Microsoft Azure Sentinel:

the power of Microsoft Threat protection

Maarten Goet

Microsoft Regional Director

@maarten_goet

Experts Live Asia Pacific

MVP

RD

Experts Live

Agenda

- Cybersecurity landscape
- How attackers think
- Microsoft Threat Protection
- Azure Sentinel

Experts Live Asia Pacific

"CYBER SECURITY IS A **CEO ISSUE.**"

-MCKINSEY

$4.0M

is the average cost of a data breach per incident.

81%

of breaches involve weak or stolen passwords.

>300K

new malware samples are created and spread every day.

87%

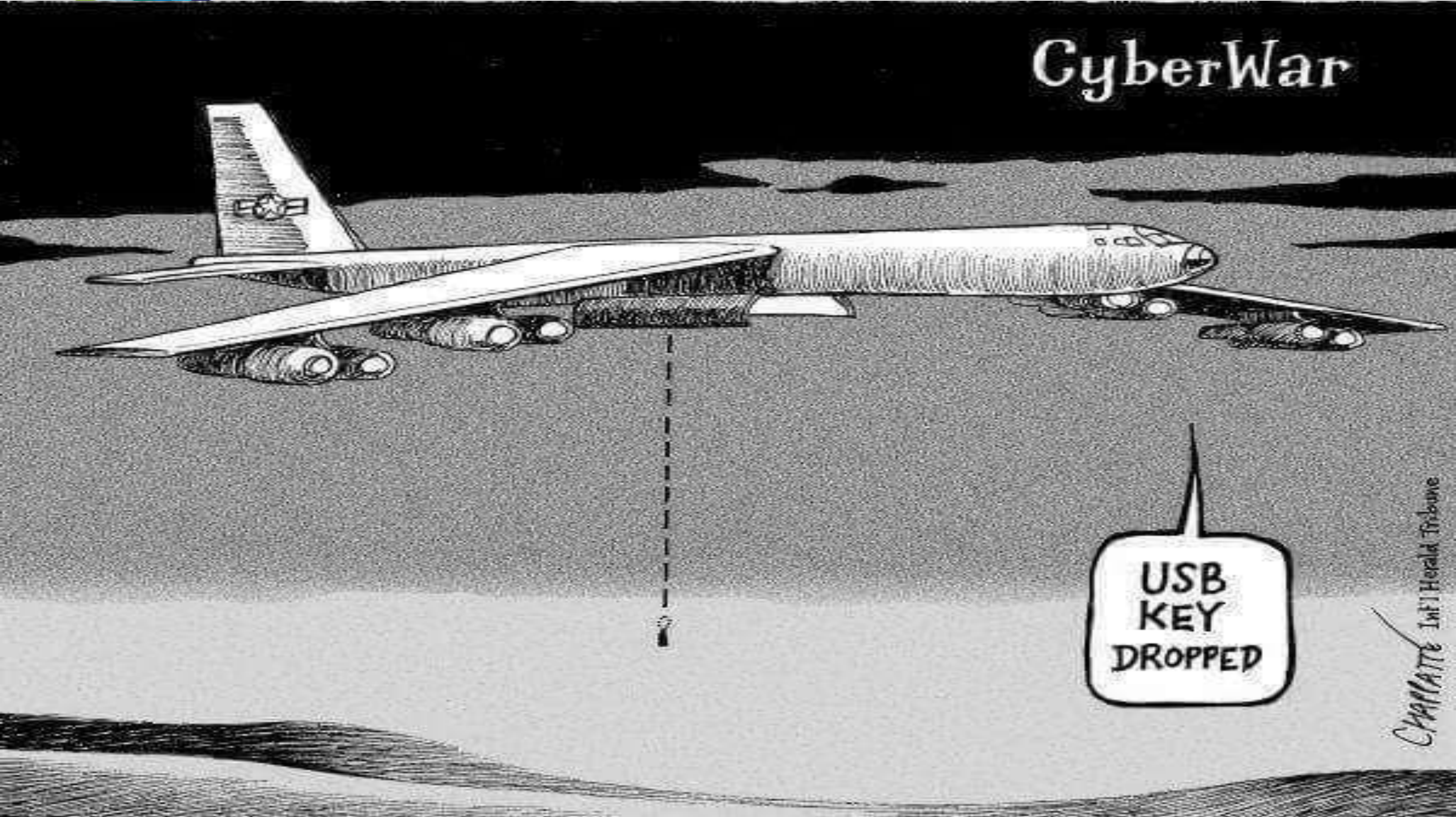
of senior managers have admitted to accidentally leaking business data.

CYBER THREATS ARE A **MATERIAL RISK** TO YOUR BUSINESS

Cybersecurity landscape

- Ransomware is down, crypto mining is up
- Phishing is still a problem
- Fileless attacks are on the rise
- Impact on business downtime more $$ than ever
- Breaches that linger
- Industrial control systems are vulnerable

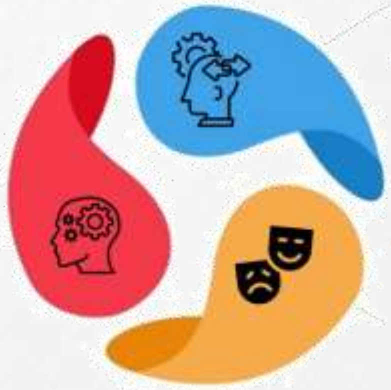
It's about people



CyberWar
USB KEY DROPPED
Chappatte
Int'l Herald Tribune

Cybersecurity culture

- Cybersecurity culture = attitude * behavior * knowledge
- CSC = A * B * K



Behaviors

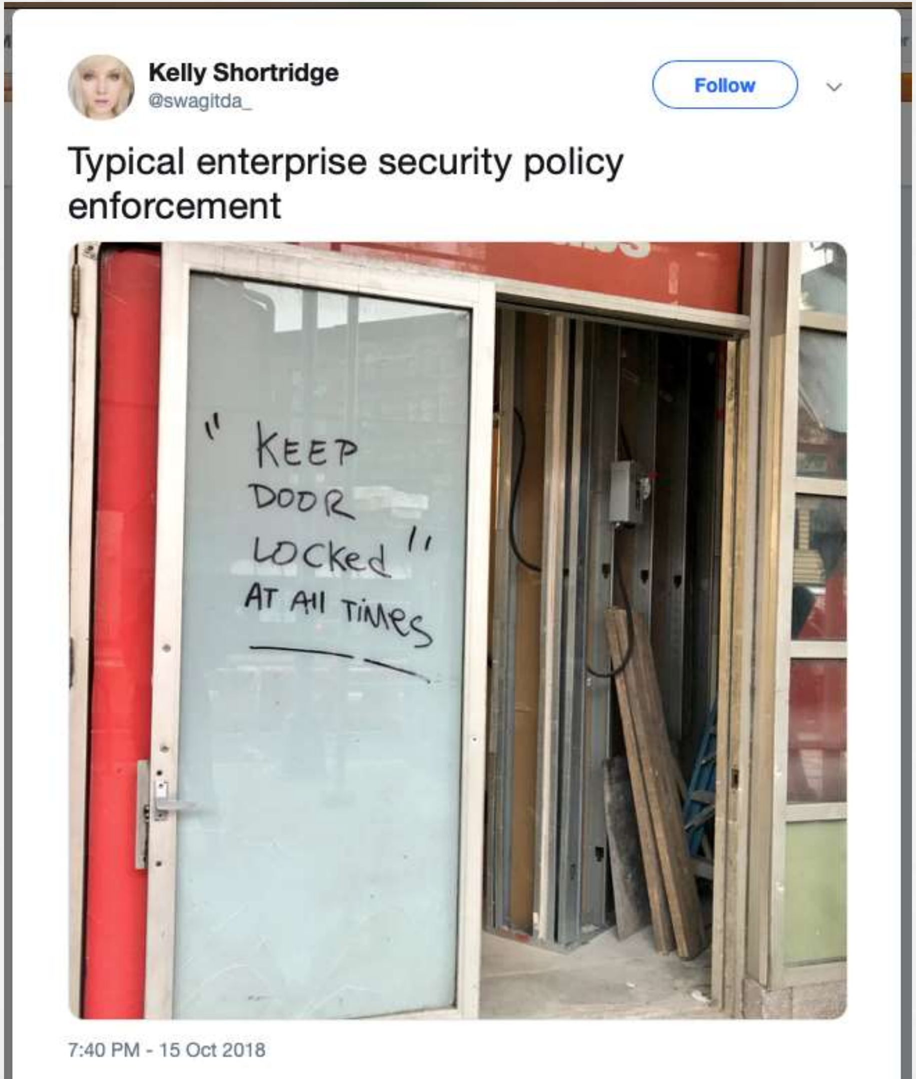
Actual or intended activities and risk-taking actions of employees that have direct or indirect impact on cybersecurity culture

Cognitions or Knowledge

Employees awareness, verifiable knowledge and beliefs regarding practices, activities and self-efficacy that are related to organizational security

Attitudes

Employees' feelings and emotions about the various activities that pertain to organizational security

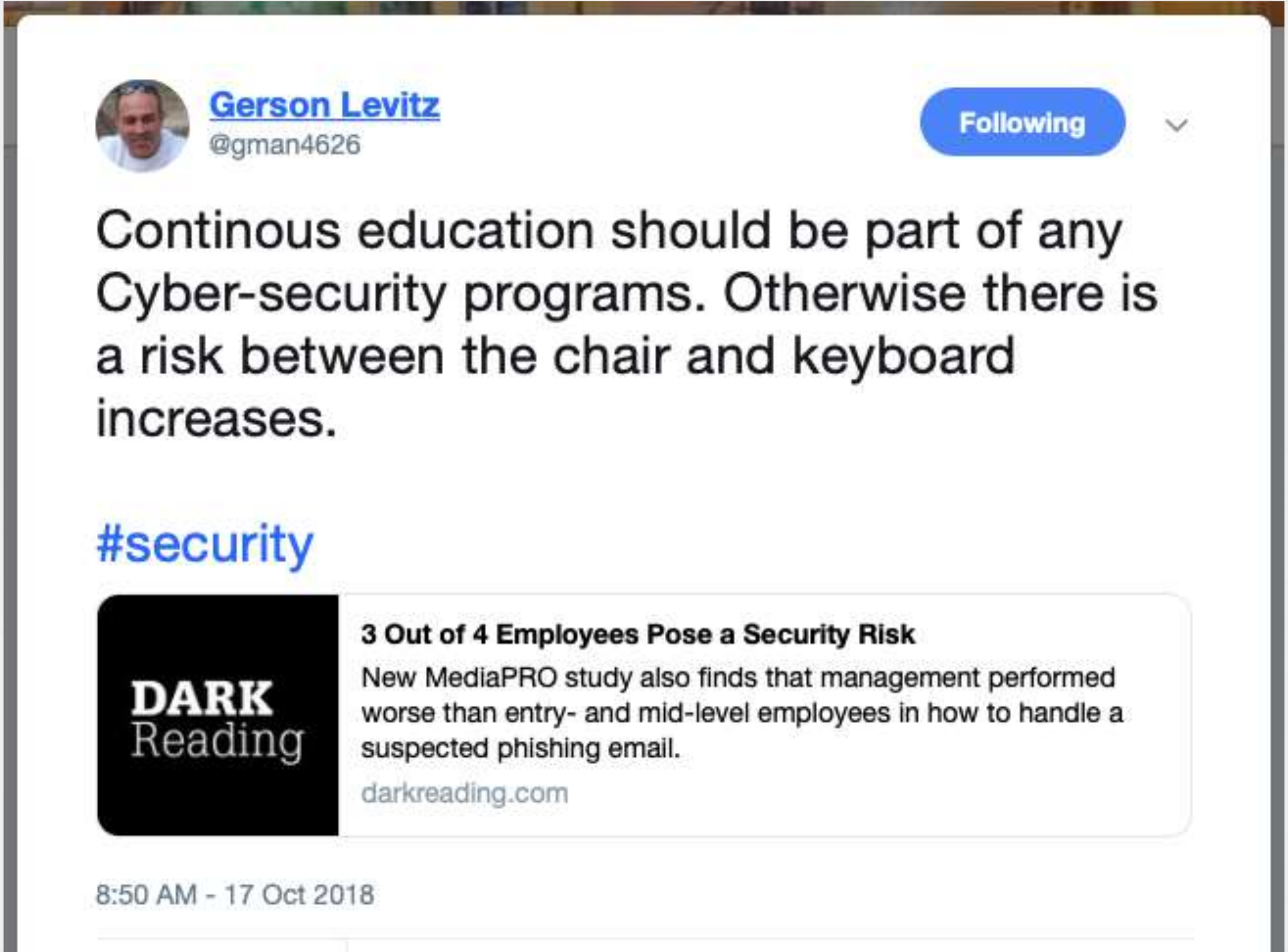


Kelly Shortridge
@swagitda_

Follow

Typical enterprise security policy enforcement

7:40 PM - 15 Oct 2018



Gerson Levitz
@gman4626

Continous education should be part of any Cyber-security programs. Otherwise there is a risk between the chair and keyboard increases.

#security

3 Out of 4 Employees Pose a Security Risk

New MediaPRO study also finds that management performed worse than entry- and mid-level employees in how to handle a suspected phishing email.

darkreading.com

8:50 AM - 17 Oct 2018

“We’re building **self-driving cars** and planning **Mars missions** –

but we haven’t even figured out how to make sure people’s

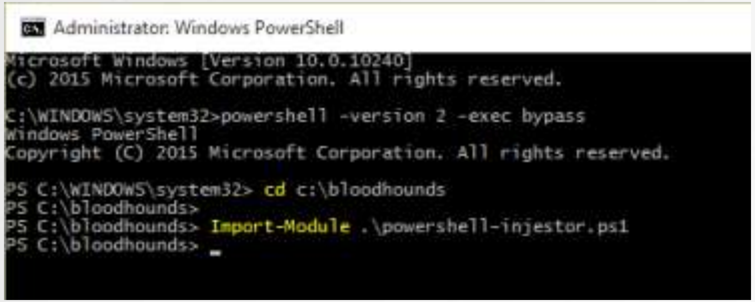
vacuum cleaners don’t join botnets..”

How attackers think

Conventional wisdom in defense

Traditional defenders	Modern defenders
Defend a list of assets	Defender a graph of assets
Manage incidents	Manage adversaries
Minimize risks by keeping incidents secret	Maximize learning by sharing incidents with trusted outside peers
View pentest results as a report card	View pentest results as input
Think about stopping attacks	They think about increasing attacker requirements

Bl00dh0und



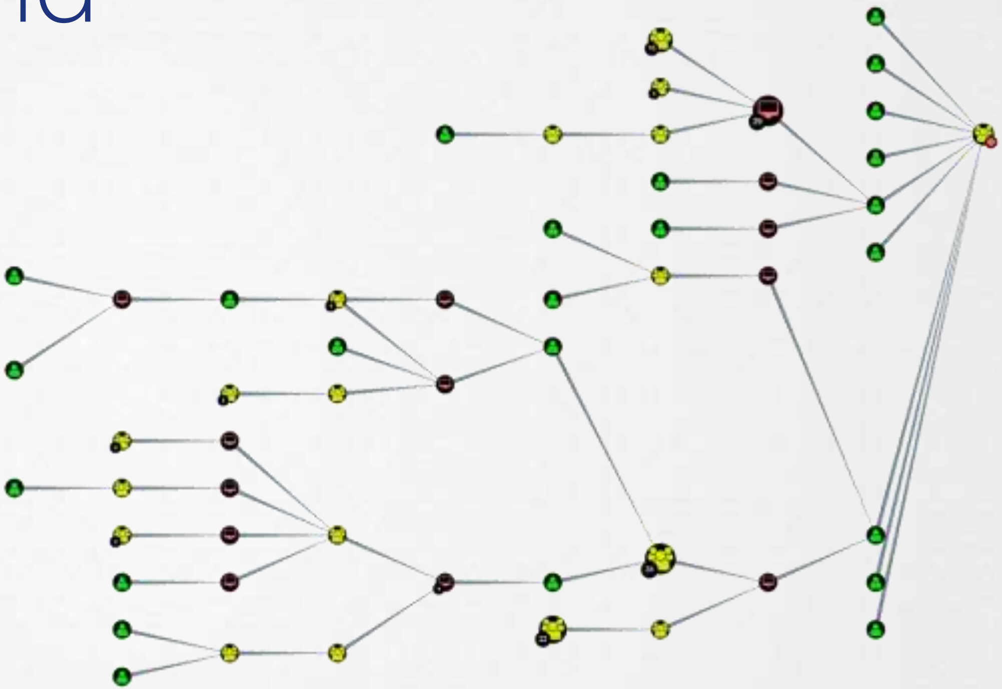
```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>powershell -version 2 -exec bypass
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> cd c:\bloodhounds
PS C:\bloodhounds>
PS C:\bloodhounds> Import-Module .\powershell-injestor.ps1
PS C:\bloodhounds> _
```

Log in to Neo4j Database

Database URL	[illegible]
DB Username	[illegible]
DB Password	[illegible]



https://github.com/BloodHoundAD/BloodHound

Microsoft Threat Protection

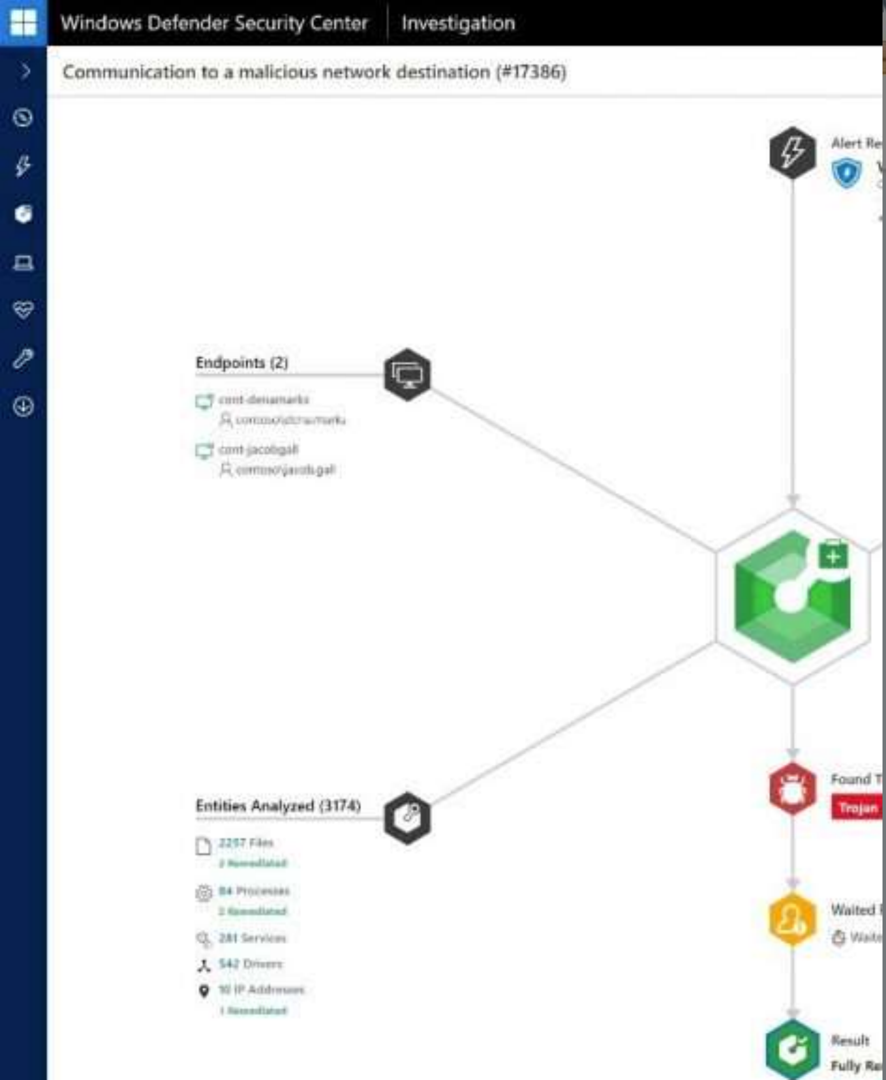
PROTECT
organizations from
advanced cyber attacks

DETECT
malicious activities

RESPOND
to threats quickly

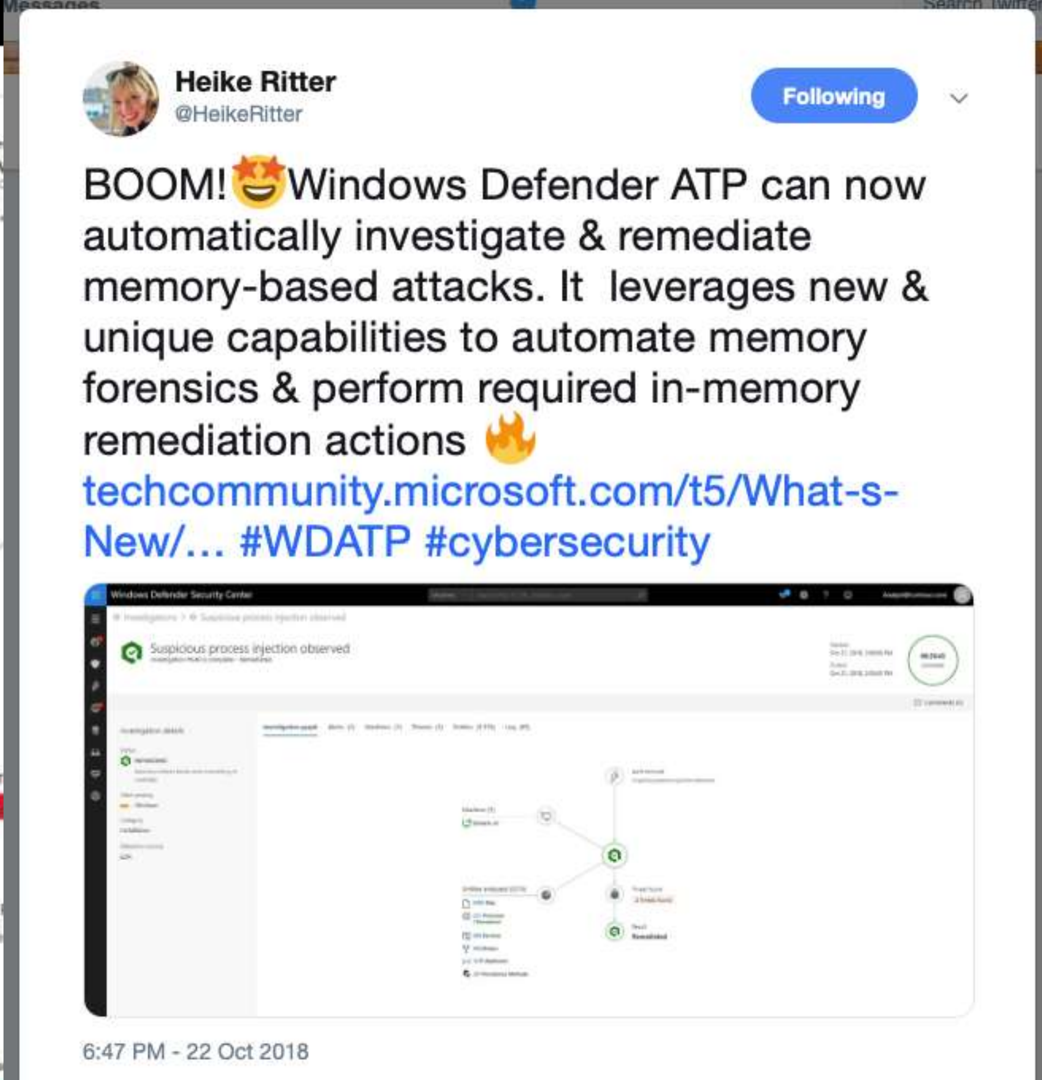
Microsoft Defender ATP

- Built-in, not bolted on
- Single pane of glass
- Unparalleled threat detections
- MacOS & Linux coming (H2 2019)
- Leveraging the power of cloud



Windows Defender Security Center | Investigation

Communication to a malicious network destination (#17386)



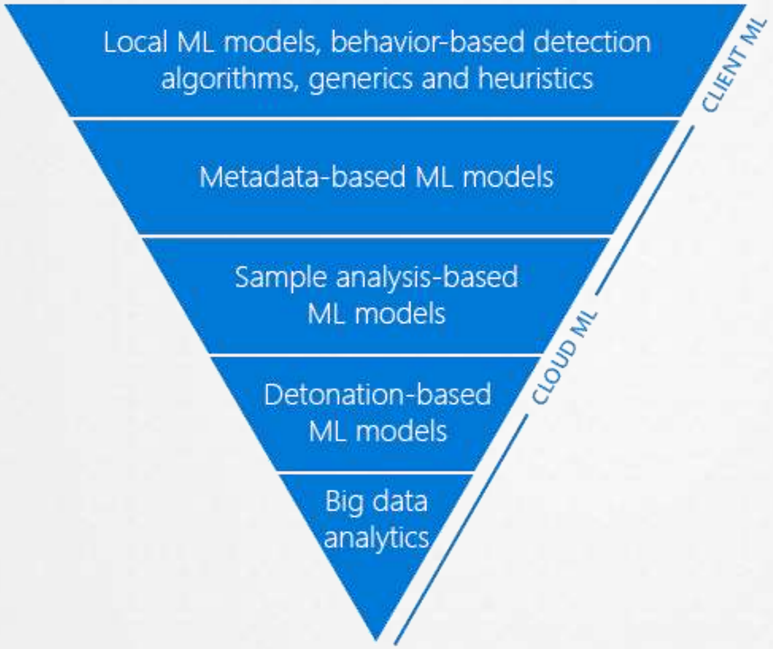
Heike Ritter
@HeikeRitter

BOOM!🤩Windows Defender ATP can now automatically investigate & remediate memory-based attacks. It leverages new & unique capabilities to automate memory forensics & perform required in-memory remediation actions 🔥 techcommunity.microsoft.com/t5/What-s-New/… #WDATP #cybersecurity

Windows Defender Security Center
Suspicious process injection observed

6:47 PM - 22 Oct 2018

Power of Cloud ML



Local ML models, behavior-based detection algorithms, generics and heuristics
Metadata-based ML models
Sample analysis-based ML models
Detonation-based ML models
Big data analytics
CLIENT ML
CLOUD ML

Protection in milliseconds
Most common malware are blocked by high-precision detection in Windows Defender AV

Protection in milliseconds
ML-powered cloud rules evaluate suspicious files based on metadata sent by the Windows Defender AV client during query

Protection in seconds
A copy of the suspicious file is uploaded for inspection by multi-class ML classifiers

Protection in minutes
The suspicious file is executed in a sandbox for dynamic analysis by multi-class ML classifiers

Protection in hours
ML models and expert rules correlated signals from a vast network of sensors to automatically classify threats

A story about a Bad Rabbit

As soon as the detonation results were available, a multi-class deep neural network (DNN) classifier that used both static and dynamic features evaluated the results and classified the sample as malware with 90.7% confidence, high enough for the cloud to start blocking.

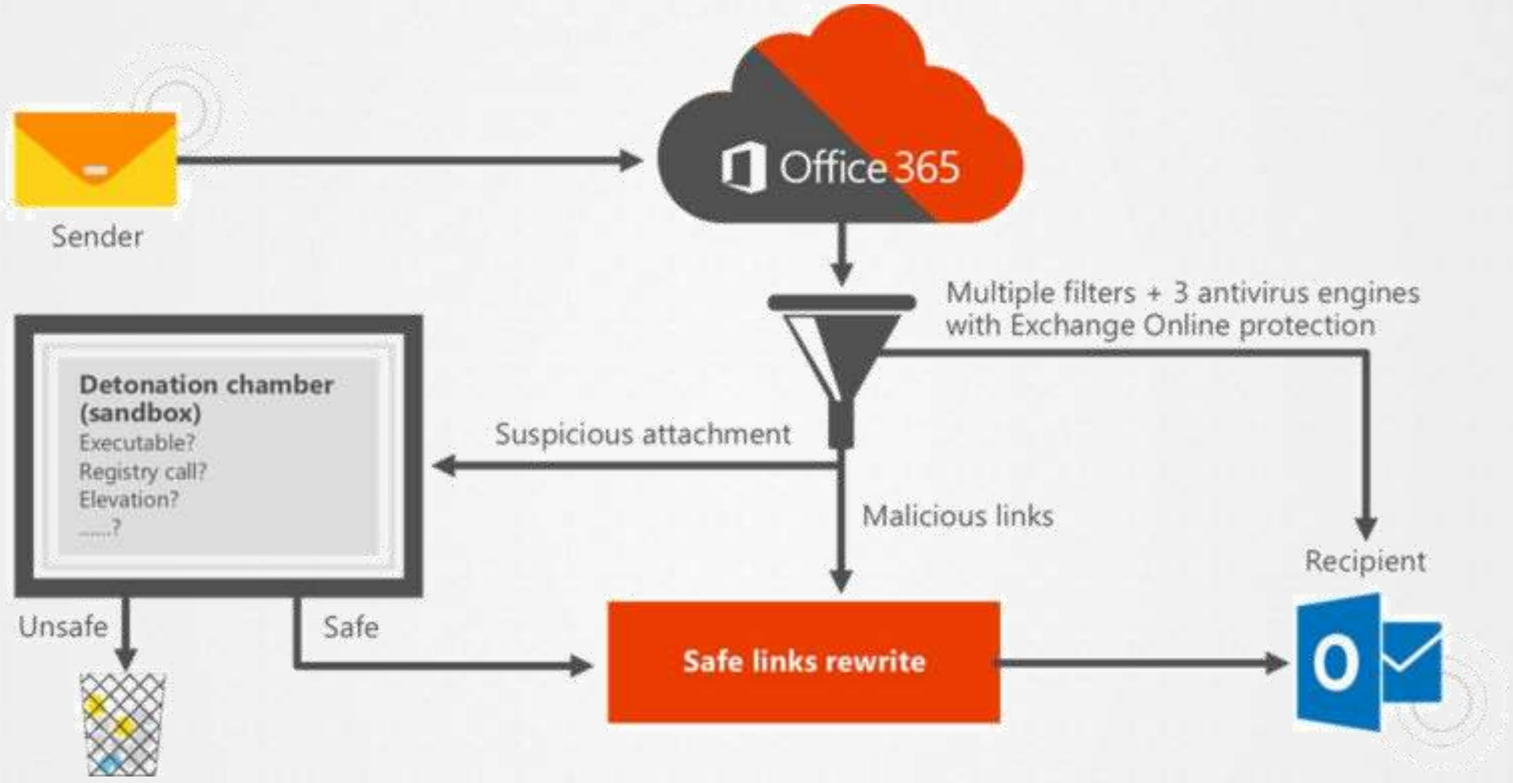
When a tenth Windows Defender ATP customer in the Ukraine was tricked into downloading the ransomware at 11:31 a.m. local time, 14 minutes after the first encounter, cloud protection service used the detonation-based malware classification to immediately protect the customer.

Microsoft Defender ATP

DEMO

Office 365 ATP

- Cloud-based intelligent filtering
- Cloud ML & detonation
- ATP safe links
- Automated investigation & response
- Attack simulators
- Threat tracking

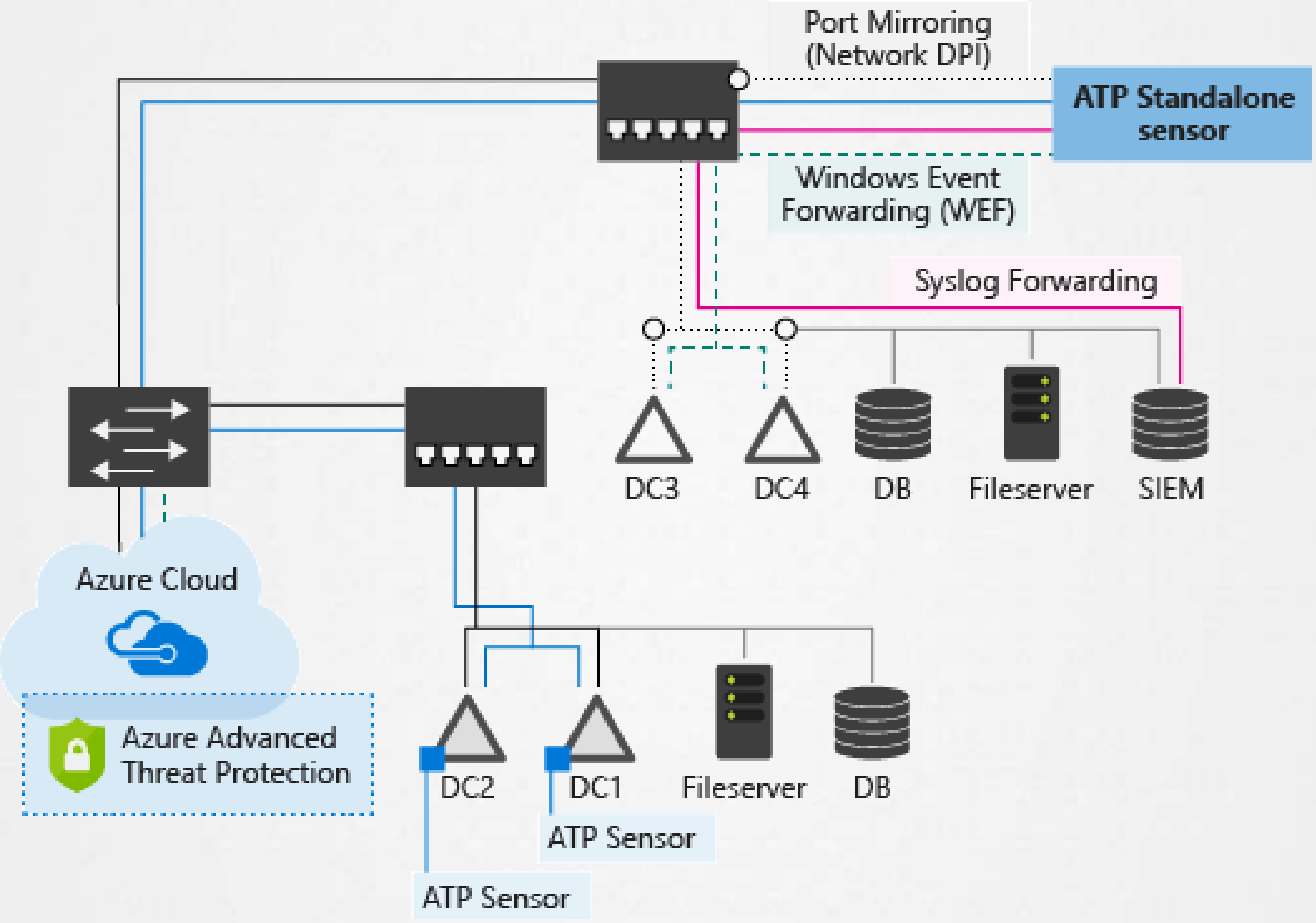

Sender
Office 365
Multiple filters + 3 antivirus engines with Exchange Online protection
Detonation chamber (sandbox)
Executable?
Registry call?
Elevation?
......?
Suspicious attachment
Malicious links
Recipient
Unsafe
Safe
Safe links rewrite

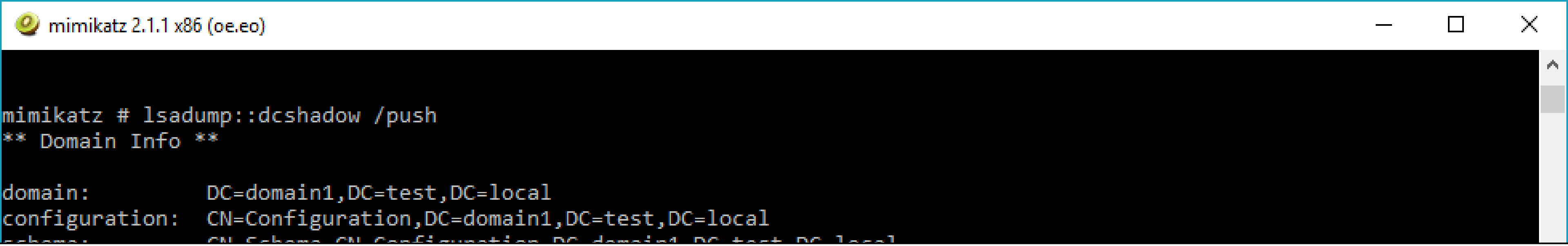
Office 365 ATP

DEMO

Azure ATP

- Detect and identify suspicious user and device activity with learning-based analytics
- Leverage threat intelligence across the cloud and on-premises environments
- Protect user identities and credentials stored in Active Directory
- Provide clear attack information on a simple timeline for fast triaging
- Monitor multiple entry points through integration with Windows Defender Advanced Threat Protection

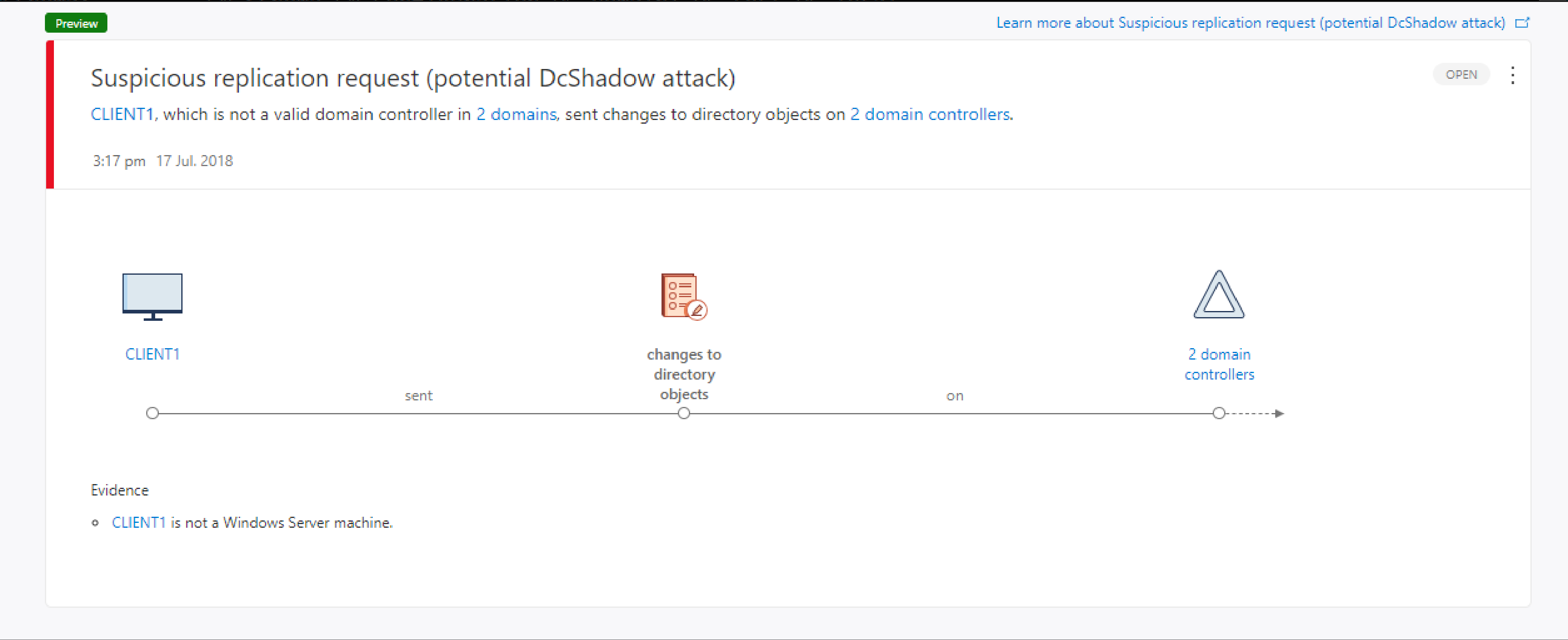

Port Mirroring (Network DPI)
ATP Standalone sensor
Windows Event Forwarding (WEF)
Syslog Forwarding
DC3
DC4
DB
Fileserver
SIEM
Azure Cloud
Azure Advanced Threat Protection
DC2
DC1
Fileserver
DB
ATP Sensor
ATP Sensor



mimikatz 2.1.1 x86 (oe.eo)

```
mimikatz # lsadump::dcshadow /push
** Domain Info **

domain:         DC=domain1,DC=test,DC=local
configuration:  CN=Configuration,DC=domain1,DC=test,DC=local
schema:         CN=Schema,CN=Configuration,DC=domain1,DC=test,DC=local
```



Preview

Learn more about Suspicious replication request (potential DcShadow attack)

Suspicious replication request (potential DcShadow attack)

OPEN

CLIENT1, which is not a valid domain controller in 2 domains, sent changes to directory objects on 2 domain controllers.

3:17 pm 17 Jul. 2018

CLIENT1 — sent — changes to directory objects — on — 2 domain controllers

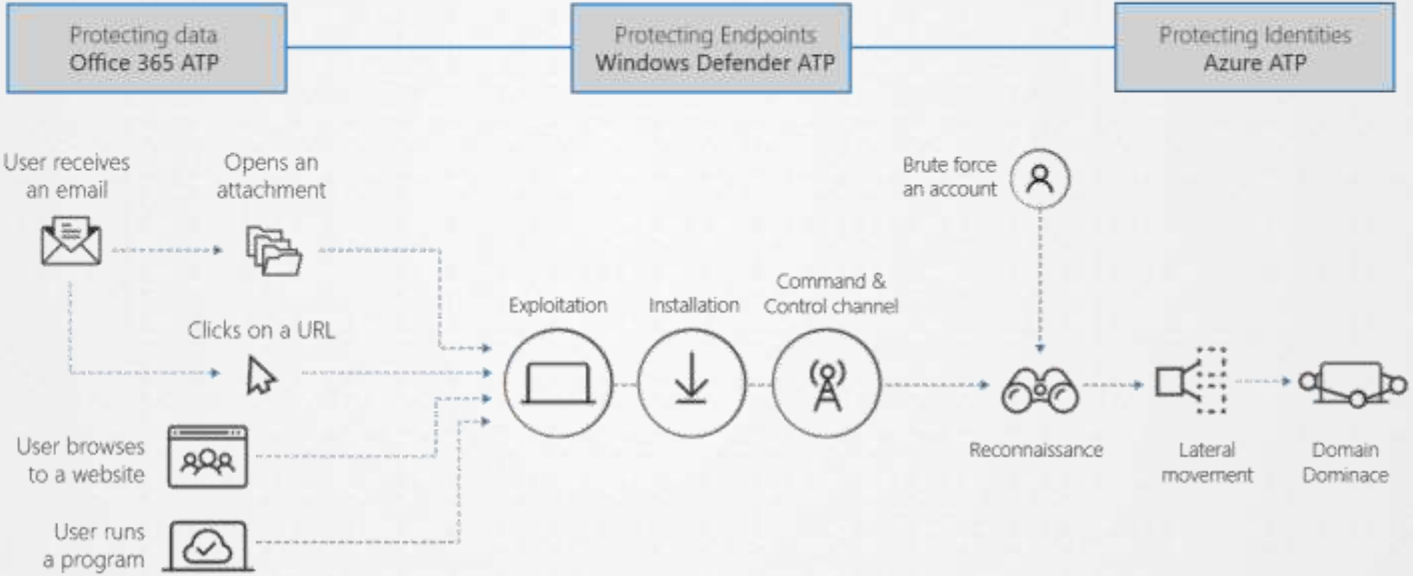
Evidence

- CLIENT1 is not a Windows Server machine.

Azure ATP

DEMO

Lateral movement



Protecting data
Office 365 ATP

Protecting Endpoints
Windows Defender ATP

Protecting Identities
Azure ATP

User receives an email

Opens an attachment

Clicks on a URL

User browses to a website

User runs a program

Exploitation

Installation

Command & Control channel

Brute force an account

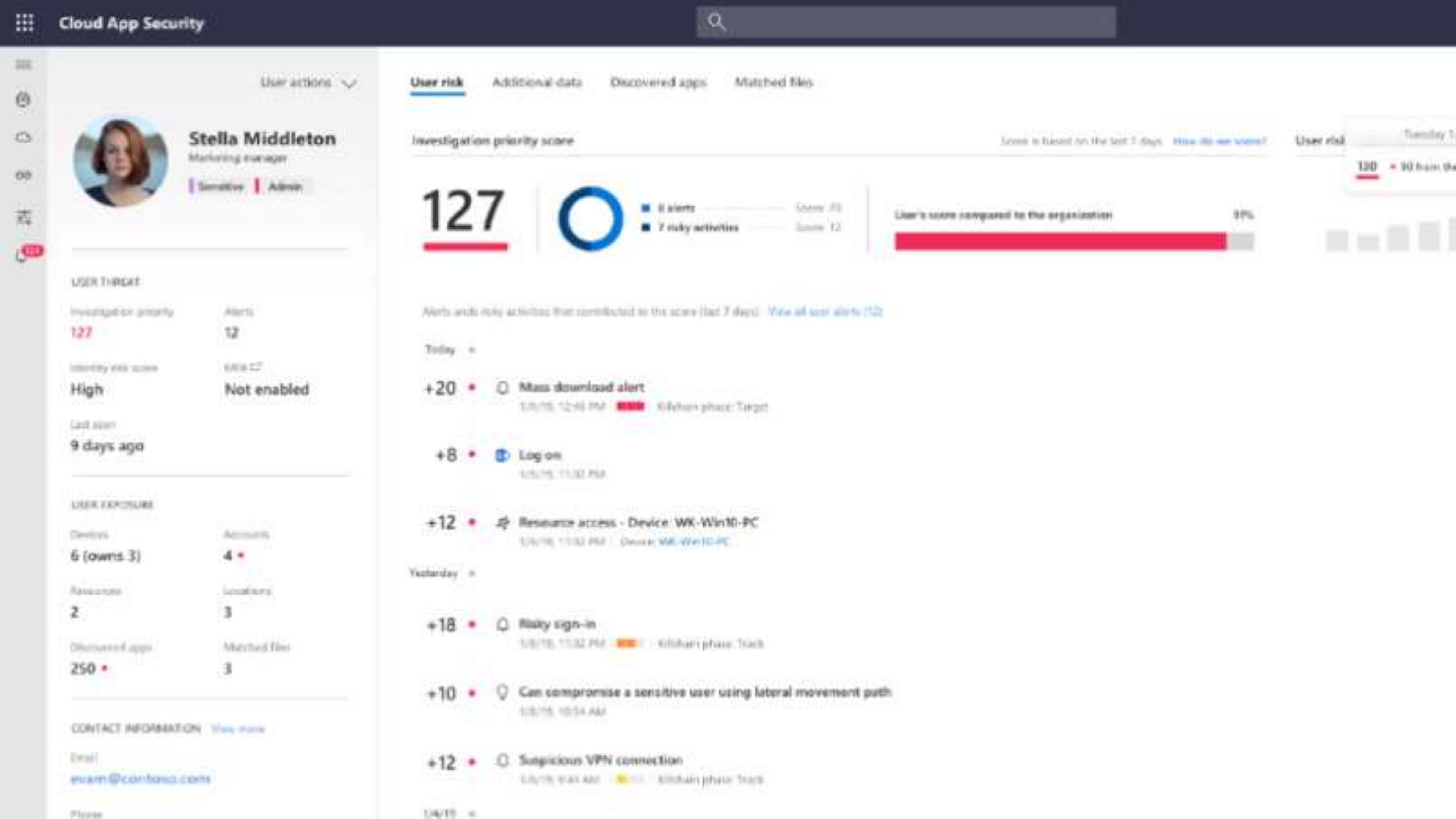
Reconnaissance

Lateral movement

Domain Dominace

MS Cloud App Security

- Cloud Access Security Broker (CASB)
- Natively integrates with Microsoft solutions (flow, Intune, SecureScore, ..)
- Discover and control the use of Shadow IT
- Protect your sensitive information anywhere in the cloud
- Assess the compliance of your cloud apps



Cloud App Security

User actions

Stella Middleton

Marketing manager

Sensitive | Admin

USER THREAT

Investigation priority
127

Alerts
12

Identity risk score
High

MFA
Not enabled

Last seen
9 days ago

USER EXPOSURE

Devices
6 (owns 3)

Accounts
4 •

Resources
2

Locations
3

Discovered apps
250 •

Matched files
3

CONTACT INFORMATION View more

Email
evanm@contoso.com

Phone

User risk | Additional data | Discovered apps | Matched files

Investigation priority score

Score is based on the last 7 days How do we score?

127

■ 8 alerts Score: 115
■ 7 risky activities Score: 12

User's score compared to the organization 93%

User risk

Tuesday 1

120 • 90 from the

Alerts and risky activities that contributed to the score (last 7 days) View all user alerts (12)

Today

+20 • Mass download alert
[illegible] Killchain phase: Target

+8 • Log on
[illegible]

+12 • Resource access - Device: WK-Win10-PC
[illegible] | Device: WK-Win10-PC

Yesterday

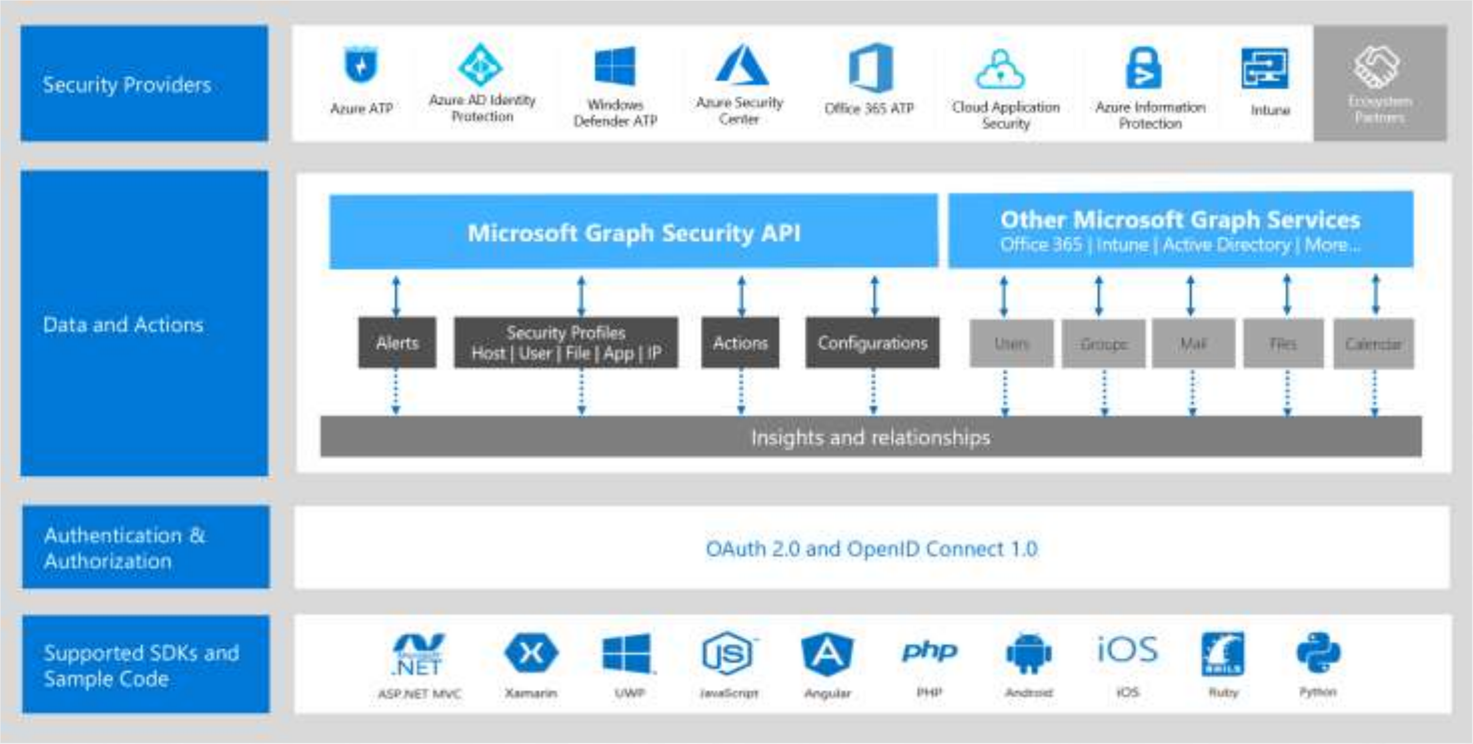
+18 • Risky sign-in
[illegible] | Killchain phase: Track

+10 • Can compromise a sensitive user using lateral movement path
[illegible]

+12 • Suspicious VPN connection
[illegible] Killchain phase: Track

[illegible]

Security Graph API



Security Providers

Azure ATP | Azure AD Identity Protection | Windows Defender ATP | Azure Security Center | Office 365 ATP | Cloud Application Security | Azure Information Protection | Intune | Ecosystem Partners

Data and Actions

Microsoft Graph Security API

Other Microsoft Graph Services
Office 365 | Intune | Active Directory | More...

Alerts | Security Profiles Host | User | File | App | IP | Actions | Configurations | Users | Groups | Mail | Files | Calendar

Insights and relationships

Authentication & Authorization

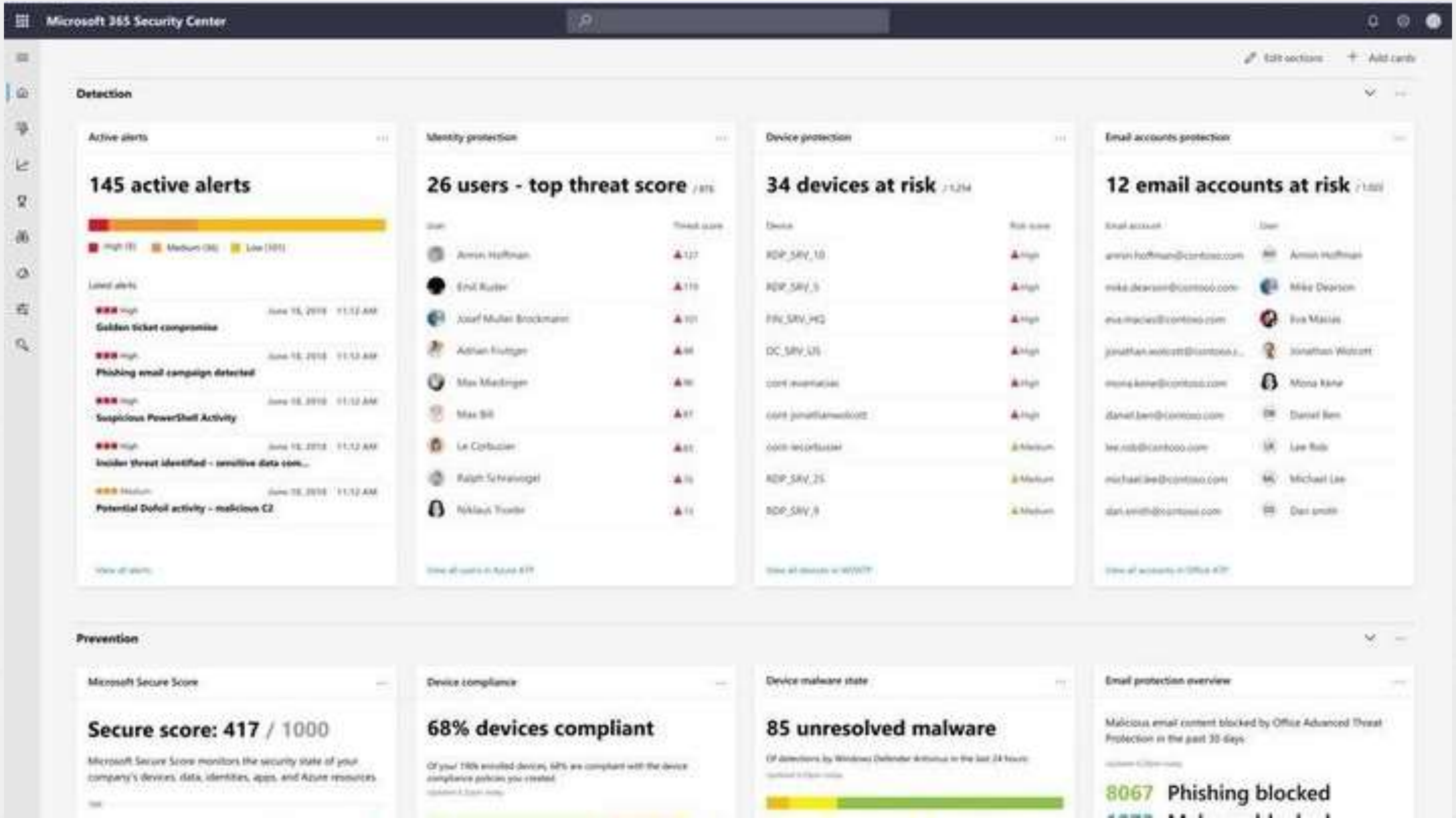
OAuth 2.0 and OpenID Connect 1.0

Supported SDKs and Sample Code

ASP.NET MVC | Xamarin | UWP | JavaScript | Angular | PHP | Android | iOS | Ruby | Python

DO YOU KNOW
WHAT THIS MEANS?

Microsoft 365 security



Microsoft 365 Security Center

Edit sections + Add cards

Detection

Active alerts

145 active alerts

🟥 High (8) 🟧 Medium (36) 🟨 Low (101)

Latest alerts

●●● High Golden ticket compromise	June 15, 2018 11:12 AM
●●● High Phishing email campaign detected	June 15, 2018 11:12 AM
●●● High Suspicious PowerShell Activity	June 15, 2018 11:12 AM
●●● High Insider threat identified - sensitive data com...	June 15, 2018 11:12 AM
●●● Medium Potential Dofoil activity - malicious C2	June 15, 2018 11:12 AM

View all alerts

Identity protection

26 users - top threat score / 815

User	Threat score
Armin Hoffman	▲127
Emil Ruder	▲119
Josef Muller Brockmann	▲101
Adrian Frutiger	▲98
Max Miedinger	▲96
Max Bill	▲87
Le Corbuzier	▲85
Ralph Schraivogel	▲76
Niklaus Troxler	▲72

View all users in Azure ATP

Device protection

34 devices at risk / 1,214

Device	Risk score
RDP_SRV_10	▲High
RDP_SRV_5	▲High
FIN_SRV_HQ	▲High
DC_SRV_US	▲High
cont evamacias	▲High
cont jonathanwolcott	▲High
cont lecorbusier	▲Medium
RDP_SRV_25	▲Medium
RDP_SRV_8	▲Medium

View all devices in WDATP

Email accounts protection

12 email accounts at risk / 1,800

Email account	User
armin.hoffman@contoso.com	Armin Hoffman
mike.dearson@contoso.com	Mike Dearson
eva.macias@contoso.com	Eva Macias
jonathan.wolcott@contoso.c...	Jonathan Wolcott
mona.kene@contoso.com	Mona Kene
daniel.ben@contoso.com	Daniel Ben
lee.rob@contoso.com	Lee Rob
michael.lee@contoso.com	Michael Lee
dan.smith@contoso.com	Dan smith

View all accounts in Office ATP

Prevention

Microsoft Secure Score

Secure score: 417 / 1000

Microsoft Secure Score monitors the security state of your company's devices, data, identities, apps, and Azure resources

Device compliance

68% devices compliant

Of your 190k enrolled devices, 68% are compliant with the device compliance policies you created

Device malware state

85 unresolved malware

Of detections by Windows Defender Antivirus in the last 24 hours

Email protection overview

Malicious email content blocked by Office Advanced Threat Protection in the past 30 days

8067 Phishing blocked

Azure Sentinel

Cloud SIEM for a Cloud world

- Azure Sentinel is SIEM-as-a-Service
- Built for a cloud world
- On top of technology you already know and love <3
  - Azure
  - Log Analytics

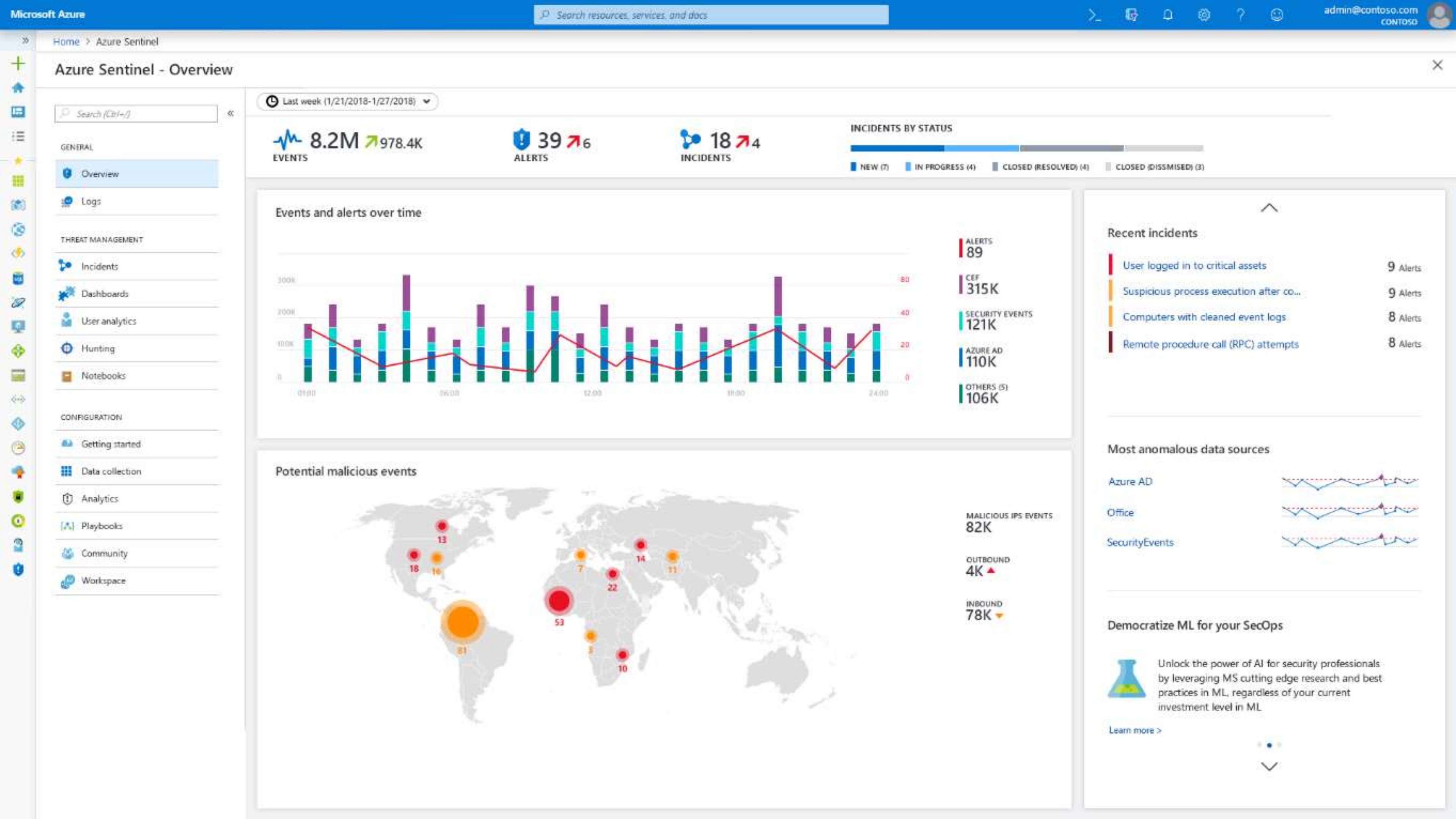
Challenges

SIEM solutions have faced four challenges traditionally:

1. You need the budget, time and appetite for it
2. Building and maintaining a (big data) infrastructure is not for the faint hearted
3. Collecting all the data from all your data sources is a daunting task
4. Making sense of all that data is also hard

Azure Sentinel

Budget:	pay-per-use
Infrastructure:	SaaS
Collection:	lots of built-in data sources
Making sense:	- dashboards
	- built-in ML (‘Fusion’)
	- GitHub KQL queries
	- GitHub Jupyter notebooks



Azure Sentinel - Overview

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

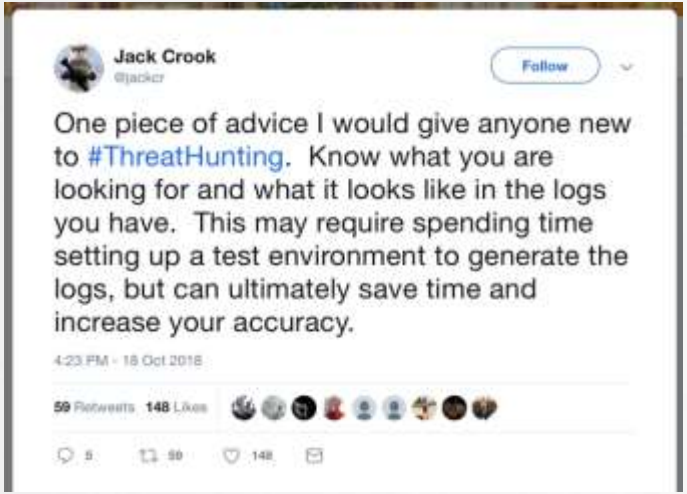
Democratize ML for your SecOps

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

Threat hunting ..

Threat Hunting

Threat Hunting



One piece of advice I would give anyone new to #ThreatHunting. Know what you are looking for and what it looks like in the logs you have. This may require spending time setting up a test environment to generate the logs, but can ultimately save time and increase your accuracy.

4:23 PM - 18 Oct 2018

59 Retweets 148 Likes

- Dr. Edmond Locard: "Every contact leaves a trace"
- Known as Locard's exchange principle

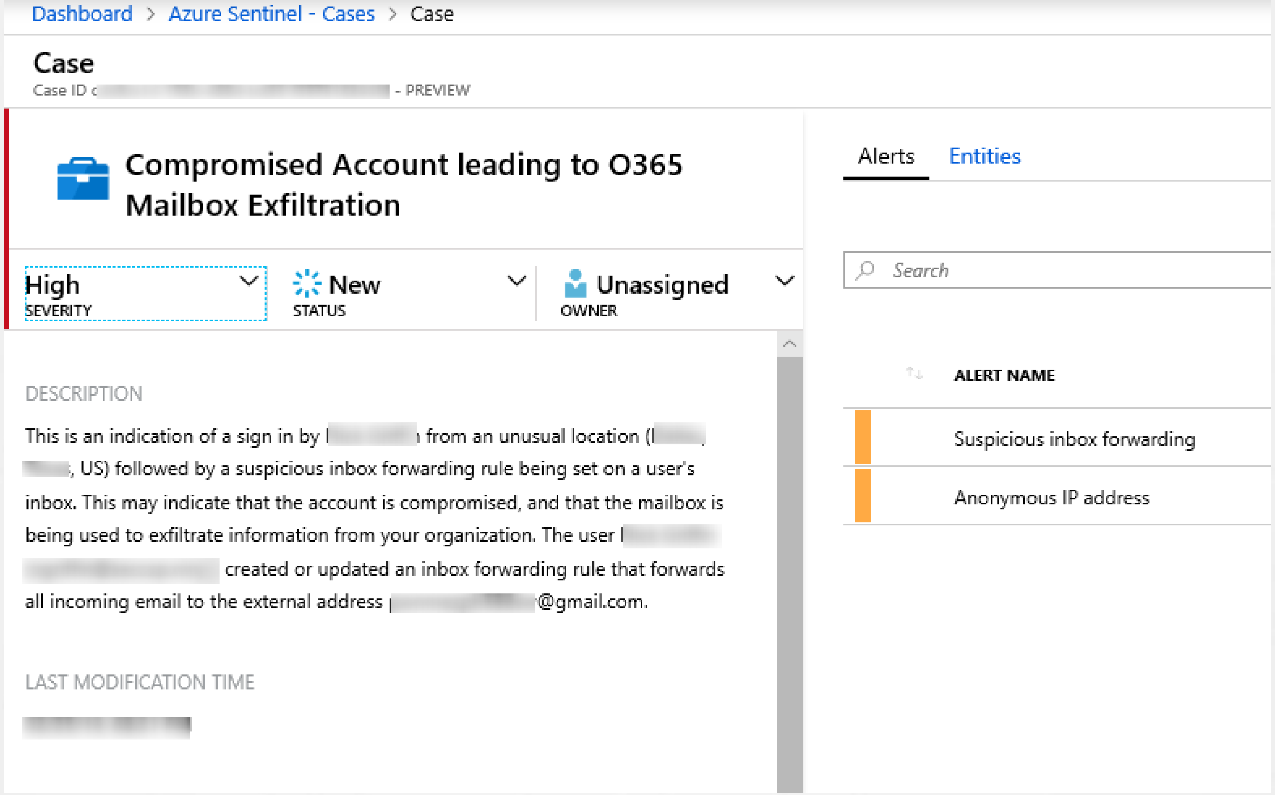
Threat Hunting

- Can be hard to do
- Programming skills
- Community is here to help
- Azure Sentinel supports:
  - KQL
  - Jupyter

Azure Sentinel

DEMO

Azure Sentinel FUSION



Dashboard > Azure Sentinel - Cases > Case

Case

Case ID [redacted] - PREVIEW

Compromised Account leading to O365 Mailbox Exfiltration

High
SEVERITY

New
STATUS

Unassigned
OWNER

DESCRIPTION

This is an indication of a sign in by [redacted] from an unusual location ([redacted], 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 [redacted] created or updated an inbox forwarding rule that forwards all incoming email to the external address [redacted]@gmail.com.

LAST MODIFICATION TIME

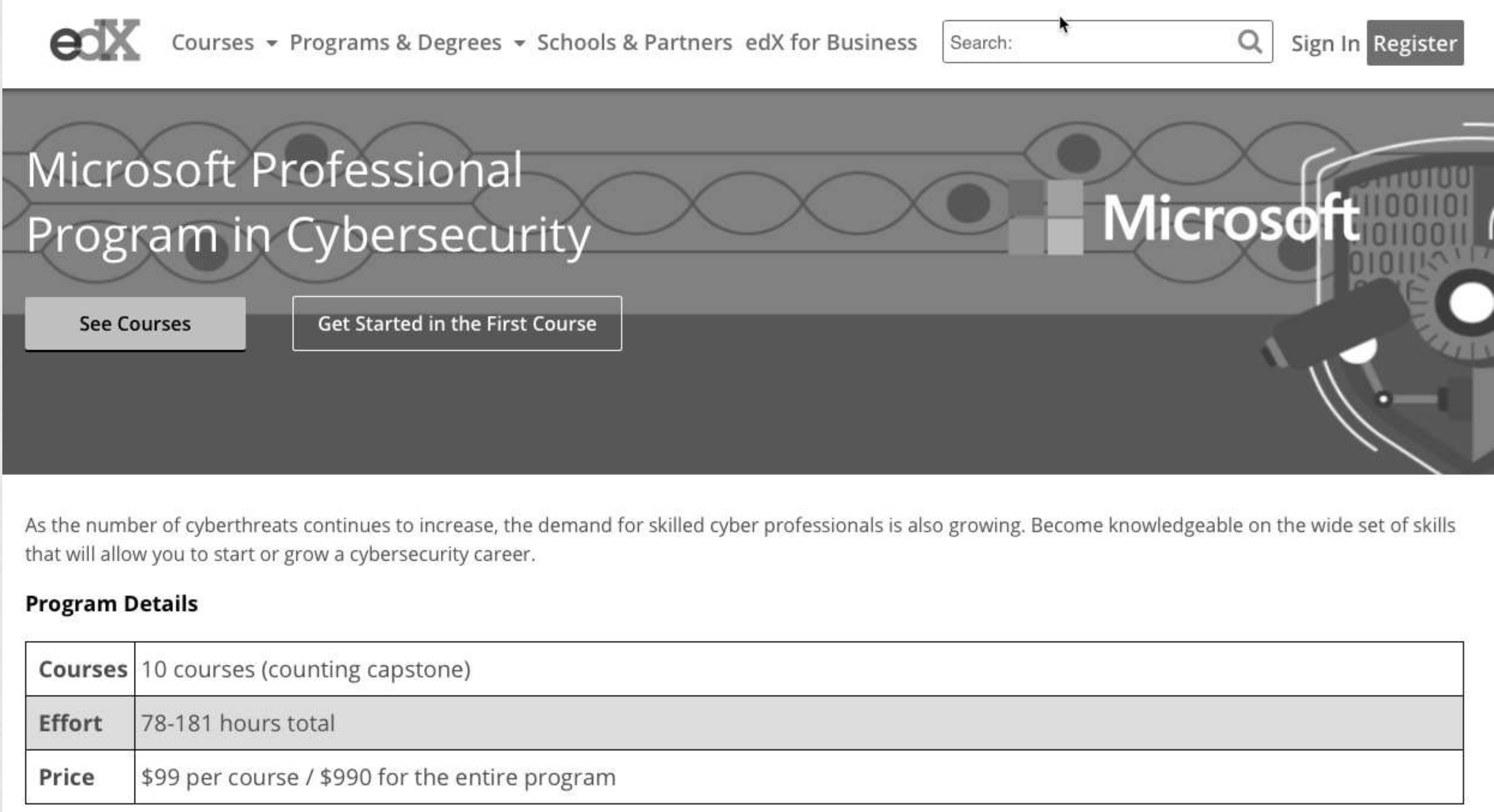
[redacted]

ALERT NAME
Suspicious inbox forwarding
Anonymous IP address

Azure Security Center

Common question: do we still need Azure Security Center? **Yes <3**

- Protection for your cloud resources
- Data source for Azure Sentinel



Microsoft Professional Program in Cybersecurity

As the number of cyberthreats continues to increase, the demand for skilled cyber professionals is also growing. Become knowledgeable on the wide set of skills that will allow you to start or grow a cybersecurity career.

Program Details

Courses	10 courses (counting capstone)
Effort	78-181 hours total
Price	$99 per course / $990 for the entire program

Summary

Microsoft *is* a security company

Microsoft 365 security is here

Cloud SIEMs are a game changer

Try Azure Sentinel today!

"Defenders think in lists.

Attackers think in graphs.

As long as this is true, attackers win."

- John Lambert, Microsoft

Experts Live

Thank you!