Azure Defender and more ...!

Maxime Coquerel - MVP Azure

MVP Microsoft® Most Valuable Professional

# Speaker

Maxime Coquerel

Director Cloud Security Architect

Email : max.coquerel@live.fr

Blog : zigmax.net (since 2012)

Github : https://github.com/zigmax

Twitter : @zig_max

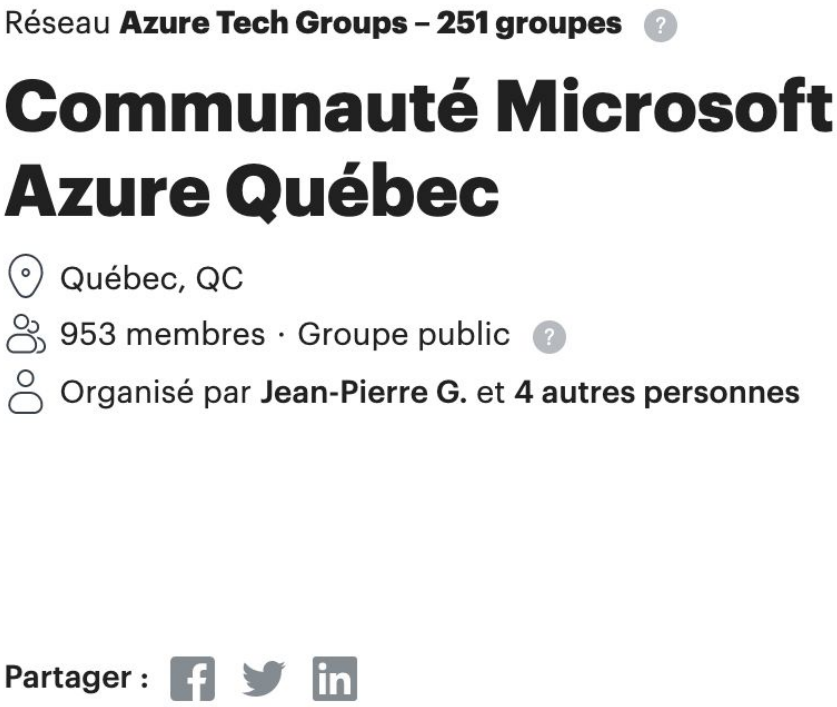
Open Source Contributor (Kubernetes / VSCode)

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!



Réseau **Azure Tech Groups – 251 groupes** ?

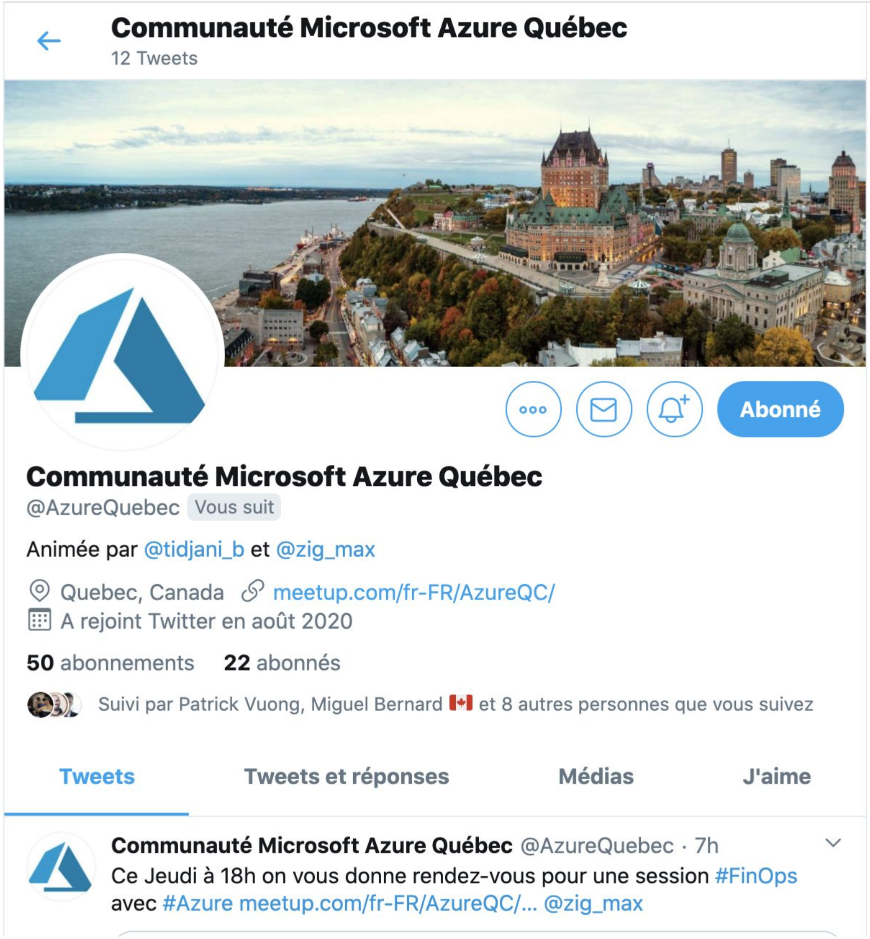
Communauté Microsoft Azure Québec

Québec, QC

953 membres · Groupe public ?

Organisé par **Jean-Pierre G.** et **4 autres personnes**

Partager :



Communauté Microsoft Azure Québec
12 Tweets

Communauté Microsoft Azure Québec
@AzureQuebec Vous suit

Animée par @tidjani_b et @zig_max

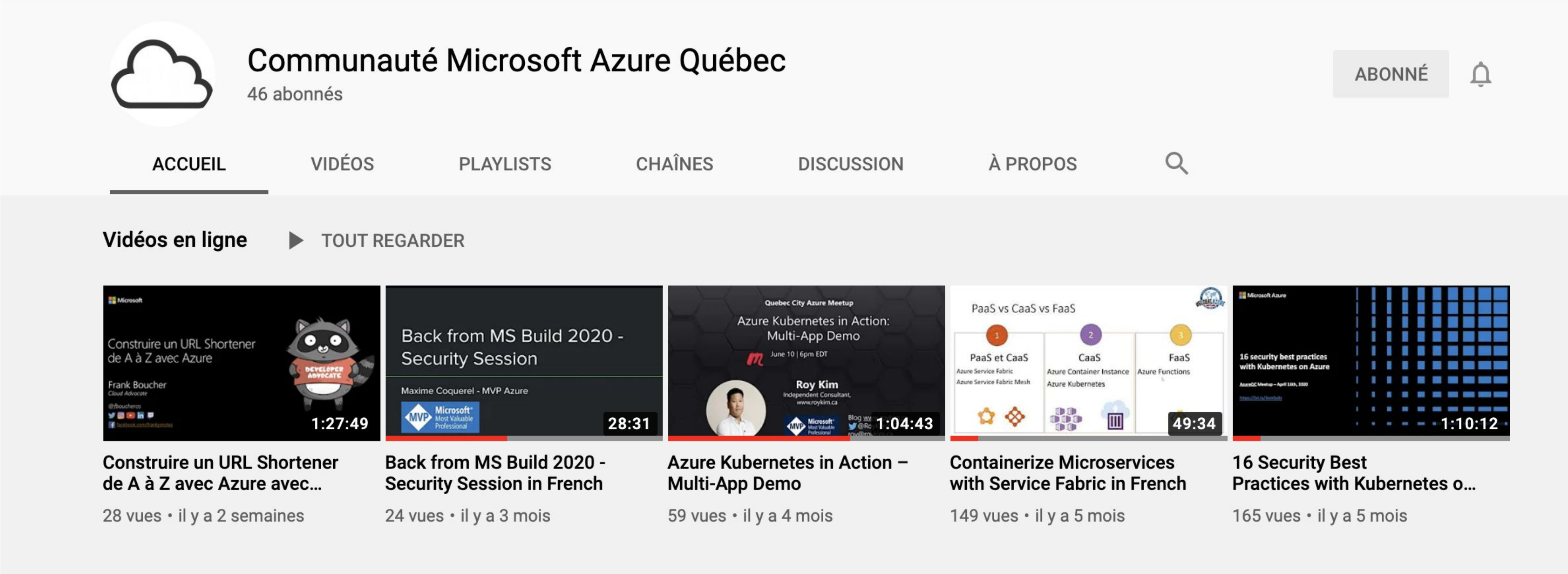
Quebec, Canada meetup.com/fr-FR/AzureQC/
A rejoint Twitter en août 2020

50 abonnements **22** abonnés

Suivi par Patrick Vuong, Miguel Bernard 🇨🇦 et 8 autres personnes que vous suivez

Communauté Microsoft Azure Québec @AzureQuebec · 7h
Ce Jeudi à 18h on vous donne rendez-vous pour une session #FinOps avec #Azure meetup.com/fr-FR/AzureQC/... @zig_max

Youtube - Communauté Azure Québec


ABONNÉ
ACCUEIL
VIDÉOS
PLAYLISTS
CHAÎNES
DISCUSSION
À PROPOS
TOUT REGARDER
Construire un URL Shortener de A à Z avec Azure
Frank Boucher
1:27:49
Back from MS Build 2020 - Security Session
Maxime Coquerel - MVP Azure
28:31
Quebec City Azure Meetup
Azure Kubernetes in Action: Multi-App Demo
June 10 | 6pm EDT
Roy Kim
1:04:43
PaaS vs CaaS vs FaaS
PaaS et CaaS
CaaS
FaaS
49:34
16 security best practices with Kubernetes on Azure
1:10:12

Communauté Microsoft Azure Québec

46 abonnés

Vidéos en ligne

Construire un URL Shortener de A à Z avec Azure avec...
28 vues • il y a 2 semaines

Back from MS Build 2020 - Security Session in French
24 vues • il y a 3 mois

Azure Kubernetes in Action – Multi-App Demo
59 vues • il y a 4 mois

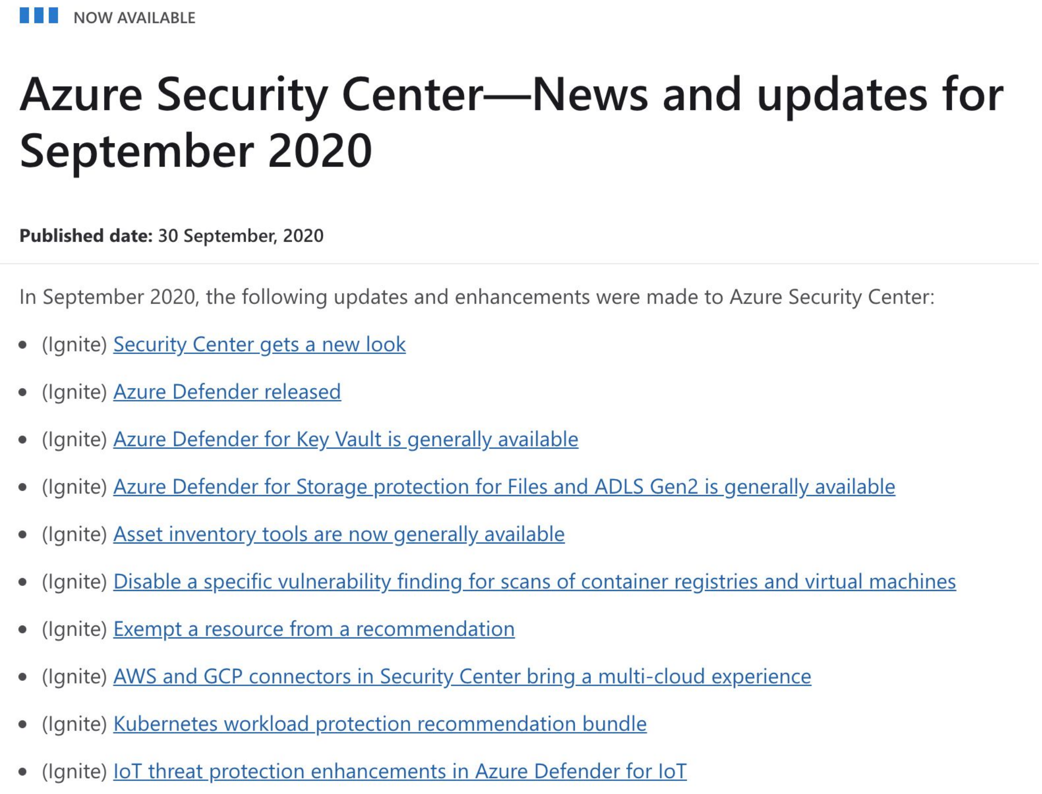
Containerize Microservices with Service Fabric in French
149 vues • il y a 5 mois

16 Security Best Practices with Kubernetes o...
165 vues • il y a 5 mois

Session Agenda / Goal

- Azure Security Center Updates
- Azure Security Center - New look
- Azure Defender
- Azure Security Center - Multi Cloud
- Asset Inventory

Azure Security Center Updates



▮▮▮ NOW AVAILABLE

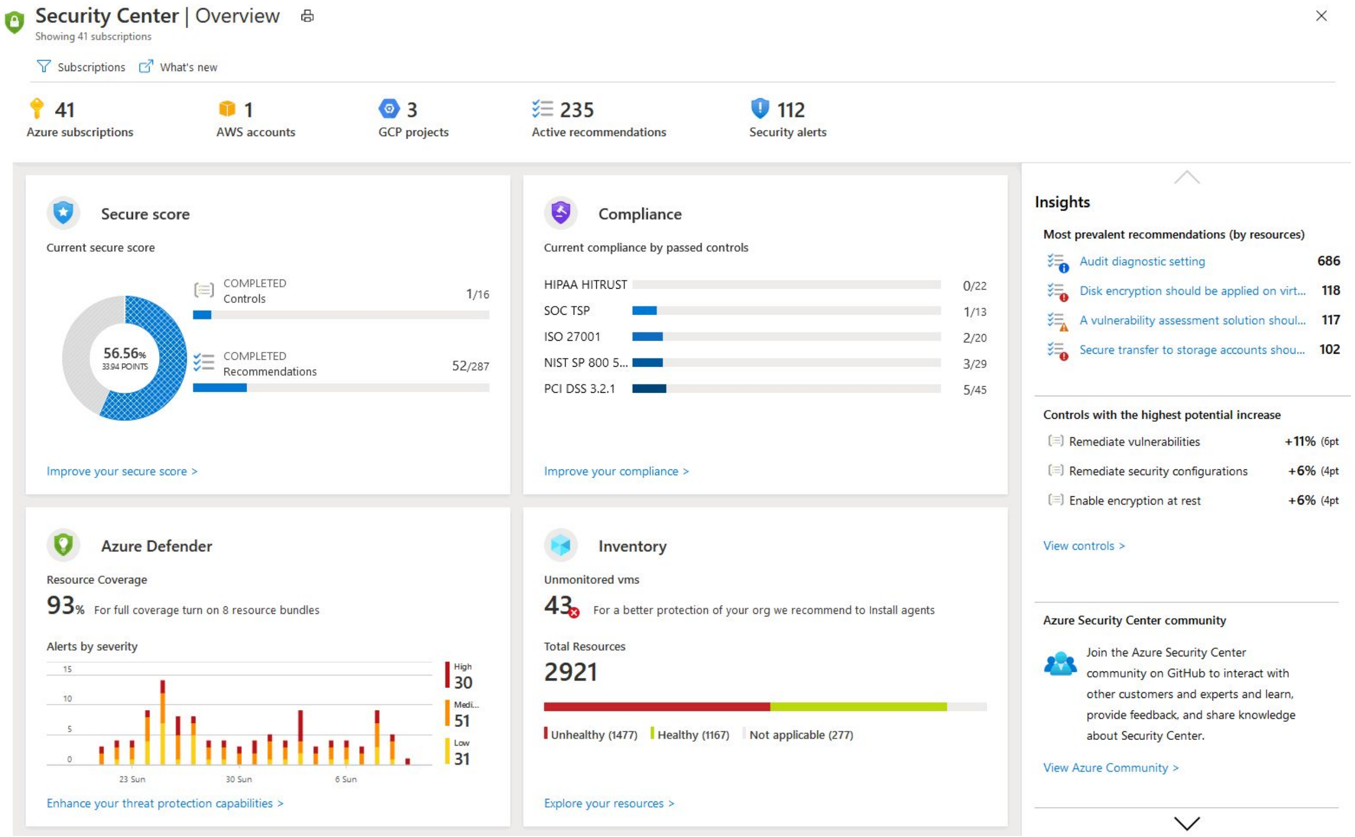
Azure Security Center—News and updates for September 2020

Published date: 30 September, 2020

In September 2020, the following updates and enhancements were made to Azure Security Center:

- (Ignite) Security Center gets a new look
- (Ignite) Azure Defender released
- (Ignite) Azure Defender for Key Vault is generally available
- (Ignite) Azure Defender for Storage protection for Files and ADLS Gen2 is generally available
- (Ignite) Asset inventory tools are now generally available
- (Ignite) Disable a specific vulnerability finding for scans of container registries and virtual machines
- (Ignite) Exempt a resource from a recommendation
- (Ignite) AWS and GCP connectors in Security Center bring a multi-cloud experience
- (Ignite) Kubernetes workload protection recommendation bundle
- (Ignite) IoT threat protection enhancements in Azure Defender for IoT

Azure Security Center - New look



Security Center | Overview

Showing 41 subscriptions

Subscriptions   What's new

41	Azure subscriptions
1	AWS accounts
3	GCP projects
235	Active recommendations
112	Security alerts

Secure score

Current secure score

56.56%
33.94 POINTS

COMPLETED Controls 1/16

COMPLETED Recommendations 52/287

Improve your secure score >

Compliance

Current compliance by passed controls

HIPAA HITRUST	0/22
SOC TSP	1/13
ISO 27001	2/20
NIST SP 800 5...	3/29
PCI DSS 3.2.1	5/45

Improve your compliance >

Azure Defender

Resource Coverage

93% For full coverage turn on 8 resource bundles

Alerts by severity

High 30
Medi... 51
Low 31

Enhance your threat protection capabilities >

Inventory

Unmonitored vms

43 For a better protection of your org we recommend to Install agents

Total Resources

2921

Unhealthy (1477)   Healthy (1167)   Not applicable (277)

Explore your resources >

Insights

Most prevalent recommendations (by resources)

Audit diagnostic setting	686
Disk encryption should be applied on virt...	118
A vulnerability assessment solution shoul...	117
Secure transfer to storage accounts shou...	102

Controls with the highest potential increase

Remediate vulnerabilities	+11% (6pt
Remediate security configurations	+6% (4pt
Enable encryption at rest	+6% (4pt

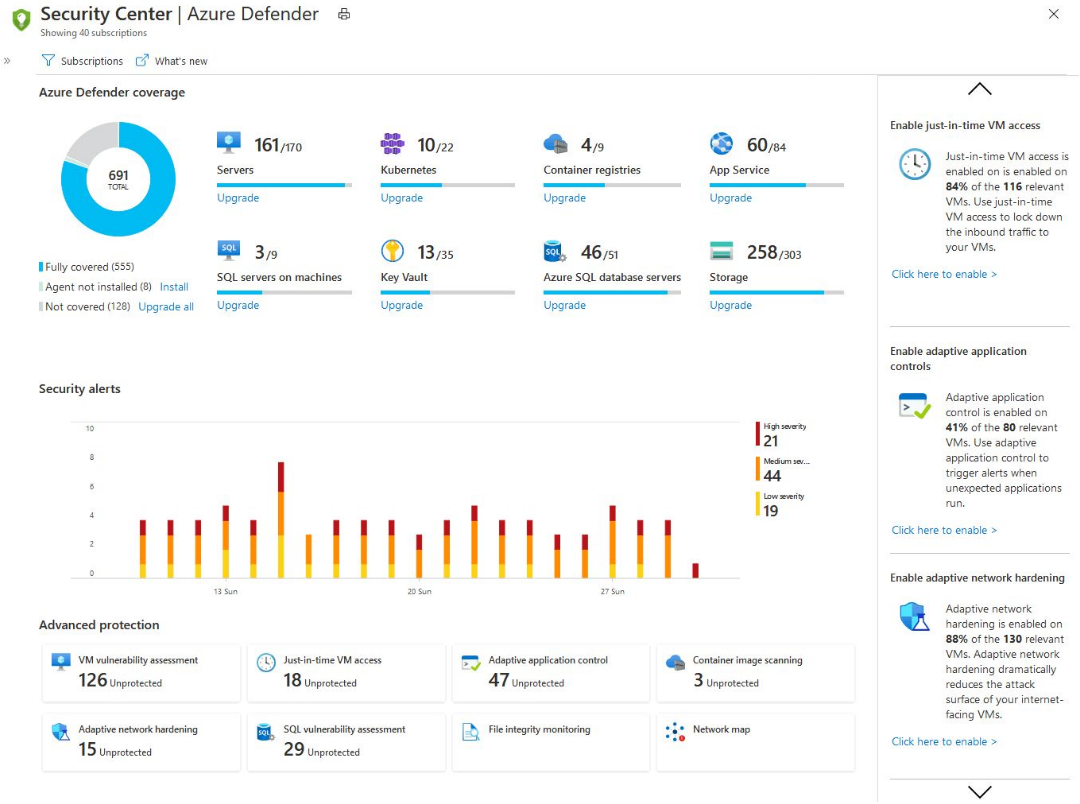
View controls >

Azure Security Center community

Join the Azure Security Center community on GitHub to interact with other customers and experts and learn, provide feedback, and share knowledge about Security Center.

View Azure Community >

Azure Defender



Azure Defender coverage

691 TOTAL

Fully covered (555)
Agent not installed (8) Install
Not covered (128) Upgrade all

161/170 Servers Upgrade	10/22 Kubernetes Upgrade	4/9 Container registries Upgrade	60/84 App Service Upgrade
3/9 SQL servers on machines Upgrade	13/35 Key Vault Upgrade	46/51 Azure SQL database servers Upgrade	258/303 Storage Upgrade

Security alerts

High severity 21
Medium sev... 44
Low severity 19

Advanced protection

VM vulnerability assessment 126 Unprotected	Just-in-time VM access 18 Unprotected	Adaptive application control 47 Unprotected	Container image scanning 3 Unprotected
Adaptive network hardening 15 Unprotected	SQL vulnerability assessment 29 Unprotected	File integrity monitoring	Network map

Enable just-in-time VM access

Just-in-time VM access is enabled on is enabled on **84%** of the **116** relevant VMs. Use just-in-time VM access to lock down the inbound traffic to your VMs.

Click here to enable >

Enable adaptive application controls

Adaptive application control is enabled on **41%** of the **80** relevant VMs. Use adaptive application control to trigger alerts when unexpected applications run.

Click here to enable >

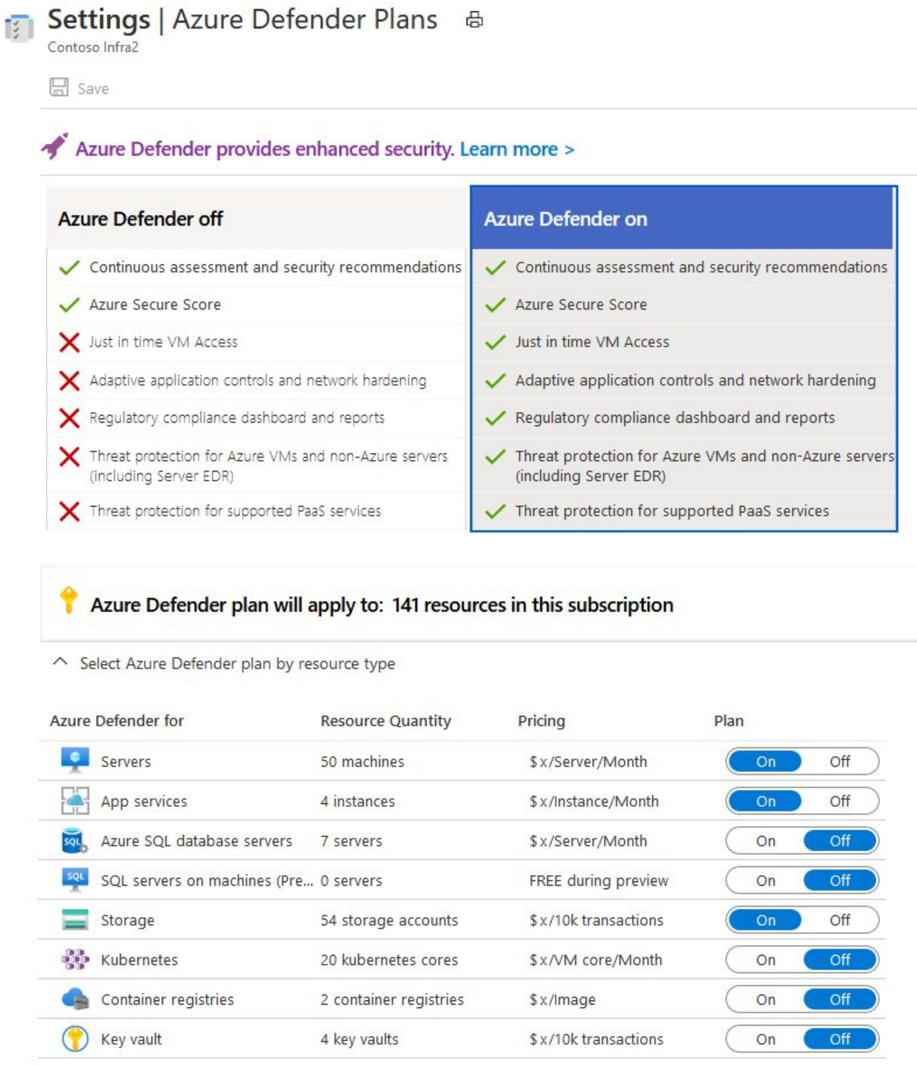
Enable adaptive network hardening

Adaptive network hardening is enabled on **88%** of the **130** relevant VMs. Adaptive network hardening dramatically reduces the attack surface of your internet-facing VMs.

Click here to enable >

Azure Defender is the cloud workload protection platform (CWPP) integrated within Security Center for advanced, intelligent, protection of your Azure and hybrid workloads. **It replaces Security Center's standard pricing tier option.**

- Azure Defender for servers
- Azure Defender for App Service
- Azure Defender for Storage
- Azure Defender for SQL
- Azure Defender for Key Vault
- Azure Defender for Kubernetes
- Azure Defender for container registries



Settings | Azure Defender Plans

Contoso Infra2

Azure Defender provides enhanced security. Learn more >

Azure Defender off	Azure Defender on
✓ Continuous assessment and security recommendations	✓ Continuous assessment and security recommendations
✓ Azure Secure Score	✓ Azure Secure Score
✗ Just in time VM Access	✓ Just in time VM Access
✗ Adaptive application controls and network hardening	✓ Adaptive application controls and network hardening
✗ Regulatory compliance dashboard and reports	✓ Regulatory compliance dashboard and reports
✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)	✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
✗ Threat protection for supported PaaS services	✓ Threat protection for supported PaaS services

Azure Defender plan will apply to: 141 resources in this subscription

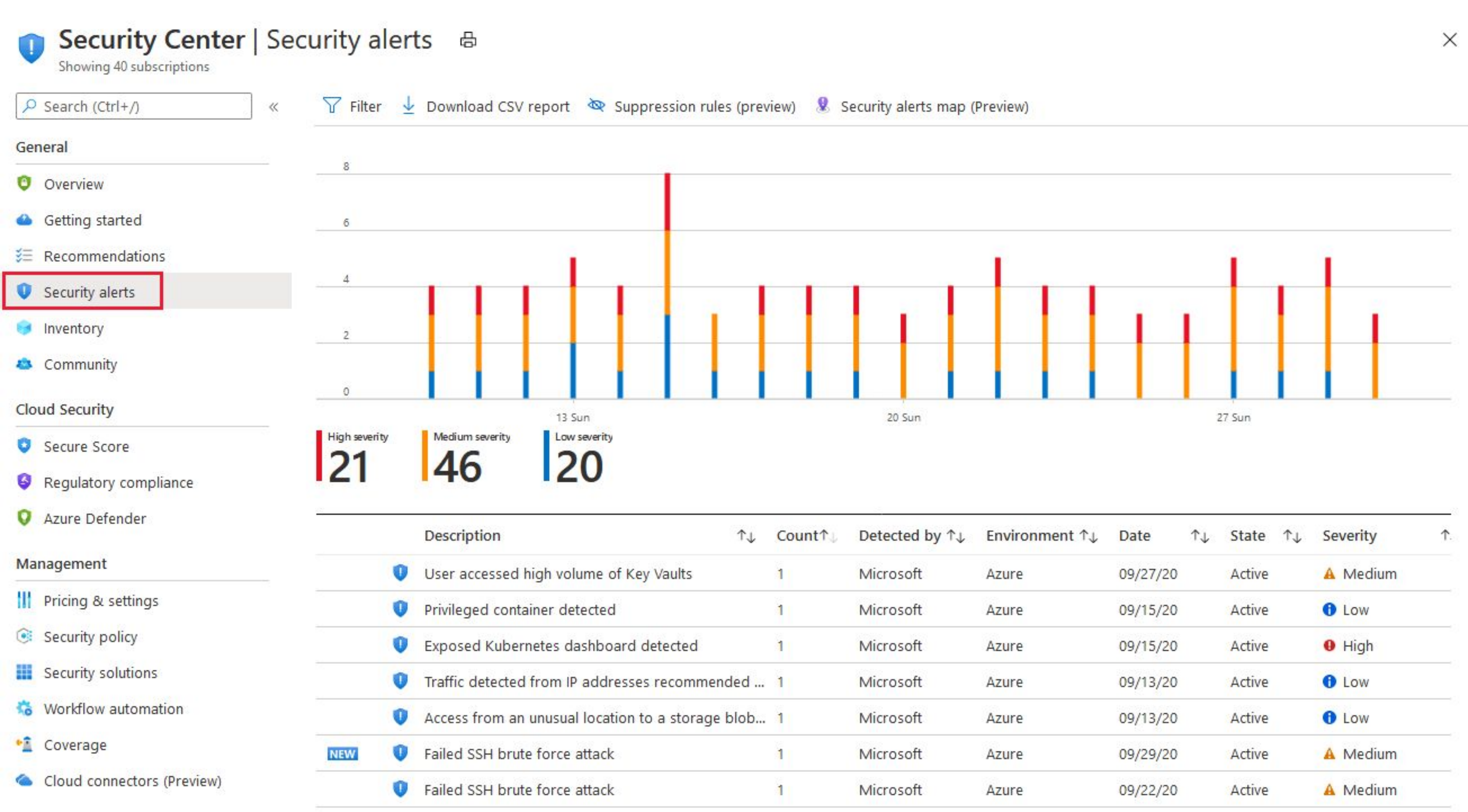
Select Azure Defender plan by resource type

Azure Defender for	Resource Quantity	Pricing	Plan
Servers	50 machines	$x/Server/Month	[✓ On] Off
App services	4 instances	$x/Instance/Month	[✓ On] Off
Azure SQL database servers	7 servers	$x/Server/Month	On [✓ Off]
SQL servers on machines (Pre...	0 servers	FREE during preview	On [✓ Off]
Storage	54 storage accounts	$x/10k transactions	[✓ On] Off
Kubernetes	20 kubernetes cores	$x/VM core/Month	On [✓ Off]
Container registries	2 container registries	$x/Image	On [✓ Off]
Key vault	4 key vaults	$x/10k transactions	On [✓ Off]

Examples of Azure Defender Alerts:

- Access from a TOR exit node to a key vault
- High volume of operations in a key vault
- Suspicious secret listing and query in a key vault
- Unusual user accessed a key vault
- Container with a sensitive volume mount detected
- Digital currency mining container detected
- Exposed Kubernetes dashboard detected
- Role binding to the cluster-admin role detected
- Access from a Tor exit node to a storage account
- Anonymous access to a storage account
- A kernel module was loaded (Linux VM)
- A logon from a malicious IP has been detected (Windows VM)
- Detected Petya ransomware indicators (Windows VM)
- And more ..

https://docs.microsoft.com/en-us/azure/security-center/alerts-reference



Security Center | Security alerts

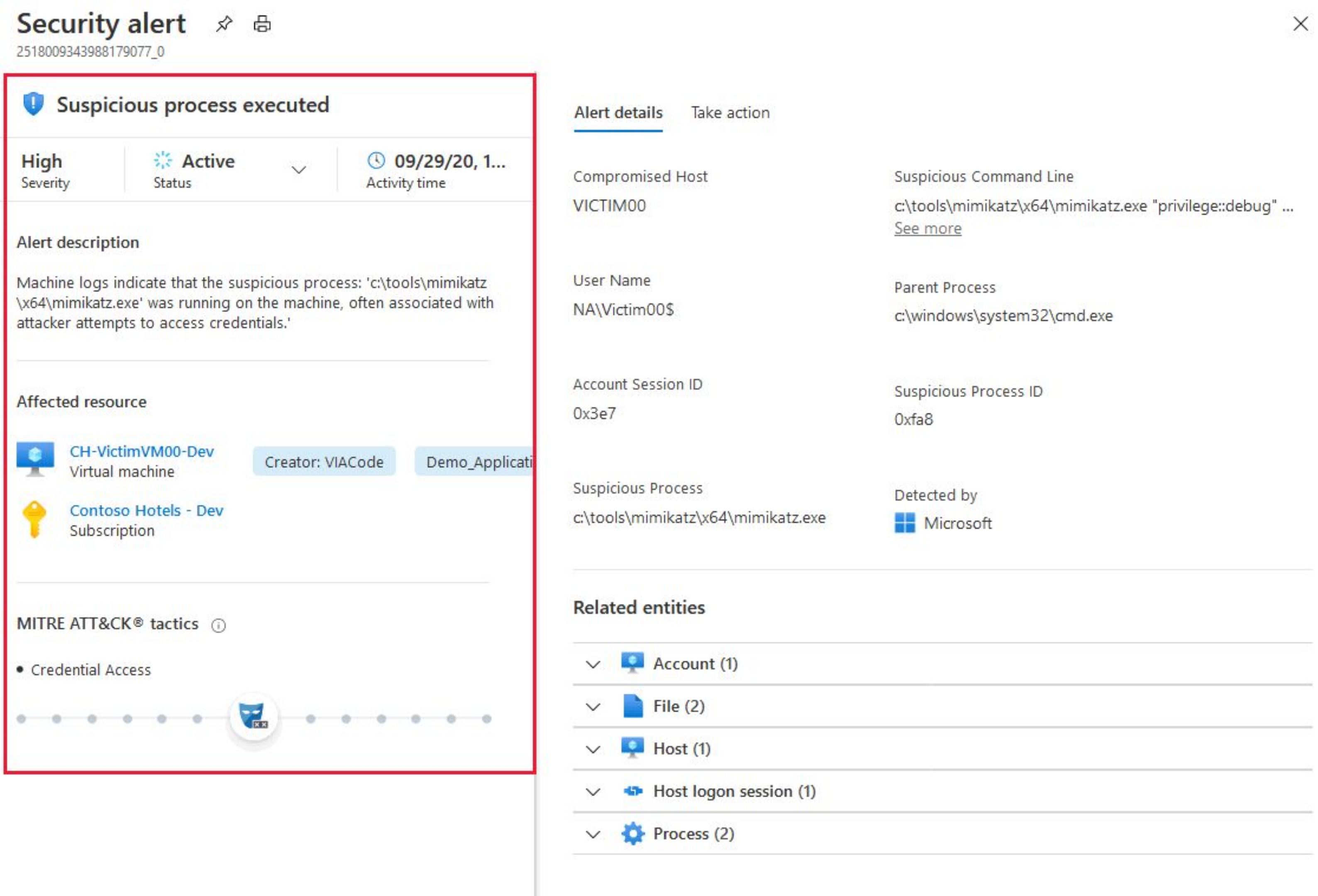
Showing 40 subscriptions

High severity 21

Medium severity 46

Low severity 20

	Description	Count	Detected by	Environment	Date	State	Severity
	User accessed high volume of Key Vaults	1	Microsoft	Azure	09/27/20	Active	Medium
	Privileged container detected	1	Microsoft	Azure	09/15/20	Active	Low
	Exposed Kubernetes dashboard detected	1	Microsoft	Azure	09/15/20	Active	High
	Traffic detected from IP addresses recommended ...	1	Microsoft	Azure	09/13/20	Active	Low
	Access from an unusual location to a storage blob...	1	Microsoft	Azure	09/13/20	Active	Low
NEW	Failed SSH brute force attack	1	Microsoft	Azure	09/29/20	Active	Medium
	Failed SSH brute force attack	1	Microsoft	Azure	09/22/20	Active	Medium



Security alert

2518009343988179077_0

Suspicious process executed

High
Severity

Active
Status

09/29/20, 1...
Activity time

Alert description

Machine logs indicate that the suspicious process: 'c:\tools\mimikatz\x64\mimikatz.exe' was running on the machine, often associated with attacker attempts to access credentials.'

Affected resource

CH-VictimVM00-Dev
Virtual machine

Creator: VIACode

Demo_Applicati

Contoso Hotels - Dev
Subscription

MITRE ATT&CK® tactics

- Credential Access

Alert details | Take action

Compromised Host
VICTIM00

Suspicious Command Line
c:\tools\mimikatz\x64\mimikatz.exe "privilege::debug" ...
See more

User Name
NA\Victim00$

Parent Process
c:\windows\system32\cmd.exe

Account Session ID
0x3e7

Suspicious Process ID
0xfa8

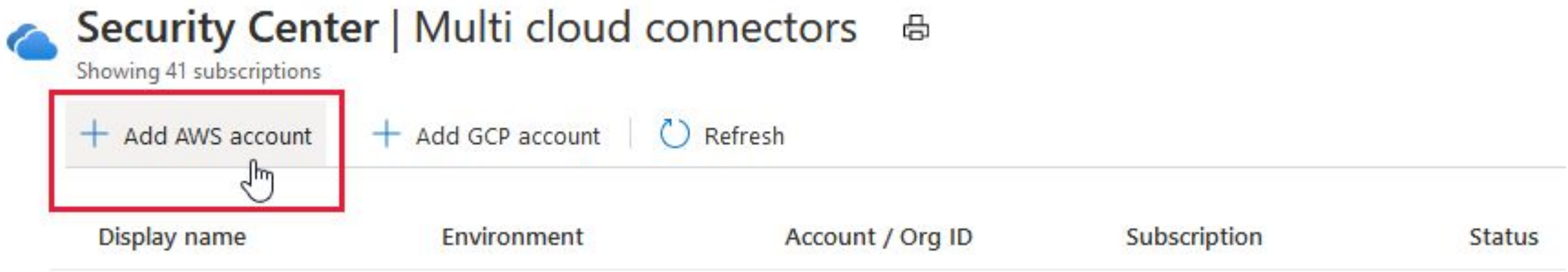
Suspicious Process
c:\tools\mimikatz\x64\mimikatz.exe

Detected by
Microsoft

Related entities

- Account (1)
- File (2)
- Host (1)
- Host logon session (1)
- Process (2)

Azure Security Center - Multi Cloud

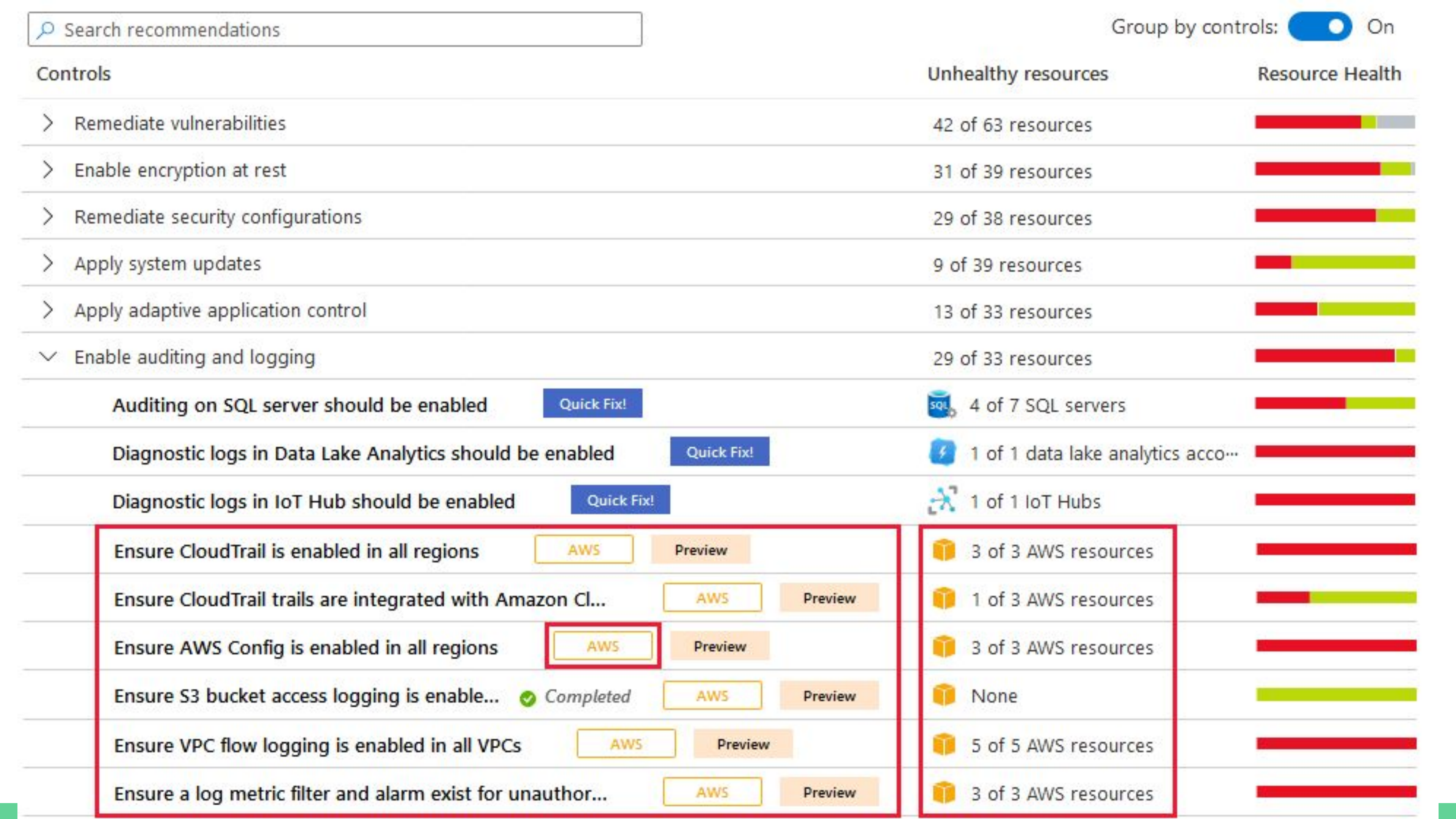


Security Center | Multi cloud connectors

Showing 41 subscriptions

Display name	Environment	Account / Org ID	Subscription	Status

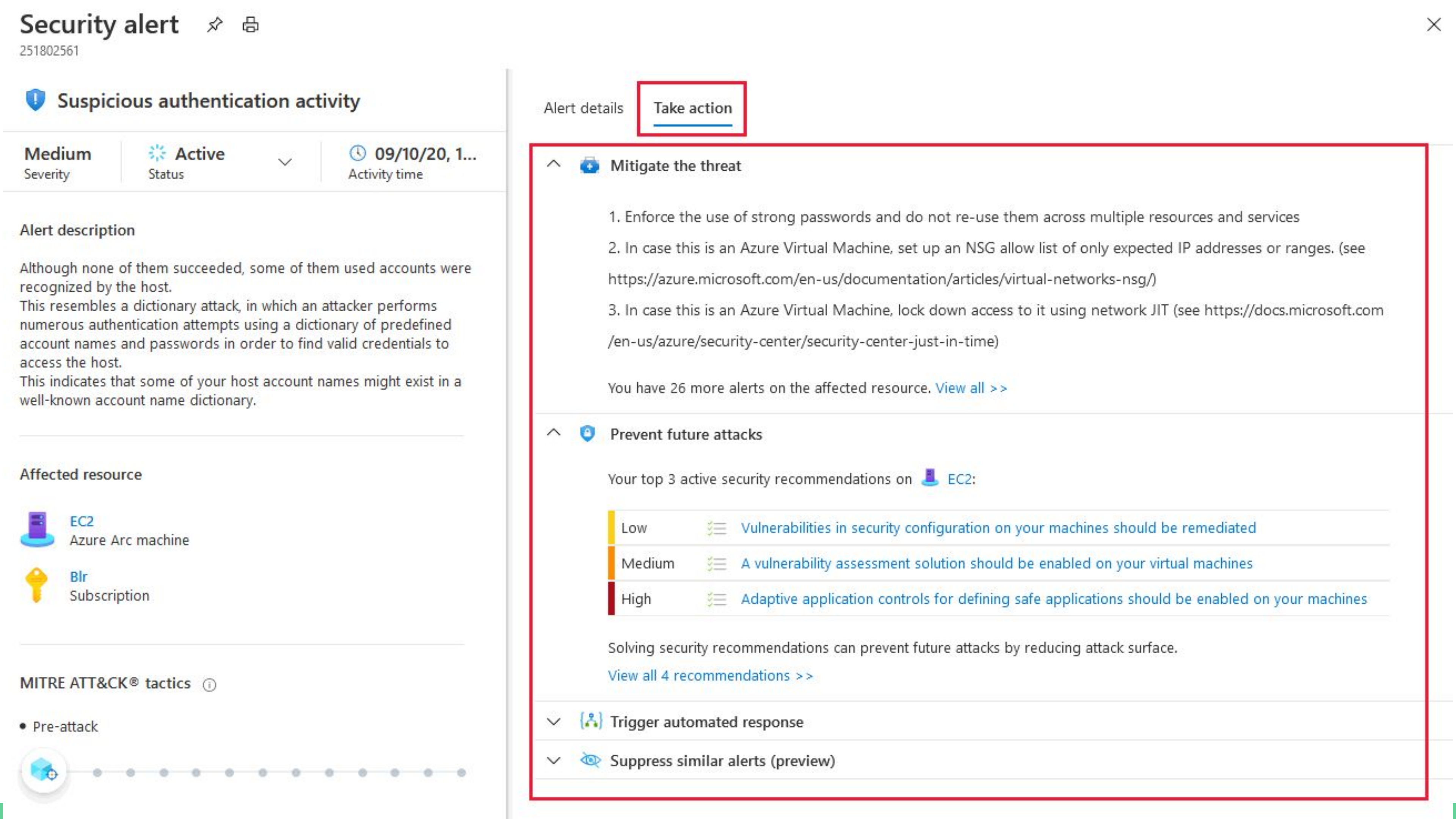
- Automatic agent provisioning (Security Center uses Azure Arc to deploy the Log Analytics agent to your AWS instances)
- Policy management
- Vulnerability management
- Embedded Endpoint Detection and Response (EDR)
- Detection of security misconfigurations
- A single view showing Security Center recommendations and AWS Security Hub findings
- Incorporation of your AWS resources into Security Center's secure score calculations
- Regulatory compliance assessments of your AWS resources



Search recommendations

Group by controls: On

Controls		Unhealthy resources	Resource Health
› Remediate vulnerabilities		42 of 63 resources	
› Enable encryption at rest		31 of 39 resources	
› Remediate security configurations		29 of 38 resources	
› Apply system updates		9 of 39 resources	
› Apply adaptive application control		13 of 33 resources	
⌄ Enable auditing and logging		29 of 33 resources	
Auditing on SQL server should be enabled	Quick Fix!	4 of 7 SQL servers	
Diagnostic logs in Data Lake Analytics should be enabled	Quick Fix!	1 of 1 data lake analytics acco···	
Diagnostic logs in IoT Hub should be enabled	Quick Fix!	1 of 1 IoT Hubs	
Ensure CloudTrail is enabled in all regions	AWS Preview	3 of 3 AWS resources	
Ensure CloudTrail trails are integrated with Amazon Cl...	AWS Preview	1 of 3 AWS resources	
Ensure AWS Config is enabled in all regions	AWS Preview	3 of 3 AWS resources	
Ensure S3 bucket access logging is enable...	✓ *Completed* AWS Preview	None	
Ensure VPC flow logging is enabled in all VPCs	AWS Preview	5 of 5 AWS resources	
Ensure a log metric filter and alarm exist for unauthor...	AWS Preview	3 of 3 AWS resources	



Security alert

251802561

Suspicious authentication activity

Medium Severity	Active Status	09/10/20, 1... Activity time

Alert description

Although none of them succeeded, some of them used accounts were recognized by the host.
This resembles a dictionary attack, in which an attacker performs numerous authentication attempts using a dictionary of predefined account names and passwords in order to find valid credentials to access the host.
This indicates that some of your host account names might exist in a well-known account name dictionary.

Affected resource

EC2
Azure Arc machine

Blr
Subscription

MITRE ATT&CK® tactics

- Pre-attack

Mitigate the threat

1. Enforce the use of strong passwords and do not re-use them across multiple resources and services
2. In case this is an Azure Virtual Machine, set up an NSG allow list of only expected IP addresses or ranges. (see https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/)
3. In case this is an Azure Virtual Machine, lock down access to it using network JIT (see https://docs.microsoft.com /en-us/azure/security-center/security-center-just-in-time)

You have 26 more alerts on the affected resource. View all >>

Prevent future attacks

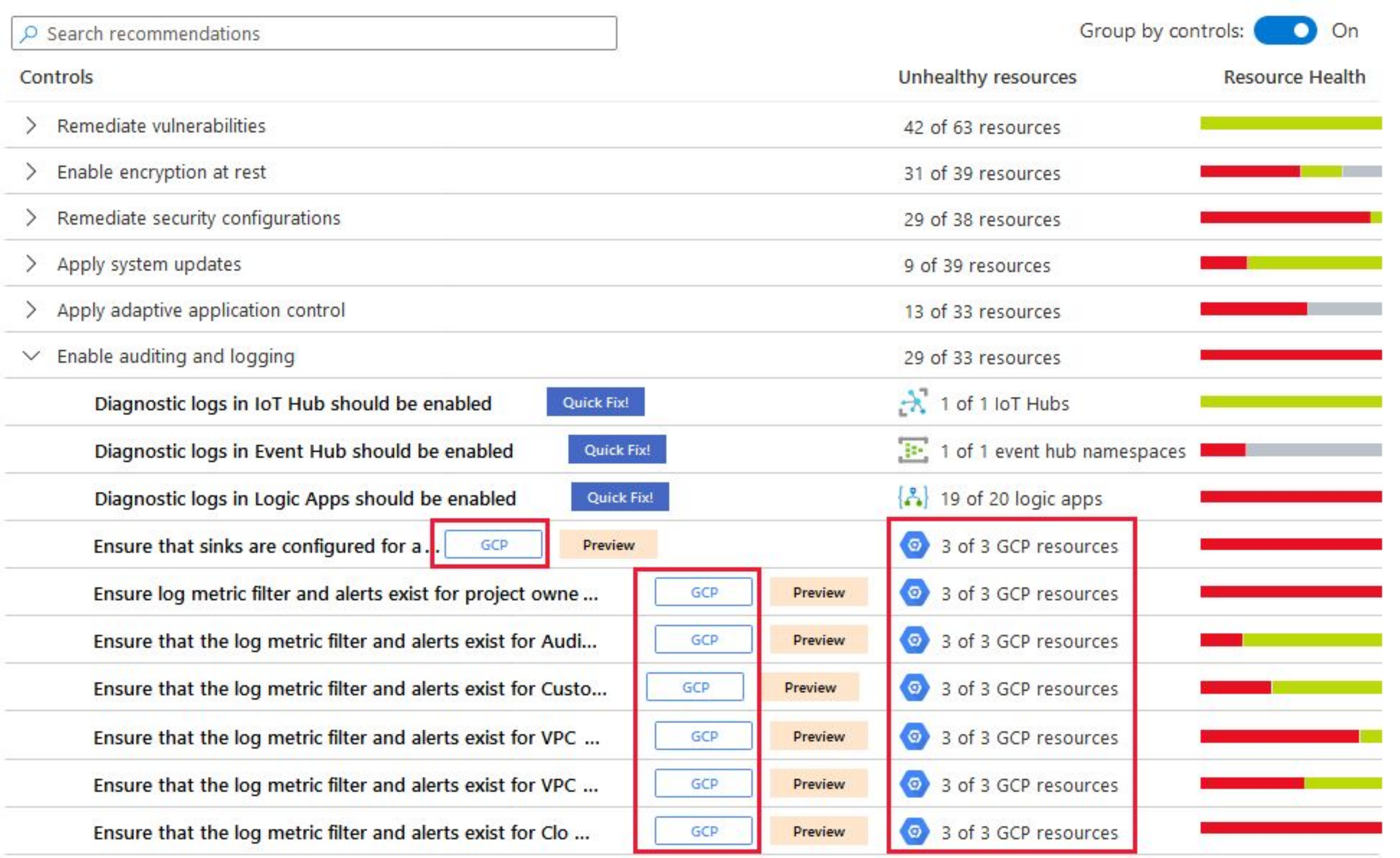
Your top 3 active security recommendations on EC2:

Low	Vulnerabilities in security configuration on your machines should be remediated
Medium	A vulnerability assessment solution should be enabled on your virtual machines
High	Adaptive application controls for defining safe applications should be enabled on your machines

Solving security recommendations can prevent future attacks by reducing attack surface.
View all 4 recommendations >>

Trigger automated response

Suppress similar alerts (preview)

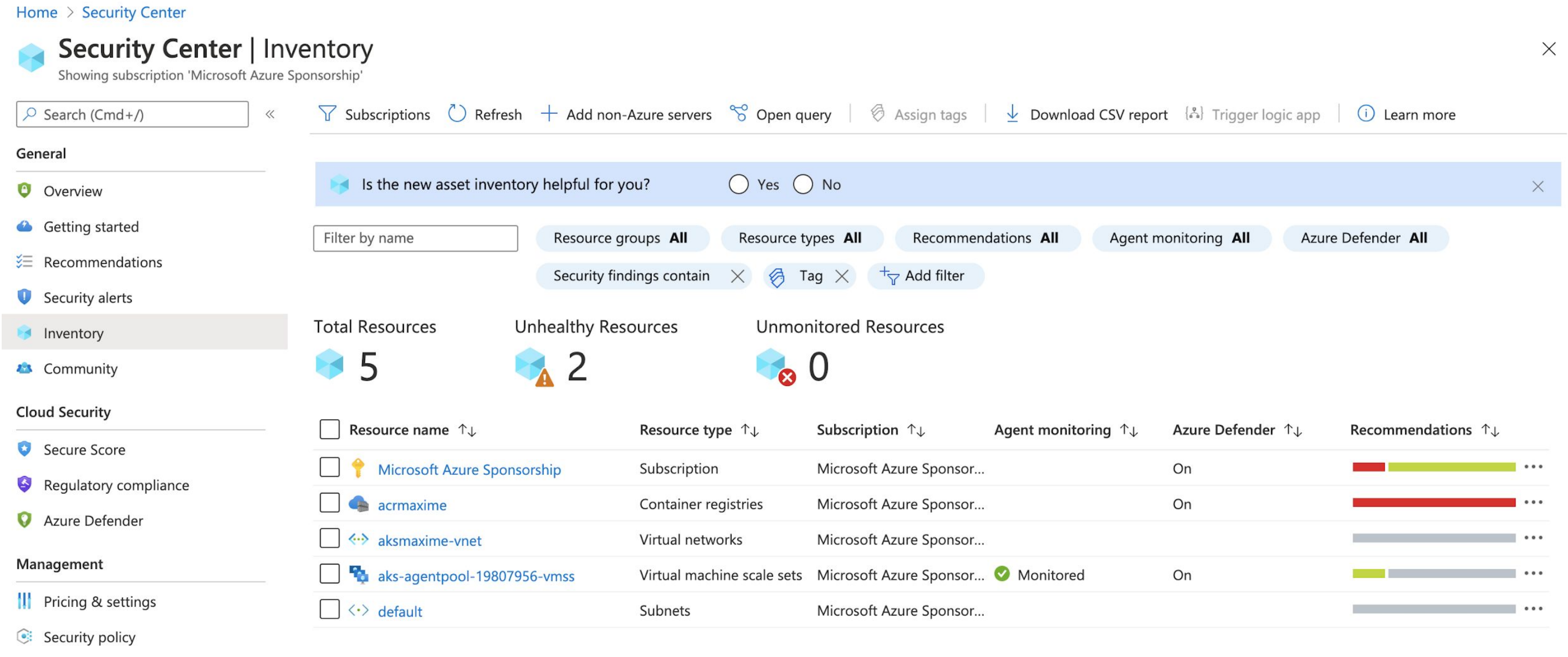


Search recommendations

Group by controls: On

Controls			Unhealthy resources	Resource Health
> Remediate vulnerabilities			42 of 63 resources	🟩
> Enable encryption at rest			31 of 39 resources	🟥🟩⬜
> Remediate security configurations			29 of 38 resources	🟥🟩
> Apply system updates			9 of 39 resources	🟥🟩
> Apply adaptive application control			13 of 33 resources	🟥⬜
∨ Enable auditing and logging			29 of 33 resources	🟥
Diagnostic logs in IoT Hub should be enabled	Quick Fix!		1 of 1 IoT Hubs	🟩
Diagnostic logs in Event Hub should be enabled	Quick Fix!		1 of 1 event hub namespaces	🟥⬜
Diagnostic logs in Logic Apps should be enabled	Quick Fix!		19 of 20 logic apps	🟥
Ensure that sinks are configured for a ...	GCP	Preview	3 of 3 GCP resources	🟥
Ensure log metric filter and alerts exist for project owne ...	GCP	Preview	3 of 3 GCP resources	🟥
Ensure that the log metric filter and alerts exist for Audi...	GCP	Preview	3 of 3 GCP resources	🟥🟩
Ensure that the log metric filter and alerts exist for Custo...	GCP	Preview	3 of 3 GCP resources	🟥🟩
Ensure that the log metric filter and alerts exist for VPC ...	GCP	Preview	3 of 3 GCP resources	🟥🟩
Ensure that the log metric filter and alerts exist for VPC ...	GCP	Preview	3 of 3 GCP resources	🟥🟩
Ensure that the log metric filter and alerts exist for Clo ...	GCP	Preview	3 of 3 GCP resources	🟥

Asset Inventory



Security Center | Inventory

Showing subscription 'Microsoft Azure Sponsorship'

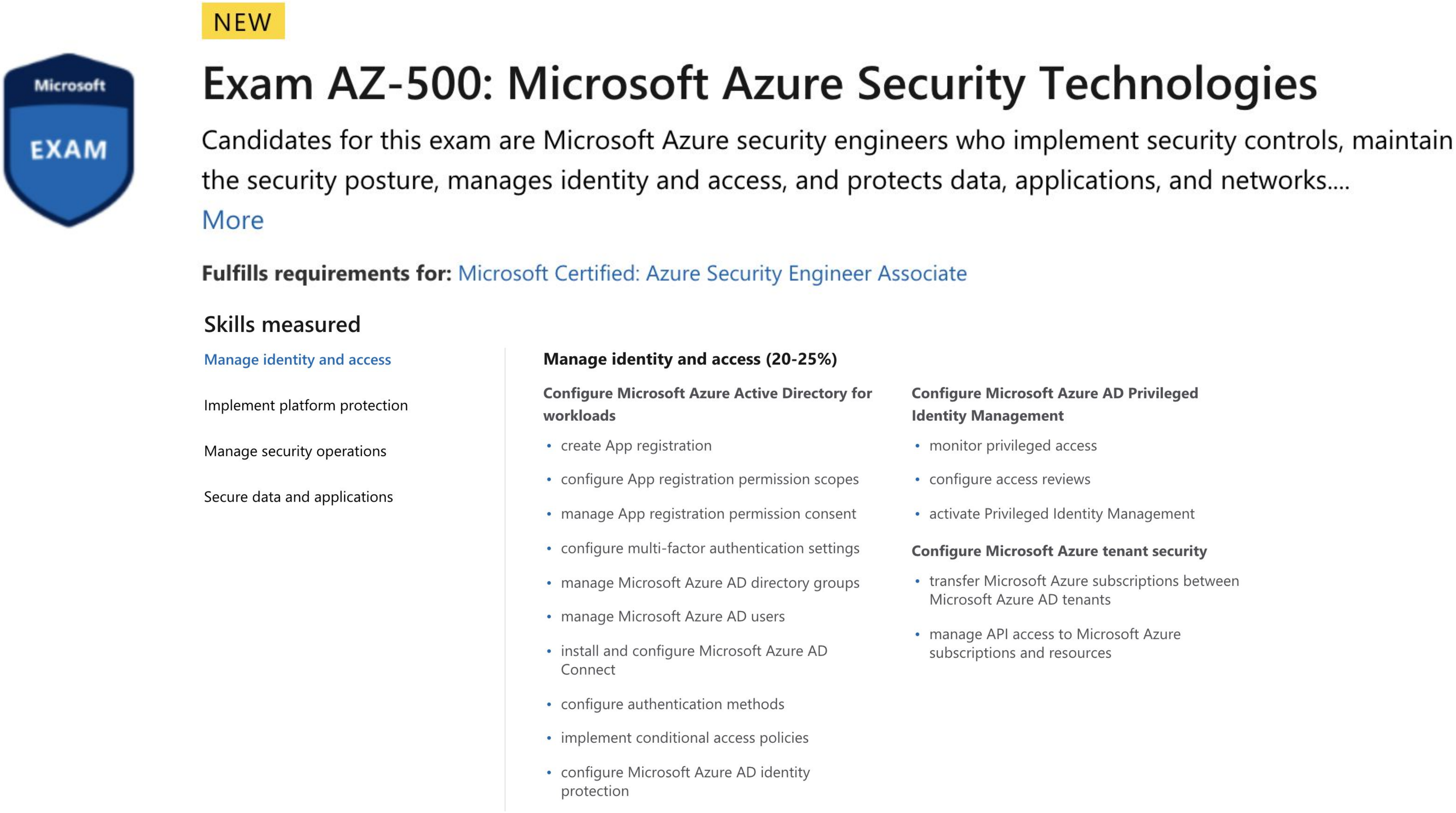
Is the new asset inventory helpful for you? ○ Yes ○ No

Total Resources 5

Unhealthy Resources 2

Unmonitored Resources 0

□	Resource name	Resource type	Subscription	Agent monitoring	Azure Defender	Recommendations
□	Microsoft Azure Sponsorship	Subscription	Microsoft Azure Sponsor...		On	🟥🟩
□	acrmaxime	Container registries	Microsoft Azure Sponsor...		On	🟥
□	aksmaxime-vnet	Virtual networks	Microsoft Azure Sponsor...			⬜
□	aks-agentpool-19807956-vmss	Virtual machine scale sets	Microsoft Azure Sponsor...	✓ Monitored	On	🟩⬜
□	default	Subnets	Microsoft Azure Sponsor...			⬜



NEW

Exam AZ-500: Microsoft Azure Security Technologies

Candidates for this exam are Microsoft Azure security engineers who implement security controls, maintain the security posture, manages identity and access, and protects data, applications, and networks.... More

Fulfills requirements for: Microsoft Certified: Azure Security Engineer Associate

Skills measured

- Manage identity and access
- Implement platform protection
- Manage security operations
- Secure data and applications

Manage identity and access (20-25%)

Configure Microsoft Azure Active Directory for workloads

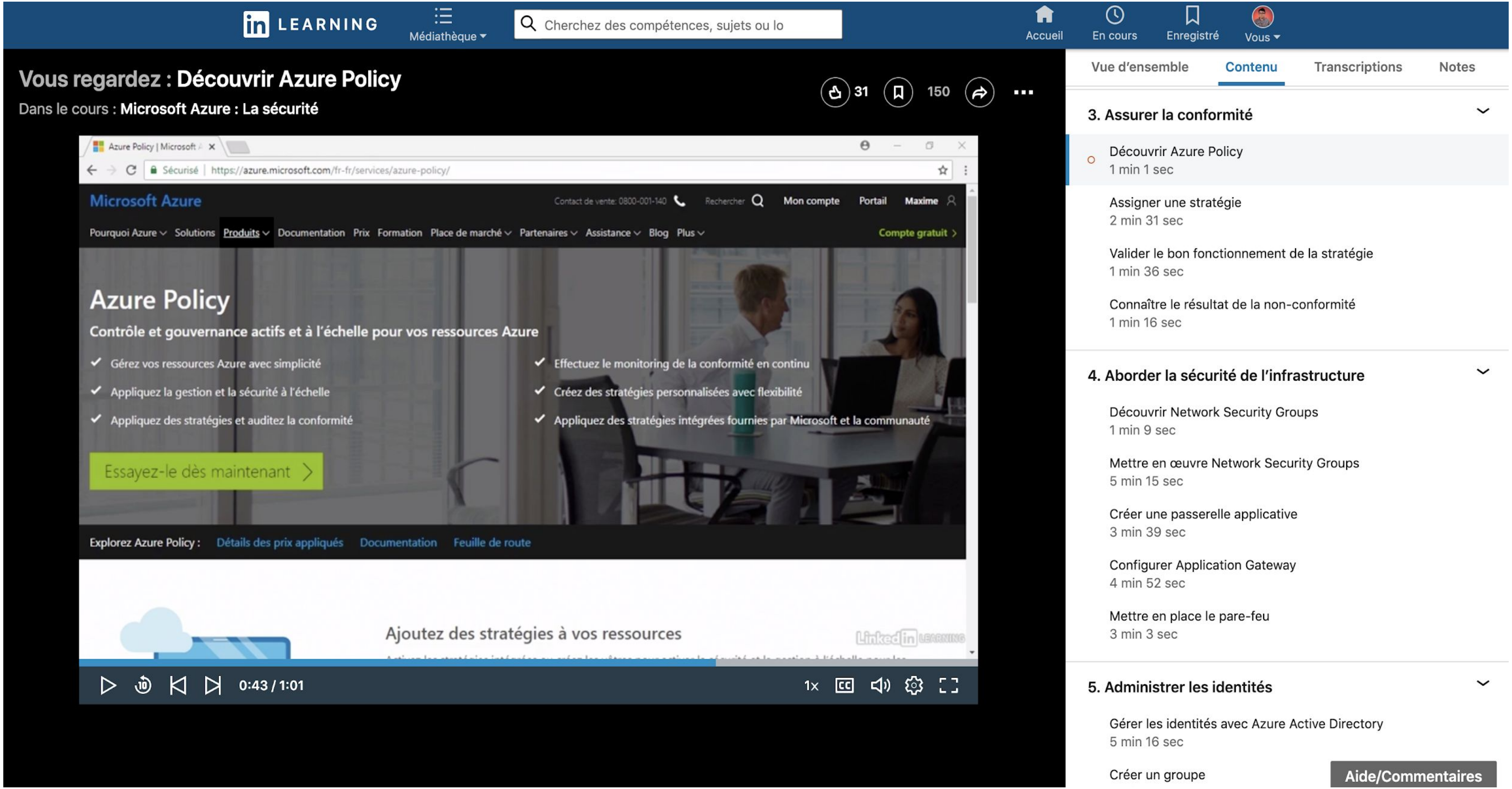
- create App registration
- configure App registration permission scopes
- manage App registration permission consent
- configure multi-factor authentication settings
- manage Microsoft Azure AD directory groups
- manage Microsoft Azure AD users
- install and configure Microsoft Azure AD Connect
- configure authentication methods
- implement conditional access policies
- configure Microsoft Azure AD identity protection

Configure Microsoft Azure AD Privileged Identity Management

- monitor privileged access
- configure access reviews
- activate Privileged Identity Management

Configure Microsoft Azure tenant security

- transfer Microsoft Azure subscriptions between Microsoft Azure AD tenants
- manage API access to Microsoft Azure subscriptions and resources



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

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 2020 - https://myignite.microsoft.com/home

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

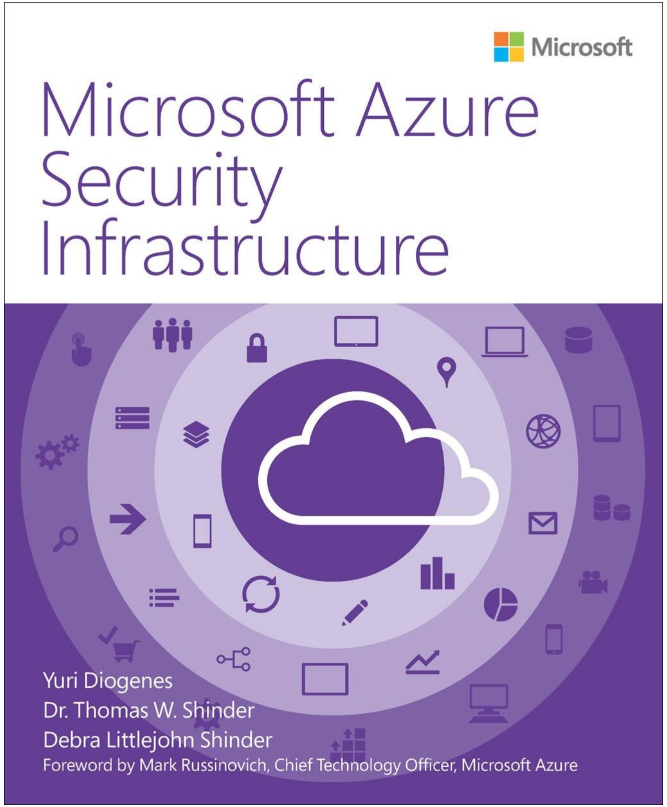
Azure Security Blog - https://azure.microsoft.com/en-us/blog/topics/security/

Maxime Blog - http://zigmax.net

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

NEW!

Books

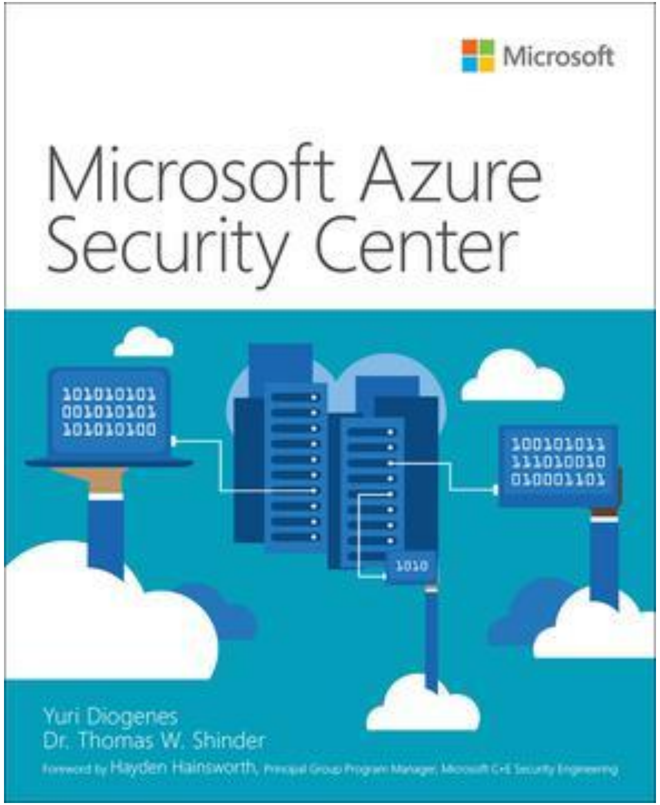


Microsoft

Microsoft Azure Security Infrastructure

Yuri Diogenes
Dr. Thomas W. Shinder
Debra Littlejohn Shinder

Foreword by Mark Russinovich, Chief Technology Officer, Microsoft Azure

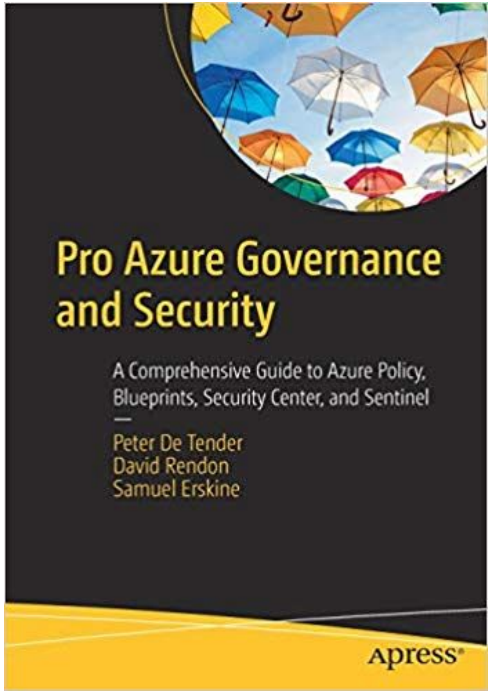


Microsoft

Microsoft Azure Security Center

Yuri Diogenes
Dr. Thomas W. Shinder

Foreword by Hayden Hainsworth, Principal Group Program Manager, Microsoft C+E Security Engineering



Pro Azure Governance and Security

A Comprehensive Guide to Azure Policy, Blueprints, Security Center, and Sentinel

Peter De Tender
David Rendon
Samuel Erskine

Apress®

Questions / Talks