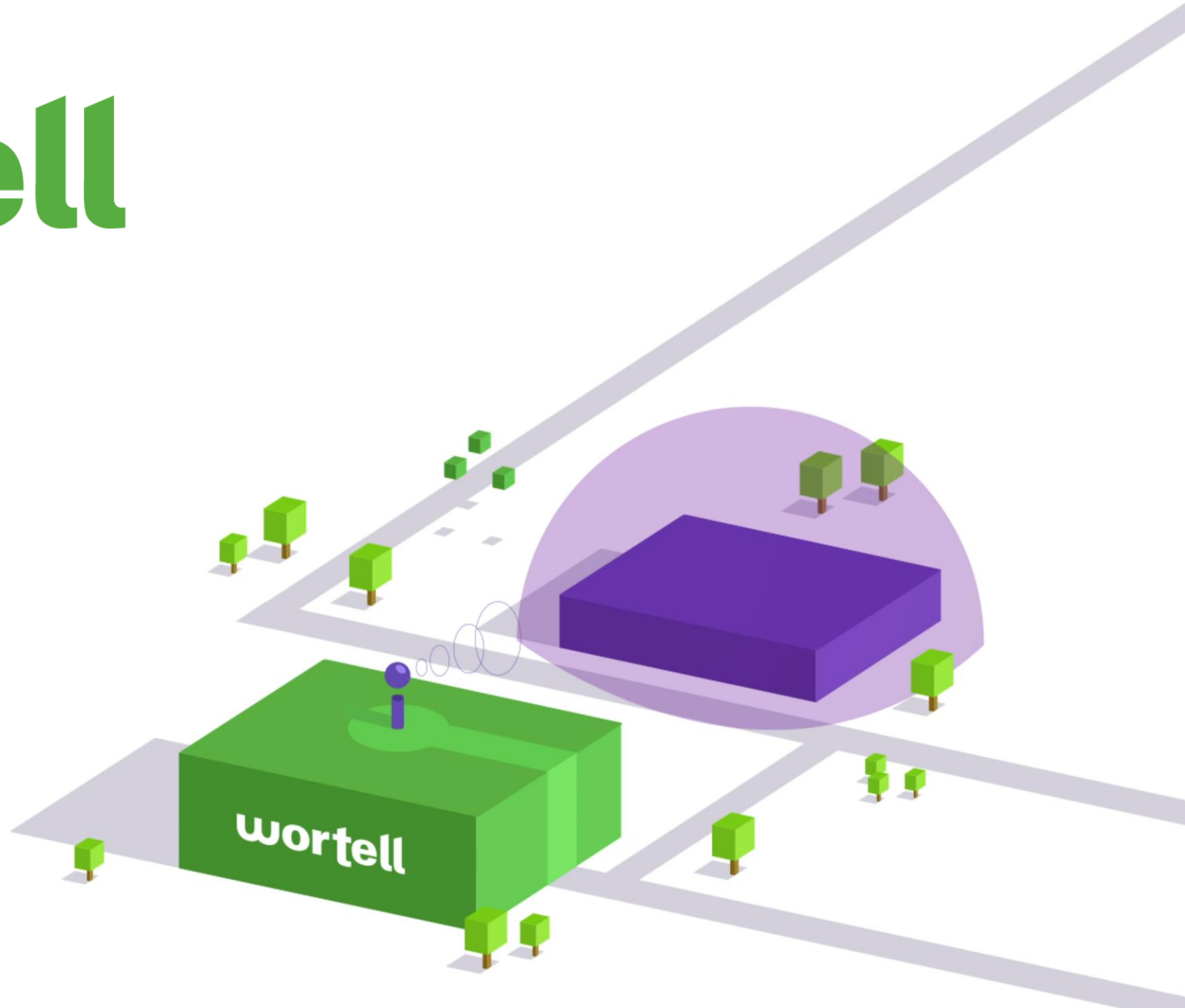


wortell

Enterprise Security



Reverse engineering Azure
Sentinel to craft a
PowerShell module_





Pouyan Khabazi
Cloud & Security Consultant_



pkm-technology.com



@pkhabazi



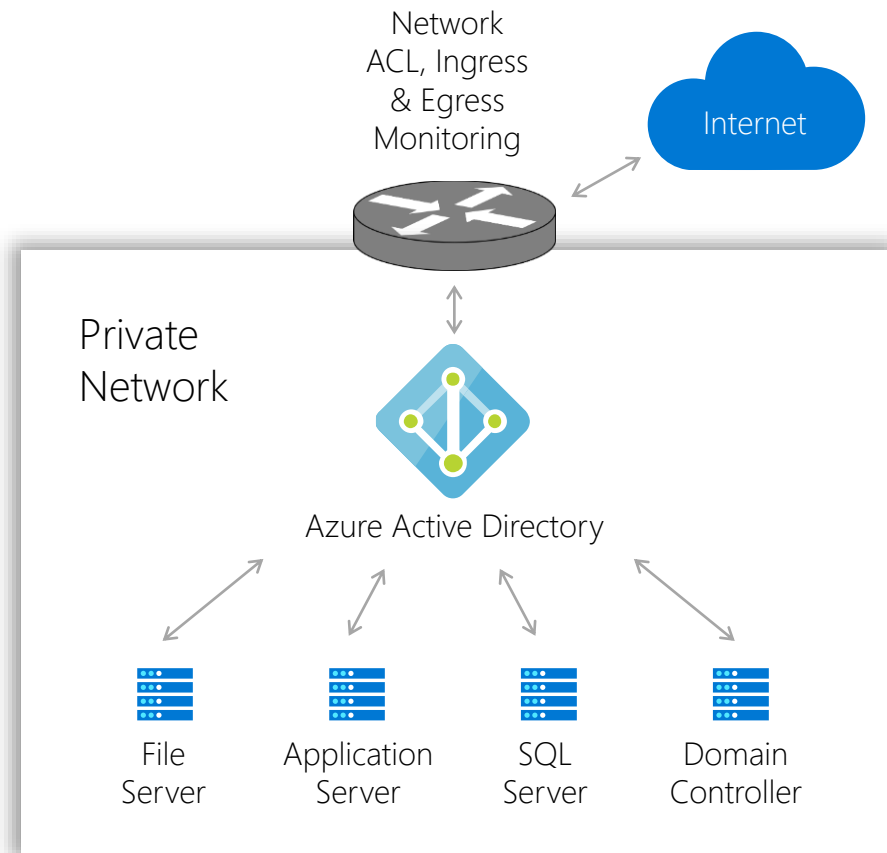
@pkhabazi

Subjects_

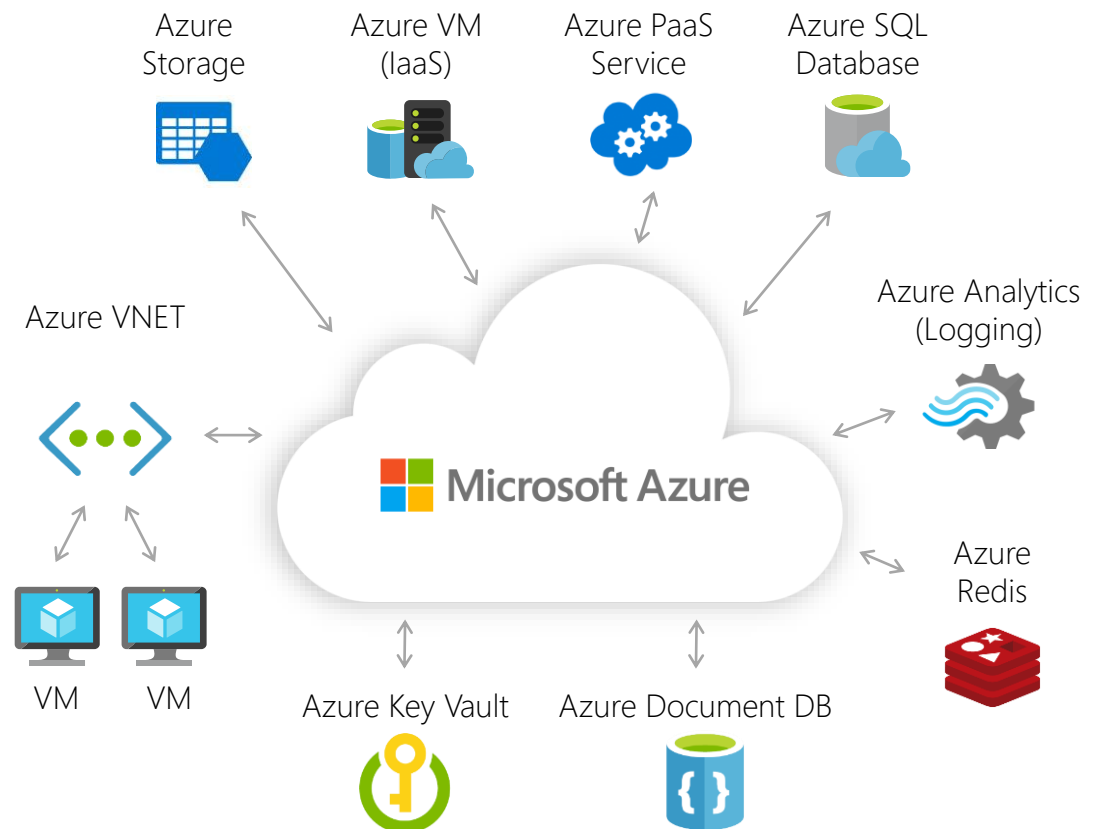
- Azure Sentinel
- Azure Resource manager
- Reverse engineering
- AzSentinel
- QA

A new world to defend_

On-premise



Cloud



cloud defender mindset_

On-premises

Server

Domain

Domain Admin

Pass the Hash

Private IPs

ACLs

RDP/SSH



On cloud

Services

Subscriptions

Subscription Admin

Credential Pivot

Public IPs

NSGs

Management APIs

Azure Sentinel_

wortell
Enterprise Security

Azure Sentinel_

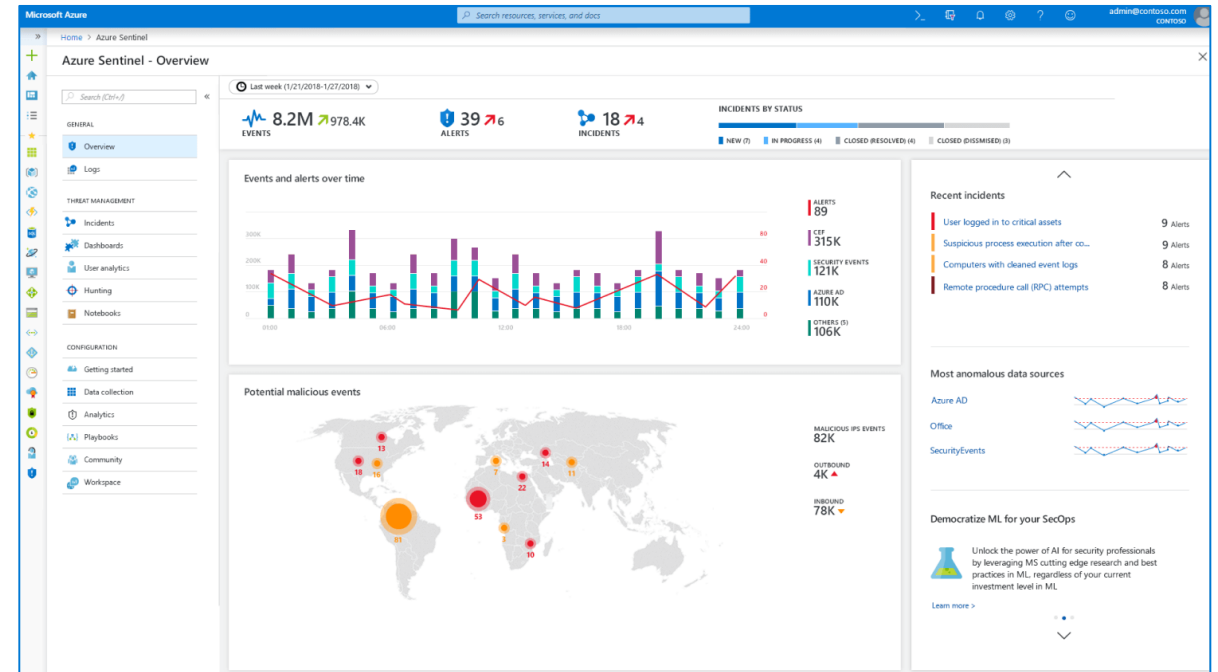
cloud-native siem

limitless cloud speed & scale

a.i. built-in

easy integration

only pay for what you use

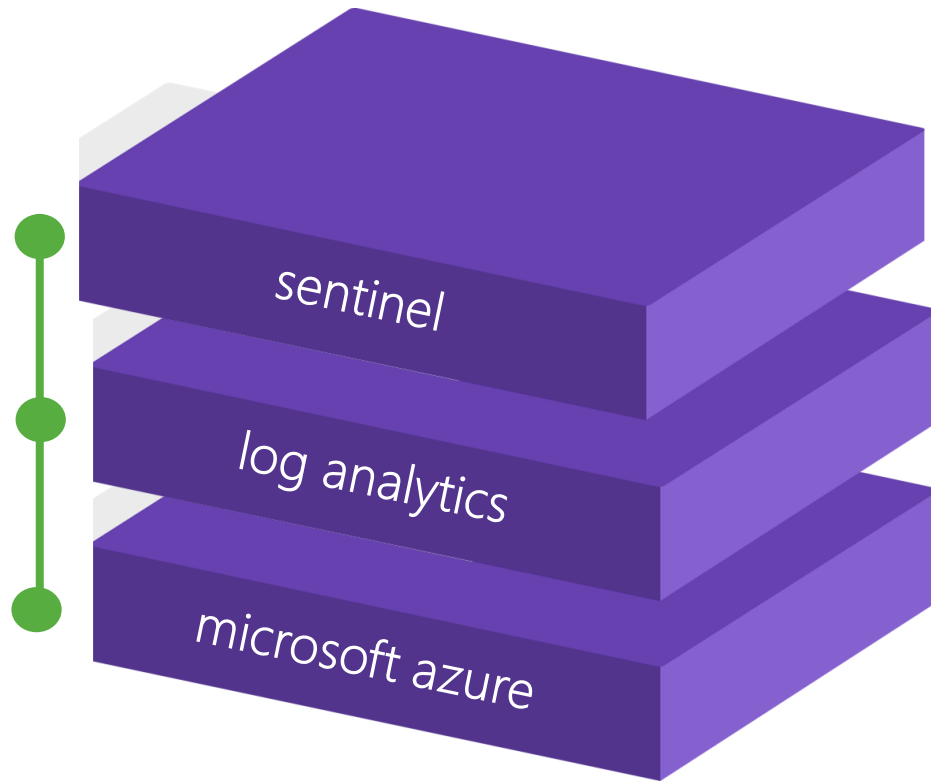


GA_

wortell
Enterprise Security



architecture_



kusto-based

unlimited scale

enterprise-grade platform



Home > Azure Sentinel workspaces > Azure Sentinel - Hunting > Logs

Logs

New Query 1* +

Help Settings Sample queries Query explorer

Run Time range: Custom Save Copy Export New alert rule Pin to dashboard

Schema Filter

Filter by name or type...

Collapse all

Active

- CompatibilityAssessment
- ContainerInsights
- DeviceHealthProd
- LogManagement
- Office365
- Security
- SecurityCenterFree
- SecurityInsights
- Updates
- WaaSUpdateInsights
- Custom Logs
- fx Functions

```
SigninLogs
| where UserPrincipalName == "info@security.wortell.nl"
or UserPrincipalName == "[redacted]@wortell[redacted].onmicrosoft.com"
or UserPrincipalName == "drbrenner@wortell.nl"
```

Completed. Showing results from the custom time range. 00:00:01.030 4 records Display time (UTC+00:00) v

TABLE CHART Columns v

Drag a column header and drop it here to group by that column

TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion	Category	ResultType	ResultSignature
2019-08-14T14:43:15.395	/tenants/[redacted]/providers/Micro...	Sign-in activity	1.0	SignInLogs	53004	None
...						
TenantId [redacted]						
SourceSystem Azure AD						
TimeGenerated [UTC] 2019-08-14T14:43:15.395Z						
ResourceId /tenants/[redacted]/providers/Microsoft.aadiam						
OperationName Sign-in activity						

Page 1 of 1 50 items per page

Analytics rules_

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

Analytic rule details

Name *

AlertRule02

Description

test

Tactics

2 selected

Severity

High

Status

Enabled

Disabled

Define the logic for your new analytic rule.

Rule query

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

Any time details set here will be within the scope defined below in the Query scheduling fields.
[View query results >](#)

Map entities - more entities coming soon!

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string or Datetime.

Entity Type	Column	
Account	<div>Choose column</div>	<div>Add</div>
Host	<div>Choose column</div>	<div>Add</div>
IP	<div>Choose column</div>	<div>Add</div>
URL	<div>Choose column</div>	<div>Add</div>

Query scheduling

Run query every *

5

Hours

Lookup data from the last * ⓘ

6

Hours

Stop running query after alert is generated ⓘ

On

Off

Alert threshold

Generate alert when number of query results

Is greater than

5

Hunting rules_

Name *

HuntingRule01

Description

test

Custom query

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

[View query results >](#)

Entity mapping - more entities coming soon!

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string or Datetime.

Entity Type	Column	
Account	<div>Choose column</div>	Add
Host	<div>Choose column</div>	Add
IP	<div>Choose column</div>	Add
URL	<div>Choose column</div>	Add
Timestamp	<div>Choose column</div>	Add

Tactics

3 selected

data connections_



Azure AD
Identity Protection



Microsoft Cloud
App Security



Azure Security
Center



Azure Advanced
Threat Protection



Azure Information
Protection



AWS



Palo Alto Networks



Cisco ASA



Barracuda



Office 365



Symantec



Fortinet



F5



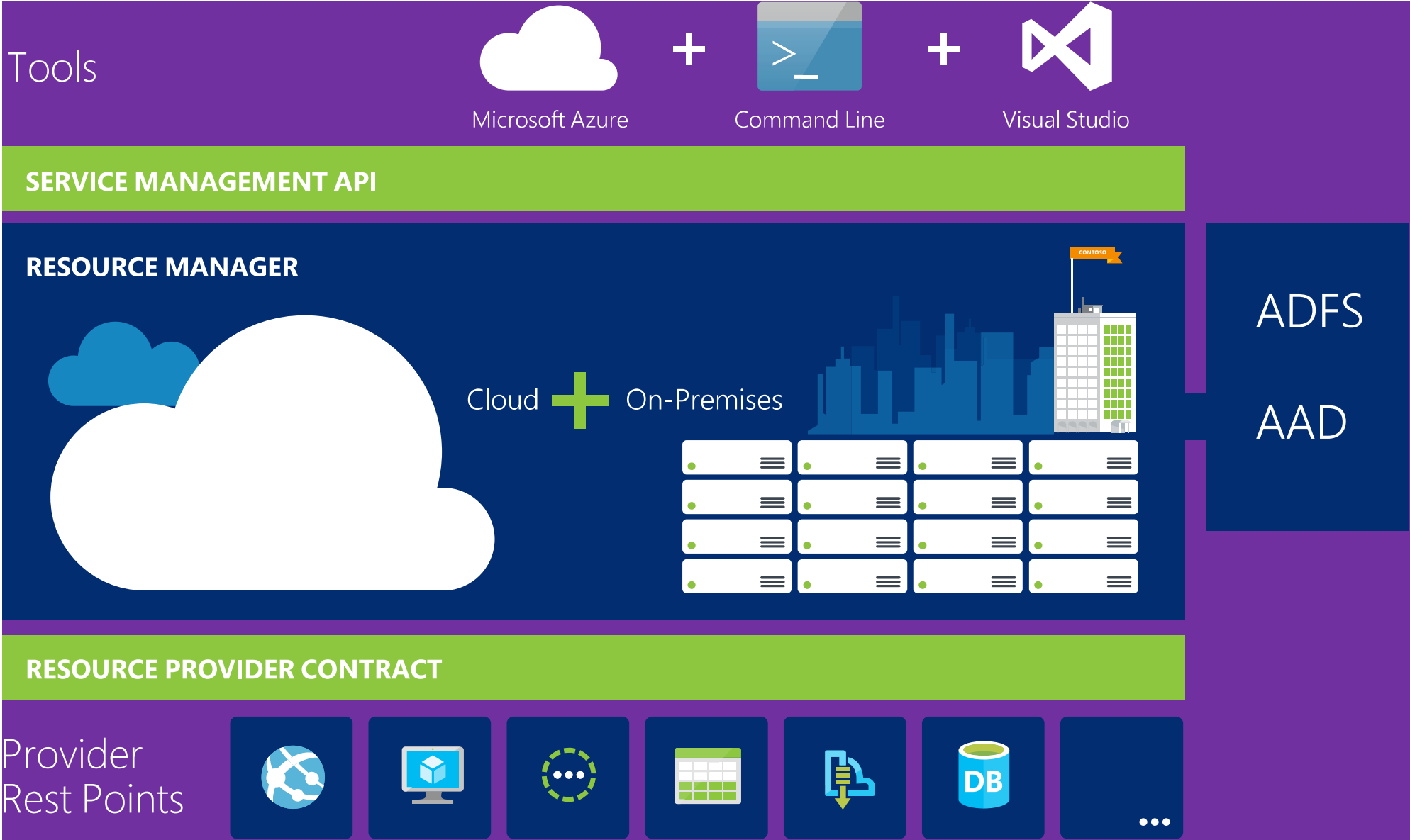
Check Point

Azure Resource Manager_



ARM_

Consistent
Management
Layer



Service Management REST API Reference_



Representational State Transfer (REST) APIs are service endpoints that support sets of HTTP operations (methods), which provide create, retrieve, update, or delete access to the service's resources.

The request URI:

- URI scheme: Indicates the protocol used to transmit the request. For example, http or **https**.
- URI host: Specifies the domain name of the REST service endpoint: **management.azure.com**
- Resource path: Specifies the resource or resource collection, which may include multiple segments used by the service in determining the selection of those resources.
- Query string (optional): Provides additional simple parameters, such as the API version or resource selection criteria.

HTTP request message header fields:

- A required HTTP method which tells the service what type of operation you are requesting. Azure REST APIs support GET, HEAD, PUT, POST, and PATCH methods.
- Optional additional header fields, as required by the specified URI and HTTP method. For example, an Authorization header that provides a bearer token containing client authorization information for the request.

HTTP request message body:

The request body is separated from the header by an empty line, formatted in accordance with the Content-Type header field. An example of an "application/json" formatted body would appear as follows:

```
{  
  "<name>": "<value>"  
}
```

Example_

{URI-scheme} :// {URI-host} / {resource-path} ? {query-string}

[https://management.azure.com/subscriptions/1654fb-ca67-408c-9fc5-9865wd/resourcegroups/dupsug17/providers/Microsoft.OperationsManagement/solutions/SecurityInsights\(pkmdemo01\)?api-version=2015-11-01-preview](https://management.azure.com/subscriptions/1654fb-ca67-408c-9fc5-9865wd/resourcegroups/dupsug17/providers/Microsoft.OperationsManagement/solutions/SecurityInsights(pkmdemo01)?api-version=2015-11-01-preview)

Reverse engineering_

wortell
Enterprise Security

Postman_

wortell
Enterprise Security

“Postman is a collaboration platform for API development. Postman's features simplify each step of building an API and streamline collaboration so you can create better APIs—faster.”



POSTMAN

Demo_

wortell
Enterprise Security

AzSentinel_

wortell
Enterprise Security

AzSentinel_



wortell / AZSentinel

Unwatch 10 Unstar 31 Fork 10

Code Issues 3 Pull requests 0 Actions Projects 0 Wiki Security Insights Settings

PowerShell module for Azure Sentinel

powershell azure security sentinel Manage topics

39 commits 1 branch 0 packages 2 releases 3 contributors MIT

Branch: master New pull request Create new file Upload files Find file Clone or download

pkhabazi Bug fixes - version 0.6.1 (#24) Latest commit a9f791f on Oct 15

.github	Revert "Build"	last month
.vscode	removed recommended extensions as most don't help the project	2 months ago
AzSentinel	Bug fixes - version 0.6.1 (#24)	last month
Tests	Revert "Build"	last month
docs	Revert "Build"	last month
examples	Bug fixes - version 0.6.1 (#24)	last month
.gitignore	Revert "Build"	last month
CONTRIBUTING.md	init release v 0.0.1	3 months ago
LICENSE	init release v 0.0.2	3 months ago
README.md	Bug fixes - version 0.6.1 (#24)	last month
changelog.md	Bug fixes - version 0.6.1 (#24)	last month

README.md

Azure Sentinel

Azure Sentinel is a cloud-native SIEM that provides intelligent security analytics for your entire enterprise at cloud scale. Get limitless cloud speed and scale to help focus on what really matters. Easily collect data from all your cloud or on-premises assets, Office 365, Azure resources, and other clouds. Effectively detect threats with built-in machine learning from Microsoft's security analytics experts. Automate threat response, using built-in orchestration and automation playbooks. [read more](#)

Functions_

- Set-AzSentinel
- New-AzSentinelAlertRule
- Get-AzSentinelAlertRule
- Import-AzSentinelAlertRule
- Remove-AzSentinelAlertRule
- Get-AzSentinelIncident
- Get-AzSentinelHuntingRule
- New-AzSentinelHuntingRule
- Remove-AzSentinelHuntingRule
- Import-AzSentinelHuntingRule

<https://github.com/wortell/AZSentinel>

JSON format alert_

To create a Azure Sentinel Rule, use the following JSON format.

```
{
  "analytics": [
    {
      "displayName": "string",
      "description": "string",
      "severity": "High",
      "enabled": true,
      "query": "SecurityEvent | where EventID == \"4688\" | where CommandLine contains \"-noni -ep bypass $\"",
      "queryFrequency": "5H",
      "queryPeriod": "5H",
      "triggerOperator": "GreaterThan",
      "triggerThreshold": 5,
      "suppressionDuration": "6H",
      "suppressionEnabled": false,
      "tactics": [
        "Persistence",
        "LateralMovement",
        "Collection"
      ]
    }
  ]
}
```


JSON format hunting_

```
{
  .."analytics": [
    ...{
      ..."displayName": "string",
      ..."description": "string",
      ..."query": "SecurityEvent | where EventID = \"4688\" | where CommandLine contains \"-noni -ep bypass $\"",
      ..."tactics": [
        ..."Persistence",
        ..."LateralMovement",
        ..."Collection"
      ]
    }
  ]
}
```

JSON property values_

The following tables describe the values you need to set in the schema.

Name	Type	Required	Allowed Values	Example
displayName	string	yes	*	DisplayName
description	string	yes	*	Description
severity	string	yes	Medium, High, Low, Informational	Medium
enabled	bool	yes	true, false	true
query	string	yes	special character need to be escaped by \	SecurityEvent where EventID == "4688" where CommandLine contains "\"-noni -ep bypass \$\"
queryFrequency	string	yes	Value must be between 5 minutes and 24 hours	5H
queryPeriod	string	yes	Value must be between 5 minutes and 24 hours	1440M
triggerOperator	string	yes	GreaterThan, FewerThan, EqualTo, NotEqualTo	GreaterThan
triggerThreshold	int	yes	The value must be between 0 and 10000	5
suppressionDuration	string	yes	Value must be between 5 minutes and 24 hours	11H
suppressionEnabled	bool	yes	true, false	true
tactics	array	yes	InitialAccess, Persistence, Execution, PrivilegeEscalation, DefenseEvasion, CredentialAccess, LateralMovement, Discovery, Collection, Exfiltration, CommandAndControl, Impact	true

Demo_

wortell
Enterprise Security

PowerShell Gallery_

<https://www.powershellgallery.com/packages/AzSentinel>



AzSentinel 0.6.1

PowerShell module for Azure Sentinel

Minimum PowerShell version
6.2

Installation Options

Install Module

Azure Automation

Manual Download

Copy and Paste the following command to install this package using PowerShellGet [More Info](#)

PS> Install-Module -Name AzSentinel

Author(s)
Pouyan Khabazi

Copyright
(c) Wortell Enterprise Security BV. All rights reserved.

> Package Details

> FileList

> Version History

Version	Downloads	Last updated
0.6.1 (current version)	219	a month ago
0.6.0	24	2 months ago

Sentinel library_



<https://github.com/netevert/sentinel-analytics-library>

netevert / sentinel-analytics-library

Watch

4

Star

16

Fork

2

Code

Issues2

Pull requests0

Actions

Projects0

Wiki

Security

Insights

The largest Sentinel detection use case library; built in AZSentinel JSON format for automated upload into Azure

azureazure-sentineluse-casesdetectionsiemdfirkustojsonpowershell

6 commits

1 branch

0 packages

0 releases

1 contributor

Branch: master

New pull request

Create new file

Upload files

Find file

Clone or download

netevert Updates and improvements

Latest commit 93e6f78 on Sep 24

AWSCloudTrail	Added microsoft detections	2 months ago
AuditLogs	Added microsoft detections	2 months ago
AzureActivity	Added microsoft detections	2 months ago
AzureDiagnostics	Added microsoft detections	2 months ago
CommonSecurityLog	Added microsoft detections	2 months ago
DnsEvents	Added microsoft detections	2 months ago
MultipleDataSources	Added microsoft detections	2 months ago
OfficeActivity	Added microsoft detections	2 months ago
SecurityEvent	Added microsoft detections	2 months ago
SigninLogs	Added microsoft detections	2 months ago
Syslog	Added microsoft detections	2 months ago
Sysmon	Minor fix	2 months ago
ThreatIntelligenceIndicator	Added microsoft detections	2 months ago
W3CIISLog	Added microsoft detections	2 months ago
README.md	Updates and improvements	2 months ago

README.md

maintained

yes

last commit

september

Total rules

217

Follow @netevert

392

Sentinel analytics library



Win een
Ninjacat t-shirt





<https://security.wortell.nl>