



# Setup a Security Risk Management System with Microsoft Sentinel, Defender and Teams

Robert Mulsow  
AI Enterprise Architect

# Sponsors

---

**FEITIAN**  
WE BUILD SECURITY

glueck  kanja

 q.beyond

 VISORIAN

# Session Roadmap

1. Context: Microsoft App Compliance
2. Process Flow
3. Product Configurations



## Microsoft 365 App Compliance Program

*This new integration will certainly provide important assistance in closing larger deals as the initial certification of becoming Microsoft 365 Certified has already proven, with a +100k subscription deal we recently closed.*

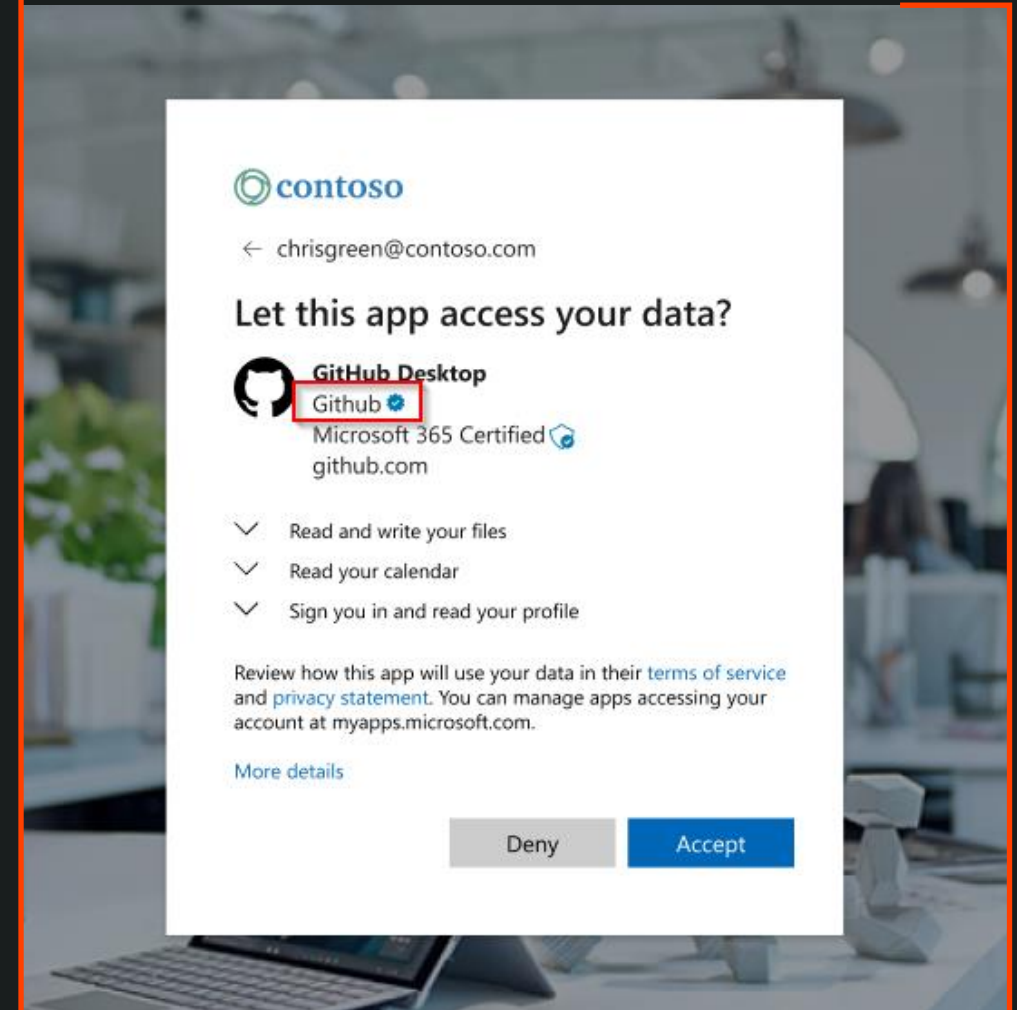
**MARTIN SEIFERT**  
CEO at officeatwork

# The App Dilemma

Excessive Privilege Requirements


Data Handling & Security

Operational Security Hygiene



# Microsoft App Compliance - Program Overview




 Verified app publisher authenticity

*Supports apps that leverage OAuth 2.0 and OpenID Connect with the Microsoft identity platform*

 Attestation  
Accessible app security & compliance info

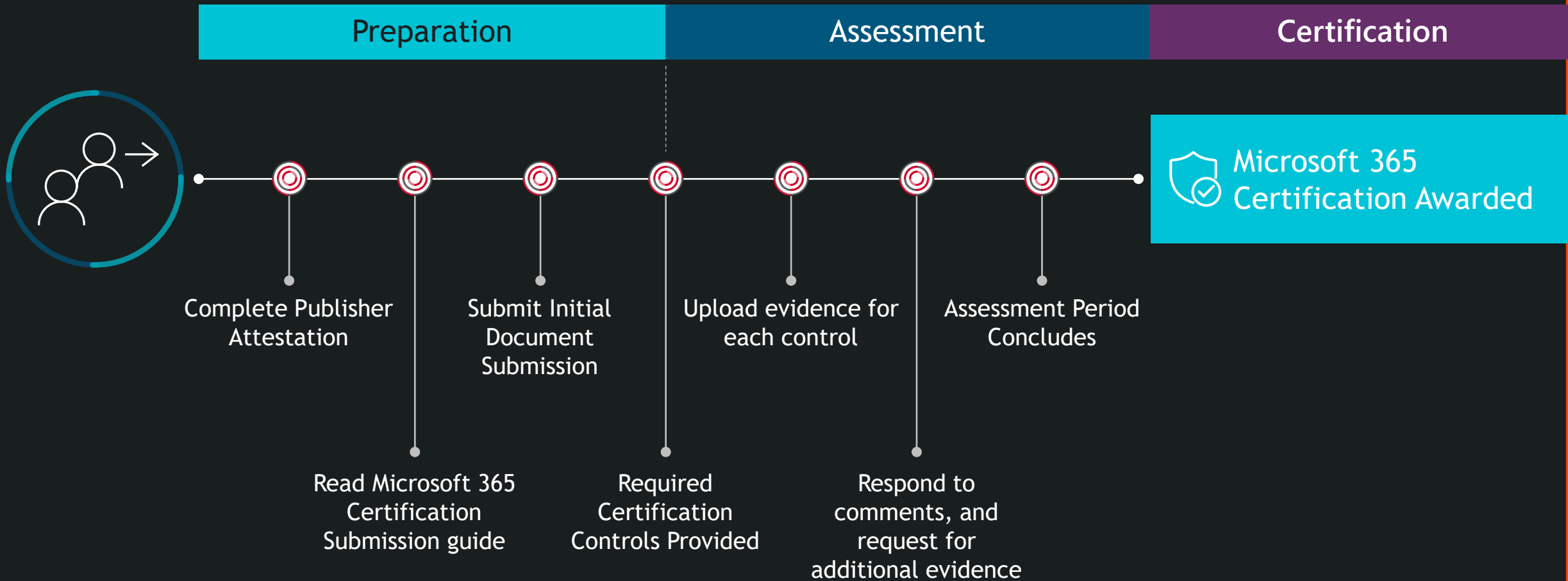
*Supports:*

- Teams apps
- M365 Apps (Word, Excel, PowerPoint, Outlook, SharePoint, OneNote, Project)
- SaaS (Web Apps which are published through Partner Center)

 Certification  
Rigorous app security audit



# Microsoft App Compliance - Certification Process



# Microsoft App Compliance - Security Domains



## Application Security

Penetration Testing  
& Review



## Operational Security

Anti-Malware, Patch  
Management,  
Incident Response,  
Firewalls, Vulnerability  
Scanning,  
Risk Management,  
Secure Software Deployment/  
Development, Account  
Management,  
Event Logging, Alerting,  
Intrusion Detection/Prevention



## Data Handling Security and Privacy

Data Encryption (At-Rest,  
In-Transit), Data Retention,  
Data Disposal, Data Access  
Management, GDPR

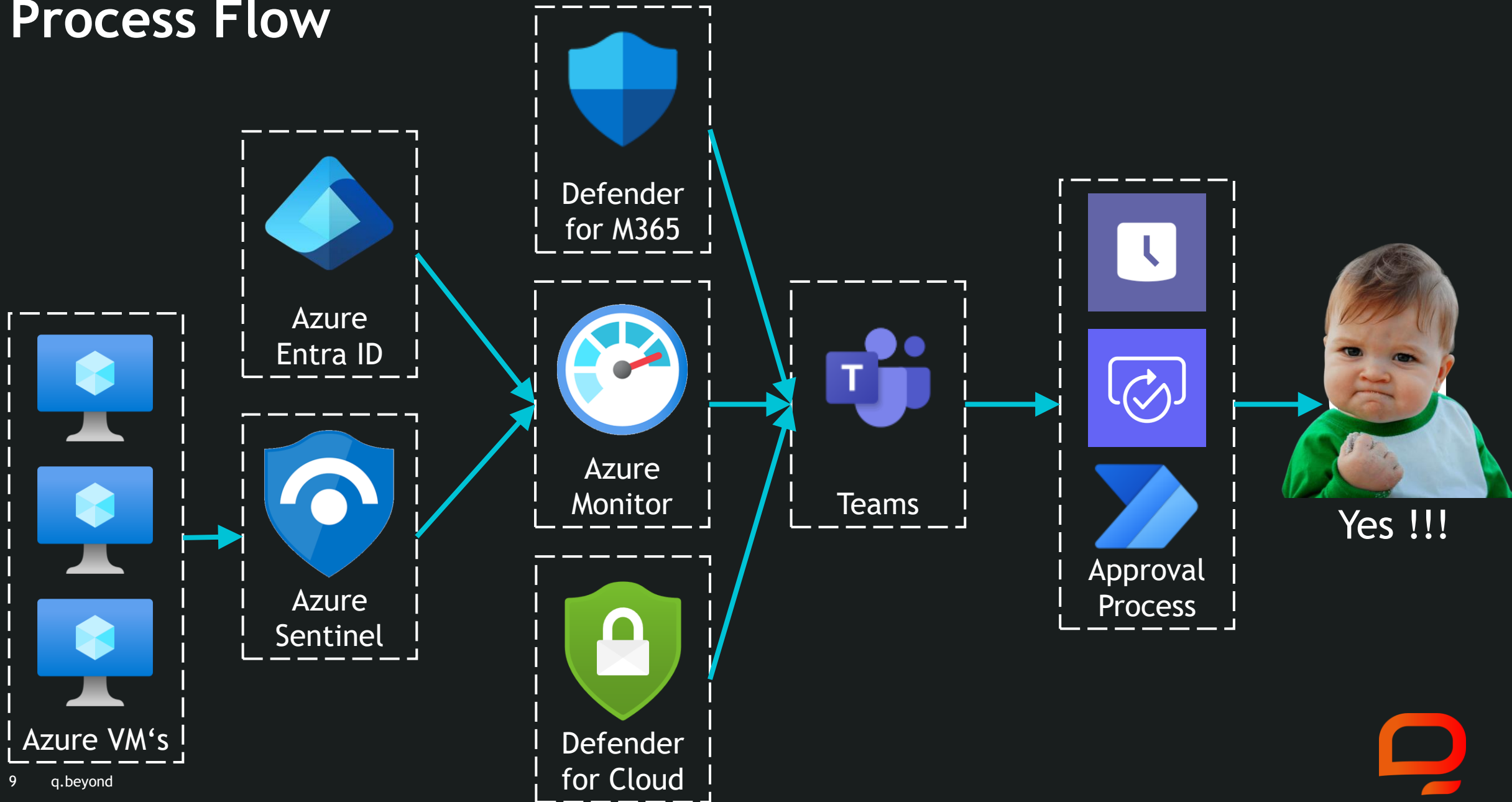


Optional: External  
Compliance Frameworks  
SOC2, PCI-DSS, ISO27001





# Process Flow





# Product Configurations

Microsoft Azure

Home > Monitor | Alerts > Alert rules > Elevation to company admin

### Elevation to company admin

Edit alert rule

Save Discard

On October 1, 2025 the Log Analytics alert API in Azure Monitor will be re

Edit the details below to modify the alert rule.  
When defining the alert rule, check that your inputs do not contain any sen

#### Scope

Select the target resource you wish to monitor.

Resource

LogAnalytics

#### Condition

Configure when the alert rule should trigger by selecting a signal and defin

Condition name

✓ Whenever the average custom log search is greater than 0

Add condition

You can define only one log signal per alert rule. To alert on more signals,

### Configure signal logic

Search query \* ⓘ

AuditLogs  
| where OperationName contains "Add member to role" and TargetResources contains "Company Administrator"

View result of query in Azure Monitor - Logs ⓘ

Query to be executed : AuditLogs | where OperationName contains "Add member to role" and TargetResources contains "Company Administrator" #| count  
For time window : 1/23/2024, 12:42 PM - 1/23/2024, 6:42 PM

It may take in the range of 6 minutes, to have the logs available for provided query [Learn more](#)

#### Alert logic

Based on ⓘ Operator ⓘ Threshold value \* ⓘ

Number of results Greater than 0

#### Condition preview

Whenever count of results in Custom log search log query for last 6 hours is greater than 0. Evaluated every 6 hours.

#### Evaluated based on

Period (in minutes) \* ⓘ Frequency (in minutes) ⓘ

360 360

Done

## Sentinel:

- Windows Event Log Collection, only

## Monitor:

- Security Event Alerting (Event Logs and broader Scope incl. Entra ID)
- Performance Monitoring
- IT Operations

### Condition

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Condition name	Estimated monthly cost (USD) ⓘ
✓ Whenever the average custom log search is greater than 0	\$ 0.50
Add condition	Total \$ 0.50



The screenshot illustrates a workflow for handling security warnings in Microsoft Teams. It consists of several overlapping windows and a text editor:

- Genehmigungen (Approvals) App:** Shows a list of approvals. A task card titled "Security Warning Review for Engineer on call shift" is highlighted. The task card includes instructions: "You are receiving this task, because a security and/or a vulnerability warnings has been detected! Please check whether or not any remediation is needed in Microsoft Cloud Security and Microsoft 365 Defender. Both dashboards are integrated in the General Tab of the Security Team." It also lists steps: "IMPORTANT --- FOLLOW THESE STEPS: Approve = No additional actions needed, Decline = Additional actions needed => create a Planner task directly from security warning message in Teams and assign responsible colleague".
- Teams Chat Window:** Shows a chat with "Robert Mulsow". A task card is visible in the chat, indicating the task is assigned to "FlowUser".
- Email (DefenderCloudonreply@microsoft.com):** Contains the message: "A Vulnerability Assessment scan has completed on your server 'sql-prod'". It also includes a link to "Ursprüngliche E-Mail anzeigen" (View original email).
- Text Editor (Untitled.txt):** Contains a process description:
 

```

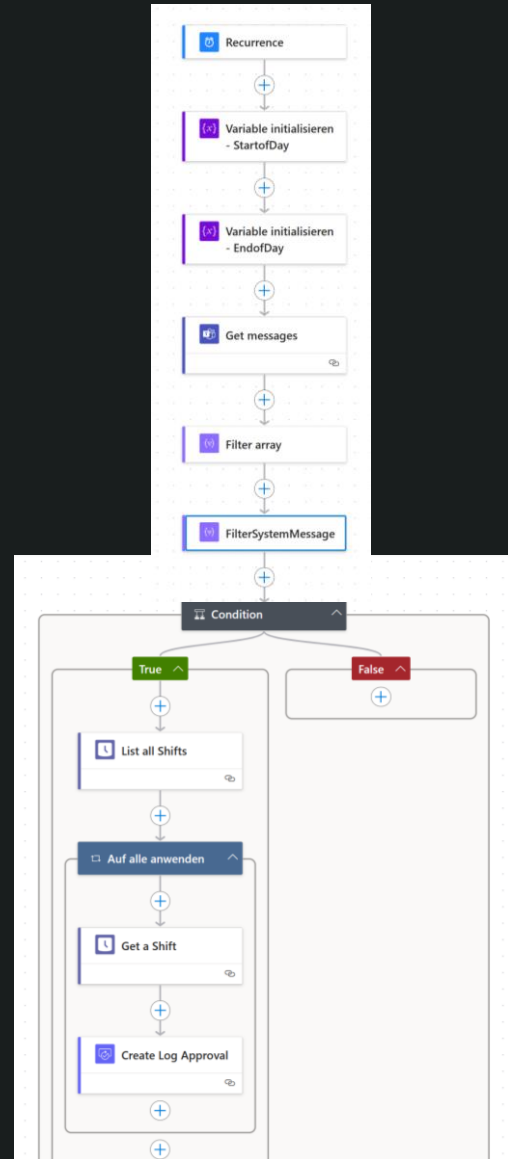
1 Process Description:
2
3 1. A Flow gets triggered, when Sentinel, or other service message
4 creates a post in Teams
5 2. Regarding Engineer on Call shift will be assigned a task
6 3. Engineer reviews Security message
7 4. Depending on security message tasks will be assigned in DevOps
8 5. Engineer completes Approval process, that security message was
9 evaluated
10

```

Red numbers 1-5 highlight key steps in the workflow:

1. Email received (DefenderCloudonreply@microsoft.com)
2. Task assigned to FlowUser
3. Task assigned to Robert Mulsow
4. Ticket created in DevOps support
5. Task assigned to Robert Mulsow

A red arrow points from the email to the task card in the Teams chat, with the text "See Remediation in next Screenshot".

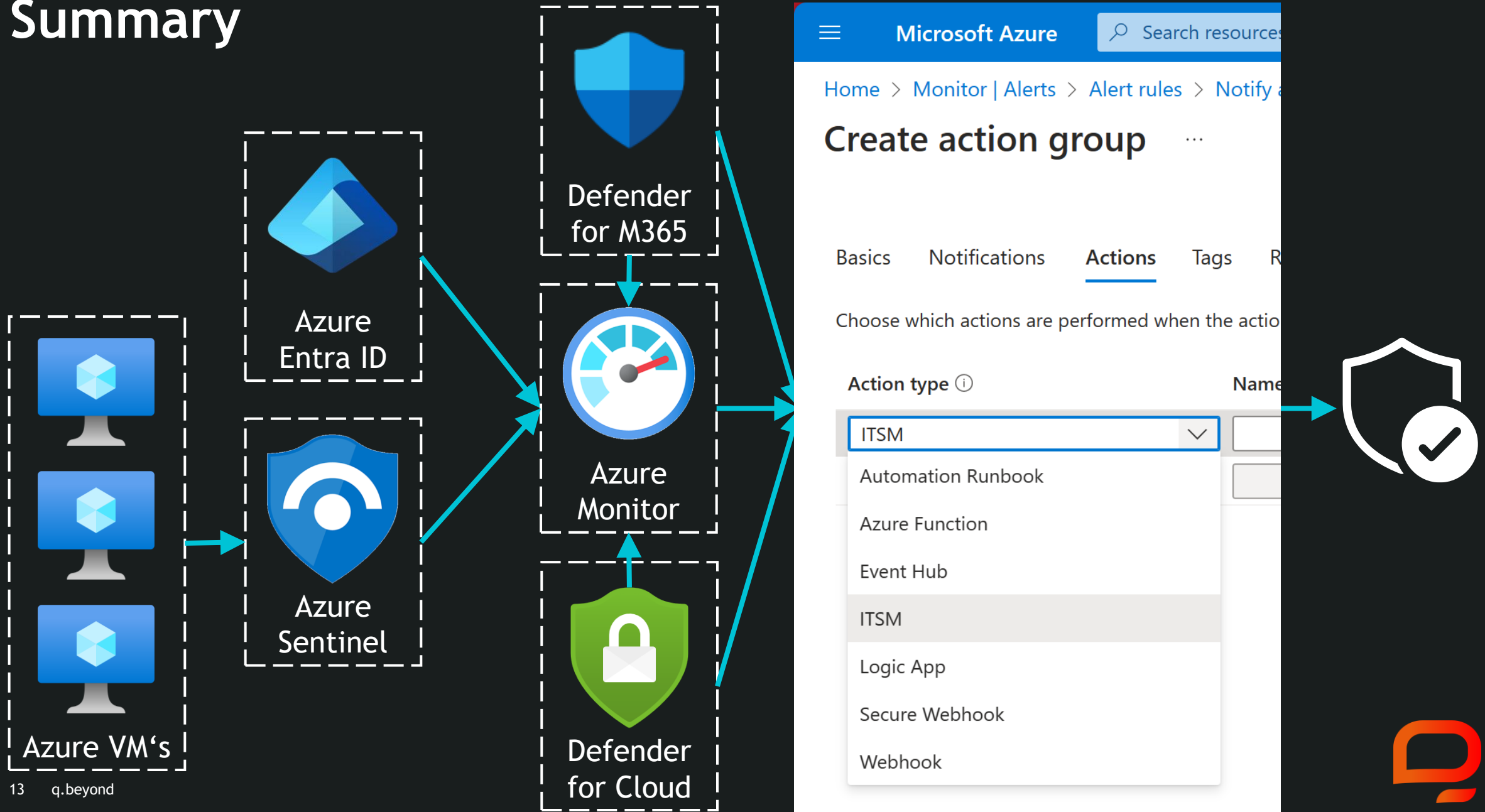


# Product Configurations

The screenshot displays the Azure DevOps Sprints interface for a project named 'Support und Betrieb'. The left sidebar contains navigation options: Suite, Overview, Boards, Work items, Backlogs, Sprints (selected), Queries, Delivery Plans, Plans, Portfolio++, Retrospectives, Portfolio plans (Beta), Time Log Summary, Estimate, Repos, Pipelines, Test Plans, Artifacts, and Portfolio++. The main area shows a Kanban board with columns: New, Active, Waiting, Test, In Progress, Resolved, and Closed. The 'New' column has three items: 7180 Infrastructure (Unassigned), 7190 Git must be updated (F), and 7196 6 checks are failing on SQL Prod - please correct (M). The 'Closed' column has three items: 7186 6 tests failed on SQL - Please fix (M), 7189 6 failing tests and SQL - please fix (M), and 7192 6 test fail on SQL Prod (M). The item 7192 is highlighted with a red rectangle. The top right shows the date range '1. Januar - 31. Dezember' and '230 work days remaining'. The bottom status bar indicates 'Analytics | Version 2.1.0' and '4 in progress'.



# Summary



# Thank you!



**Robert Mulsow | AI Enterprise Architect**

Let's keep in touch!



→ [linkedin.com/in/robert-mulsow/](https://www.linkedin.com/in/robert-mulsow/)



→ @Rob\_The\_Ninja



→ [www.qbeyond.de](https://www.qbeyond.de)



→ <https://blog.qbeyond.de/>

