



Thijs Lecomte &  
Robbe Van den Daele<sup>+</sup>

# Architecting a SOC on Defender XDR and Microsoft Sentinel



SquaredUp



infinity



kpn  
Partner Network



INS PARK



cegeka

# Speakers



**Robbe Van den  
Daele**

Security Consultant &  
SOC Engineer @ The  
Collective



**Thijs Lecomte**

Head of Managed  
Services @ The Collective  
Security MVP



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka



# What are we going to discuss?

1. Architecture
2. Multi-tenant authentication
3. Automated deployments
4. Exclusion Management
4. Detection Engineering
5. Data Collection
6. Playbooks / Automations
8. Case Management



SquaredUp



infinity



INTERSTELLAR



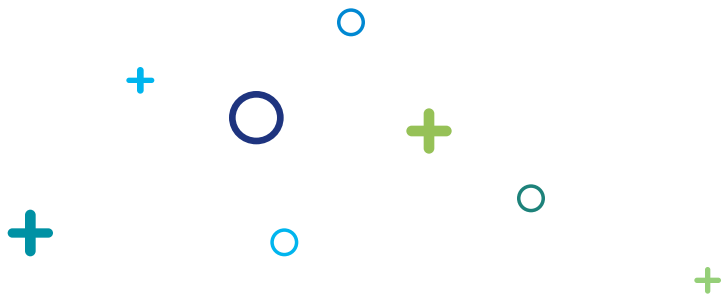
kpn  
Partner Network



INS PARK



cegeka



# 1. Architecture



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network

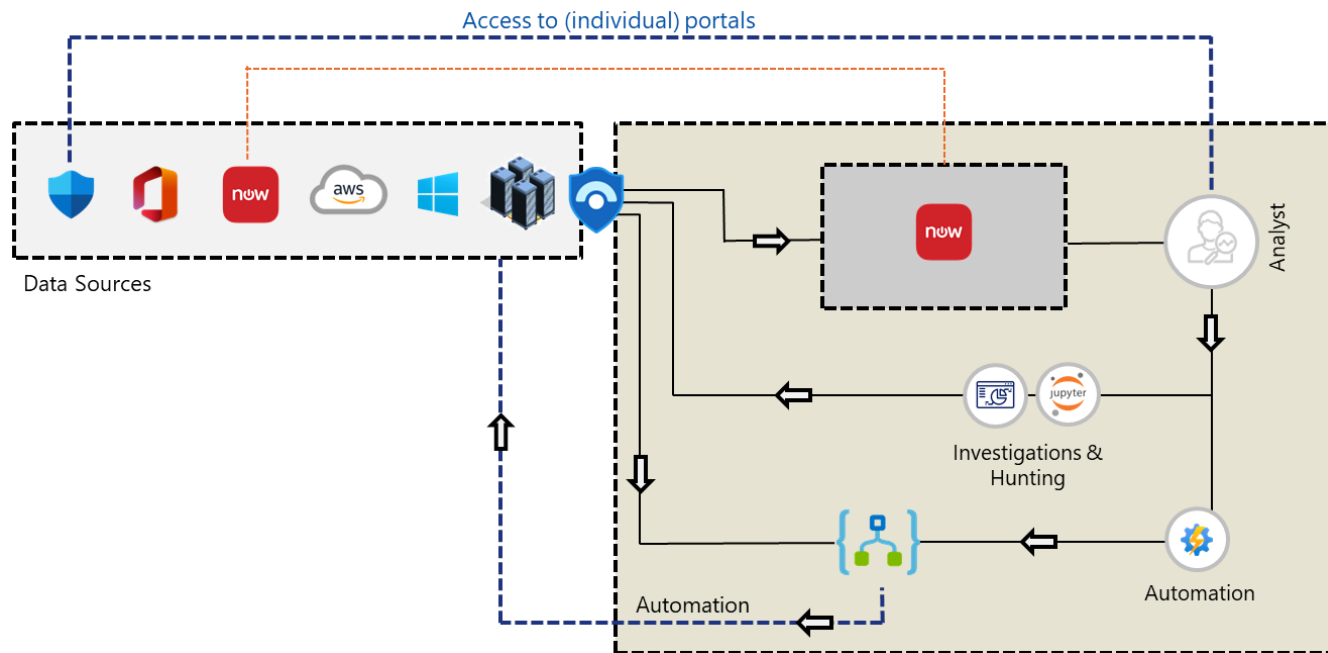


INSPARK

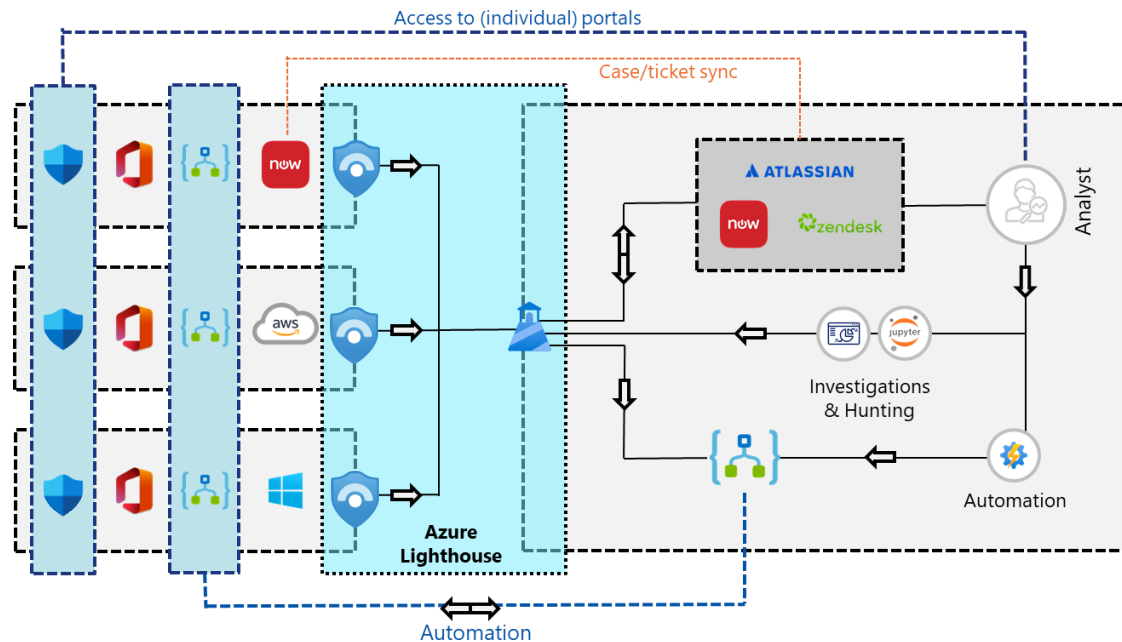


cegeka

# Single-tenant architecture



# Multi-tenant architecture





# Multi workspace setup



REGULATORY  
COMPLIANCE



DATA  
OWNERSHIP



MULTIPLE  
TENANTS



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka



# Multi workspace setup

- MSSP should deploy a workspace for each customer in the customer tenant
- Keep architecture as simple as possible for each 'customer'
- Make sure you have a central management system



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka



# Managing a multi workspace setup



Incidents → Multi workspace incident view

Home > **Microsoft Sentinel**

Microsoft

[+ Create](#) [Manage view](#) [Refresh](#) [Export to CSV](#) [Open query](#) [View incidents](#) [Feedback](#)

Filter for any field... [Subscription == 71 of 82 selected](#) [Resource group == all](#) [Location == all](#) [Add filter](#)

Showing 1 to 4 of 4 records. [No grouping](#) [List view](#)

<input checked="" type="checkbox"/> Name	Resource group	Location	Subscription	Directory
<input checked="" type="checkbox"/> ContosoCorpSentinelWorkspace	demo_catalog	East US	Partner_Sandbox	Microsoft
<input checked="" type="checkbox"/> CyberSecuritySOC	soc	Central US	CyberSecSOC	contosohotels.com
<input checked="" type="checkbox"/> Sentinel-Development	demo_catalog	West Europe	Security - Common	Microsoft
<input checked="" type="checkbox"/> temp-workspace	demo_catalog	West Europe	Security - Common	Microsoft

< Previous Page  of 1 Next >



# Managing a multi workspace setup

Queries → Multi workspace queries

- Using workspace() expression with union operator
- Can be used in analytic rules (not recommended for MSSP's)
  - Max 20 workspaces (5 recommended)
  - Incident exists in main tenant
- Good for investigations, threat hunting, and workbooks



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network

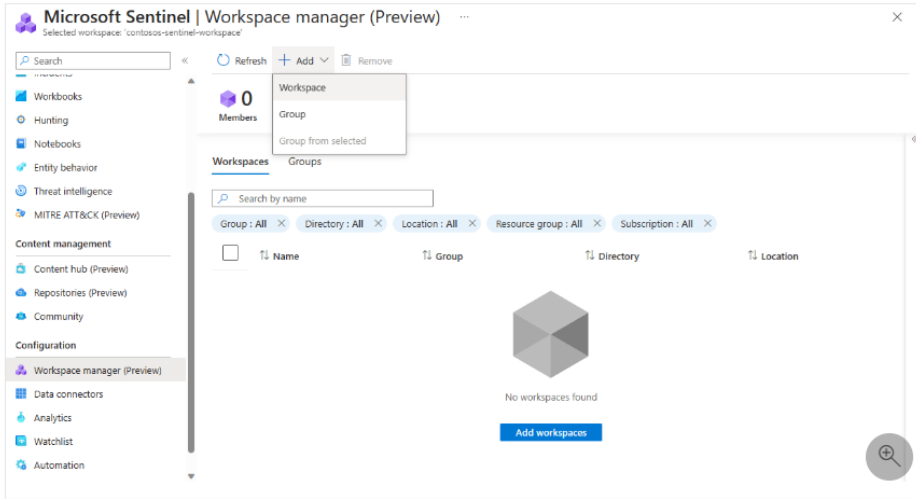


INS PARK



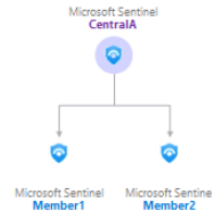
cegeka

# Workspace manager

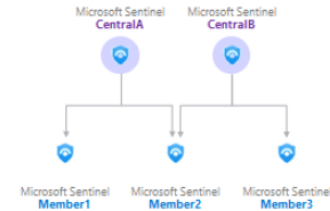


## Possible Workspace Manager Architectures

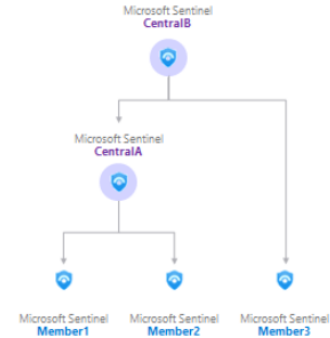
### Simple / Direct-Link



### Co-Management



### N-Tier



SquaredUp



kpn  
Partner Network



INS PARK



cegeka



# Protecting intellectual property as MSSP



Hosting content in  
MSSP tenant



Restricting content  
in customer tenant



Contractual  
agreement



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka

# Protecting intellectual property as MSSP



Hosting content



Restrict access



Contractual  
agreement

Incidents & alerts in customer tenant?

No

Yes

Yes

Customer transparency?

No

No

Yes

Straight-forward setup?

No

Yes/No

Yes

Protective controls?

Yes

Yes/No

Yes/No





## 2. Authentication for multi-tenant deployments



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka

# What are the options?



GDAP



Lighthouse



Guest Users



Named Admins



SquaredUp



infinity



kpn  
Partner Network



INS PARK



cegeka

# What are the options?



GDAP



Lighthouse



Guest Users



Named Admins

User object in customer tenant?

No

No

Yes

Yes

Auth properties in customer tenant?

No

No

No

Yes

Granular roles supported?

Yes/No

Yes

Yes

Yes

Admin Accounts?

Yes

Yes

No

Yes

Customer has access control?

No

No

Yes

Yes



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka



# What are the options?

MSSP Preferred  
(MTO)



GDAP



Lighthouse



Guest Users

Customer Preferred



Named Admins



# 3. Automated deployment



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



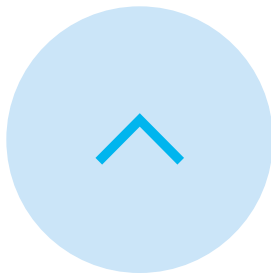
INSPARK



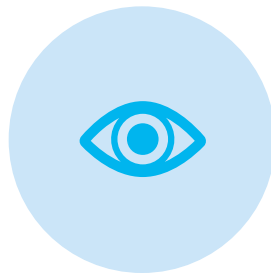
cegeka



# The need for automated deployment



REDUCING  
MANUAL EFFORT



FOUR EYES  
PRINCIPLE



AUTOMATIC  
VALIDATION



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka

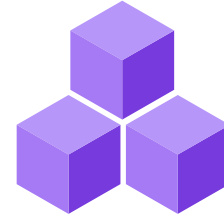
# What are the options?



Azure  
DevOps



Sentinel  
Repositories



Workspace  
Manager

Native Implementation?

No

Yes

Yes

Automated Deployment

Yes

Yes

No

Customization possible?

Yes

Yes

No

Four-eyes principle

Yes

Yes

No

Automatic validation (naming...)

Yes

Yes\*

No



SquaredUp



infinity



kpn  
Partner Network



INS PARK



cegeka



# ARM vs Bicep

Personal choice

Ease of exporting



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka



# Supported resources

- Everything Sentinel-related
  - Data Connectors?
- Defender Custom Detections
- Other Defender resources



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka



# The Collective Setup

- Overrides
- Specific data sources
  - Variables per customer
- Timing of deployments
- Deploy everything or only changes



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network

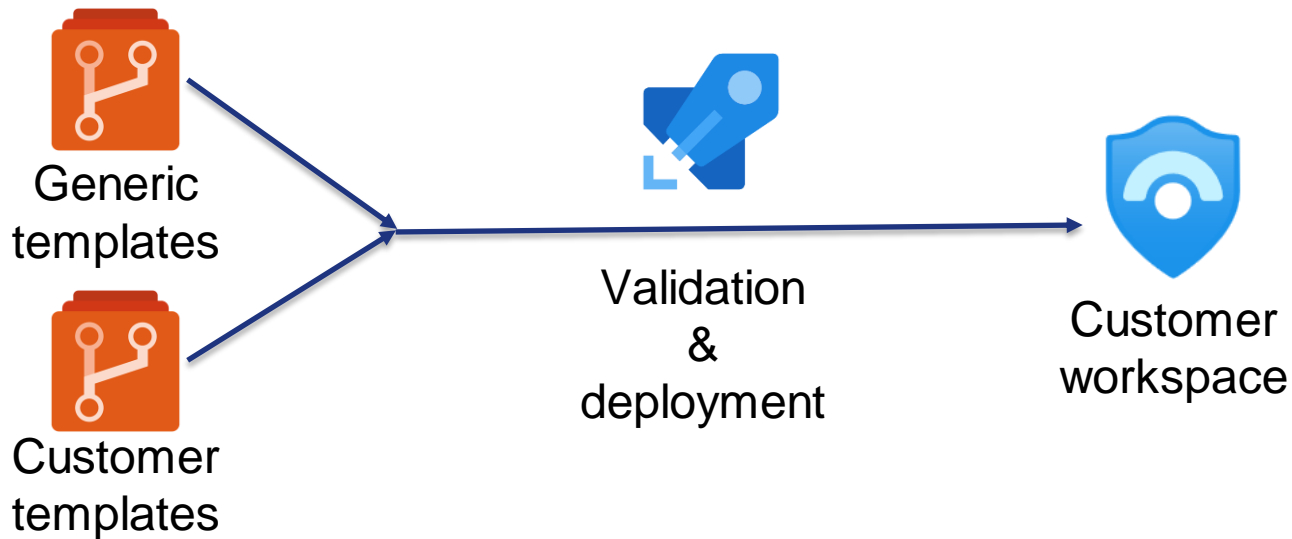


INSPARK



cegeka

# Sample Setup







## 4. Exclusion management



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka



# Why do you need exclusions?

- Decrease false positive
- Avoid negative impact



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka



# Where to add exclusions

- Analytic rules/custom detection rules
- Sentinel Automation Rules
- Defender Alert Tuning
- Defender Indicators
- MDI exclusions



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka



# Best practices

- Exclusion register
- Customer notice / approval
- Approval
  - CI/CD Integration
- Avoid incidents



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network

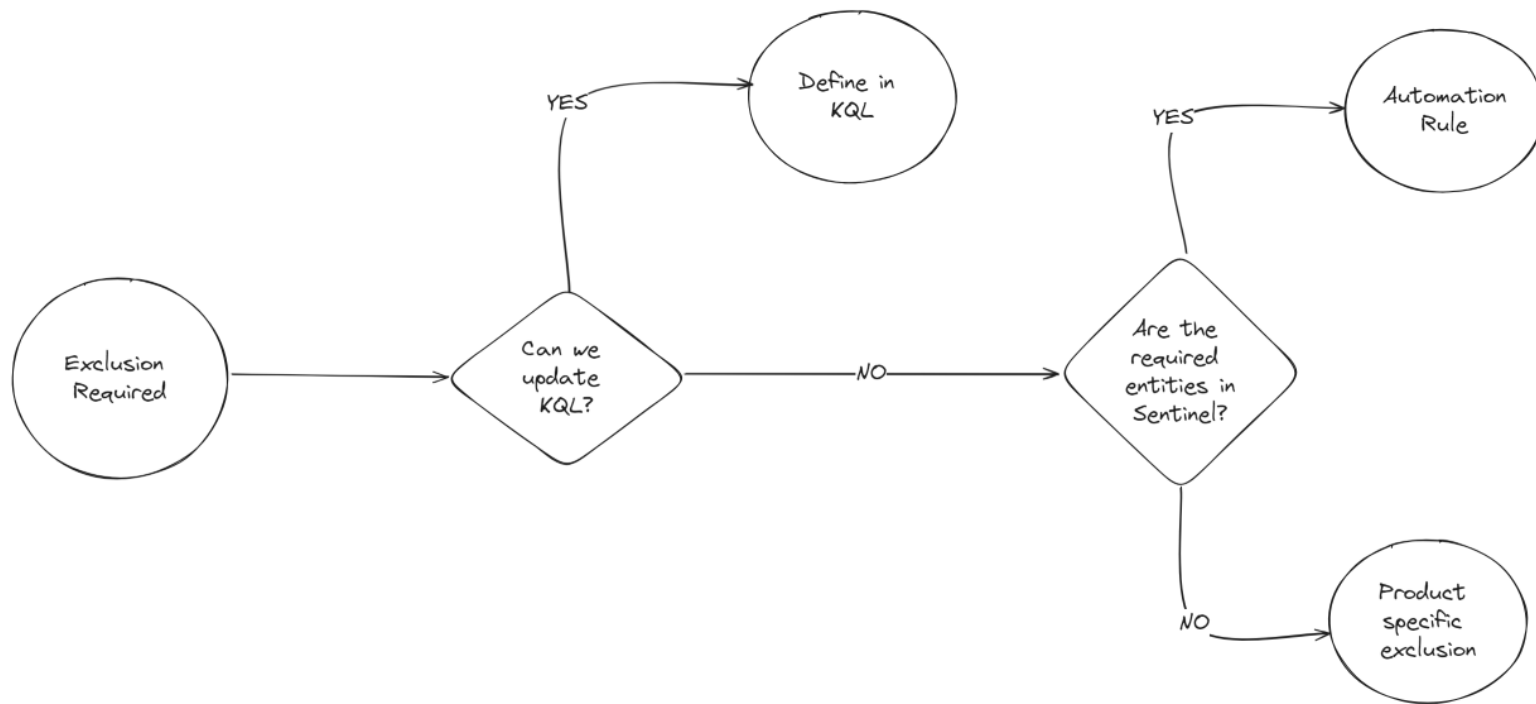


INS PARK



cegeka

# Decision tree





# 5. Detection Engineering



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka



# Why?



CLOSE GAPS IN DETECTION  
MECHANISMS



REDUCED DWELL TIME



DETECT ADVANCED ADVERSARIES  
EVADING TRADITIONAL  
DETECTION SOFTWARE



SquaredUp



infinity



INTERSTELLAR



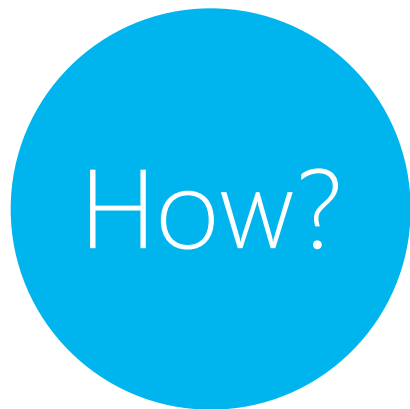
kpn  
Partner Network



INS PARK



cegeka



1

Building detection rules

2

Adding tools or data sources

3

Changing data collection logic



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka



# Types of detection rules



(SUSPECTED)  
THREATS



ANOMALIES



ITEMS OF  
SPECIAL INTEREST

# Types of detection rules



C2  
COMMUNICATION

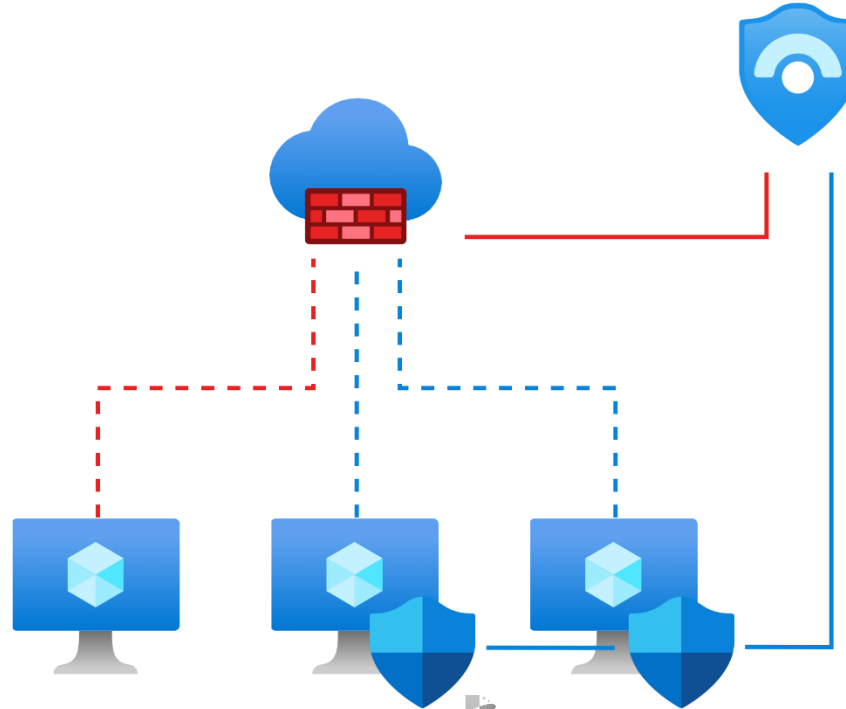


USAGE OF  
UNUSUAL TLD'S

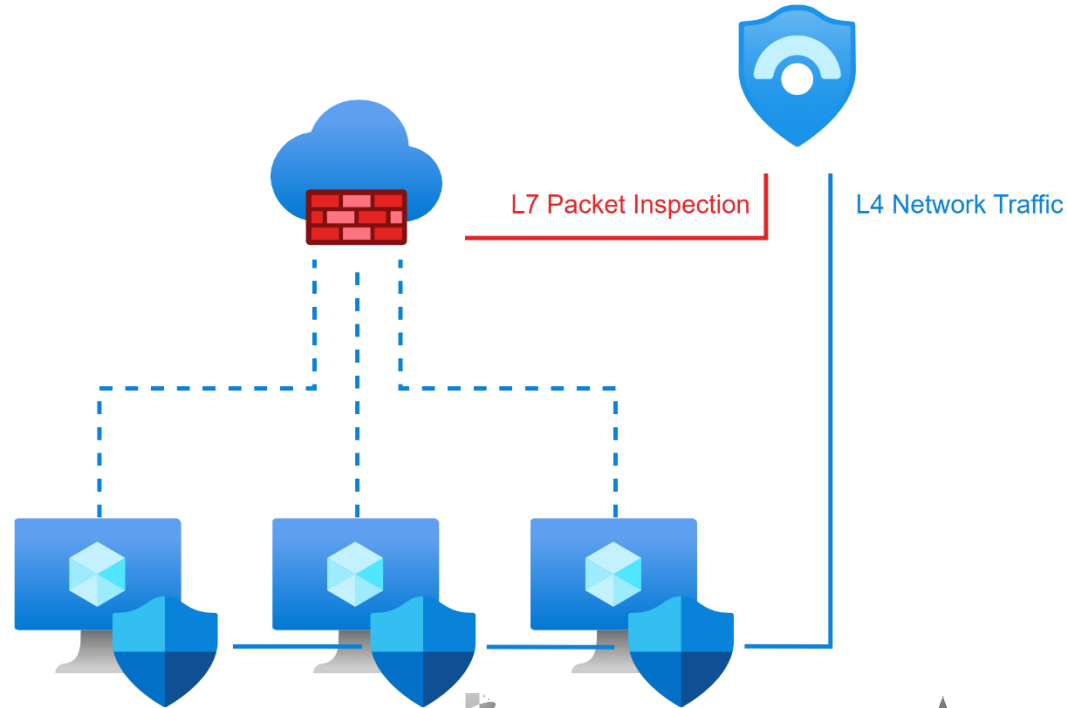


DNS LOOKUP OF  
ILLEGAL SITE

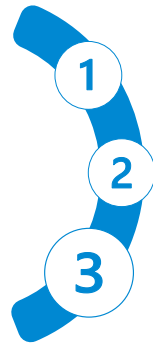
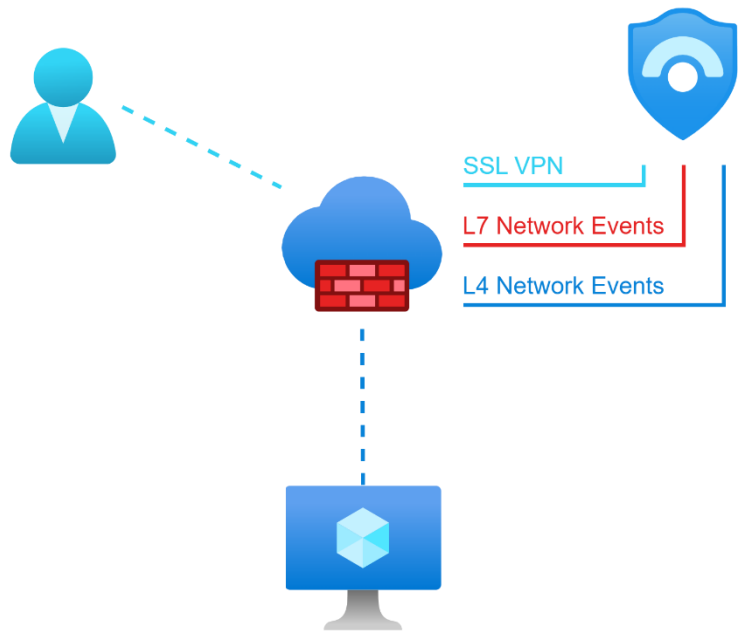
# Adding tools or data



# Adding tools or data



# Data collection logic



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka

# Where do you start?



Identify crown jewels and  
evaluate data value

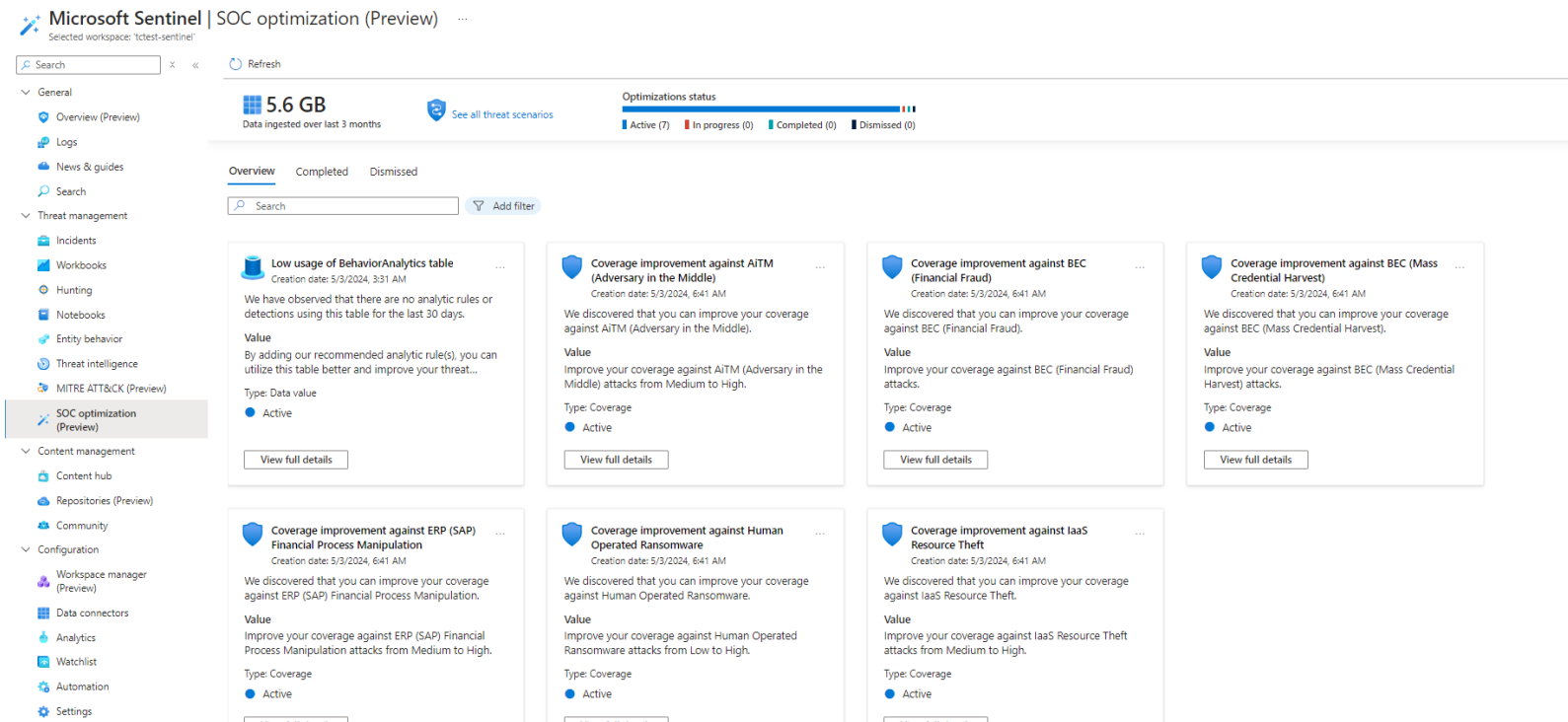


Search capture points



Start with a basic but diverse  
coverage

# SOC Optimization – Basic Detection Gap Analysis



# SOC Optimization – Basic Detection Gap Analysis

## Coverage improvement against BEC (Financial Fraud)

🔄 Mark as in progress ✓ Complete 🗑 Dismiss 🗨 Provide feedback

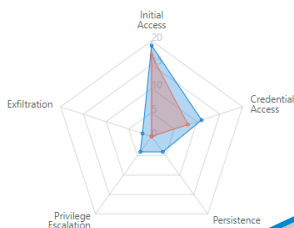
Optimization is calculated every 24 hours | Last update: 3/5/2024

Description  
We discovered that you can improve your coverage against BEC (Financial Fraud).  
[Show more](#)

Status  
● Active  
Type  
● Coverage

Value  
Improve your coverage against BEC (Financial Fraud) attacks.

Improve coverage



Recommended

[View all MITRE ATT&CK technique improvement](#)

Take action  
Go to content hub and add 8 new analytic rules. You can also create your own rule to achieve the recommended level of coverage. [Learn more.](#)

⚠ Pay attention  
For optimal fit, we recommend tuning the detections.

[Go to Content hub](#)

## MITRE ATT&CK technique improvement

Tactic	Current	Recommended
Initial Access (1)		
T1566 - Phishing	7	9
Credential Access (1)		
T1110 - Brute Force	2	5
Persistence (2)		
T1098 - Account Manipulation	0	3
T1078 - Valid Accounts	10	13
Privilege Escalation (1)		
T1078 - Valid Accounts	10	14
Exfiltration (1)		
T1020 - Automated Exfiltration	0	2

## Coverage improvement against BEC (Financial Fraud)

🔄 Refresh ⚙ Install 🗨 Guides & Feedback

⚠ Analytic Rules may be dependent on OOTB parsers to be installed to function. Please ensure that the relevant parsers are deployed in the workspace.

4

Installed content items

2

Configuration needed

Search...

<input type="checkbox"/>	Content name	Created content	Content type	Version	Status
<input type="checkbox"/>	New User Assigned to Privileged Role	...	AnalyticRule	1.1.0	Installed
<input type="checkbox"/>	Admin promotion after Role Management Application Permission Grant	...	AnalyticRule	1.0.4	Installed
<input type="checkbox"/>	Privileged Account Permissions Changed	...	AnalyticRule	1.0.1	...
<input type="checkbox"/>	User Added to Admin Role	...	AnalyticRule	1.0.2	...
<input type="checkbox"/>	Cisco SEG - Malicious attachment not blocked	...	AnalyticRule	1.0.1	...
<input type="checkbox"/>	Cisco SEG - Multiple suspicious attachments received	...	AnalyticRule	1.0.1	...
<input type="checkbox"/>	[Recommended] Cisco Secure Email Gateway via AMA	...	DataConnector	1.0.0	...
<input type="checkbox"/>	Office365 SharePoint File transfer above threshold	...	AnalyticRule	1.0.2	...
<input type="checkbox"/>	Office365 SharePoint File transfer above threshold	...	AnalyticRule	1.0.2	...
<input type="checkbox"/>	Microsoft Entra ID	See rule 1 items	DataConnector	1.0.0	Installed
<input type="checkbox"/>	Microsoft 365 (formerly, Office 365)	See rule 1 items	DataConnector	2.0.0	Installed
<input type="checkbox"/>	Okta Single Sign-On (using Azure Functions)	...	DataConnector	1.0.0	...
<input type="checkbox"/>	Okta Single Sign-On (Preview)	...	DataConnector	1.0.0	...



SquaredUp



Partner Network



INSPIRE



cegeka



# Advanced Detection Gap Analysis

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (3/3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5/5)	Abuse Elevation Control Mechanism (4/4)	Abuse Elevation Control Mechanism (4/4)	Adversary-in-the-Middle (3/3)	Account Discovery (4/4)	Exploitation of Remote Services	Adversary-in-the-Middle (3/3)	Application Layer Protocol (4/4)	Automated Exfiltration (1/1)	Account Access Removal
Gather Victim Host Information (4/4)	Acquire Infrastructure (8/8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9/9)	BITS Jobs	Access Token Manipulation (5/5)	Access Token Manipulation (5/5)	Brute Force (4/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3/3)	Compromise Accounts (3/3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14/14)	Boot or Logon Autostart Execution (14/14)	BITS Jobs	Credentials from Password Stores (5/5)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2/2)	Exfiltration Over Alternative Protocol (3/3)	Data Encrypted for Impact
Gather Victim Network Information (6/6)	Compromise Infrastructure (7/7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5/5)	Boot or Logon Initialization Scripts (5/5)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2/2)	Automated Collection	Data Obfuscation (3/3)	Exfiltration Over C2 Channel	Data Manipulation (3/3)
Gather Victim Org Information (4/4)	Develop Capabilities (4/4)	Phishing (3/3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (4/4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (7/7)	Browser Session Hijacking	Dynamic Resolution (3/3)	Disk Wipe (2/2)	Defacement (2/2)
Phishing for Information (3/3)	Establish Accounts (3/3)	Replication Through Removable Media	Inter-Process Communication (3/3)	Compromise Client Software Binary	Domain Policy Modification (2/2)	Deploy Container	Forge Web Credentials (2/2)	Cloud Service Object Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2/2)	Endpoint Denial of Service (4/4)	Firmware Corruption
Search Closed Sources (2/2)	Obtain Capabilities (6/6)	Supply Chain Compromise (3/3)	Native API	Create Account (3/3)	Domain Policy Modification (2/2)	Direct Volume Access	Input Capture (4/4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Inhibit System Recovery	Network Denial of Service (2/2)
Search Open Technical Databases (5/5)	Stage Capabilities (6/6)	Trusted Relationship	Scheduled Task/Job (5/5)	Create or Modify System Process (4/4)	Event Triggered Execution (16/16)	Execution Guardrails (1/1)	Modify Authentication Process (8/8)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (2/2)	Ingress Tool Transfer	Resource Hijacking	Service Stop
Search Open Websites/Domains (3/3)	Valid Accounts (4/4)	Serverless Execution	Event Triggered Execution (16/16)	Event Triggered Execution (16/16)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2/2)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (4/4)	Data from Information Repositories (3/3)	Multi-Stage Channels	Scheduled	
Search Victim-Owned Websites		Shared Modules	External Remote Services	External Remote Services	Hijack Execution Flow (12/12)	Hide Artifacts (10/10)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		
		Software Deployment Tools	Hijack Execution Flow (12/12)	Hijack Execution Flow (12/12)	Implant Internal Image	Impair Defenses (10/10)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Protocol Tunneling		
		System Services (2/2)	User Execution (3/3)	User Execution (3/3)	Modify Authentication Process (8/8)	Indicator Removal (9/9)	OS Credential Dumping (8/8)	Group Policy Discovery		Data from Removable Media	Proxy (4/4)		
		Windows Management Instrumentation	Valid Accounts (4/4)	Valid Accounts (4/4)	Office Application Startup (6/6)	Indirect Command Execution	Steal Application Access Token	Network Service Discovery		Data from Staged (2/2)	Remote Access Software		
						Masquerading (8/8)	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (3/3)	Traffic Signaling (2/2)		
						Modify Authentication Process (8/8)	Steal or Forge Kerberos Tickets	Network Sniffing		Input Capture	Web Service (3/3)		
								Password Policy Discovery					
								Peripheral Device Discovery					
								Permission Groups Discovery (3/3)					

MITRE ATT&CK® Navigator v5.0.1



SquaredUp



kpn Partner Network

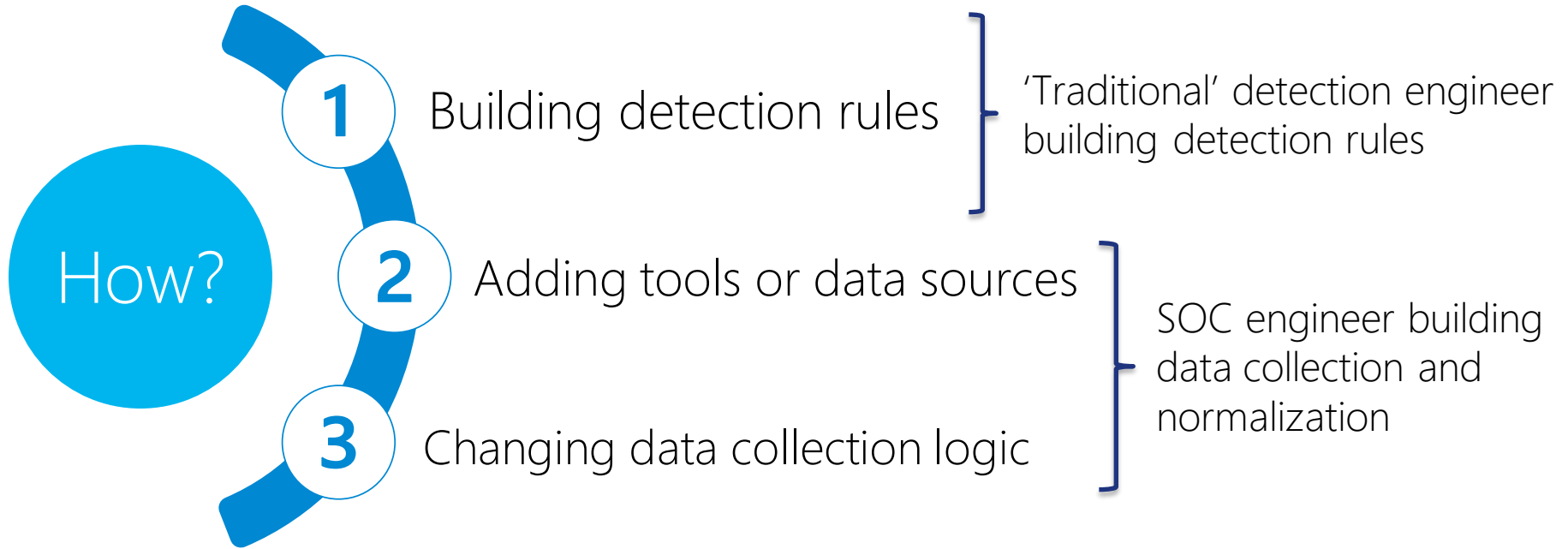


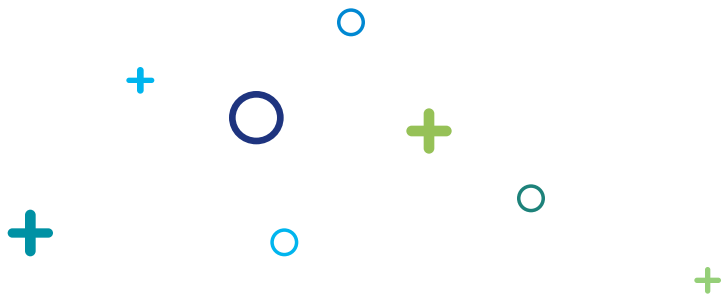
INS PARK



cegeka

# Detection Engineering Responsibilities





## 6. Data collection



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



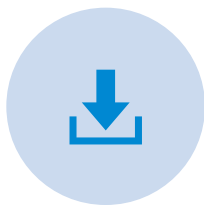
INSPARK



cegeka



# Data Collection



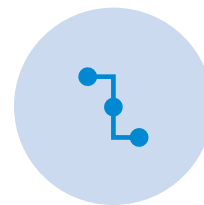
AGENTS



FORWARDERS



CODELESS  
CONNECTOR  
PLATFORM



API INTEGRATION



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka

# Agents

## Microsoft Monitor Agent

- Legacy
- Less flexibility
- No data transformation
- Connected to Log Analytics Workspace
- End of life

## Microsoft Defender for Endpoint

- Less flexibility
- Easy deployment
- No data transformation
- Connected to Defender XDR

## Azure Monitor Agent

- More flexibility
- Data transformations available
- Associated to DCRs
- Azure ARC

## Sysmon

- Extra agent
- MMA or AMA still needed
- Good for edge cases



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka



# Forwarders

- Forward data from device where no agent install is possible
- Network appliances, hypervisors, etc.
- Syslog, beats, log4j, SNMP, etc.
- Mainly used in on-premise scenario's



# Forwarders



Azure Monitor Agent

- Easier than Logstash
- Normalization and transformation via DCR



Logstash

- Local filtering
- DCR support
- Can run in containers
- Variety of input plugins
- No ARC onboarding



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka

# Codeless Connector Platform

The screenshot shows the configuration page for the 'Microsoft Defender for Endpoint Device Inventory' connector. The interface is dark-themed. On the left, there's a sidebar with a 'Delete' button, a status indicator showing 'Disconnected Status' and 'Custom Provider', and a 'Last Log Received' timestamp. Below this is a description area and a table for 'Content source' and 'Version'. The table shows 'Microsoft Defender for Endpoint Device Inventory' with version '1.0.0'. There's also an 'Author' section showing 'Custom' and 'Supported by Microsoft Corporation | Email'. Below that is a 'Related content' section with 'Workbooks', 'Queries', and 'Analytics rules templates'. At the bottom left is a 'Data received' section with a line graph showing data points from March 7 to March 13. The graph shows a single data point at March 7. Below the graph is a 'Data types' section showing 'MDEDeviceInventory\_CL --'. On the right, there's a 'Prerequisites' section stating 'To integrate with Microsoft Defender for Endpoint Device Inventory make sure you have: Workspace: read and write permissions are required.' Below that is a 'Configuration' section with a 'Connect the thing' button. Underneath, there are input fields for 'Client ID' and 'Client Secret', and a 'Connect' button at the bottom.

Microsoft Defender for Endpoint Device Inventory

Delete

Microsoft Defender for Endpoint Device Inventory

Disconnected Status Custom Provider Last Log Received

Description

This is the connector description.

Last data received

...

Content source Version

Microsoft Defender for Endpoint Device Inventory 1.0.0

Author Supported by

Custom Microsoft Corporation | Email

Related content

Workbooks Queries Analytics rules templates

Data received Go to log analytics

4 3 2 1 0

March 7 March 8 March 9 March 10 March 11 March 13

MDEDeviceInventory...

0

Data types

MDEDeviceInventory\_CL --

Prerequisites

To integrate with Microsoft Defender for Endpoint Device Inventory make sure you have:

✓ Workspace: read and write permissions are required.

Configuration

Connect the thing

This is the Mockaroo connector. This will send data to the APIKeyAuthTest DCR via the AWS2 DCE.

Client ID

Client Secret

Connect

## Create Codeless Connectors with the Codeless Connector Builder (Preview)

By  Matthew Lowe

Published Mar 14 2024 05:21 PM

6,005 Views



\*Please note: This workbook is considered Public Preview as there is some supplementary content that is still being finalized while the core functionality is finished. There will be an update in the future to move this to GA.\*

Hate JSON templates? Looking to make your own Codeless Connectors for Microsoft Sentinel? You're in luck. This workbook sets out to create a UI experience for creating Codeless Connectors in order to make it as easy as possible.

This solution currently has not been merged with the main Microsoft Sentinel repository, so it will not appear in Content Hub yet. You can find it for the time being in my personal repo: [raw.githubusercontent.com/malowe101/Sentinel-Projects/master/CCP\\_Builder\\_Preview/CCP-Preview-Full-Workbook](https://raw.githubusercontent.com/malowe101/Sentinel-Projects/master/CCP_Builder_Preview/CCP-Preview-Full-Workbook)



SquaredUp







# API integration

- Two ways
  - Workspace ID & Key (old way)
  - Log Ingestion API
- When data source does not have polling API
- When you want a 'push' scenario



SquaredUp



infinity



INTERSTELLAR



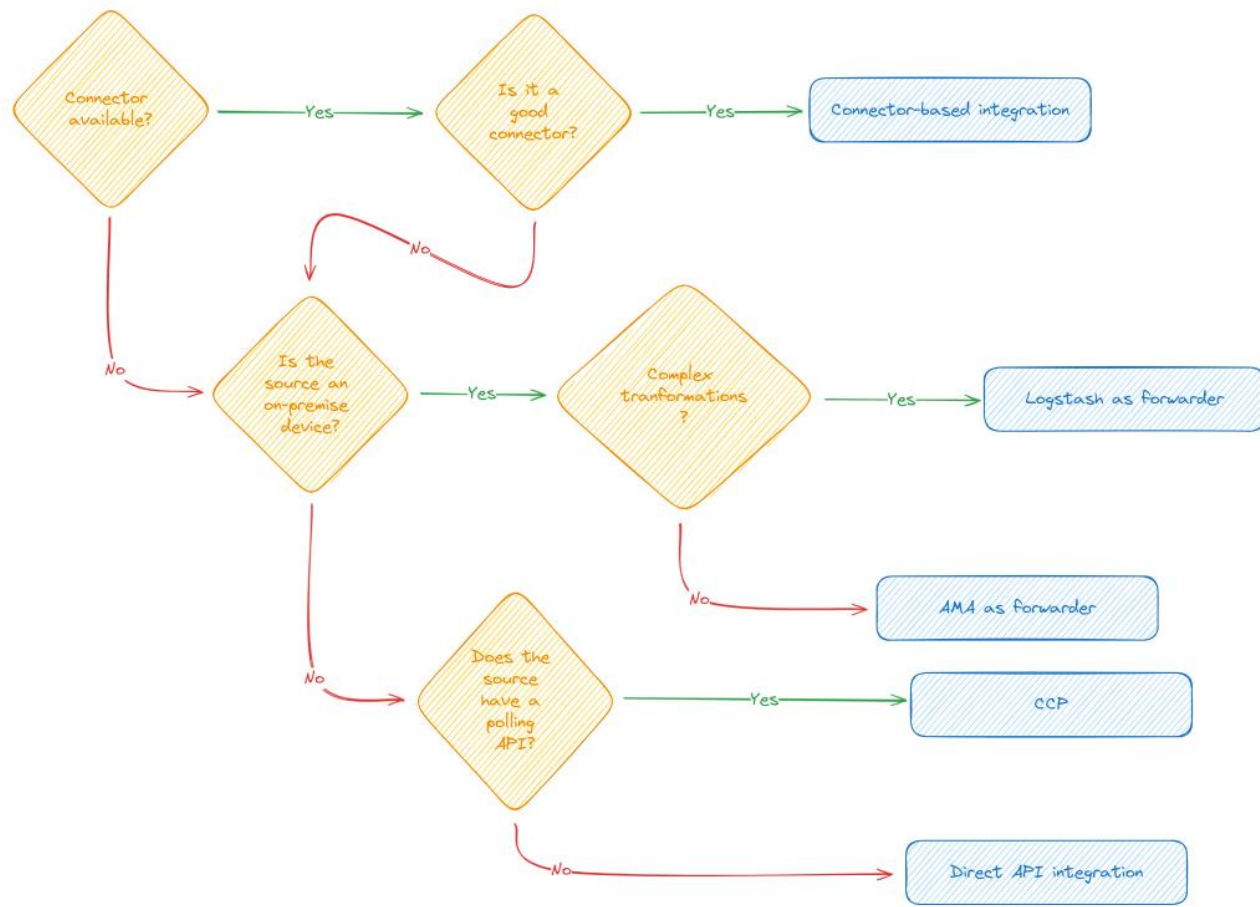
kpn  
Partner Network



INS PARK

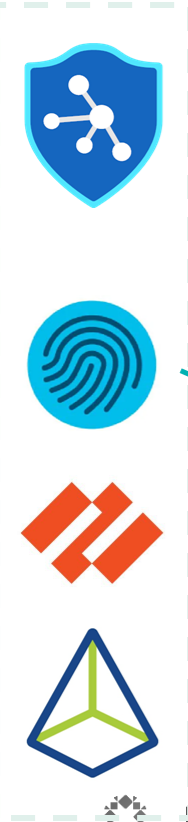


cegeka





On-premise



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka

Cloud Solutions



CATO  
NETWORKS



Native

Native

CCP

Workspace Key

HTTPS

Syslog

Syslog

Syslog

HTTPS

Log  
Ingestion  
API





# 7. Playbook & automations



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka

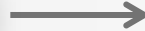
# Automation - Playbooks



Build automated and scalable playbooks that integrate across tools



Azure Logic Apps



Security products

Ticketing systems  
(ServiceNow)

Additional tools



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka



# Common use cases

- Synchronization/notification
- Enrichment
- Action
  - Password reset
  - Device Isolation



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka



# Playbooks for MSSP's

*Have a uniform way to reset a password,  
independent of the customers'  
willingness/trust in automation.*



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka



# Parameter usage

- Single Logic App Across customers
- Parameters configuring:
  - Actions
  - Exclusions
  - Notifications



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network

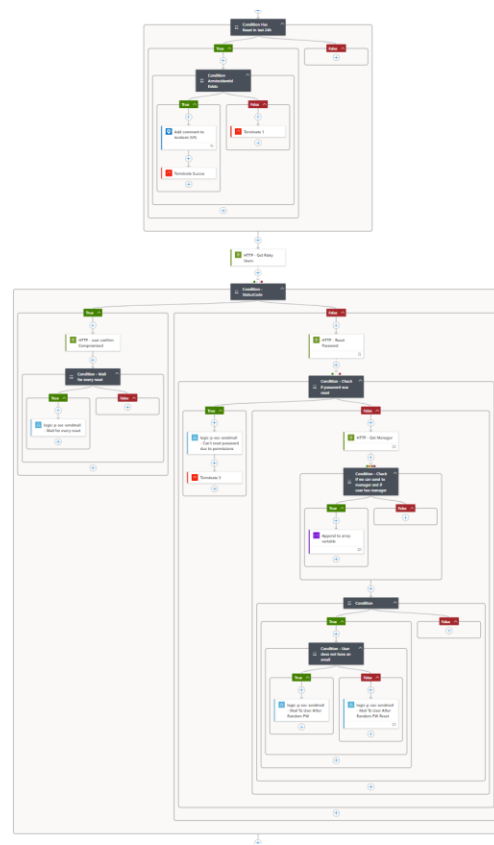


INSPARK



cegeka







# Logic Apps vs Azure Functions

- Native triggers
- Disadvantages:
  - Loops
  - Complex object/array changes



# Azure API Management

- Sub-playbooks
- Multi-tenant scenario
  - Rate limiting



SquaredUp



infinity



INTERSTELLAR



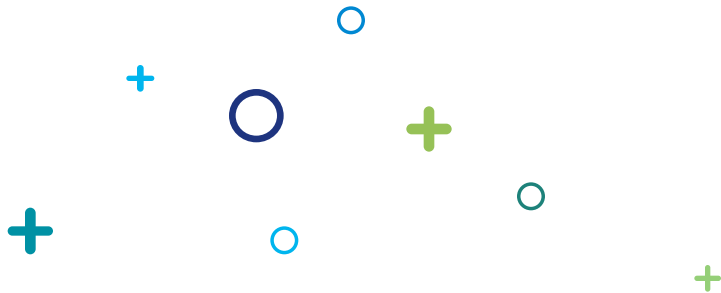
kpn  
Partner Network



INSPARK



cegeka



## 8. Case Management



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka



# Incident Management



SENTINEL



ITSM TOOLING



3<sup>RD</sup> PARTY  
SOAR



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka



# Sentinel Limitations

- Multiple queues
- Customizations
  - Fields
  - Status



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka



# ITSM Tool

- Integration into other business processes
- Lacking SOAR capabilities



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka



# 3<sup>rd</sup> party SOAR

- Feature rich
- Strong investigation experience
- Automation location – Sentinel?
- Additional price



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka





# The Collective Implementation

- JIRA Cloud
- Heavily customized
- Custom sync engine
- Automation within Sentinel
  - Customers' tenant



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka



## 9. Closing off



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INSPARK



cegeka

# Closing off

## Complexity

Building a SOC requires a lot of different specializations

01

02

## Doing the right thing isn't easy

Least Privilege & Native has it's disadvantages

## Personal Approach

Every XDR & SIEM deployment is different – threat is as such

04

03

## Native

Leverage, then build



SquaredUp



infinity



INTERSTELLAR



kpn  
Partner Network



INS PARK



cegeka



Please evaluate this session in the App.

# THANK YOU

**Are there any questions?**





## Next Sessions

**The art of knowing your SIEM & XDR Data- Bert-Jan Pals (19&20)**

**Attack Path Based Detection Engineering – Olaf Hartong (16)**

**Mastering PIM – Louis Mastelinck (21)**

