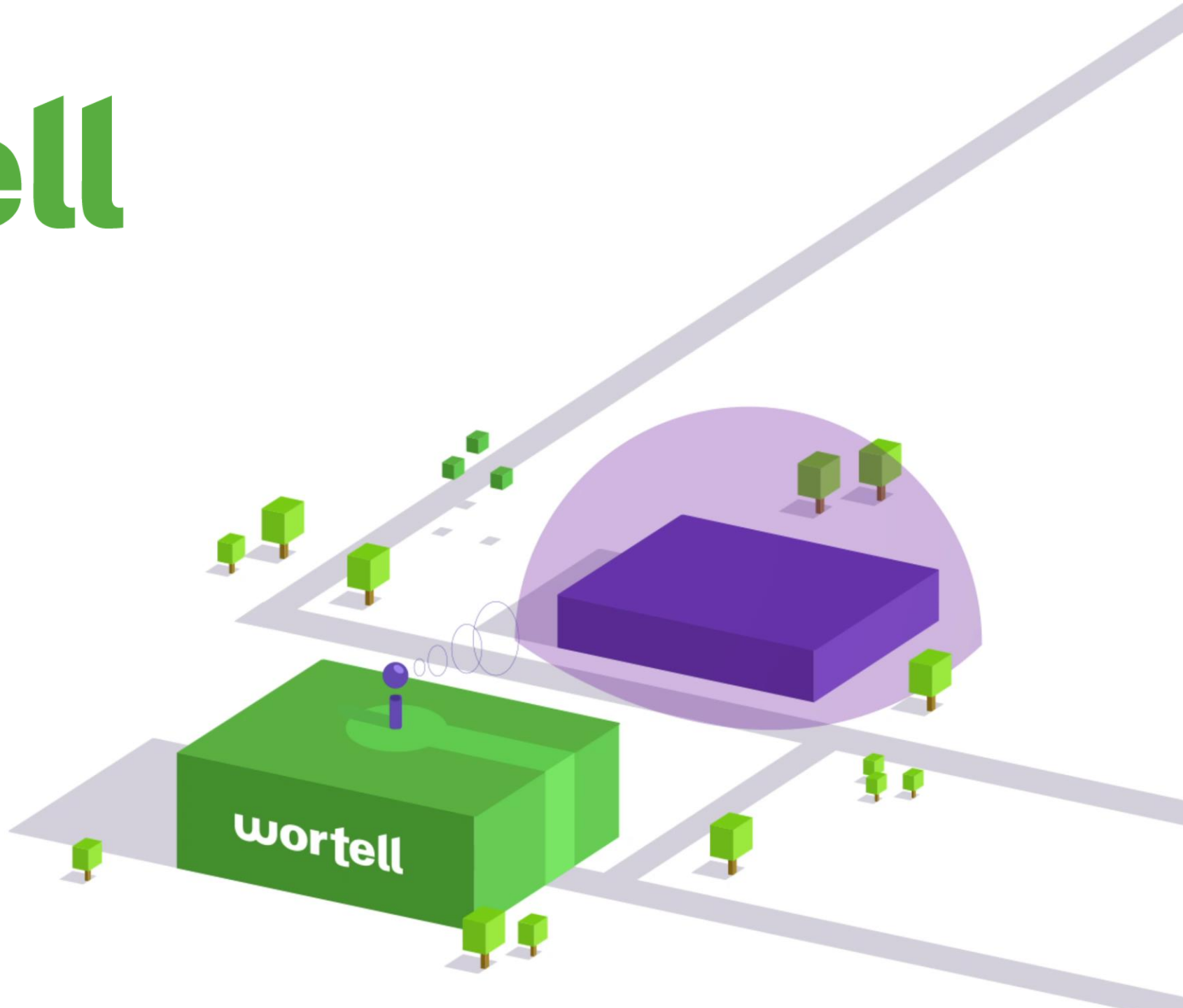
wortell

Enterprise Security



Reverse engineering Azure Sentinel to craft a PowerShell module_

wortell

Enterprise Security

wortell
Enterprise Security

Pouyan Khabazi
Cloud & Security Consultant_

pkm-technology.com

@pkhabazi

@pkhabazi

Subjects_

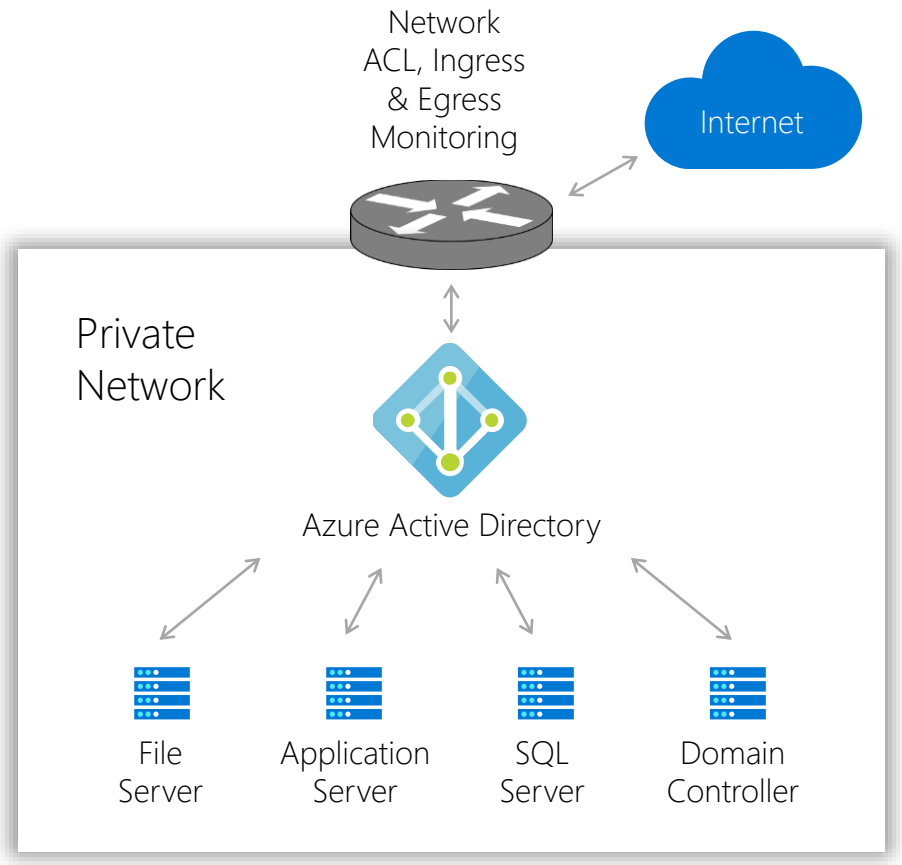
wortell
Enterprise Security

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

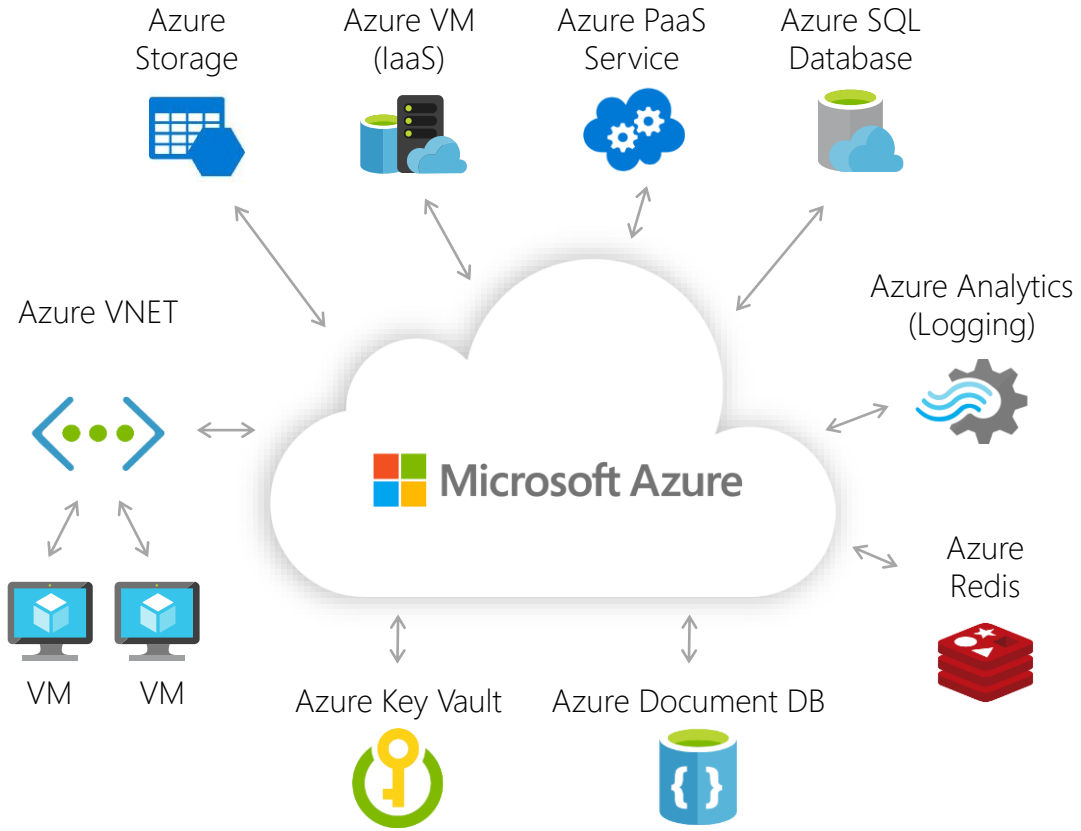
A new world to defend_

wortell
Enterprise Security

On-premise

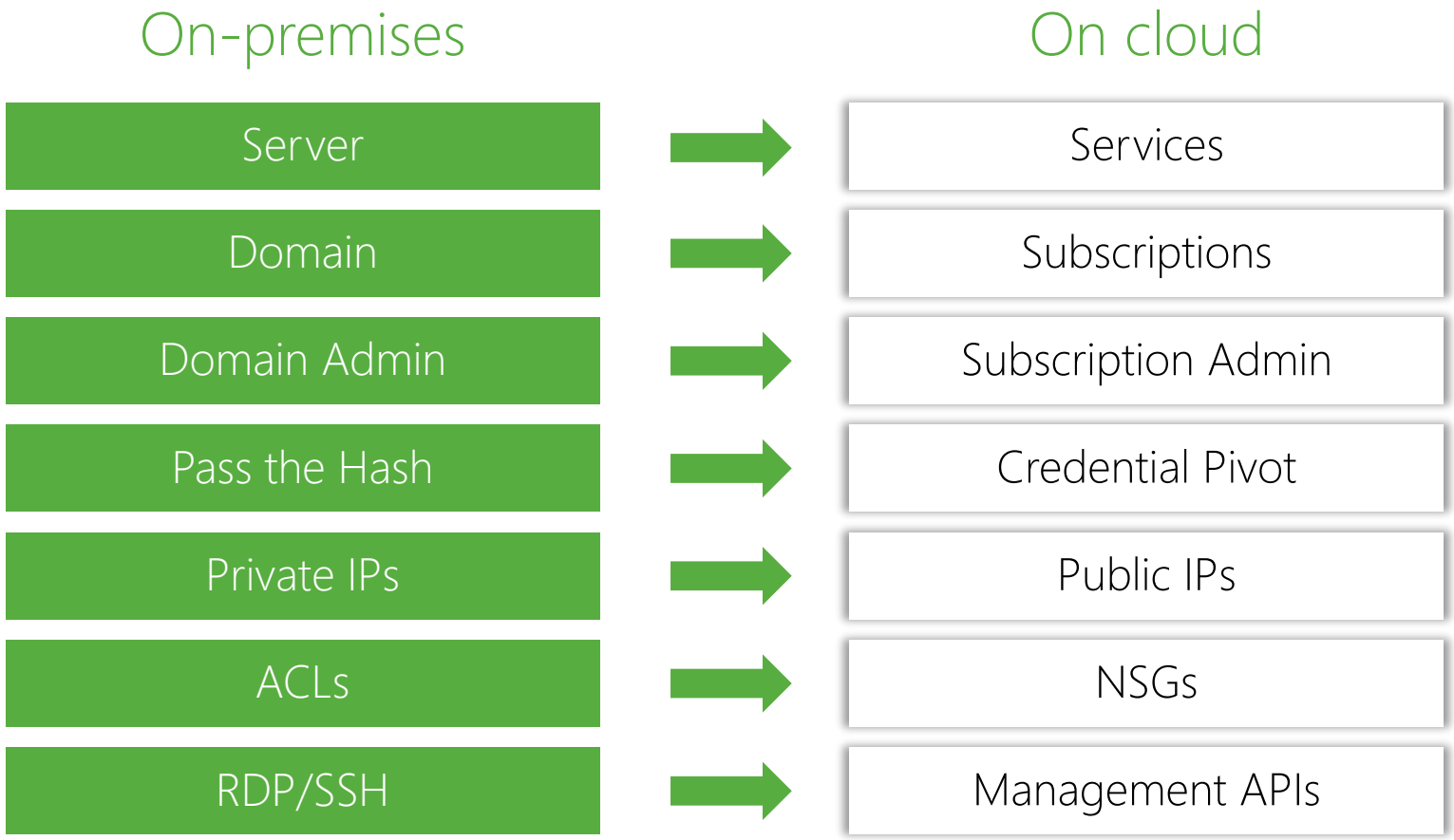


Cloud



cloud defender mindset_

wortell
Enterprise Security



Azure Sentinel_

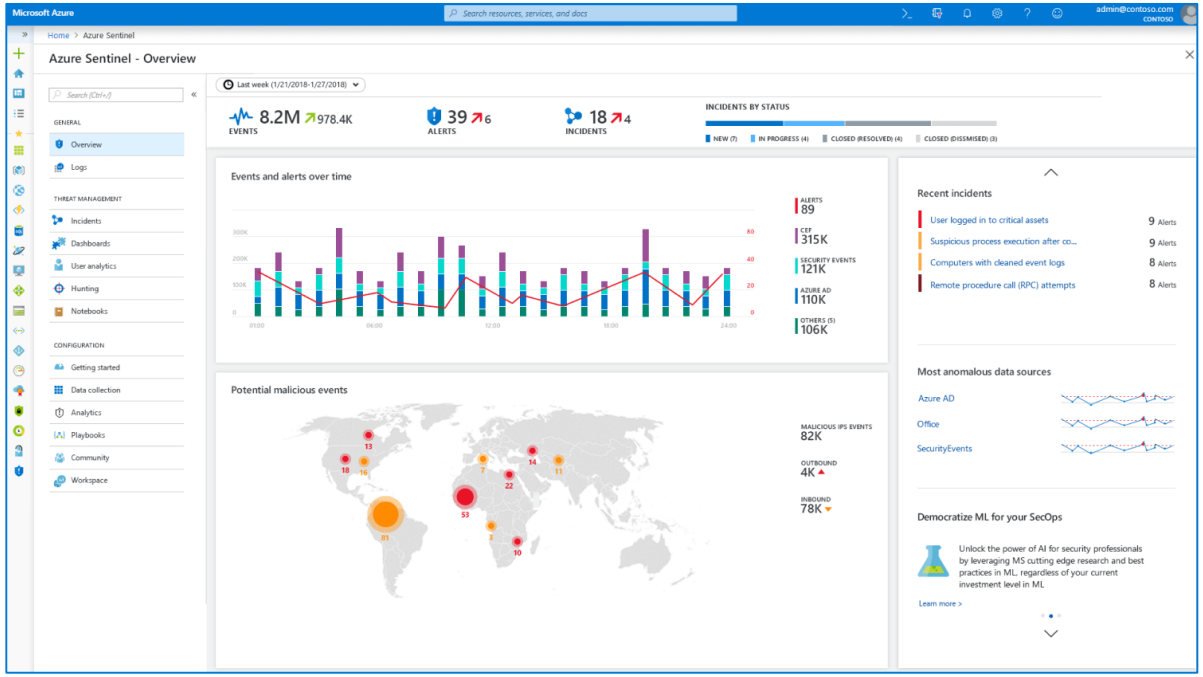
wortell

Enterprise Security

Azure Sentinel_

wortell
Enterprise Security

- cloud-native siem
- limitless cloud speed & scale
- a.i. built-in
- easy integration
- only pay for what you use

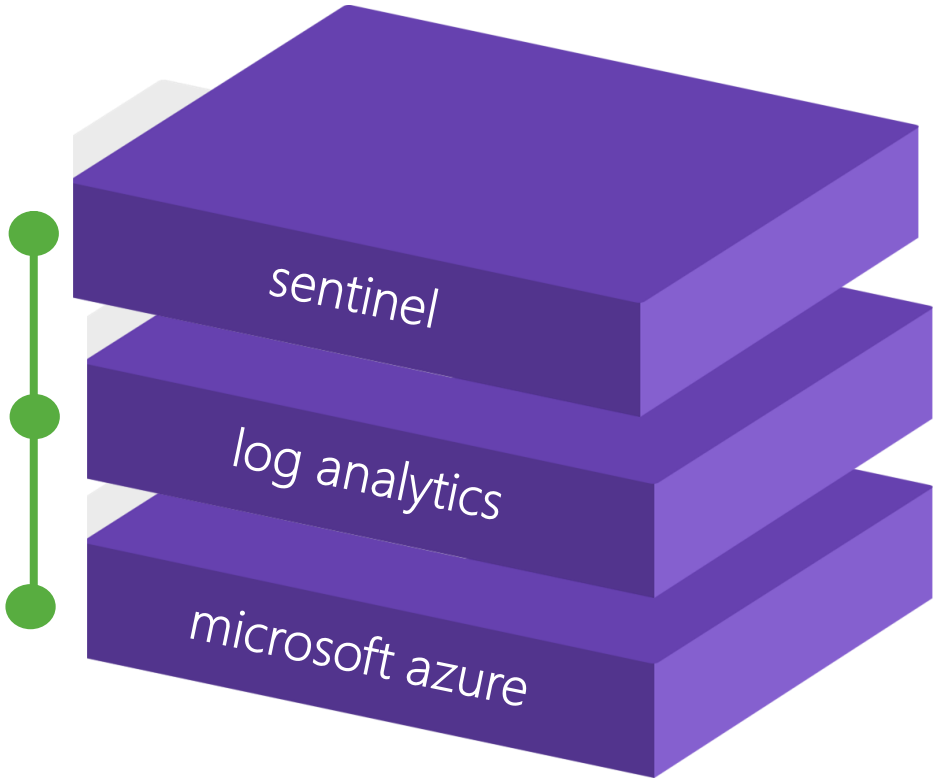


GA_

wortell
Enterprise Security

architecture_

wortell
Enterprise Security



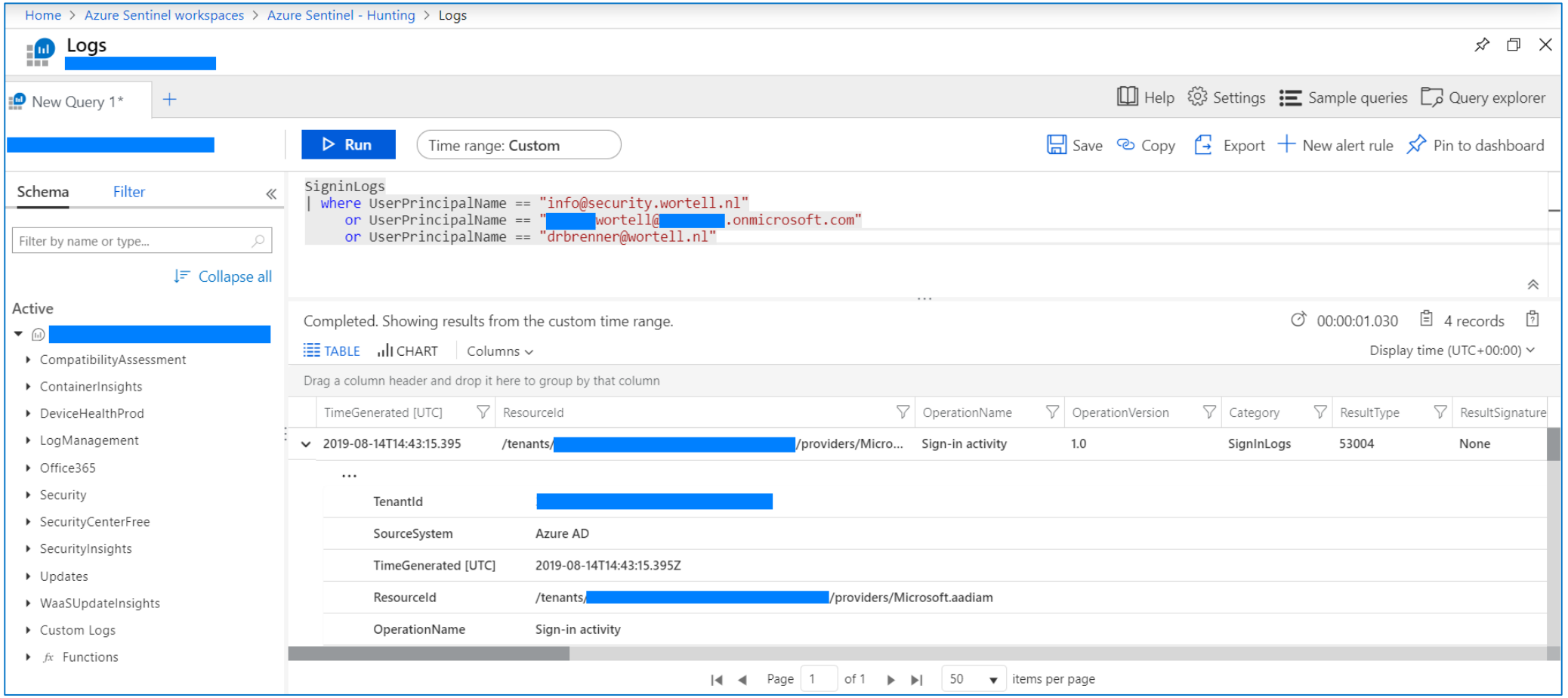
kusto-based

unlimited scale

enterprise-grade platform

KQL based_

wortell
Enterprise Security



Analytics rules_

wortell
Enterprise Security

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	Choose column	Add
Host	Choose column	Add
IP	Choose column	Add
URL	Choose column	Add

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_

wortell
Enterprise Security

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	Choose column	Add
Host	Choose column	Add
IP	Choose column	Add
URL	Choose column	Add
Timestamp	Choose column	Add

Tactics

3 selected

data connections_

wortell
Enterprise Security

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_

wortell

Enterprise Security

ARM_

wortell
Enterprise Security

Consistent Management Layer

Tools

Microsoft Azure + Command Line + Visual Studio

SERVICE MANAGEMENT API

RESOURCE MANAGER

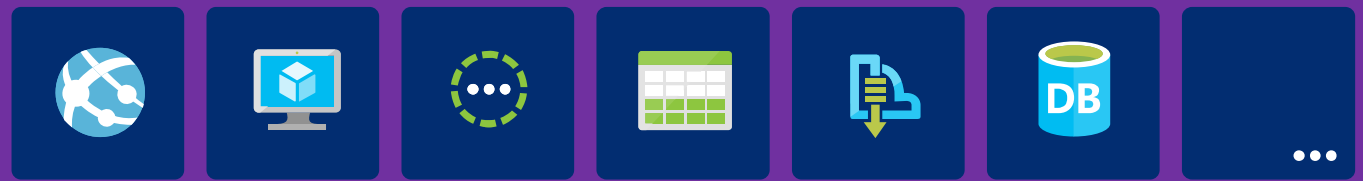
Cloud + On-Premises

ADFS

AAD

RESOURCE PROVIDER CONTRACT

Provider Rest Points



Service Management REST API Reference_

wortell
Enterprise Security

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_

wortell
Enterprise Security

{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

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

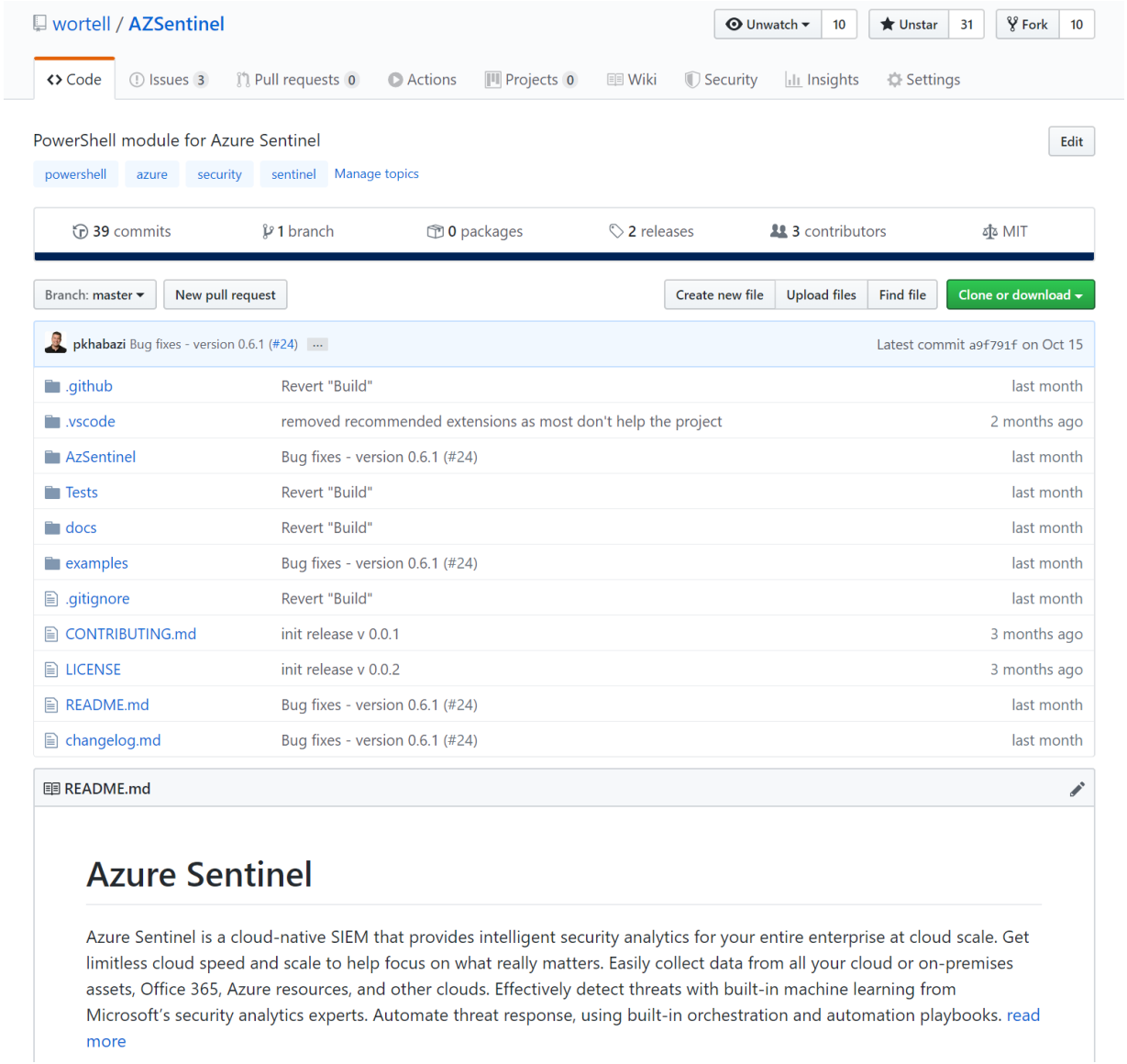
AzSentinel_

wortell

Enterprise Security

AzSentinel_

wortell
Enterprise Security



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_

wortell
Enterprise Security

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_

wortell
Enterprise Security

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

JSON property values_

wortell
Enterprise Security

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_

wortell
Enterprise Security

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

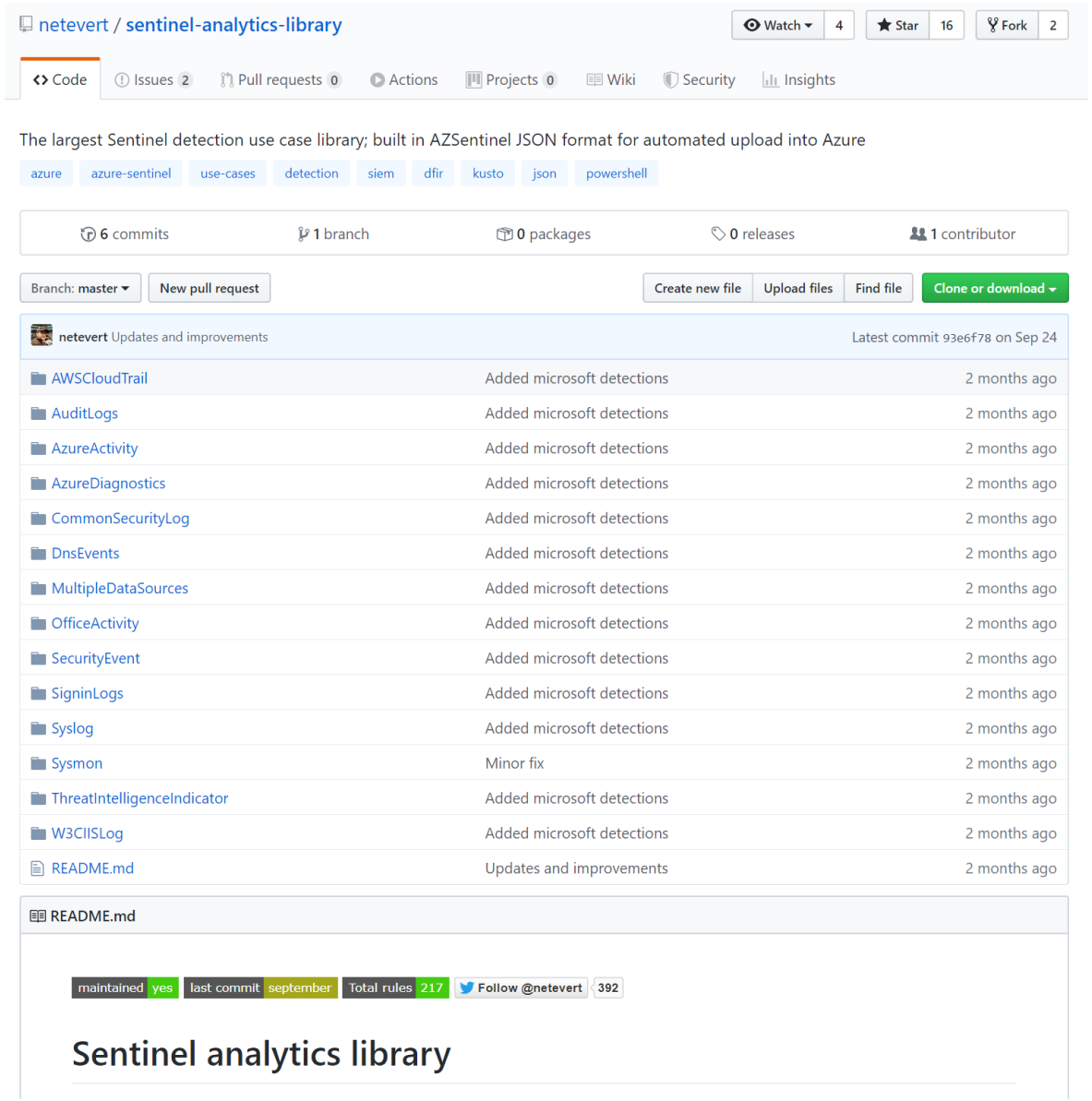
Version History

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

Sentinel library_

wortell
Enterprise Security

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



netevert / sentinel-analytics-library

Watch 4 | Star 16 | Fork 2

Code | Issues 2 | Pull requests 0 | Actions | Projects 0 | Wiki | Security | Insights

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

azure | azure-sentinel | use-cases | detection | siem | dfir | kusto | json | powershell

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

ENTERPRISE SECURITY

WORTELL

Win een Ninjacat t-shirt

https://security.wortell.nl