



nextfence 
managed sentinel

ROBECO 
The Investment Engineers

Azure Sentinel Ninja Style

Pouyan Khabazi

Cloud Security & DevOps - Founder @NextFence



pkm-technology.com



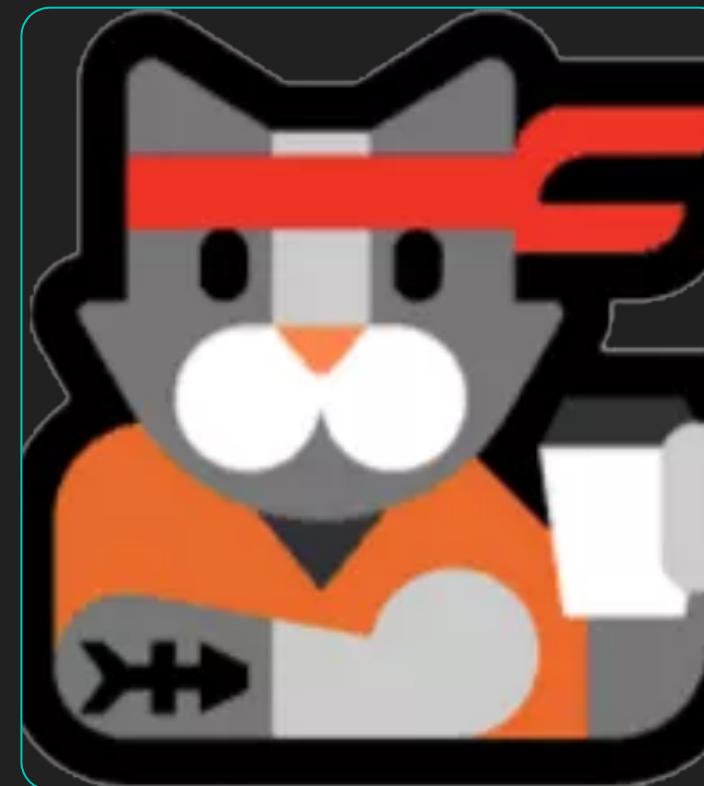
@pkhabazi



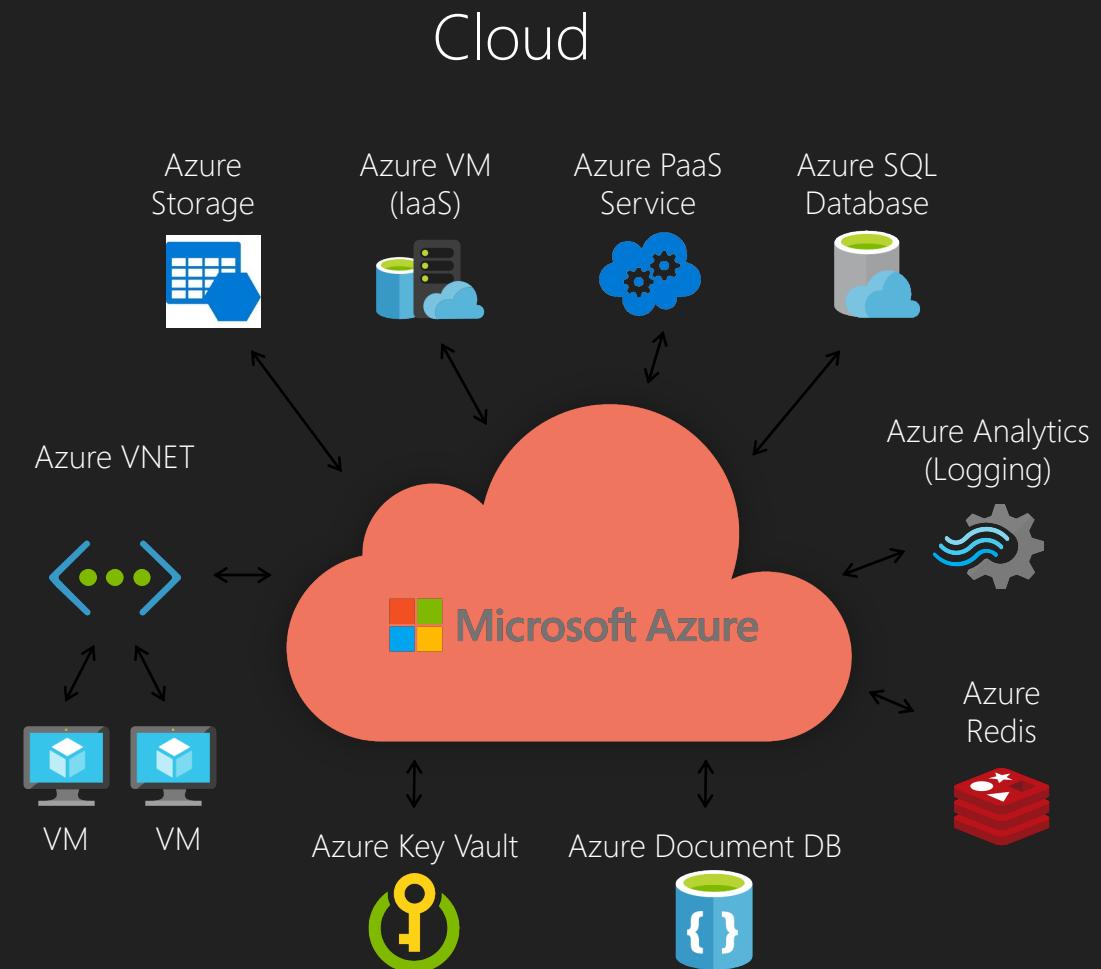
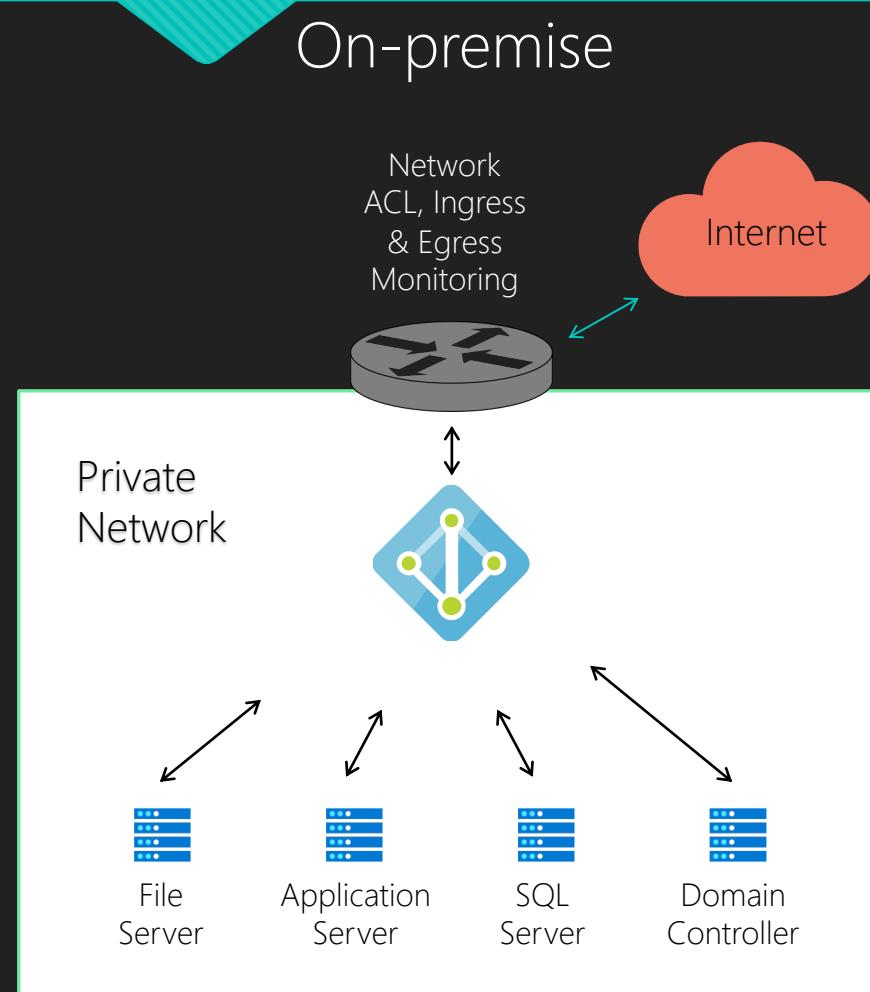
@pkhabazi

Subjects

- A new world to defend
- Azure Sentinel
- Why DevOps?
- Deploying ninja style
- Demo
- Q&A



A new world to defend

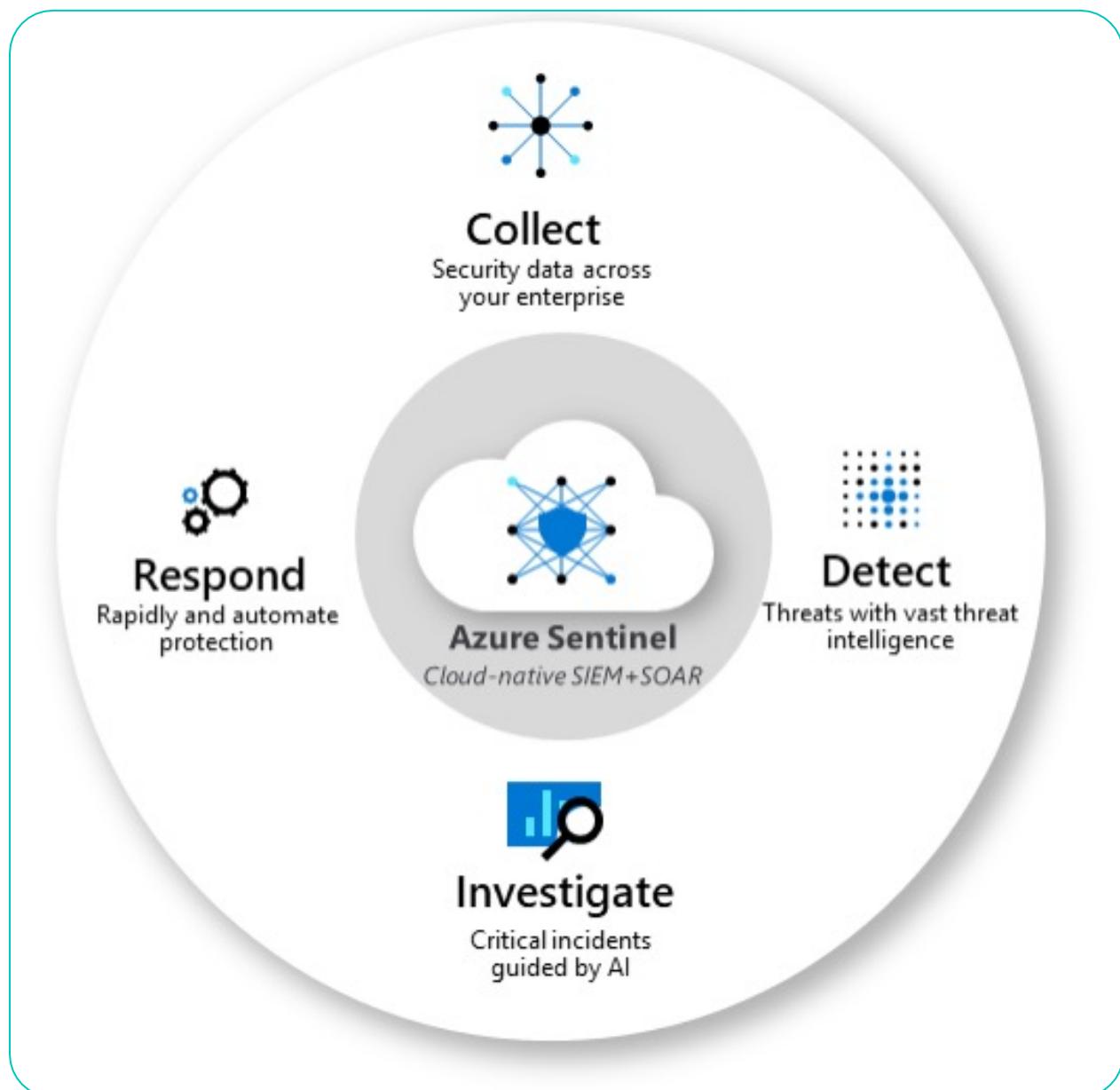


The challenges

- Traditional SIEM's require a lot of infrastructure and maintenance
- Collecting all the data and normalizing is a daunting task
- Lots of signals; how do we make sense of it all
- Too many disconnected products
- Defending the cloud requires a different skill- and toolset

MICROSOFT AZURE SENTINEL IS A SCALABLE, CLOUD-NATIVE, SECURITY INFORMATION EVENT MANAGEMENT (SIEM) AND SECURITY ORCHESTRATION AUTOMATED RESPONSE (SOAR) SOLUTION.

Azure Sentinel



Architecture

Sentinel

Kusto-based

Log Analytics

Unlimited scale

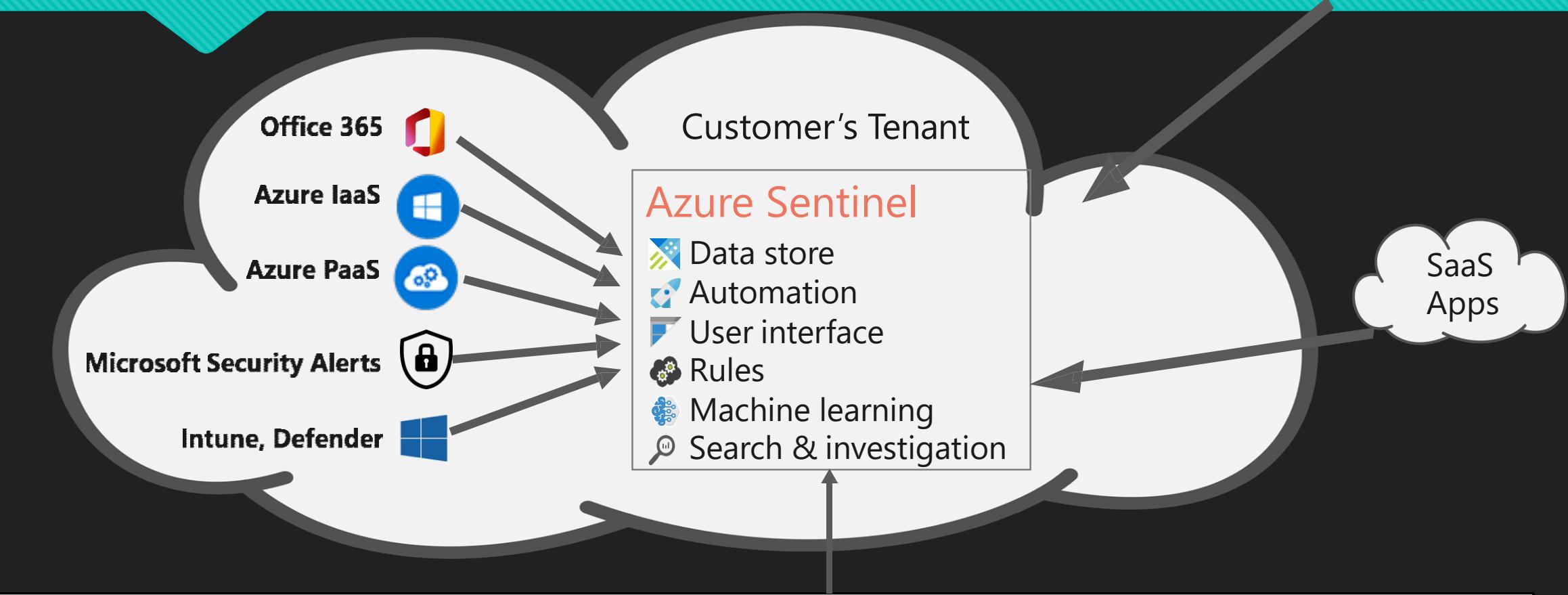
Azure

Enterprise-grade platform

KQL

```
OfficeActivity
| where Operation in~ ("Add-MailboxPermission", "Add-MailboxFolderPermission", "Set-Mailbox", "New-ManagementRoleAssignment")
  and not(UserId has_any ('NT AUTHORITY\\SYSTEM (Microsoft.Exchange.ServiceHost)', 'devilfish-applicationaccount') and Operation in~
("Add-MailboxPermission", "Set-Mailbox"))
| extend timestamp = TimeGenerated, AccountCustomEntity = UserId, IPCustomEntity = ClientIP
```

One SIEM to rule them all



On Premises

Data Connectors



Azure AD
Identity Protection



Microsoft Cloud
App Security



Azure Security
Center



Microsoft 365 Defender



Azure Information
Protection



AWS



Palo Alto Networks



Cisco ASA



Barracuda



Office 365



Symantec



Fortinet



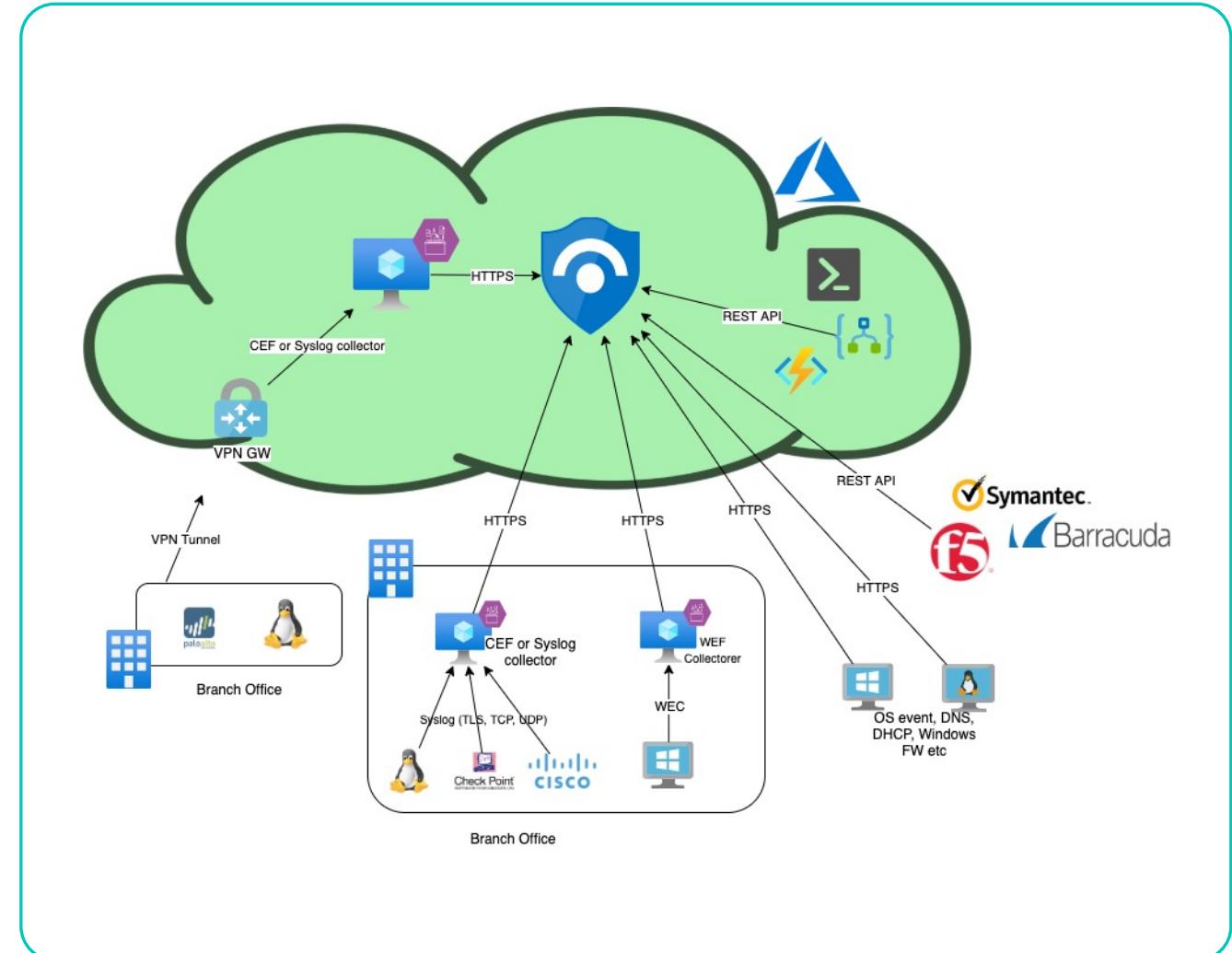
F5



Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point

And on-prem



Data connector and costs

Data Connector	License	Permissions	Cost
Azure Activity	None	Subscription Reader	Free
Azure Defender	ASC Standard	Security Reader	Free
Azure Active Directory	Any AAD License	Global Admin or Security Admin	Billed
Azure Active Directory Identity Protection	AAD Premium 2	Global Admin or Security Admin	Free
Office 365	None	Global Admin or Security Admin	Free
Microsoft Cloud App	MCAS	Global Admin or Security Admin	Free
Microsoft Defender for Identity	MDI	Global Admin or Security Admin	Free
Microsoft Defender for Endpoint	MDI	Global Admin or Security Admin	Free
Threat Intelligence Platforms	None	Global Admin or Security Admin	Billed
Security Events	None	None	Billed
Syslog	None	None	Billed
DNS (Preview)	None	None	Billed
Windows Firewall	None	None	Billed

0 Saved workbooks 106 Templates 0 Updates

My workbooks **Templates**

Search

 AI Analyst Darktrace Model Breach Summary
DARKTRACE

 AI Vectra Detect
VECTRA AI

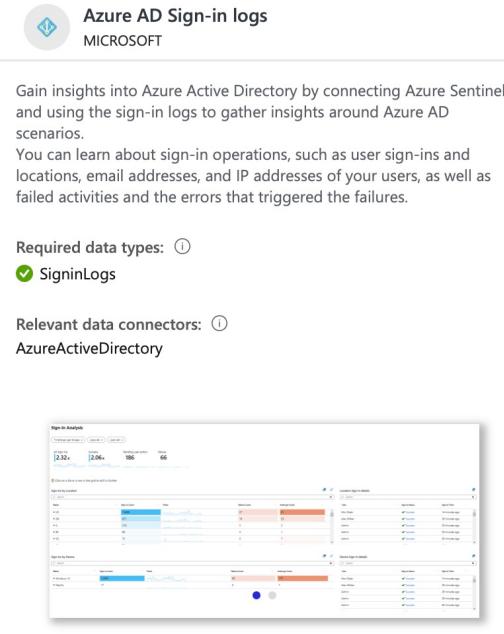
 Alsid for AD | Indicators of Attack
ALSID

 Alsid for AD | Indicators of Exposure
ALSID

 Analytics Efficiency
MICROSOFT

 ASC Compliance and Protection
AZURE SENTINEL COMMUNITY

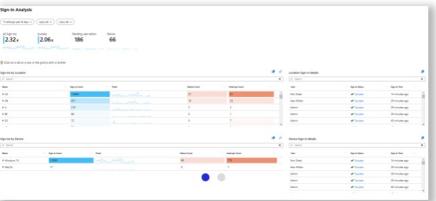
 AWS Network Activities
MICROSOFT


Azure AD Sign-in logs
MICROSOFT

Gain insights into Azure Active Directory by connecting Azure Sentinel and using the sign-in logs to gather insights around Azure AD scenarios.
You can learn about sign-in operations, such as user sign-ins and locations, email addresses, and IP addresses of your users, as well as failed activities and the errors that triggered the failures.

Required data types: ⓘ
 SigninLogs

Relevant data connectors: ⓘ
AzureActiveDirectory


[View template](#) [Save](#)

Workbooks

Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure, and combine them into unified interactive experiences.

TimeRange: Last 14 days

Apps: All

User Name Prefix: All

User Name: All

Category: All

Country: All

All Sign-ins

1.74k

Success

1.7k

Failure

29

Pending user action

7

💡 Click on a tile or a row in the grid to drill-in further

Sign-ins by Location

Name		↑↓ Sign-in Count	↑↓ Trend	Failure Count	↑↓ Interrupt Count	↑↓ Category
<input type="checkbox"/>	> NL	31		0	1	SignInLogs
<input type="checkbox"/>	> NL	31		0	1	SignInLogs
<input type="checkbox"/>	> GB	15		15	0	NonInteractiveUserSi
<input type="checkbox"/>	> IE	7		7	0	NonInteractiveUserSi
<input type="checkbox"/>	> Unknown country	2		0	2	SignInLogs

Location Sign-in details

User			↑↓ Sign-in Status
Pouyan Khabazi			✓ Success
Pouyan Khabazi			✓ Success
Pouyan Khabazi			✓ Success
Pouyan Khabazi			✓ Success
Pouyan Khabazi			✓ Success
Pouyan Khabazi			✓ Success
Pouyan Khabazi			✓ Success

Azure AD Sign-in logs

Analytics

Microsoft security - Microsoft security templates automatically create Azure Sentinel incidents from the alerts generated in other Microsoft security solutions, in real time.

Fusion (preview) - Based on Fusion technology, advanced multistage attack detection in Azure Sentinel uses scalable machine learning algorithms that can correlate many low-fidelity alerts and events across multiple products into high-fidelity and actionable incidents.

ML behavioral analytics (preview) - These templates are based on proprietary Microsoft machine learning algorithms, so you cannot see the internal logic of how they work and when they run. Because the logic is hidden and therefore not customizable, you can only create one rule with each template of this type.

Scheduled - You can use the scheduled and customize the query logic and scheduling settings to create new rules.

Anomaly (preview) - Anomaly rule templates use SOC-ML (machine learning) to detect specific types of anomalous behavior.

82
Active rules

Rules by severity
High (6) Medium (37) Low (15) Informational (24)

Active rules Rule templates

 Search

Severity : All

Rule Type : All

More (2)

Severity ↑↓	Name ↑↓	Rule Type ↑↓	Data Sources	Tactics
High	TEARDROP memory-on...	Scheduled	Microsoft 365 Defe...	🔒 ⚡
High	Alsid Password Guessing	Scheduled	Alsid for Active Dire...	🔒 Credential Access
High	Solorigate Named Pipe	Scheduled	Security Events	➡️ Lateral Moveme...
High	[IN USE] Modified doma...	Scheduled	Azure Active Direct...	🔒 Credential Access
High	Create incidents based ...	Microsoft Secur...	Azure Active Direct...	
High	[IN USE] First access cre...	Scheduled	Azure Active Direct...	🔒 Credential Access
High	Security Service Registr...	Scheduled	Security Events +1 ⓘ	✖️ Defense Evasion
High	Solorigate Network Bea...	Scheduled	DNS (Preview) +5 ⓘ	➡️ Command and ...
High	[IN USE] Suspicious appl...	Scheduled	Azure Active Direct...	➡️ 🔒
High	Create incidents based ...	Microsoft Secur...	Microsoft Defender ...	

< Previous Page 1 of 7 Next >

LEARN MORE
[About analytics rules](#)

TEARDROP memory-only dropper

High Severity Scheduled Rule Type

Persistence

Rule query

```
DeviceEvents
| where ActionType has
"ExploitGuardNonMicrosoftSignedBlocked"
| where InitiatingProcessFileName contains
"svchost.exe" and FileName contains
"NetSetupSvc.dll"
```

Rule frequency

Run query every 1 day



Note:

- You haven't used this template yet; You can use it to create analytics rules.
- One or more data sources used by this rule is missing. This might limit the functionality of the rule.

[Create rule](#)

Templates

General Set rule logic Incident settings (Preview) Automated response Review and create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *
AlertRule01

Id
0f294e4a-5f91-443e-b1e6-519de4284c37

Description

Tactics
3 selected

Severity
Medium

Status
 Enabled Disabled

Rule query
Any time details set here will be within the scope defined below in the Query scheduling fields.

```
SecurityEvent | where EventID == "4688" | where CommandLine contains "-noni -ep bypass $"
```

[View query results >](#)

Alert enrichment (Preview)

- ▽ Entity mapping
- ▽ Custom details
- ▽ Alert details

Query scheduling

Run query every *
5 Hours

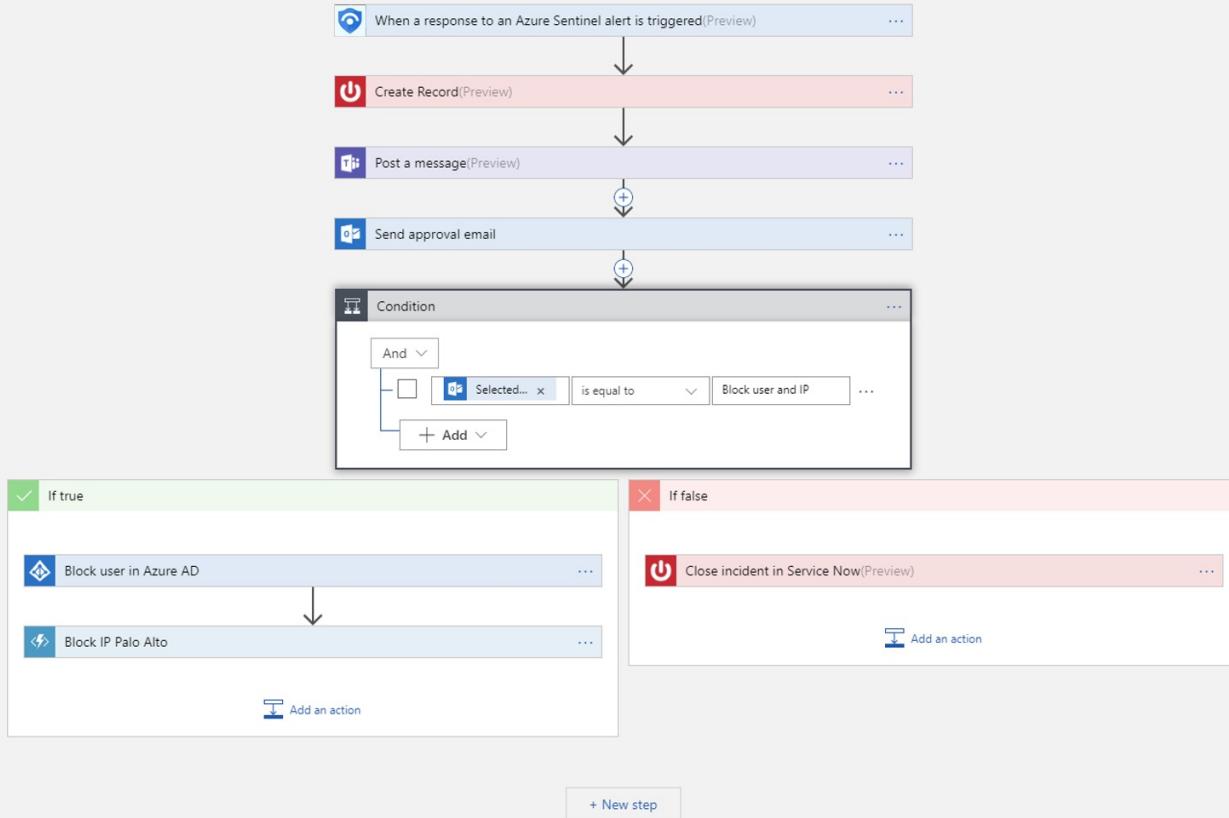
Lookup data from the last * ⓘ
6 Hours

Analytics KQL

SOAR - Playbooks

Automation rules allow you to centrally manage all the automation of incident handling. Automation rules streamline automation use in Azure Sentinel and enable you to simplify complex workflows for your incident orchestration processes.

Automation & Response



Time to go
DevOps
Ninja style



Why DevOps?

The main reason is to implement the "shift left" Way of Working (Wow). The term 'shift left' refers to a practice in software development where teams focus on quality, work on problem prevention instead of detection, and begin testing earlier than ever before.

What do we need?

Shifting left requires two key DevOps practices:

- Continuous testing
- Continuous deployment

Continuous testing involves automating tests and running those tests as early and often as possible. Continuous deployment automates the provisioning and deployment of new builds, enabling continuous testing to happen quickly and efficiently.

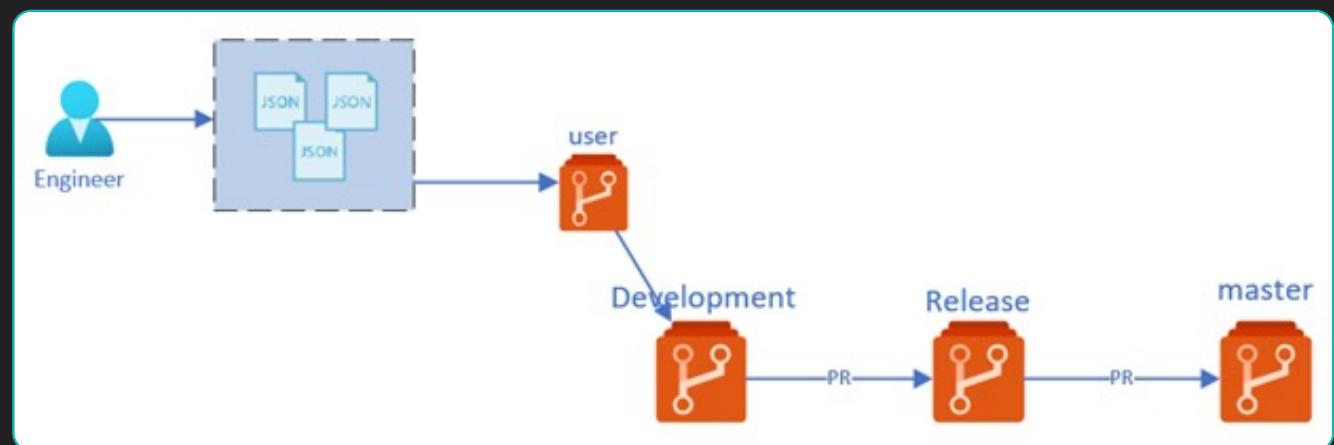
Security as Code (SaC)

Security as Code (SaC) manages infrastructure (networks, virtual machines, load balancers, even your Azure Sentinel rules and settings) in a **descriptive** model, using the same versioning as DevOps teams use for source code.

```
{  
    "displayName": "string",  
    "description": "string",  
    "AlertRuleTemplateName": "string",  
    "severity": "High",  
    "enabled": true,  
    "query": "SecurityEvent | where EventID == \"4688\" | where CommandLine contains \"-noni -ep t",  
    "queryFrequency": "5H",  
    "queryPeriod": "5H",  
    "triggerOperator": "GreaterThan",  
    "triggerThreshold": 5,  
    "suppressionDuration": "6H",  
    "suppressionEnabled": false,  
    "tactics": [  
        "Persistence",  
        "LateralMovement",  
        "Collection"  
    ],  
    "playbookName": "string",  
    "aggregationKind": "string",  
    "incidentConfiguration": {  
        "createIncident": true,  
        "groupingConfiguration": {  
            "GroupingConfigurationEnabled": true,  
            "reopenClosedIncident": true,  
            "lookbackDuration": "PT6H",  
            "entitiesMatchingMethod": "string",  
            "groupByEntities": [  
                "Account",  
                "Ip",  
                "Host",  
                "Url",  
                "FileHash"  
            ]  
        }  
    }  
}
```

Repository

Git is a free and open-source distributed version control system designed to handle everything from small to very large projects with speed and efficiency.



Pipelines - Automate your workflow

Azure Pipelines automatically builds and tests code projects to make them available to others. It works with just about any language or project type. Azure Pipelines combines continuous integration (CI) and continuous delivery (CD) to constantly and consistently test and build your code and ship it to any target.

Continues testing

Pester provides a framework for writing and running tests. Pester is most commonly used for writing unit and integration tests, but it is not limited to just that. It is also a base for tools that validate whole environments, computer deployments, database configurations, and so on.

The screenshot shows a continuous integration dashboard for a pull request titled "demo PR". The status is "Active" with 125 files and 1 PR. The "Overview" tab is selected, showing a summary of the build status:

- Build.Validation**: Build failed. A message states: "There are one or more test failures detected in result files. Detailed summary of published test results can be viewed in the Tests tab."
- At least 1 reviewer must approve**
- No merge conflicts** (Last checked: Just now)

Below this, a detailed view for the "#20201008.14 demo PR" build is shown under the "Tests" tab. The summary indicates 1 run completed (0 passed, 1 failed), with 4 unique failing tests in the last 14 days. The test results are visualized in two donut charts:

- Passed: 5 (Green)
- Failed: 2 (Red)
- New: 0 (Grey)
- Existing: 0 (Grey)

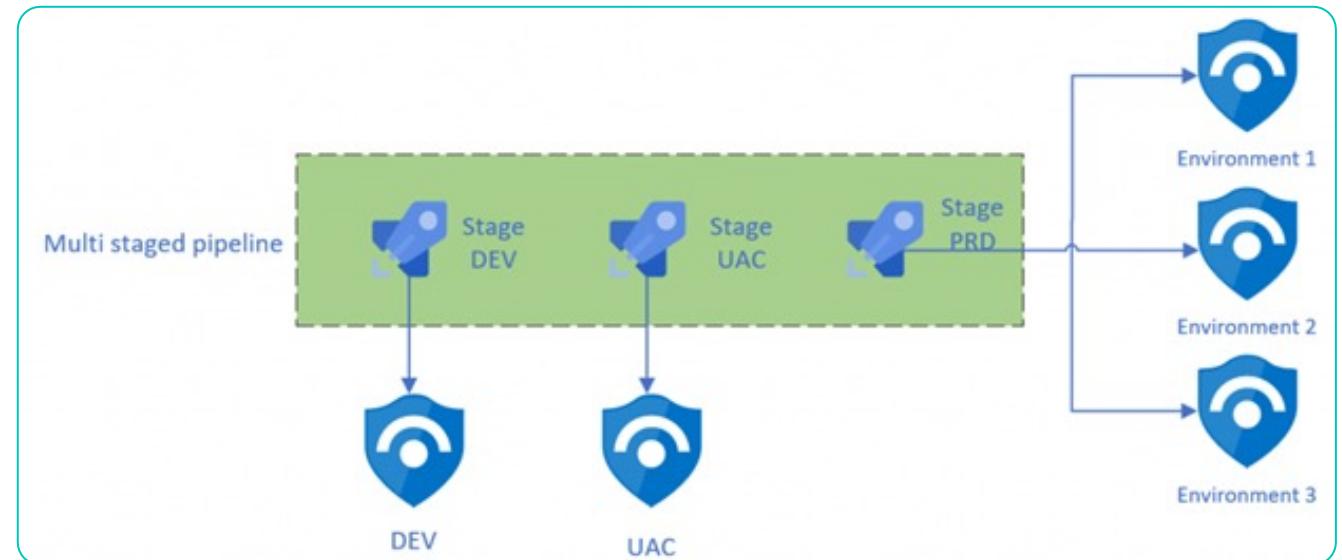
Key statistics from the summary table:

Metric	Value
Total tests	7
Passed	5
Failed	2
Others	0
Pass percentage	71.42%
Run duration	600ms
Tests not reported	0

At the bottom, a table lists individual test results:

Test	Duration	Failing since	Fails
NUnit_TestResults_712 (2/7)	0:00:00.600	Thursday	Curr
Azure Sentinel AlertRules Tests.Scheduled rules have the minimum elements(" /home/vsts/work/1/s/Set	0:00:00.270	Thursday	Curr
Azure Sentinel Hunting rules Tests.Hunting rules have the minimum elements(" /home/vsts/work/1/s/Set	0:00:00.030	Thursday	Curr

Continuous deployment



Pipeline Template

Pipeline Templates let us define reusable content, logic, and parameters. Templates function in two ways. You can insert reusable content with a template or use a template to control what is allowed in a pipeline.

```
- template: pipelines/steps.yml
parameters:
  environment: Dev
  azureSubscription: ""
  WorkspaceName: " # Enter the Azure Sentinel Workspace name
  SubscriptionId: 'cd466daa-3528-481e-83f1-7a7148706287'
  ResourceGroupName: ""
  ResourceGroupLocation: 'westeurope'
  EnableSentinel: true
  analyticsRulesFile: SettingFiles/AlertRules.json # leave empty if you dont
  huntingRulesFile: SettingFiles/HuntingRules.json # leave empty if you do
  PlaybooksFolder: Playbooks/ # leave empty if you dont want to configure Playbo
  ConnectorsFile: SettingFiles/DataConnectors.json # leave empty if you do
  WorkbooksFolder: Workbooks/
  WorkbookSourceId: "" # leave empty if you dont want to configure Workbook
```

The image displays two side-by-side screenshots of a CI/CD pipeline interface, likely from Azure DevOps, illustrating a deployment process across three environments: Development, Acceptance, and Production.

Pipeline #20201011.3 update sub

- Triggered by:** Pouyan Khabazi
- Repository and version:** pipeline, master, commit 0ed5936
- Time started and elapsed:** Today at 9:54 PM, 2m 36s
- Related:** 0 work items, 0 artifacts
- Tests and coverage:** Get started
- View 3 changes**

Stages:

- Deploying to Develo...**: 1 job completed, 1m 19s (Status: Success)
- Deploying to Accept...**: Skipped
- Deploying to Product...**: 1 job completed, 1m 5s (Status: Success)

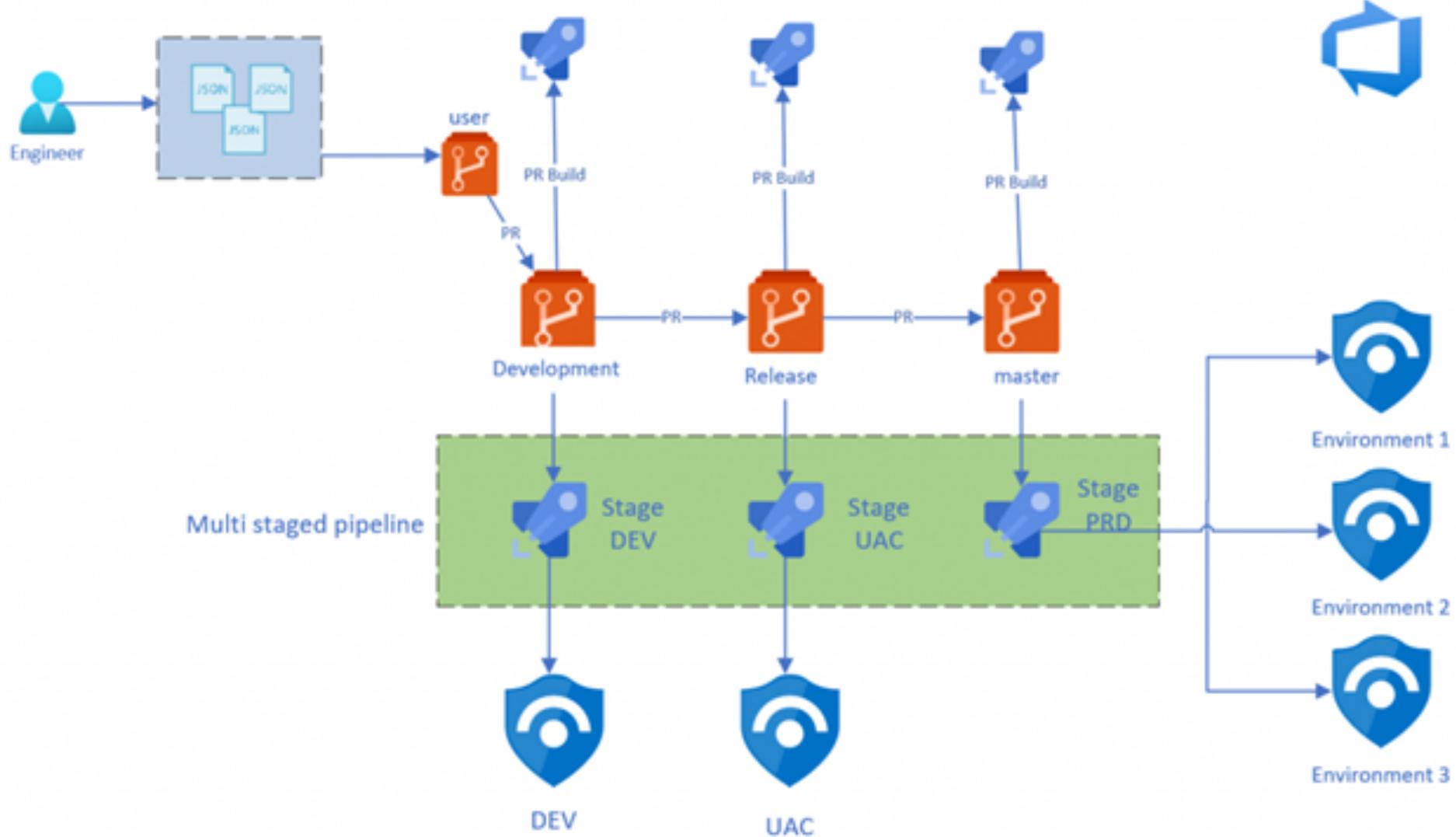
Pipeline #20201011.5 restore typo

- Triggered by:** Pouyan Khabazi
- Repository and version:** pipeline, feature/pouyan, commit ed5979
- Time started and elapsed:** Today at 9:57 PM, 1m 19s
- Related:** 0 work items, 0 artifacts
- Tests and coverage:** Get started
- View 24 changes**

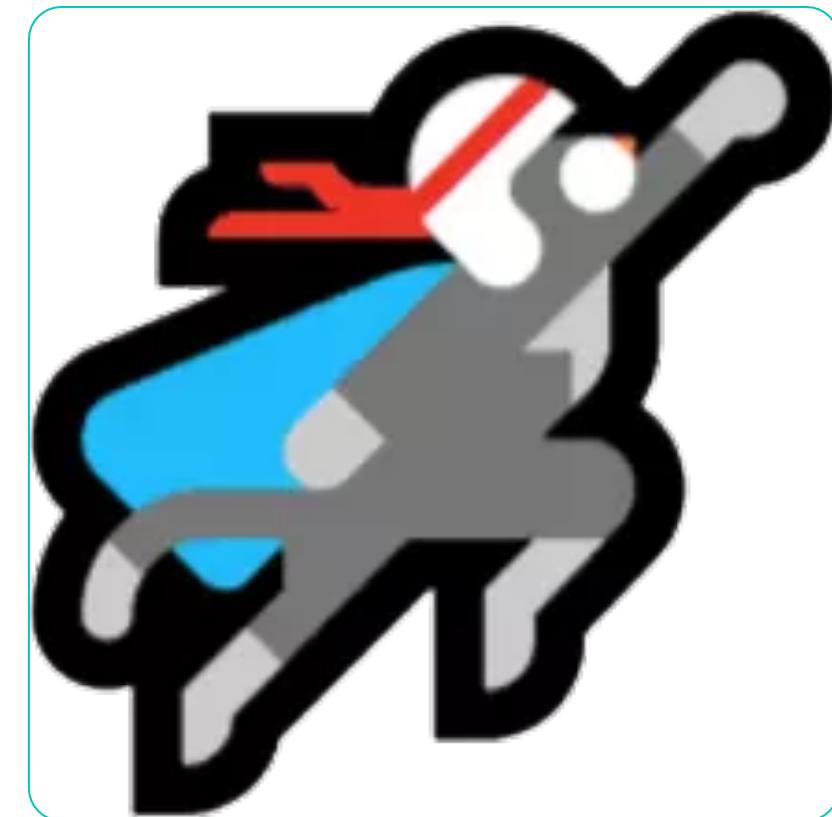
Stages:

- Deploying to Develo...**: 1 job completed, 1m 17s (Status: Success)
- Deploying to Accept...**: Skipped
- Deploying to Product...**: Skipped

Example



Demo



Demo content

Code: <https://github.com/pkhabazi/sentineldevops>

Blog: <https://techcommunity.microsoft.com/t5/azure-sentinel/deploying-and-managing-azure-sentinel-ninja-style/ba-p/1858073>

Great community work

- [sentinel-all-in-one](#) by @soricloud
- <https://kustoking.com> @castello_johnny
- SecureHats by @DijkmanRogier
- Grand Connector List by @Oshezaf
- Sentinel Ninja Training by @Oshezaf
- <https://getrevue.co/profile/AzureSentinelToday> by @RodTrent
- Azure Sentinel GitHub by Microsoft, the community and you
- Azure Sentinel - Microsoft Tech Community by Microsoft, the community and you

Questions?



Pouyan Khabazi
Cloud Security & DevOps – Founder @NextFence



pkm-technology.com



@pkhabazi



@pkhabazi



Microsoft®
Most Valuable
Professional