

WELCOME
TO

ESPC

JOIN THE
CONVERSATION
#ESPC24



Achieve More

WITH
MICROSOFT
365



59° 16' 43" N
18° 0' 55" E

Stockholm**24**

The most complex product in Azure?



Mastering Cloud Security: A Deep Dive into **Defender for Cloud** for IT Pros and Developers

PIERRE THOOR

CYBERSECURITY, ONEVINN, SWEDEN

Agenda

1

Defender for
Cloud
Overview

2

Securing
Hybrid
Environments

3

Enhancing
DevOps
Security

4

Protect ARM
Deployment

5

Best Practices
&
Key Learning

Demos



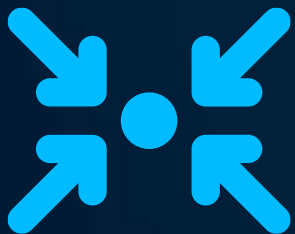
The importance of Cloud Security



Overview of Microsoft Defender for Cloud







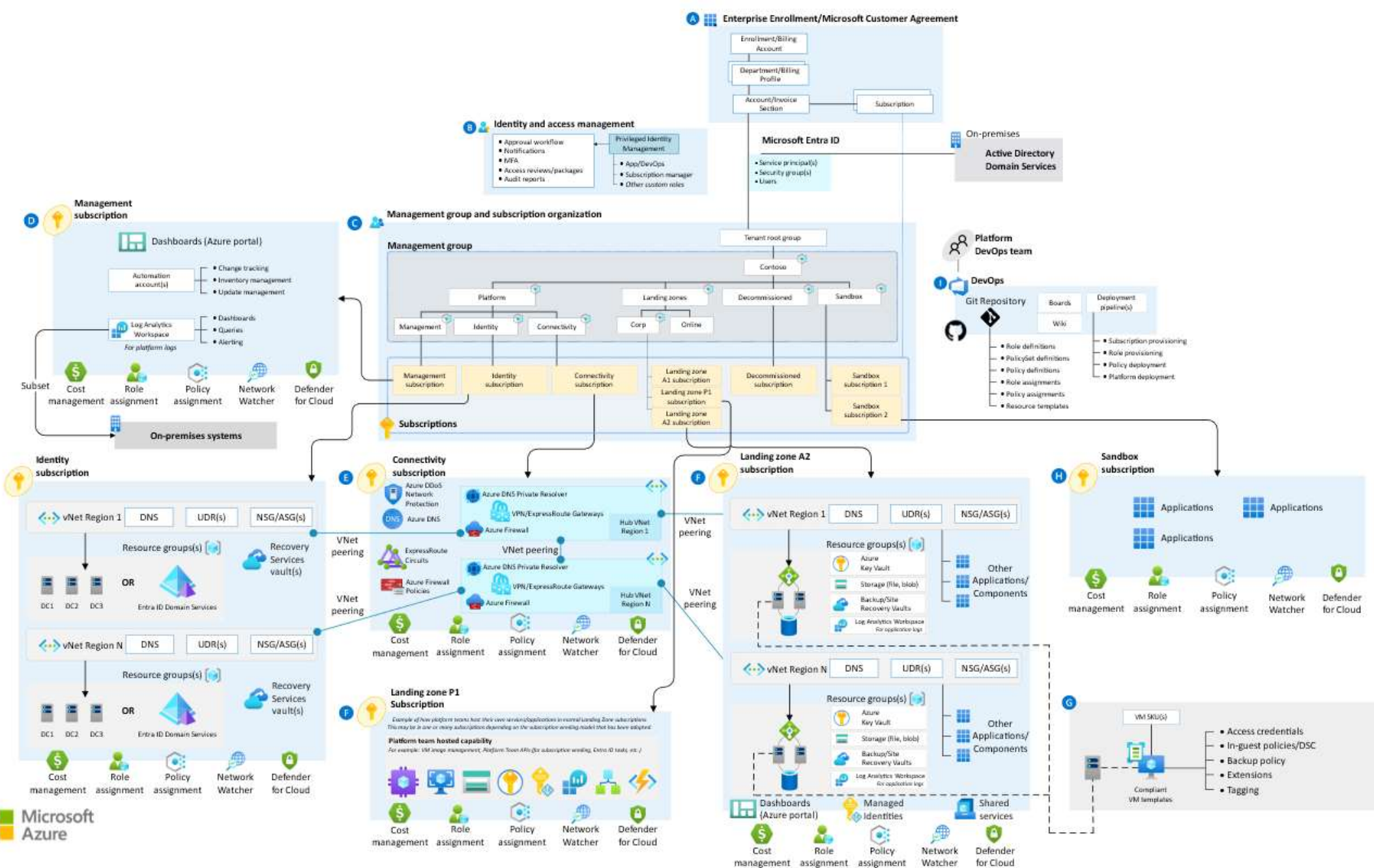
Align with Azure
Enterprise Scale
Landing Zone concept



Azure Policy
framework

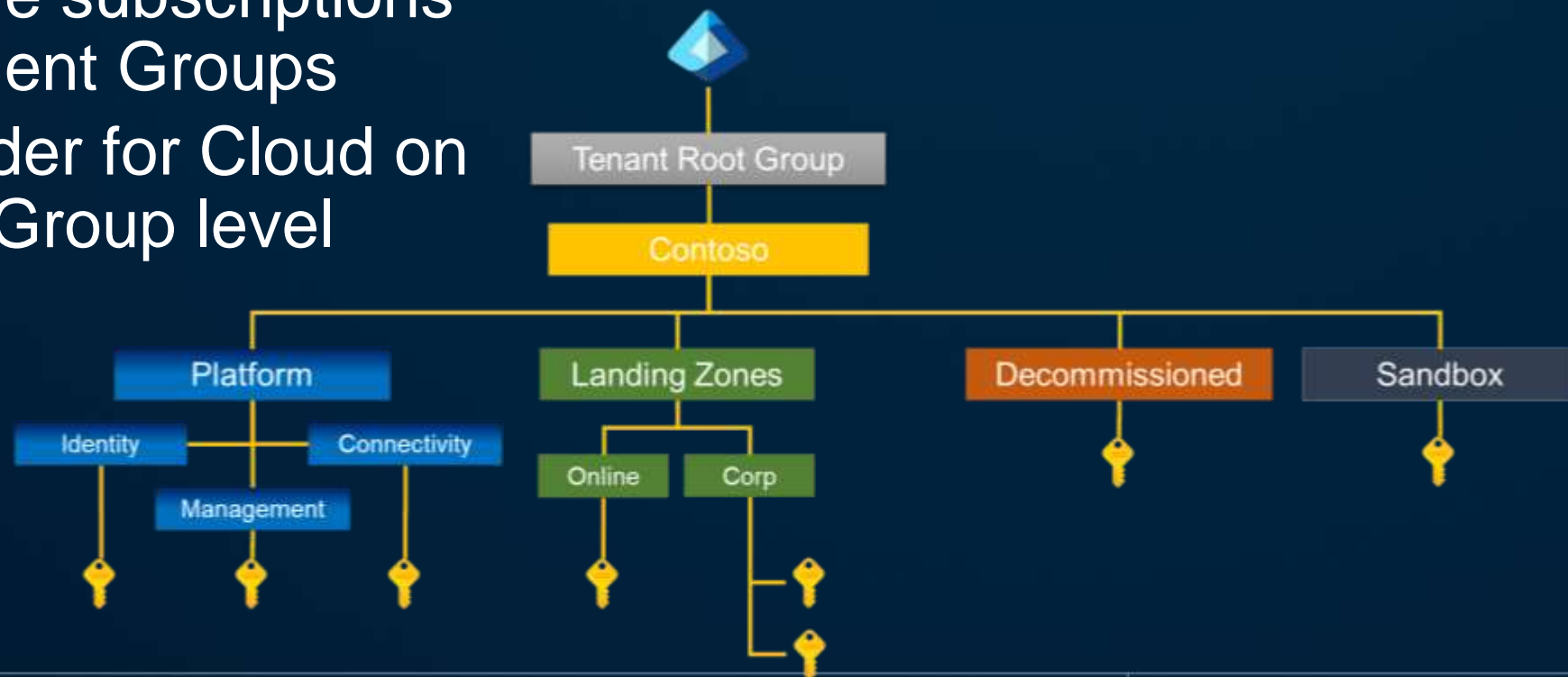


Integrate with
Defender XDR for
correlation purposes

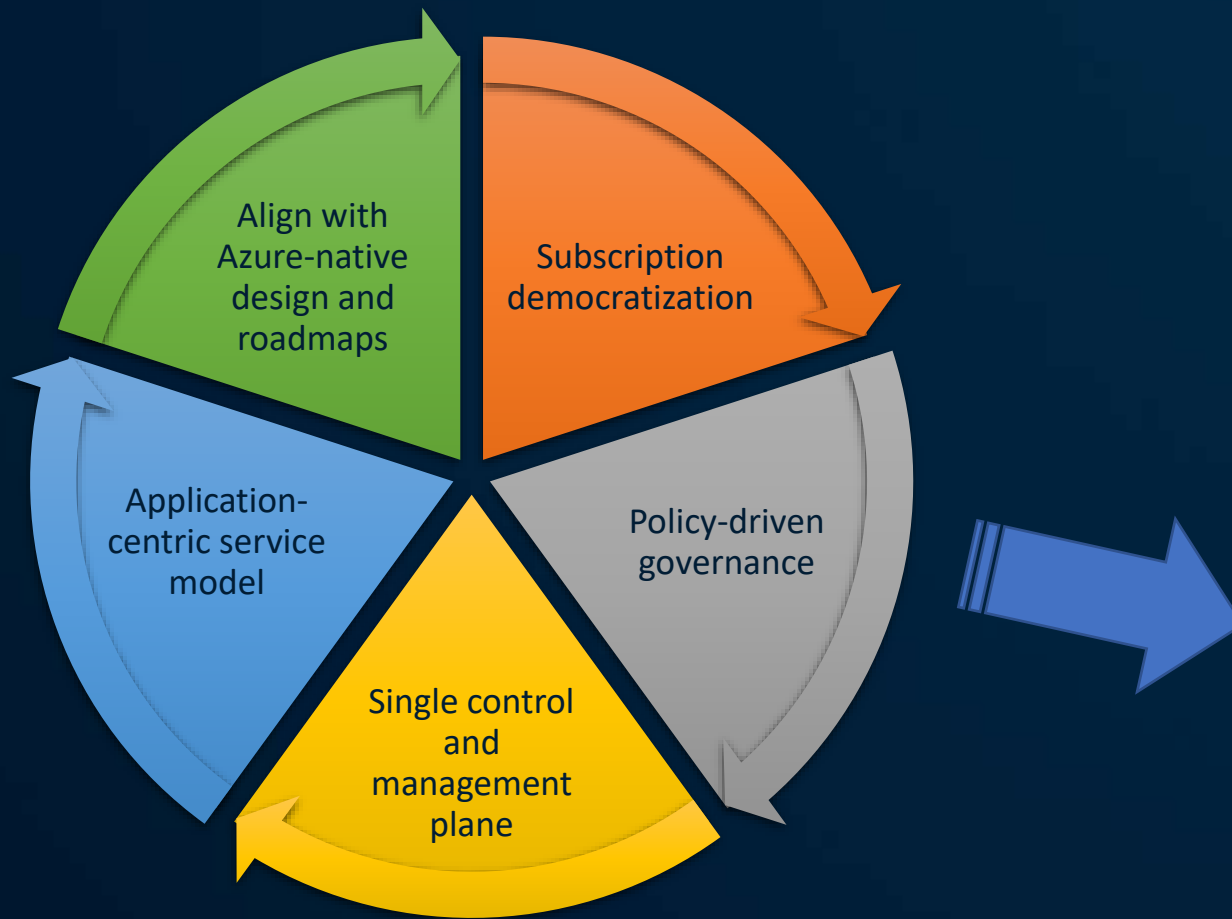


Prepare

- Azure Policy within Enterprise Scale implementation
 - Organize Azure subscriptions into Management Groups
 - Enable Defender for Cloud on Management Group level

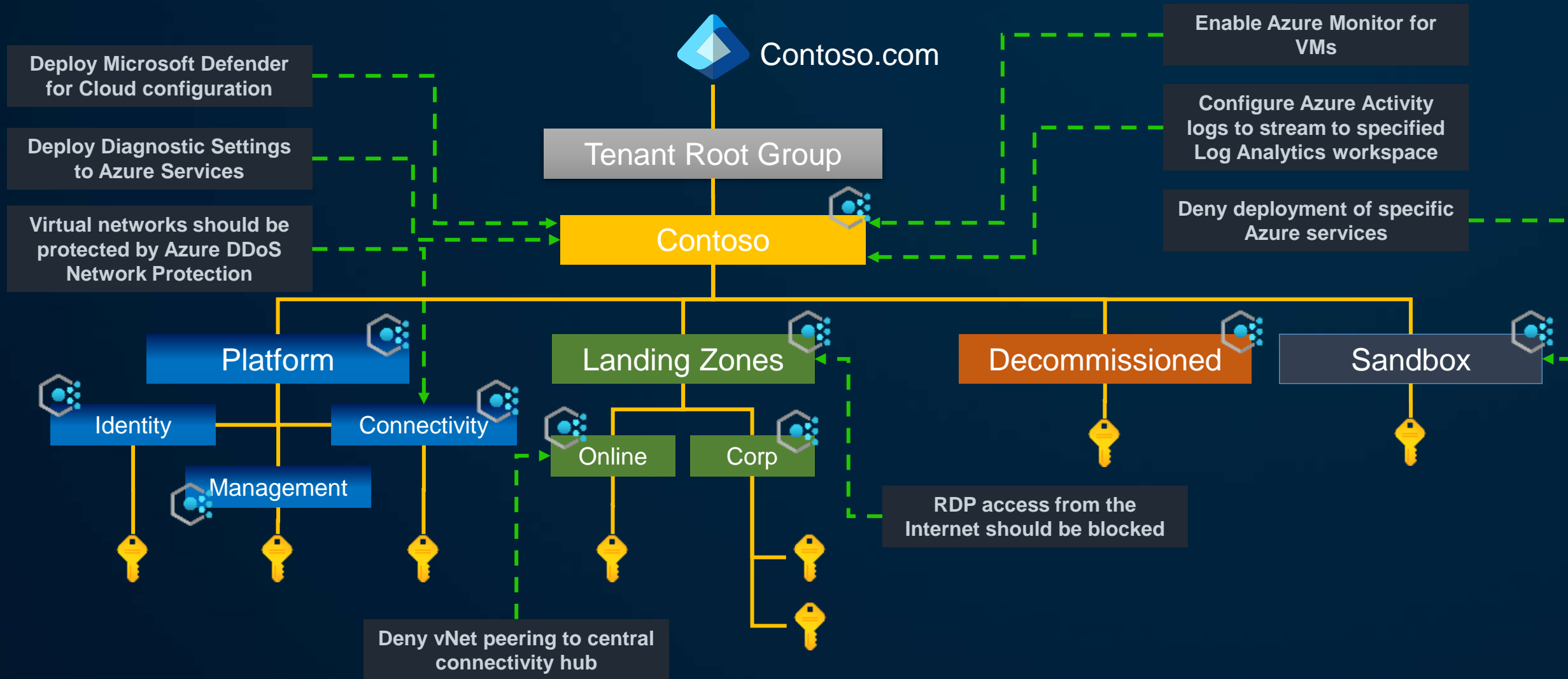


Design Principals



Azure Policy and `deployIfNotExist` enables autonomy in the platform, and reduces operational burden as you scale your deployments and subscriptions in the Azure landing zone architecture. The primary purpose is to ensure that subscriptions and resources are compliant, while empowering application teams to use their own preferred tools/clients to deploy.

Azure Policy (examples)



Prepare

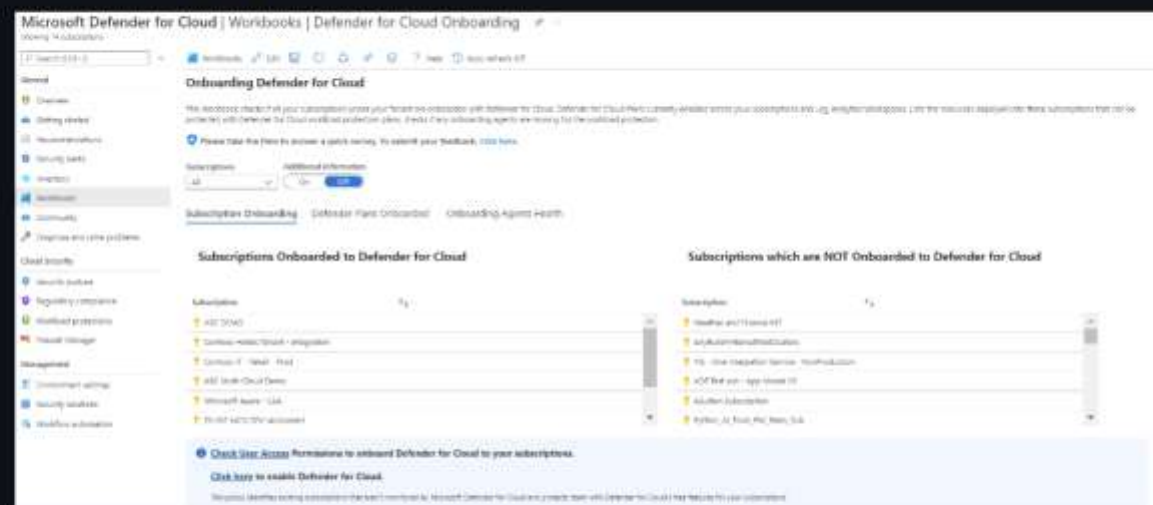
Defender for Cloud Onboarding Workbook

Author: Vasavi Pasula

This Onboarding Workbook checks if all your subscriptions under your Tenant are onboarded with Defender for Cloud, Defender for Cloud Plans currently enabled across your subscriptions and Log Analytics Workspaces, Lists the resources deployed into these subscriptions that can be protected with Defender for Cloud workload protection plans, checks if any onboarding agents are missing for the workload protection. The dashboard is powered by Azure Resource Graph (ARG) queries and divided into different sections. The workbook can be edited, and all queries can be modified to meet your needs.

The workbook provides different Tabs organized as:

- Subscription Onboarding
- Defender Plans Onboarded
- Onboarding Agents Health



Try it on the Azure Portal

You can deploy the workbook by clicking on the buttons below:



Checkout the blog [here](#) to learn more details about this workbook [here](#)



Edit | Auto refresh: Off

Onboarding Defender for Cloud

This Workbook checks if all your subscriptions under your Tenant are onboarded with Defender for Cloud, Defender for Cloud Plans currently enabled across your subscriptions and Log Analytics Workspaces, Lists the resources deployed into these subscriptions that can be protected with Defender for Cloud workload protection plans, checks if any onboarding agents are missing for the workload protection.

Please take the time to answer a quick survey. To submit your feedback, [click here](#).

Subscriptions

All

Additional information

On

Off

Subscription Onboarding

Defender Plans Onboarded

Onboarding Agents Health

Subscriptions Onboarded to Defender for Cloud

Search

Subscription

↑↓

- Visual Studio Enterprise Subscription – MPN
- (MCT) Visual Studio Enterprise Subscription
- Microsoft Azure Sponsorship
- (MVP) Visual Studio Enterprise Subscription
- Pay-As-You-Go
- (Onevinn) Visual Studio Enterprise-prenumeration –

Subscriptions which are NOT Onboarded to Defender for Cloud

The query returned no results.

[Check User Access](#) Permissions to onboard Defender for Cloud to your subscriptions.

[Click here](#) to enable Defender for Cloud.

This policy identifies existing subscriptions that aren't monitored by Microsoft Defender for Cloud and protects them with Defender for Cloud's free features for your subscriptions.

Defender Plans in your Subscriptions onboarded to Defender for Cloud

[DCSPM](#) [Servers](#) [API](#) [AppService](#) [Databases](#) [Storage](#) [Containers](#) [Key Vault](#) [Resource Manager](#) [DNS](#) [Devops](#) [AWS](#) [GCP](#)

This section provides an overview of all the onboarded subscriptions and their corresponding Defender plan status. Click the **on/off** status to be redirected to the subscription's Defender Plans page. Edit the plan status to **on/off** and click **'Save'** the settings to save your changes

Defender CSPM Status on Azure Subscriptions

Search						
Subscription	↑↓	Defender CSPM	↑↓	ResourceType	↑↓	DCSPMResources↑↓
🔑 (MVP) Visual Studio Enterprise Sub		Off		🖥️ Virtual machine		2
🔑 Microsoft Azure Sponsorship		On		🖥️ Virtual machine		14
🔑 Microsoft Azure Sponsorship		On		💾 Storage account		6

Agentless Capabilities

This section provides an overview of Defender plan status and the Agentless Capabilities. Click the **on/off** status to be redirected to the subscription's **Settings & monitoring** page. Edit the settings and click **'Continue'** and **'Save'** the settings to save your changes. **Not Available** indicates **Defender CSPM** plan is not enabled

Defender CSPM - Agentless Capabilities Status on Azure Subscriptions

Search

Subscription	↑↓	Defender CSPM	↑↓	AgentlessVmScanning	↑↓	SensitiveDataDiscovery	↑↓	ContainerRegistriesVA	↑↓	AgentlessDiscoveryForKub...↑↓
🔑 Visual Studio Enterprise Subscrip...		Off				Not Available		Not Available		Not Available
🔑 (MCT) Visual Studio Enterprise Sub		Off				Not Available		Not Available		Not Available
🔑 Microsoft Azure Sponsorship		On				On		On		On
🔑 (MVP) Visual Studio Enterprise Sub		Off				Not Available		Not Available		Not Available

Defender plan

N/A



Save



Settings & monitoring

Enable all plans

Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at \$15/Billable resource/month.

Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free Details >		Full	<input type="checkbox"/> On <input type="checkbox"/> Off
Defender CSPM	Based on subscription size, counting Compute and Data resources Defender CSPM is free until August 1st. When enabling Defender CSPM, automatic discount. Details >			<input type="checkbox"/> On <input checked="" type="checkbox"/> Off

Cloud Workload Protection (CWP)

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

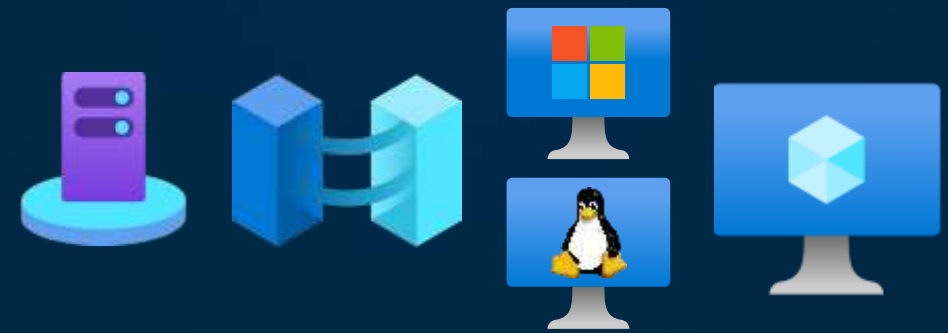
Plan	Pricing	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (\$15/Server/Month) ⓘ Change plan >	2 servers		<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
App Service	\$15/Instance/Month ⓘ Details >	0 instances		<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Databases	Selected: 0/4 ⓘ Select types >	Protected: 0/0 instances		<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Storage	\$10/Storage account/month On-upload malware scanning (\$0.15/GB) ⓘ Details >	0 storage accounts		<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Containers	\$7/VM core/Month ⓘ Details >	0 container registries; 0 kubernetes cores		<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
Key Vault	\$0.02/10k transactions Details >	0 key vaults		<input type="checkbox"/> On <input checked="" type="checkbox"/> Off

Only Subscription Owners can fully enable DCSPM



Securing Hybrid Environments with Azure Arc and Defender for Servers

Azure Arc lab with Azure VMs



Try out Azure Arc with simple steps:

- Set environment variable:
 - `[System.Environment]::SetEnvironmentVariable("MSFT_ARC_TEST", 'true', [System.EnvironmentVariableTarget]::Machine)`
- Remove all extensions from the Azure VM
 - `az vm extension list -g <rgName> --vm-name <vmName>`
 - `az vm extension delete -g <rgName> --vm-name <vmName> -n <extensionName>`
- Disable Azure VM guest agent
 - `Set-Service WindowsAzureGuestAgent -StartupType Disabled -Verbose`
 - `Stop-Service WindowsAzureGuestAgent -Force -Verbose`
- Firewall settings:
 - `New-NetFirewallRule -Name BlockAzureIMDS -DisplayName "Block access to Azure IMDS" -Enabled True -Profile Any -Direction Outbound -Action Block -RemoteAddress 169.254.169.254`
- Install **Azure Arc connected machine agent** via script, GPO or with other tooling

Attacks from Azure

- Custom Script Extensions
 - Run command

Attacks inside VM

- Mimikatz
- Atomic Red

DEMO



MITRE ATT&CK Framework

1. Reconnaissance
2. Resource Development
3. Initial Access
- 4. Execution**
5. Persistence
6. Privilege Escalation
7. Defense Evasion
8. Credential Access
9. Discovery
10. Lateral Movement
11. Collection
12. Command and Control
13. Exfiltration
14. Impact





Secure the Azure Arc agent

```
azcmagent config set incomingconnections.enabled false
```

```
azcmagent config set guestconfiguration.enabled false
```

```
azcmagent config set extensions.allowlist  
"Microsoft.Azure.Monitor/AzureMonitorWindowsAgent, Microsoft.  
Azure.AzureDefenderForServers/MDE.Windows"
```

Enhancing DevOps Security with Defender for DevOps

**I'm a developer and want to deploy
some Azure resources**

Feature	Foundational CSPM	Defender CSPM	Prerequisites
Connect Azure DevOps repositories	✓	✓	
Security recommendations to fix code vulnerabilities	✓	✓	GitHub Advanced Security for Azure DevOps for CodeQL findings, Microsoft Security DevOps extension
Security recommendations to discover exposed secrets	✓	✓	GitHub Advanced Security for Azure DevOps (\$49 per month per active committer)
Security recommendations to fix open source vulnerabilities	✓	✓	GitHub Advanced Security for Azure DevOps (\$49 per month per active committer)
Security recommendations to fix infrastructure as code misconfigurations	✓	✓	Microsoft Security DevOps extension (free extension from Marketplace) or Microsoft Security DevOps action
Security recommendations to fix DevOps environment misconfigurations	✓	✓	N/A
Pull request annotations		✓	
Code to cloud mapping for Containers		✓	Microsoft Security DevOps extension (free extension from Marketplace)
Code to cloud mapping for Infrastructure as Code templates		✓	Microsoft Security DevOps extension (free extension from Marketplace)
Attack path analysis		✓	Enable Defender CSPM on an Azure Subscription in the same tenant as the DevOps Connector
Cloud security explorer		✓	Enable Defender CSPM on an Azure Subscription in the same tenant as the DevOps Connector

Microsoft Security DevOps GitHub action

1 Trivy



2 Checkov



3 Template Analyzer





Spot the misconfiguration

...

```
resource webApp 'Microsoft.Web/sites@2020-06-01' = {  
  name: appName  
  location: location  
  kind: 'app'  
  properties: {  
    httpsOnly: false  
    serverFarmId: appServicePlan.id  
  }  
}
```

...

DEMO



MITRE ATT&CK Framework

1. Reconnaissance



2. Resource Development

3. Initial Access

4. Execution

5. Persistence

6. Privilege Escalation

7. Defense Evasion

8. Credential Access

9. Discovery

10. Lateral Movement

11. Collection

12. Command and Control

13. Exfiltration

14. Impact

**I'm an application owner and want
to deploy some Azure resources**

Thinking about?



SECURITY



ALIGNMENT



COST
OPTIMIZATION



**As the owner of the
subscription, you are
! RESPONSIBLE !**

DEMO



MITRE ATT&CK Framework

1. Reconnaissance
2. Resource Development
3. Initial Access
4. Execution
5. Persistence



6. Privilege Escalation

7. Defense Evasion
8. Credential Access



9. Discovery

10. Lateral Movement



11. Collection

12. Command and Control
13. Exfiltration
14. Impact

Cloud Security Posture Management: Defender CSPM

Microsoft Sentinel (SIEM) & Defender XDR

CSPM

- Find misconfigurations
- Get compliance issues
- Find security threats in our cloud environment

Correlation and integration

Incidents > Hands-on keyboard attack was launched from a compromised account (attack disruption)

Hands-on keyboard attack was launched from a compromise...

[Manage incident](#) [Tasks](#) ...

High | Active | Unassigned | Ransomware | Lateral Movement | Attack Disruption

Important! A potentially compromised account was contained automatically by attack disruption in Microsoft Defender XDR. For more details, select the Assets > Users tab or go to the [Action center](#).

[Attack story](#) Alerts (62) Assets (5) Investigations (6) Evidence and Response (97) Summary

Alerts

[Play attack story](#)[Unpin all](#) [Show all](#)

- Nov 12, 2024 1:29 PM Resolved
Mimikatz credential theft tool
entraconnect0.contoso.local localadmin
- Nov 12, 2024 2:22 PM New
Suspicious Microsoft Defender Antivirus exclusion
entraconnect0.contoso.local
- Nov 12, 2024 2:22 PM New
Suspicious Microsoft Defender Antivirus exclusion
entraconnect0.contoso.local
- Nov 12, 2024 2:27 PM New
Compromised account conducting hands-on-keyboard attack
entraconnect0.contoso.local localadmin

[View incident details](#)

Incident graph

[Layout](#)☒ Group similar nodes

— Communication Association

Microsoft Sentinel | Data connectors

Selected workspace: 'thoorsentinel-v2'


Refresh Guides & Feedback

 **17**
Onboarded Connectors

 **13**
Connected

 **0**
Updates

 More content at
Content hub

 Search by name or provider

Providers : **All**

Data Types : **All**

Status : **All**



Security Events via Legacy Agent
Microsoft

Solution
Windows Security Events

...



Subscription-based Microsoft Defender for Cloud (Legacy)
Microsoft

Solution
Microsoft Defender for Cloud

...



Syslog via Legacy Agent
Microsoft

Solution
Syslog

...



Tenant-based Microsoft Defender for Cloud (Preview)
Microsoft

Solution
Microsoft Defender for Cloud

...



Threat intelligence - TAXII
Microsoft

Solution
Threat Intelligence

...



Threat Intelligence Platforms - BEING DEPRECATED (Prev...

Solution

...

Microsoft Sentinel | Data connectors

Selected workspace: 'thoorsentinel-v2'

Refresh Guides & Feedback

17
Onboarded Connectors

13
Connected

0
Updates

More content at
Content hub

Search by name or provider

Providers : All

Data Types : All

Status : All



Security Events via Legacy Agent
Microsoft

Solution
Windows Security Events



Subscription-based Microsoft Defender for Cloud (Legacy)
Microsoft

Solution
Microsoft Defender for Cloud



Syslog via Legacy Agent
Microsoft

Solution
Syslog



Tenant-based Microsoft Defender for Cloud (Preview)
Microsoft

Solution
Microsoft Defender for Cloud



Threat intelligence - TAXII
Microsoft

Solution
Threat Intelligence



Threat Intelligence Platforms - BEING DEPRECATED (Prev...

Solution

Best practices

(yes, we need to lean into something)

Guidelines/Best practices



ENTERPRISE
SCALE
LANDING
ZONES



AZURE
POLICY
FRAMEWORK



TIERING IN
AZURE



SECURITY
FIRST



DO NOT
EXPOSE
AZURE
RESOURCES

Do you think that MDC is the most
complex product in Azure?

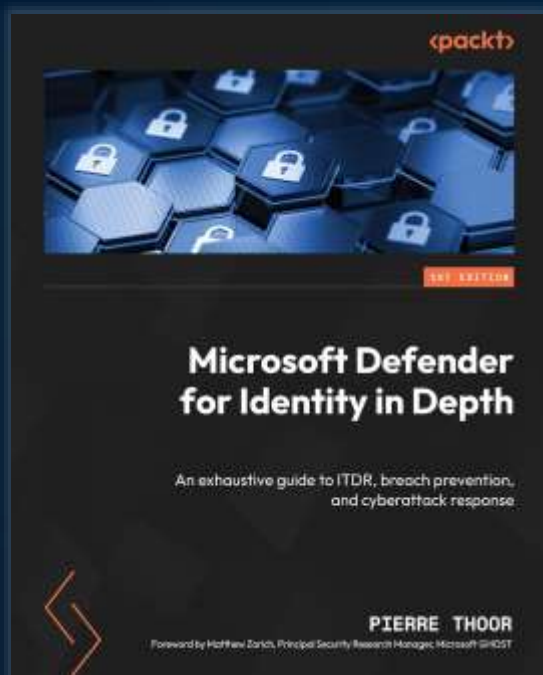
Key learning

- Defender for Cloud is **MASSIVE** and **COMPLEX**
- Continuous monitoring and visibility **IS** crucial
- Integrate **security** early in the development, no more **misconfigurations**
- Help the SecOps team in **understanding your environment** better
- Participate in proactive **threat hunting** sessions with SecOps
- Having an **Incident Response plan** at hand



<https://github.com/pthoor/ESPC24>

Thank you!



Pierre Thoor



pierrethoor.bsky.social



Microsoft Defender for Identity in Depth
available from 20th December



<https://thoor.tech>

onevinn



Please rate
this session
on the app

