



Azure Sentinel



MKDOCS



Azure DevOps



GitHub

Microsoft Sentinel

Czy SaaS jest możliwy?

Mateusz Czerniawski



Arcontar

SOC as a Code



SOC as a Code



Cost
reduction



Faster
execution



Reduce
human error



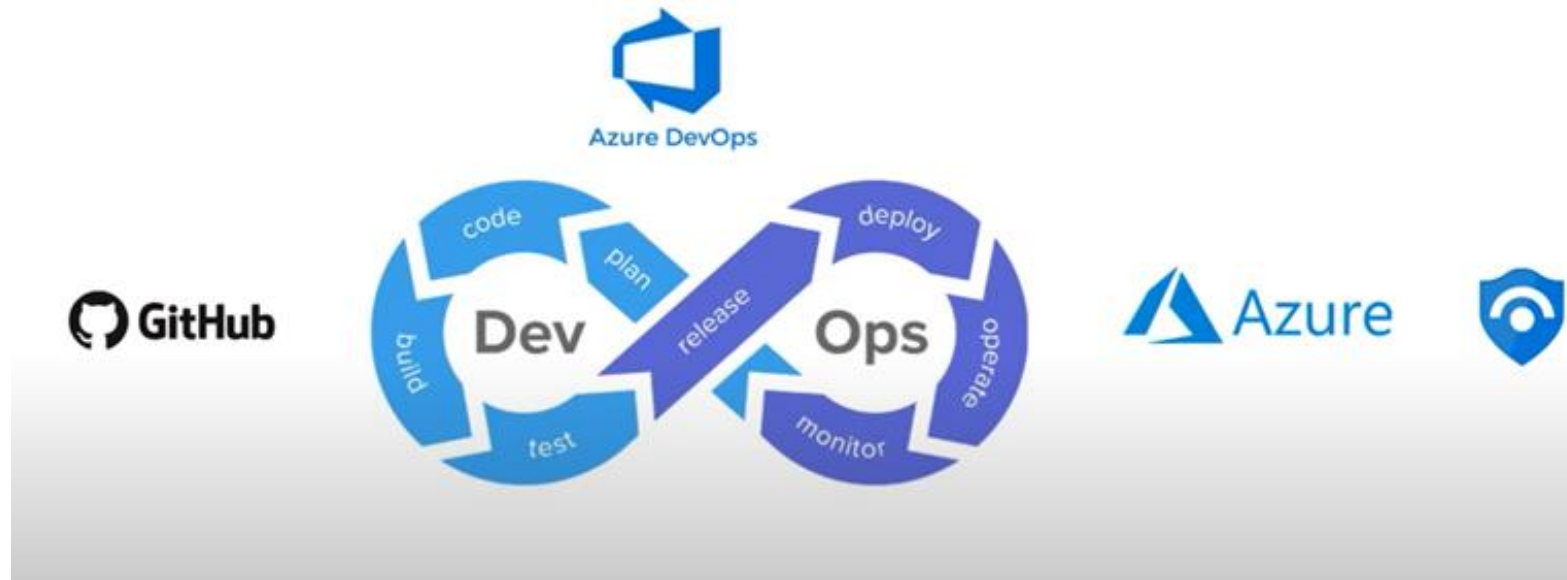
Change
management



Enhanced
Security

SOC as a Code

Azure Sentinel As Code – Prototype



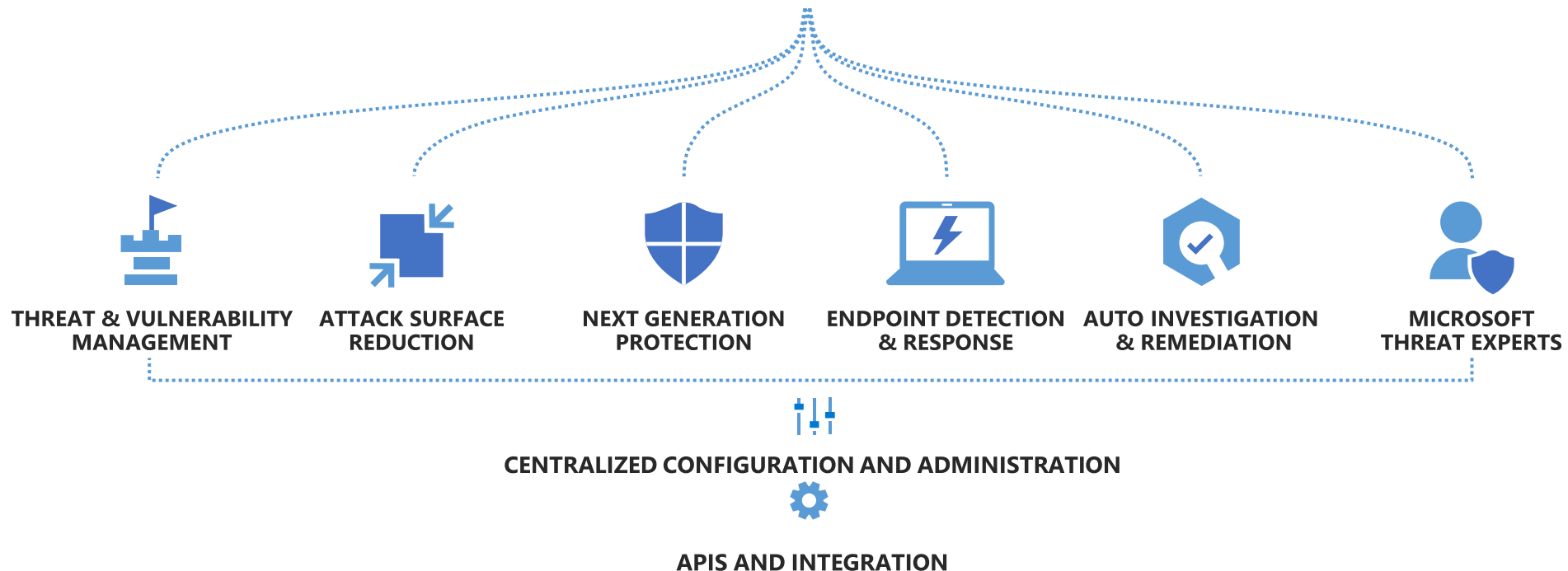
Agenda

- Intro to Sentinel
- Deploy and Manage Sentinel as Code
 - Challenges with at scale management
- Automating Sentinel Components
 - The good, the bad and the ugly
 - Promise of SaaC[™] 😊 delivered?
- Bonus - Documentation as Code (DaaC)
- Demo
- Q&A

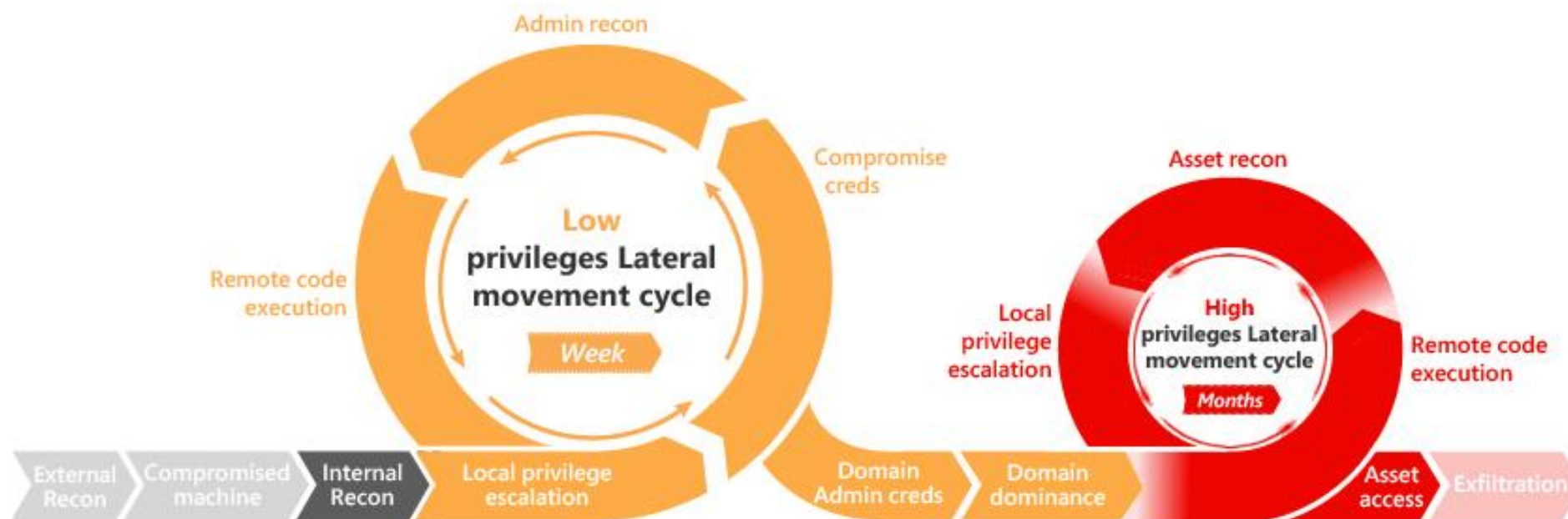
Anti-Malware



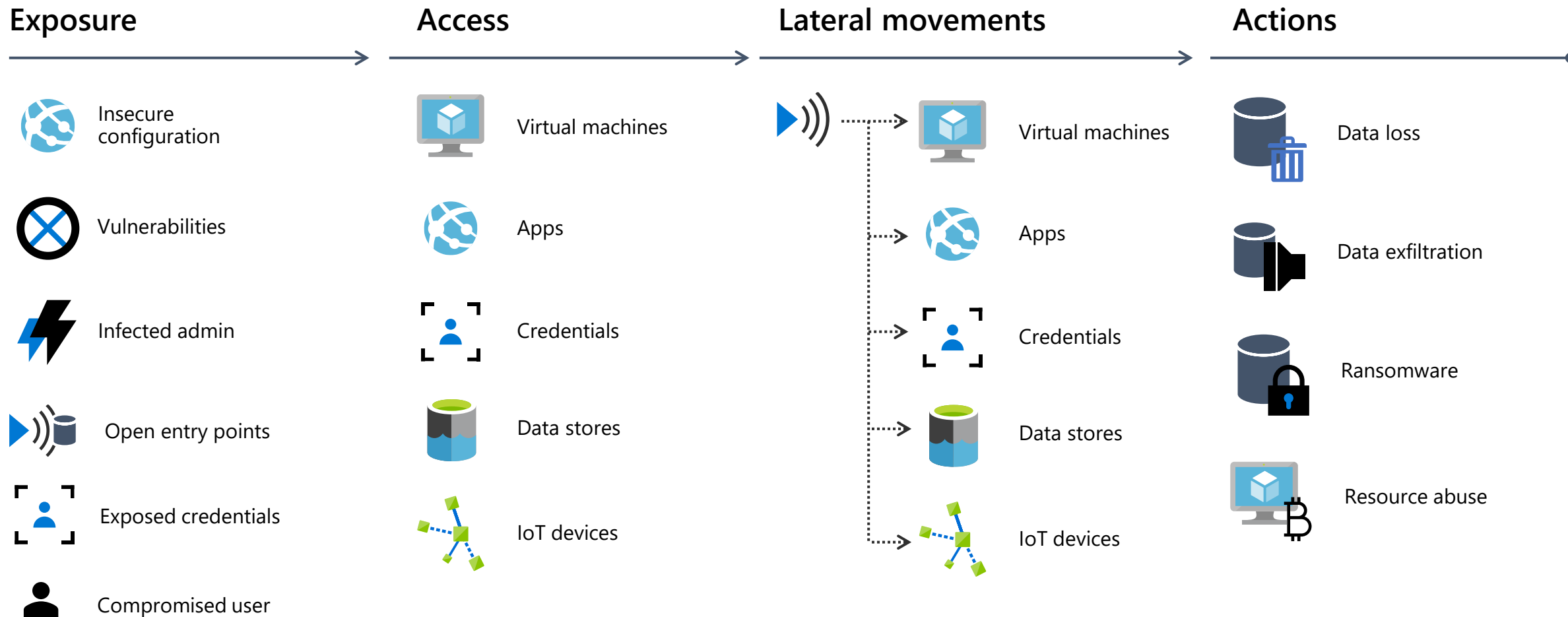
Microsoft Defender for Endpoint



Kill chain attack



The cloud kill chain model



Mitre ATT&CK

Reconnaissance

10 techniques

Resource Development

7 techniques

Initial Access

9 techniques

Execution

12 techniques

Persistence

19 techniques

Privilege Escalation

13 techniques

Defense Evasion

40 techniques

Credential Access

15 techniques

Discovery

29 techniques

Lateral Movement

9 techniques

Collection

17 techniques

Command and Control

16 techniques

Exfiltration

9 techniques

Impact

13 techniques

Challenges with at scale management

- Working with multiple Azure Sentinel environments
 - Multi-workspace scenarios
 - Geolocation, compliance requirements, customer engagement
 - Multi-tenant environments
 - Dev/Test/Prod environments
 - Multiple SOC's
- Different team capabilities
 - SOC, Threat hunters, Data Engineers, Blue/Red/Purple Teams, Developers
- Auditing and documenting

GitOps – Definition & Principles



Git as the source of truth for a system



Git as the single place where we operate (create, change, and delete)



All changes are observable



System state described declaratively



State declaration versioned in source control



Approved changes are applied automatically



Agents enforce desired state

Sentinel Demo



The Good, the Bad and the Ugly

- How it began
 - Deploy Sentinel environment with code:
 - <https://github.com/javiersoriano/sentinelascode>
 - <https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/deploying-and-managing-microsoft-sentinel-as-code/ba-p/1131928>

The Good, the Bad and the Ugly

Deploy Sentinel environment with code:

Powershell Module AzSentinel - <https://github.com/wortell/AZSentinel>

Component	Automated with
Onboarding	API, Powershell, ARM
Alert Rules	API, Powershell
Hunting Queries	API, Powershell
Playbooks	ARM
Workbooks	ARM
Connectors	API

The Good, the Bad and the Ugly

YAML all the way

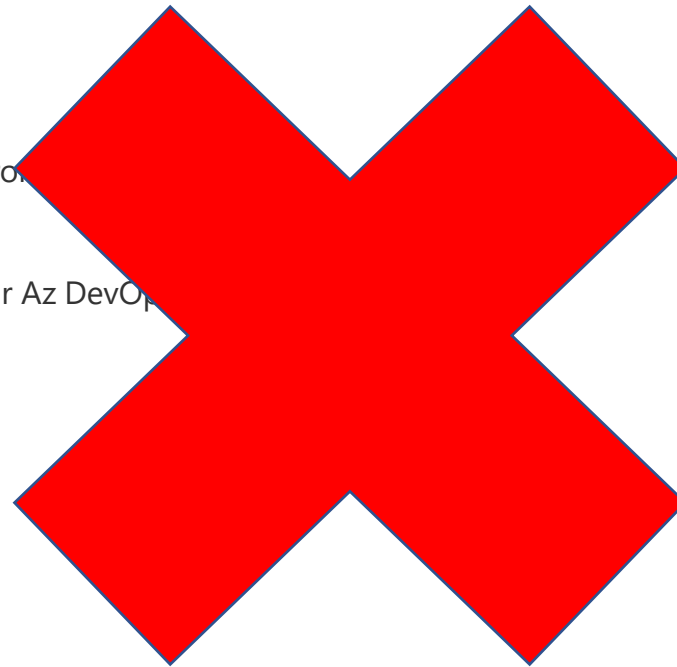
YAML:

- **Y** : *Yelling*
- **A** : *At*
- **M** : *My*
- **L** : *Laptop*


The Good, the Bad and the Ugly


Sentinel as Code in Azure DevOps


- Create an Azure DevOps organization
- Create a project in Azure DevOps
- Create a service connection to your Azure environment
- Create variables
- Connect your existing code repository with your Az DevOps
- Create pipelines



A better way?

 **Microsoft Sentinel**
Selected workspace: 'la-prod'

 Refresh

 **Arc-Sentinel**
Name

Azure DevOps Source control	15 minutes ago Last updated
--------------------------------	--------------------------------


Description
--


Repository
https://dev.azure.com/Arc-Sentinel/Sentinel/_git/Sentinel


Branch
main


Deployment logs
https://dev.azure.com/Arc-Sentinel/319fee3f-0f3b-422f-81a9-58289b7287a5/_build?definitionId=1


Content types ⓘ


 Analytics rules

 Hunting queries

 Workbooks

 Automation rules

 Parsers

 Playbooks

review)

This is the Way!


- Access to a GitHub or Azure DevOps repository
- An Owner role in the resource group that contains your Microsoft Sentinel workspace
- (undocumented yet) Third party application access via OAuth
 - [https://dev.azure.com/{{orgName}}/ settings/organizationPolicy](https://dev.azure.com/{{orgName}}/settings/organizationPolicy)

Policies

Application connection policies



On

Third-party application access via OAuth 

This is the Way!

- How it began
 - Deploy Sentinel environment with code:
 - <https://github.com/javiersoriano/sentinelascode>
 - <https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/deploying-and-managing-microsoft-sentinel-as-code/ba-p/1131928>
- How it's going
 - Microsoft Sentinel in Repositories
 - <https://docs.microsoft.com/en-us/azure/sentinel/ci-cd>

This is the Way!



- GitHub jump-start content with unified Microsoft Sentinel and Microsoft 365 Defender repository

<https://github.com/Azure/Azure-Sentinel/>

<https://github.com/Azure/Azure-Sentinel-Notebooks>

Automating Sentinel Components



Analytics rules



Hunting queries



Playbooks



Automation rules



Parsers







Workbooks

Sentinel Documentation

- Jupyter Notebooks
- Azure Static Web Page
- OneNote
- Sharepoint / Content Management Systems

Sentinel Documentation

- Jupyter Notebooks

- Requires Machine Learning -    
- Perform custom analytics (with some Python machine learning features)
- Create data visualizations (i.e. custom timelines and process trees)
- Integrate data sources outside of Microsoft Sentinel (i.e. an on-premises data set)

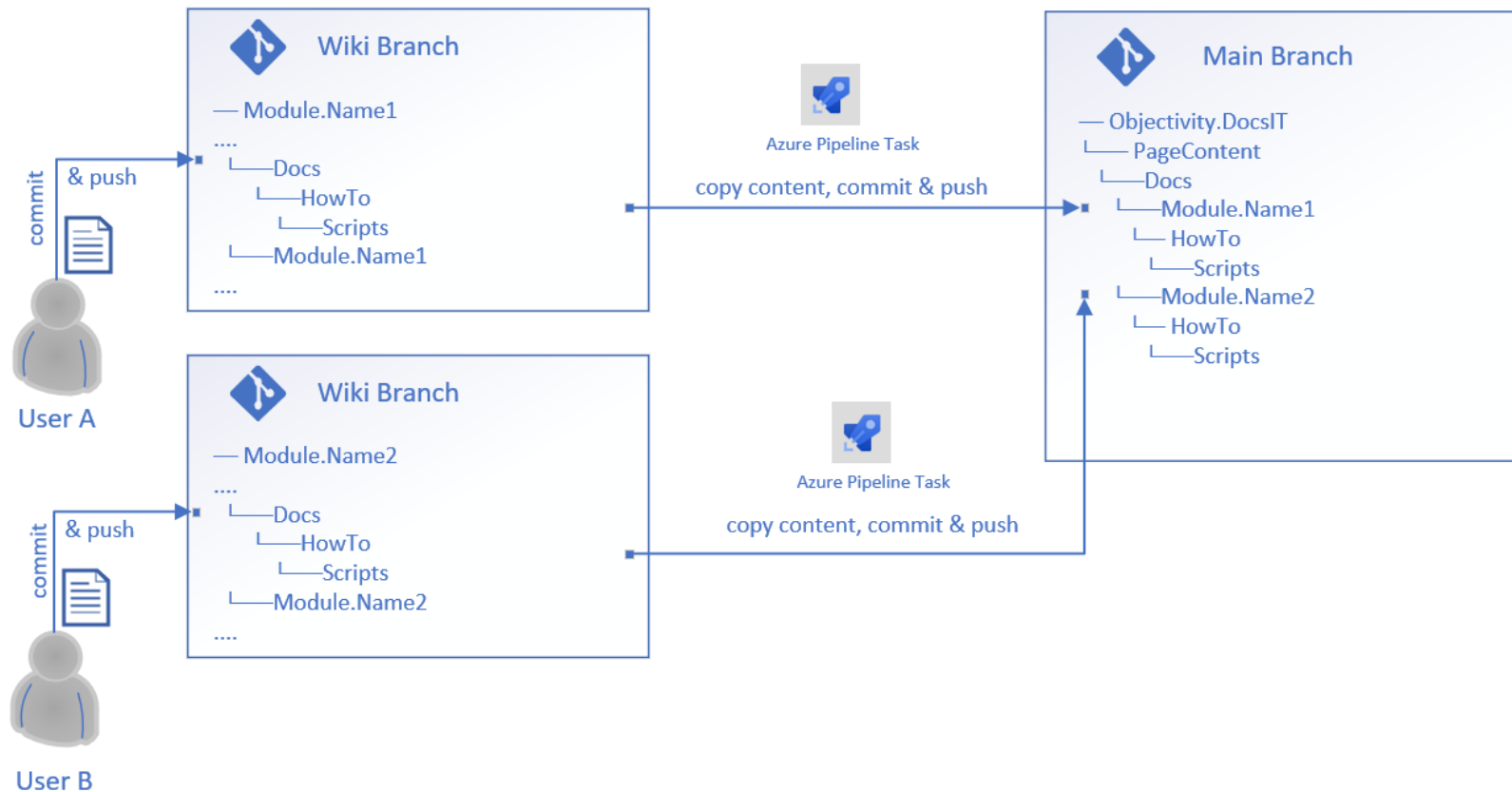
<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

Azure 'Docs'

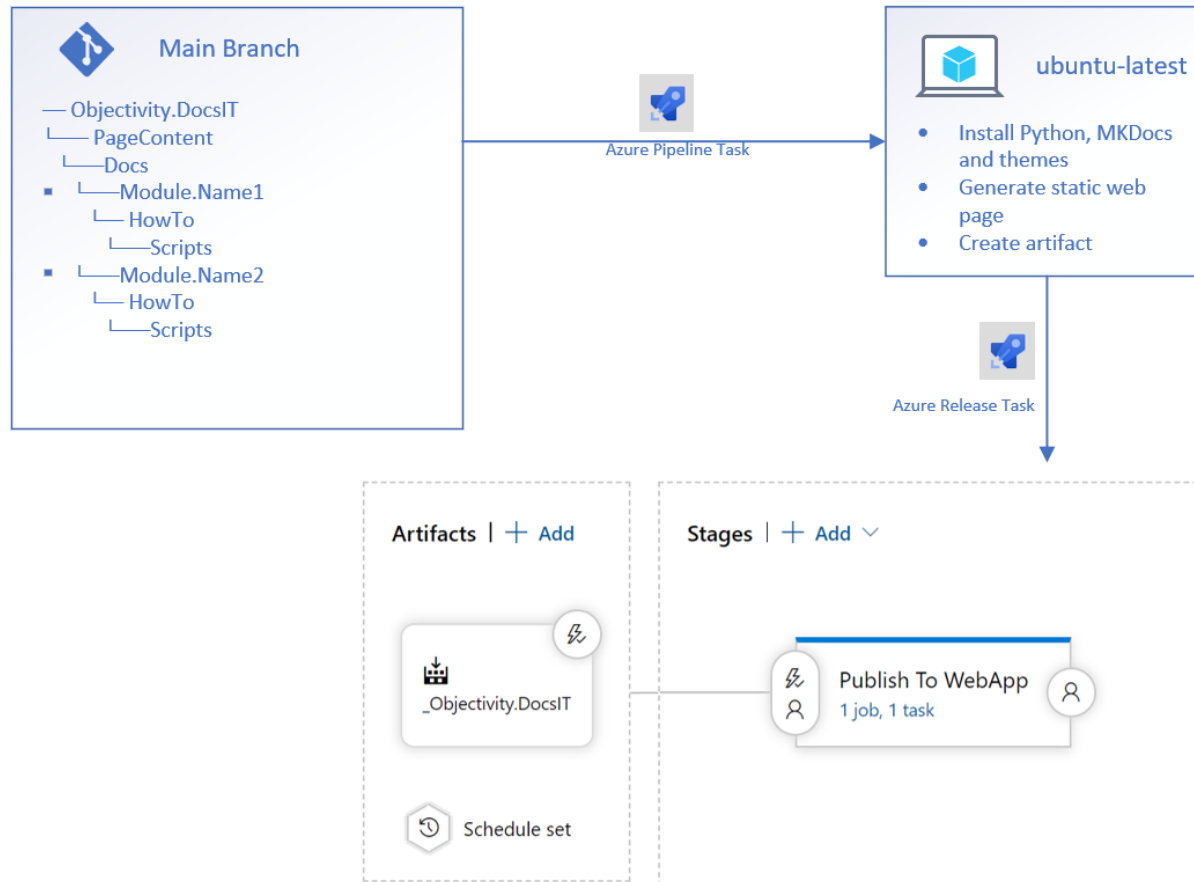
- Static WebPage
 - Low cost 💰
 - Easy to use - MKDocs (MarkdownMonster / VSCode/ NodePad++, Edge)
 - Automated (Azure DevOps Pipelines)
 - Secure - Azure WebApp (+ Azure AD)
- More details: PSConfBook3 - <https://leanpub.com/psconfbook3>

Azure Docs

5

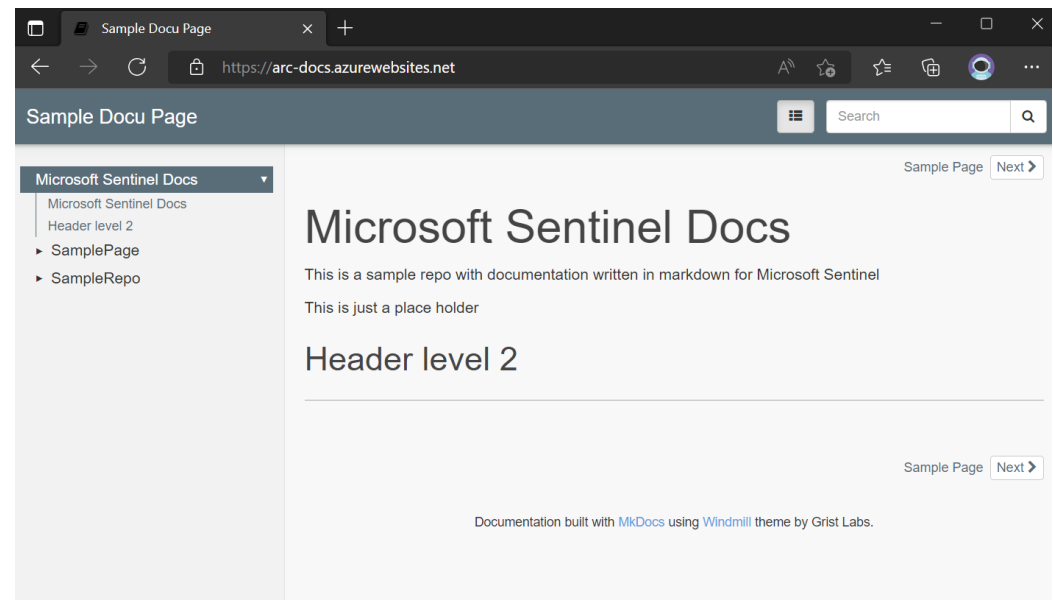
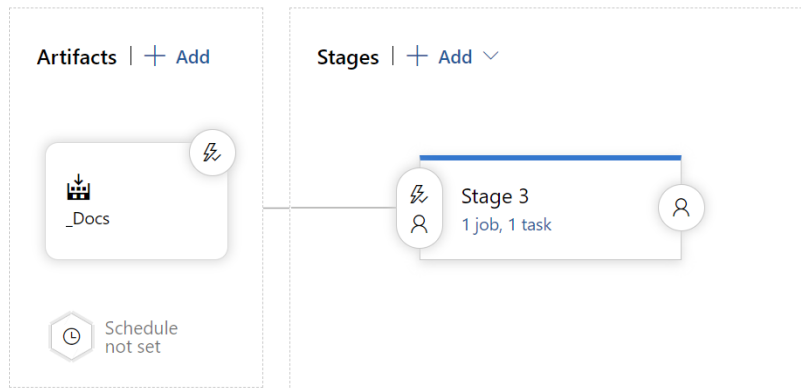


Azure Docs

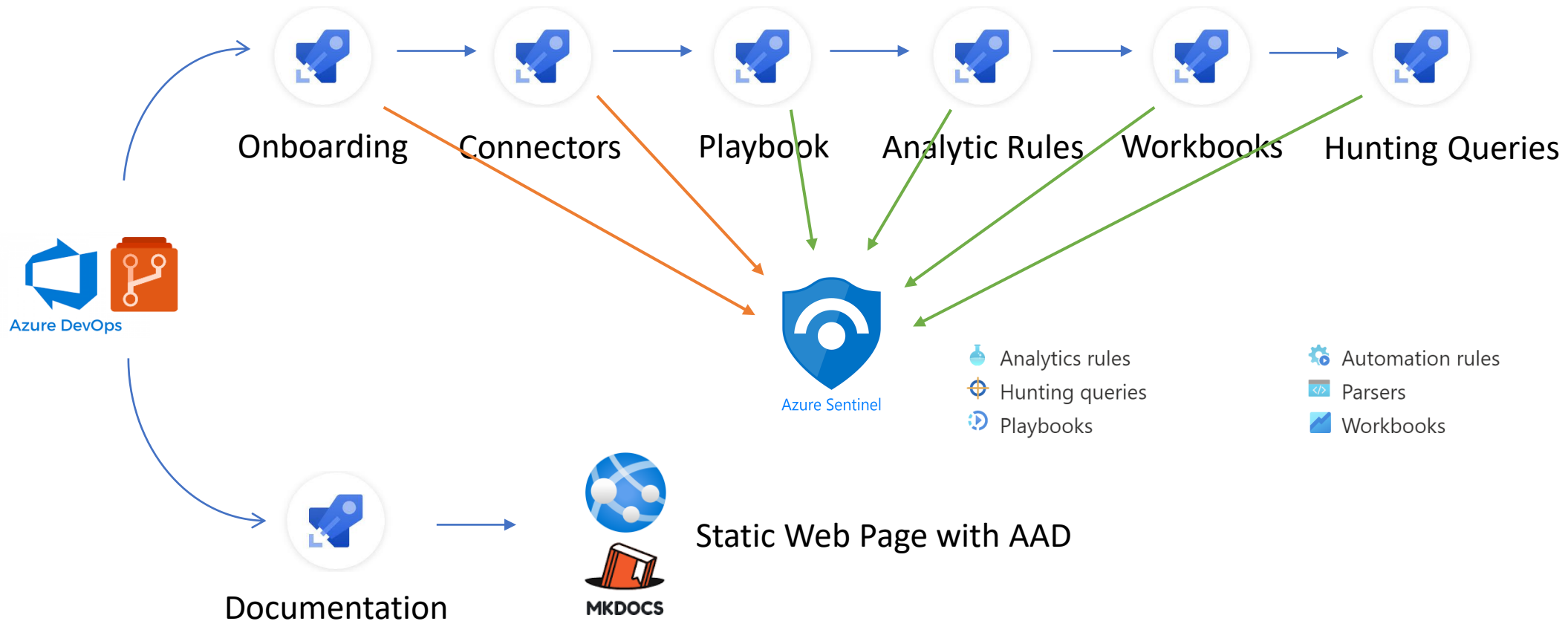


Azure Docs

- Modify the deployment path
- Add docs folder and deployment yaml
- Create static web app
- Create pipeline and release



Megazord Pipeline



Demo



Thank you

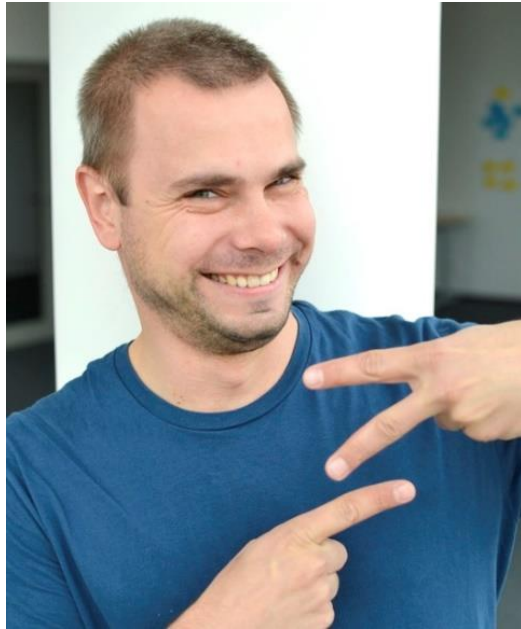
SysOps/DevOps Polska MeetUp Online #55



Questions



about_Speaker



Mateusz Czerniawski - MVP

Arcontar



mczerniawski@arcon.net.pl



[@Arcontar](https://twitter.com/Arcontar)



www.mczerniawski.pl



[mczerniawski](https://github.com/mczerniawski)

