

# Defending Microsoft environments at scale

Vineet Bhatia (@ThreatHunting)

15 Mar 2018





# Agenda

- Introduction and Background
- Microsoft security stack in Windows 10
- Defense model based on MITRE ATTACK and the Microsoft stack
- Event data collection at scale and the role of telemetry
- Security stack in the cloud (Azure, Office365)
- Q&A



# Introduction

- Vineet Bhatia
- Focus on Threat Detection, Prevention and Response
- Pharma, Retail, Banking and Aviation industries



# Problem statement

1. Declutter the number of agents on endpoints.
2. Remove dependencies on point solutions.
3. Implement security outside traditional network boundaries.



# Microsoft security stack in Windows 10

## Windows Defender SmartScreen

- App and website reputation checks.
- Checks run when app is first run.
- Only performed on downloaded apps.
- E.g.: Detects crypto-currency miners: <http://bit.ly/2tPVeNM>

## Credential Guard

- Virtualization of security process.
- Protects secrets such as NTLM and KTG.
- Windows 10 and Server 2016 covered.

## Enterprise Cert. Pinning

- Protect internal domains from chaining.
- Pin X509 Cert and Public Key to the root.

## Memory Protections

- Control Flow Guard: <http://bit.ly/2DnSarz>
- Code Integrity Guard
- Arbitrary Code Guard: <http://bit.ly/2Gryeam>
- Windows Defender Exploit Guard: <http://bit.ly/2p7EDjS>
- Previously limited to DEP/SEHOP/ASLR.

## Device Guard

- Windows Defender Application Control. <http://bit.ly/2FK5A32>
- Previously Code Integrity Policies.
- Application whitelisting with kernel protection.
- Windows 10 and Server 2016 covered.

## Windows Defender

- Antivirus and Antimalware protection.
- Base Product + Enhanced WDATP.
- First came out in Windows 8.
- Exploit Guard launched Dec 2017 (see memory protections).
- Application Guard: <http://bit.ly/2Ir1HBW>

## Untrusted Font Blocking

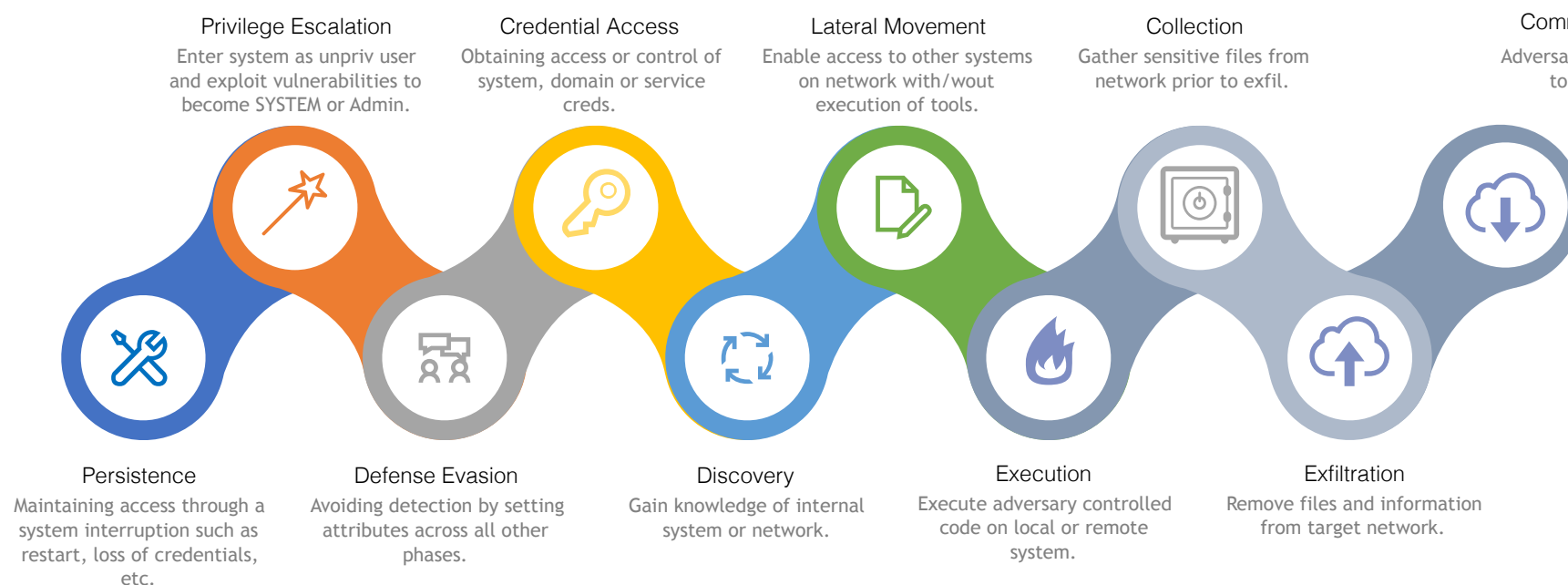
- Font Parsing Attacks (Elevation of Priv.)
- Fixed in Windows 10 Build 1703 (AppContainer)
- Merged with Kernel Pool Protections.

## Others

- UEFI Secure Boot - Firmware tampering.
- Early Launch Anti-Malware (ELAM) - Starts antimalware prior to the start of non-MSFT drivers.
- Device Health Attestation (DHA) - Posture assessment prior to connectivity.



# MITRE ATT&CK Framework



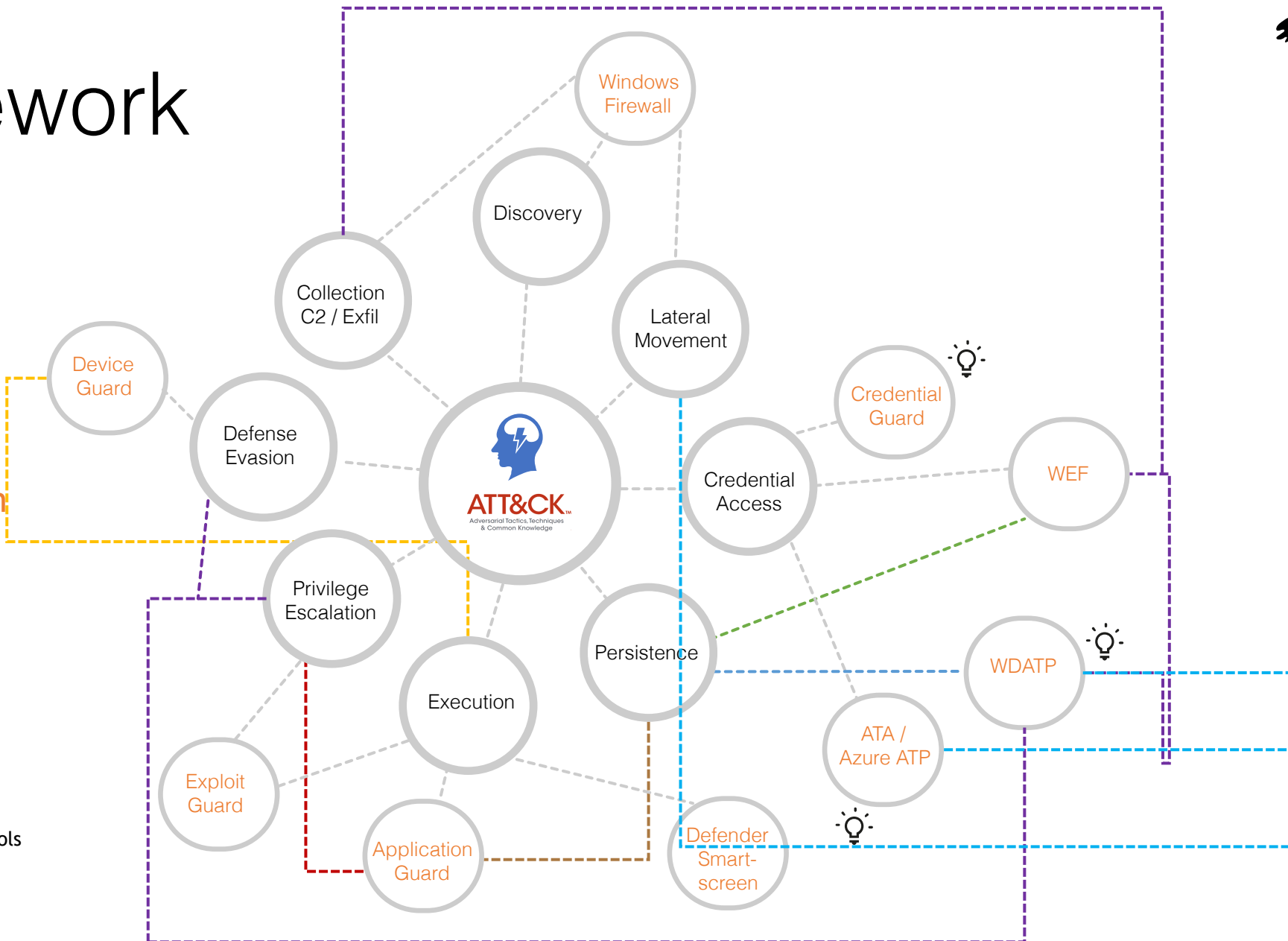
**ATT&CK™**  
Adversarial Tactics, Techniques  
& Common Knowledge



# Framework

Single Platform Approach

💡 Higher efficiency controls





# Data collection and analysis at scale

25,000 PCs

6,000 Servers

50% remote users across 300 cities

Multiple cloud environments

10 Terabytes of Log Data Everyday



*If everything seems under control, you're not going fast enough. - Mario Andretti*





# What doesn't work at scale?

“Trying is the first step towards failure.”  
- Homer Simpson (1987)



- Multiple Agents on the same host may result in duplicate or conflicting telemetry.
- Collecting logs in the cloud as you would inside your datacenter.
- Waiting for machines to “phone-in” to the corporate network after being on the road.



# A working defense model

Detection	Prevention
Windows Event Forwarding OR Sysmon OR Windows Defender ATP*	Windows Firewall
Advanced Threat Analytics OR Azure ATP	Windows Defender ATP / Exploit Guard / Application Guard
Azure Identity P1/P2	Credential Guard
SIEM of choice	Device Guard

\* Windows 10 and Server 2016 only


What will you find?	What will you stop?
Host Based Activity	Anomalous traffic in/out of the host
Network Activity To/From Hosts	Exploits from running at any priv. level
Anomalous use of credentials / priv.	All untrusted code on your PCs
Visibility into what happens on the cloud	Ability to run Mimikatz on your domain (Maybe)





# Living off the land – For Defense

 <https://twitter.com/mattifestation/status/972654625554771969>




**Matt Graeber**  
@mattifestation

Following

I completely ditched AV on one of my main laptops today. In its place, probably the most aggressive Device Guard policy I've ever configured that I will monitor aggressively. This is quite liberating. I look forward to hearing how stupid/naive I am.

6:05 AM - 11 Mar 2018

23 Retweets 205 Likes



39

23

205



Tweet your reply



# How does this come together?

- Single Inventory of assets using SCCM, baselining using DHA.
- Ability to collect basic forensic data rapidly using Sysmon.
- Uniform logging standard across the enterprise using GPMC.
- Ability to identify identity and privilege misuse using MS-ATA.
- Collect telemetry from all endpoints using Windows Defender.



# Basic environment hygiene



**NCSC UK**

@ncsc

Follow

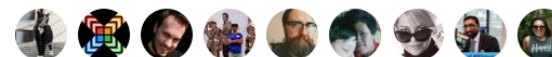


It's always fun to talk about omnipotent + omniscient hackers, and the super-sneaky espionage attacks they can do. But for most the biggest risks remain:

- not keeping software up to date
- poor network configuration management
- poor credential management

1:03 PM - 12 Mar 2018

119 Retweets 134 Likes



2



119



134



<https://twitter.com/ncsc/status/973122188344791040>



# Windows 10 Telemetry Data

- Diagnostic data sent by Windows system is configured in the GPO.
- Privacy considerations should be studied before configuration.
- See More on Telemetry Privacy at: <http://bit.ly/2DnmzpS>

WD ATP on Windows 10 (1709) and later:

- Perform investigations, optimize firewall and bitlocker configurations and investigate identities.
- Perform automated remediation (WDATP AIRS).
- Write custom Threat Hunting rules and query endpoints for matches (WDATP Advanced Hunting).



# Use Case: Monitoring

- Option 1: Windows Event Forwarding
- Option 2: Sysmon XML
- Option 3: Windows Defender ATP

**Example:** Investigating Privilege Escalation on your network  
[https://attack.mitre.org/wiki/Privilege\\_Escalation](https://attack.mitre.org/wiki/Privilege_Escalation)

Mapping MITRE ATT&CK to Windows hunting techniques:

- Roberto Rodriguez Threat Hunting Playbook:  
[https://github.com/Cyb3rWard0g/ThreatHunter-Playbook/tree/master/attack\\_matrix/windows](https://github.com/Cyb3rWard0g/ThreatHunter-Playbook/tree/master/attack_matrix/windows)



# Example: Investigating Privilege Escalation

## Option 1: Using Windows Event Forwarding

Privilege Escalation	Scenarios	Windows Event Log	Sysmon Event IDs	See Also
Accessibility Features	SETHC.exe UTILMAN.exe OSK.exe Magnify.exe Narrator.exe DisplaySwitch.exe AtBroker.exe	4656 - A handle to a Registry key or Registry Value was requested. 4657 - A registry value was modified. 4660 - An registry key or value was deleted or removed. 4663 - An attempt was made to access a Registry key or Registry Value  Look for changes to: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\{name of the executable}	Sysmon Event ID 12,13 and 14 - Registry Modification	Enable registry auditing: auditpol /set /subcategory:"Registry" /success:enable





# Example: Investigating Privilege Escalation

## Option 1: Using Windows Event Forwarding

Privilege Escalation	Scenarios	Windows Event Log	Sysmon Event IDs	See Also
AppCert DLLs	CreateProcess CreateProcessAsUser CreateProcessWithLoginW CreateProcessWithTokenW WinExec	4657 - A registry value was modified.  Look for changes or any new DLL locations being added to: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\AppCertDlls	Sysmon Event ID 12, 13 and 14 - Registry Modification	<a href="https://github.com/threathunting/sysmon-config/blob/master/sysmonconfig-export.xml#L400">https://github.com/threathunting/sysmon-config/blob/master/sysmonconfig-export.xml#L400</a>



# Example: Investigating Privilege Escalation

## Option 1: Using Windows Event Forwarding

Privilege Escalation	Scenarios	Windows Event Log	Sysmon Event IDs	See Also
Applnit DLLs	User32.dll loading unknown third party DLL	4657 - A registry value was modified.  Look for changes or any new DLL locations being added to: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows OR HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows	Sysmon Event ID 7 - DLL (image) load by process  User32.dll loading unusual DLL should trigger	The Applnit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled.  <a href="https://github.com/threathunting/sysmon-config/blob/master/sysmonconfig-export.xml#L260">https://github.com/threathunting/sysmon-config/blob/master/sysmonconfig-export.xml#L260</a>  Also consider running this on all systems and pulling data back for analysis: autorunsc -a d -h -m -s -u *



# Example: Investigating Privilege Escalation

## Option 2: Using Event Data (Sysmon Query)\$

If you pooled your data into a SIEM of your choice, you could search event data using structured queries.

Example, on Splunk, you could search the sysmon index :

\$: Requires Sysmon and config XML to be configured:

<https://github.com/threathunting/sysmon-config>



# Example: Malware Hunting

## Option 2: Using Sysmon data in Splunk

splunk> App: Sysmon App for Splunk

Sysmon OverviewNetwork ActivityProcess ActivityFile ActivityRegistry OverviewInvestigationMachine Activity

Investigator

Suspicious Indicators

Process Finder

Process Timeline

Registry Overview

Autoruns

USB Connection

File Creation Overview

File Search

Process Overview

Process Watch

ProcessMonitor - cmd.exe

ProcessMonitor - powershell.exe

ProcessMonitor - rundll32.exe

ProcessMonitor - net.exe

ProcessMonitor - sc.exe

ProcessMonitor- RarePrograms

*Credits to @jarrettp and @m\_haggis for providing the base fork of this config.*

*<https://github.com/MHaggis/sysmon-splunk-app>*



# Example: Investigating Privilege Escalation

## Option 3: Windows Defender ATP (Advanced Hunting)

Windows Defender Advanced Threat Protection (WDATP) includes a new module that allows you to query the backend schema directly. This capability is called **Advanced Hunting**. See: <http://bit.ly/2p6O8zl>

### ▼ Schema



- ⊕ - 📄 AlertEvents
- ⊕ - 📄 ProcessCreationEvents
- ⊕ - 📄 NetworkCommunicationEvents
- ⊕ - 📄 FileCreationEvents
- ⊕ - 📄 RegistryEvents
- ⊕ - 📄 LogonEvents
- ⊕ - 📄 ImageLoadEvents
- ⊕ - 📄 MiscEvents

```
//Accessibility_features_misuse_detection
RegistryEvents
| where EventTime >= ago(1h)
| where RegistryKey contains
@"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options"
| project InitiatingProcessParentName, InitiatingProcessFileName,
ActionType, RegistryKey, RegistryKeyValueName,
RegistryKeyValueData, RegistryKeyPreviousKeyValueName,
RegistryKeyPreviousKeyValueData
```



# Example: Investigating Privilege Escalation

## Option 3: Windows Defender ATP (Advanced Hunting)

```
//AppCertDLL_detection
```

```
RegistryEvents
```

```
| where EventTime >= ago(1h)
```

```
| where RegistryKey contains @"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session  
Manager\AppCertDlls"
```

```
| project InitiatingProcessParentName, InitiatingProcessFileName, ActionType, RegistryKey,  
RegistryKeyValueName, RegistryKeyValueData,  
RegistryKeyPreviousKeyValueName, RegistryKeyPreviousKeyValueData
```



# Example: Investigating Privilege Escalation

## Option 3: Windows Defender ATP (Advanced Hunting)

```
//ApplnitDLL_detection
```

```
RegistryEvents
```

```
| where EventTime >= ago(1h)
```

```
| where RegistryKey contains @"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows  
NT\CurrentVersion\Windows" or RegistryKey contains
```

```
@"HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows"
```

```
| project InitiatingProcessParentName, InitiatingProcessFileName, ActionType, RegistryKey,  
RegistryKeyValueName, RegistryKeyValueData,  
RegistryKeyPreviousKeyValueName, RegistryKeyPreviousKeyValueData
```



# Example: Investigating Privilege Escalation

## Option 3: Windows Defender ATP (Advanced Hunting)

More hunting scripts and scenarios:

Gibin John: 

<https://github.com/beahunt3r/Windows-Hunting>

Examples:

- Detecting Impacket Use in the Organization.
- Identifying BITSAdmin execution.
- ProcDump execution.





# Example: Investigating Privilege Escalation

## Option 3: Windows Defender ATP (Advanced Hunting)

More hunting scripts and scenarios:

Gibin John: 

<https://github.com/beahunt3r/Windows-Hunting>

 Indication\_ClearEventlog

 Indication\_OutPut\_Redirection

 Indication\_RemoteShareMounting

 Indication\_Tool\_IMPACKET artifact

 Indication\_Tool\_ProcDump\_possible

 Network\_Cscript\_Wscript

 Network\_PowerShell

 Process\_Bitsadmin Executions


 Process\_Bitsadmin transfer

 Process\_Certutil\_decode in appdata

 Process\_Possible\_MSOOffice\_Abuse

 Process\_Rundll32\_Control\_RunDLL

 Process\_Rundll32\_DllRegisterServer

 Process\_Rundll32\_Sus

 Process\_Rundll32\_possible hta remote

 Process\_Rundll32\_roaming

 Process\_at.exe execution

 Process\_wmic\_process call

 Process\_wscript\_js execution

 Process\_wscript\_suspicious rar:zip



# Automated Remediation

## Option 3: Windows Defender ATP (AIRS)

### Alert Triggered via WDATP telemetry data (Step 1)

⚡ Powershell dropped a suspicious file on the machine



Powershell dropped a suspicious file on the machine

Actions ▾

Severity: Medium  
Category: Delivery  
Detection source: EDR

Automated investigation pending approval ( 28 ) ⓘ

Alert context

🏠 d170930203df6ba  
👤 contoso\test

---

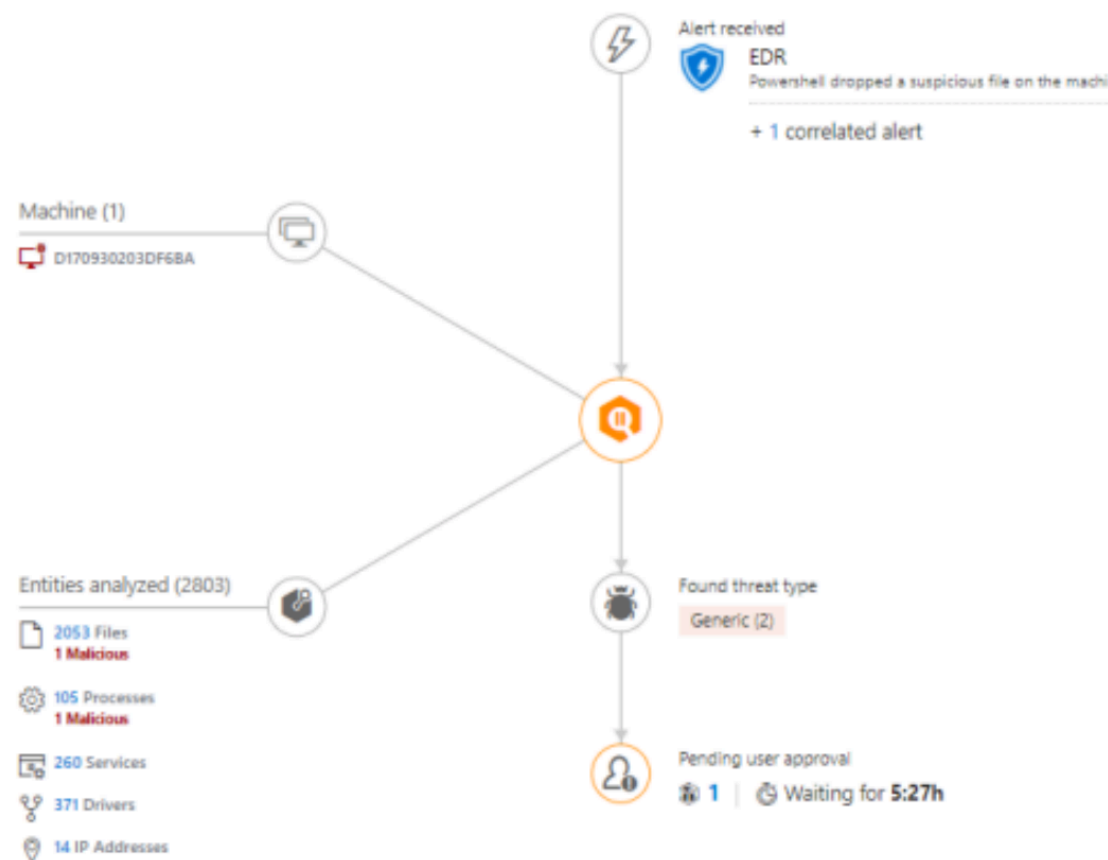
First activity: 02.12.2018 | 12:24:17  
Last activity: 02.12.2018 | 12:24:17



# Automated Remediation

## Option 3: Windows Defender ATP (AI)

Invoke automated artefact collection and triage (Step 2)



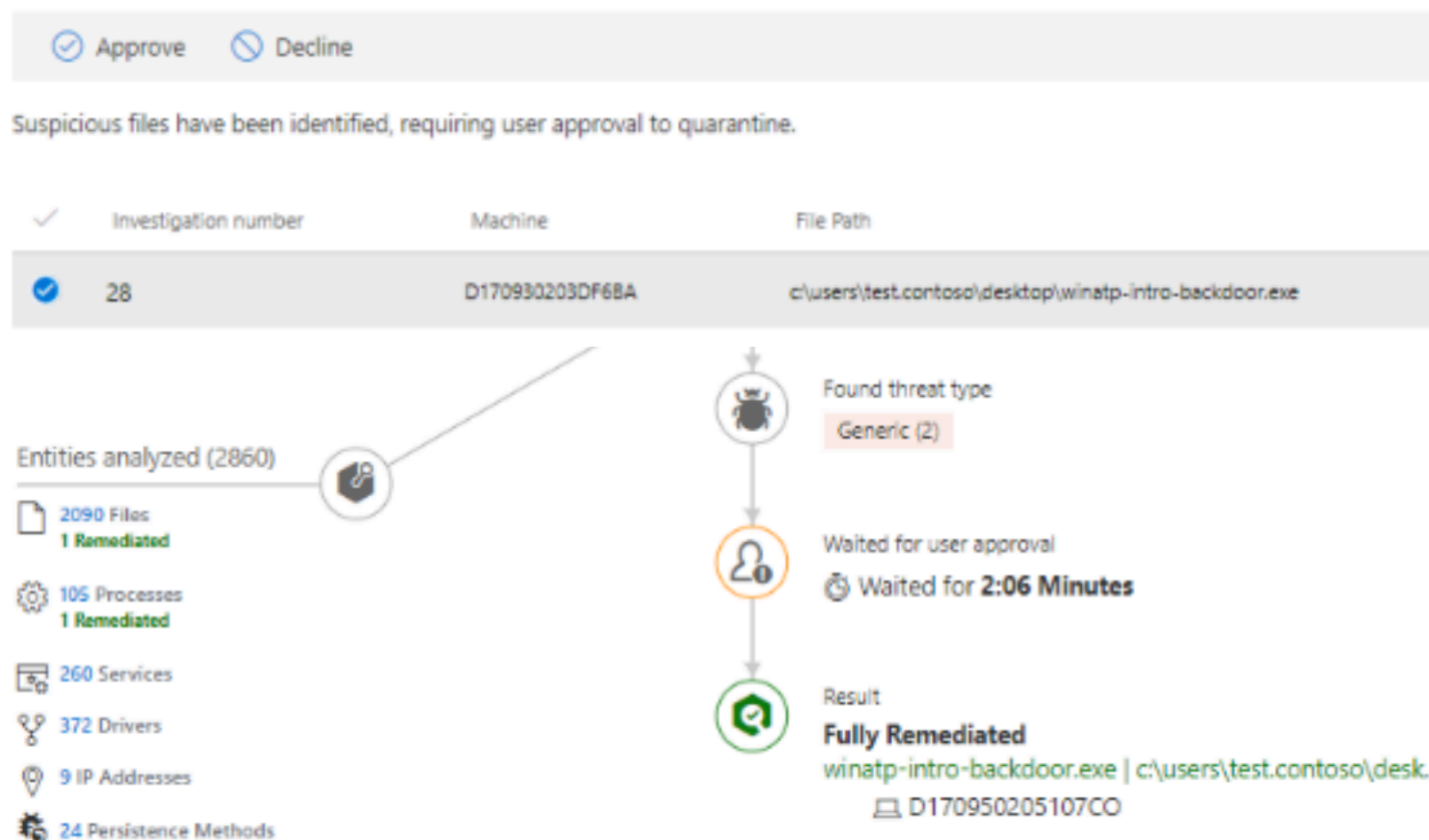


# Automated Remediation

## Option 3: Windows Defender ATP (AIRS)

Approve remediation in workflow (Step 3)

Machine fully remediated (Step 4)



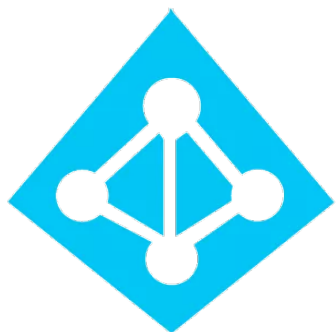


# Microsoft security stack in the cloud

- Cloud App Security: <http://bit.ly/2FACJlR>



- Azure Active Directory Identity Protection: <http://bit.ly/2p7nczH>
- Azure ATP: <http://bit.ly/2lm3sR2>



# Further Reading

What	Where
Microsoft Docs - Windows 10 Defense	<a href="http://bit.ly/2FE52Mi">http://bit.ly/2FE52Mi</a>
The evolution of MITRE ATT&CK	<a href="http://bit.ly/2tLDR0s">http://bit.ly/2tLDR0s</a>
Windows Defender ATP Tech Community	<a href="http://bit.ly/2GnwNKa">http://bit.ly/2GnwNKa</a>
Threathunting using Sysmon	<a href="http://bit.ly/2InacxP">http://bit.ly/2InacxP</a>
Azure ATP Tech Community	<a href="http://bit.ly/2Im3sR2">http://bit.ly/2Im3sR2</a>



# Questions?

## Defending Microsoft environments at scale



Vineet Bhatia (@ThreatHunting)



<https://github.com/threathunting/Published-Content>

