Curso SC 200

Microsoft Security Operation Analitcs

Curso de Preparação para Realização do Exame de Certificação SC 200.

Instrutor: Célio Ramos

Formação: Graduado em Segurança da Informação e Pós-graduado em Gerenciamento de Projetos e MBA Gestão de Qualidade de Software e 14x Microsoft Azure

Microsoft 365
CERTIFIED
SECURITY ADMINISTRATOR
ASSOCIATE

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

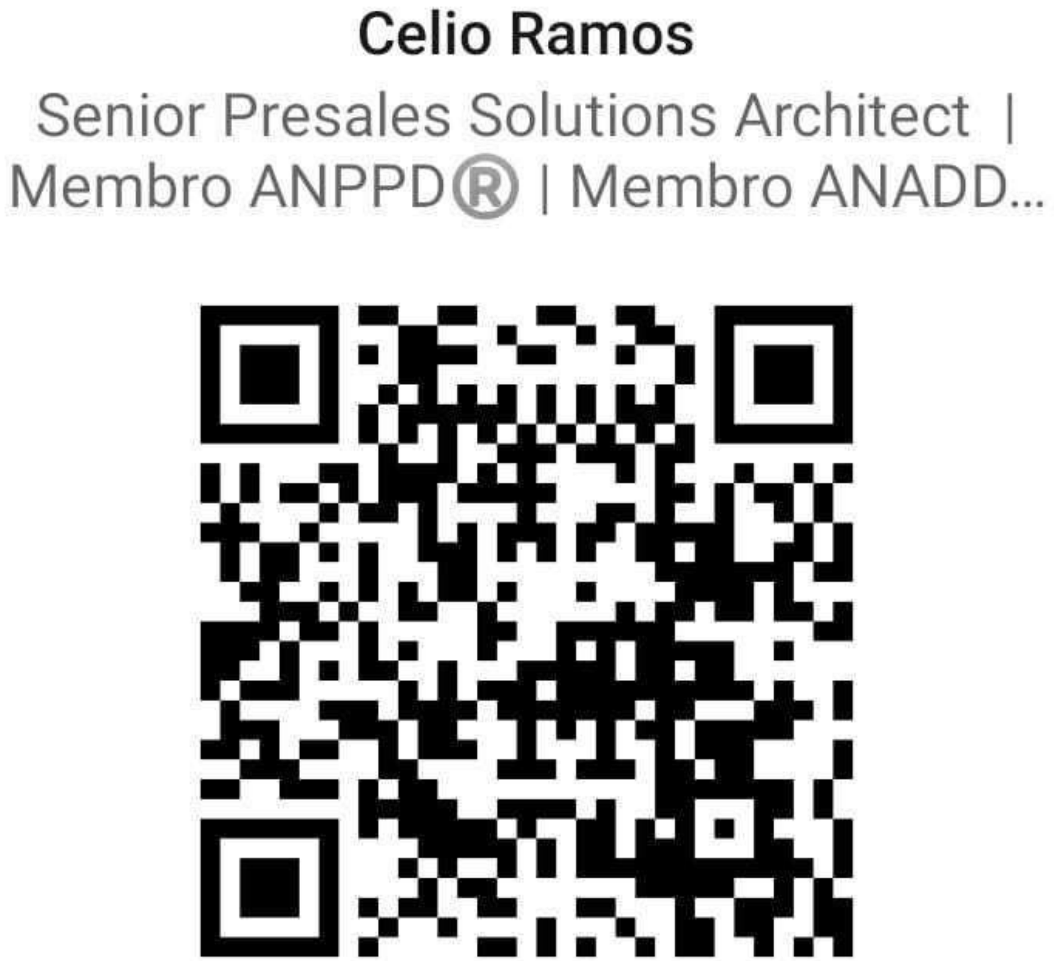
MICROSOFT CERTIFIED TRAINER
Microsoft
MCT
Trainer
2022 - 2023

Microsoft
CERTIFIED
DEVOPS ENGINEER
EXPERT

Microsoft
CERTIFIED
AZURE SOLUTIONS ARCHITECT
EXPERT

Microsoft
CERTIFIED
CYBERSECURITY ARCHITECT
EXPERT

Meio de Contato:



Celio Ramos

Senior Presales Solutions Architect | Membro ANPPD® | Membro ANADD...

bora
lá

Certification areas (SC-200)

Study areas	Weights
Mitigate threats using Microsoft 365 Defender	25-30%
Mitigate threats using Microsoft Defender for Cloud	25-30%
Mitigate threats using Microsoft Sentinel	40-45%

- This course maps to the exam SC-200: Microsoft Security Operations Analyst
- Percentages indicate the relative weight of each area on the exam.
- The higher the percentage, the more questions you are likely to see in that area.

Microsoft Defender for DNS

Microsoft Defender for DNS provides an extra layer of protection for your cloud resources by:

- Continuously monitoring all DNS queries from your Azure resources
- Running advanced security analytics to alert you about suspicious activity

Microsoft Security

Configure your Microsoft Sentinel environment

Agenda

- Introduction to Microsoft Sentinel
- Create and manage Microsoft Sentinel workspaces
- Query logs in Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
- Utilize threat intelligence in Microsoft Sentinel

Introduction to Microsoft Sentinel

Introduction

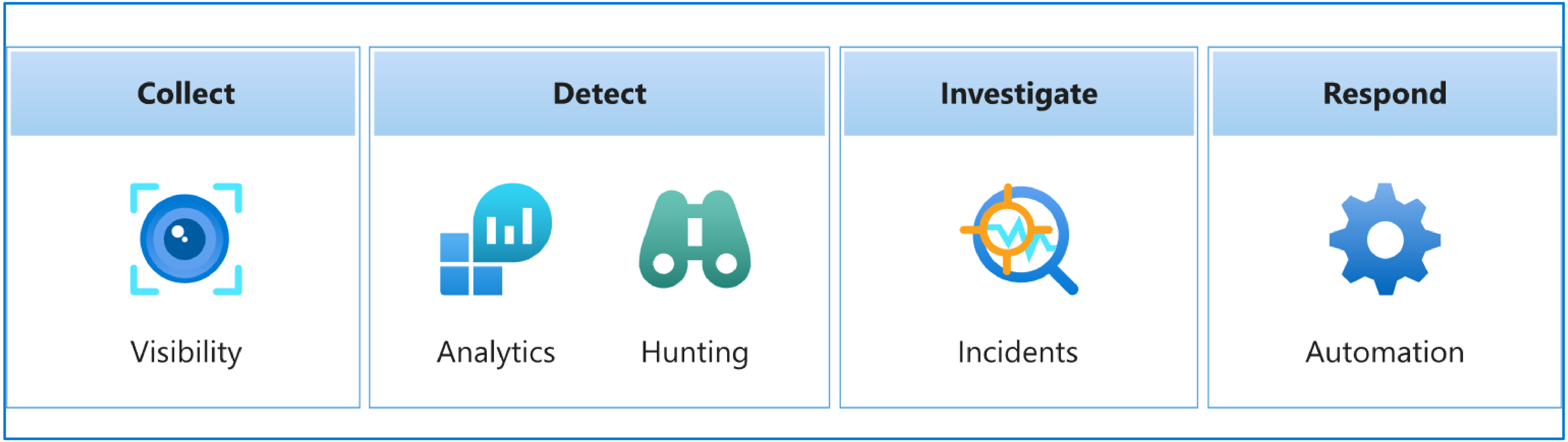
After completing this module, you will be able to:

- Identify the various components and functionality of Microsoft Sentinel

- Identify use cases where Microsoft Sentinel would be a good solution

Microsoft Sentinel explained

Microsoft Sentinel is a cloud-native SIEM. A SIEM system is a tool that an organization uses to collect, analyze, and perform security operations on its computer systems.



Collect

Visibility

Detect

Analytics

Hunting

Investigate

Incidents

Respond

Automation

How Microsoft Sentinel works

Microsoft Sentinel SIEM Solution Components

Data connectors

Parsers

Workbooks

Analytic rules

Hunting queries

Notebooks

Incidents and investigations

Automation playbooks and Azure Logic Apps custom connectors

Watchlists

When to use Microsoft Sentinel

Microsoft Sentinel is a solution for performing security operations on your cloud and on-premises environments.

Use Microsoft Sentinel if you want to:

- Collect event data from various sources.
- Perform security operations on that data to identify suspicious activity

Security operations could include:

- Visualization of log data.
- Anomaly detection.
- Threat hunting.
- Security incident investigation
- Automated response to alerts and incidents.

Decide whether it's the right fit for you:

- Cloud-native SIEM. There are no servers to provision, so scaling is effortless.
- Benefits of Microsoft research and machine learning.
- Support for hybrid cloud and on-premises environments.
- SIEM and a data lake all in one.

Clear requirements:

- Support for data from multiple cloud environments
- Features and functionality required for a security operations center (SOC), without too much administrative overhead

Create and manage Microsoft Sentinel workspaces

Introduction

After this module, you will be able to:

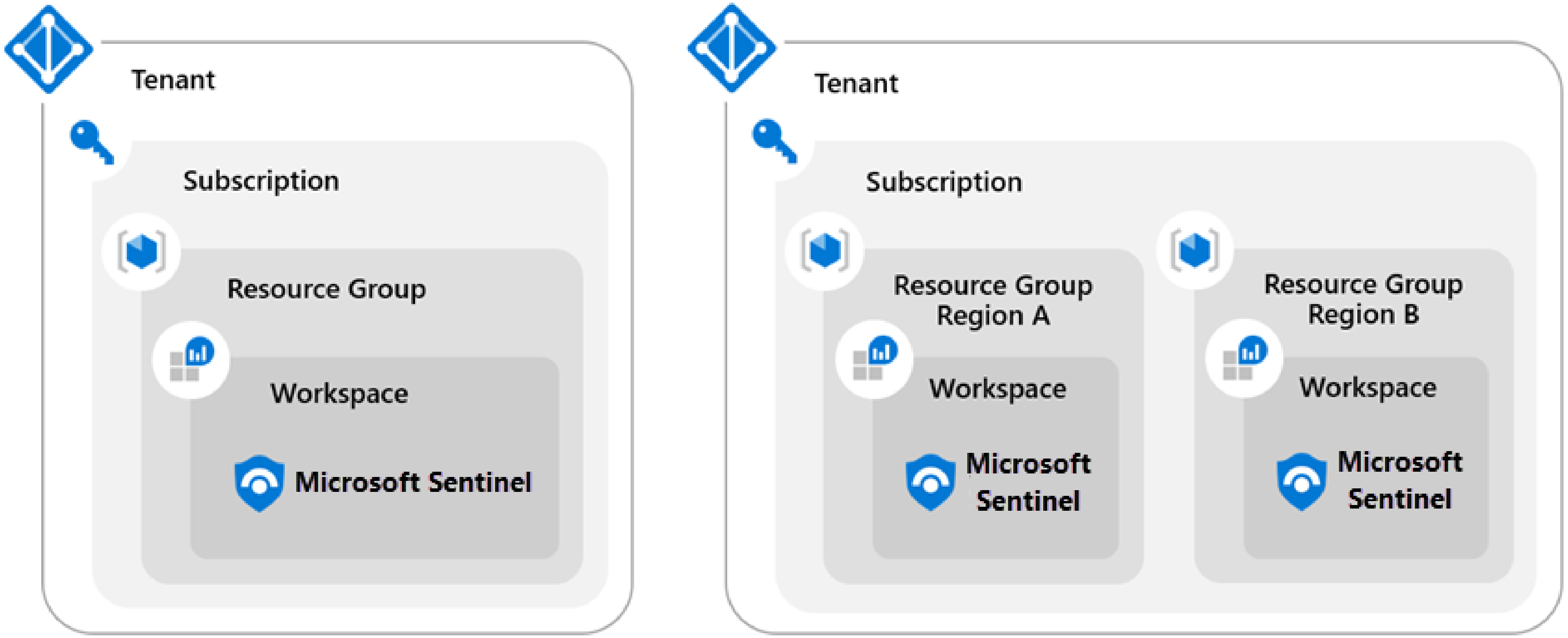
- Describe Microsoft Sentinel workspace architecture
- Install Microsoft Sentinel workspace
- Manage a Microsoft Sentinel workspace

Plan for the Microsoft Sentinel workspace

1 Single-Tenant with a single Microsoft Sentinel Workspace

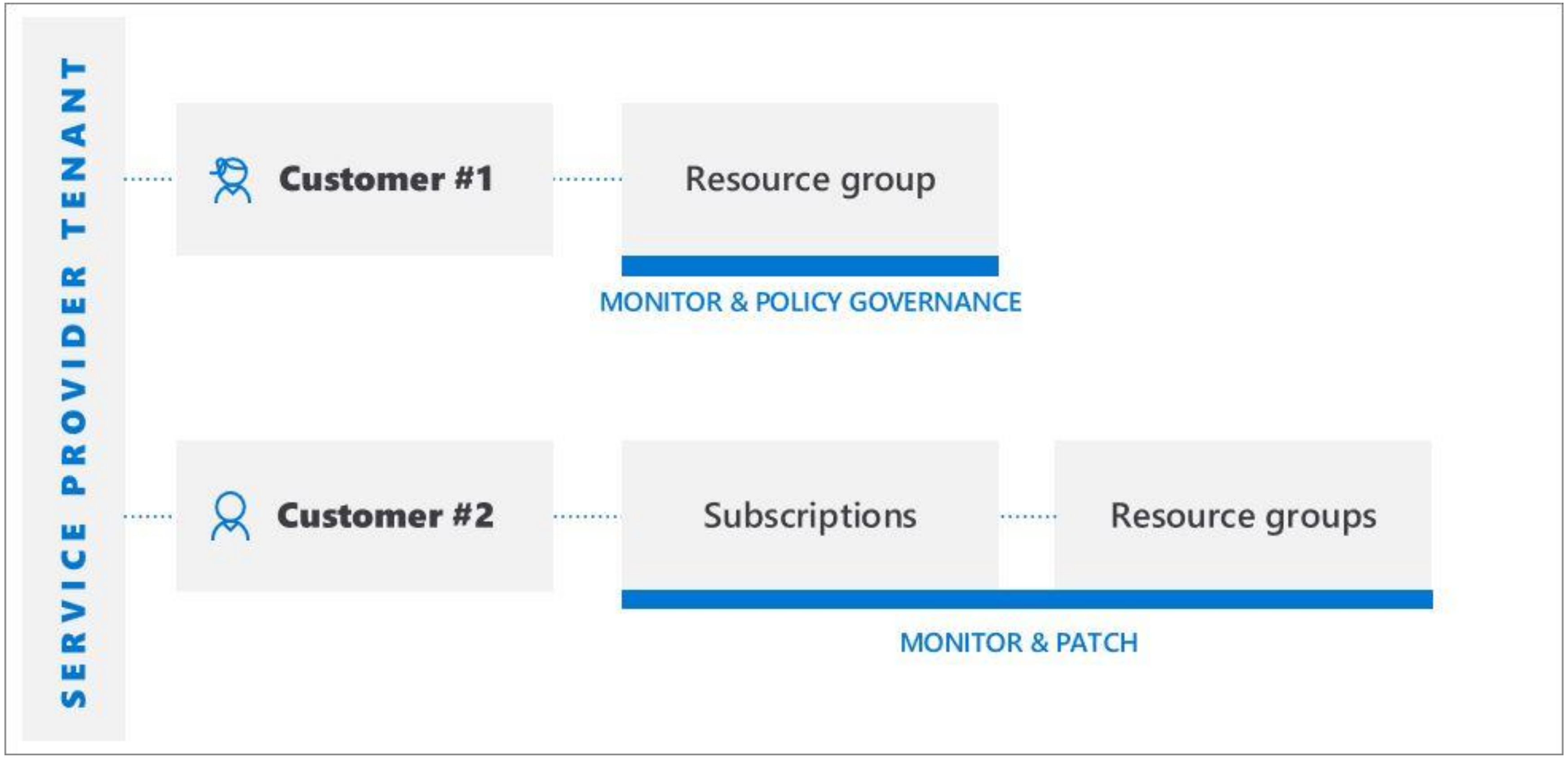
2 Single-Tenant with regional Microsoft Sentinel Workspaces

3 Multi-Tenant



Manage workspaces across tenants using Azure Lighthouse

If you must manage a Microsoft Sentinel workspace not in your tenant, implementing Azure Lighthouse will provide the option to enable your access to the tenant. Once Azure Lighthouse is onboarded, use the directory + subscription selector on the Azure portal to select all the subscriptions containing workspaces you manage.



Create a Microsoft Sentinel workspace

1

Microsoft Sentinel installation prerequisites

Have the required permissions for the Azure Subscription.

2

Create and configure a Log Analytics Workspace

Plan for the Region selection.

3

Add Microsoft Sentinel to the workspace

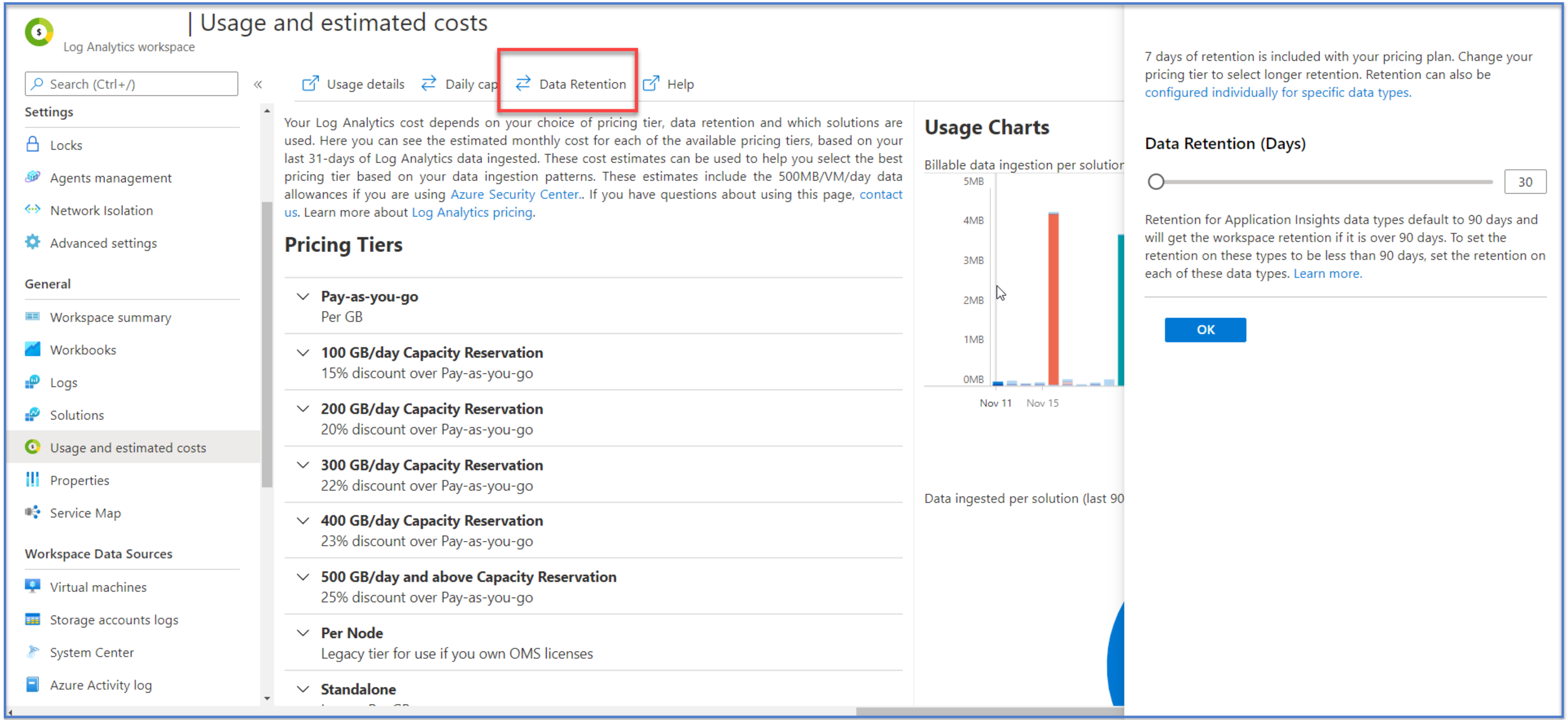
Select the newly created Log Analytics Workspace.

Microsoft Sentinel permissions and roles

- Microsoft Sentinel-specific roles
- Azure roles and Azure Monitor Log Analytics roles
- Microsoft Sentinel roles and allowed actions
- Custom roles and advanced Azure RBAC

Manage Microsoft Sentinel settings

As configurações de ambiente do Microsoft Sentinel são gerenciadas em duas áreas. No Microsoft Sentinel e no espaço de trabalho do Log Analytics onde o Microsoft Sentinel reside. Para configurar a Retenção de Logs:



| Usage and estimated costs

Your Log Analytics cost depends on your choice of pricing tier, data retention and which solutions are used. Here you can see the estimated monthly cost for each of the available pricing tiers, based on your last 31-days of Log Analytics data ingested. These cost estimates can be used to help you select the best pricing tier based on your data ingestion patterns. These estimates include the 500MB/VM/day data allowances if you are using Azure Security Center.. If you have questions about using this page, contact us. Learn more about Log Analytics pricing.

Pricing Tiers

- Pay-as-you-go
  Per GB
- 100 GB/day Capacity Reservation
  15% discount over Pay-as-you-go
- 200 GB/day Capacity Reservation
  20% discount over Pay-as-you-go
- 300 GB/day Capacity Reservation
  22% discount over Pay-as-you-go
- 400 GB/day Capacity Reservation
  23% discount over Pay-as-you-go
- 500 GB/day and above Capacity Reservation
  25% discount over Pay-as-you-go
- Per Node
  Legacy tier for use if you own OMS licenses
- Standalone

7 days of retention is included with your pricing plan. Change your pricing tier to select longer retention. Retention can also be configured individually for specific data types.

Data Retention (Days)

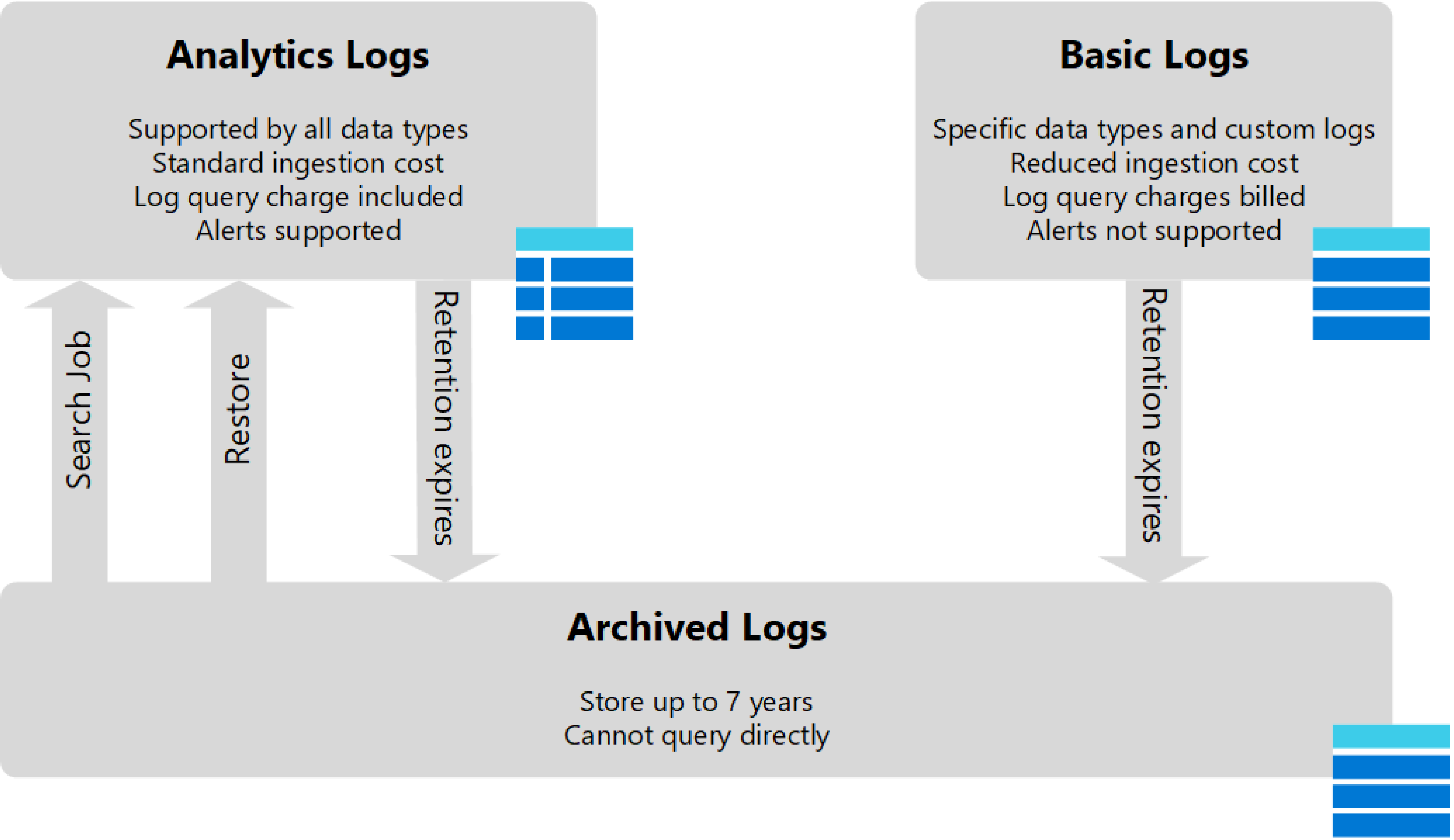
30

Retention for Application Insights data types default to 90 days and will get the workspace retention if it is over 90 days. To set the retention on these types to be less than 90 days, set the retention on each of these data types. Learn more.

Configure Logs

There are three primary log types in Microsoft Sentinel:

- Analytics Logs
- Basic Logs
- Archive Logs



Analytics Logs

Supported by all data types
Standard ingestion cost
Log query charge included
Alerts supported

Basic Logs

Specific data types and custom logs
Reduced ingestion cost
Log query charges billed
Alerts not supported

Archived Logs

Store up to 7 years
Cannot query directly

Query logs in Microsoft Sentinel

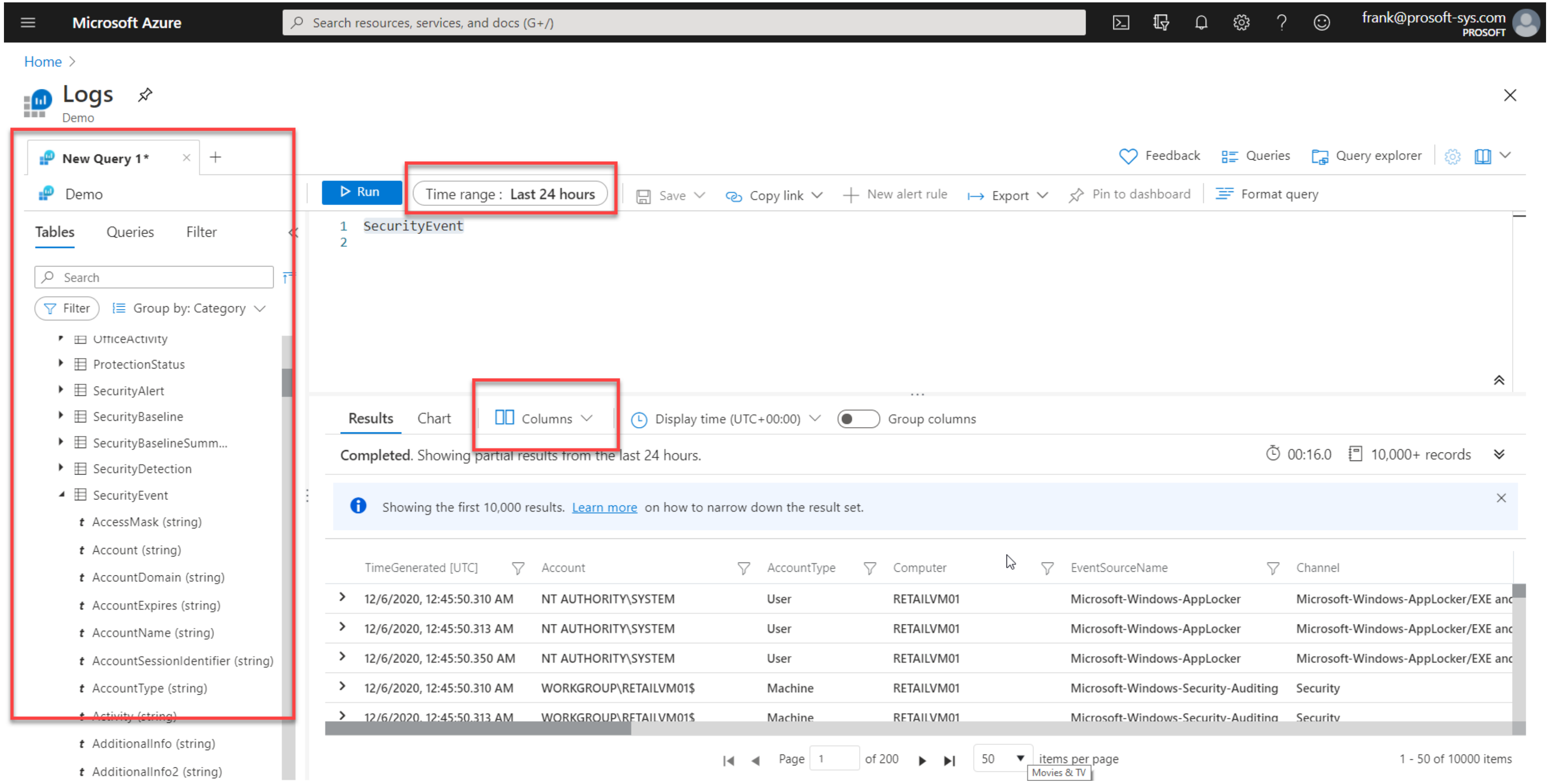
Introduction

After completing this module, you will be able to:

- Use the Logs page to view data tables in Microsoft Sentinel
- Query the most used tables using Microsoft Sentinel

Query logs in the logs page

A janela de consulta permite que você execute consultas, salve consultas, execute consultas salvas, crie uma nova regra de alerta e exporte.



```
SecurityEvent
```

Completed. Showing partial results from the last 24 hours.

Showing the first 10,000 results. Learn more on how to narrow down the result set.

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel
12/6/2020, 12:45:50.310 AM	NT AUTHORITY\SYSTEM	User	RETAILVM01	Microsoft-Windows-AppLocker	Microsoft-Windows-AppLocker/EXE and
12/6/2020, 12:45:50.313 AM	NT AUTHORITY\SYSTEM	User	RETAILVM01	Microsoft-Windows-AppLocker	Microsoft-Windows-AppLocker/EXE and
12/6/2020, 12:45:50.350 AM	NT AUTHORITY\SYSTEM	User	RETAILVM01	Microsoft-Windows-AppLocker	Microsoft-Windows-AppLocker/EXE and
12/6/2020, 12:45:50.310 AM	WORKGROUP\RETAILVM01$	Machine	RETAILVM01	Microsoft-Windows-Security-Auditing	Security
12/6/2020, 12:45:50.313 AM	WORKGROUP\RETAILVM01$	Machine	RETAILVM01	Microsoft-Windows-Security-Auditing	Security

Understand Microsoft Sentinel tables

Table:	Description
SecurityAlert	Contains Alerts Generated from Sentinel Analytical Rules. Also, it could include Alerts created directly from a Sentinel Data Connector
SecurityIncident	Alerts can generate Incidents. Incidents are related to Alert(s).
ThreatIntelligenceIndictor	Contains user-created or data connector ingested Indicators such as File Hashes, IP Addresses, Domains.
Watchlist	A Microsoft Sentinel watchlist contains imported data.

Understand common tables

Table:	Description
AzureActivity	Entries from the Azure Activity log
AzureDiagnostics	Stores resource logs for services that use Azure Diagnostics mode.
AuditLogs	Audit log for Azure Active Directory.
CommonSecurityLog	Syslog messages using the Common Event Format (CEF).
OfficeActivity	Audit logs for Office 365 tenants (Exchange, SharePoint and Teams).
SecurityEvent	Security events collected from windows devices.
SigninLogs	Azure Activity Directory Sign in logs.
Syslog	Syslog events on Linux computers using the Log Analytics agent.
Event	Sysmon Events collected from a Windows host.
WindowsFirewall	Windows Firewall Events

Understand Microsoft 365 Defender tables (examples)

Table:	Description
CloudAppEvents	Events in cloud apps and Microsoft Defender for Cloud Apps.
DeviceEvents	Device events table contains information about various event types.
DeviceFileEvents	File creation, modification, and other file system events.
DeviceInfo	Including their OS version, active users, and computer name.
DeviceLogonEvents	User logons and other authentication events.
DeviceNetworkEvents	Network connections and related events.
DeviceProcessEvents	Process creation and related events.
DeviceRegistryEvents	Creation and modification of registry entries.
DeviceTvm*	Microsoft Defender Vulnerability Management Security & Software information.
EmailEvents	Microsoft 365 email events, including email delivery and blocking events
IdentityInfo	Account information from various sources, including Azure Active Directory

Use watchlists in Microsoft Sentinel

Introduction

After completing this module, you will be able to:

- Create a watchlist in Microsoft Sentinel
- Use KQL to access the watchlist in Microsoft Sentinel
- Update a watchlist in Microsoft Sentinel

Plan for Microsoft Sentinel watchlists

1 Investigar ameaças e responder a incidentes rapidamente com a rápida importação de endereços IP, hashes de arquivos e outros dados de arquivos CSV. Depois de importado, você pode usar pares nome-valor da lista de observação para associações e filtros em regras de alerta, caça a ameaças, pastas de trabalho, blocos de anotações e consultas gerais.

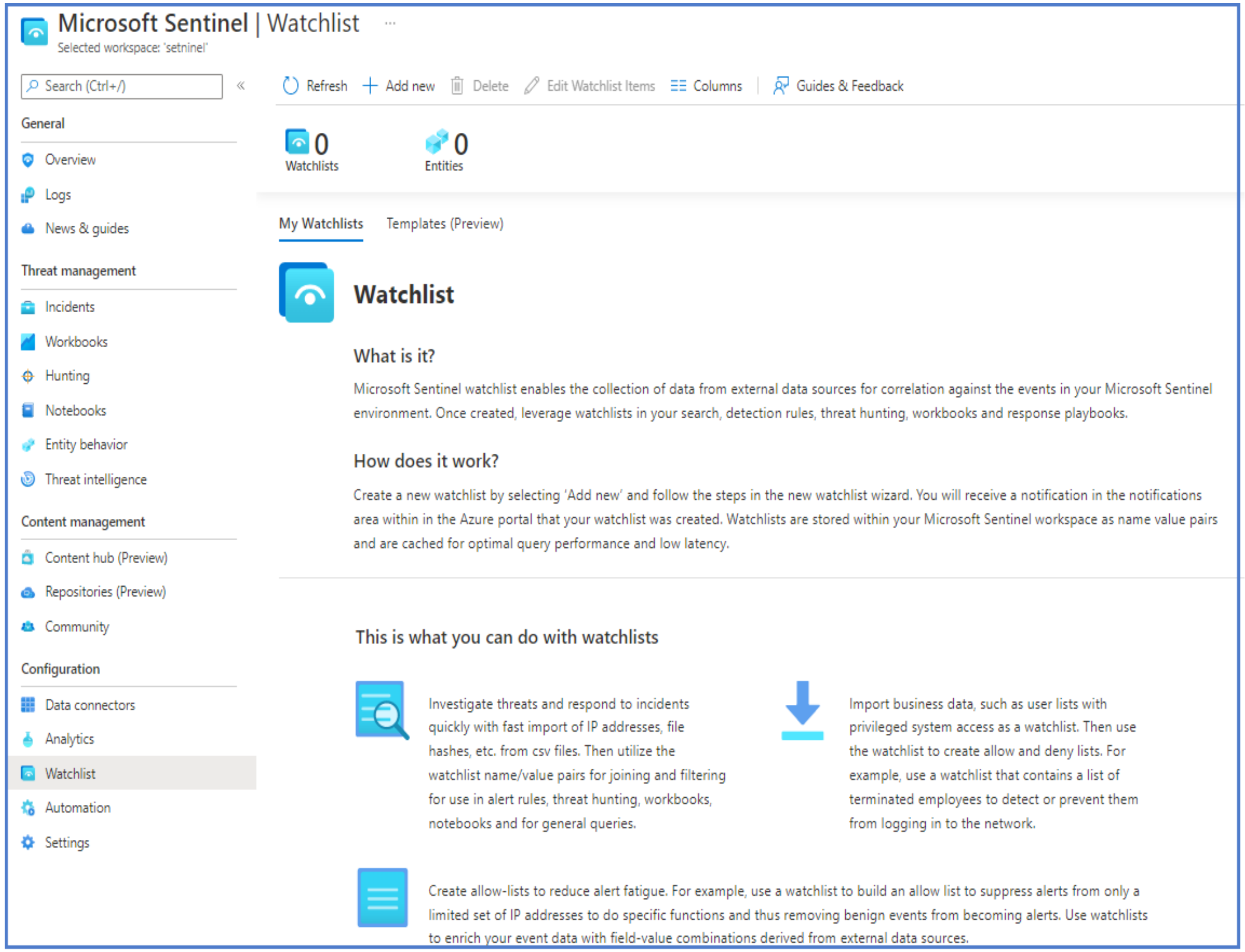
2 Importando dados corporativos como uma lista de observação. Por exemplo, importe listas de usuários com acesso privilegiado ao sistema ou funcionários encerrados e use a lista de observação para criar listas de permissão e negação usadas para detectar ou impedir que esses usuários façam logon na rede.

3 Reduzir a fadiga de alerta. Crie listas de permissões para suprimir alertas de um grupo de usuários, como usuários de endereços IP autorizados que executam tarefas que normalmente acionariam o alerta e impedem que eventos benignos se tornem alertas.

4 Enriquecendo os dados do evento. Use listas de observação para enriquecer os dados do evento com combinações nome-valor derivadas de fontes de dados externas.

Create a watchlist

KQL:_GetWatchlist('HighValueMachines')



Watchlist

What is it?

Microsoft Sentinel watchlist enables the collection of data from external data sources for correlation against the events in your Microsoft Sentinel environment. Once created, leverage watchlists in your search, detection rules, threat hunting, workbooks and response playbooks.

How does it work?

Create a new watchlist by selecting 'Add new' and follow the steps in the new watchlist wizard. You will receive a notification in the notifications area within in the Azure portal that your watchlist was created. Watchlists are stored within your Microsoft Sentinel workspace as name value pairs and are cached for optimal query performance and low latency.

This is what you can do with watchlists

Investigate threats and respond to incidents quickly with fast import of IP addresses, file hashes, etc. from csv files. Then utilize the watchlist name/value pairs for joining and filtering for use in alert rules, threat hunting, workbooks, notebooks and for general queries.

Import business data, such as user lists with privileged system access as a watchlist. Then use the watchlist to create allow and deny lists. For example, use a watchlist that contains a list of terminated employees to detect or prevent them from logging in to the network.

Create allow-lists to reduce alert fatigue. For example, use a watchlist to build an allow list to suppress alerts from only a limited set of IP addresses to do specific functions and thus removing benign events from becoming alerts. Use watchlists to enrich your event data with field-value combinations derived from external data sources.

Manage Watchlists

Update individual items

Bulk update items

Utilize threat intelligence in Microsoft Sentinel

Introduction

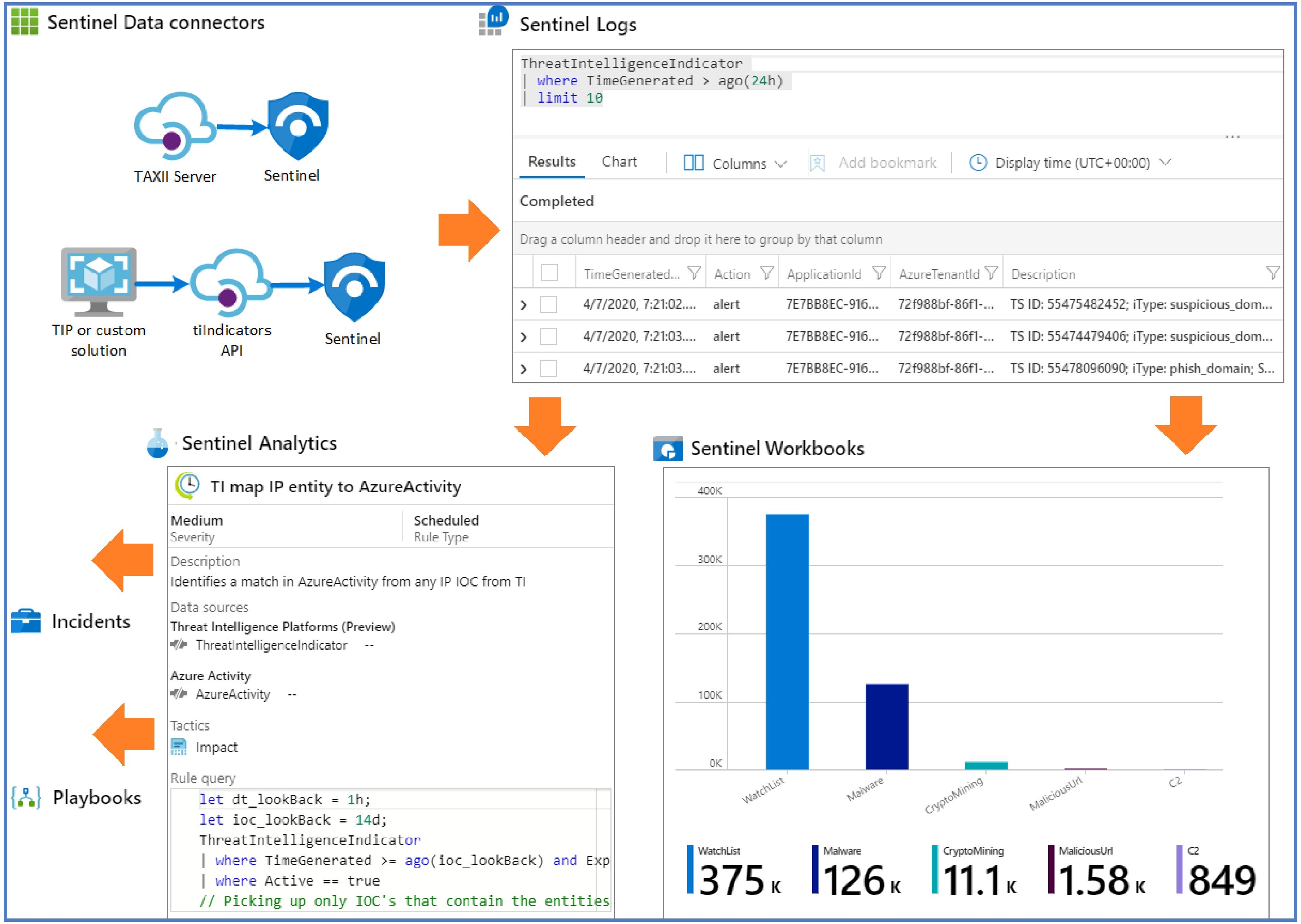
After completing this module, you will be able to:

- Manage threat indicators in Microsoft Sentinel

- Use KQL to access threat indicators in Microsoft Sentinel

Define threat intelligence

Os indicadores de ameaça são dados que associam observações como URLs, hashes de arquivos ou endereços IP a atividades de ameaças conhecidas, como phishing, botnets ou malware.



```
ThreatIntelligenceIndicator
| where TimeGenerated > ago(24h)
| limit 10
```

Completed

Drag a column header and drop it here to group by that column

TimeGenerated...	Action	ApplicationId	AzureTenantId	Description
4/7/2020, 7:21:02....	alert	7E7BB8EC-916...	72f988bf-86f1-...	TS ID: 55475482452; iType: suspicious_dom...
4/7/2020, 7:21:03....	alert	7E7BB8EC-916...	72f988bf-86f1-...	TS ID: 55474479406; iType: suspicious_dom...
4/7/2020, 7:21:03....	alert	7E7BB8EC-916...	72f988bf-86f1-...	TS ID: 55478096090; iType: phish_domain; S...

TI map IP entity to AzureActivity

Medium
Severity

Scheduled
Rule Type

Description
Identifies a match in AzureActivity from any IP IOC from TI

Data sources
Threat Intelligence Platforms (Preview)
ThreatIntelligenceIndicator --

Azure Activity
AzureActivity --

Tactics
Impact

Rule query

```
let dt_lookBack = 1h;
let ioc_lookBack = 14d;
ThreatIntelligenceIndicator
| where TimeGenerated >= ago(ioc_lookBack) and Exp
| where Active == true
// Picking up only IOC's that contain the entities
```

Manage your threat indicators

In the Threat intelligence area, you can view, sort, filter, and search your imported threat indicators without even writing a Logs KQL query. This area also allows you to create threat indicators directly within the Microsoft Sentinel interface and perform everyday threat intelligence administrative tasks like indicator tagging and creating new indicators related to security investigations.

```
The indicators can be accessed in KQL by querying the ThreatIntelligenceIndicator
table.

//KQL
ThreatIntelligenceIndicator
```

Knowledge check

Check your knowledge
with the module quiz
in your course viewer

Microsoft Security