Architecting a SOC on Defender XDR and Microsoft Sentinel

Thijs Lecomte &

Robbe Van den Daele

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Speakers

Robbe Van den Daele

Security Consultant & SOC Engineer @ The Collective

Thijs Lecomte

Head of Managed Services @ The Collective
Security MVP

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

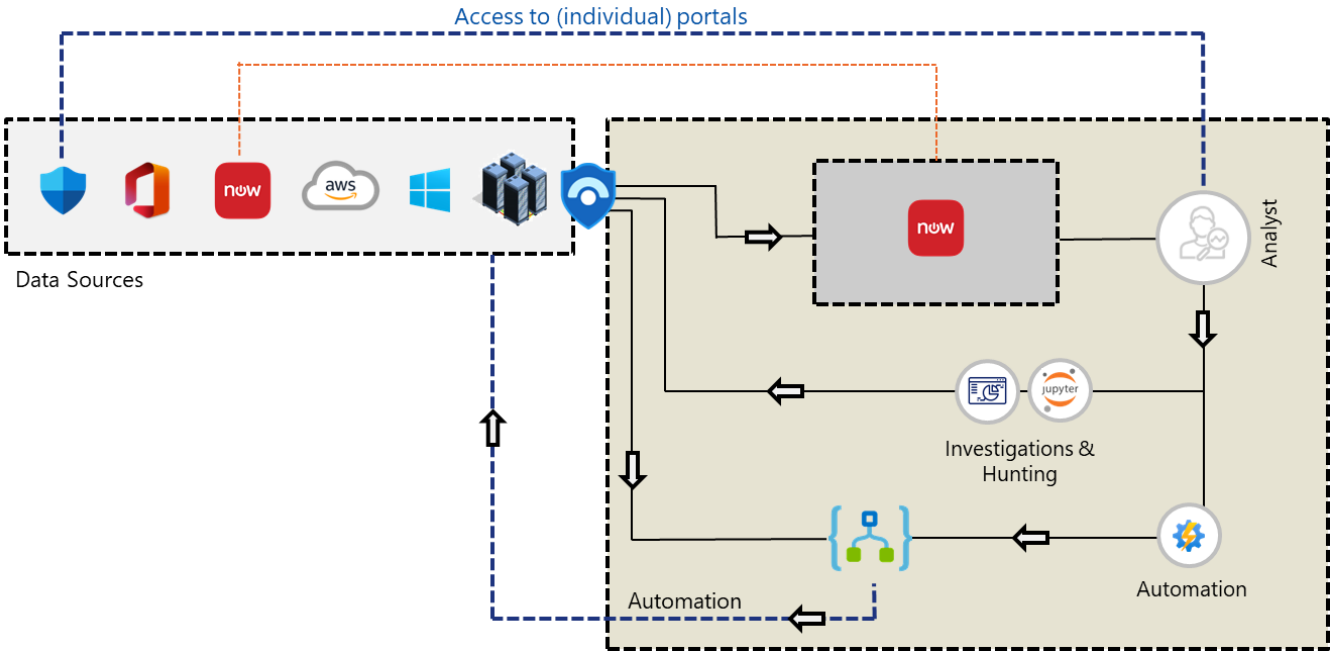
What are we going to discuss?

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

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

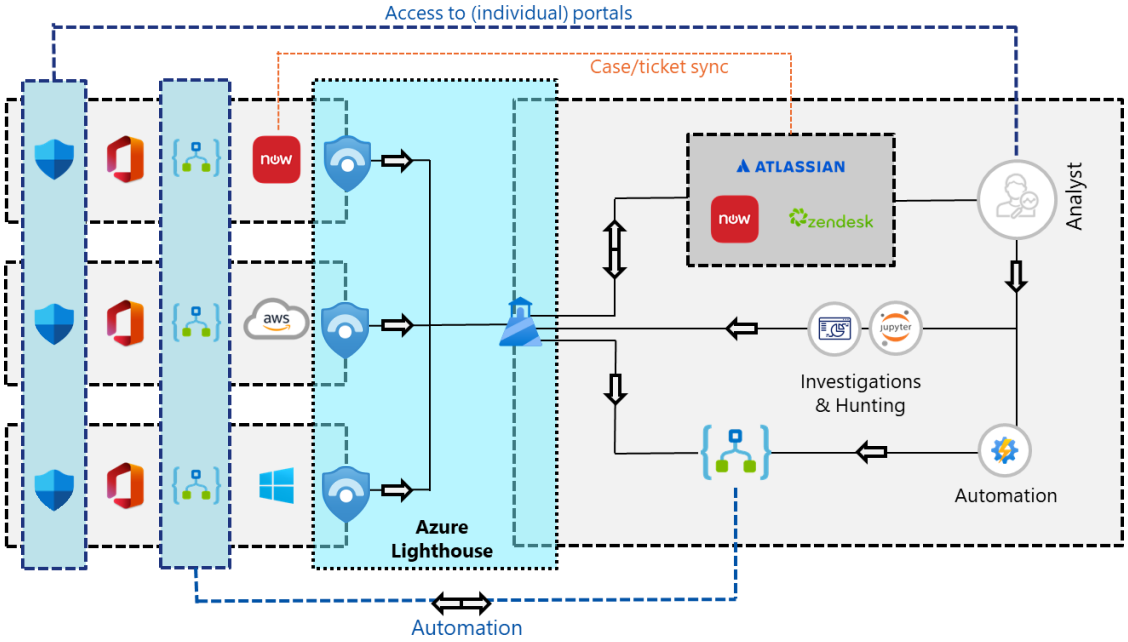
1. Architecture

Single-tenant architecture



rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Multi-tenant architecture



rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Multi workspace setup

REGULATORY COMPLIANCE

DATA OWNERSHIP

MULTIPLE TENANTS

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Multi workspace setup

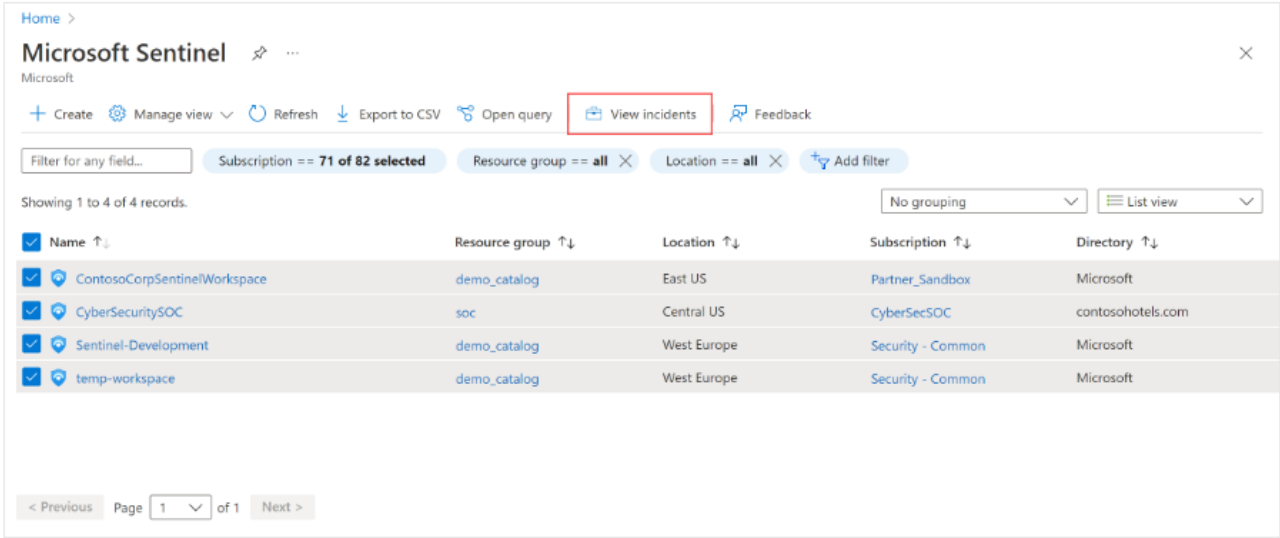
- MSSP should deploy a workspace for each customer in the customer tenant

- Keep architecture as simple as possible for each ‘customer’

- Make sure you have a central management system

Managing a multi workspace setup

Incidents → Multi workspace incident view



rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

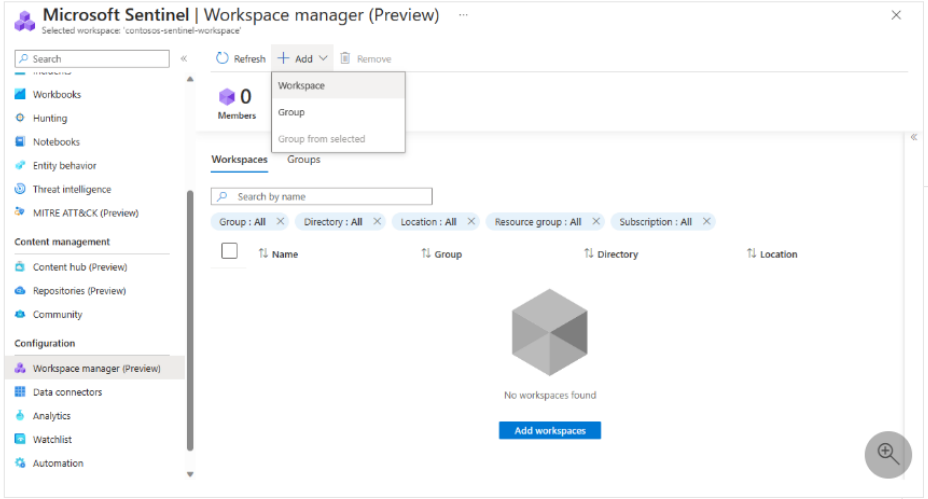
Managing a multi workspace setup

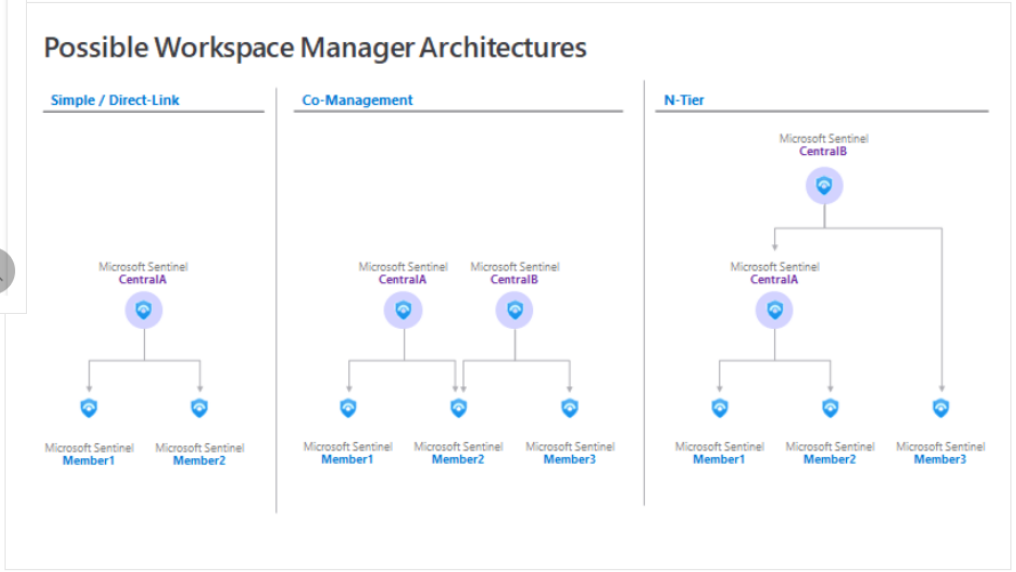
Queries → Multi workspace queries

- 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

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Workspace manager





rubrik Dell Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Protecting intellectual property as MSSP

Hosting content in MSSP tenant

Restricting content in customer tenant

Contractual agreement

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK 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**

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

2. Authentication for multi-tenant deployments

What are the options?

GDAP

Lighthouse

Guest Users

Named Admins

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

What are the options?

GDAP

Lighthouse

Guest Users

Named Admins

	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

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

What are the options?

MSSP Preferred
(MTO)

GDAP

Lighthouse

Guest Users

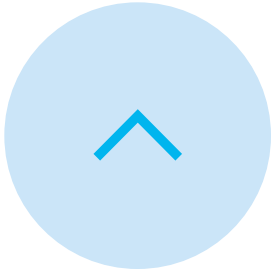
Customer Preferred

Named Admins

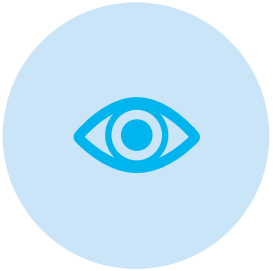
rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

3. Automated deployment

The need for automated deployment



REDUCING
MANUAL EFFORT

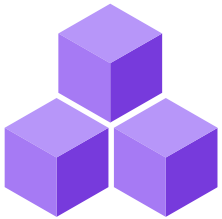


FOUR EYES
PRINCIPLE

AUTOMATIC
VALIDATION

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK 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

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

ARM vs Bicep

Personal choice

Ease of exporting

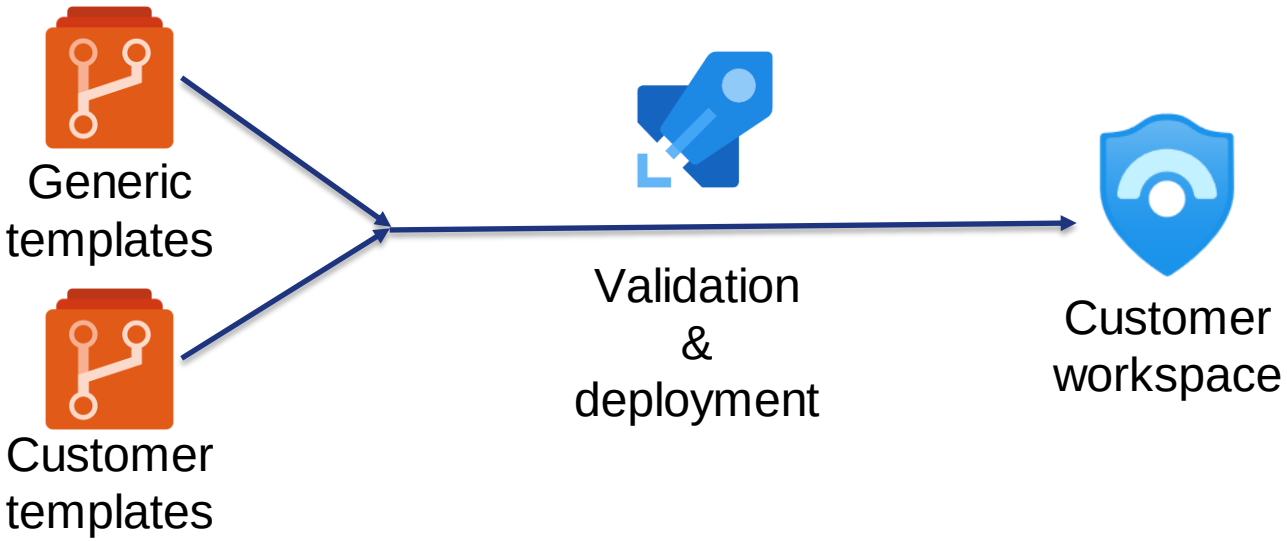
Supported resources

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

The Collective Setup

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

Sample Setup



4. Exclusion management

Why do you need exclusions?

- Decrease false positive
- Avoid negative impact

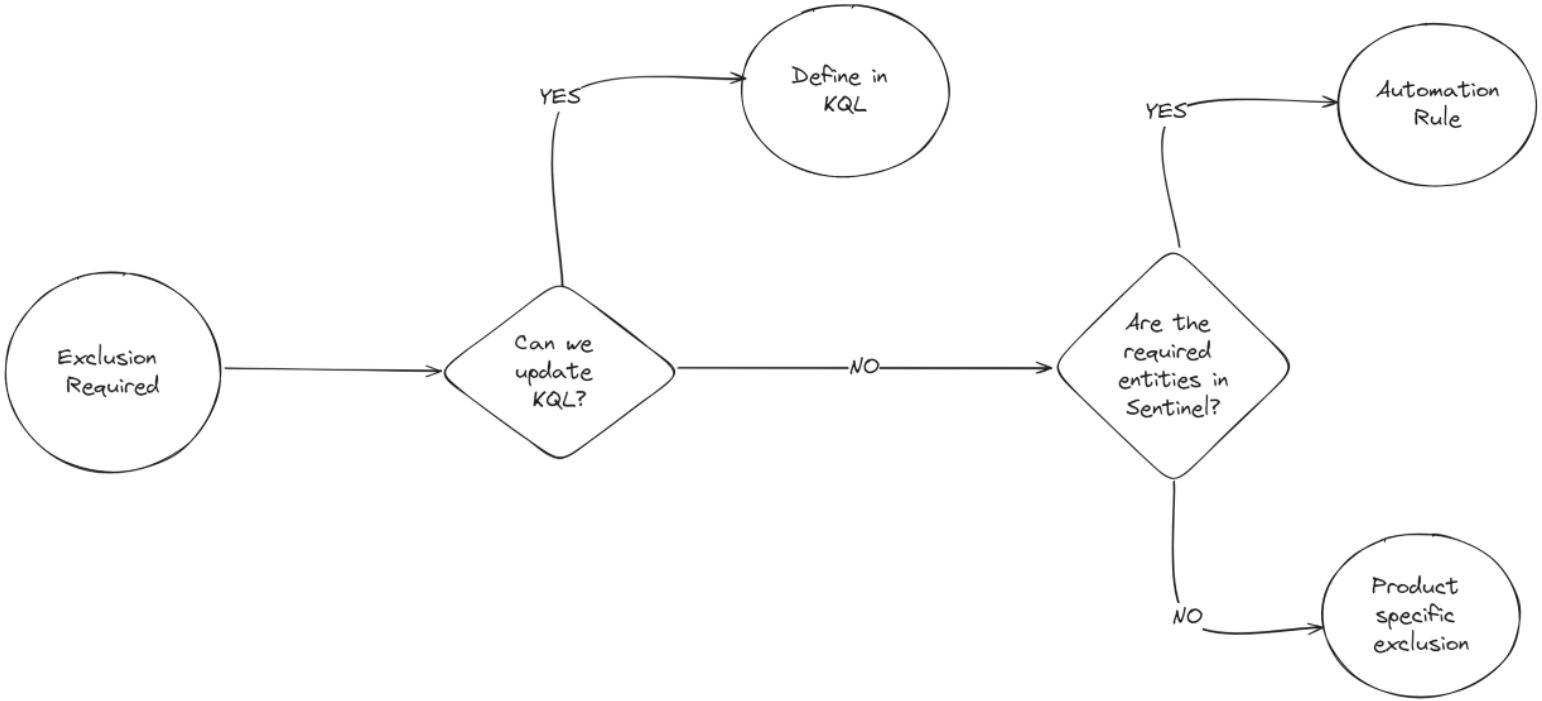
Where to add exclusions

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

Best practices

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

Decision tree



5. Detection Engineering

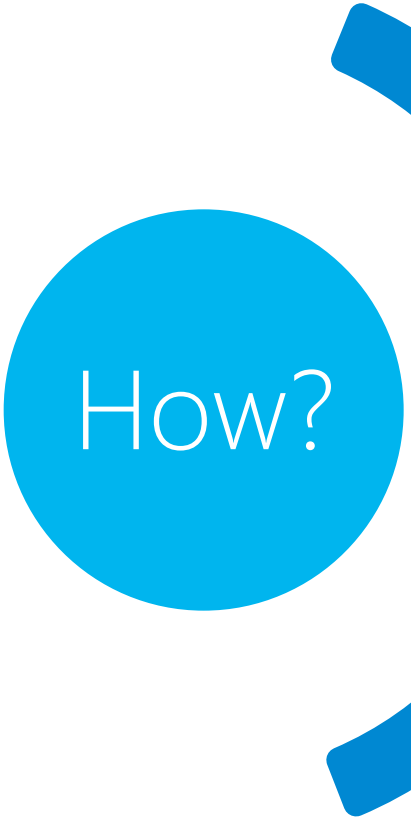
Why?

CLOSE GAPS IN DETECTION MECHANISMS

REDUCED DWELL TIME

DETECT ADVANCED ADVERSARIES EVADING TRADITIONAL DETECTION SOFTWARE

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka



1. Building detection rules
2. Adding tools or data sources
3. Changing data collection logic

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Types of detection rules

(SUSPECTED) THREATS

ANOMALIES

ITEMS OF SPECIAL INTEREST

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Types of detection rules

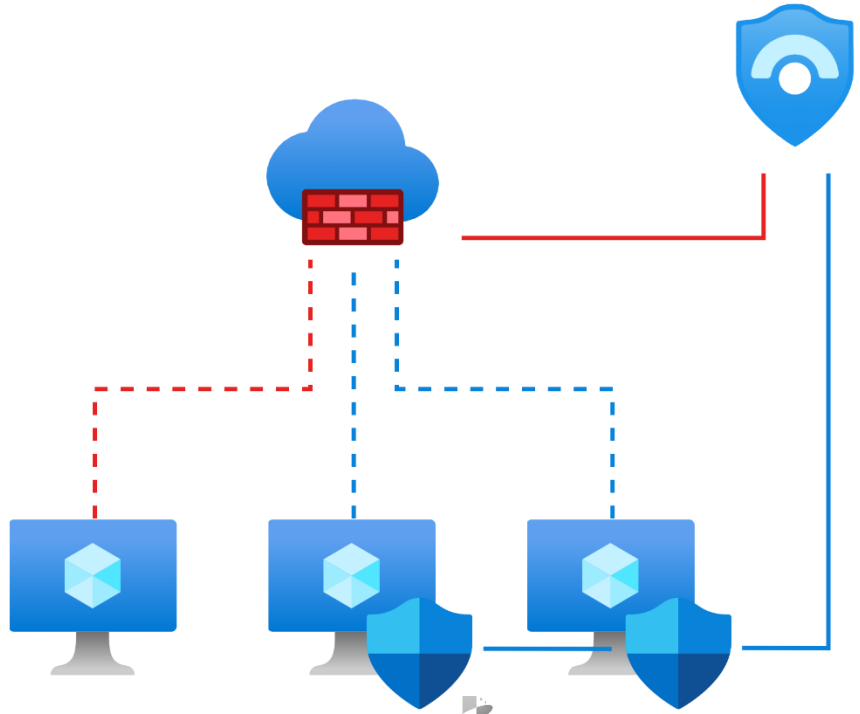
C2 COMMUNICATION

USAGE OF UNUSUAL TLD'S

DNS LOOKUP OF ILLEGAL SITE

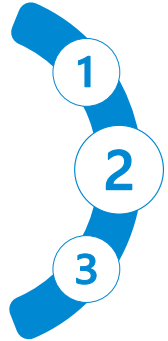
rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

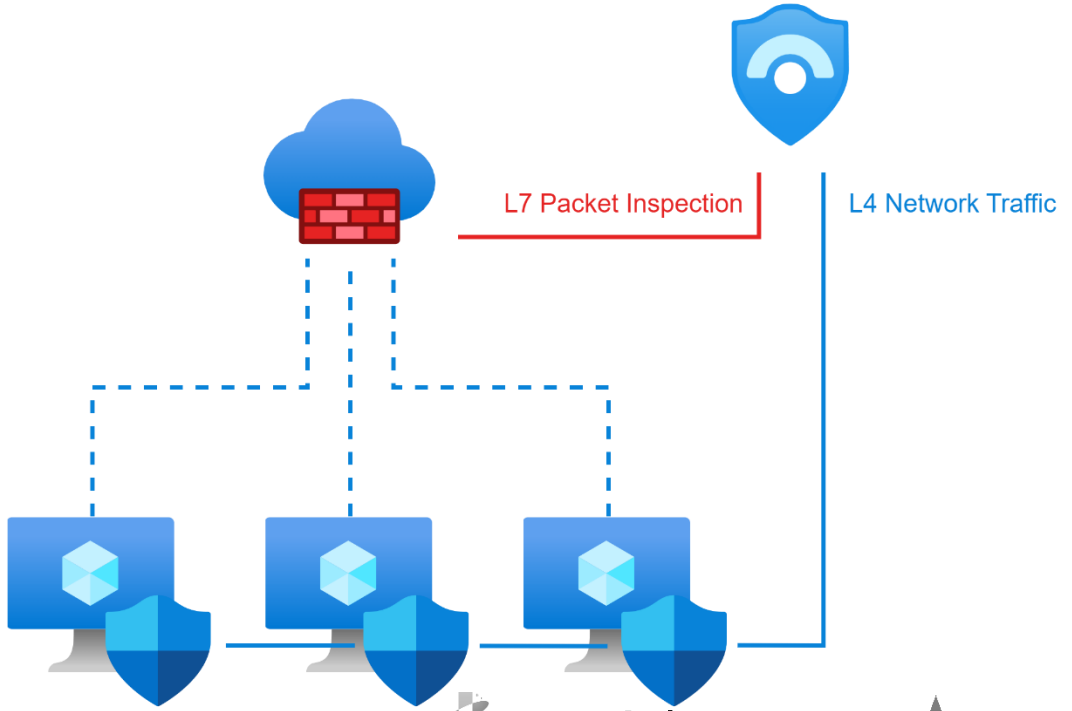
Adding tools or data



rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

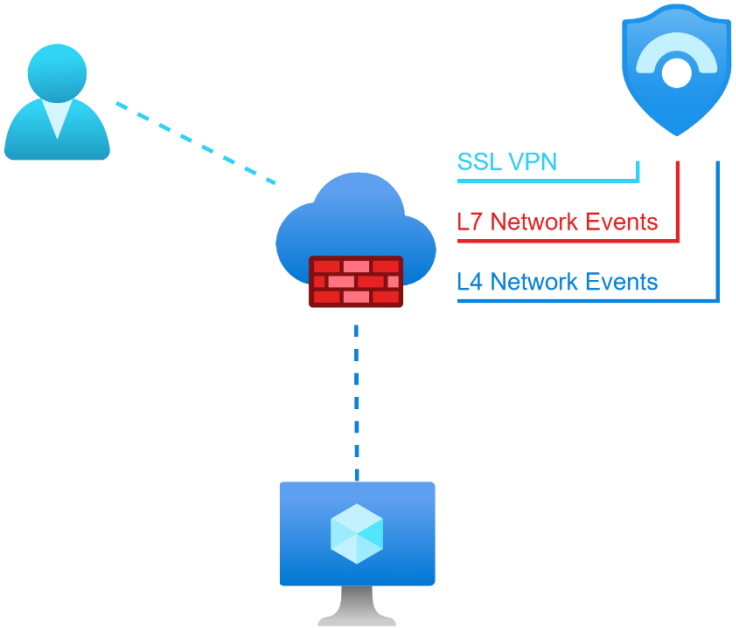
Adding tools or data



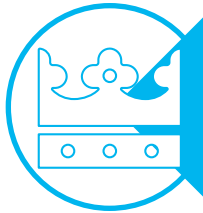


rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

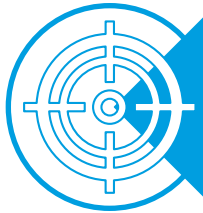
Data collection logic



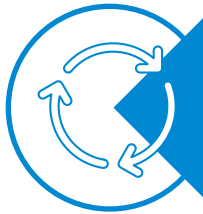
Where do you start?



Identify crown jewels and evaluate data value



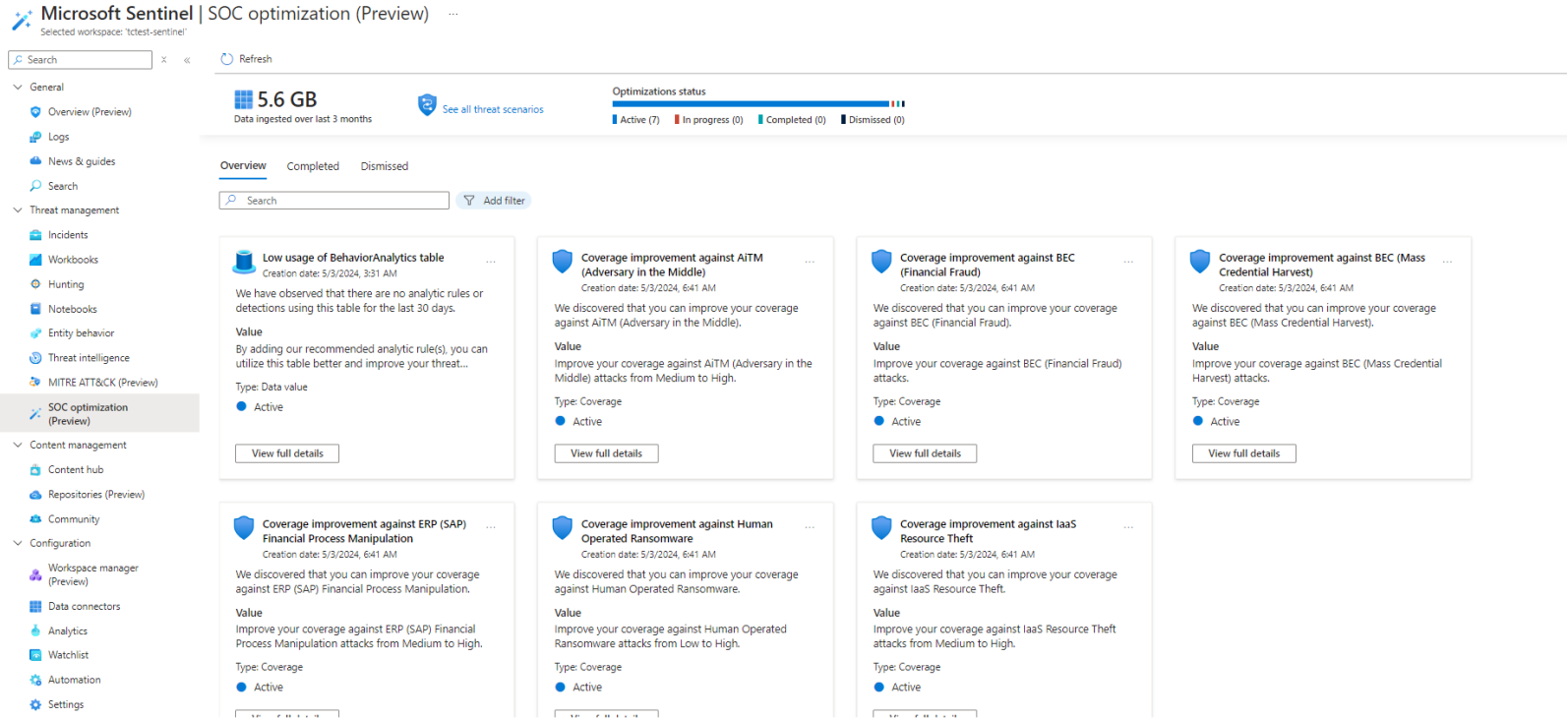
Search capture points



Start with a basic but diverse coverage

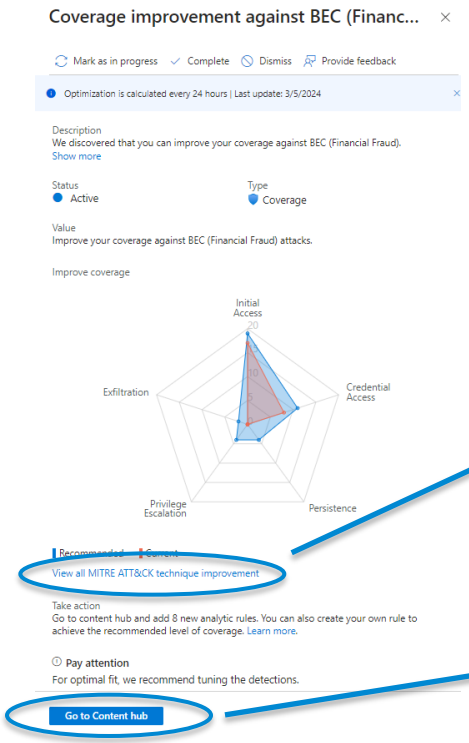
rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

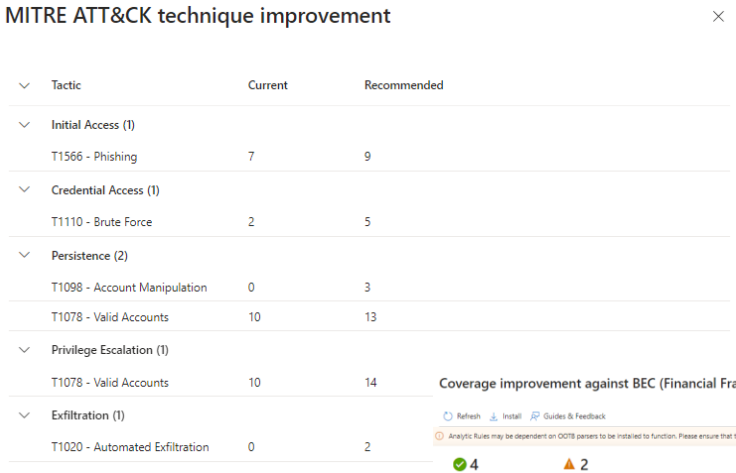
SOC Optimization – Basic Detection Gap Analysis

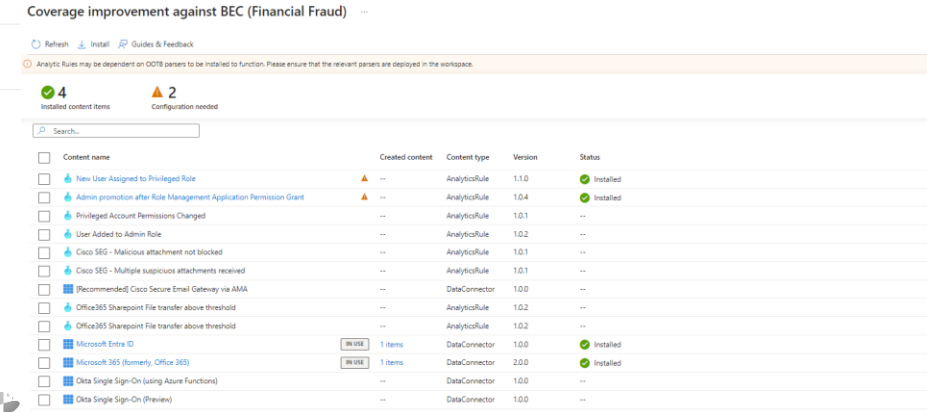


rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

SOC Optimization – Basic Detection Gap Analysis





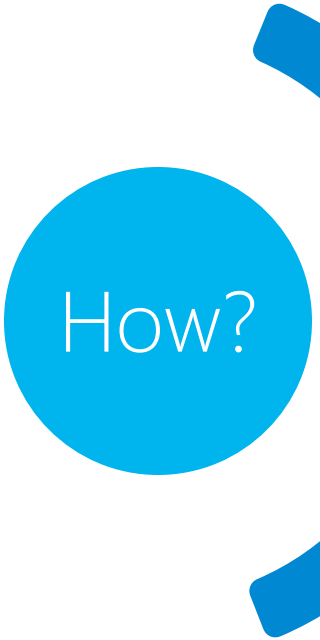


rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Advanced Detection Gap Analysis

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Detection Engineering Responsibilities



1. Building detection rules
2. Adding tools or data sources
3. Changing data collection logic

‘Traditional’ detection engineer building detection rules

SOC engineer building data collection and normalization

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

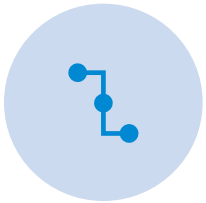
6. Data collection

Data Collection

AGENTS

FORWARDERS

CODELESS CONNECTOR PLATFORM



API INTEGRATION

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK 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

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

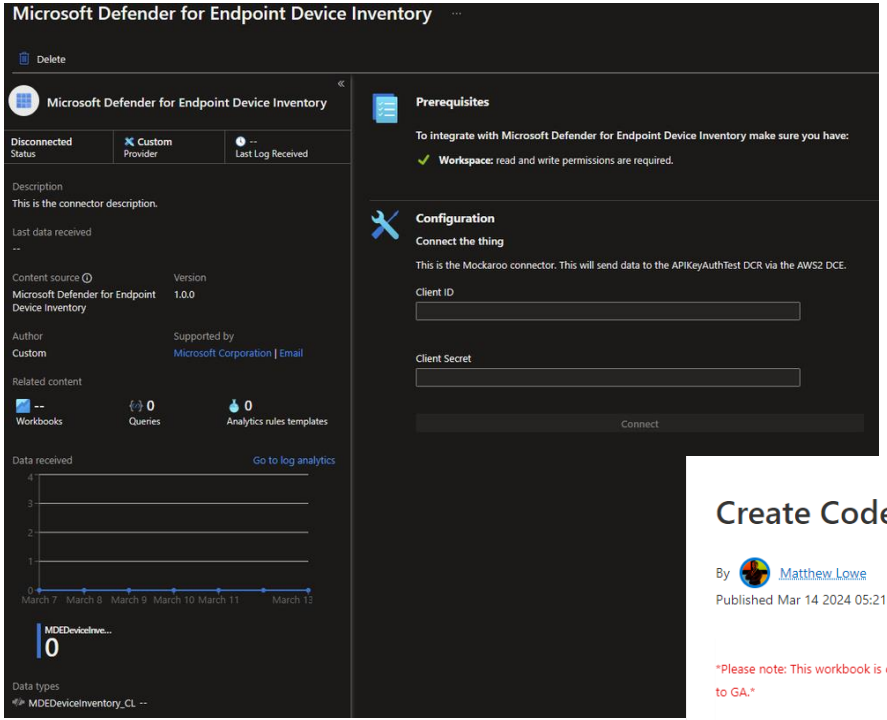
- Easier than Logstash
- Normalization and transformation via DCR

Logstash

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

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

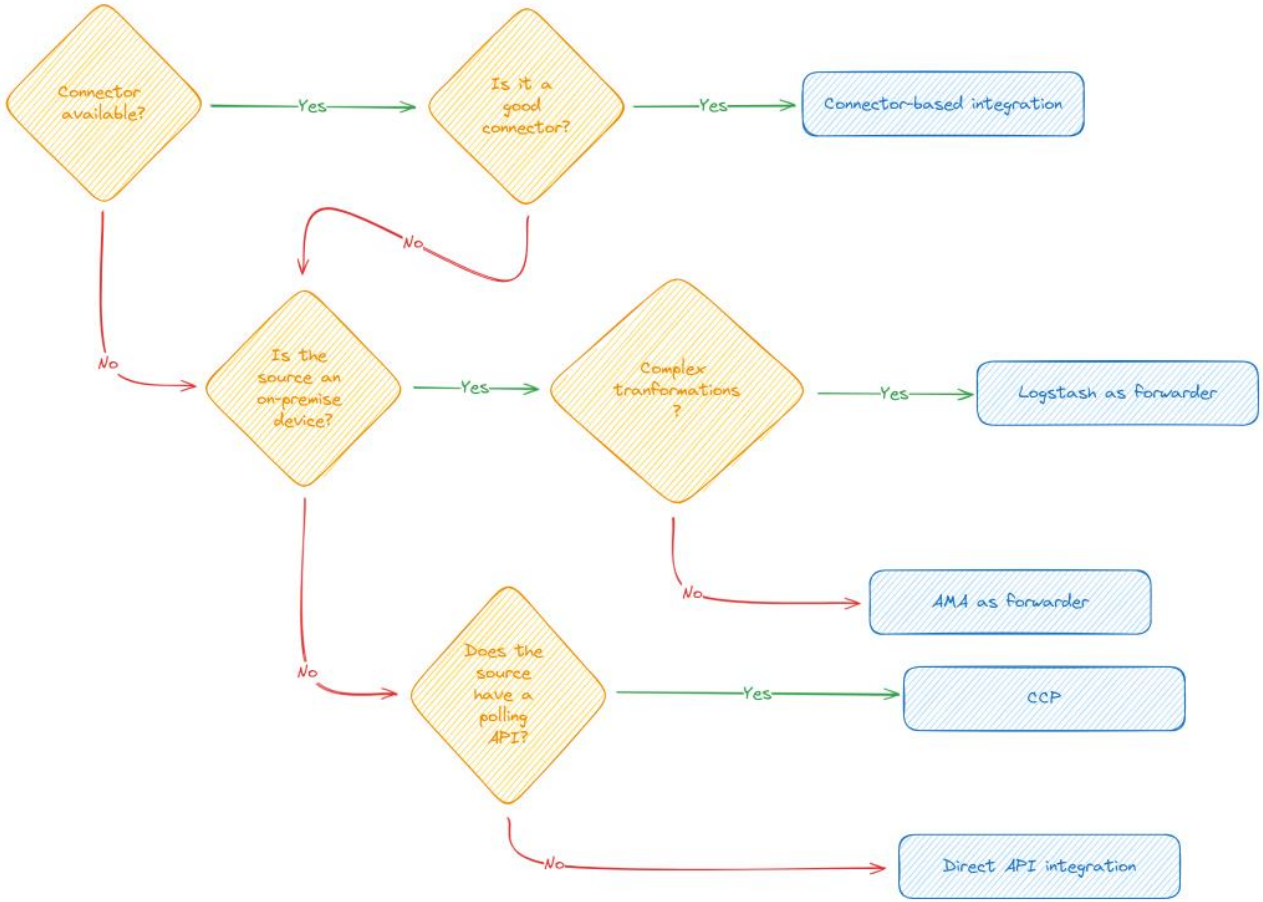
Codeless Connector Platform

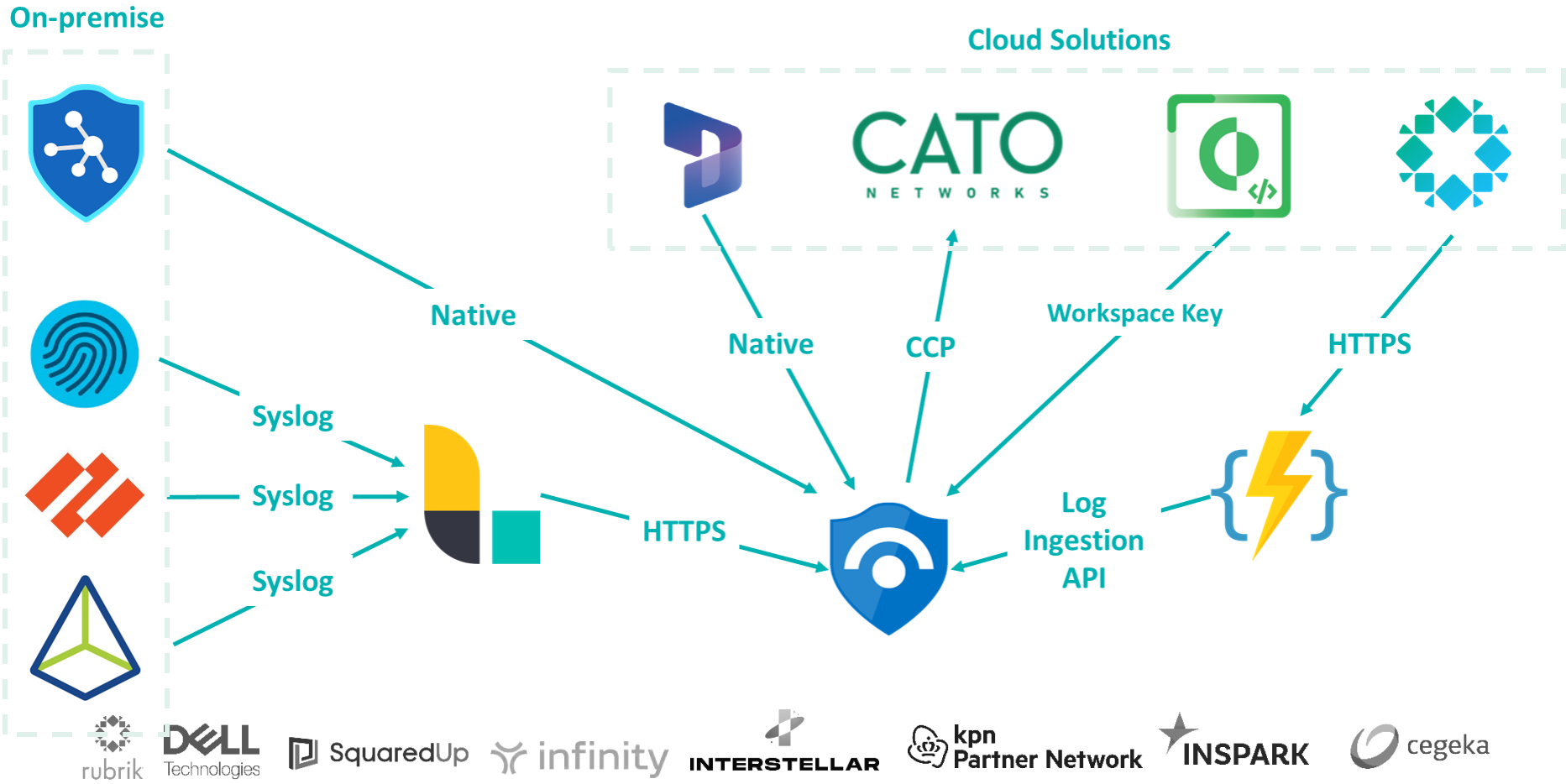


rubrik DELL Technologies SquaredUp in

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

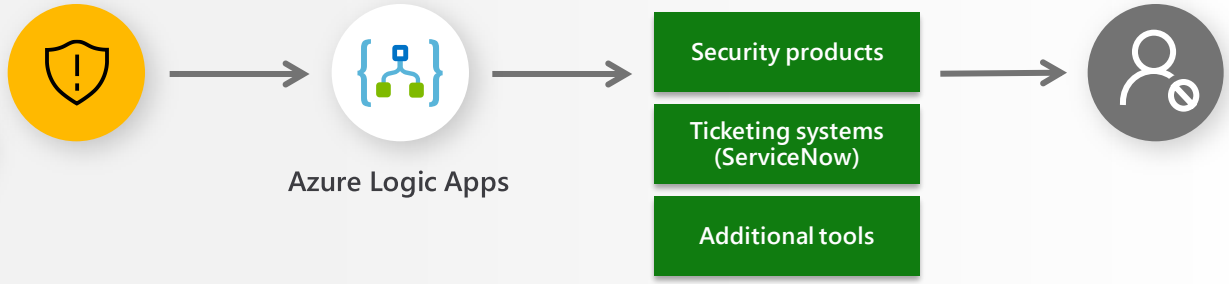



On-premise
Cloud Solutions
CATO
NETWORKS
Native
Native
CCP
Workspace Key
HTTPS
Syslog
Syslog
Syslog
HTTPS
Log
Ingestion
API
rubrik
DELL
Technologies
SquaredUp
infinity
INTERSTELLAR
kpn
Partner Network
INSPARK
cegeka

7. Playbook & automations

Automation - Playbooks

Build automated and scalable playbooks that integrate across tools



rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Common use cases

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

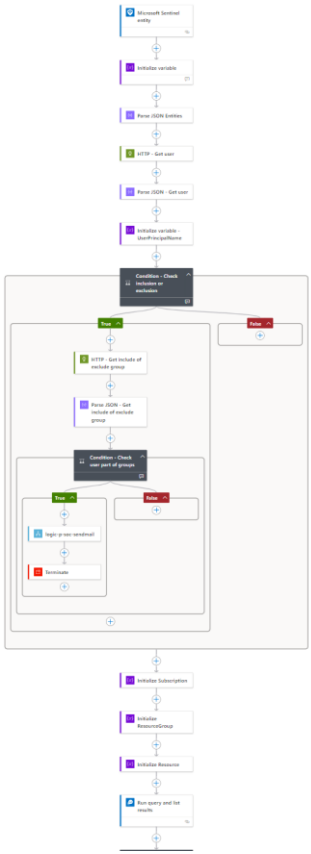
Playbooks for MSSP's

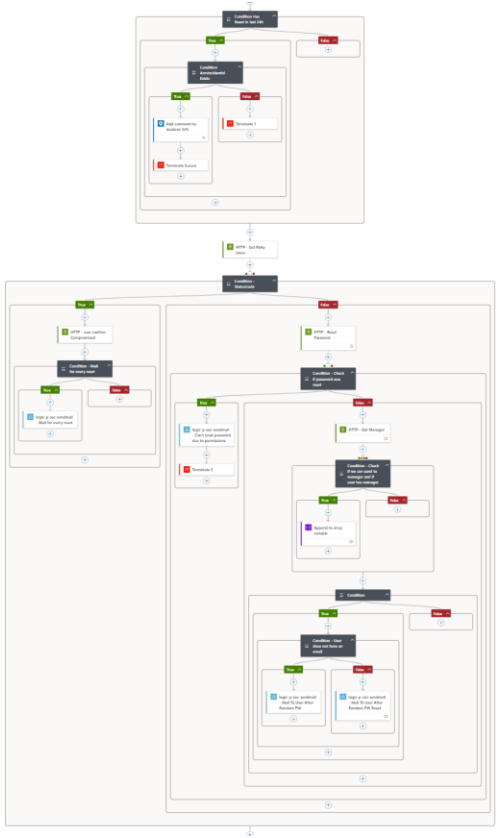
Have a uniform way to reset a password, independent of the customers' willingness/trust in automation.

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Parameter usage

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





rubrik DELL Technologies 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

8. Case Management

Incident Management

SENTINEL

ITSM TOOLING

3RD PARTY

SOAR

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Sentinel Limitations

- Multiple queues
- Customizations
  - Fields
  - Status

ITSM Tool

- Integration into other business processes
- Lacking SOAR capabilities

3rd party SOAR

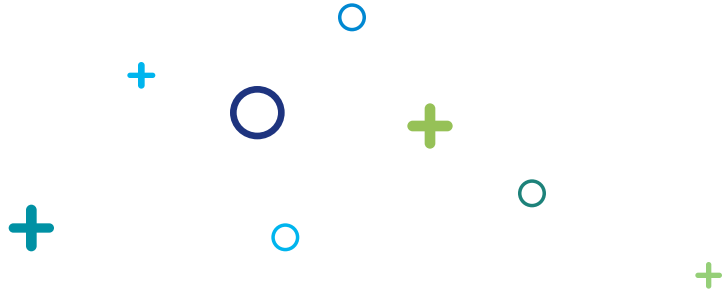
- Feature rich
- Strong investigation experience
- Automation location – Sentinel?
- Additional price

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

The Collective Implementation

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

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka



9. Closing off

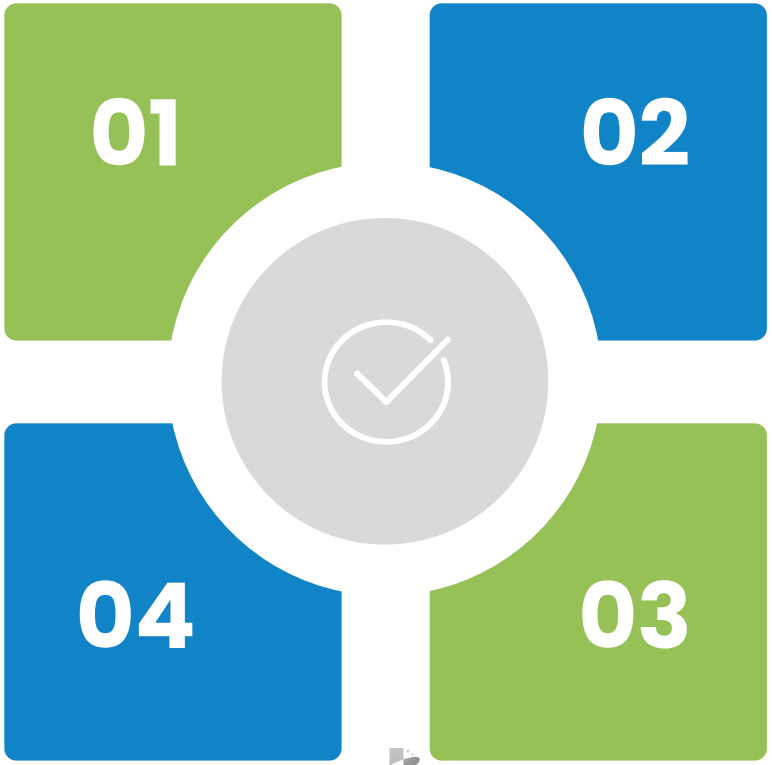
Closing off

Complexity

Building a SOC requires a lot of different specializations

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

Native

Leverage, then build

rubrik DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK 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)