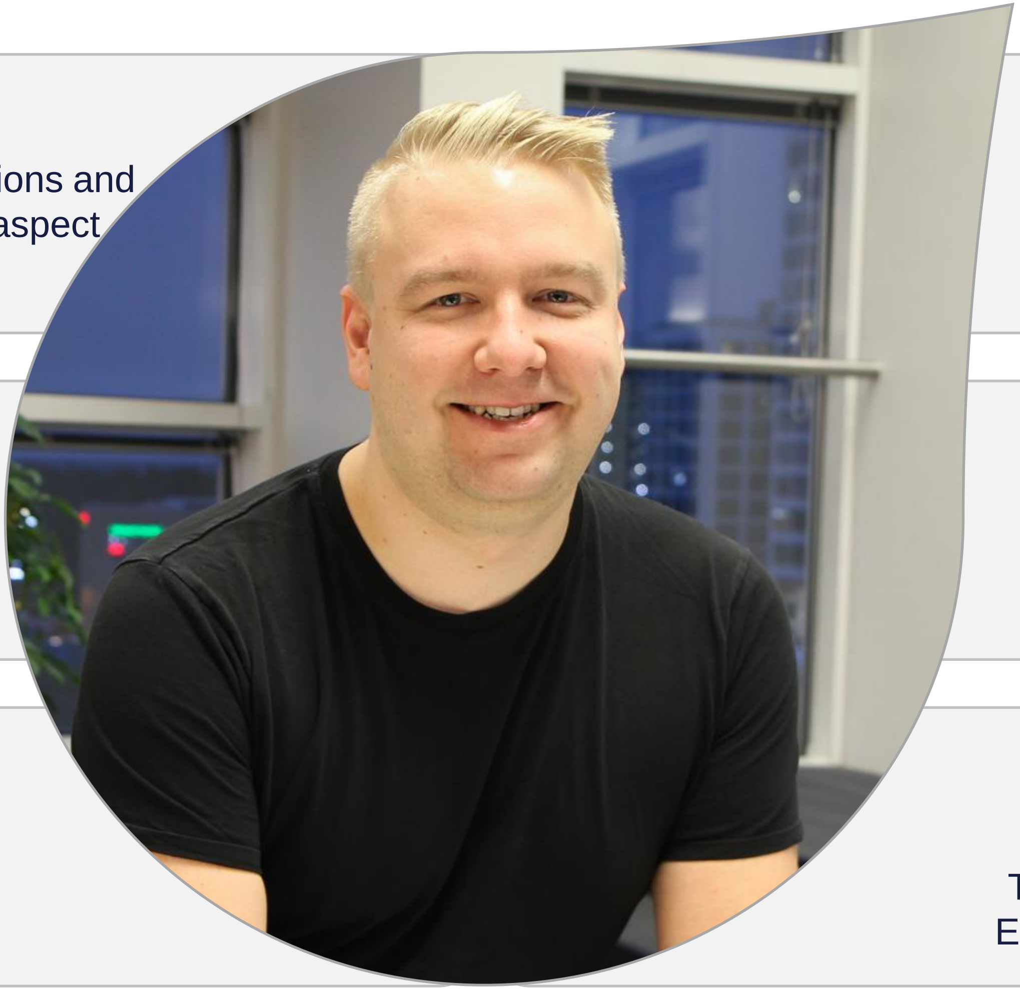
Governing Defender for Cloud in Multicloud

6.10.2022 Markus Lintuala

A SUSTAINABLE
FUTURE THROUGH
DIGITALISATION

Markus Lintuala



Focus

Public and hybrid cloud solutions and architectures with a security aspect

Elisa Oyj

Senior Technical Consultant

Blog

https://bloggerz.cloud

Certifications

Yep, some of those

Hobbies

IT, Aviation, Food

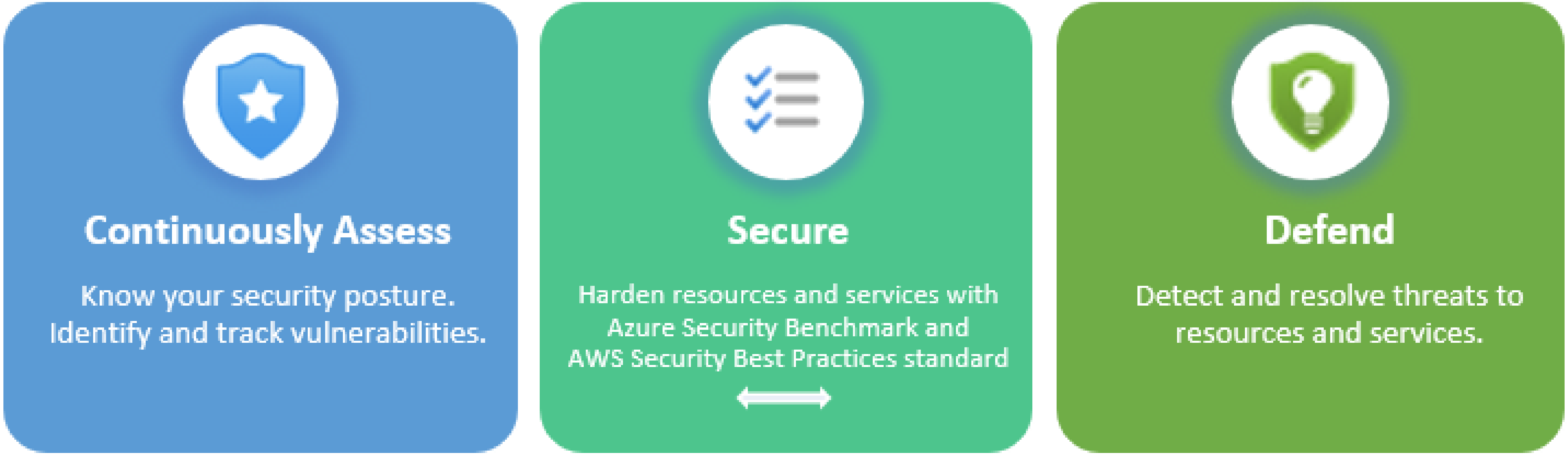
Contact

LinkedIn: lintuala
Twitter: @MarkusLintuala
E-mail: markus@lintuala.fi

Agenda

- What is Microsoft Defender for Cloud
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP)
- How to deploy…
  - Azure subscription?
  - AWS account?
  - GCP project?
- Managing CSPM recommendations
- Microsoft Sentinel Connection
- Manage through API
- Q&A

What is Microsoft Defender for Cloud



Continuously Assess

Know your security posture.
Identify and track vulnerabilities.

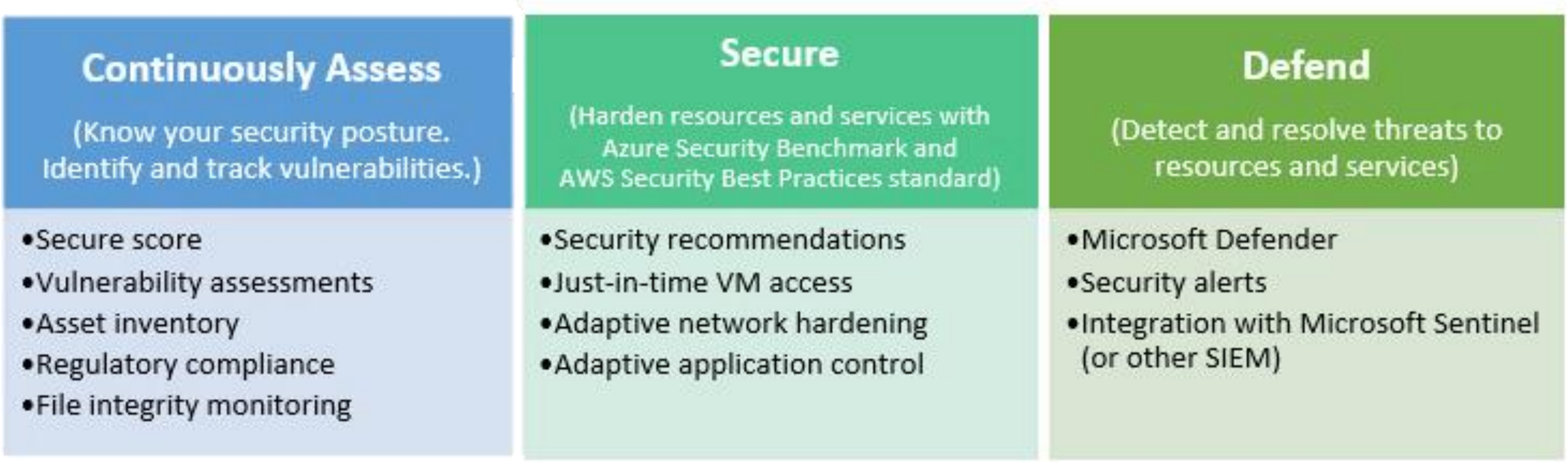
Secure

Harden resources and services with
Azure Security Benchmark and
AWS Security Best Practices standard

Defend

Detect and resolve threats to
resources and services.

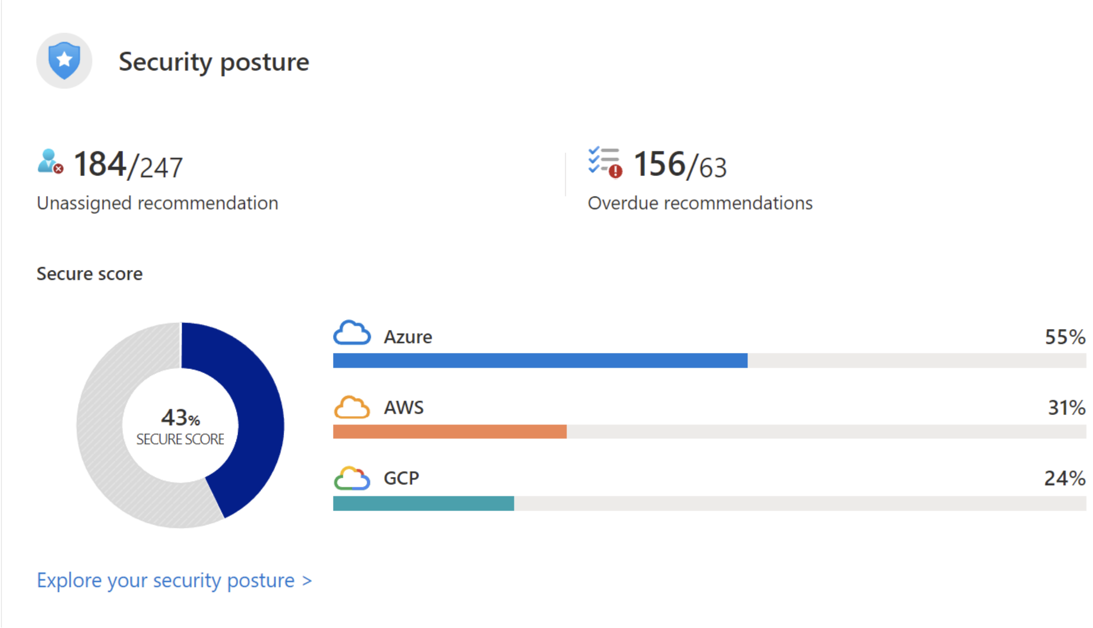
What is Microsoft Defender for Cloud



Continuously Assess	Secure	Defend
(Know your security posture. Identify and track vulnerabilities.)	(Harden resources and services with Azure Security Benchmark and AWS Security Best Practices standard)	(Detect and resolve threats to resources and services)
•Secure score •Vulnerability assessments •Asset inventory •Regulatory compliance •File integrity monitoring	•Security recommendations •Just-in-time VM access •Adaptive network hardening •Adaptive application control	•Microsoft Defender •Security alerts •Integration with Microsoft Sentinel (or other SIEM)

Cloud Security Posture Management (CSPM)

- See your current cloud security situation against configurations
- Measured with a secure score
- Lists recommendations on resource level
- Recommendations has a weighted values that relates to Security score
- You can add your own policies, but those are not counted towards a secure score



Security posture

184/247
Unassigned recommendation

156/63
Overdue recommendations

Secure score

43% SECURE SCORE

Azure 55%

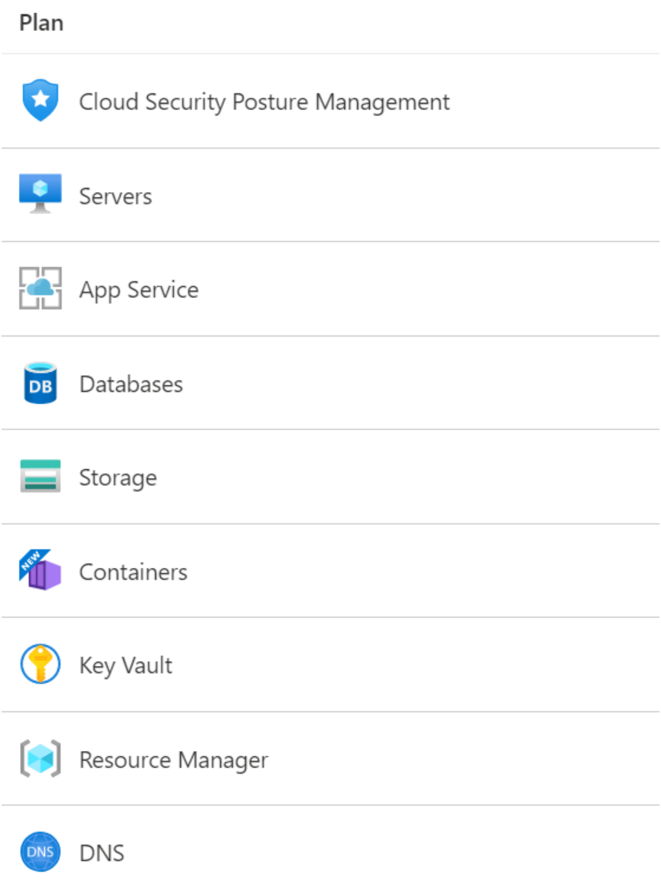
AWS 31%

GCP 24%

Explore your security posture >

Cloud Workload Protection Platform (CWPP)

- Deeper insight for each IaaS and PaaS services
- Only way to increase security in your PaaS resources
- Many enhanced features which protects your infrastructure
- Costs per resource



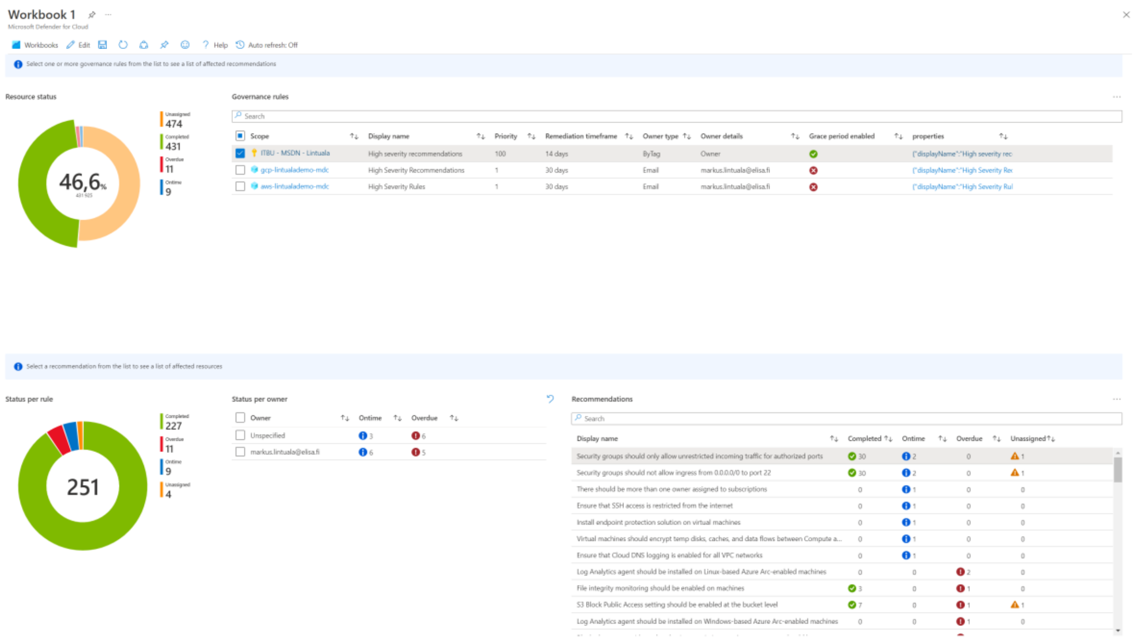
Plan
Cloud Security Posture Management
Servers
App Service
Databases
Storage
Containers
Key Vault
Resource Manager
DNS

How to deploy…

- Azure subscription?
- AWS account?
- GCP project?

Managing CSPM recommendations

- Group by applications!
- Solve recommendations from resource group point of view
- User Defender for Cloud governance tool (or your own processes) to follow-up recommendation fixing process



Select one or more governance rules from the list to see a list of affected recommendations

Resource status

Governance rules

Search

☐	Scope	Display name	Priority	Remediation timeframe	Owner type	Owner details	Grace period enabled	properties
☑	ITBU - MSDN - Lintuala	High severity recommendations	100	14 days	ByTag	Owner	✓	{"displayName":"High severity rec
☐	gcp-lintualademo-mdc	High Severity Recommendations	1	30 days	Email	markus.lintuala@elisa.fi	✗	{"displayName":"High Severity Rec
☐	aws-lintualademo-mdc	High Severity Rules	1	30 days	Email	markus.lintuala@elisa.fi	✗	{"displayName":"High Severity Rul

Select a recommendation from the list to see a list of affected resources

Status per rule

Status per owner

☐	Owner	Ontime	Overdue
☐	Unspecified	3	6
☐	markus.lintuala@elisa.fi	6	5

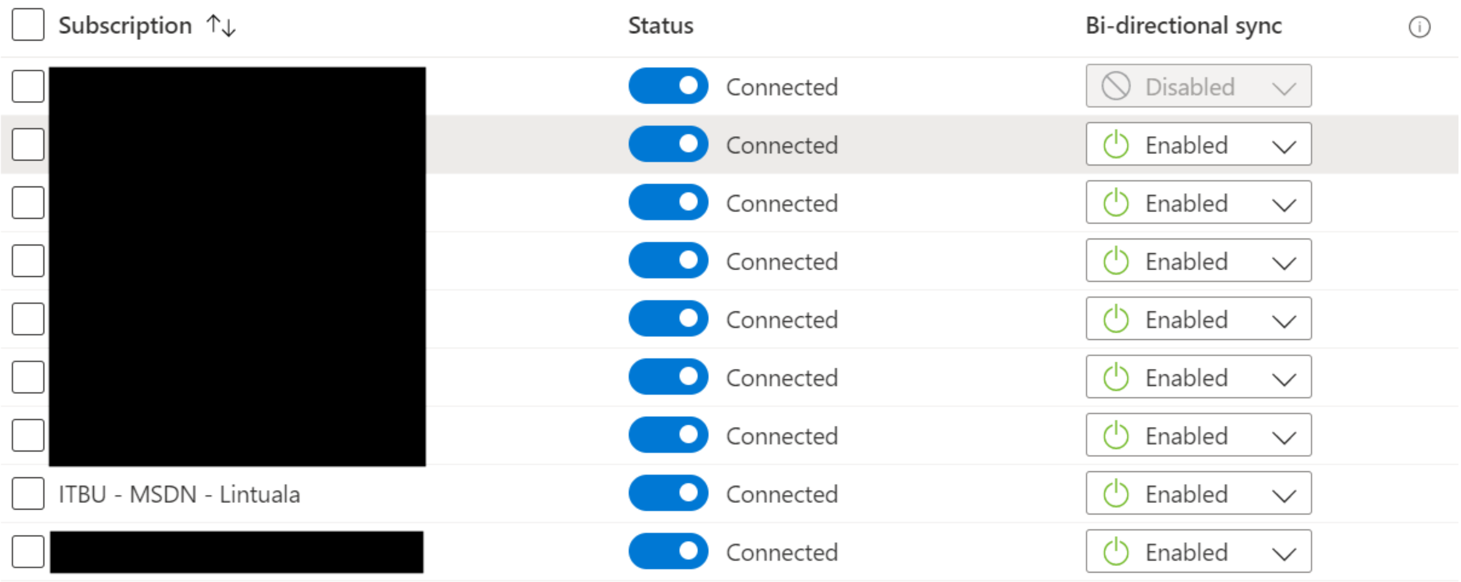
Recommendations

Search

Display name	Completed	Ontime	Overdue	Unassigned
Security groups should only allow unrestricted incoming traffic for authorized ports	30	2	0	1
Security groups should not allow ingress from 0.0.0.0/0 to port 22	30	2	0	1
There should be more than one owner assigned to subscriptions	0	1	0	0
Ensure that SSH access is restricted from the internet	0	1	0	0
Install endpoint protection solution on virtual machines	0	1	0	0
Virtual machines should encrypt temp disks, caches, and data flows between Compute a...	0	1	0	0
Ensure that Cloud DNS logging is enabled for all VPC networks	0	1	0	0
Log Analytics agent should be installed on Linux-based Azure Arc-enabled machines	0	0	2	0
File integrity monitoring should be enabled on machines	3	0	1	0
S3 Block Public Access setting should be enabled at the bucket level	7	0	1	1
Log Analytics agent should be installed on Windows-based Azure Arc-enabled machines	0	0	1	0

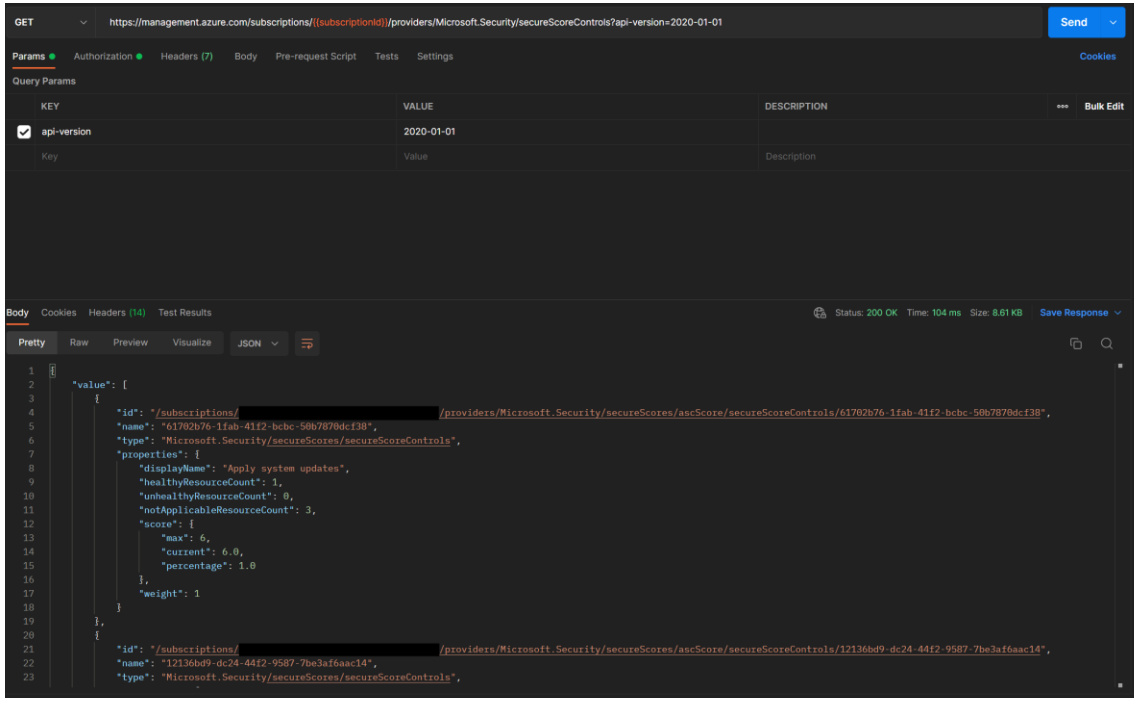
Microsoft Sentinel Connection

- Add new data connector *Microsoft Defender for Cloud* from Microsoft Sentinel
- Bi-directional alert sync available
- Turn it on!



□	Subscription ↑↓	Status	Bi-directional sync ⓘ
□	[redacted]	Connected	Disabled
□	[redacted]	Connected	Enabled
□	[redacted]	Connected	Enabled
□	[redacted]	Connected	Enabled
□	[redacted]	Connected	Enabled
□	[redacted]	Connected	Enabled
□	[redacted]	Connected	Enabled
□	ITBU - MSDN - Lintuala	Connected	Enabled
□	[redacted]	Connected	Enabled

Manage through API



GET https://management.azure.com/subscriptions/{{subscriptionId}}/providers/Microsoft.Security/secureScoreControls?api-version=2020-01-01

Query Params

	KEY	VALUE	DESCRIPTION
☑	api-version	2020-01-01	
	Key	Value	Description

Status: 200 OK Time: 104 ms Size: 8.61 KB

```
{
    "value": [
        {
            "id": "/subscriptions/[redacted]/providers/Microsoft.Security/secureScores/ascScore/secureScoreControls/61702b76-1fab-41f2-bcbc-50b7870dcf38",
            "name": "61702b76-1fab-41f2-bcbc-50b7870dcf38",
            "type": "Microsoft.Security/secureScores/secureScoreControls",
            "properties": {
                "displayName": "Apply system updates",
                "healthyResourceCount": 1,
                "unhealthyResourceCount": 0,
                "notApplicableResourceCount": 3,
                "score": {
                    "max": 6,
                    "current": 6.0,
                    "percentage": 1.0
                },
                "weight": 1
            }
        },
        {
            "id": "/subscriptions/[redacted]/providers/Microsoft.Security/secureScores/ascScore/secureScoreControls/12136bd9-dc24-44f2-9587-7be3af6aac14",
            "name": "12136bd9-dc24-44f2-9587-7be3af6aac14",
            "type": "Microsoft.Security/secureScores/secureScoreControls",
```

- Pretty good API-documentation
- Follows Azure’s REST API architecture
- Easy to integrate for your own services or dashboards or where ever
- Microsoft Defender for Cloud REST APIs | Microsoft Learn

Q & A

Thanks!

Slides available
@cloud/PublicSpeaking/AzureAndFriends at main · mmaraa/cloud (github.com)