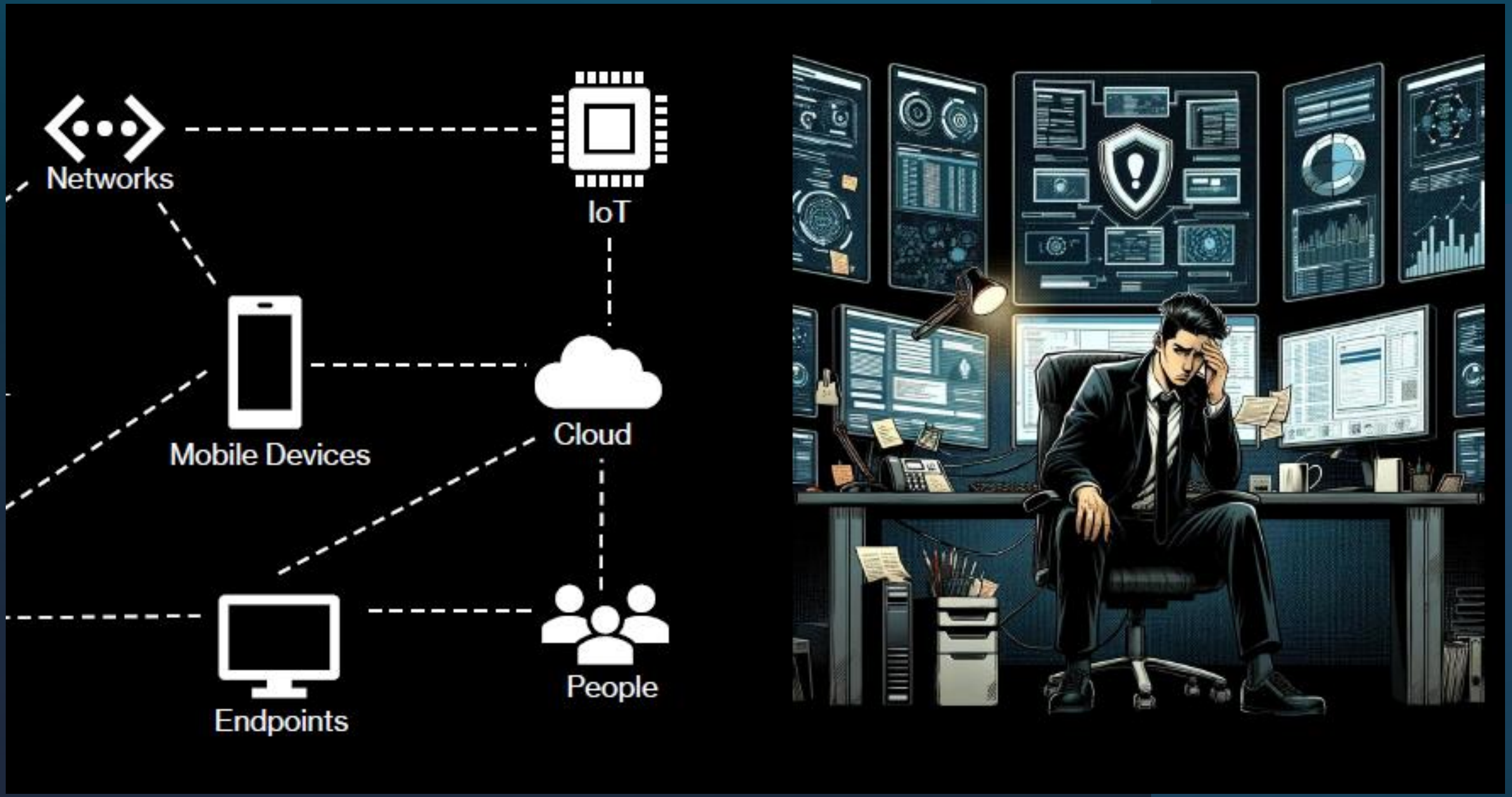
Microsoft Sentinel

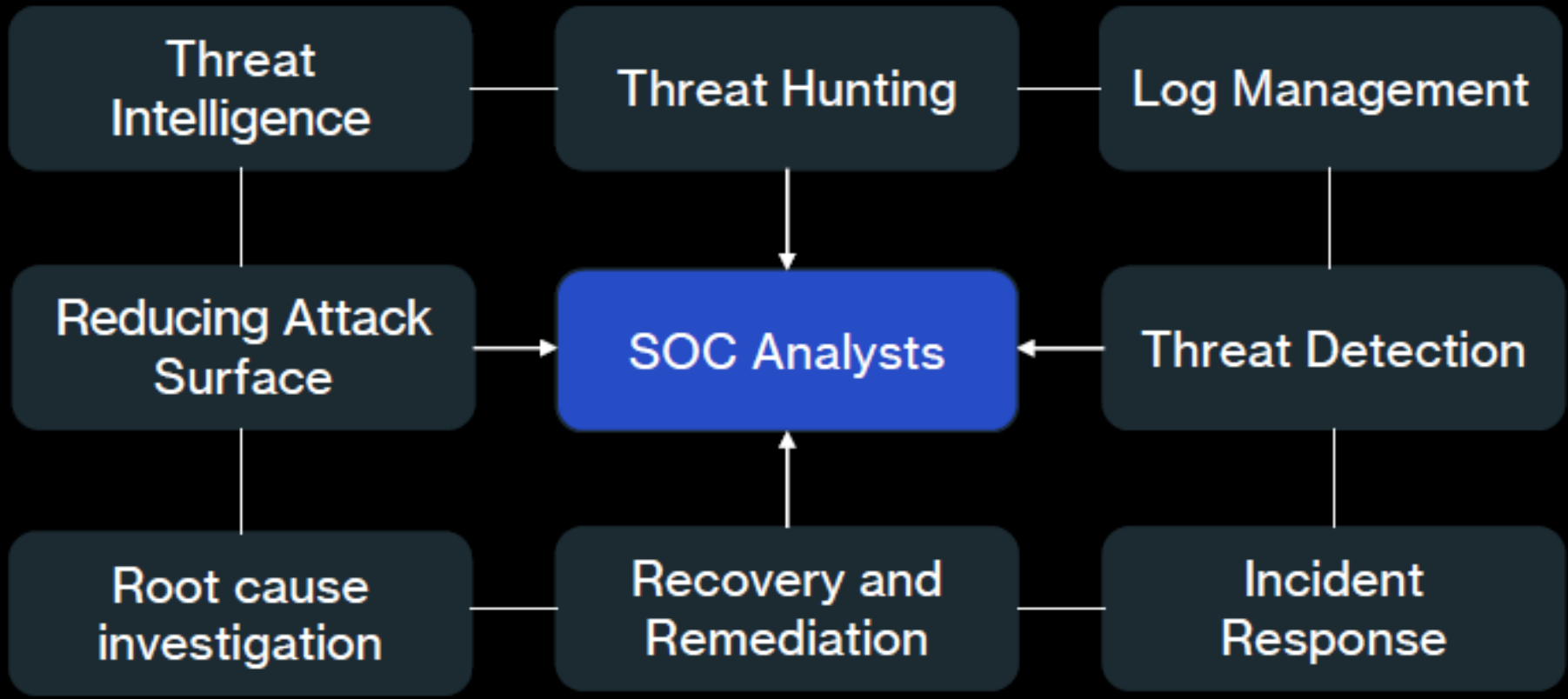
Leveraging Microsoft Sentinel for Threat Management and Response


Networks
IoT
Mobile Devices
Cloud
Endpoints
People

Cyber Security Challenges

- Lack of Security People
- Lack of Automation
- Many disconnected products
- Noisy alerts and false positives
- More sophisticated threats
- Overwhelming access to data
- Evolving regulatory landscape
- A lot of alerts are never really investigated

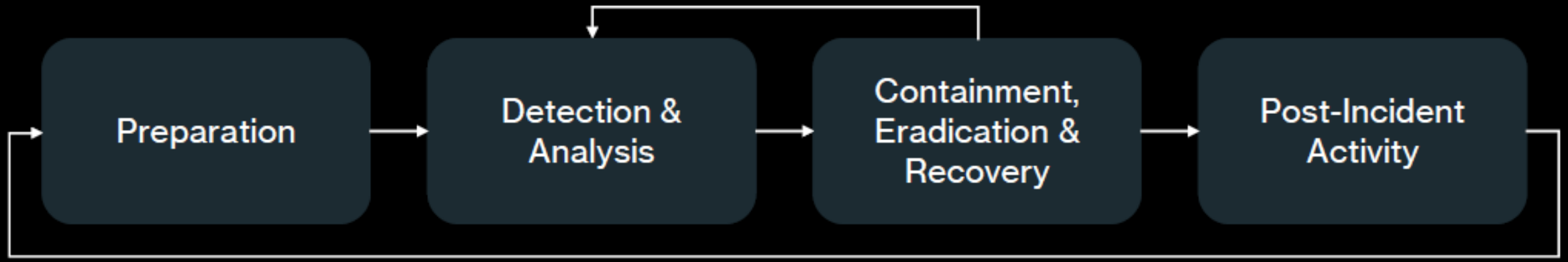
What is a Security Operations Center (SOC)?



SOC Model


Tier 3
• Proactive Threat Hunting
• Advanced Forensics
5% of Alerts
Tier 2
• Advanced malware
• Hard tasks
25% of Alerts
Tier 1
• Commodity malware
• Easier tasks that can or should not be automated
70% of Alerts
Automation
• Commodity malware
• Repetitive Tasks
• Mimics the steps an analyst would take in easy cases

Cyber Security Incident Response Process



NIST 800-61: Computer Security Incident Handling Guide

EDR, XDR, SIEM & SOAR

EDR	• Endpoint Detection and Response • Behavior monitoring for endpoints	Defender for Endpoint
XDR	• Extended Detection and Response • Behavior monitoring beyond the endpoint	Defender XDR Defender for Cloud
SIEM	• Security Information & Event Management • Centralized collection, correlation and analysis of logs	Sentinel
SOAR	• Security Orchestration, Automation & Response • Automates incident response procedures	Sentinel + Azure Logic Apps

Blue and Red Teaming

- Security Monitoring
- Incident Response
- Forensics
- Threat Hunting

- Vulnerability Assessments
- Penetration Testing
- Social Engineering
- Simulate adversary TTPs

Purple Teaming

Blue and Red collaborate to improve security posture

Collaborative simulation of adversary TTPs

Drastic upskilling of both teams

What is a Threat?

Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Intelligence, Threat Intelligence and CTI

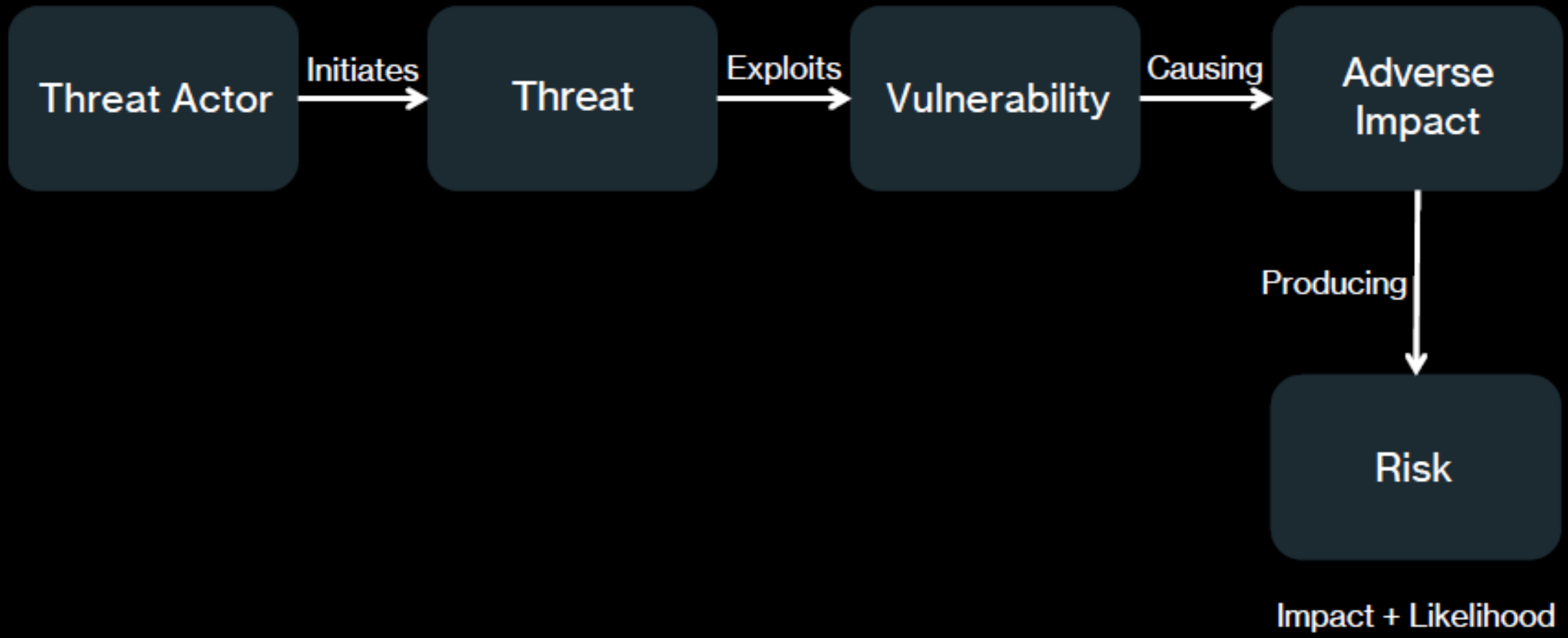
Cyber Threat Intelligence (CTI)

What is Cyber Threat Intelligence?

“Cyber Threat intelligence is knowledge about adversaries and their motivations, intentions, and methods that is collected, analyzed, and disseminated in ways that help security and business staff at all levels protect critical assets of the enterprise.”

Enabling Threat-Informed-Defense

Threat, Vulnerability & Risk



Threat-Informed-Defense

- What is the mission of my organization?
- What threat actors are interested in my organizations industry?
- What are the motivations of those threat actors?
- What TTPs are those threat actors using?
- How can I detect and protect my organization against those TTPs?

Tactics, Techniques and Procedures

- Tactics: The high-level description of the behavior and strategy of a threat actor.
- Techniques: These are the non-specific guidelines and intermediate methods that describe how a tactic action can be realized.
- Procedures: These refer to the sequence of actions performed using a technique to execute on an attack tactic. The procedure involves detailed descriptions activities.

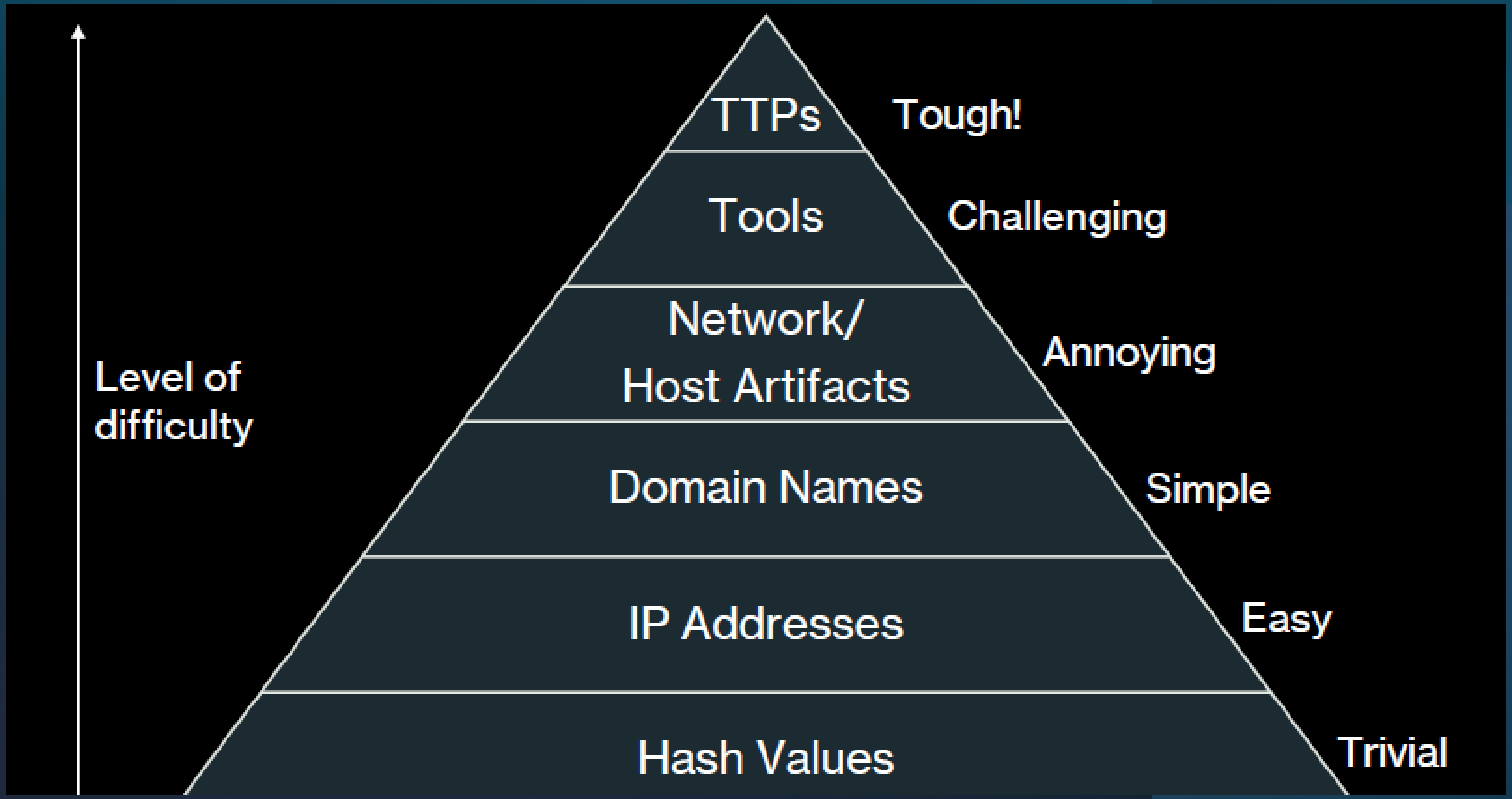
Reconnaissance

Scanning

Vulnerability Scanning

IOCs and IOAs

- IOC: An Indicator of Compromise (IOC) is evidence on a system that indicates that the security of the network has been breached.
- IOA: Indicators of attack (IOA) focus on detecting the intent of what an attacker is trying to accomplish and its behavior, regardless of the malware or exploit used in an attack.


Level of difficulty
TTPs
Tough!
Tools
Challenging
Network/
Host Artifacts
Annoying
Domain Names
Simple
IP Addresses
Easy
Hash Values
Trivial

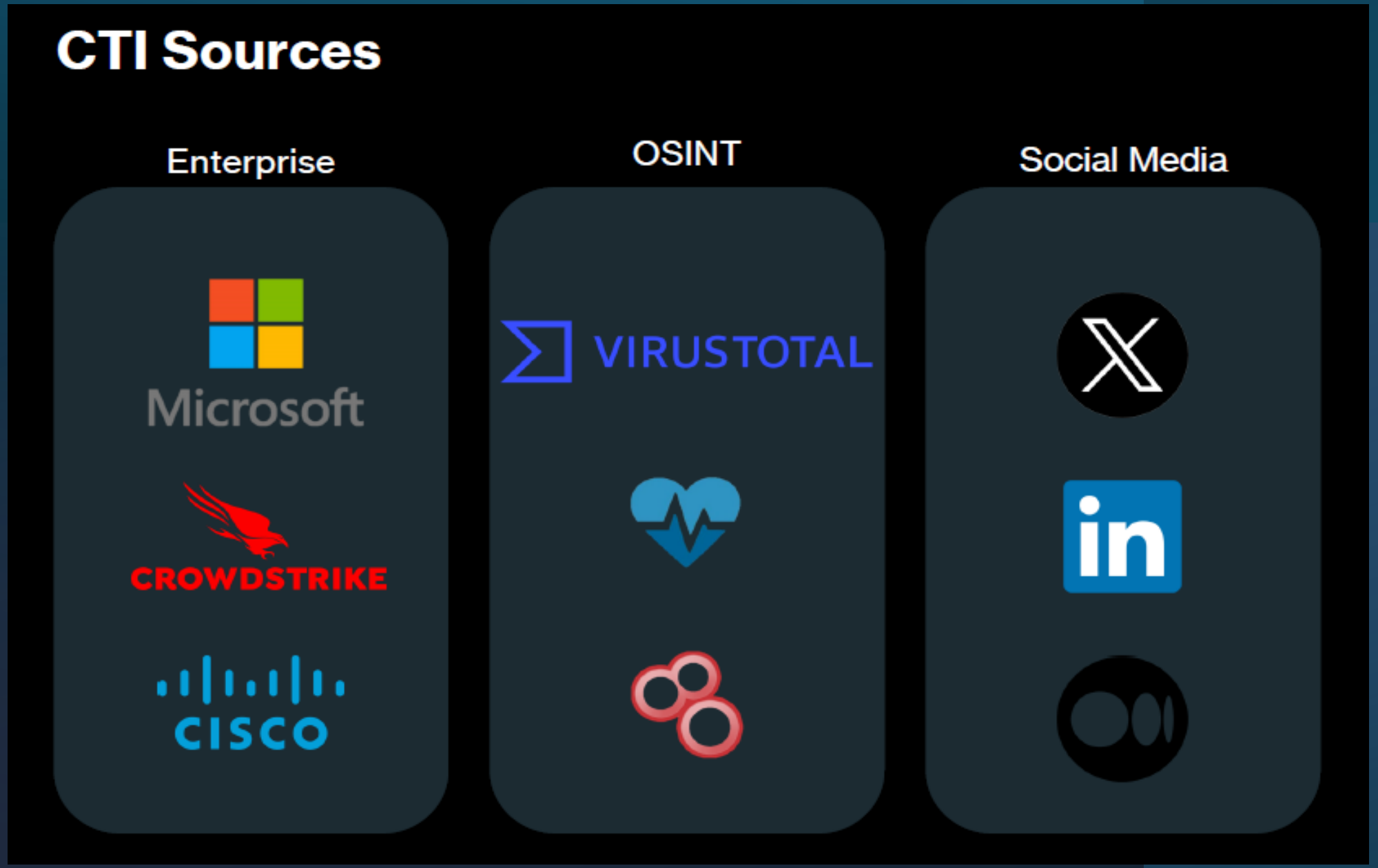
What is Threat Hunting?

Threat Hunting is the practice of proactively searching for cyber threats that are lurking undetected in your environment.

There are two Threat Hunting Models:

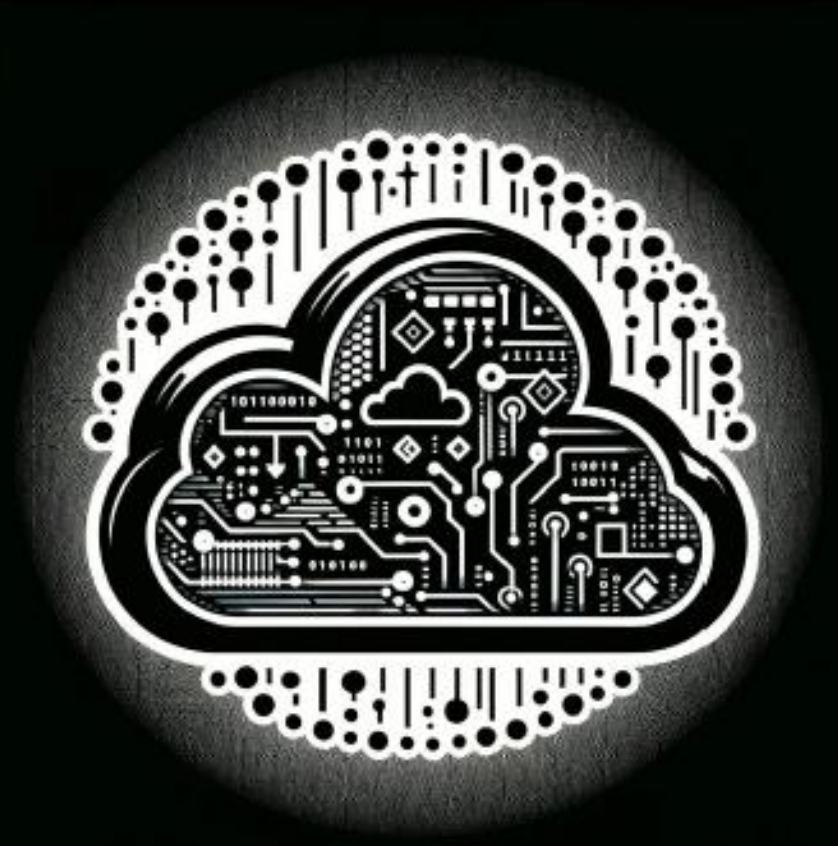
1) Intelligence-based Hunting: Leverage IOCs, hash values, IP addresses, domain names or host artifacts
2) Hypothesis-based Hunting: Hunt based on IOAs and TTPs of adversaries

CTI Sources


Enterprise
Microsoft
CROWDSTRIKE
CISCO
OSINT
VIRUSTOTAL
Social Media

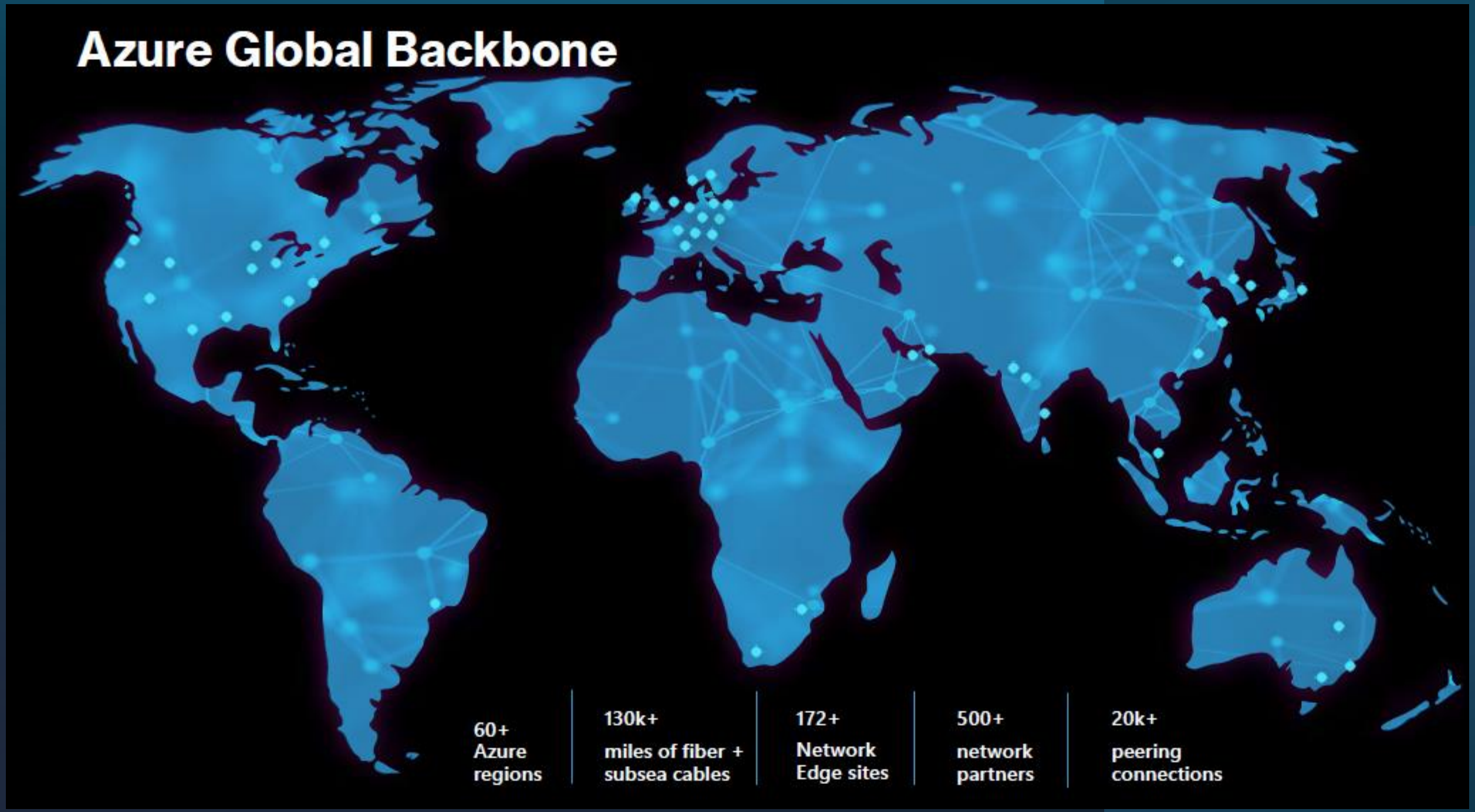
Cloud Computing Properties

- On-demand self service
- Broad network access
- Resource pooling
- Rapid elastic
- Measured service



Public, Private, Hybrid Cloud

Azure Global Backbone



Shared Responsibility in Azure

Responsibility	On-prem	IaaS	PaaS	SaaS
Information and Data	■	■	■	■
Devices (Mobile and PCs)	■	■	■	■
Accounts and Identities	■	■	■	■
Identity and Directory Infrastructure	■	■	■	■
Applications	■	■	■	
Network Controls	■	■	■	
Operating System	■	■		
Physical Hosts	■			
Physical Network	■			
Physical Datacenter	■			

Azure Subscription Types

Free

- Free credits for 30 days
- Some services are free for 13 months

Student

- Free credits for 12 months
- No credit card required

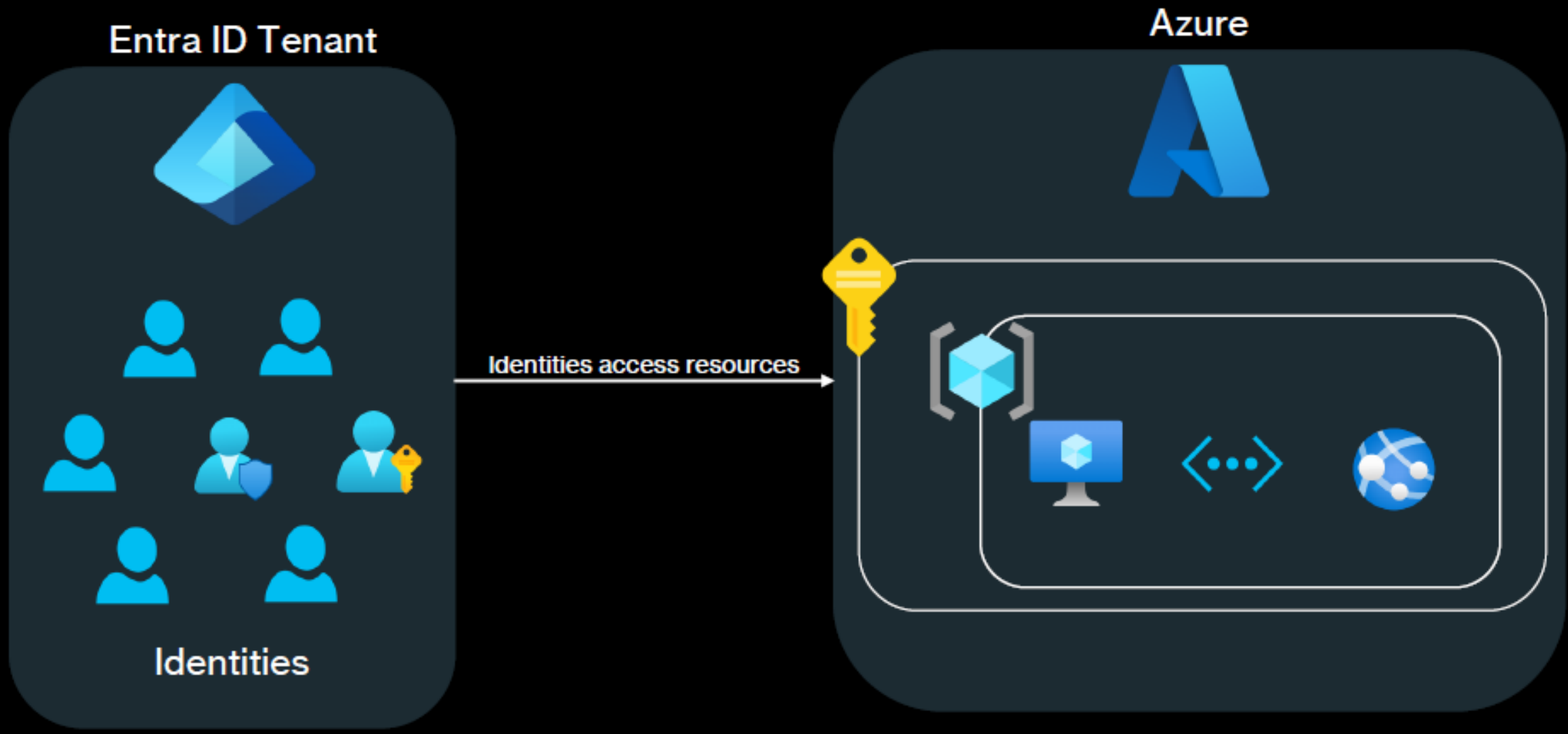
Pay As You Go

- Pay for what you use
- Credit card required

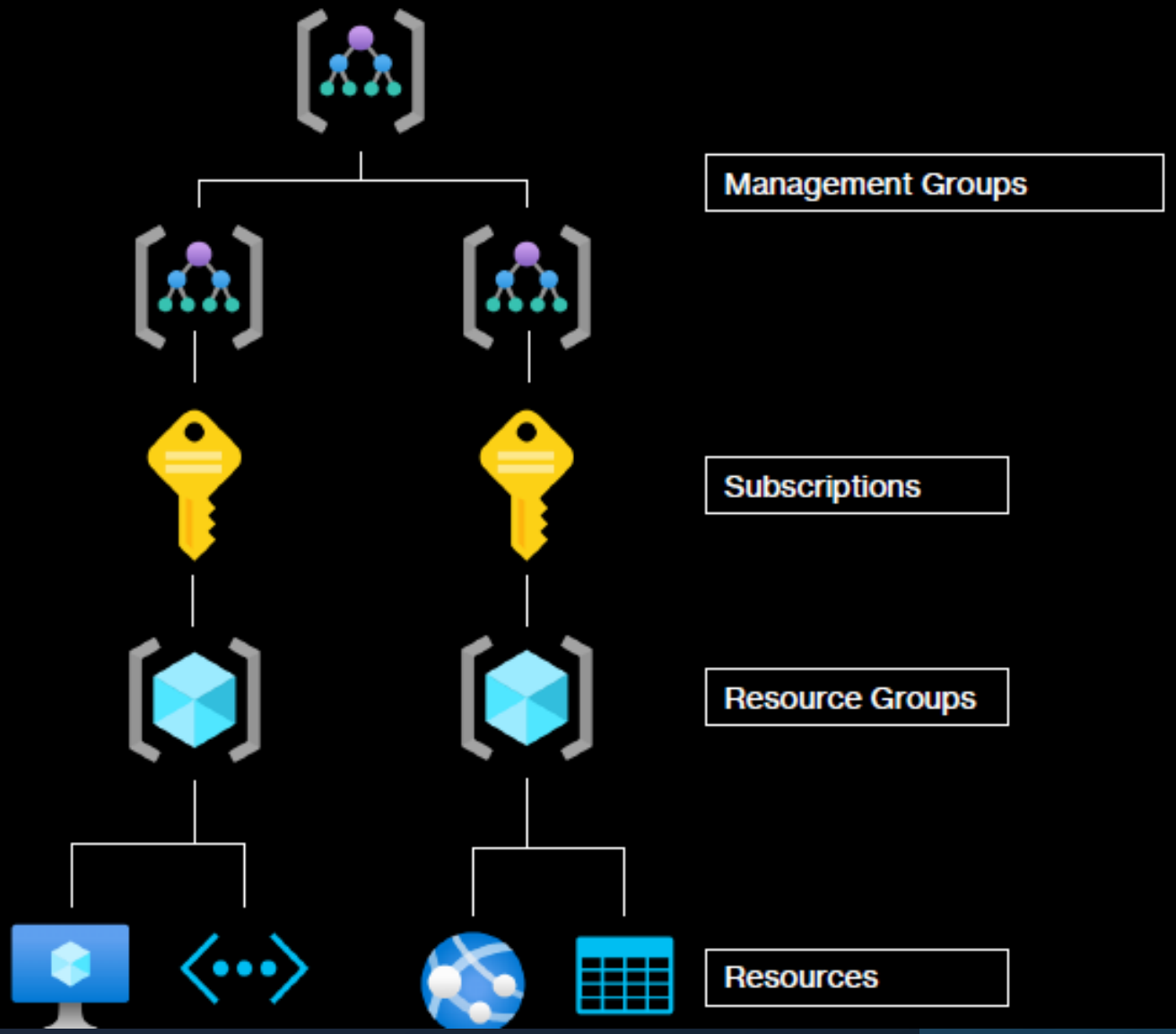
Enterprise Agreement

- One consumption agreement for all Azure services
- Various different billing models

Entra ID Tenants and Azure Subscriptions



Azure Resource Hierarchy



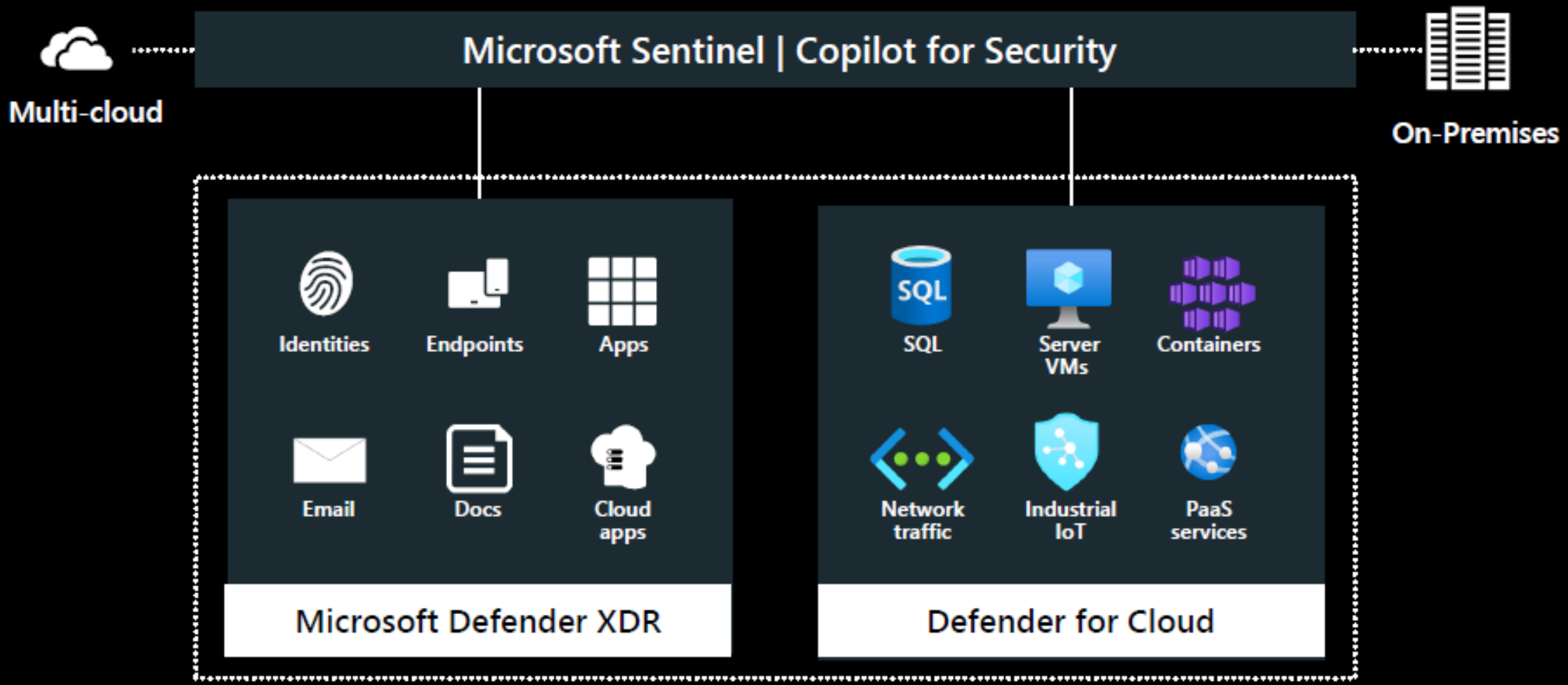
What is Zero Trust?

- Zero Trust is a security strategy
- It is not a product or a service

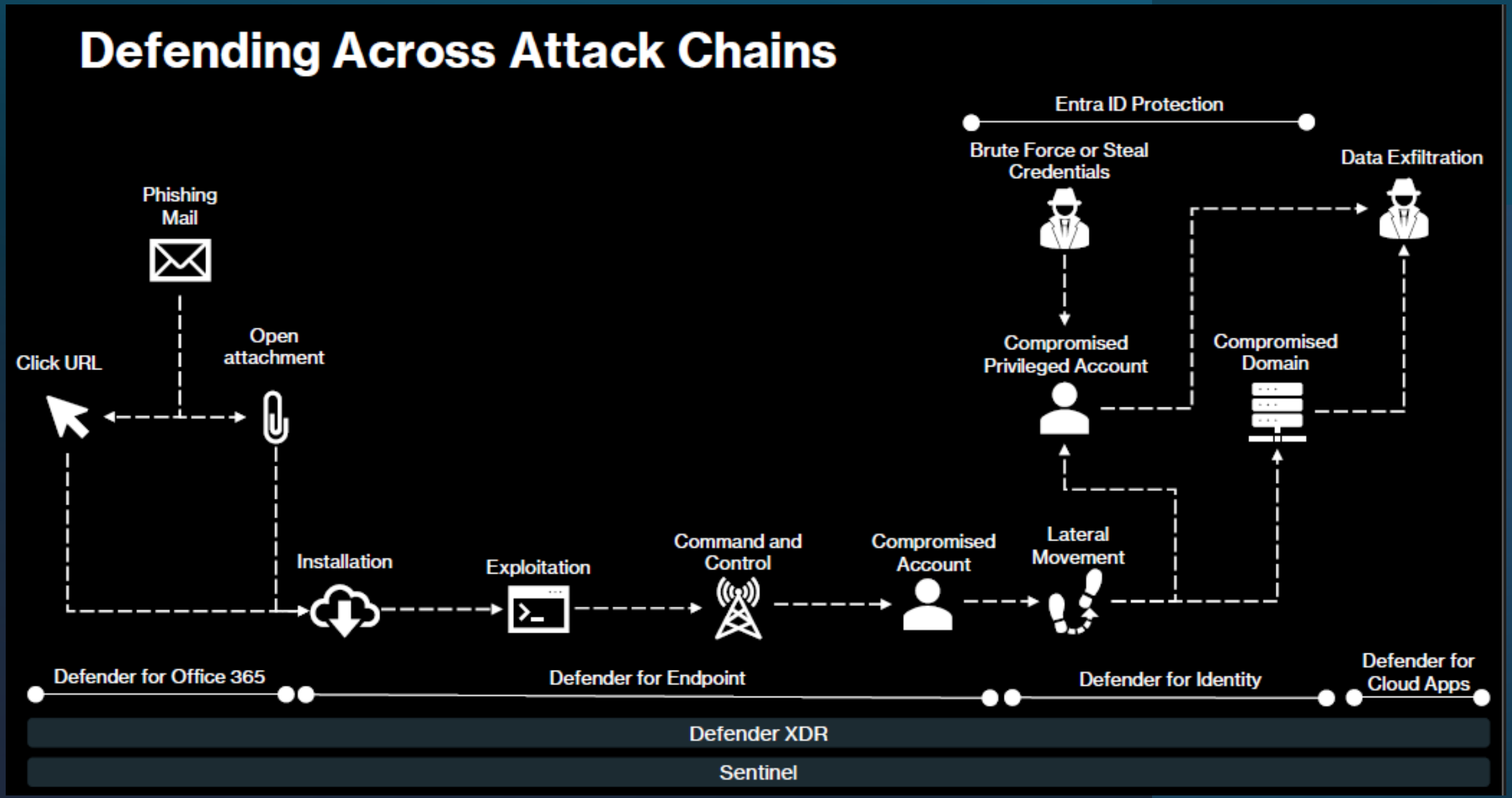
There are 3 core principles of Zero Trust:

1) Verify explicitly
2) Use least-privilege access
3) Assume breach

The Microsoft Security Cosmos



Defending Across Attack Chains



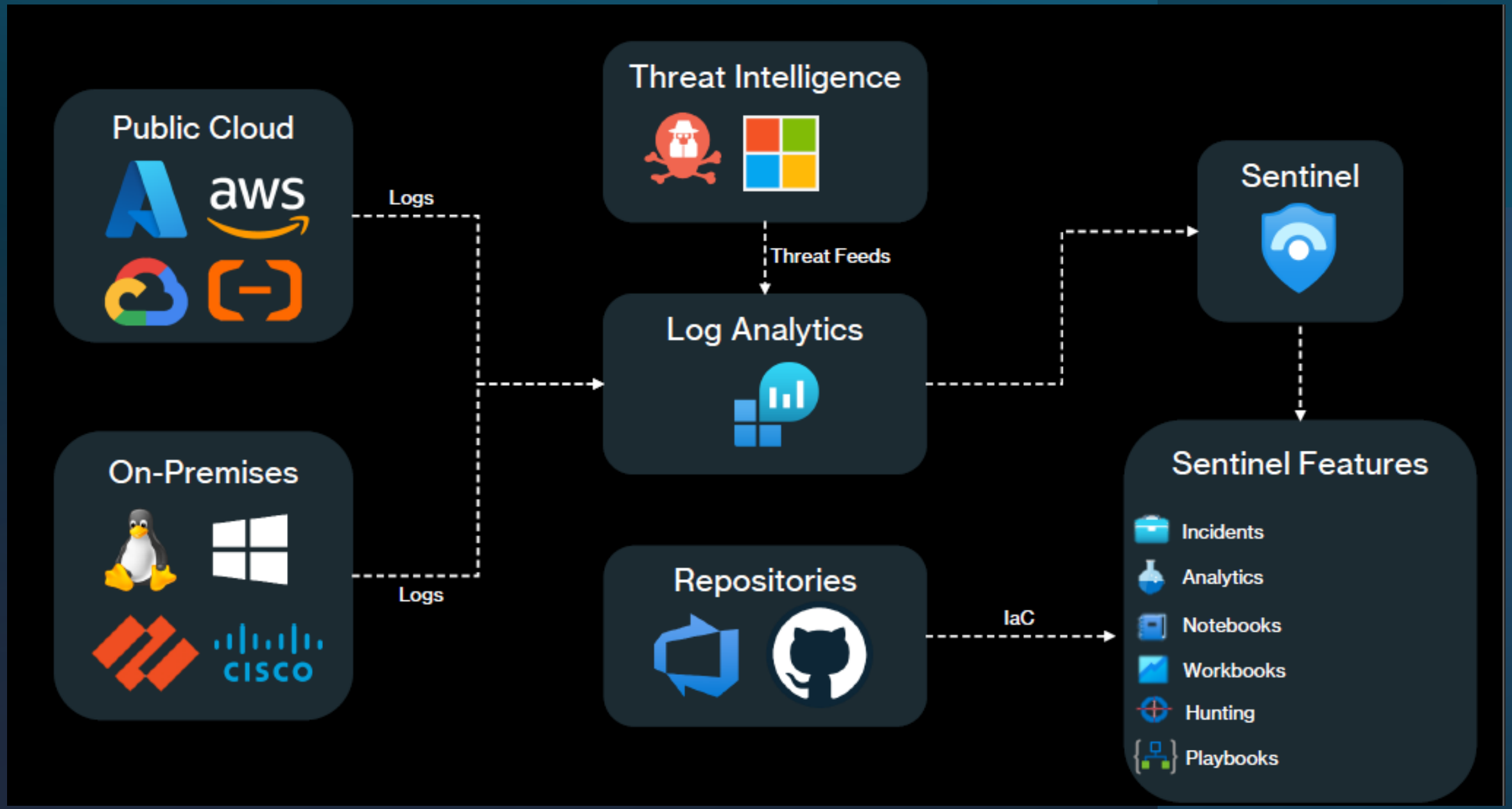
What is Microsoft Sentinel?

- Cloud-native SIEM & SOAR
- Pay-as-you-go
- Collect data at scale
- Detect and investigate threats
- Respond to threats rapidly

Software as a service (SaaS)

- Azure provides everything but the configuration of the applications
- You cannot control anything but the configuration of the applications
- Example for a SaaS service: Microsoft Sentinel

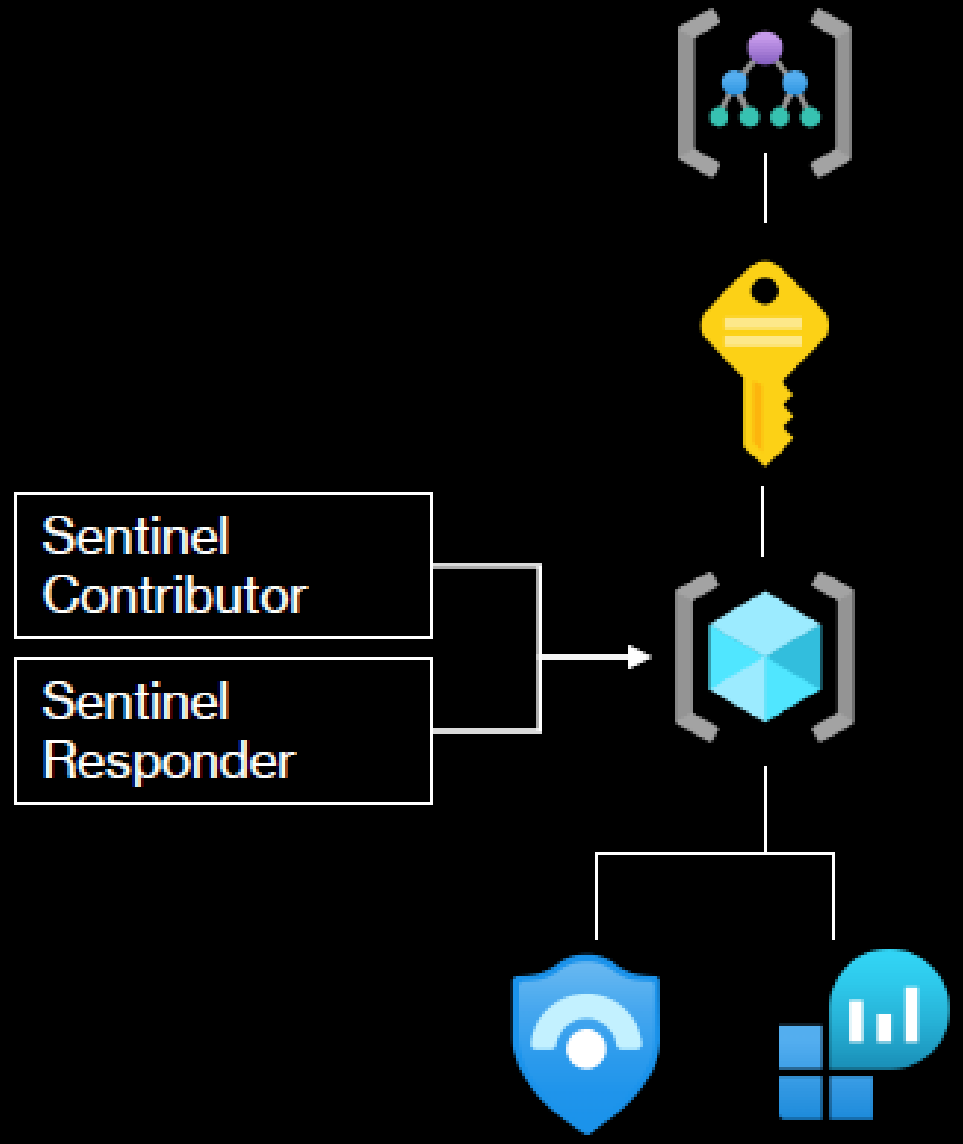
Responsibility	SaaS
Information and Data	
Devices (Mobile and PCs)	
Accounts and Identities	
Identity and Directory Infrastructure	
Applications	
Network Controls	
Operating System	
Physical Hosts	
Physical Network	
Physical Datacenter	


Public Cloud
aws
Logs
Threat Intelligence
Threat Feeds
Sentinel
Log Analytics
On-Premises
CISCO
Logs
Repositories
IaC
Sentinel Features
Incidents
Analytics
Notebooks
Workbooks
Hunting
Playbooks

Deploying Sentinel

- There are a few prerequisites to deploy Sentinel:
  - Azure Tenant
  - Active Azure Subscription
  - Azure Resource Group
  - Azure Log Analytics Workspace

Azure RBAC



Sentinel Built-in Roles

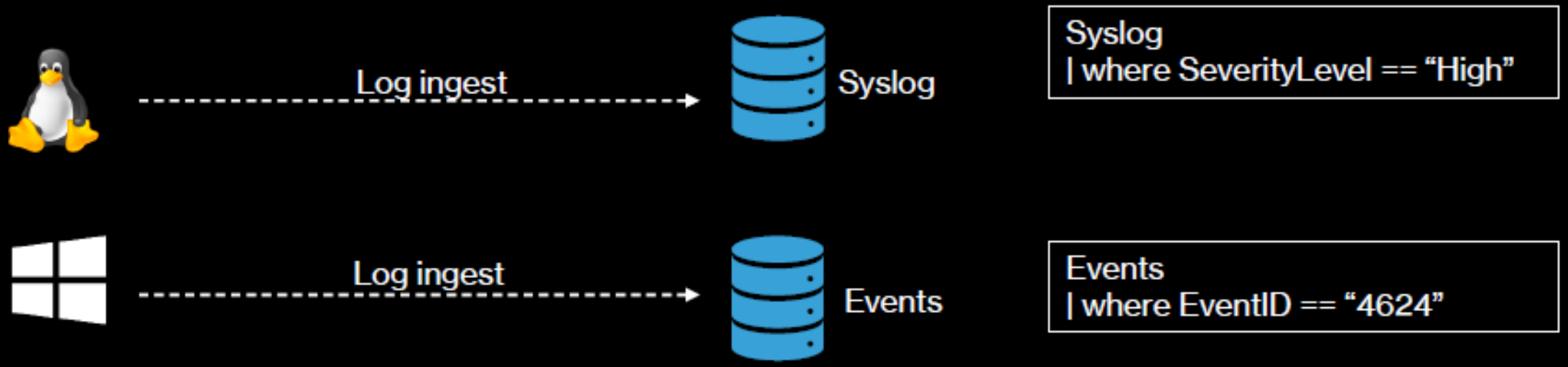
Role	Create and edit Analytics rules, Workbooks, and other Microsoft Sentinel resources	Manage incidents (dismiss, assign, etc.)	View data, Incidents, Workbooks, and other Microsoft Sentinel resources	Configure data connectors	View and run playbooks	Create and edit playbooks
Microsoft Sentinel Reader	--	--	✓	--	--	--
Microsoft Sentinel Responder	--	✓	✓	--	--	--
Microsoft Sentinel Contributor	✓	✓	✓	✓	--	--
Microsoft Sentinel Playbook Operator	--	--	--	--	✓	--
Logic App Contributor	--	--	--	✓	✓	✓

Log Analytics

- Used to ingest and query logs
- Serves as a backbone for Sentinel and other monitoring services
- Logs are stored in a “Log Analytics Workspace”
- Sentinel is just a workspace Add-On for Log Analytics (Security Insights)

Log Analytics - Tables

- All connected data sources are ingested in specific tables



Log Analytics

- Log Analytics workspaces are not a relational database
- There is no hierarchy since it is a flat list containing tables
- Workspaces store logs in tables with well-defined attributes
- Queries are executed with KQL
- Queries can extend beyond the local workspace

Log Analytics

- 30 days retention by default and can extended to 730 days = 2 Years
- Table level RBAC
- Data is encrypted in-transit and at-rest

Azure Service Limits: https://learn.microsoft.com/en-us/azure/azure-monitor/service-limits

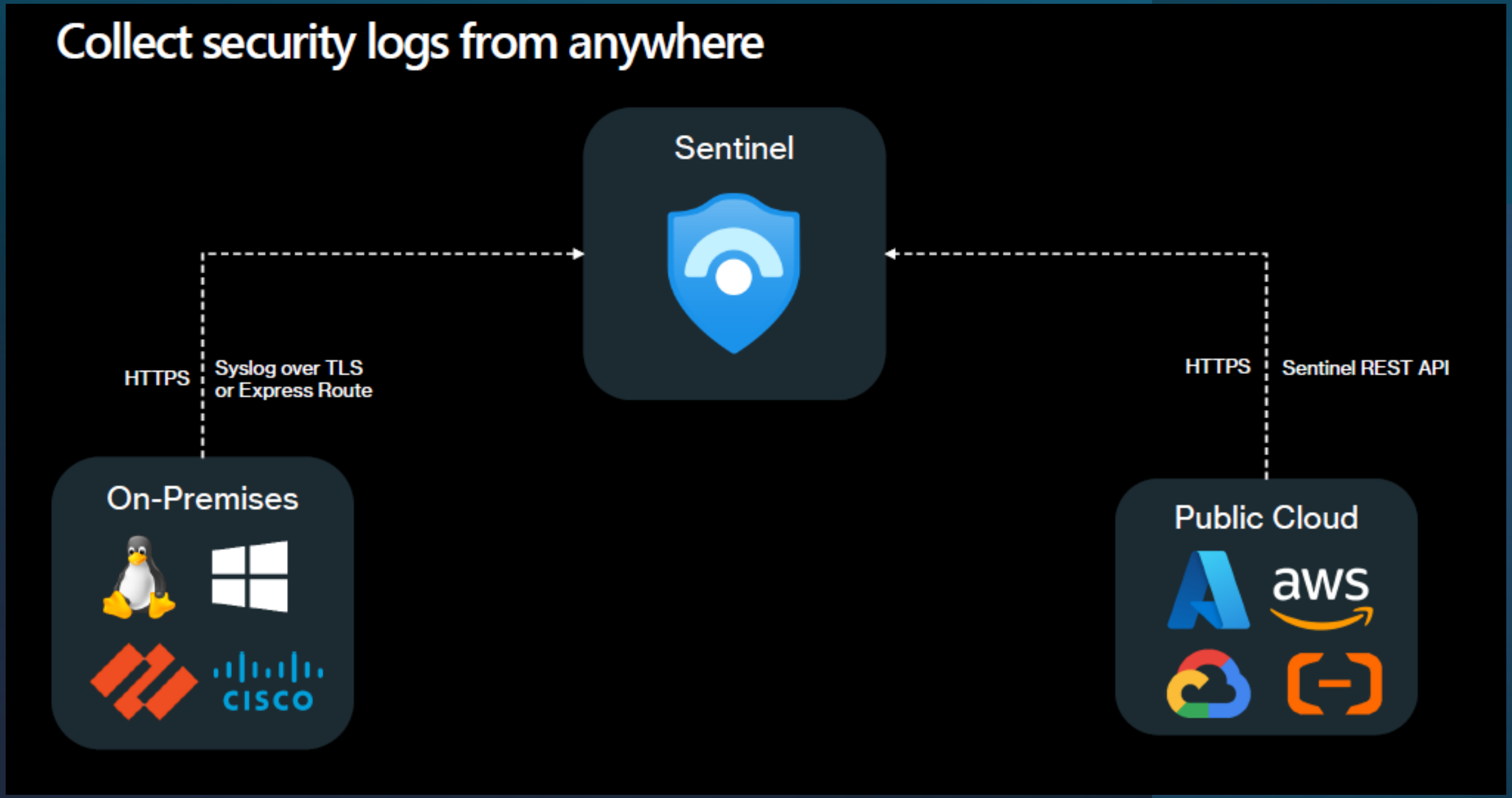
Log Analytics Dedicated Cluster

Log Analytics supports a premium dedicated cluster option with the following features:

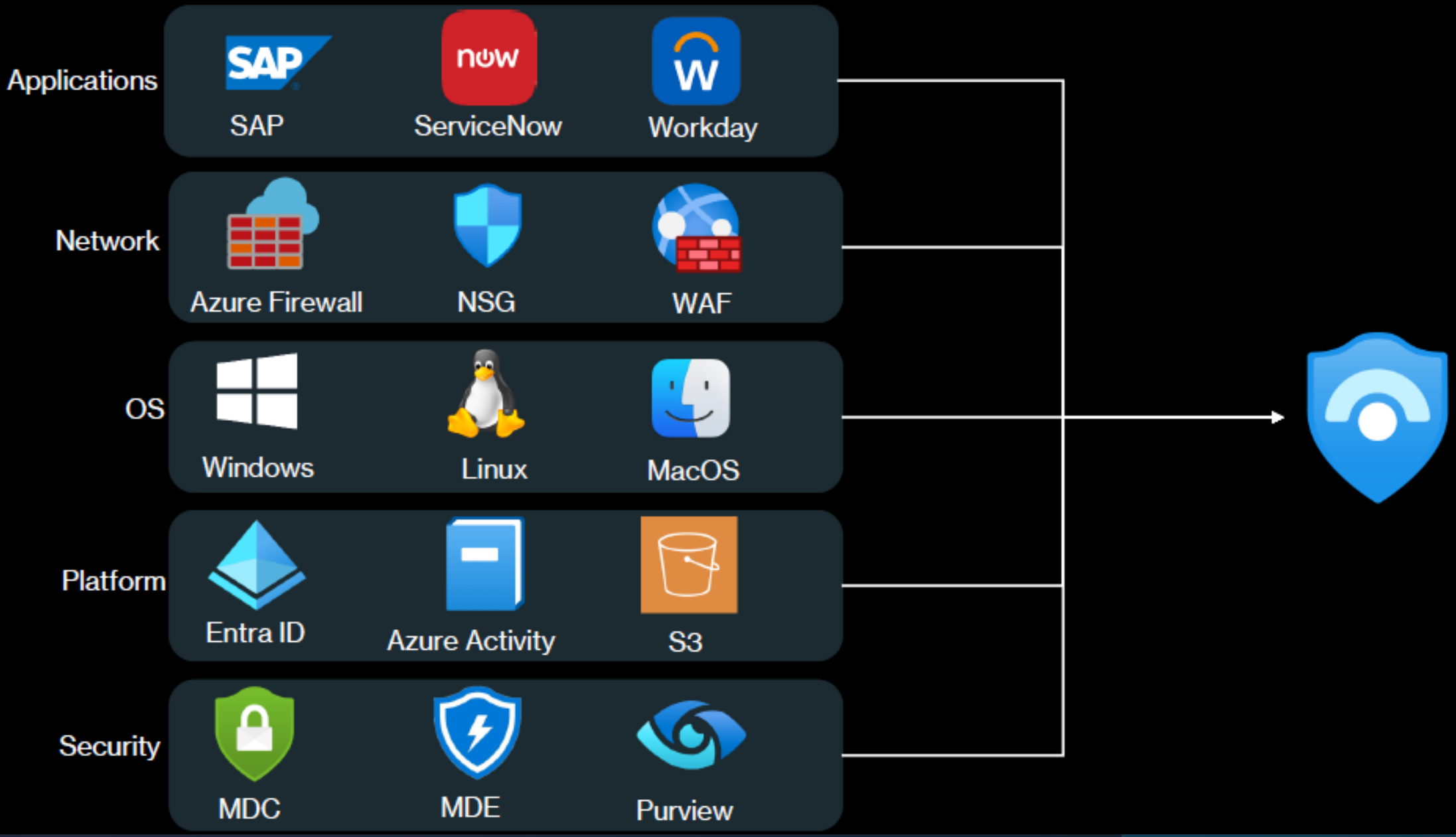
- Customer Lockbox
- Double encryption of data at rest
- Support for Availability Zones
- Increased performance for cross-workspace queries

Minimum commitment: 100GB per day

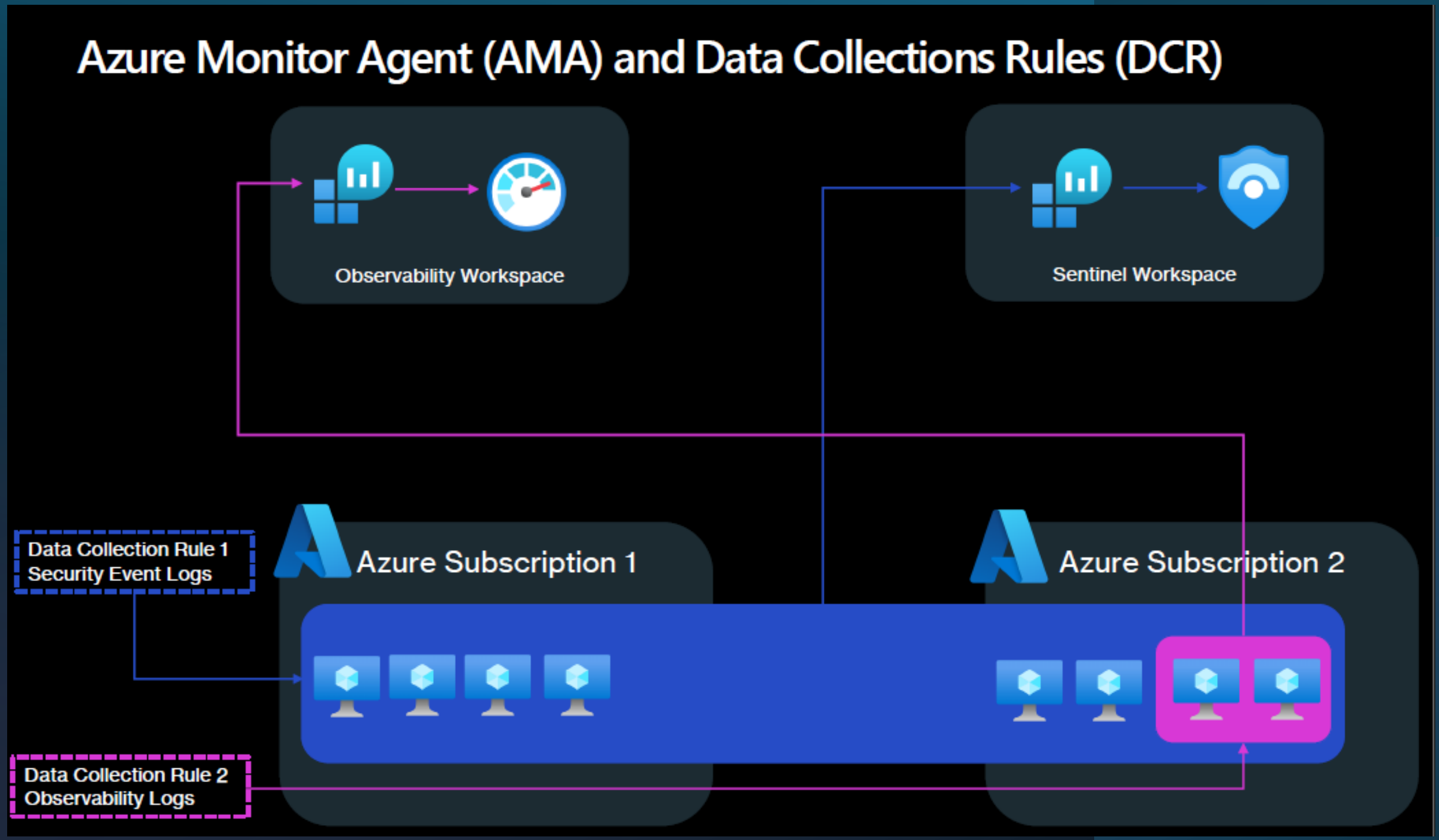
Collect security logs from anywhere



Typical data sources for a SIEM



Azure Monitor Agent (AMA) and Data Collections Rules (DCR)

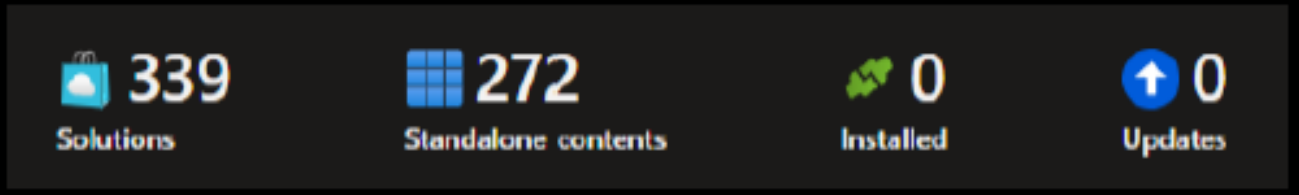


Data Connectors

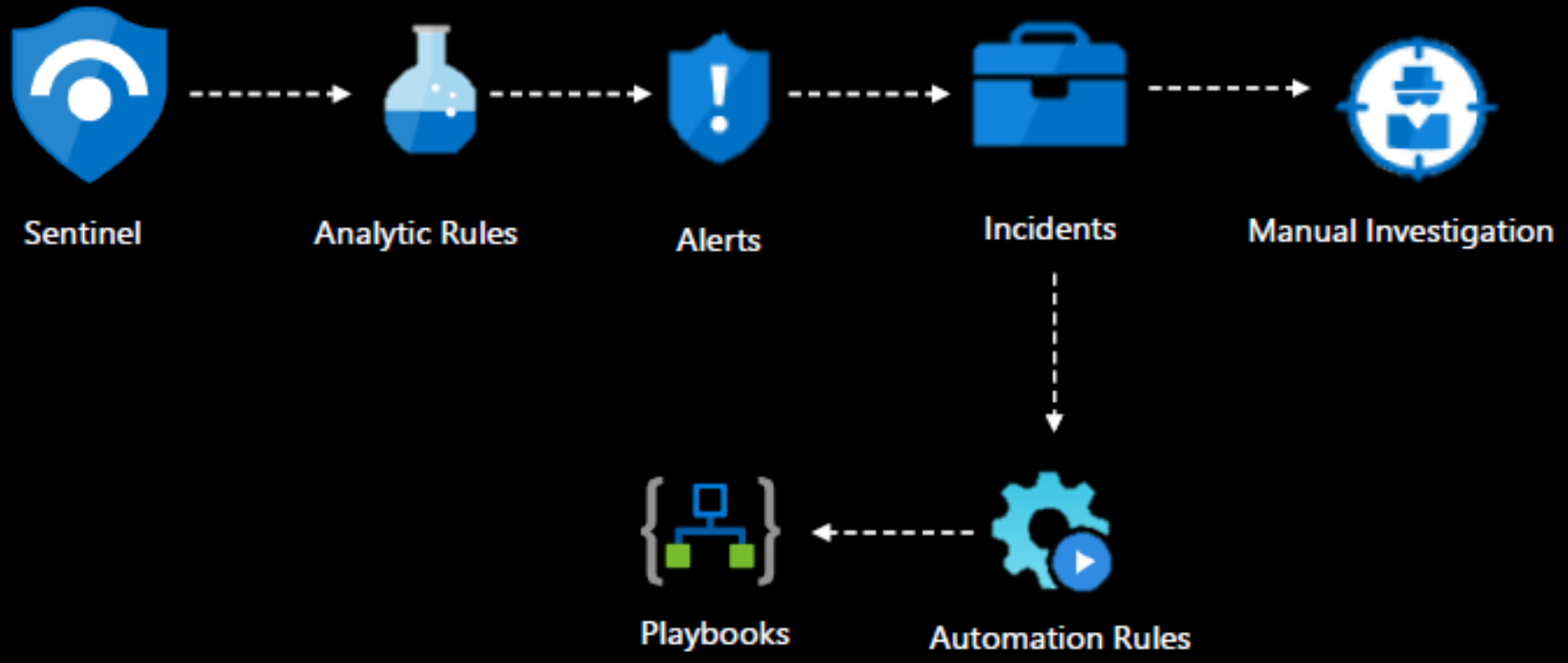
- Over 200 prebuild connectors are available in the content hub, e.g.
  - Entra ID
  - Entra ID Protection
  - M365 Defender
  - Defender for Cloud
  - Azure Activity
  - AWS
  - Threat Intelligence – TAXII
- You can also build custom connectors if your data source is not in the content hub yet

Sentinel Content Hub

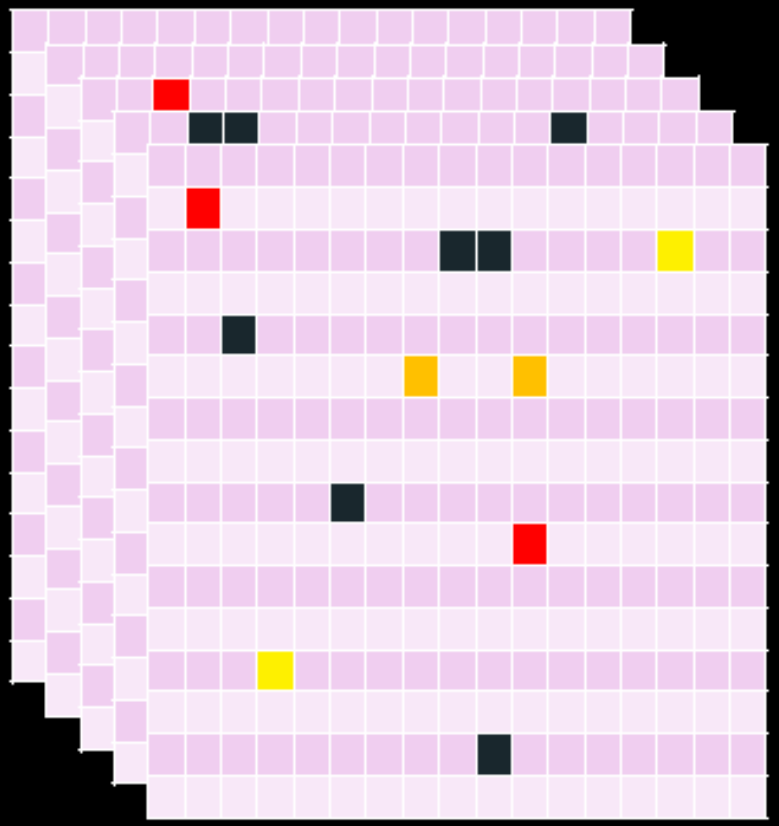
- Marketplace for ARM-based sentinel solutions such as connectors, analytic rules, hunting queries & more
- Includes Microsoft data sources but also 3rd party solutions, from e.g. :
  - Zscaler
  - Palo Alto
  - CrowdStrike
  - CheckPoint



Sentinel Workflow

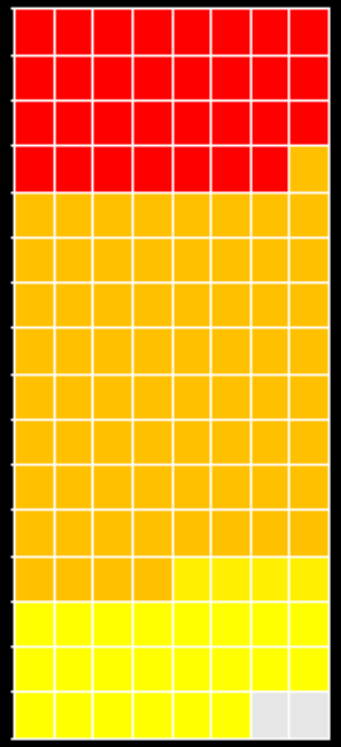


Sentinel Incident Correlation



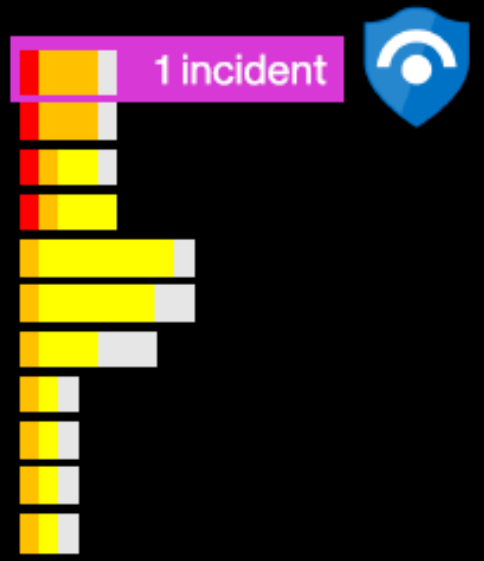
Events

millions to billions



Alerts

group/promote
interesting Events



Incidents

group related Alerts

Analytic Rules

- Analytic Rules are your SIEM use-cases defined via KQL
- Sentinel comes with over 500 rule templates
- Limit of 512 rules per workspace
- 7 Types of analytic rules:
  - Scheduled
  - Near-Real-Time (NRT)
  - Fusion
  - ML Behavior Analytics
  - Threat Intelligence
  - Microsoft Security
  - Anomaly

Scheduled Rules

- Analytic Rules that continuously run in a defined timeframe
- An alert is fired if a condition is met
- Scheduled rules are the default rule type and most analytic rules will have this rule type

Near-Real-Time Rules (NRT)

- Analytic Rules that run continuously and shall provide “up-to-the-minute” threat detections
- NRTs run once every minute in reality
- Limit of 50 NRT rules per workspace

Fusion

- Analytic Rule that is an advanced multistage attack detection feature including over 120 detections across multiple Microsoft data sources:
  - Entra ID Protection
  - Defender for Cloud
  - Defender for IoT
  - Defender XDR
  - Sentinel scheduled rules
  - Sentinel NRT rules
- There can only be one Fusion rule per Sentinel workspace

ML Behavior Analytic Rules

- Analytic Rule that monitors for unusual Windows RDP and Linux SSH logons based on pre-defined scenarios
- Scenarios include:
  - Unusual IP - This IP address has not or has rarely been seen in last 30 days.
  - Unusual Geo - The IP address, city, country and ASN have not (or rarely) been seen in last 30 days.
  - New user - A new user logs in from an IP address and geo location, both or either of which are not expected to be seen in the last 30 days.

Threat Intelligence Rules

- Generates an alert when a Microsoft Defender Threat Intelligence Indicator gets matched with your event logs
- The alerts are very high fidelity

Microsoft Security Rules

- Analytic rules that are alert forwarders from other Microsoft security services, such as:
  - Defender for Endpoint
  - Defender for Identity
  - Defender for Cloud

Anomaly Rules

- Non-alerting informational rules from UEBA
- Detect deviations from a baseline
- Designed to provide more context on entities and to enrich threat hunting

What is Ingestion Delay?

- Ingestion Delay is the time between log creation at the source and ingestion into Sentinel
- Ingestion Delay can significantly mess with your scheduled analytic rules
- Important: Scheduled Rules consider the timestamp of the data source not the timestamp of ingest

Countering Ingestion Delay 1/3

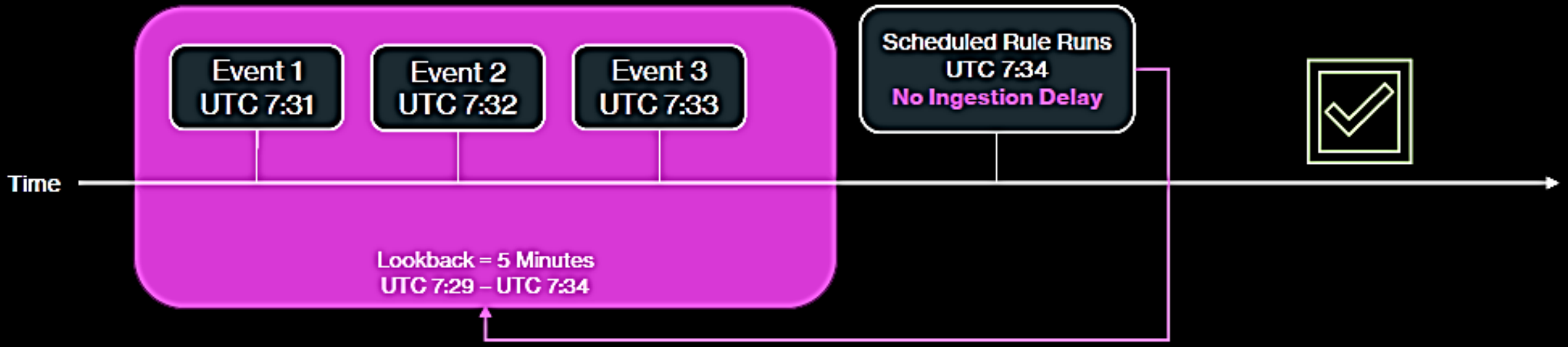
Query scheduling

Run query every *

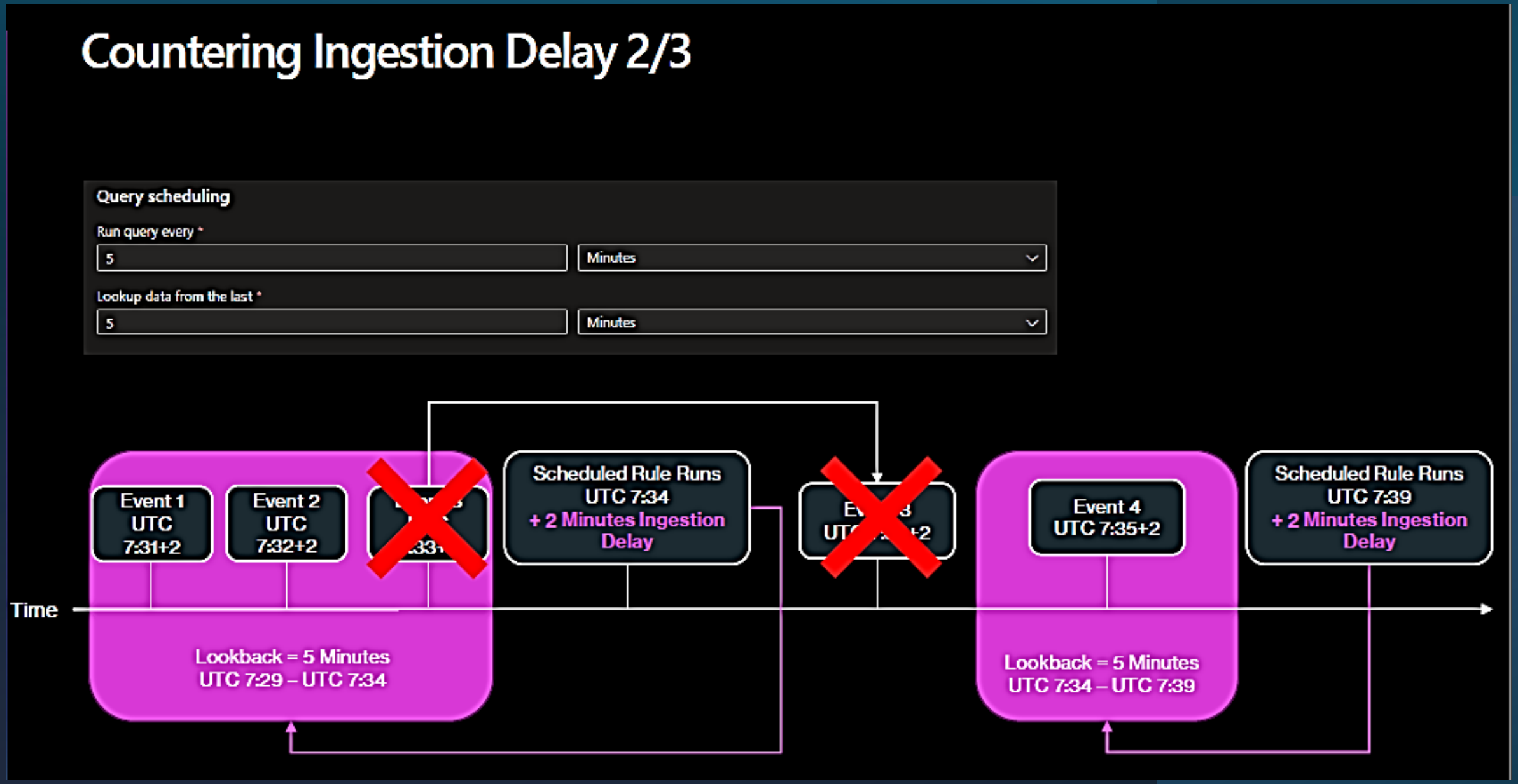
5 | Minutes

Lookup data from the last *

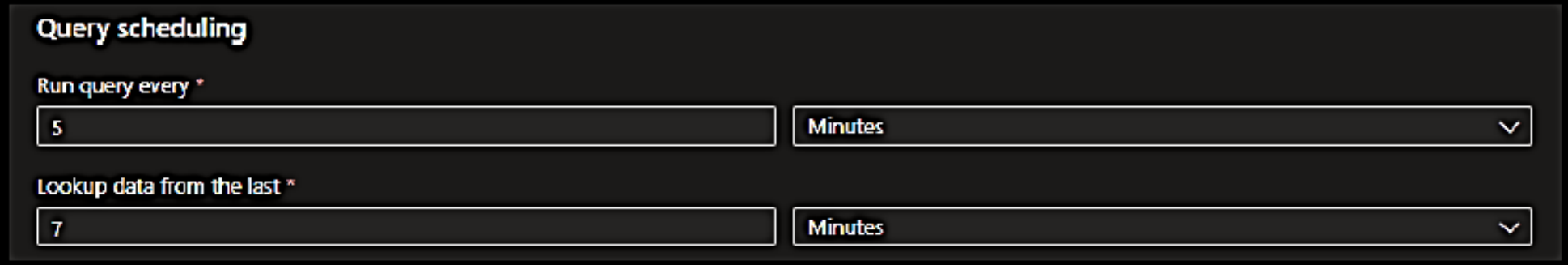
5 | Minutes

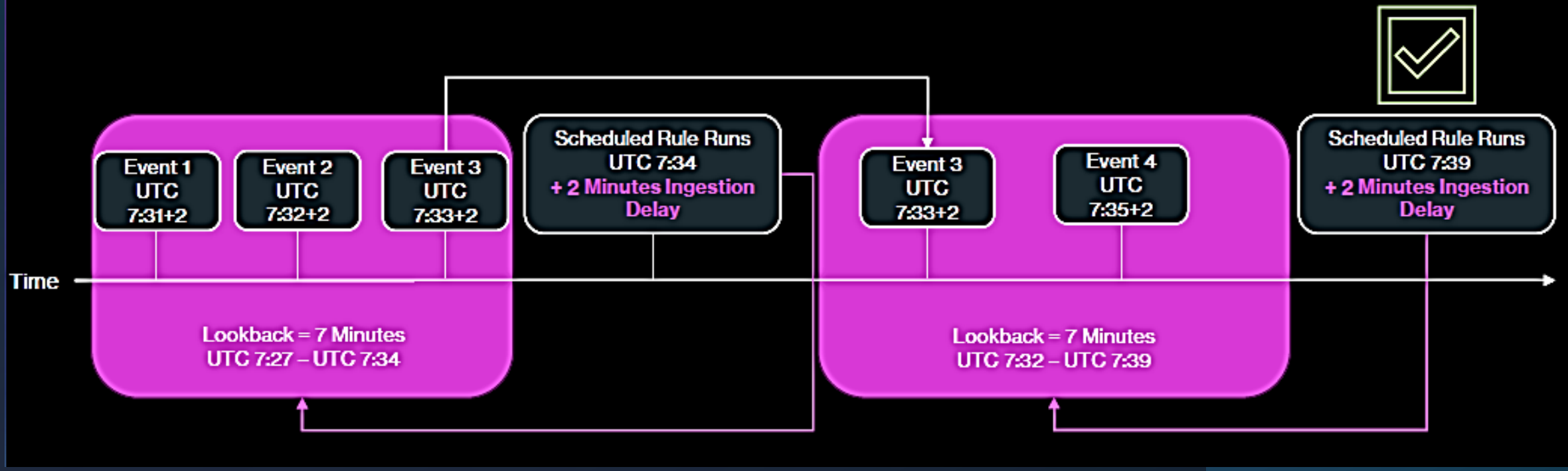


Countering Ingestion Delay 2/3



Countering Ingestion Delay 3/3





Threat Hunting

What is Threat Hunting?

- Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in your environment
- Instead of only relying on your analytic rules in Sentinel you additionally hunt for threats via KQL

Threat Hunting

There are two Threat Hunting Models:

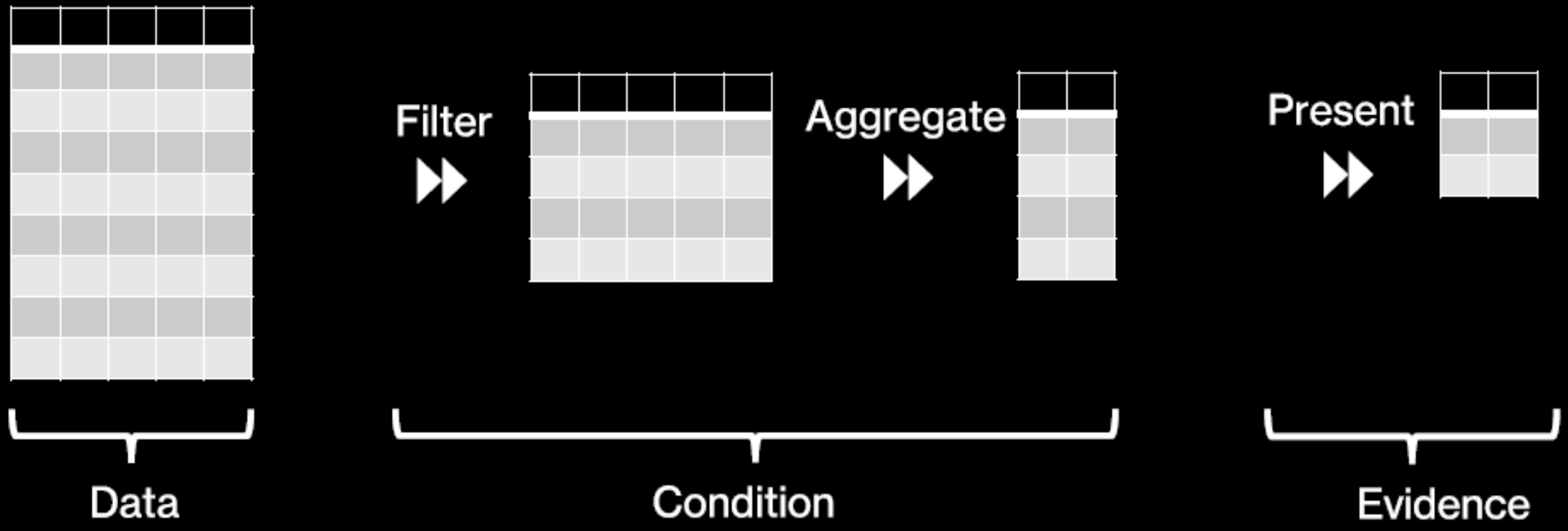
1) Intelligence-based Hunting → Utilizes IoCs, hash values, IP addresses, domain names or host artifacts
2) Hypothesis-based Hunting: Hunts are done based on IOAs and TTPs of adversaries

KQL Query Development Process

1. Hypothesis
   - A query always begins with a hypothesis that you want to prove or disprove, such as: Is this IoC part of my logs?
2. Determine required tables
   - Determine the required tables for your query
3. Explore table schema
   - Consider the schema
4. Filter away
5. Visualize

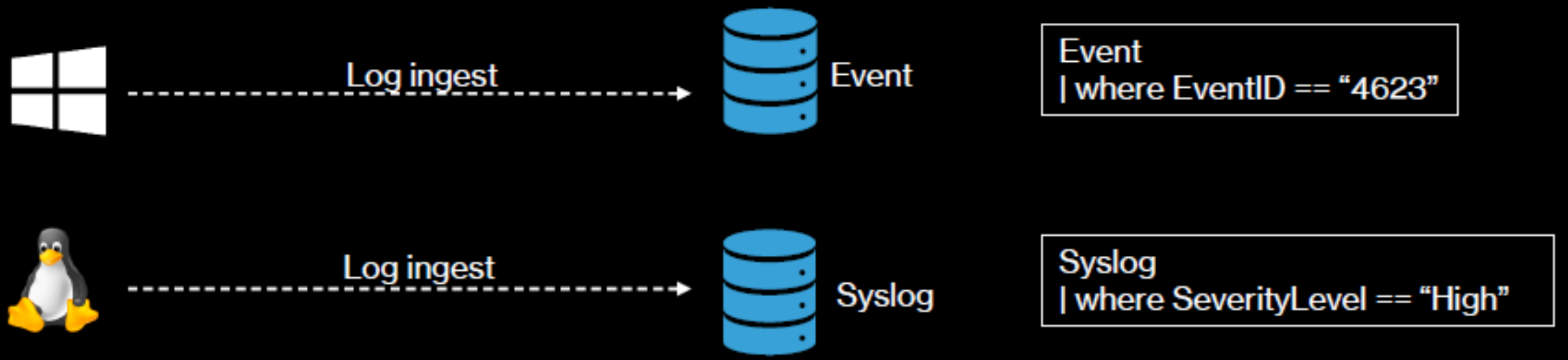
Kusto Query Language (KQL)

```
SecurityEvent
| where EventID == "4264"
| summarize count () by Account
| top 10 by count
```



Log Analytics - Tables

- All connected data sources are ingested in specific tables



KQL 101

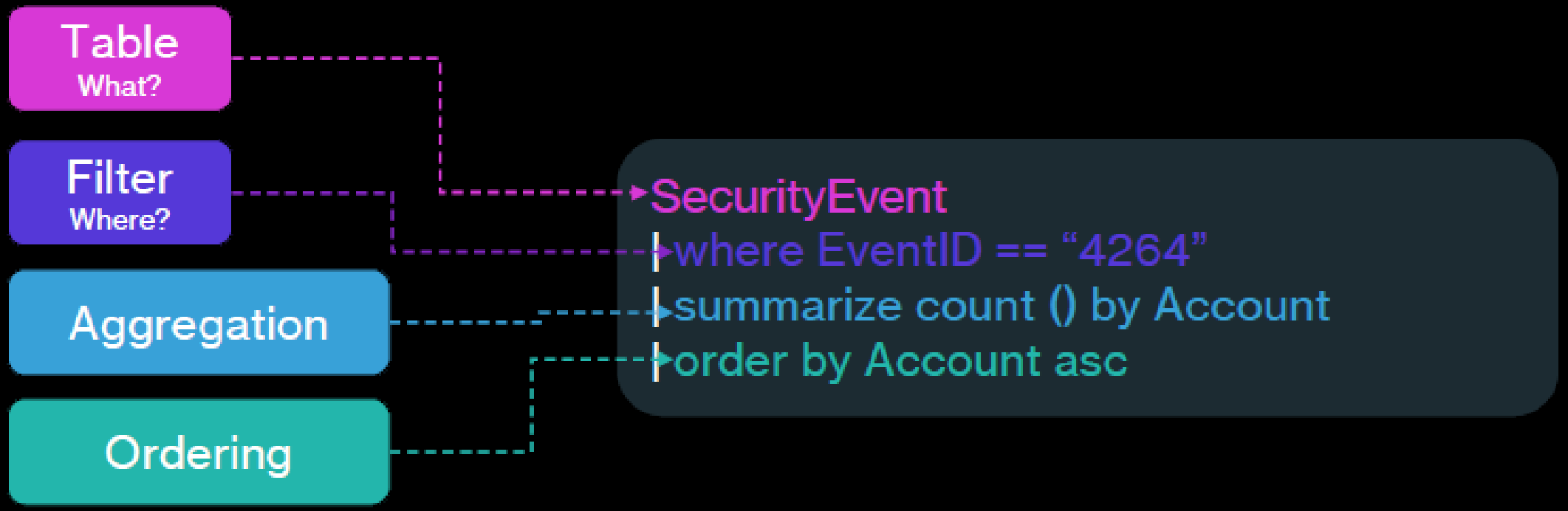
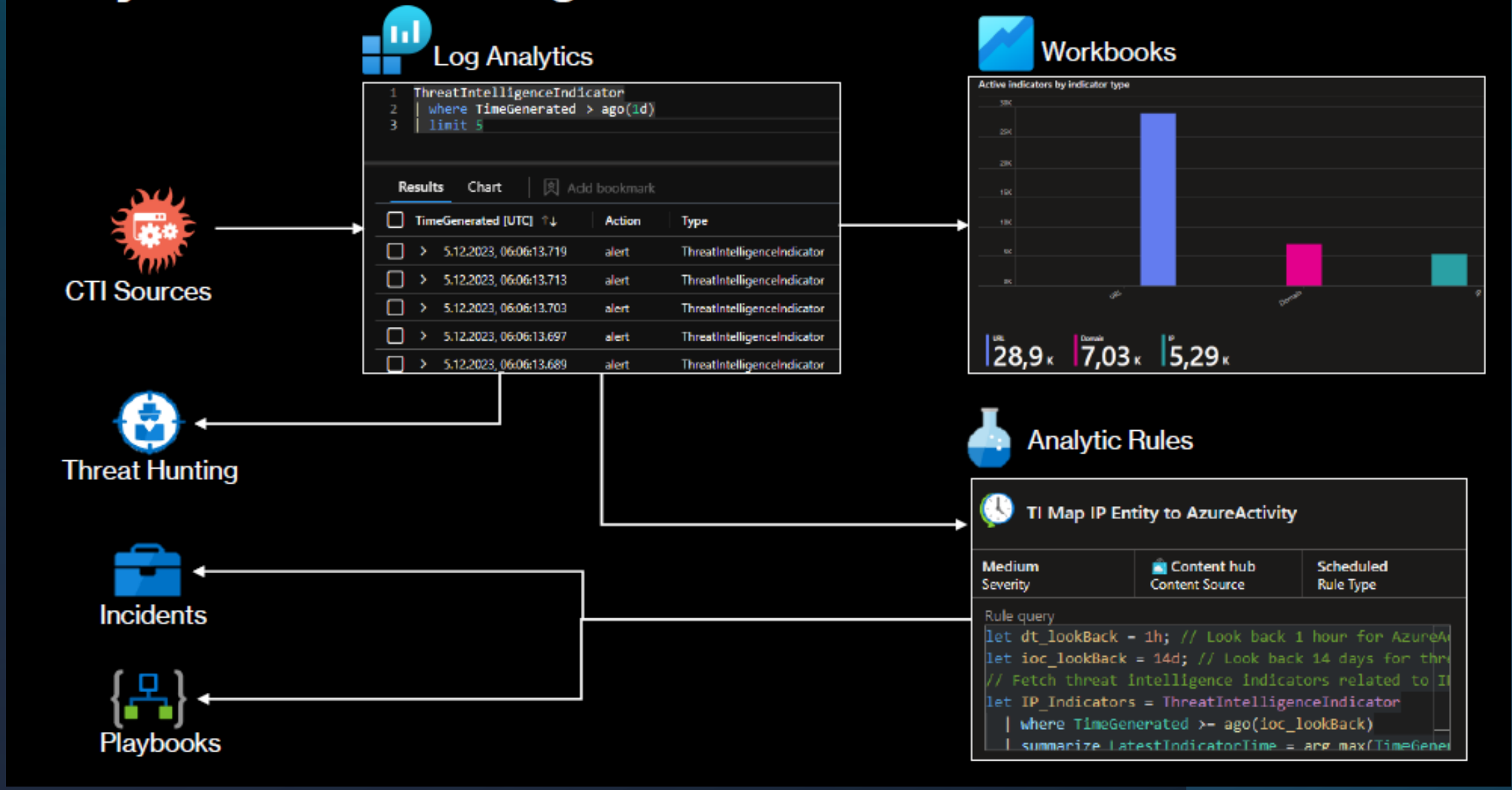


Table
What?
Filter
Where?
Aggregation
Ordering
SecurityEvent
| where EventID == “4264”
| summarize count () by Account
| order by Account asc

KQL – Important Operators

Operator	Action
where	Filters on a specific predicate
search	Searches all columns in the table for the value
limit /take	Returns the specified number of records
count	Counts records in the input table
summarize	Groups the rows according to the by group columns, and calculates aggregations over each group
render	Renders results as a graphical output, e.g. a piechart
extend	Creates a calculated column and adds it to the result set
project	Selects the columns to include in the order specified
distinct	Produces a table with the distinct combination of the provided columns of the input table
sort	Sort the rows of the input table by one or more columns in ascending or descending order
let	Creates a temporary variable that can be referenced
union	Takes two or more tables and returns all their rows
Join	Merges the rows of two tables to form a new table by matching values of the specified columns from each table

Cyber Threat Intelligence



STIX & TAXII

- STIX (Structured Threat Information eXpression)
- TAXII (Trusted Automated eXchange of Indicator Information)
- Purpose: Share Threat Intelligence

STIX & TAXII

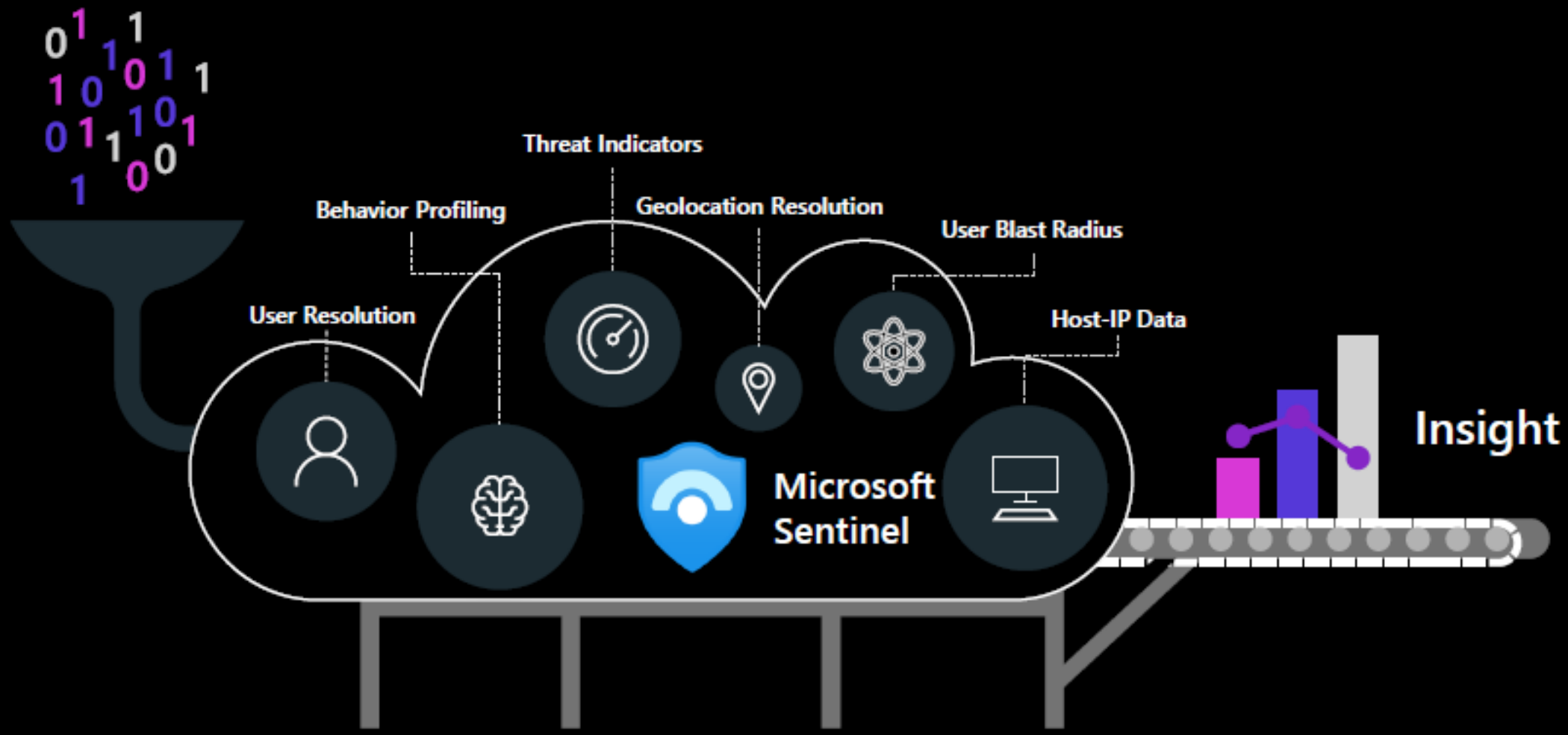
- STIX
  - Standardized language build on JSON
  - Enables the exchange of CTI between systems
- TAXII
  - The protocol that transmits STIX insights via HTTPS

Threat Intelligence in Sentinel

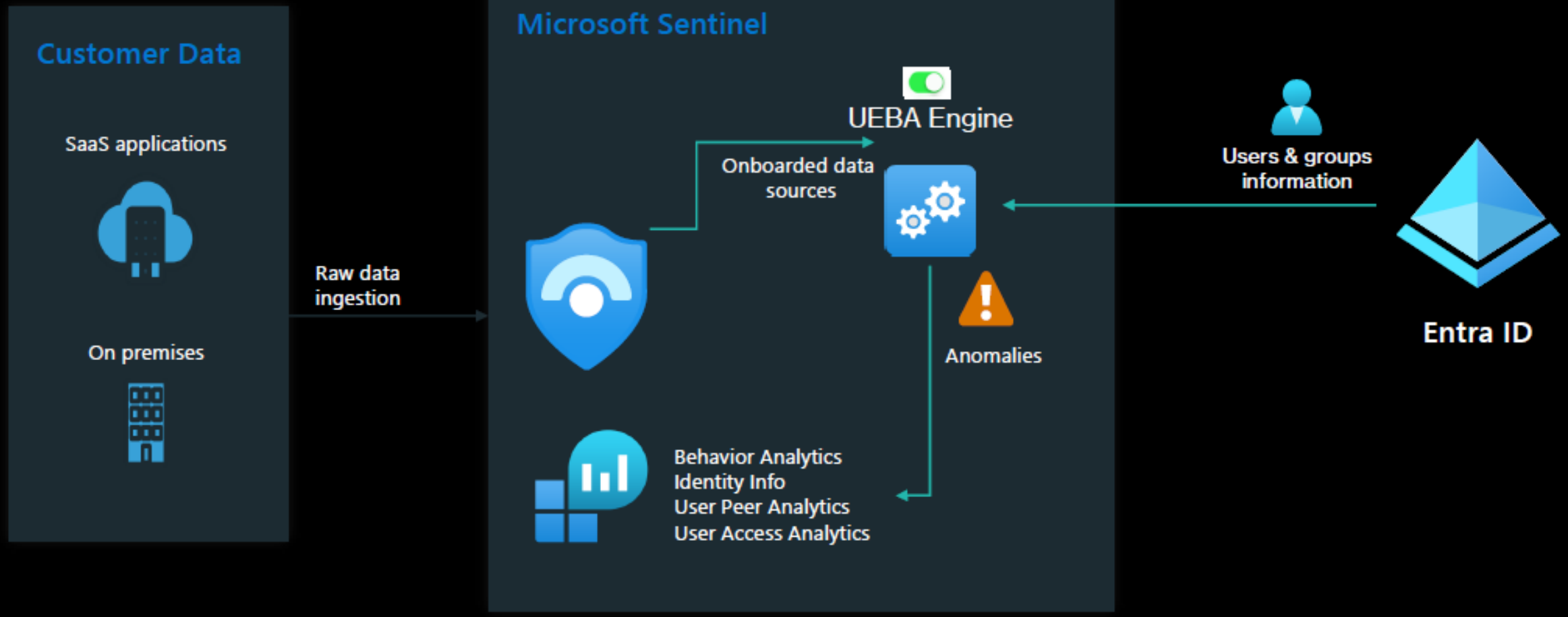
In Sentinel, Threat Intelligence can be used in:

- Analytic Rules
- Threat Hunting
- Incidents
- Workbooks
- Notebooks
- Playbooks

User and Entity Behavior Analytics (UEBA)



UEBA


Customer Data
SaaS applications
On premises
Raw data ingestion
Microsoft Sentinel
UEBA Engine
Onboarded data sources
Anomalies
Behavior Analytics
Identity Info
User Peer Analytics
User Access Analytics
Users & groups information
Entra ID

MITRE ATT&CK Framework

Adversarial Tactics, Techniques (ATT) & Common Knowledge (CK)

Funded by US Homeland Security

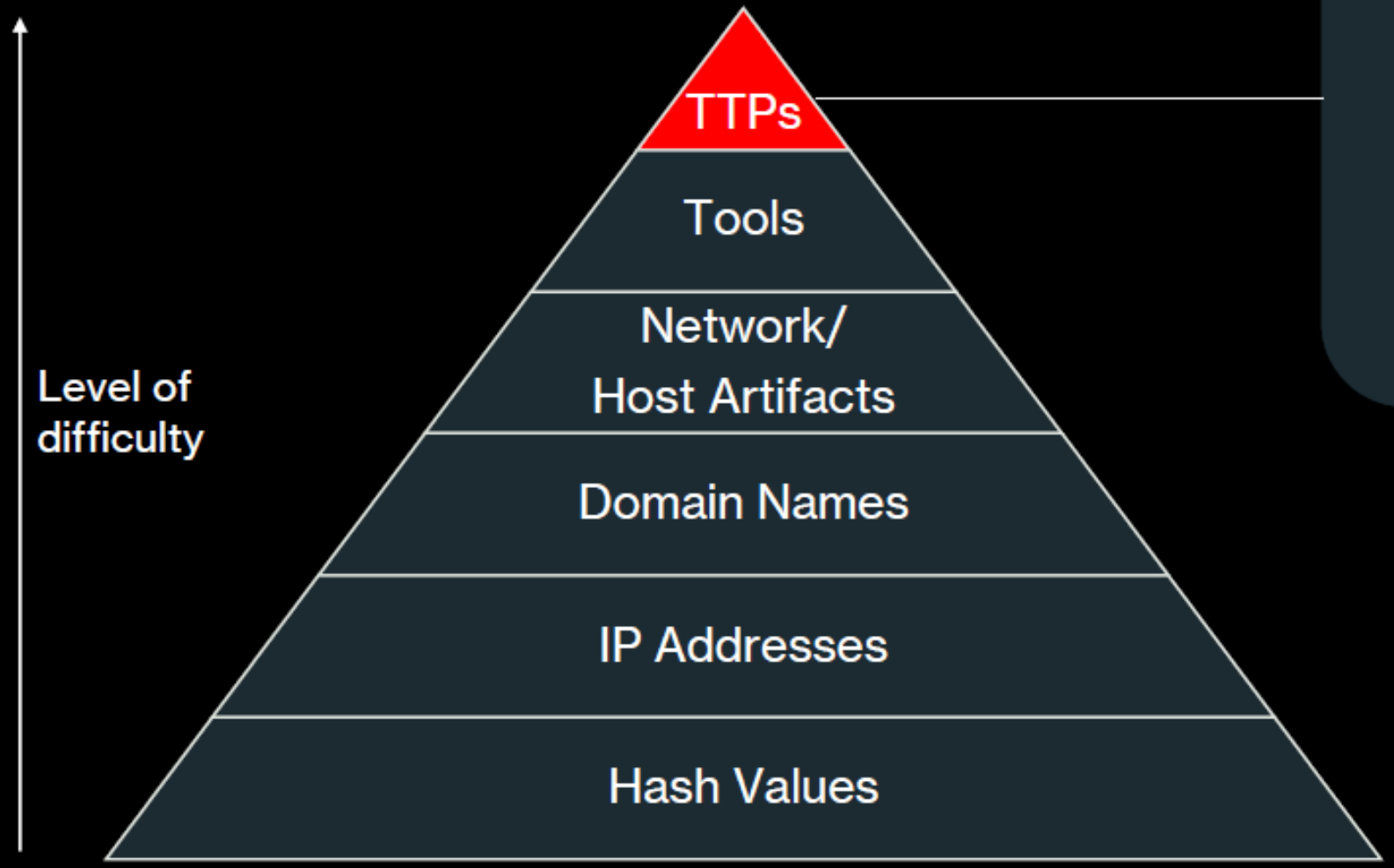
Tactics, Techniques, & Procedures (TTPs)

TTPs help cyber professionals categorize, describe, and defend against known attack methods

MITRE ATT&CK Framework

- MITRE ATT&CK™ "is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies"
- MITRE ATT&CK®

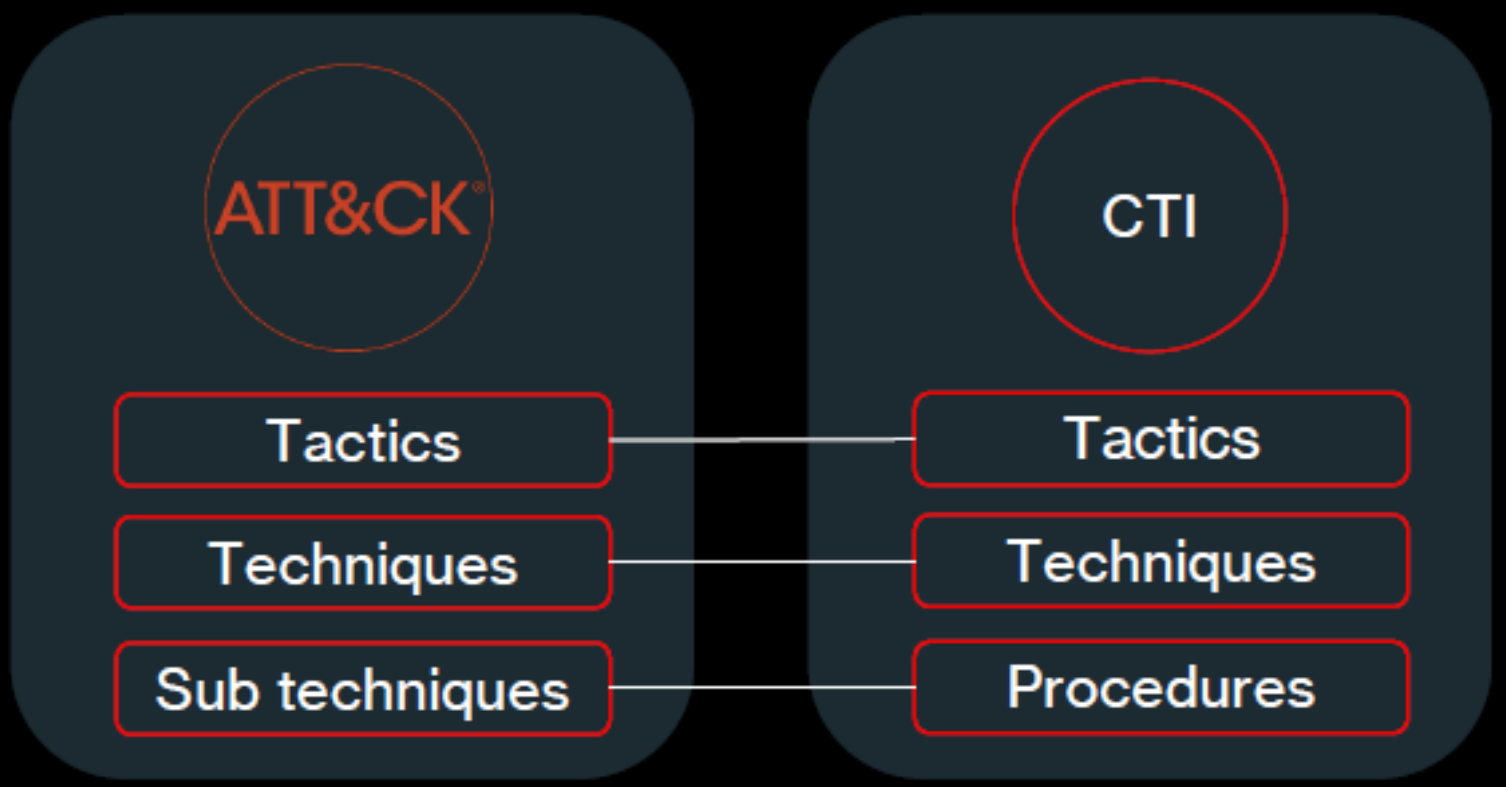
ATTACK & Pyramid of Pain



ATT&CK®

- Tactics
- Techniques
- Sub techniques

TTPs in ATT&CK



ATT&CK Matrices

Enterprise

Mobile

ICS

Google Workspace

ATT&CK Tactics

- The WHY of an adversary attacking an orga
- Tactical adversary objectives
- 14 Tactics

ATT&CK Tactics

ID	Tactic	Behavior
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

ATT&CK Techniques

- The HOW an adversary performs its attack
- 201 Techniques

ATT&CK Techniques - Examples

Tactic	Technique
Reconnaissance	Active Scanning
Resource Development	Develop Capabilities
Initial Access	Phishing
Execution	Scheduled Task
Persistence	Create Account
Privilege Escalation	Escape to Host
Defense Evasion	Masquerading
Credential Access	Brute Force
Discovery	Account Discovery
Lateral Movement	Internal Spearphishing
Collection	Email Collection
Command and Control	Encrypted Channel
Exfiltration	Exfiltration over C2
Impact	Data Destruction

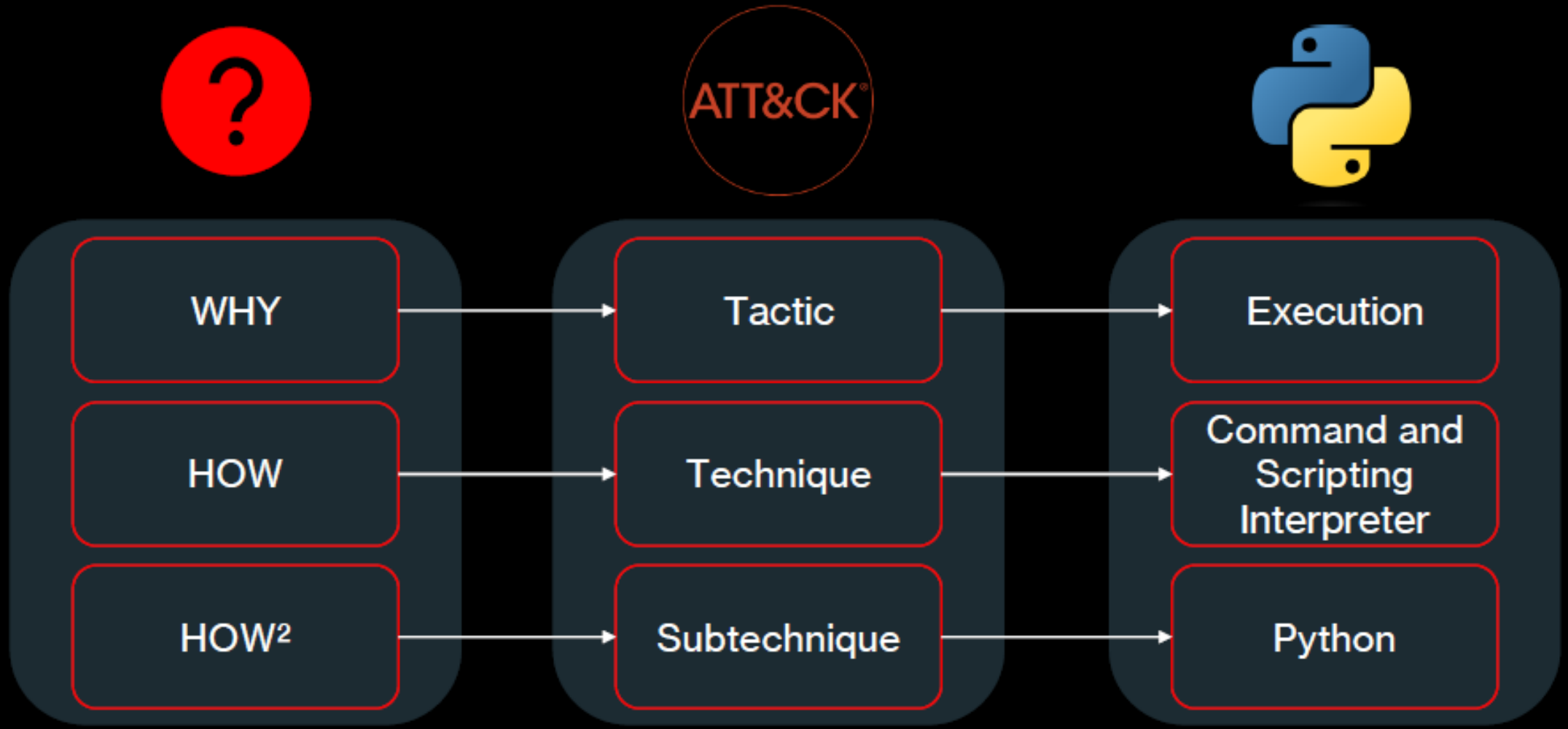
ATT&CK Subtechniques

- The HOW an adversary performs its attack, but more detailed than techniques
- 424 Sub-techniques

ATT&CK Subtechniques - Examples

Tactic	Technique	Subtechnique
Reconnaissance	Active Scanning	Vulnerability Scanning
Resource Development	Develop Capabilities	Malware
Initial Access	Phishing	Spearphishing Attachment
Execution	Scheduled Task	Cron
Persistence	Create Account	Local Account
Privilege Escalation	Process Injection	Dynamic-link Library Injection
Defense Evasion	Masquerading	Double File Extension
Credential Access	Brute Force	Password Spraying
Discovery	Account Discovery	Cloud Account
Lateral Movement	Remote Services	Remote Desktop Protocol
Collection	Email Collection	Remote Email Collection
Command and Control	Encrypted Channel	Asymmetric Cryptography
Exfiltration	Exfiltration Over Alternative Protocol	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Impact	Network Denial of Service	Direct Network Flood

Tactics, Techniques and Sub-techniques



ATT&CK Data Sources

- Data source provide the source for collected telemetry
- Helps you identify the correct data source to combat TTPs with monitoring

Tactic	Technique	Subtechnique	Data Source
Reconnaissance	Active Scanning	Vulnerability Scanning	Network Traffic

ATT&CK Detections

- High level detection strategies for TTPs
- Especially focused on techniques and Subtechniques
- Gives a guideline on what to with the collected telemetry

Tactic	Technique	Subtechnique	Detection
Reconnaissance	Active Scanning	Vulnerability Scanning	Network Traffic Content & Flow

ATT&CK Mitigations

- Preventive configuration to reduce the attack surface
- Enables organizations to modify configuration so that TTPs may be prevented entirely
- Sometimes this is not possible to implement

Tactic	Technique	Subtechnique	Mitigation
Reconnaissance	Active Scanning	Vulnerability Scanning	Pre-compromise

Tactic	Technique	Subtechnique	Mitigation
Privilege Escalation	Scheduled Task / Job	Scheduled Task	Privileged Account Management

ATT&CK Groups

- Related behavior tracked with a common identifiable name
- Some adversary groups have multiple names associated with them due to vendors tracking groups with their own naming convention
  - Microsoft uses weather + origin, e.g. Midnight Blizzard
  - CrowdStrike uses animals + origin, e.g. Fancy Bear
  - Mandiant uses numbers, e.g. APT41

ATT&CK Software

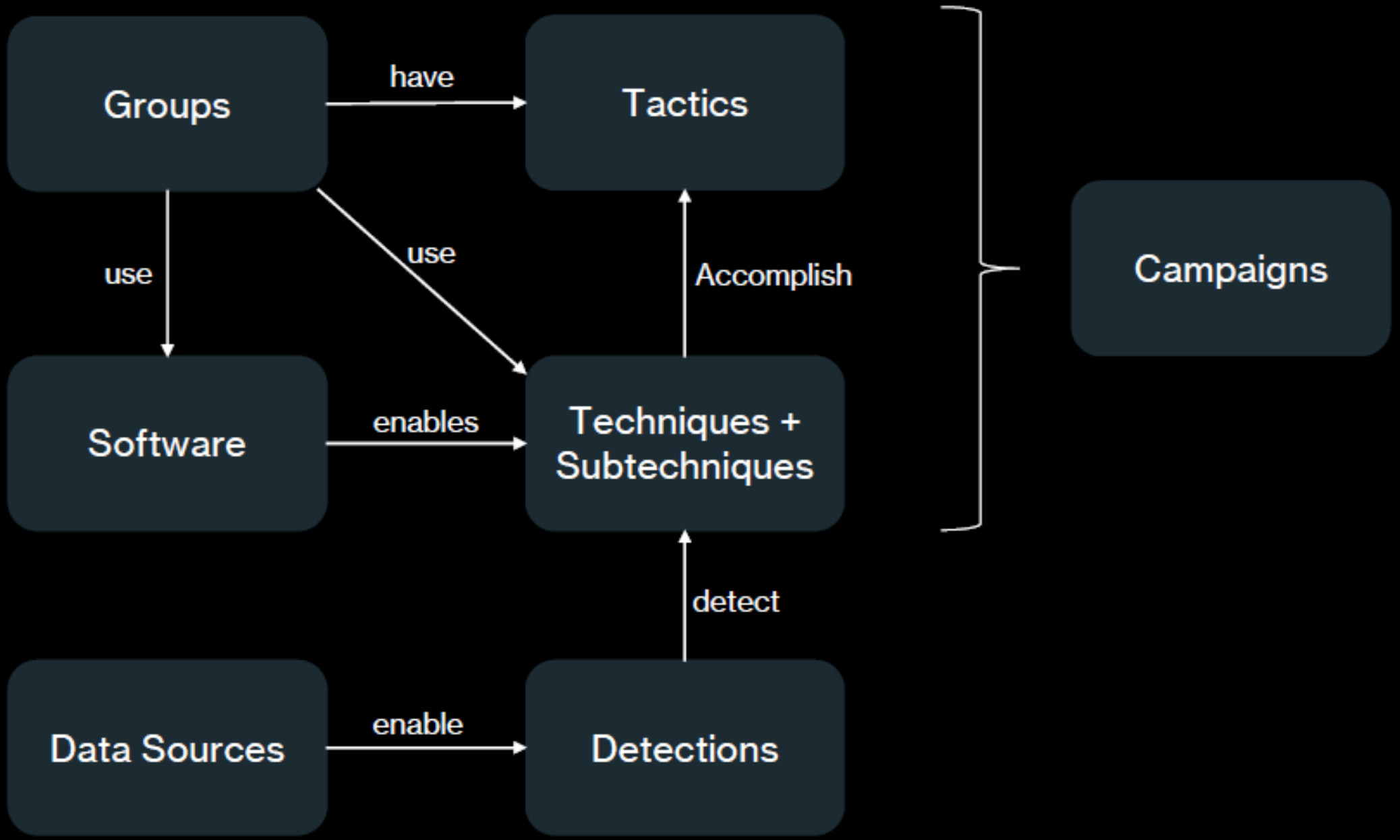
- Actual tools or malware used by adversaries
- Software is always linked to techniques, groups and campaigns
- Tools can be commercial, open-source, built-in, or publicly available software
- Malware can be commercial, custom closed source, or open-source software intended to be used for malicious purposes

ATT&CK Campaigns

- Intrusion activity conducted over a specific period of time with common targets and objectives

ID	Name	Description
C0025	2016 Ukraine Electric Power Attack	2016 Ukraine Electric Power Attack was a Sandworm Team campaign during which they used Industroyer malware to target and disrupt distribution substations within the Ukrainian power grid. This campaign was the second major public attack conducted against Ukraine by Sandworm Team.
C0012	Operation CuckooBees	Operation CuckooBees was a cyber espionage campaign targeting technology and manufacturing companies in East Asia, Western Europe, and North America since at least 2019. Security researchers noted the goal of Operation CuckooBees, which was still ongoing as of May 2022, was likely the theft of proprietary information, research and development documents, source code, and blueprints for various technologies. Researchers assessed Operation CuckooBees was conducted by actors affiliated with Winnti Group, APT41, and BARIUM.

ATT&CK Relations



Evolution of ATT&CK

- ATT&CK is a constantly evolving framework
- ATT&CK is updated roughly every 6 months
- New adversary behavior is added in the form of TTPs

Group: APT41 / Winnti

China's Winnti APT Compromises National Grid in Asia for 6 Months

Attacks against critical infrastructure are becoming more commonplace and, if a recent PRC-sponsored attack is anything to go by, easier to pull off.

Chinese APT group Winnti stole trade secrets in years-long undetected campaign

Gaming company targeted by Chinese Winnti hackers

BASF, Siemens, Henkel, Roche target of cyber attacks

Chinese hacker group APT41 uses recent exploits to target companies worldwide

Cyber Threat Intelligence

"Based on new intelligence reports, we believe APT41 / Winnti may target us as well"

ATT&CK: Group APT41 / Winnti

APT41

APT41 is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, APT41 has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. APT41 overlaps at least partially with public reporting on groups including BARIUM and Winnti Group.[1][2]

Winnti Group

Winnti Group is a threat group with Chinese origins that has been active since at least 2010. The group has heavily targeted the gaming industry, but it has also expanded the scope of its targeting.[1][2][3] Some reporting suggests a number of other groups, including Axiom, APT17, and Ke3chang, are closely linked to Winnti Group.[4]

Campaigns of APT41 / Winnti

ID	Name	Description
C0017	C0017	C0017 was an APT41 campaign conducted between May 2021 and February 2022 that successfully compromised at least six U.S. state government networks through the exploitation of vulnerable Internet facing web applications. During C0017, APT41 was quick to adapt and use publicly-disclosed as well as zero-day vulnerabilities for initial access, and in at least two cases re-compromised victims following remediation efforts. The goals of C0017 are unknown, however APT41 was observed exfiltrating Personal Identifiable Information (PII).
C0012	Operation CuckooBees	Operation CuckooBees was a cyber espionage campaign targeting technology and manufacturing companies in East Asia, Western Europe, and North America since at least 2019. Security researchers noted the goal of Operation CuckooBees, which was still ongoing as of May 2022, was likely the theft of proprietary information, research and development documents, source code, and blueprints for various technologies. Researchers assessed Operation CuckooBees was conducted by actors affiliated with Winnti Group, APT41, and BARIUM.

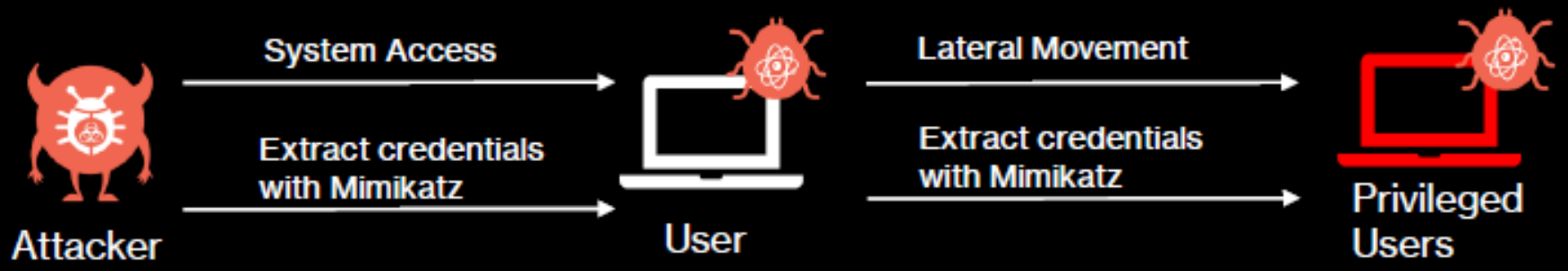
Techniques of APT41 / Winnti

- APT41: Leveraged 74 unique techniques and sub-techniques
- Winnti: Leveraged 6 unique techniques and sub-techniques

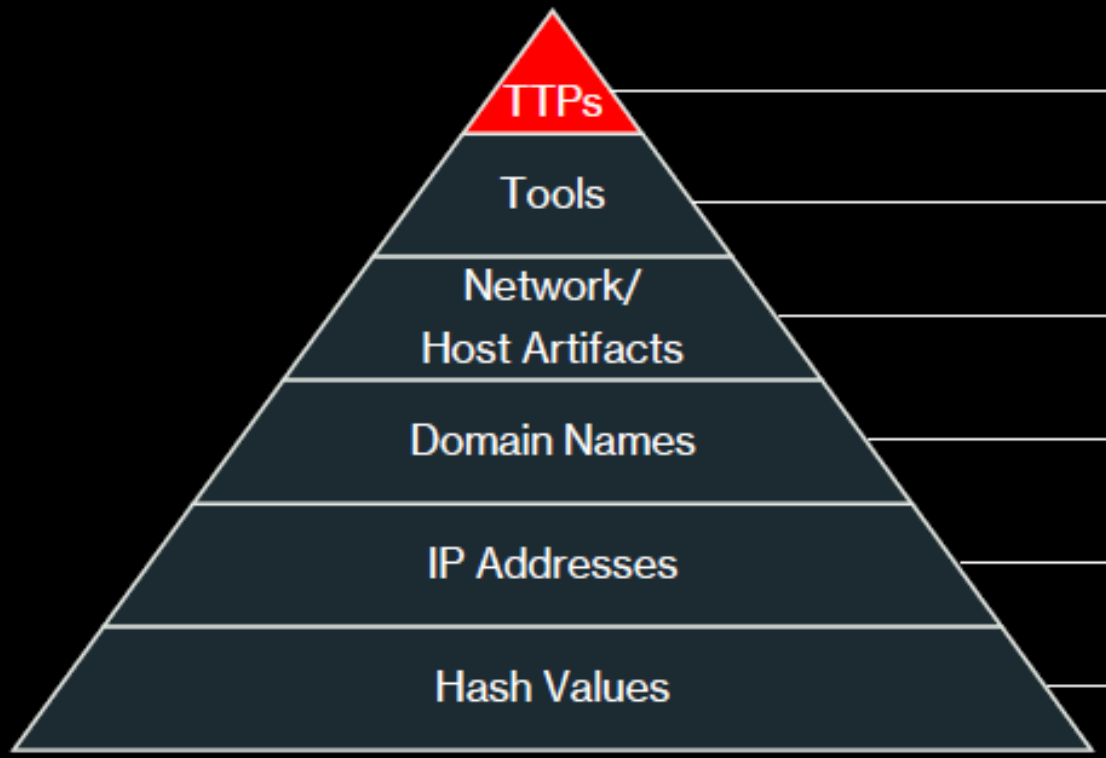
Mimikatz

```
  .#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr  6 2014 22:02:03)
 .## ^ ##.
## / \ ##  /* * *
## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
 '#####'                                     with  13 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 515764 (00000000:0007deb4)
Session           : Interactive from 2
User Name         : Gentil Kiwi
Domain            : vm-w7-ult-x
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * LM       : d0e9aee149655a6075e4540af1f22d3b
         * NTLM     : cc36cf7a8514893efccd332446158b1a
         * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
        tspkg :
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * Password : waza1234/
```

Technique: OS Credential Dumping: LSASS Memory



Pyramid of Pain for the Campaign

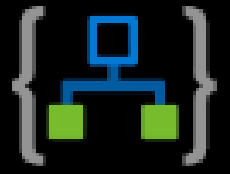


- Building a different tool that accomplishes the same as Mimikatz is tough!
- Changing the Mimikatz is challenging
- Changing the network is annoying
- Changing the domains for the campaign is simple
- Changing the IPs for the campaign is easy
- Changing the Hash of Mimikatz is trivial

Why automate?

- Security Automation is not: Isolating machines
- Security Automation is: Mimicking the steps an Analyst would take when responding to incidents
- Automation has a positive impact on:
  - Mean time to react
  - SOC efficiency
  - Cost
  - Standardized responses to incidents

Automation Capabilities

- Automation Rules 
  - Basic Automations
- Playbooks
  - Complex Automations →Think SOAR 

Automation Rules 

- Allow for centralized automation of incident handling
- Used to automate simple actions in your triage, such as:
  - Assigning users to incidents
  - Tagging incidents
  - Changing status of incidents
  - Triggering playbooks

Playbooks 

- Used to automate complex tasks → this is your SOAR!
- Used to trigger Azure Logic Apps
- Playbooks can also be triggered from Automation Rules

Automation Rules vs. Playbooks

	Playbooks	Automation Rules
Price	Logic Apps	Free
Purpose	SOAR	Automation as part of Triage
Scope	Close to limitless	Limited to Sentinel
Rule Types	Scheduled rules only	All rule types
Trigger	Sentinel & external triggers	Sentinel incidents

Azure Logic App Workflows

Example 1: Sentinel playbook triggers ticket creation in ServiceNow ITSM

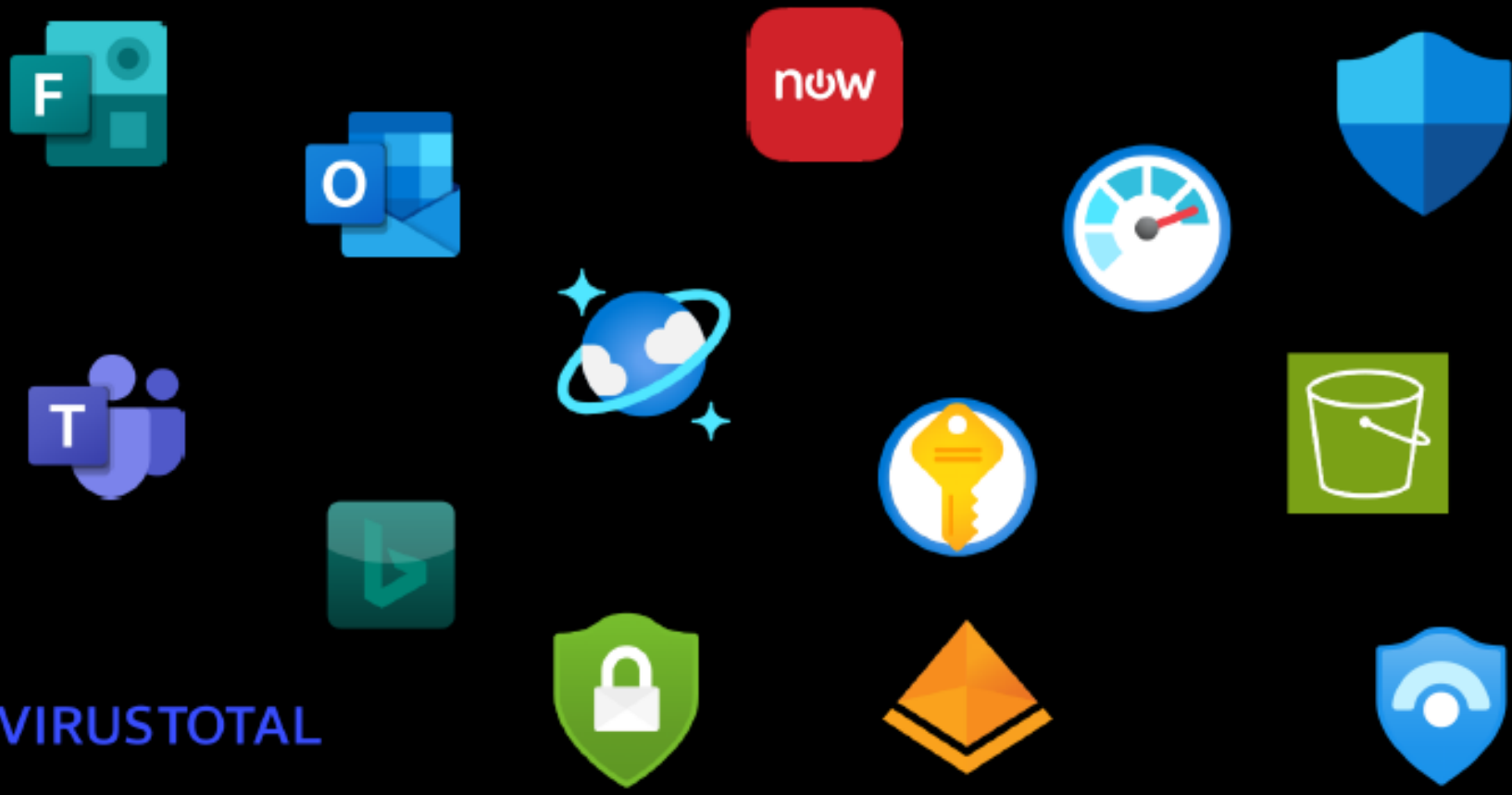
Example 2: User completes security incident form that creates an incident in Sentinel

Azure Logic App Workflows

Example 3: ChatGPT enriches Incident with explanation for a MITRE ATT&CK Tactic

Example 4: VirusTotal enriches Incident with analysis of IoCs

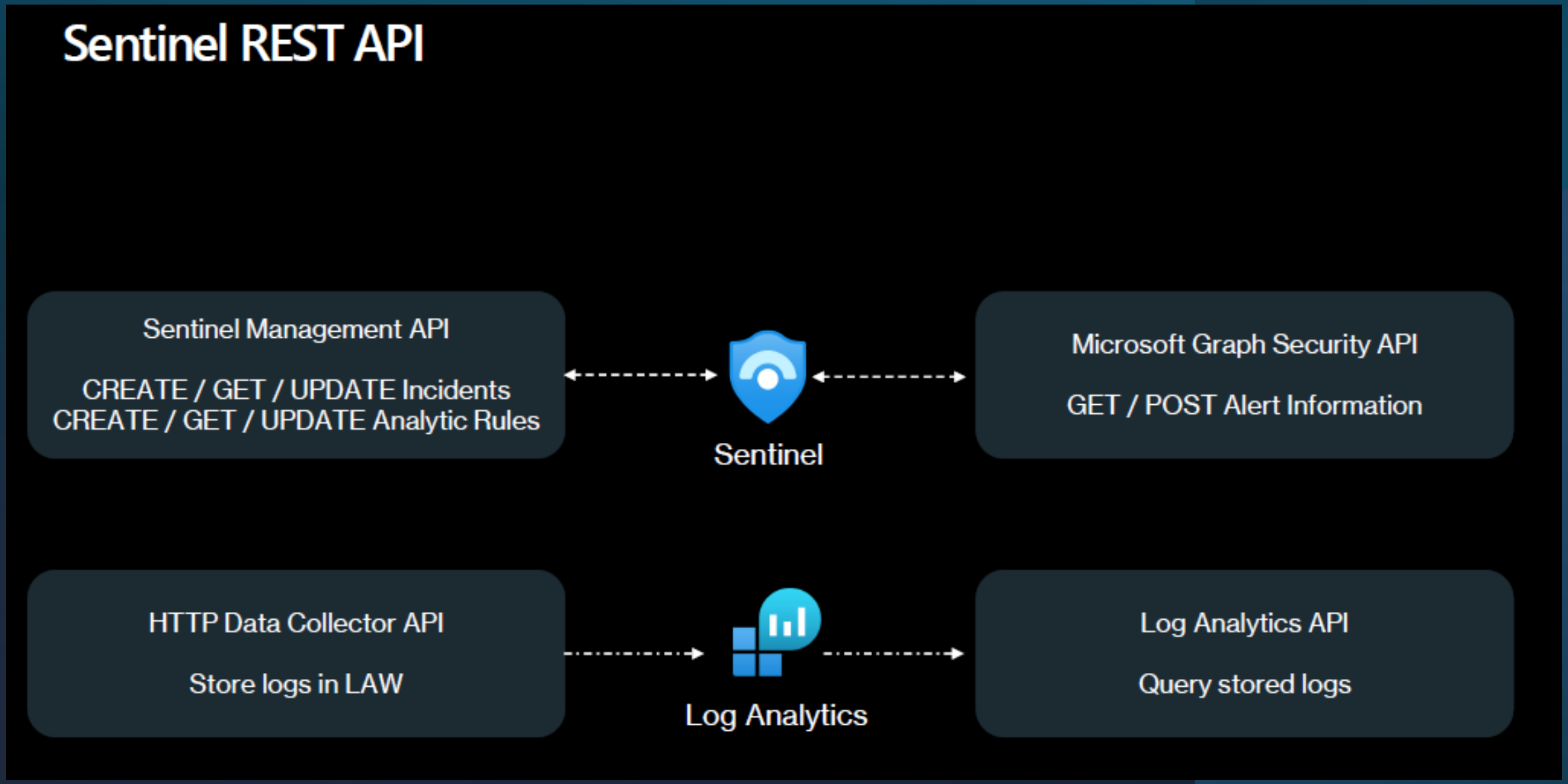
Logic App Connectors



Sentinel REST API

- Sentinel has several APIs that you can interact with:
  - Sentinel Management API
  - Microsoft Graph Security API
  - Azure Log Analytics API
  - HTTP data Collector API

Sentinel REST API



Workbooks 

- Workbooks are used to visualize data in e.g. dashboards
- 100s of templates are pre-built by Microsoft
- Can be customized with KQL

Watchlists 

- Static lists that can be referenced in KQL queries
- Use cases:
  - VIPs
  - Former employees
  - Lost & stolen devices
  - Exceptions
  - Critical assets

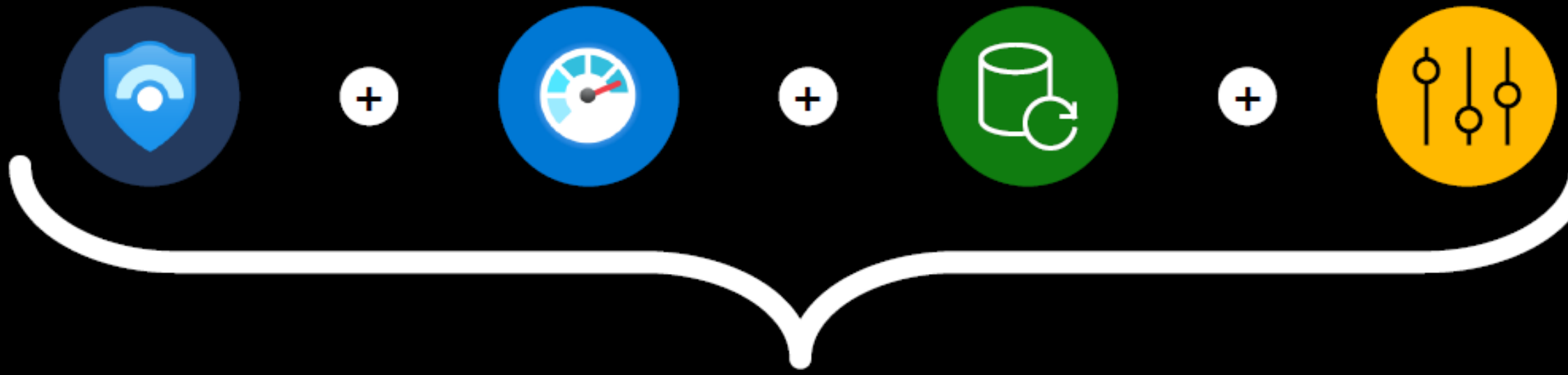
Legacy Pricing Model

Microsoft Sentinel price

Azure Monitor Log Analytics price

Data retention, restore and archiving price

Advanced capabilities



Microsoft Sentinel is billed for data ingested in to an Azure Monitor Log Analytics workspace and analyzed in Microsoft Sentinel.

Current Pricing Model

Microsoft Sentinel price

Data retention, restore and archiving price

Advanced capabilities

Microsoft Sentinel is billed based on data ingested, retention, and any automation costs

Commitment Tiers

Tier	Microsoft Sentinel Price	Effective Per GB Price[1]	Savings Over Pay-As-You-Go
Pay-As-You-Go	**$5.22** per GB-ingested	**$5.22** per GB-ingested	N/A
100 GB per day	**$342.52** per day	**$3.43** per GB	34%
200 GB per day	**$633.56** per day	**$3.17** per GB	39%
300 GB per day	**$924.60** per day	**$3.09** per GB	41%
400 GB per day	**$1,198.48** per day	**$3.00** per GB	43%
500 GB per day	**$1,460.80** per day	**$2.93** per GB	44%
1,000 GB per day	**$2,863.40** per day	**$2.87** per GB	45%
2,000 GB per day	**$5,538.80** per day	**$2.77** per GB	47%
5,000 GB per day	**$13,321** per day	**$2.67** per GB	49%
10,000 GB per day	**$25,576** per day	**$2.56** per GB	51%
25,000 GB per day	**$61,467.50** per day	**$2.46** per GB	53%
50,000 GB per day	**$117,990** per day	**$2.36** per GB	55%

[1]Data ingested into Microsoft Sentinel exceeding the selected daily commitment tier is charged at the effective tier prices listed above.

Sentinel Log Types

Analytics logs

Security and activity logs

- Used for continuous threat monitoring
- Available for 90 days, with option to archive
- Pay-as-you-go pricing with volume discounts and commitment tiers

Basic logs

High-volume logs

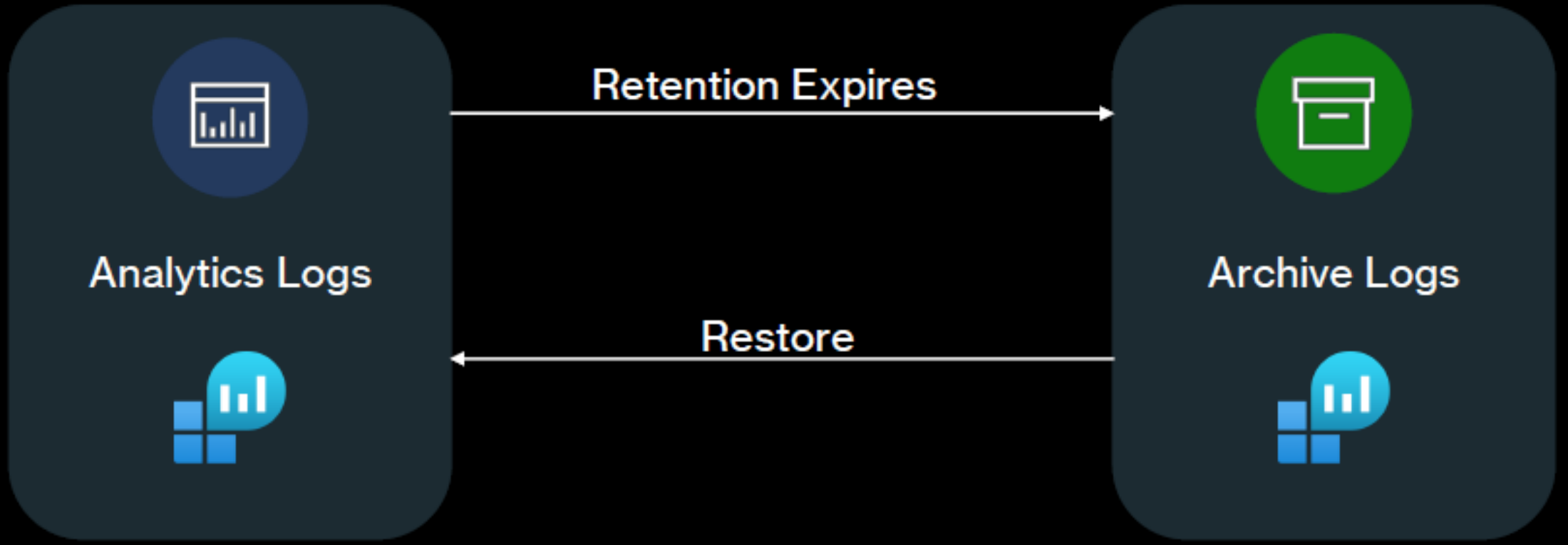
- Accessed on-demand for ad-hoc querying, investigations, and automation
- Supports ingestion-time parsing and transformation
- Available for 8 days, with option to archive

Archive

Low-cost, long-term storage

- Meet compliance requirements
- Archive data up to 7 years
- Easily search and restore archived logs

Archive and Restore Logs



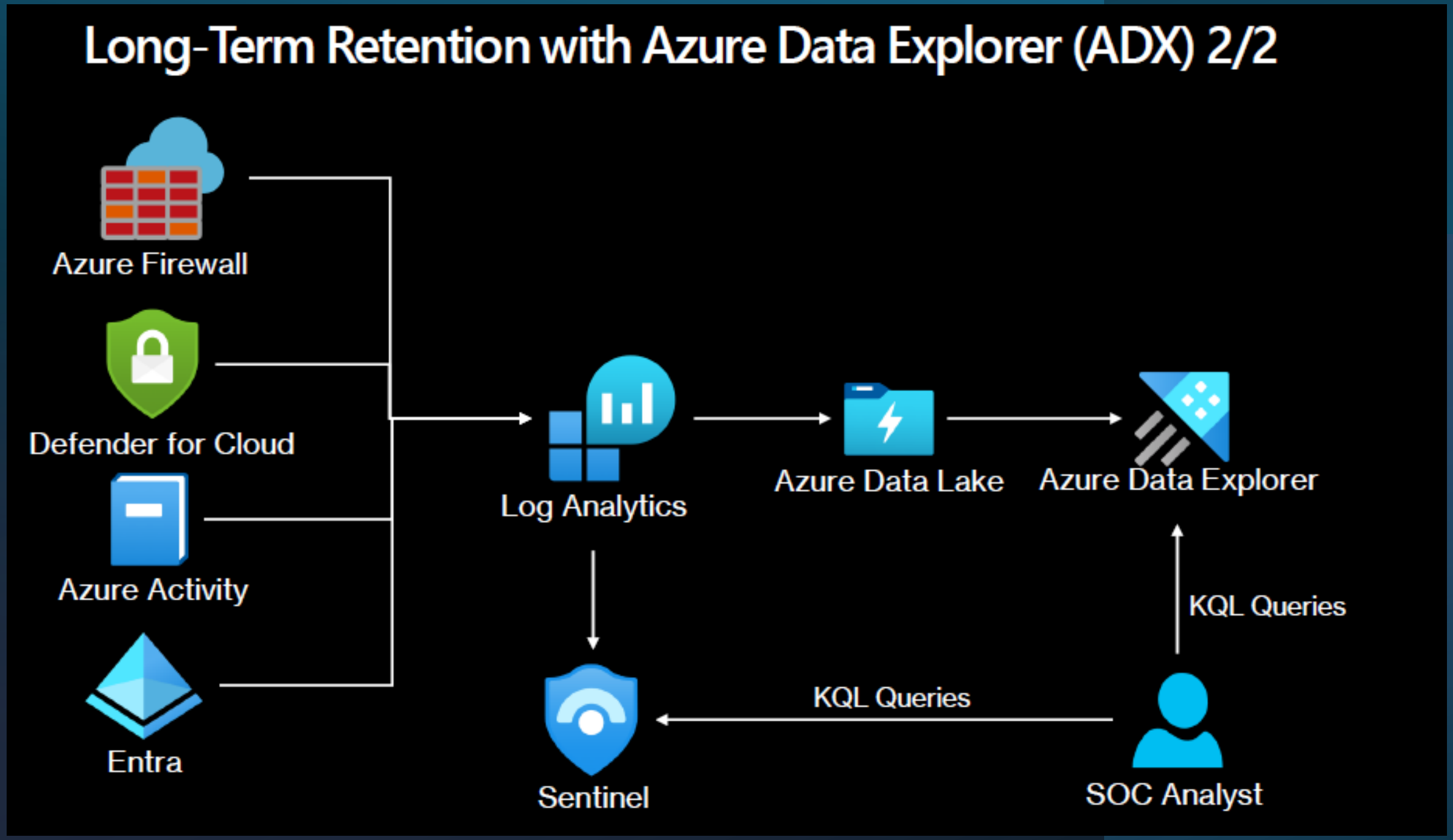
Long-Term Retention with Sentinel Archived Logs

- Simple long-term retention log type in Sentinel
- Max retention is 7 years
- Limited Threat Hunting experience

Long-Term Retention with Azure Data Explorer (ADX) 1/2

- ADX is a big data interactive analytics platform
- ADX is an individual Azure Service – not a Sentinel feature
- No out-of-the-box SIEM or SOAR features
- Threat Hunting with KQL

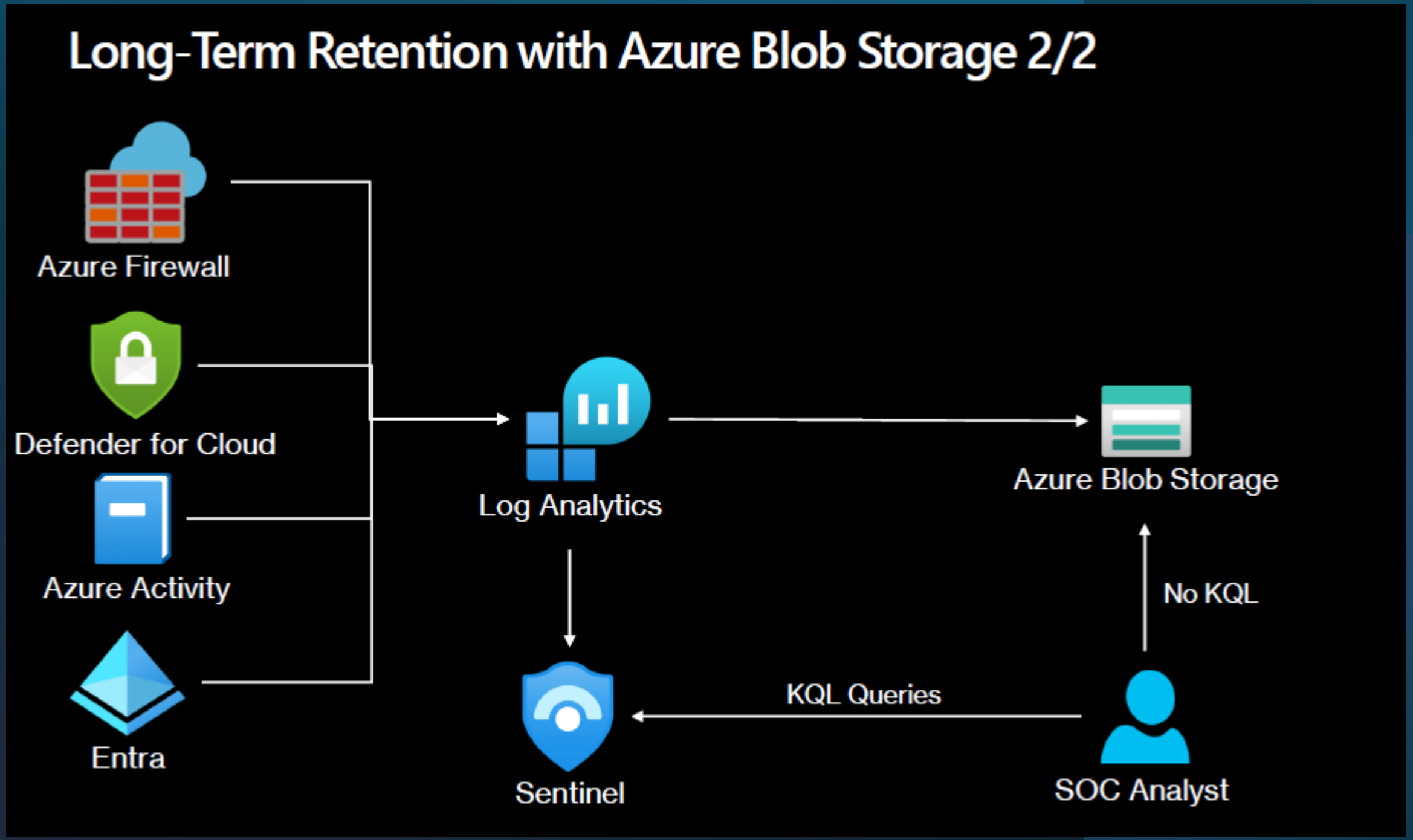
Long-Term Retention with Azure Data Explorer (ADX) 2/2



Long-Term Retention with Azure Blob Storage 1/2

- Simple PaaS storage service
- No SIEM or SOAR features
- No threat hunting with KQL

Long-Term Retention with Azure Blob Storage 2/2

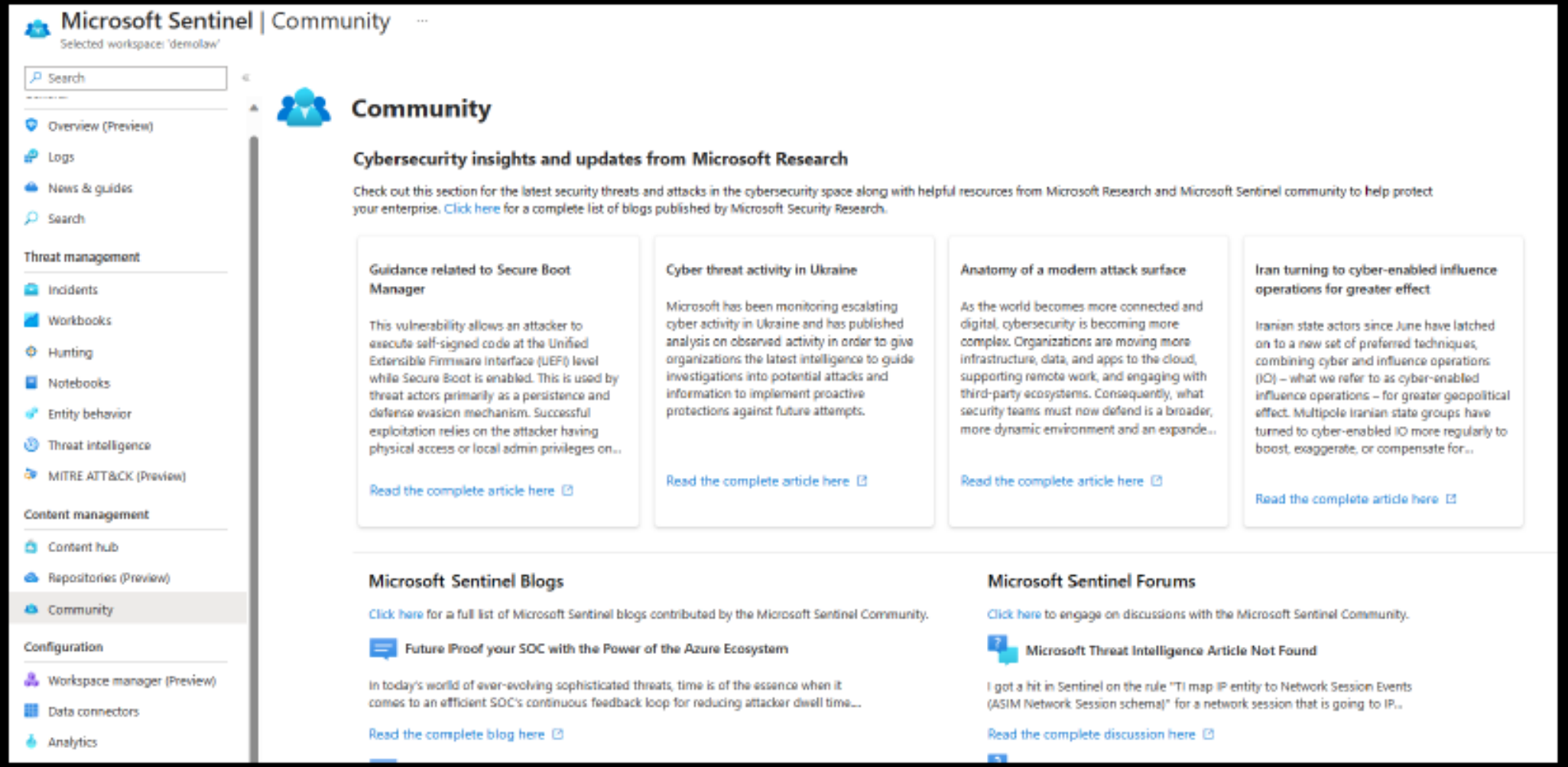


Long-Term Retention Side-by-Side

Storage Options	Sentinel Analytics Logs	Sentinel Archived Logs	Azure Data Explorer	Azure Blob Storage
Performance	High	Medium	High	Medium
Maximum Retention	2 years	7 years	Unlimited	400 years
Cloud Model	SaaS	SaaS	PaaS	PaaS
Cost	High	Low	Medium	Low
Purpose	• Daily SOC operations	• Long-term storage to search and restore data • Limited for threat hunting	• Long-term storage to search and restore data • Extended threat hunting	• Long-term storage to search and restore data

Sentinel Content Community

- Browse the Community blade in the Azure Portal
- “Deploy to Azure” is often supported



Sentinel Community Resources

Microsoft Sentinel Tech Community: techcommunity.microsoft.com

What's New in Microsoft Sentinel: https://aka.ms/AzureSentinelWhatsNew

Microsoft Sentinel Blog: https://aka.ms/AzureSentinelBlog

Microsoft Security Blog: https://www.microsoft.com/security/blog/

Official Sentinel GitHub Repository: https://aka.ms/AzureSentinel/GitHub

Cloud Security Private Preview program: https://aka.ms/prseccom

Azure Cloud Blog: https://azurecloudai.blog/category/microsoft-sentinel/

Podcasts and VODs

Microsoft Security Webinars: https://aka.ms/SecurityWebinars

Azure Security Community: https://aka.ms/SecurityCommunityVideos

Microsoft Security YouTube: https://www.youtube.com/microsoftsecurity

Azure Security Email List: https://aka.ms/SecurityEmailList

Azure Security Podcast: https://aka.ms/AzSecPod

Microsoft Security Insights Podcast: http://microsoftsecurityinsights.com/

Sentinel Training

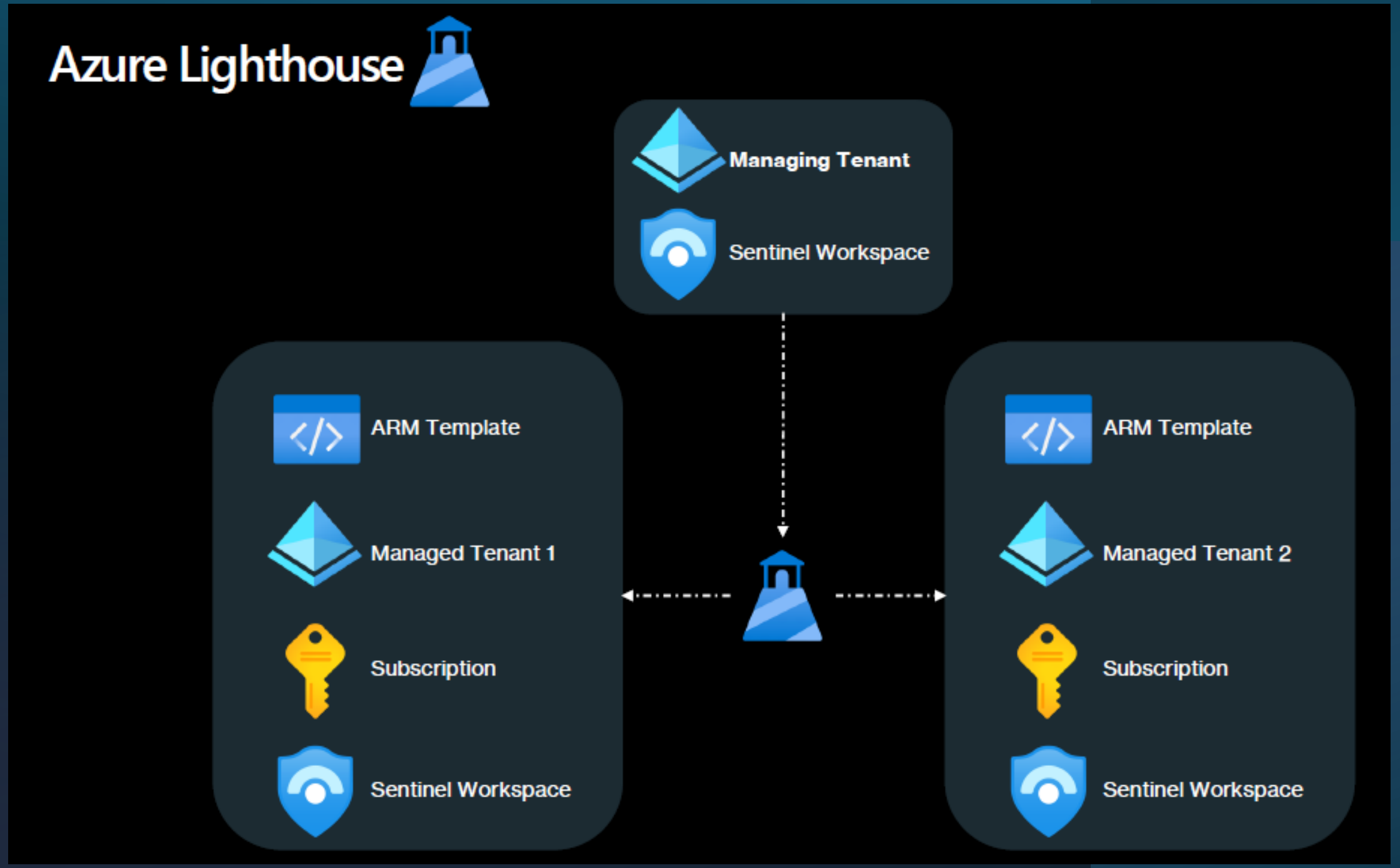
Microsoft Sentinel Documentation: https://learn.microsoft.com/en-us/azure/sentinel/

Microsoft Sentinel Ninja Training: https://aka.ms/SentinelNinja

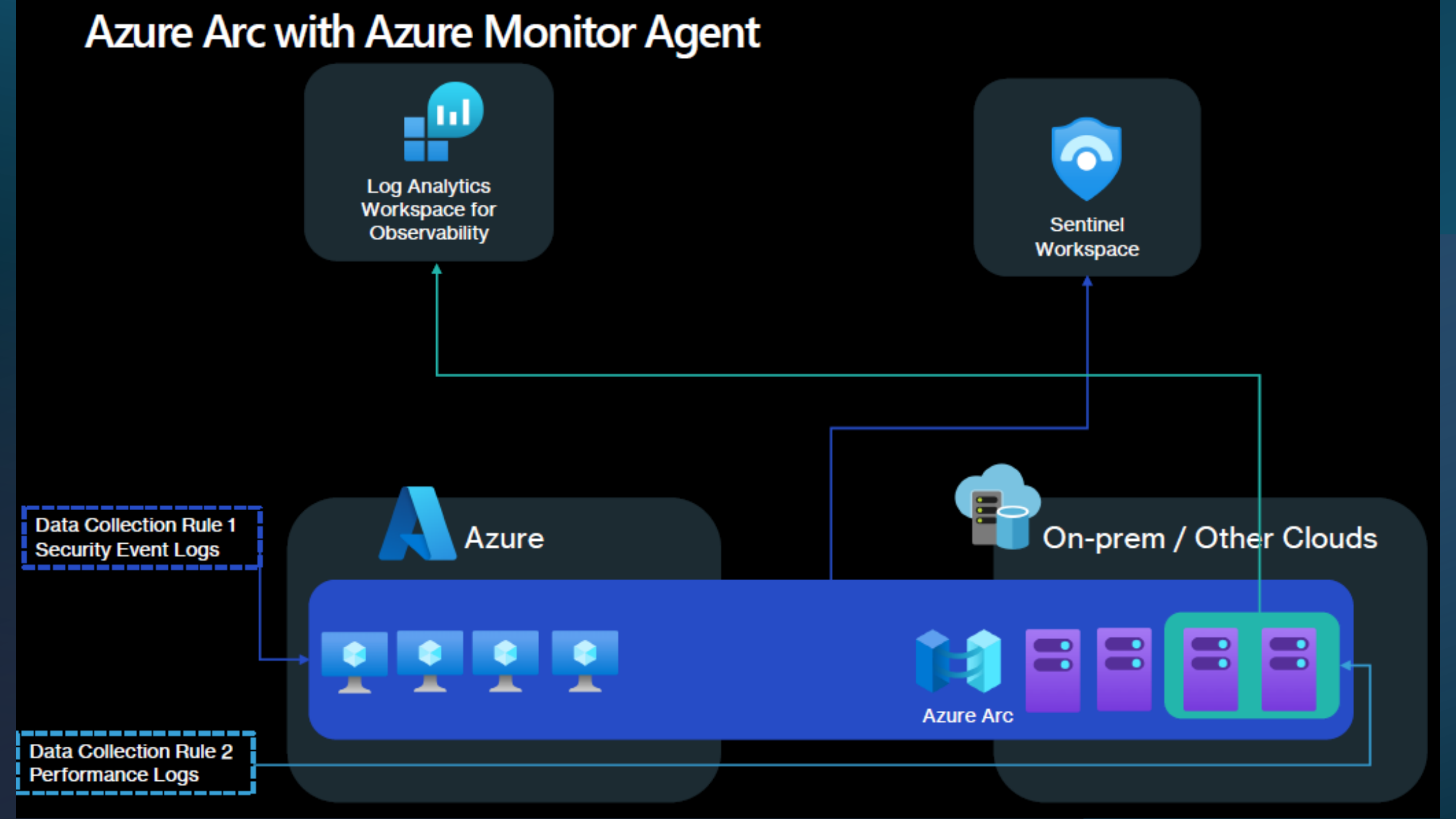
Microsoft SOC Analyst Exam: https://learn.microsoft.com/en-us/learn/certifications/exams/sc-200

Azure Lighthouse 

- Lighthouse is an individual Azure Service
- Provides the ability to manage resources across multiple tenants
- You can manage resources from your own tenant instead of switching to other tenants
- Resources that can be managed via Lighthouse are e.g.:
  - Sentinel
  - Defender for Cloud
  - Azure Monitor


Azure Lighthouse
Managing Tenant
Sentinel Workspace
ARM Template
Managed Tenant 1
Subscription
Sentinel Workspace
ARM Template
Managed Tenant 2
Subscription
Sentinel Workspace

Azure Arc with Azure Monitor Agent



Notebooks

- Notebooks allow you to use Python Jupyter notebooks for ML, visualization and data analysis in Sentinel
- You must first create an Azure ML Workspace
- Using Python Packages, you can utilize e.g.:
  - Statistics and numerical computing
  - Machine learning and deep learning
  - Visualizations and graphics
  - Data processing and analysis

What is Infrastructure as Code (IaC)?

- Infrastructure as Code (IaC) is managing and provisioning of infrastructure through code instead of manual processes
- Benefits:
  - Reduced errors
  - Increased deployment speed at scale
  - Improved deployment consistency
  - Cost reduction
  - Security & governance by design

Repositories

- Repositories help you automating the deployment and management of your Sentinel content through central repositories with IaC
- Repositories can be either GitHub or Azure DevOps
- Supported content types:
  - Analytics rules
  - Hunting queries
  - Automation rules
  - Playbooks
  - Parsers
  - Workbooks

Managing Sentinel with Azure ARM Templates

- JSON files that represent your resources as Code

Azure Storage Account

JSON

```
"resources": [
  {
    "type": "Microsoft.Storage/storageAccounts",
    "apiVersion": "2022-09-01",
    "name": "mystorageaccount",
    "location": "centralus",
    "sku": {
      "name": "Standard_LRS"
    },
    "kind": "StorageV2"
  },
]
```

Managing Sentinel with Azure Bicep

- Domain-specific language that uses declarative syntax to deploy Azure resources

Azure Storage Account

Bicep

```
param location string = resourceGroup().location
param storageAccountName string = 'toylaunch${uniqueString(resourceGroup().id)}'

resource storageAccount 'Microsoft.Storage/storageAccounts@2021-06-01' = {
  name: storageAccountName
  location: location
  sku: {
    name: 'Standard_LRS'
  }
  kind: 'StorageV2'
  properties: {
    accessTier: 'Hot'
  }
}
```

Managing Sentinel with Terraform

- Cloud agnostic IaC language

Azure Storage Account

```
resource "azurerm_resource_group" "example" {
  name     = "example-resources"
  location = "West Europe"
}

resource "azurerm_storage_account" "example" {
  name                     = "storageaccountname"
  resource_group_name      = azurerm_resource_group.example.name
  location                 = azurerm_resource_group.example.location
  account_tier             = "Standard"
  account_replication_type = "GRS"

  tags = {
    environment = "staging"
  }
}
```

What is Azure DevOps?

Azure Boards

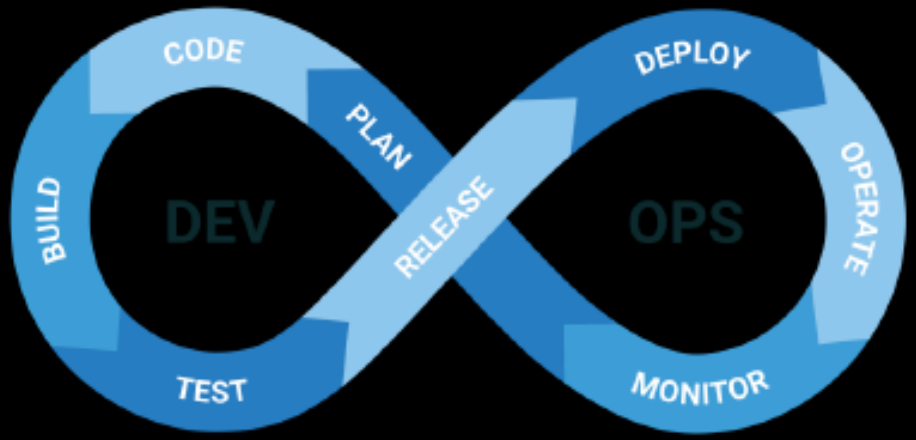
Azure Pipelines

Azure Repos

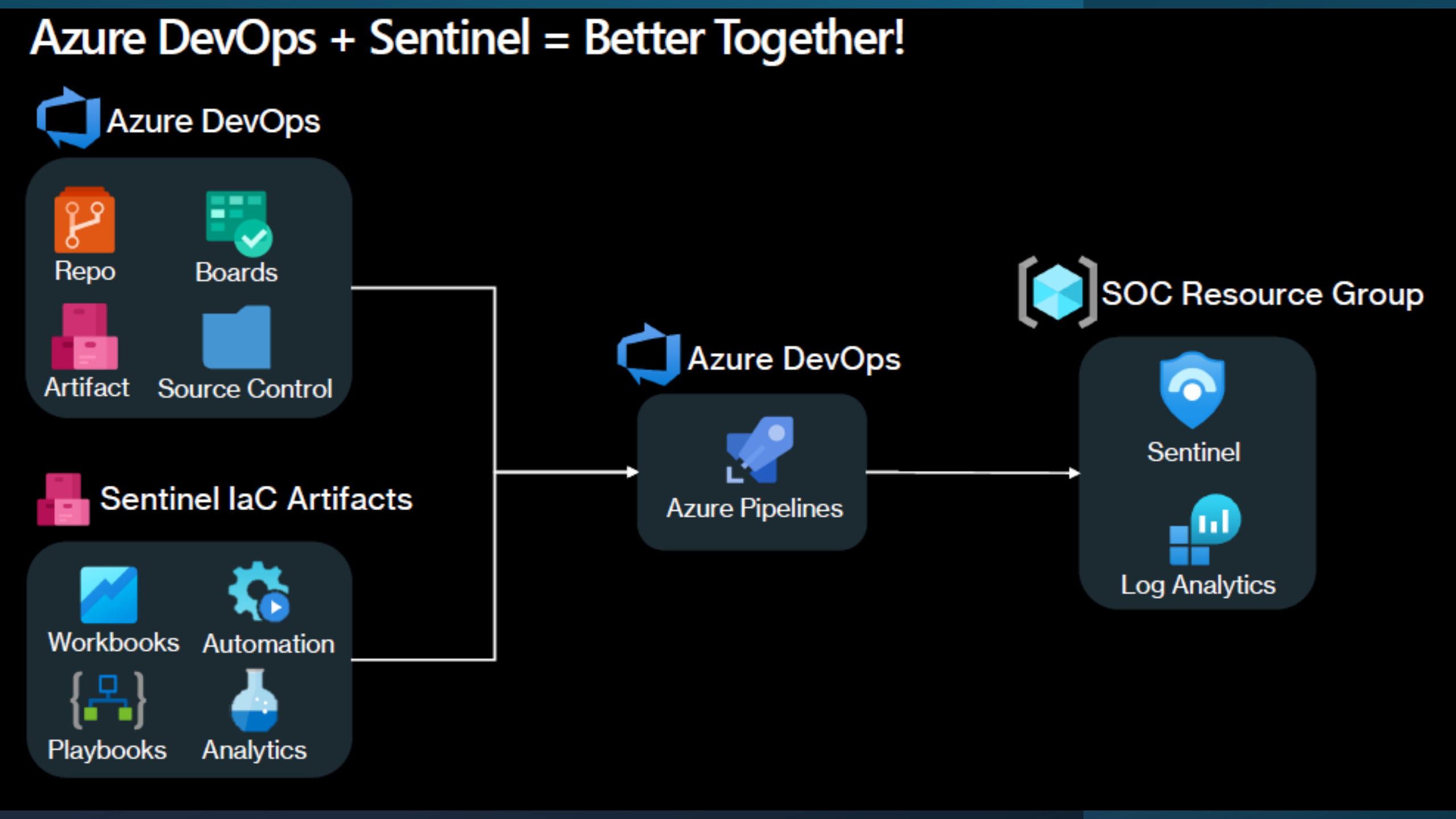
Azure Artifacts

Azure Test Plans

Azure DevOps



Azure DevOps + Sentinel = Better Together!



End of presentation

Thank you!