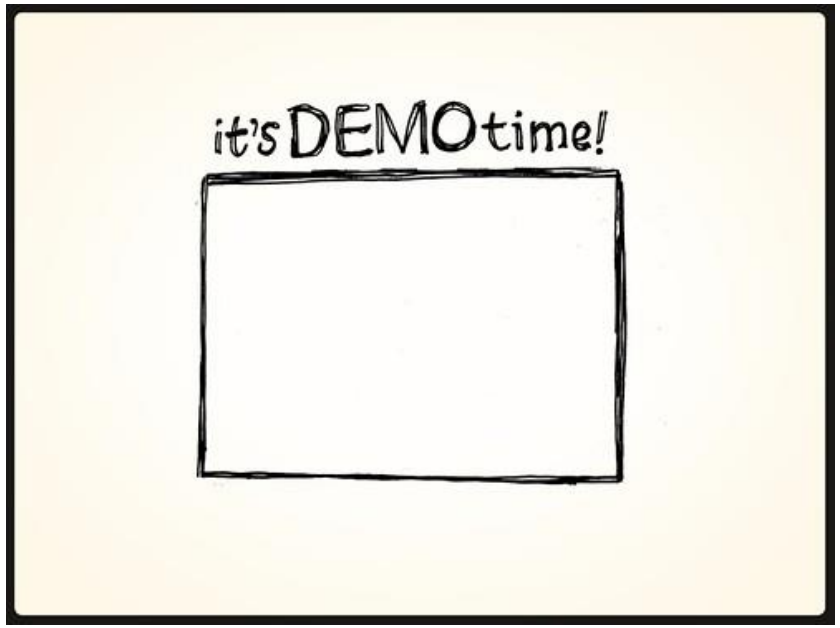
- Limit the exposure of those highly privileged service principals by auditing the users, groups, and service principals that have been granted any of the following AzureAD/Graph roles:
- - Application Administrator (including those scoped specifically to the Service Principal)
- - Cloud Application Administrator (including those scoped specifically to the Service Principal)
- - Directory Synchronization Accounts
- - Hybrid Identity Administrator
- - Partner Tier1 Support
- - Partner Tier2 Support
- Application.ReadWrite.All
- ServicePrincipalEndpoint.ReadWrite.All

#3 Audit Privileges Held Against automation account, logic app, azure function.

- - Limit the accounts with least privileged approach.

https://medium.com/specter-ops-posts/managed-identity-attack-paths-part-1-automation-accounts-82667d17187a

Preview: repository



Microsoft Security

USER GROUP NORWAY

Microsoft Security
USER GROUP NORWAY

github.com/msugn
@MsSecUGNorway
#MsUGN