Azure Security Updates Microsoft Ignite 2021

Maxime Coquerel - MVP Azure

Microsoft® MVP Most Valuable Professional

# Speaker

Maxime Coquerel

Director Cloud Security Architecture

Email : max.coquerel@live.fr

Blog : zigmax.net (since 2012)

Github : https://github.com/zigmax

Twitter : @zig_max

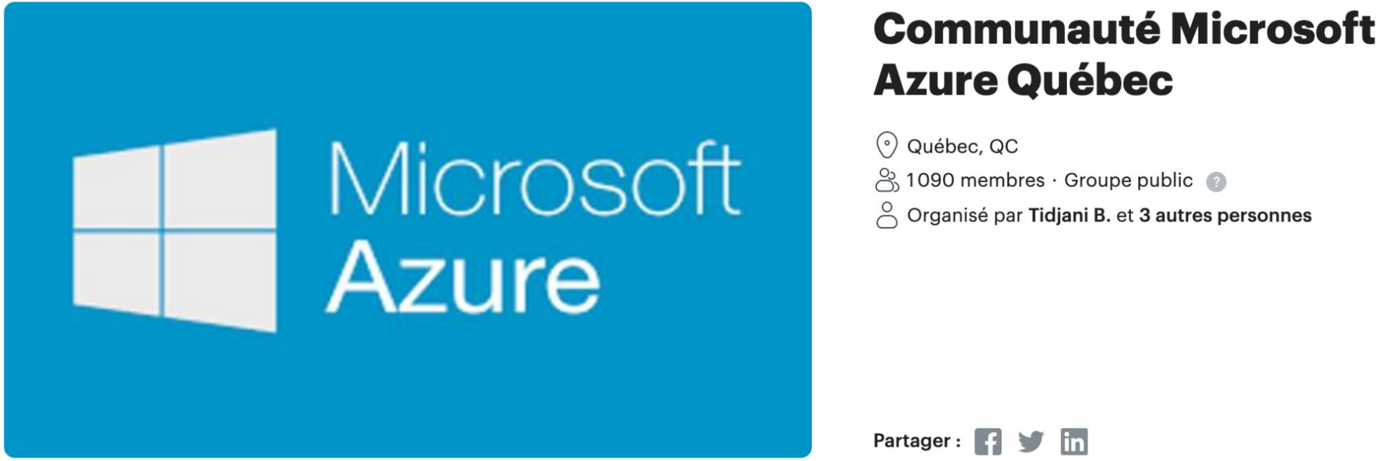
Open Source Contributor (Kubernetes / VSCode)

Microsoft® MVP Most Valuable Professional

Disclaimer

“Any views or opinions expressed in this presentation are those of the presenter and not necessarily represent the view and opinions of my employer, its ownership, management or its employees .“

Thank you!



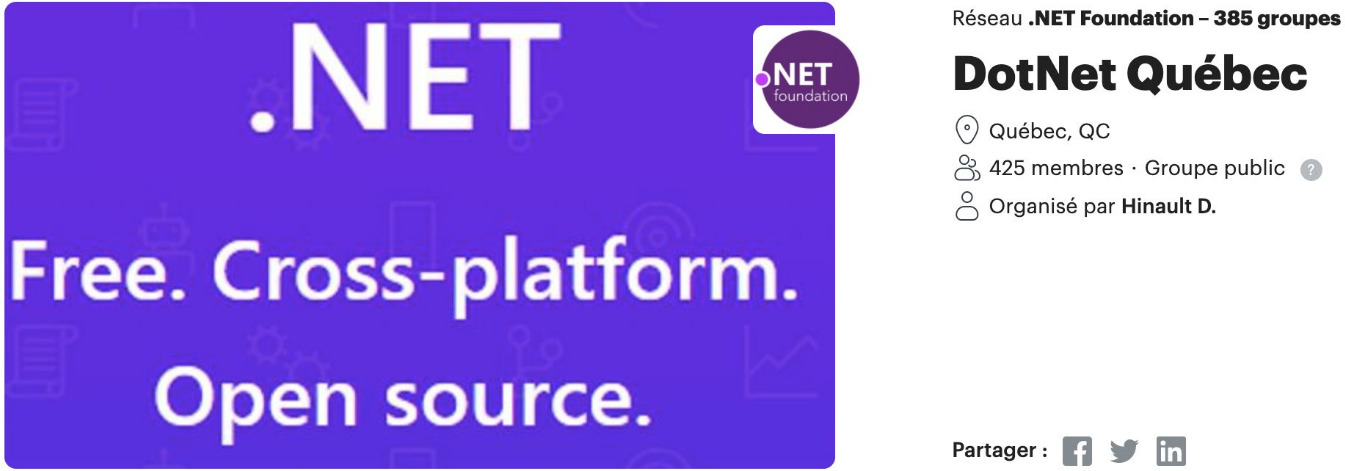
Communauté Microsoft Azure Québec

Québec, QC

1090 membres · Groupe public ?

Organisé par **Tidjani B.** et **3 autres personnes**

Partager :



Réseau **.NET Foundation – 385 groupes**

DotNet Québec

Québec, QC

425 membres · Groupe public ?

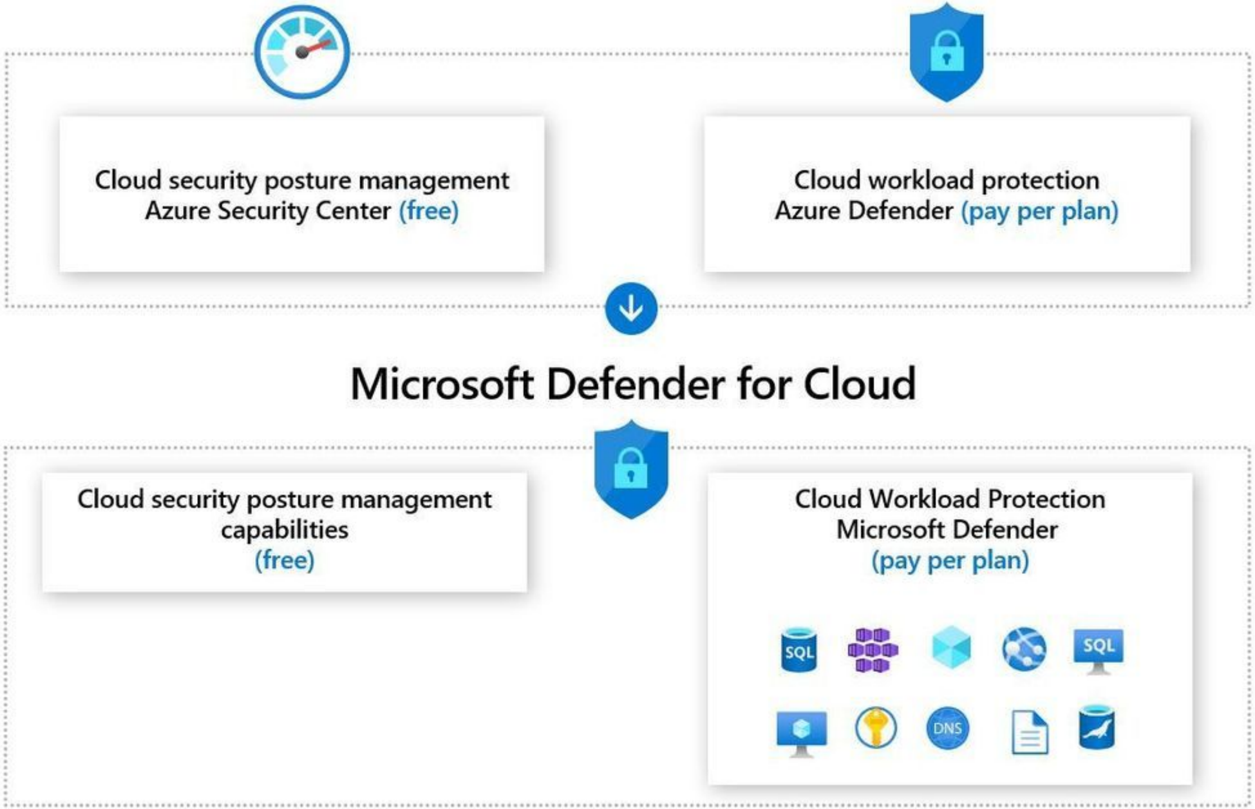
Organisé par **Hinault D.**

Partager :

Session Agenda / Goal

- **Microsoft Defender for Cloud**
- **Identity sensitive data in cloud resources**
- **New approach to multi cloud scenarios (AWS)**
- **Security recommendations now map to the MITRE Attack Framework**
- **Microsoft Defender for Server**
- **Azure Security Benchmark v3**

A new name! - Microsoft Defender for Cloud



Cloud security posture management
Azure Security Center (free)

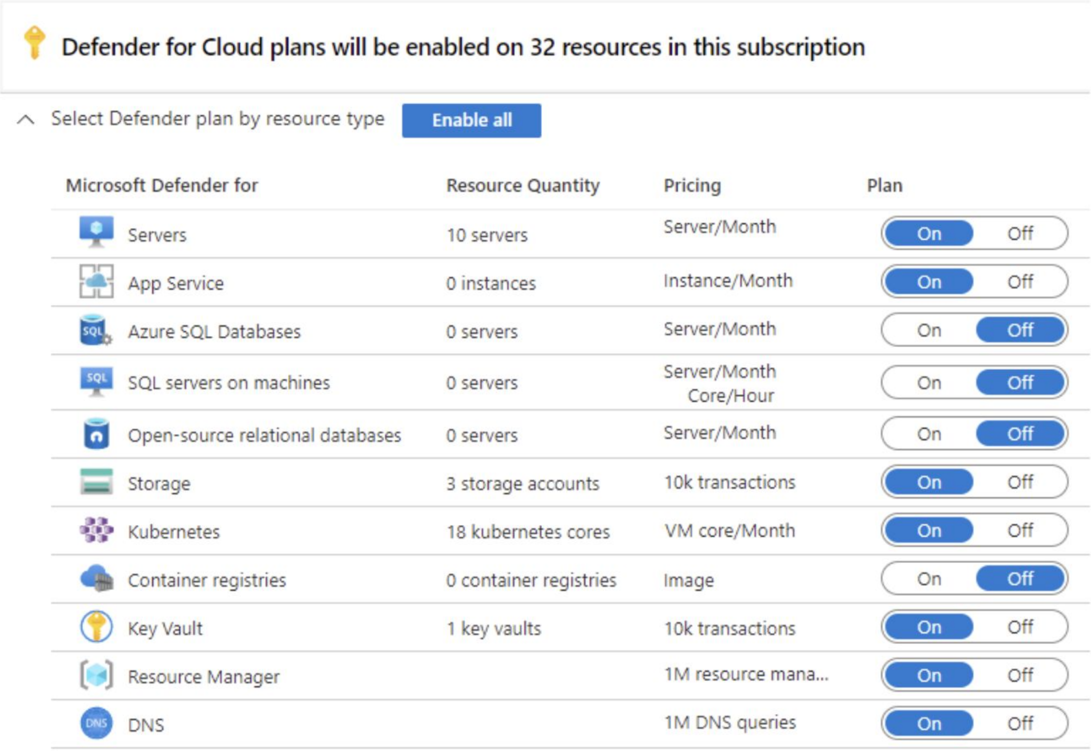
Cloud workload protection
Azure Defender (pay per plan)

Microsoft Defender for Cloud

Cloud security posture management capabilities
(free)

Cloud Workload Protection
Microsoft Defender
(pay per plan)

Overview of the enhanced security plans in Defender for Cloud



Defender for Cloud plans will be enabled on 32 resources in this subscription

Select Defender plan by resource type

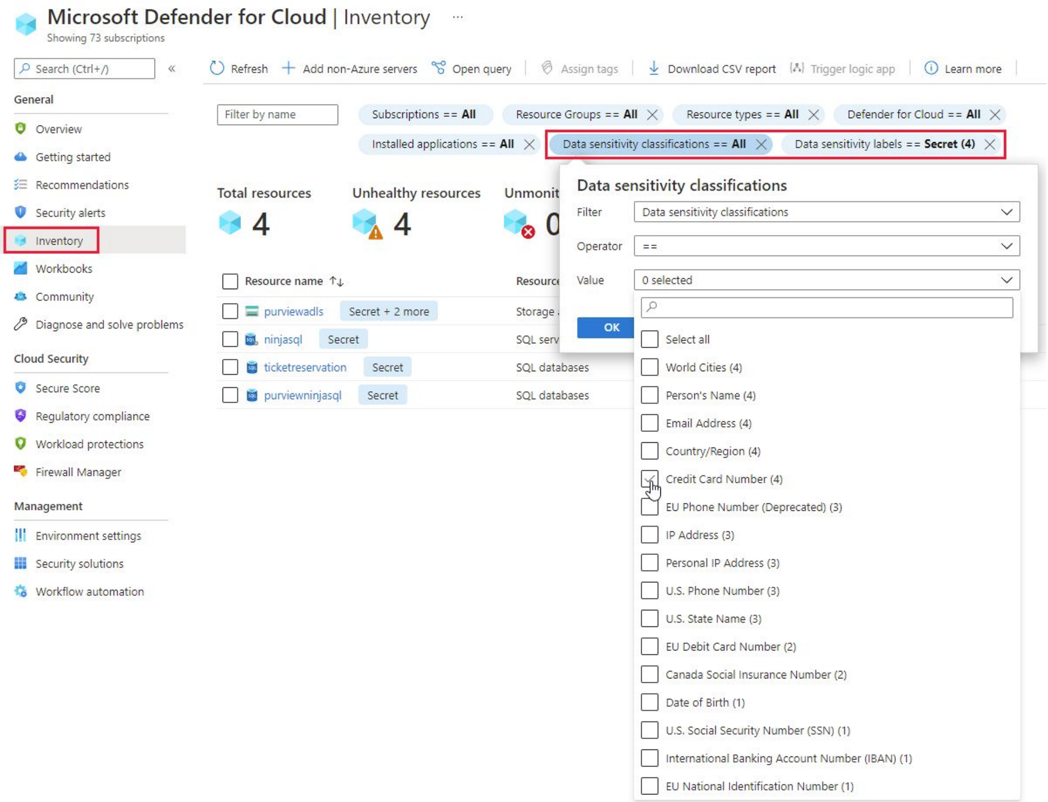
Microsoft Defender for	Resource Quantity	Pricing	Plan
Servers	10 servers	Server/Month	[✓ On] Off
App Service	0 instances	Instance/Month	[✓ On] Off
Azure SQL Databases	0 servers	Server/Month	On [✓ Off]
SQL servers on machines	0 servers	Server/Month Core/Hour	On [✓ Off]
Open-source relational databases	0 servers	Server/Month	On [✓ Off]
Storage	3 storage accounts	10k transactions	[✓ On] Off
Kubernetes	18 kubernetes cores	VM core/Month	[✓ On] Off
Container registries	0 container registries	Image	On [✓ Off]
Key Vault	1 key vaults	10k transactions	[✓ On] Off
Resource Manager		1M resource mana...	[✓ On] Off
DNS		1M DNS queries	[✓ On] Off

Identify sensitive data in cloud resources

- Integrated with Azure Purview

With automated data discovery, sensitive data classification, and end-to-end data lineage, Purviev helps organizations manage and govern data in hybrid and multi-cloud environments.

- New filters called Data sensitivity classification and Data sensitivity label



Subscriptions == **All** | Resource Groups == **All** | Resource types == **All** | Defender for Cloud == **All** | Installed applications == **All** | Data sensitivity classifications == **All** | Data sensitivity labels == **Secret (4)**

□ Resource name ↑↓		Resource
□ purviewadls	Secret + 2 more	Storage
□ ninjasql	Secret	SQL serv
□ ticketreservation	Secret	SQL databases
□ purviewninjasql	Secret	SQL databases

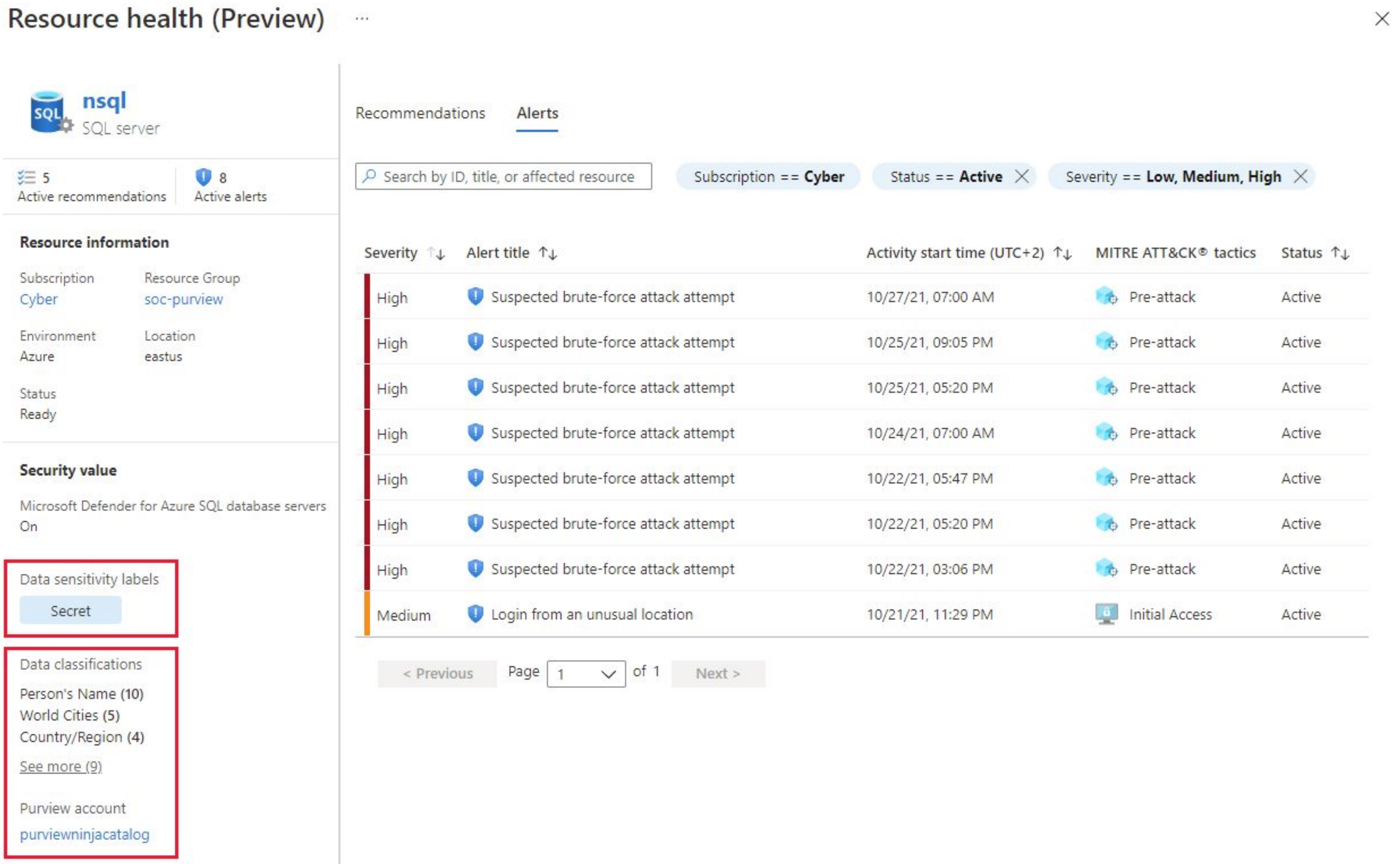
Data sensitivity classifications

Filter: Data sensitivity classifications

Operator: ==

Value: 0 selected

□ Select all
□ World Cities (4)
□ Person's Name (4)
□ Email Address (4)
□ Country/Region (4)
☑ Credit Card Number (4)
□ EU Phone Number (Deprecated) (3)
□ IP Address (3)
□ Personal IP Address (3)
□ U.S. Phone Number (3)
□ U.S. State Name (3)
□ EU Debit Card Number (2)
□ Canada Social Insurance Number (2)
□ Date of Birth (1)
□ U.S. Social Security Number (SSN) (1)
□ International Banking Account Number (IBAN) (1)
□ EU National Identification Number (1)



Resource health (Preview)

nsql
SQL server

5
Active recommendations

8
Active alerts

Resource information

Subscription
Cyber

Resource Group
soc-purview

Environment
Azure

Location
eastus

Status
Ready

Security value

Microsoft Defender for Azure SQL database servers
On

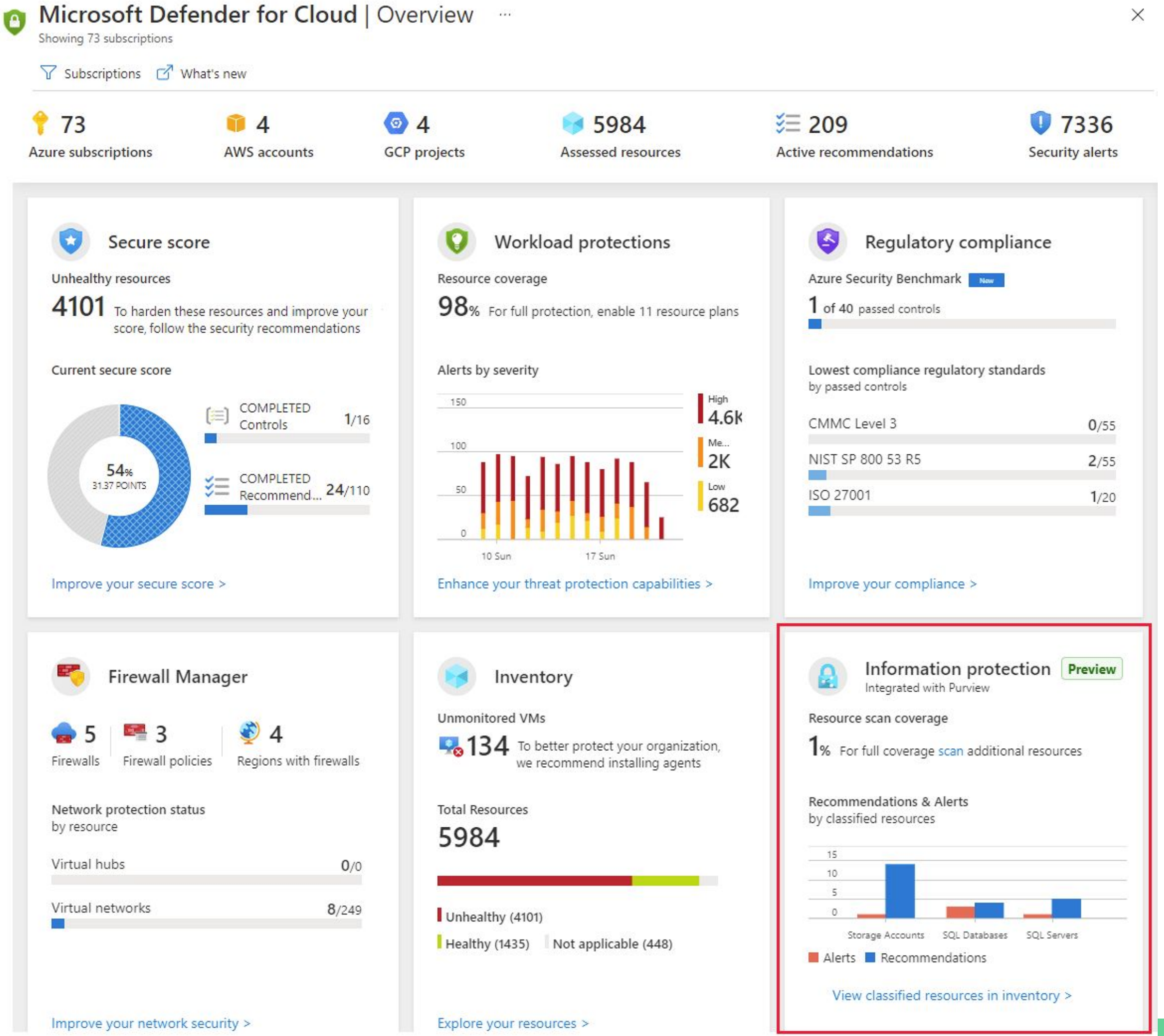
Data sensitivity labels
Secret

Data classifications
Person's Name (10)
World Cities (5)
Country/Region (4)
See more (9)

Purview account
purviewninjacatalog

Subscription == **Cyber**   Status == **Active**   Severity == **Low, Medium, High**

Severity	Alert title	Activity start time (UTC+2)	MITRE ATT&CK® tactics	Status
High	Suspected brute-force attack attempt	10/27/21, 07:00 AM	Pre-attack	Active
High	Suspected brute-force attack attempt	10/25/21, 09:05 PM	Pre-attack	Active
High	Suspected brute-force attack attempt	10/25/21, 05:20 PM	Pre-attack	Active
High	Suspected brute-force attack attempt	10/24/21, 07:00 AM	Pre-attack	Active
High	Suspected brute-force attack attempt	10/22/21, 05:47 PM	Pre-attack	Active
High	Suspected brute-force attack attempt	10/22/21, 05:20 PM	Pre-attack	Active
High	Suspected brute-force attack attempt	10/22/21, 03:06 PM	Pre-attack	Active
Medium	Login from an unusual location	10/21/21, 11:29 PM	Initial Access	Active



Microsoft Defender for Cloud | Overview

Showing 73 subscriptions

Subscriptions | What's new

73	4	4	5984	209	7336
Azure subscriptions	AWS accounts	GCP projects	Assessed resources	Active recommendations	Security alerts

Secure score

Unhealthy resources

4101 To harden these resources and improve your score, follow the security recommendations

Current secure score

54% 31.37 POINTS

COMPLETED Controls 1/16

COMPLETED Recommend... 24/110

Improve your secure score >

Workload protections

Resource coverage

98% For full protection, enable 11 resource plans

Alerts by severity

High 4.6K

Me... 2K

Low 682

Enhance your threat protection capabilities >

Regulatory compliance

Azure Security Benchmark New

1 of 40 passed controls

Lowest compliance regulatory standards
by passed controls

CMMC Level 3	0/55
NIST SP 800 53 R5	2/55
ISO 27001	1/20

Improve your compliance >

Firewall Manager

5	3	4
Firewalls	Firewall policies	Regions with firewalls

Network protection status
by resource

Virtual hubs	0/0
Virtual networks	8/249

Improve your network security >

Inventory

Unmonitored VMs

134 To better protect your organization, we recommend installing agents

Total Resources

5984

Unhealthy (4101)

Healthy (1435) Not applicable (448)

Explore your resources >

Information protection Preview

Integrated with Purview

Resource scan coverage

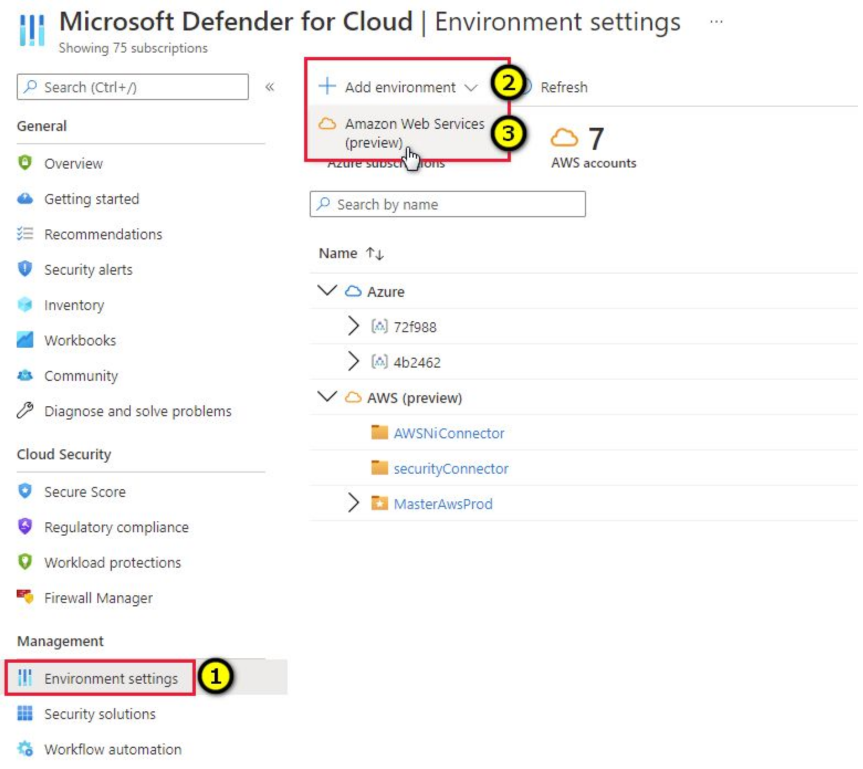
1% For full coverage scan additional resources

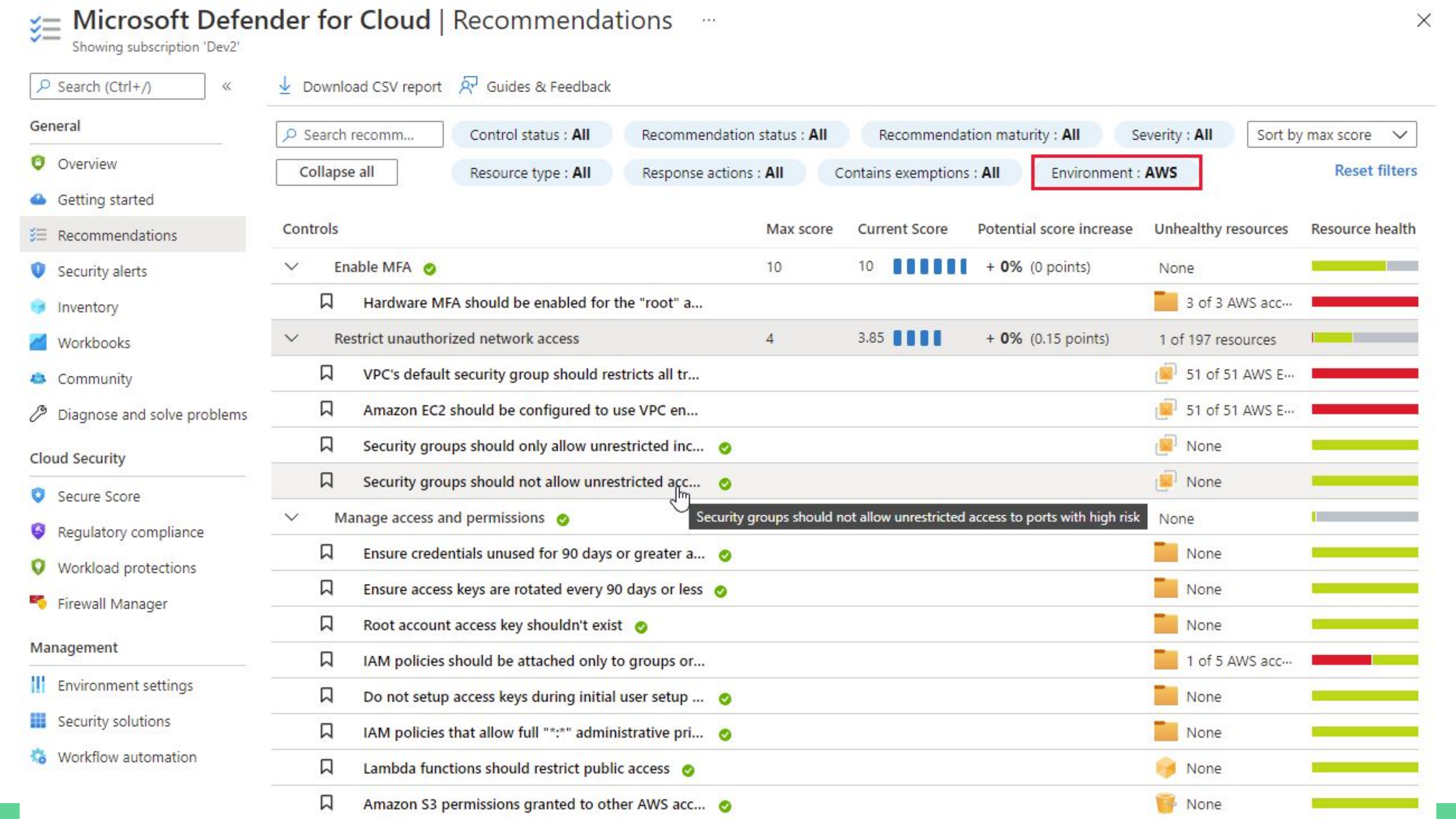
Recommendations & Alerts
by classified resources

View classified resources in inventory >

New approach to multi-cloud scenarios

- Seamless onboarding using AWS API
- 160+ out of the box recommendations, CIS, PCI & AWS Foundational Security Best Practices support, multi-cloud view in Secure Score
- EKS support, easier onboarding for workloads





Microsoft Defender for Cloud | Recommendations

Showing subscription 'Dev2'

Search (Ctrl+/)

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Secure Score
- Regulatory compliance
- Workload protections
- Firewall Manager

Management

- Environment settings
- Security solutions
- Workflow automation

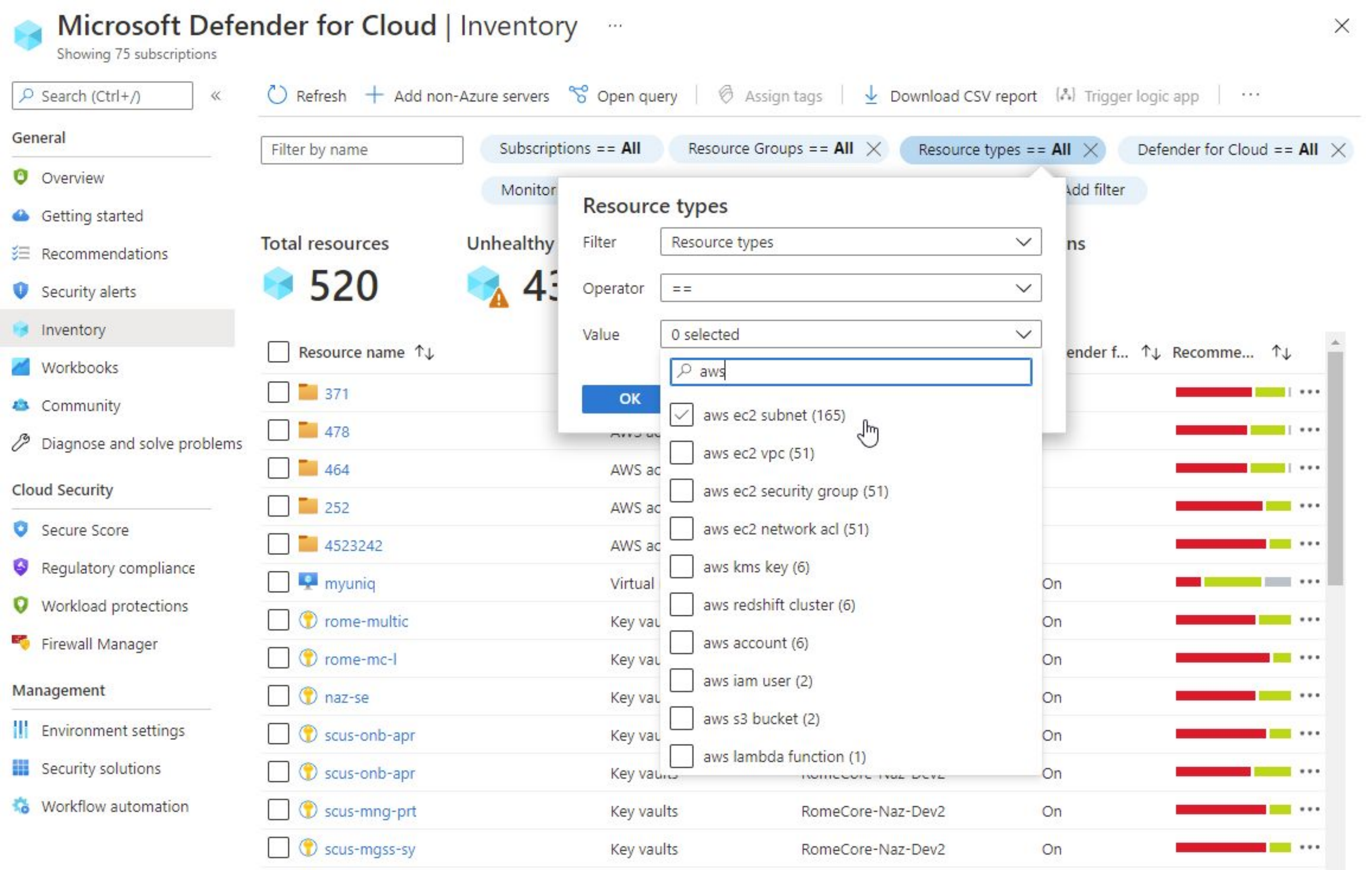
Control status : **All** | Recommendation status : **All** | Recommendation maturity : **All** | Severity : **All** | Sort by max score

Resource type : **All** | Response actions : **All** | Contains exemptions : **All** | Environment : **AWS**

Controls	Max score	Current Score	Potential score increase	Unhealthy resources
Enable MFA ✓	10	10	+ 0% (0 points)	None
Hardware MFA should be enabled for the "root" a...				3 of 3 AWS acc...
Restrict unauthorized network access	4	3.85	+ 0% (0.15 points)	1 of 197 resources
VPC's default security group should restricts all tr...				51 of 51 AWS E...
Amazon EC2 should be configured to use VPC en...				51 of 51 AWS E...
Security groups should only allow unrestricted inc... ✓				None
Security groups should not allow unrestricted acc... ✓				None
Manage access and permissions ✓				None
Ensure credentials unused for 90 days or greater a... ✓				None
Ensure access keys are rotated every 90 days or less ✓				None
Root account access key shouldn't exist ✓				None
IAM policies should be attached only to groups or...				1 of 5 AWS acc...
Do not setup access keys during initial user setup ... ✓				None
IAM policies that allow full "*:*" administrative pri... ✓				None
Lambda functions should restrict public access ✓				None
Amazon S3 permissions granted to other AWS acc... ✓				None

Resource health

Security groups should not allow unrestricted access to ports with high risk



Microsoft Defender for Cloud | Inventory

Showing 75 subscriptions

Subscriptions == **All**

Resource Groups == **All**

Resource types == **All**

Defender for Cloud == **All**

Total resources 520

Unhealthy 43

Resource types

Filter: Resource types

Operator: ==

Value: 0 selected

aws

☑ aws ec2 subnet (165)

☐ aws ec2 vpc (51)

☐ aws ec2 security group (51)

☐ aws ec2 network acl (51)

☐ aws kms key (6)

☐ aws redshift cluster (6)

☐ aws account (6)

☐ aws iam user (2)

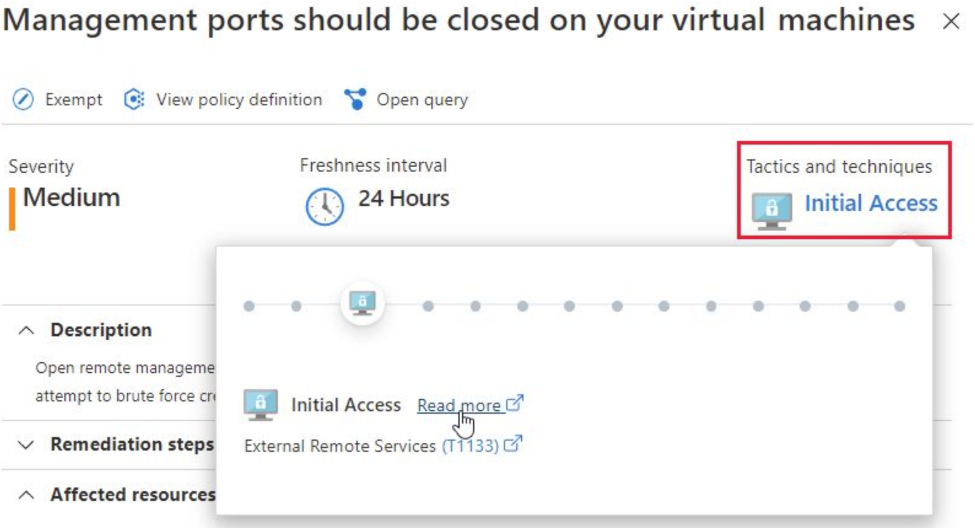
☐ aws s3 bucket (2)

☐ aws lambda function (1)

Resource name			ender f...	Recomme...
371				
478				
464	AWS ac			
252	AWS ac			
4523242	AWS ac			
myuniq	Virtual		On	
rome-multic	Key vau		On	
rome-mc-l	Key vau		On	
naz-se	Key vau		On	
scus-onb-apr	Key vau		On	
scus-onb-apr	Key vaults		On	
scus-mng-prt	Key vaults	RomeCore-Naz-Dev2	On	
scus-mgss-sy	Key vaults	RomeCore-Naz-Dev2	On	

Security recommendations now map to the MITRE Att&ck Framework

- Use threat and vulnerability management to discover vulnerabilities and misconfigurations in near real time with the integration with Microsoft Defender for Endpoint
- No need for additional agents or periodic scans
- Threat and vulnerability management prioritizes vulnerabilities based on the threat landscape and detections in your organization
- Azure Resource Graph query results for relevant recommendations include the MITRE ATT&CK tactics and techniques.



Management ports should be closed on your virtual machines

Severity: Medium

Freshness interval: 24 Hours

Tactics and techniques: Initial Access

Description

Open remote manageme
attempt to brute force cr

Remediation steps

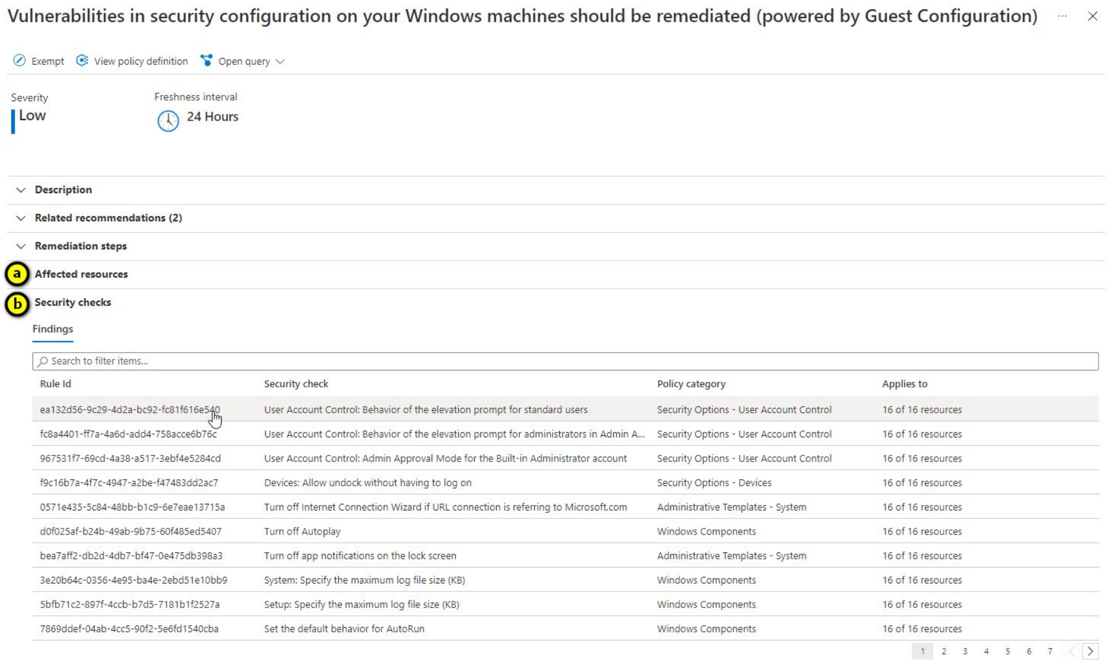
Affected resources

Initial Access Read more

External Remote Services (T1133)

Microsoft Defender for Server

- Integration with TVM is now GA
- Use threat and vulnerability management to discover vulnerabilities and misconfigurations in near real time with the integration with Microsoft Defender for Endpoint
- No need for additional agents or periodic scans
- Threat and vulnerability management prioritize vulnerabilities based on the threat landscape and detections in your organization



Vulnerabilities in security configuration on your Windows machines should be remediated (powered by Guest Configuration)

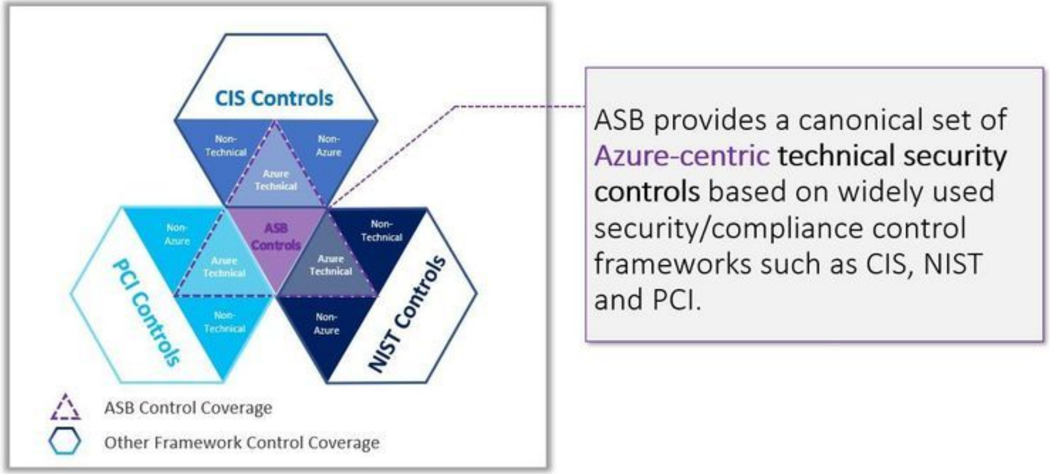
Severity: Low

Freshness interval: 24 Hours

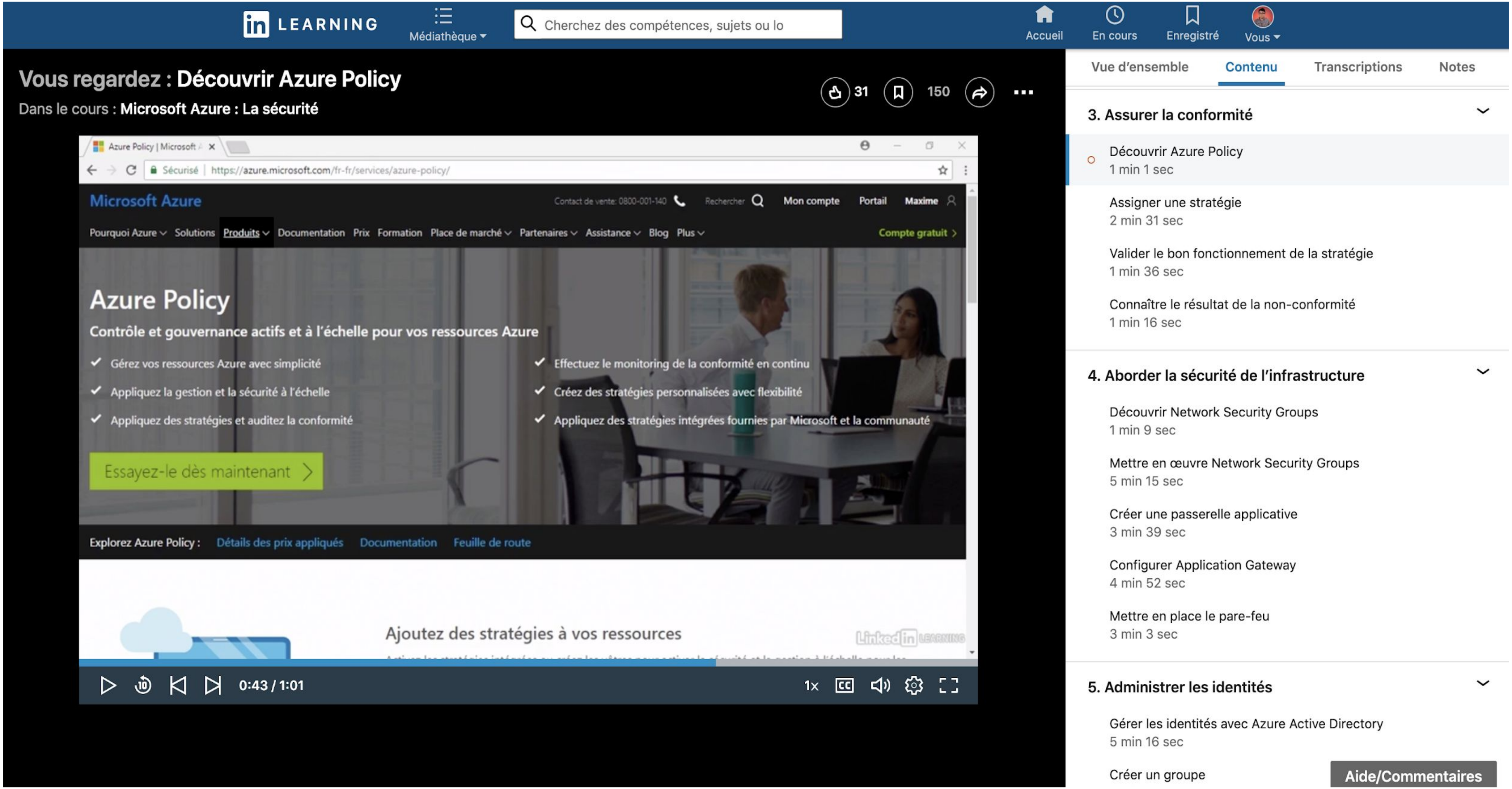
Rule Id	Security check	Policy category	Applies to
ea132d56-9c29-4d2a-bc92-fc81f616e540	User Account Control: Behavior of the elevation prompt for standard users	Security Options - User Account Control	16 of 16 resources
fc8a4401-ff7a-4a6d-add4-758acce6b76c	User Account Control: Behavior of the elevation prompt for administrators in Admin A...	Security Options - User Account Control	16 of 16 resources
967531f7-69cd-4a38-a517-3ebf4e5284cd	User Account Control: Admin Approval Mode for the Built-in Administrator account	Security Options - User Account Control	16 of 16 resources
f9c16b7a-4f7c-4947-a2be-f47483dd2ac7	Devices: Allow undock without having to log on	Security Options - Devices	16 of 16 resources
0571e435-5c84-48bb-b1c9-6e7eae13715a	Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Administrative Templates - System	16 of 16 resources
d0f025af-b24b-49ab-9b75-60f485ed5407	Turn off Autoplay	Windows Components	16 of 16 resources
bea7aff2-db2d-4db7-bf47-0e475db398a3	Turn off app notifications on the lock screen	Administrative Templates - System	16 of 16 resources
3e20b64c-0356-4e95-ba4e-2ebd51e10bb9	System: Specify the maximum log file size (KB)	Windows Components	16 of 16 resources
5bfb71c2-897f-4ccb-b7d5-7181b1f2527a	Setup: Specify the maximum log file size (KB)	Windows Components	16 of 16 resources
7869ddef-04ab-4cc5-90f2-5e6fd1540cba	Set the default behavior for AutoRun	Windows Components	16 of 16 resources

Azure Security Benchmark v3

- Additional control mappings for PCI-DSS v3.2.1
- Collaborated with Center for Internet Security (CIS) to map ASB v3 controls with CIS Controls v8
- New controls for DevOps Security and Key and Certificate management
- Restructured control guidance for more granular and actionable insights
- ASB v3 is the new default in the Regulatory Compliance Dashboard in Microsoft Defender for Cloud



ASB provides a canonical set of Azure-centric **technical security controls** based on widely used security/compliance control frameworks such as CIS, NIST and PCI.



Vous regardez : **Découvrir Azure Policy**

Dans le cours : **Microsoft Azure : La sécurité**

Azure Policy

Contrôle et gouvernance actifs et à l'échelle pour vos ressources Azure

- ✓ Gérez vos ressources Azure avec simplicité
- ✓ Appliquez la gestion et la sécurité à l'échelle
- ✓ Appliquez des stratégies et auditez la conformité
- ✓ Effectuez le monitoring de la conformité en continu
- ✓ Créez des stratégies personnalisées avec flexibilité
- ✓ Appliquez des stratégies intégrées fournies par Microsoft et la communauté

Explorez Azure Policy : Détails des prix appliqués Documentation Feuille de route

Ajoutez des stratégies à vos ressources

3. Assurer la conformité

- ○ Découvrir Azure Policy
  1 min 1 sec
- Assigner une stratégie
  2 min 31 sec
- Valider le bon fonctionnement de la stratégie
  1 min 36 sec
- Connaître le résultat de la non-conformité
  1 min 16 sec

4. Aborder la sécurité de l'infrastructure

- Découvrir Network Security Groups
  1 min 9 sec
- Mettre en œuvre Network Security Groups
  5 min 15 sec
- Créer une passerelle applicative
  3 min 39 sec
- Configurer Application Gateway
  4 min 52 sec
- Mettre en place le pare-feu
  3 min 3 sec

5. Administrer les identités

- Gérer les identités avec Azure Active Directory
  5 min 16 sec
- Créer un groupe

Source: https://www.linkedin.com/learning/microsoft-azure-la-securite/decouvrir-azure-policy

Technical Resources

Microsoft Ignite 2021 - https://myignite.microsoft.com/home

Microsoft Technical Community Content
https://github.com/Microsoft/TechnicalCommunityContent

Azure Security Blog - https://azure.microsoft.com/en-us/blog/topics/security/

Maxime Blog - http://zigmax.net

Channel Youtube - Communauté Azure Quebec
https://www.youtube.com/channel/UCYLAJgoYFLYf0d4jWXuC1cA

Questions / Talks