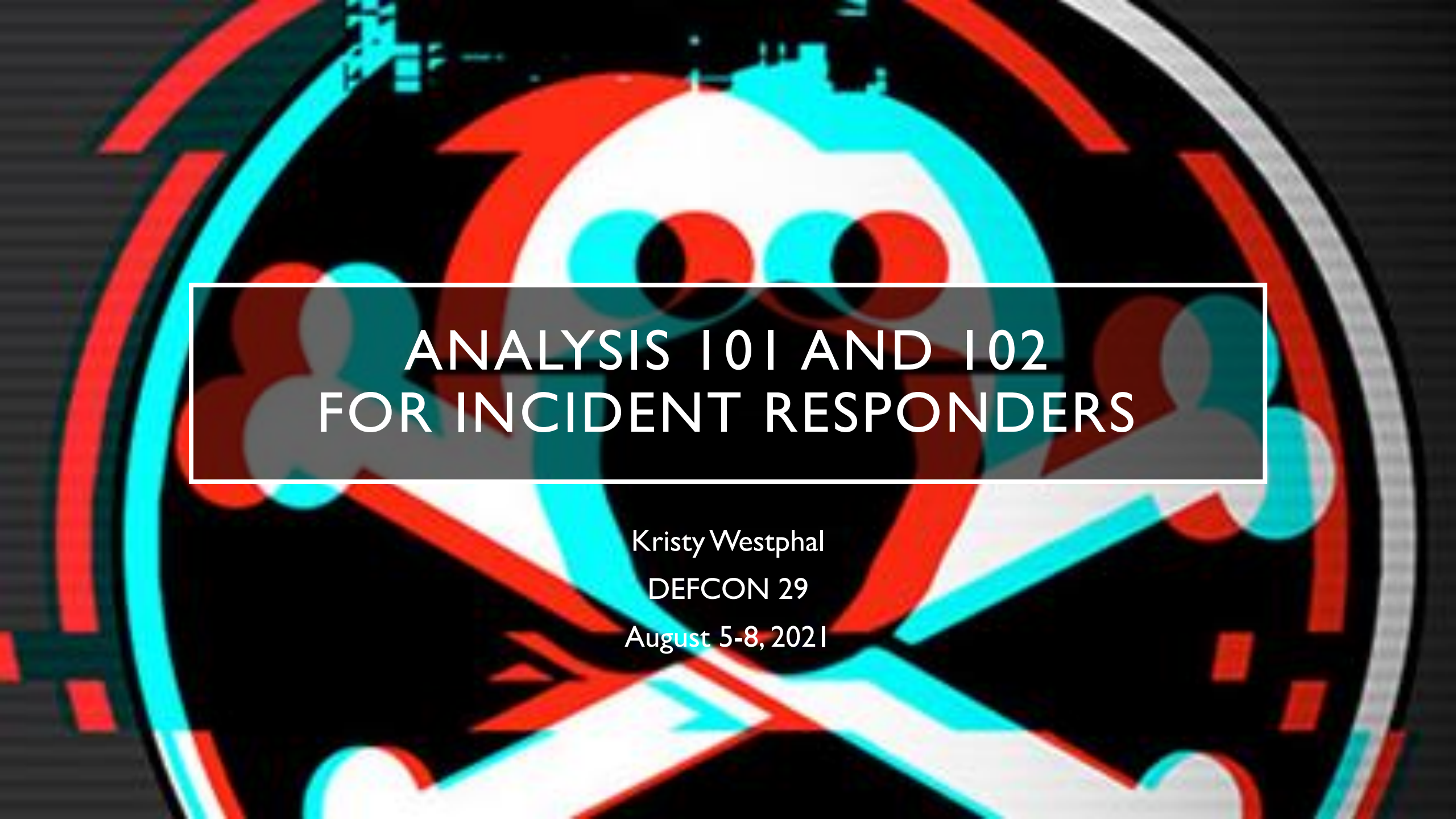


ANALYSIS 101 AND 102 FOR INCIDENT RESPONDERS

Kristy Westphal

DEFCON 29

August 5-8, 2021

A FOUR HOUR TOUR….

- Introduction
- Ignorance and importance to analysis
- On to hands on!
- Log analysis
- Network forensics
- Endpoint forensics
- A quick side journey to Cloud incident response
- Putting it all together
- Flipping the story: Threat Hunting
- Use case-a-palooza!

WHAT DID YOU JUST SAY?

- This class is about how to approach analysis techniques
- Not about how to use tools or hack stuff
- It's all about understanding what you've found

WHY AM I HERE?

- Information security leader specializing in security assessments, operational risk and program development
- Security is painful all around; hopefully I can help
- Let's share knowledge and make it less painful for all of us!

A LITTLE IGNORANCE

Why is this important?

"Ignorance is the absence of fact, understanding, insight, or clarity about something." – Firestein

It is very difficult to find a black cat in a dark room—especially when there is no cat.

“In complex systems, decision-making calls for judgments under uncertainty, ambiguity and time pressure. In those settings, options that appear to work are better than perfect options that never get computed.”

-Sidney Dekker

ANALYSIS IS LIKE SOLVING A MYSTERY…

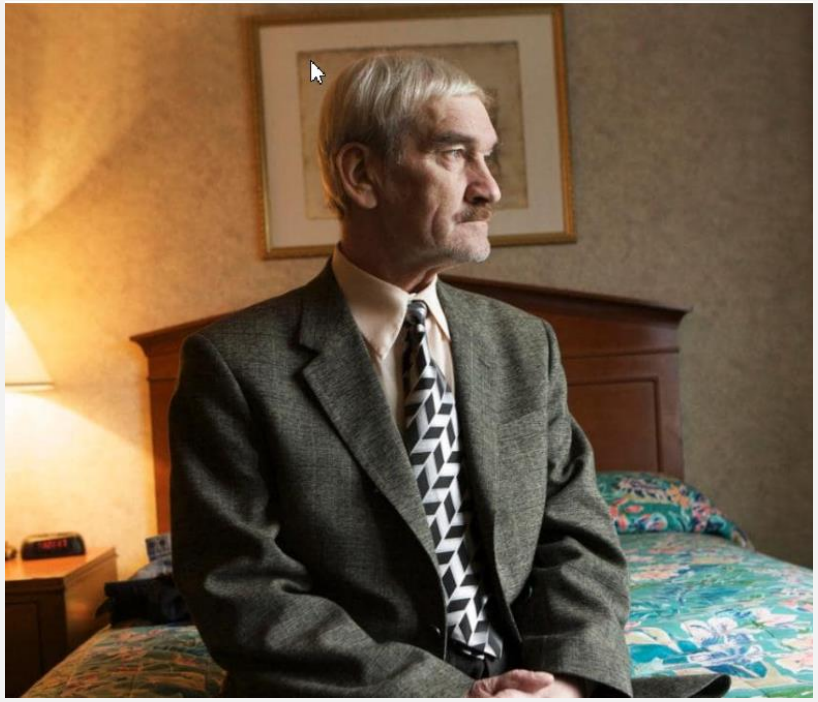
"I was trained as a physicist, and in physics we're always trying to figure out how the world works," he explained. "But you have to ask the right questions. You have to investigate things. You always have to be willing to question your assumptions. DDoS defense is very similar. You can't just look at the attacks you're getting. You have to be more proactive and try to attract more attacks and take some risks.“

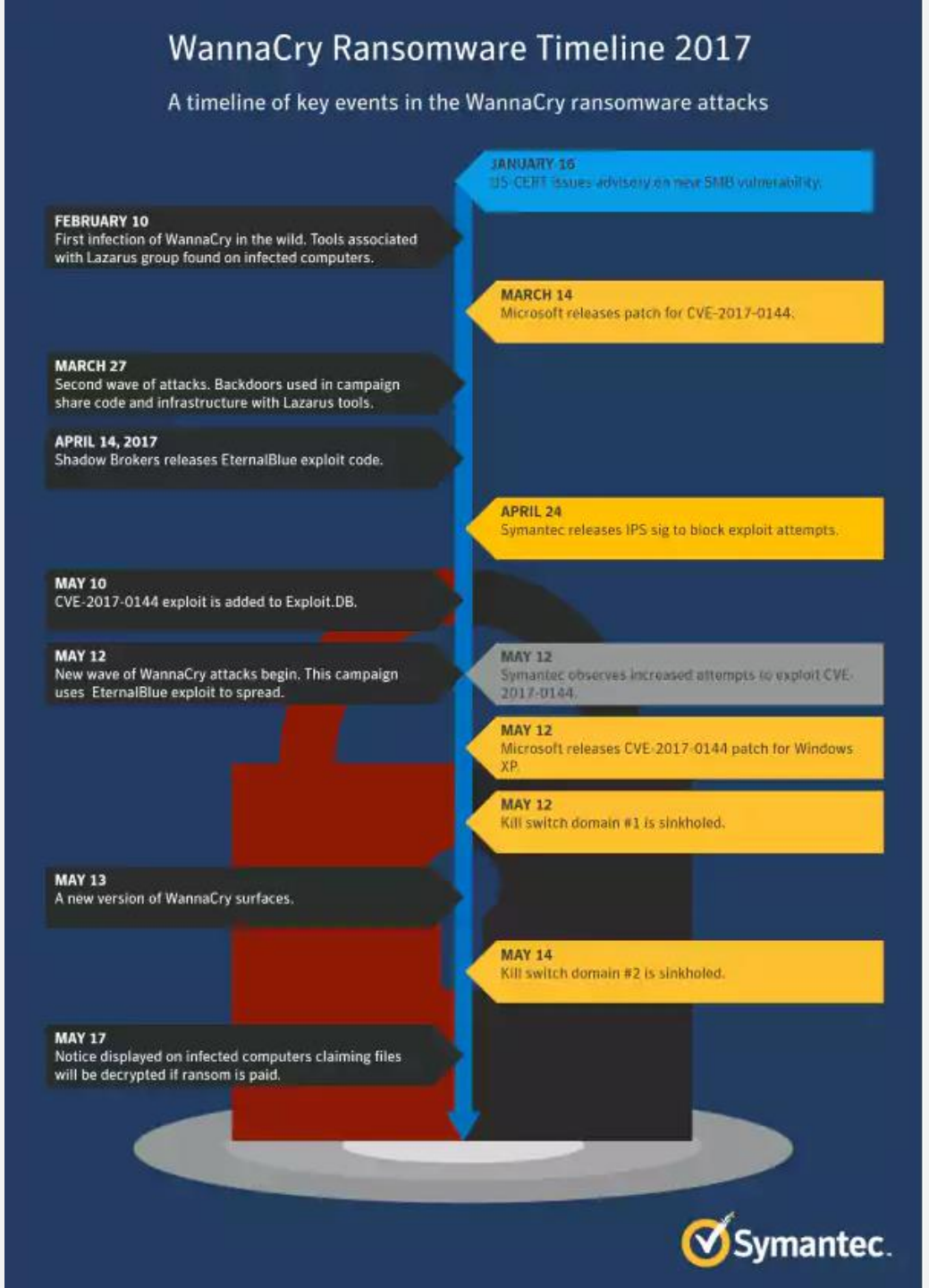
–Damian Menscher

LET'S LOOK AT SOME HISTORICAL EXAMPLES

HOW TO SAVE THE WORLD

- Stanislav Petrov literally saved the world, in the face of wildly incomplete information





But you know what the most interesting thing is?

"We might even go a step further and recognize that there are unknowable unknowns—things that we cannot know due to some inherent and implacable limitation." -Firestein

ANALYSIS PARALYSIS

(this also is Totter)

WHAT JUSTIFIES GOOD ANALYSIS?

- Context
- Accepting that you don’t know everything
- Understanding there is more than one way to analyze something
- A little humility…

TRADITIONAL ANALYSIS TECHNIQUES

- Qualitative v Quantitative
- We are generally trying to solve problems
  - Mind Maps
  - Ishiwaka diagram (cause and effect diagrams)
  - Five forces (could be twisted to security analysis)
  - TOC (Theory of Constraints)
  - CPM (Critical Path Method)
- These are great, but maybe not how to approach technical analysis
  - So we turn to data analysis (yes, Big Data too)

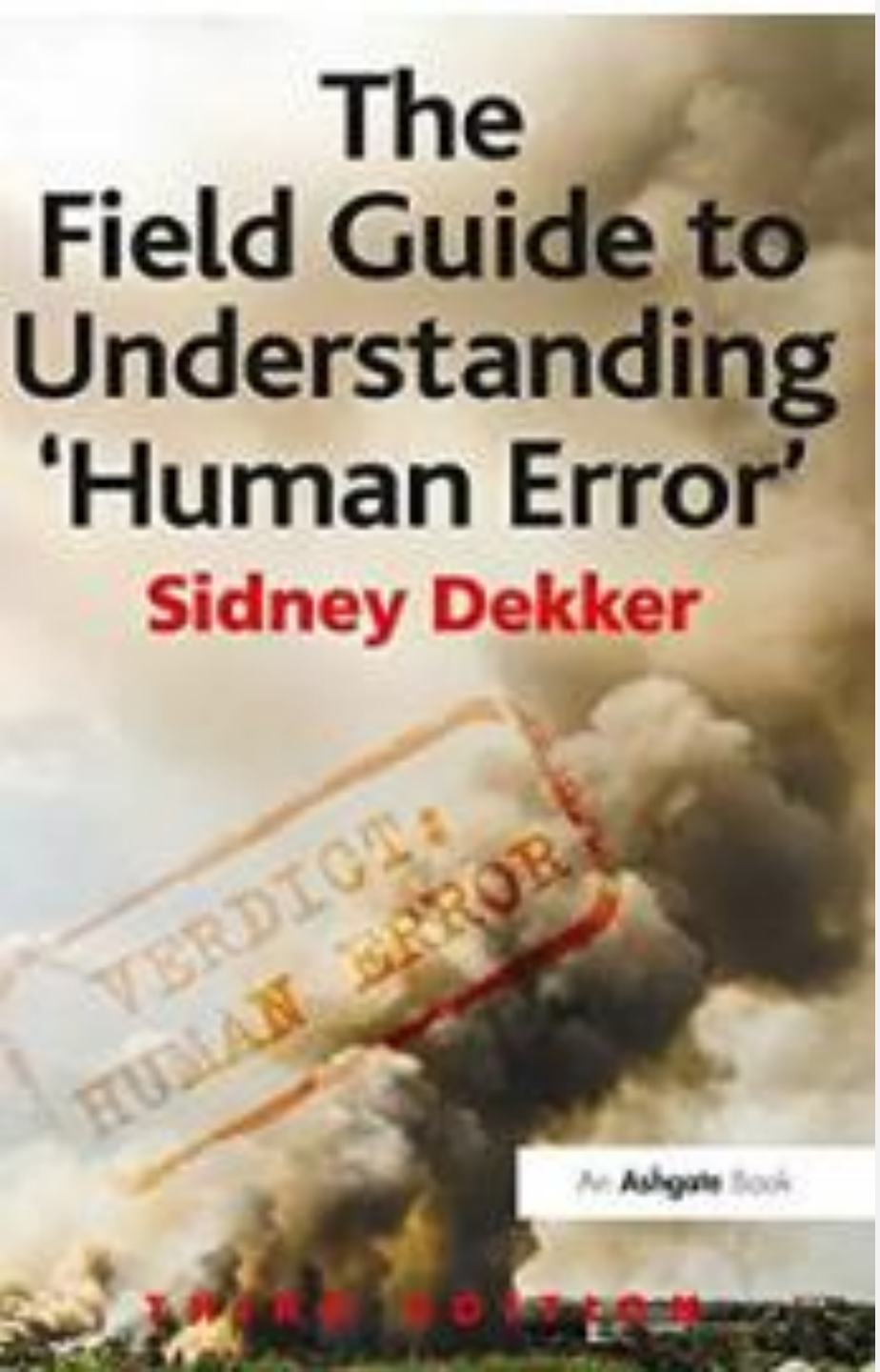
HOW DO YOU LIKE TO DO ANALYSIS?

- Spreadsheets?
- Text searches?
- Trend graphs?
- Data lakes?
- Did you say ‘reading log files?’

THINK ABOUT A TASK YOU ARE GIVEN- HOW DO YOU ANALYZE IT?

- You put together a timeline/project plan
- You work diligently to achieve it
- Yet the steps you originally map out never end up completed like you originally planned
  - Oftentimes, the end-result isn't what was originally asked for either

BUT MAYBE A LITTLE PROCESS



KEEP THIS IN MIND…

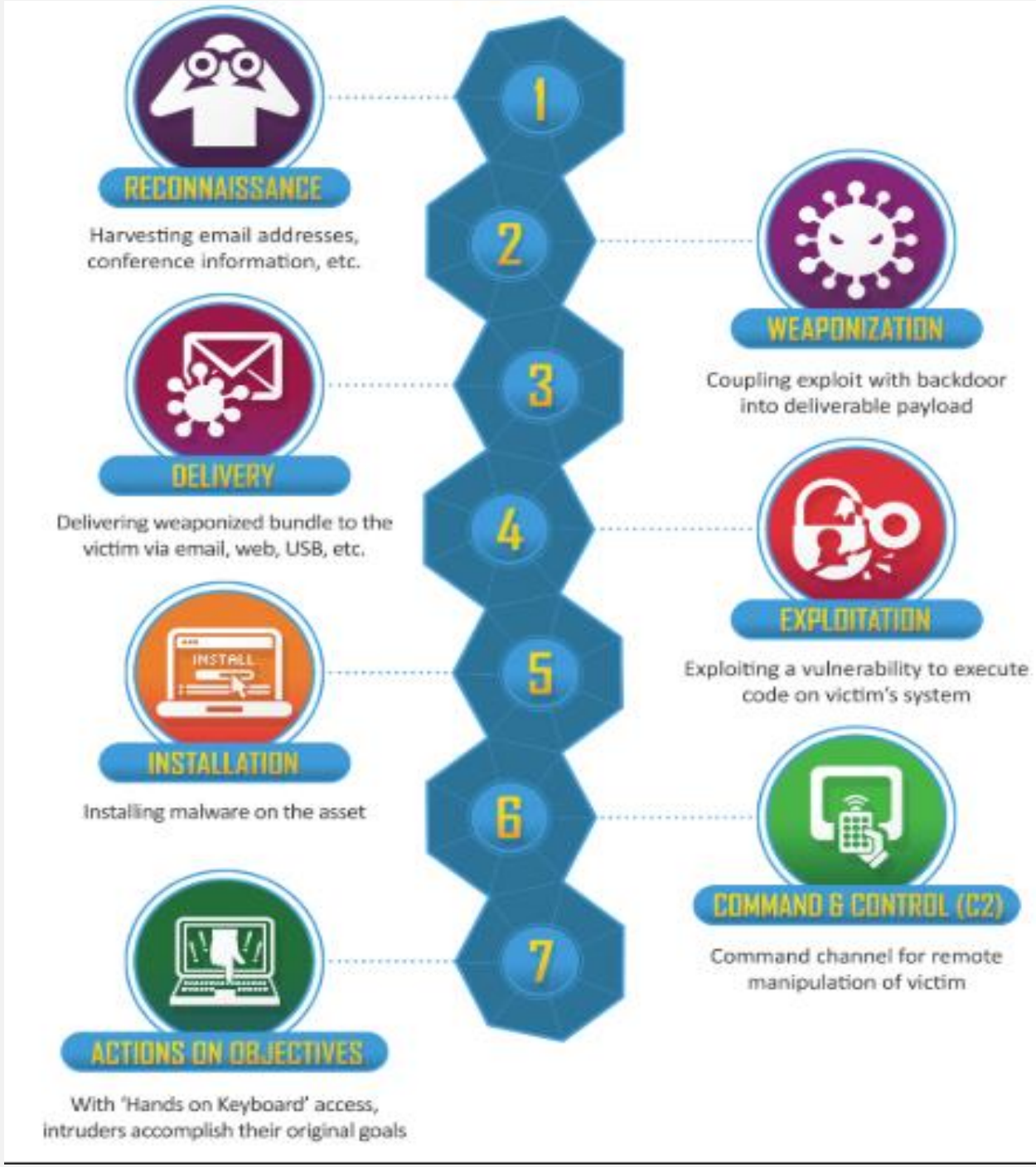
- Getting human factors data
- Building a timeline
- Putting data in context
- Leaving a trace
- Constructing causes
- Making recommendations

WAYS TO DO SECURITY OPERATIONS/SECURITY ANALYSIS

- Know the tools/controls
  - How they work
  - How they are implemented
- Know your enemy
- Follow the bread crumbs
  - Pivot through the tools
- But know how to read the logs
  - How? Open source or vendor resources

MAYBE SOME REGULAR STARTING POINTS

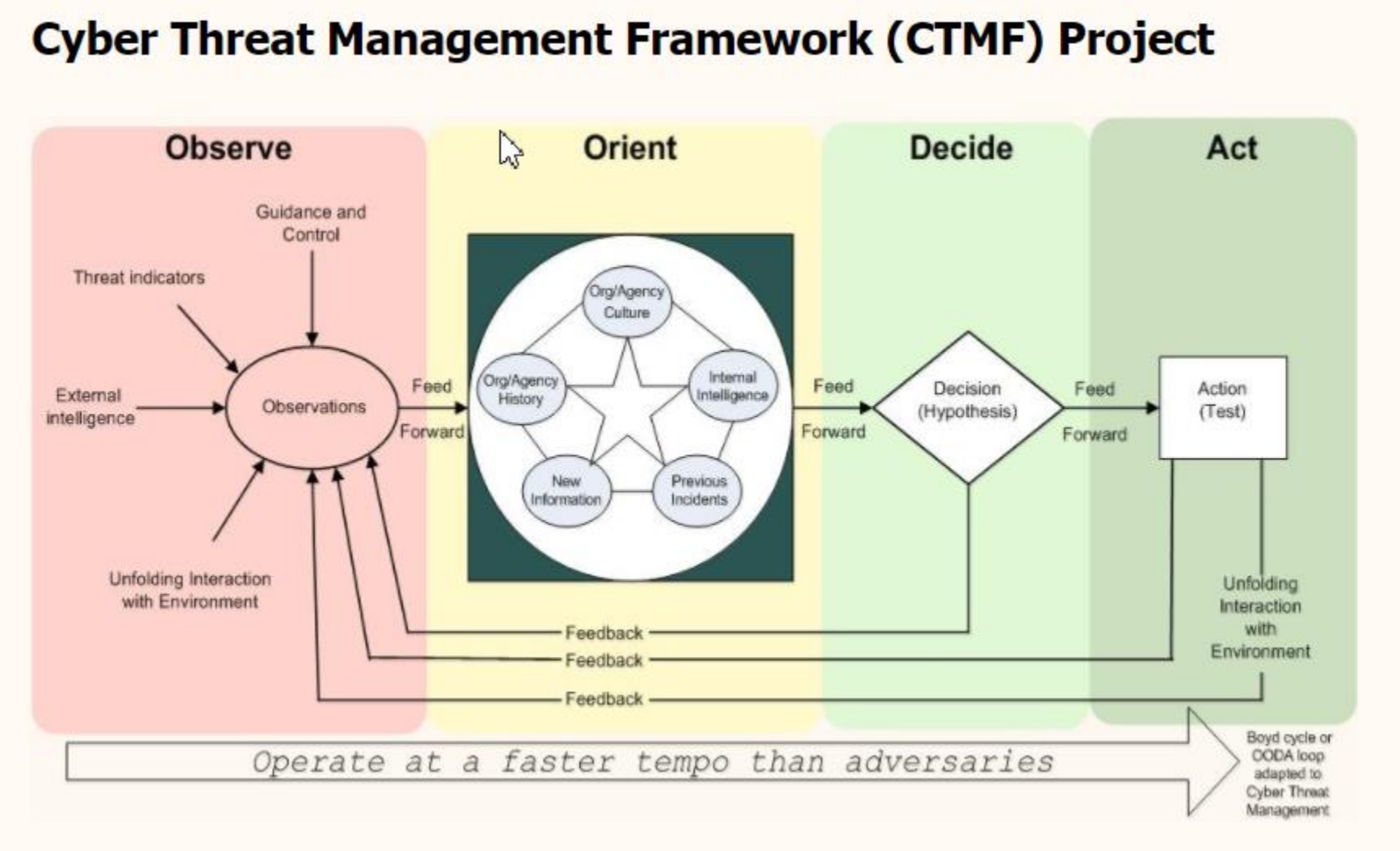
- So this thing happened (an alert, or you find something in a log)
- What steps to analyze?
  - Logs
  - OSINT
  - Threat Intel data
  - Google
  - IOCs
  - Kill Chain


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

THEN MAYBE APPLY A LITTLE DREAD (LONGER TERM)

- I just felt that eyeroll. Yes, from you.
- But think about it; we need to think a little differently
- Having a framework for your questions can be helpful
- So use as you see fit
  - For Damage: How big would the damage be if the attack succeeded?
  - For Reproducibility: How easy is it to reproduce an attack to work?
  - For Exploitability: How much time, effort, and expertise is needed to exploit the threat?
  - For Affected Users: If a threat were exploited, what percentage of users would be affected?
  - For Discoverability: How easy is it for an attacker to discover this threat?

ANOTHER WAY TO GO



SPEED ROUND OF SAMPLES

WHAT DOES THIS MEAN?


```
0C1AFAD4 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFAE4 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFAF4 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB04 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB14 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB24 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB34 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB44 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB54 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB64 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C ................
0C1AFB74 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 90 90 ..............ÉÉ
0C1AFB84 EB 19 5B 4B 90 33 C9 90 80 7B 01 E9 75 01 C3 66 δ↓[KÉ3╔ÉÇ{☺☺u☺├f
0C1AFB94 B9 7B 04 80 34 0B D8 E2 FA EB 05 E8 E2 FF FF FF ╣{♦Ç4♂╪Γ·§♣§Γ
0C1AFBA4 E9 E1 03 00 00 5F 64 A1 30 00 00 00 8B 40 0C 8B Θß♥..._di0...ï@.ï
0C1AFBB4 70 1C AD 8B 68 08 8B F7 6A 0F 59 E8 81 03 00 00 p∟↓ïh◘ï≈j☼Y§ü♥..
0C1AFBC4 90 E2 F8 68 33 32 00 00 68 55 73 65 72 54 8B 46 ÉΓ°h32..hUserTïF
0C1AFBD4 0C E8 EF 02 00 00 8B E8 6A 01 59 E8 61 03 00 00 .§∩☺..ï§j☺Y§a♥..
0C1AFBE4 E2 F9 68 6F 6E 00 00 68 75 72 6C 6D 54 8B 46 0C Γ·hon..hurlmTïF.
0C1AFBF4 E8 D0 02 00 00 8B E8 6A 01 59 E8 42 03 00 00 E2 §╨☺..ï§j☺Y§B♥..Γ
0C1AFC04 F9 68 6C 33 32 00 68 73 68 65 6C 54 8B 46 0C E8 ·hl32.hshelTïF.§
0C1AFC14 B1 02 00 00 8B E8 6A 01 59 E8 23 03 00 00 E2 F9 ▒☺..ï§j☺Y§#♥..Γ·
0C1AFC24 81 EC 00 01 00 00 8B DC 81 C3 80 00 00 00 6A 00 ü∞.☺..ï▄ü├Ç...j.
0C1AFC34 6A 1A 53 6A 00 FF 56 44 33 C0 40 80 3C 03 00 75 j→Sj. VD3└@Ç<♥.u
0C1AFC44 F9 89 86 90 00 00 00 C7 04 03 5C 61 2E 65 C7 44 ·ëåÉ...╟♦♥\a.e╟D
0C1AFC54 03 04 78 65 00 00 33 C9 51 51 53 57 51 33 C0 8B ♥♦xe..3╔QQSWQ3└ï
0C1AFC64 46 40 E8 5E 02 00 00 83 F8 00 0F 85 7F 01 00 00 F@§^☻..â°.☼à⌂0..
0C1AFC74 6A 00 6A 00 6A 03 6A 00 6A 02 68 00 00 00 C0 53 j.j.j♥j.j☻h...└S
0C1AFC84 8B 46 24 E8 3D 02 00 00 83 F8 FF 0F 84 5E 01 00 ïF$§=☻..â° ☼ä^☺.
0C1AFC94 00 89 46 60 6A 00 50 FF 56 28 89 46 64 8B 86 90 .%▒F`j.PˠV(%▒F
0C1AFCA4 00 00 00 C7 04 03 5C 62 2E 65 C7 44 03 04 78 65 ...╟♦♥\b.e╟D♥♦xe
```

OR HOW ABOUT THIS?

Syslog Examples - SSH

```
<38>Aug  1 09:13:58 groot sshd[19468]: Accepted publickey
for wraquel from 10.12.23.15 port 49474 ssh2: RSA
2b:cb:82:f0:22:d7:8a:f6:cd:70:43:b3:de:cf:5d:ee

<86>2016-08-01T09:13:48.764820-05:00 bastion sshd[2193]:
Accepted keyboard-interactive/pam for wraquel from
10.12.23.15 port 49458 ssh2

<38>Aug  1 14:05:17 dev2 sshd[31622]: Failed password for
root from 10.11.128.16 port 48593 ssh2

<38>Aug  1 09:37:20 honeypot sshd[9256]: Failed password
for invalid user pi from 192.168.58.61 port 59699 ssh2
```


CTSC

WHAT DOES THIS MEAN?

Jul 16 10:54:39 SourceFire SFIMS: [1:469:1] ICMP PING NMAP [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 210.22.215.77 -> 67.126.151.137

- *"The known is never safe; it is never quite sufficient."*

-Firestein

LET'S TALK ABOUT THE THREE CS

- *Critical Thinking*
- Communication
- Control of the Message

STOP. THINK CRITICALLY

CRITICAL SECURITY THINKING

Critical security thinking is a term for the practice of using logic and facts to form an idea about security

That idea may be an answer, a conclusion, or a characterization of something or someone so that verification tests can be well defined

As an answer or a conclusion- which one makes the most sense?

As a characterization - you'll know what you need to verify. It will also help you respect different opinions or viewpoints beyond security itself

Critical thinking help you address contradictory conclusions and explore alternate consequences

Even if the critical security thinking model can't provide an answer it should tell you what facts are still missing and from where you need to get them

CRITICAL THINKING PROCESS

Process is "Dependent on the Analyst being able to discern true statements or at least recognize the degree of possible falsity or dynamic properties in a statement." -OSSTM

"The Analyst will need to have a good understanding of what is being analyzed and of logical fallacies used to make qualifiers, statements based on fallacious concepts usually in the form of axioms or best practices." - OSSTM

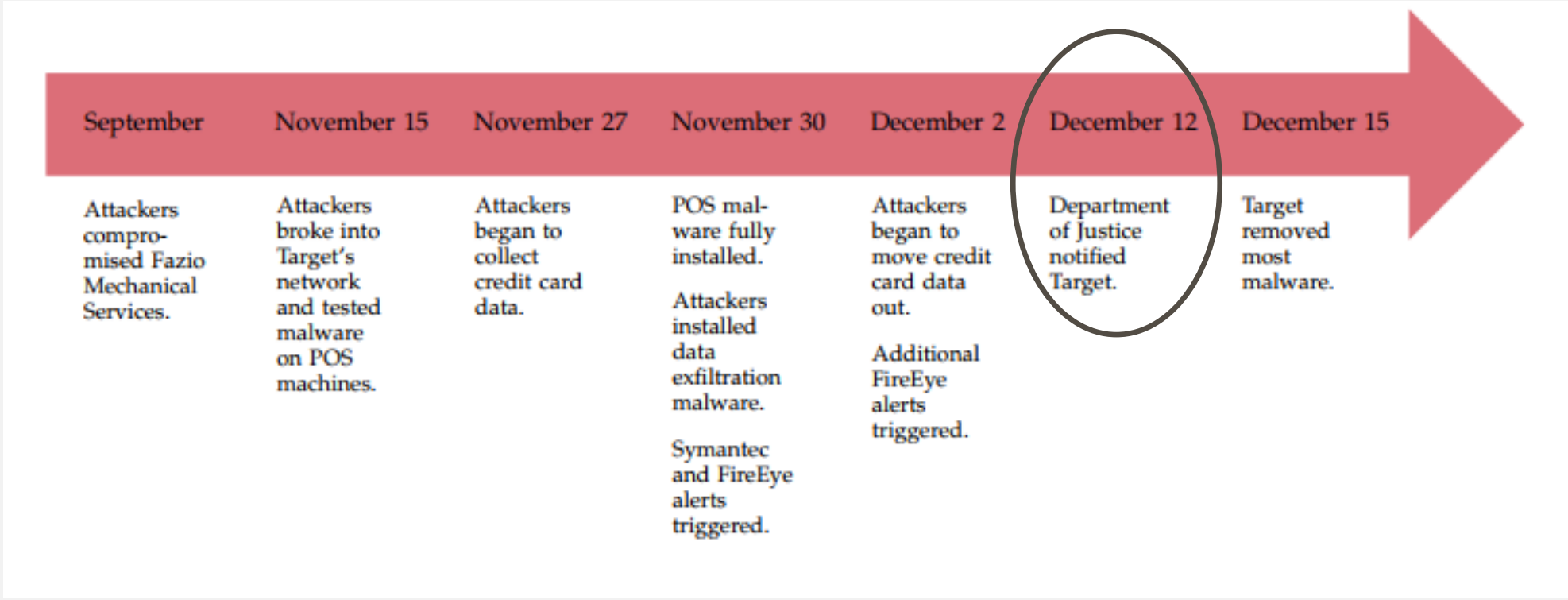
THE SIX STEP ANALYSIS TECHNIQUE

1. Build your knowledge of the target
2. Determine the global level of experience
3. Determine any bias or ulterior motives
4. Translate jargon
5. Be sure the test platform analysis has been properly calibrated
6. Assure that the you get the most direct answer

LET'S TALK ABOUT TARGET (YES, AGAIN)

"Predicting or targeting some specific advance is less useful than aiming for deeper understanding." –Firestein

Ouch!



HYPOTHESIS OR NO?

"…you may often miss data that would lead to a better answer, or a better question, because it doesn't fit your idea."– Firestein

- Virus outbreak on an IaaS platform

LET'S DISSECT A SITE FOR A SECOND…

- /m/deals/christmas-gifts/sports-and-outdoors
- /m/deals/christmas-gifts/sports-and-outdoors/camping?_be_shelf_id=4138&cat_id=4125_546956_4128
- /account/login?tid=0&returnUrl=%2Fbrowse%2Fmovies%2F4096_530598
- /account/signup?tid=0&returnUrl=%2Fbrowse%2Fmovies%2F4096_530598
- /account/trackorder
- /account/login?tid=0&returnUrl=/easyreorder
- /account/signup
- /cart?source=pac
- /checkout/#/sign-in
- /checkout/#/fulfillment

BUT HOW DO I START?

- By asking questions
- Always assume (yes, you have permission) that you don't know everything
- What are the facts?
- How are some various ways that the facts came about?
- Where did the incident start (or where do you think it started?)
- How was the incident even detected?
- What is normal behavior in the environment?
- What are some ways around the normal stuff?
- Are there related events?
- Has anyone outside the company seen your indicators? (Google to the rescue!)
- What other data do you need?
- What is the flow of the incident?

LET'S DO THIS!!

LOG ANALYSIS

- What is interesting?
- What is not interesting
- How to verify how interesting it really is

SO WHAT IS THIS??

Fri Dec 15 18:00:24 2000
Acct-Session-Id = "219397689601 7"
User-Name = "e2"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Framed-User
Framed-Protocol = PPP
Framed-IP-Address = 11.10.10.125
Calling-Station-Id = "+15678023561"
NAS-IP-Address = 11.10.10.11
NAS-Port-Id = 8
Acct-Delay-Time = 0
Timestamp = 976896024
Request-Authenticator = Unverified

Fri Dec 15 18:32:09 2000
Acct-Session-Id = "219397689601 7"
User-Name = "e2"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Acct-Output-Octets = 5382
Acct-Input-Octets = 7761
Service-Type = Framed-User
Framed-Protocol = PPP
Framed-IP-Address = 11.10.10.125
Acct-Session-Time = 1905
NAS-IP-Address = 11.10.10.11
NAS-Port-Id = 8
Acct-Delay-Time = 0
Timestamp = 976897929
Request-Authenticator = Unverified

YOUR TURN!

FOR THOSE WHO ARE BRAVE….LOOKING FOR VOLUNTEERS TO:

- Tell us what you think you found
- Tell us about your approach
- Tell us how you supported your theory

NETWORKS

NETWORK ANALYSIS

- I see this thing, now what?
- What tools do you have available?
- What might you need to understand the full picture?
  - The infamous network drawing

WHAT EXACTLY IS THIS?

- Everything that happens in between devices
  - Trying to follow an endpoint or attacker's path
- Firewalls, IDS/IPS, WAF, Packet Capture, Netflow
- Yes, more logs!
- And understanding what controls are in place and what their 'view' is

- 1.0 2017-12-13T08:16:02.130Z Z123412341234 example.com A NOERROR UDP FRA6 192.168.1.1 -
- 1.0 2017-12-13T08:15:50.235Z Z123412341234 example.com AAAA NOERROR TCP IAD12 192.168.3.1 192.168.222.0/24
- 1.0 2017-12-13T08:16:03.983Z Z123412341234 example.com ANY NOERROR UDP FRA6 2001:db8::1234 2001:db8:abcd::/48
- 1.0 2017-12-13T08:15:50.342Z Z123412341234 bad.example.com A NXDOMAIN UDP IAD12 192.168.3.1 192.168.111.0/24
- 1.0 2017-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT NOERROR UDP JFK5 192.168.1.2 -

7/11/2017 6:14:44 AM 0598 PACKET 0000007029866CF0 UDP Snd (external forwarder IP) 6973 Q [0001 D NOERROR] A (8)services(9)example(3)com(0)

7/11/2017 6:14:44 AM 0598 PACKET 00000070214 1E170 UDP Snd (Internal Machine 1) 428c R Q [8281 DR SERVFAIL] A (8)services(9)example(3)com(0)

7/11/2017 6:14:44 AM 0598 PACKET 00000070214 1E170 UDP Snd (internal Machine 2) 86f3 R Q [8281 DR SERVFAIL] A (8)services(9)example(3)com(0)

7/11/2017 6:14:44 AM 0598 PACKET 00000070214 1E170 UDP Snd (Internal Machine 3) 3250 R Q [8281 DR SERVFAIL] A (8)services(9)example(3)com(0)

Aggregated flows 850332
Top 10 flows ordered by bytes:
Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port Flags Tos Packets Bytes pps bps Bpp Flows
2005-08-30 06:50:11.218 700.352 TCP 126.52.54.27:47303 -> 42.90.25.218:435 ..... 0 1.4 M 2.0 G 2023 5.6 M 1498 1
2005-08-30 06:47:06.504 904.128 TCP 198.100.18.123:54945 -> 126.52.57.13:119 ..... 0 567732 795.1 M 627 2.5 M 1468 1
2005-08-30 06:47:06.310 904.384 TCP 126.52.57.13:45633 -> 91.127.227.206:119 ..... 0 321148 456.5 M 355 4.0 M 1490 1
2005-08-30 06:47:14.315 904.448 TCP 126.52.57.13:45598 -> 91.127.227.206:119 ..... 0 320710 455.9 M 354 4.0 M 1490 1
2005-08-30 06:47:14.316 904.448 TCP 126.52.57.13:45629 -> 91.127.227.206:119 ..... 0 317764 451.5 M 351 4.0 M 1489 1
2005-08-30 06:47:14.315 904.448 TCP 126.52.57.13:45634 -> 91.127.227.206:119 ..... 0 317611 451.2 M 351 4.0 M 1489 1
2005-08-30 06:47:06.313 904.384 TCP 126.52.57.13:45675 -> 91.127.227.206:119 ..... 0 317319 451.0 M 350 4.0 M 1490 1
2005-08-30 06:47:06.313 904.384 TCP 126.52.57.13:45619 -> 91.127.227.206:119 ..... 0 314199 446.5 M 347 3.9 M 1490 1
2005-08-30 06:47:06.321 790.976 TCP 126.52.54.35:59898 -> 132.94.115.59:2466 ..... 0 254717 362.4 M 322 3.7 M 1491 1
2005-08-30 06:47:14.316 904.384 TCP 126.52.54.35:59773 -> 55.107.224.187:11709 ..... 0 272710 348.5 M 301 3.1 M 1340 1

107023683l,0,3175466240,198.32.11.5,1,1500,3175436989,3175436989,0,0,130.74.208.0,169.232.72.0,198.32.11.4,33,35,1373,4753,6,0,16,16,16,25656,52
107023683l,0,3175466240,198.32.11.5,3,1884,3175408565,3175433201,0,0,130.74.208.0,169.232.72.0,198.32.11.4,33,35,1373,4753,6,0,24,16,16,25656,52
107023683l,0,3175466240,198.32.11.5,1,628,3175448463,3175448463,0,0,130.74.208.0,169.232.112.0,198.32.11.4,33,35,1373,3855,6,0,24,16,16,25656,52
107023683l,0,3175466240,198.32.11.5,1,1500,3175442525,3175442525,0,0,130.74.208.0,169.232.112.0,198.32.11.4,33,35,1373,3864,6,0,16,16,16,25656,52
107023683l,0,3175466240,198.32.11.5,1,1500,3175451974,3175451974,0,0,130.74.208.0,169.232.112.0,198.32.11.4,33,35,1373,3831,6,0,16,16,16,25656,52
107023683l,0,3175466240,198.32.11.5,6,3768,3175398562,3175449061,0,0,130.74.208.0,169.232.112.0,198.32.11.4,33,35,1373,3831,6,0,24,16,16,25656,52
1070236836,0,3175471250,198.32.11.5,1,92,3175454577,3175454577,0,0,130.18.248.0,202.28.48.0,198.32.11.4,18,35,0,0,1,0,0,16,24,10546,4621
1070236836,0,3175471250,198.32.11.5,1,92,3175414202,3175414202,0,0,130.18.248.0,165.132.224.0,198.32.11.4,18,35,0,0,1,0,0,16,16,10546,4665
1070236836,0,3175471250,198.32.11.5,1,92,3175433202,3175433202,0,0,130.18.248.0,210.103.24.0,198.32.11.4,18,35,0,0,1,0,0,16,17,10546,9768
1070236836,0,3175471250,198.32.11.5,1,92,3175403033,3175403033,0,0,130.18.248.0,211.248.144.0,198.32.11.4,18,35,0,0,1,0,0,16,17,10546,9768

Sep 7 06:25:17 PIXName %PIX-7-710005: UDP request discarded from 0.0.0.0/68 to outside:255.255.255.255/67
Sep 7 06:25:23 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:23 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:23 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:24 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:24 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:24 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:25 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:25 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:25 PIXName %PIX-7-710005: UDP request discarded from 1.1.1.1/137 to outside:1.1.1.255/137
Sep 7 06:25:28 PIXName %PIX-7-609001: Built local-host db:10.0.0.1
Sep 7 06:25:28 PIXName %PIX-6-302013: Built inbound TCP connection 141968 for db:10.0.0.1/60749 (10.0.0.1/60749) to NP Identity Ifc: 10.0.0.2/22 (10.0.0.2/22)
Sep 7 06:25:28 PIXName %PIX-7-710002: TCP access permitted from 10.0.0.1/60749 to db:10.0.0.2/ssh
Sep 7 06:26:20 PIXName %PIX-5-304001: 203.87.123.139 Accessed URL 10.0.0.10:/Home/index.cfm
Sep 7 06:26:20 PIXName %PIX-5-304001: 203.87.123.139 Accessed URL 10.0.0.10:/aboutus/volunteers.cfm
Sep 7 06:26:49 PIXName %PIX-4-106023: Deny udp src outside:204.16.208.49/58939 dst dmz:10.0.0.158/1026 by access-group "acl_outside" [0x0, 0x0]
Sep 7 06:26:49 PIXName %PIX-4-106023: Deny udp src outside: 204.16.208.49/58940 dst dmz:10.0.0.158/1027 by access-group "acl_outside" [0x0, 0x0]
Sep 7 06:31:26 PIXName %PIX-7-711002: Task ran for 330 msec, Process= ssh_init, PC = fddd93, Traceback = 0x00FF1E6B 0x00FE1890 0x00FE0D3C 0x00FD326A 0x00FC0BFC 0x00FDBB8E 0x00FDBA4D 0x00FCD846 0x00FBF09C 0x001C76AE 0x00A01512 0x009CF6B5 0x00BDB9CE 0x00BDA502
Sep 7 06:31:32 PIXName %PIX-6-315011: SSH session from 10.0.0.254 on interface db for user "" disconnected by SSH server, reason: "TCP connection closed" (0x03)

YOUR TURN!

ENDPOINTS

ENDPOINT FORENSICS

- I don't have time for full forensics, what can I do in a brief time period?
- What does the information gathered mean?
- Set your scope first
- What behavior are you seeing?
  - Indicators?
- If you have a little time:
  - Sysmon
  - CrowdResponse
  - Redline
- If not grab these:
  - Rift

Supported Operating Systems

CrowdResponse supports 32-bit and 64-bit versions of:

- Workstation:
  - Windows XP
  - Windows Vista
  - Windows 7
  - Windows 8
  - Windows 8.1
  - Windows 10
- Server:
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012

found in the *CrowdResponse User Guide.pdf* file included

the contents of the downloaded ZIP file into a location of
re. Similarly for uninstalling; simply delete the file(s) you
or permanently deleting them. It is possible there may be
in the Registry. There can be safely ignored or manually
egedit) and navigating to
`dStrike` or
`trike` and noting the name of the tool there and

File | C:/Users/kamee/Documents/DEFCON29/CrowdResponse/CrowdResponse_drivers.html

Apps Gmail YouTube Maps Imported Other bookmarks Reading list

Produced by the free CrowdStrike tool *CrowdResponse*

Module: drivers

system	driver_file	driver_base	path	name
output	\SystemRoot\system32\ntoskrnl.exe	0xFFFFF8074B000000	C:\Windows\system32\	ntoskrnl.exe
output	\SystemRoot\system32\hal.dll	0xFFFFF80749DC0000	C:\Windows\system32\	hal.dll
output	\SystemRoot\system32\kd.dll	0xFFFFF80749DD0000	C:\Windows\system32\	kd.dll
output	\SystemRoot\system32\mcupdate_GenuineIntel.dll	0xFFFFF80749A20000	C:\Windows\system32\	mcupdate_GenuineInte
output	\SystemRoot\System32\drivers\CLFS.SYS	0xFFFFF8074F400000	C:\Windows\System32\drivers\	CLFS.SYS
output	\SystemRoot\System32\drivers\tm.sys	0xFFFFF80749DE0000	C:\Windows\System32\drivers\	tm.sys
output	\SystemRoot\system32\PSHED.dll	0xFFFFF8074F470000	C:\Windows\system32\	PSHED.dll
output	\SystemRoot\system32\BOOTVID.dll	0xFFFFF80749E10000	C:\Windows\system32\	BOOTVID.dll
output	\SystemRoot\System32\drivers\FLTMGR.SYS	0xFFFFF8074F5B0000	C:\Windows\System32\drivers\	FLTMGR.SYS
output	\SystemRoot\System32\drivers\msrpc.sys	0xFFFFF8074F650000	C:\Windows\System32\drivers\	msrpc.sys
output	\SystemRoot\System32\drivers\ksecdd.sys	0xFFFFF8074F620000	C:\Windows\System32\drivers\	ksecdd.sys
output	\SystemRoot\System32\drivers\clipsp.sys	0xFFFFF8074F490000	C:\Windows\System32\drivers\	clipsp.sys
output	\SystemRoot\System32\drivers\cmimcext.sys	0xFFFFF8074F6C0000	C:\Windows\System32\drivers\	cmimcext.sys
output	\SystemRoot\System32\drivers\werkernel.sys	0xFFFFF8074F6D0000	C:\Windows\System32\drivers\	werkernel.sys

WHAT ELSE?

- Directory listing
- Sticky Keys
- Prefetch
- Pslist
- Registry Dump
- Shim
- System Info

- Can be deployed via SCCM or PSExec or whatevs

This is frac/rift for Windows info gathering

```
#Get the system hive
system32\/config\/SYSTEM$
#Get the default hive
system32\/config\/DEFAULT$
#Get the sam hive
system32\/config\/SAM$
#Get the security hive
system32\/config\/SECURITY$
#Get the software hive
system32\/config\/SOFTWARE$
#Get the contents of the Tasks directory for Windows 2000, XP, @003
\/Windows\/Tasks\/
#Get the Contents of the Tasks directory for Windows 7+
\/Windows\/System32\/Tasks\/
#Get a copy of the task scheduler logs
Microsoft-Windows-TaskScheduler*\.evtx$
#Gathers all users ntuser.dat files
ntuser.dat$
#Win7 shellbag data
#\Users\[user]\AppData\Local\Microsoft\Windows\UsrClass.dat
usrclass.dat$
#Win8 Application Experience and Compatibility  C:\Windows\AppCompat\Programs\Amcache.hve
amcache.hve$
#journeyintoir.blogspot.com/2014/04/triaging-with-recentfilecachebcf-file.html
RecentFilecache.bcf$
#Get the contents of the Prefetch directory
\/Windows\/prefetch\/
```

Second half…..

```
#Event Logs for Vista+
system32\/winevt\/logs\/
#Event Logs for WinXP
\/appevent.evt$
\/sysevent.evt$
\/secevent.evt$
#WinXP Recycle Bin
\/info2$
#Vista+ Reycle Bin; Gets Index files
\/\$Recycle.bin\/S-.*\/\$I.*
#Gets everything in the Recycle.bin folder
#\/\$Recycle.bin\/
#Page file
#\/pagefile.sys$
#Hibernation file
#\/hiberfil.sys$
#Microsoft Malicious Software Removal (MSRT)
\/Windows\/Debug\/mrt.log$
\/Windows\/Debug\/mrteng.log$
#Windows Defender Logs
\/ProgramData\/Microsoft\/Windows Defender\/Support\/.*log$
#Powershell Info
\/Windows\/System32\/wbem\/Repository\/OBJECTS.DATA$
\/Windows\/System32\/wbem\/Repository\/FS\/OBJECTS.DATA$
#Syscache.hve  https://github.com/libyal/winreg-kb/blob/master/documentation/SysCache.asciidoc
\/System Volume Information\/Syscache.hve
```

This is frac/rift for *nix info gathering

```
#Shell Info
\.bash_history
\.bashrc
\/\.csh
\/\.zsh
\/\.sh_history
\/\.profile
#SSH
\.ssh
#etc dir
^\/etc\/
#Cron
^\/var\/spool\/at
^\/var\/spool\/cron
^\/var\/spool\/anacron
#logs
^\/var\/log\/
^\/var\/adm\/
```

Sample Windows event log

- System
  - Provider
  [Name] Microsoft-Windows-Sysmon
  [Guid] {5770385F-C22A-43E0-BF4C-06F5698FFBD9}

  EventID 1
  Version 5
  Level 4
  Task 1

  Opcode 0

  Keywords 0x8000000000000000

  - TimeCreated

  [SystemTime] 2019-06-21T17:49:33.036975300Z

  EventRecordID 2380270

  Correlation

  - Execution
  [ProcessID] 4212
  [ThreadID] 7464
  Channel Microsoft-Windows-Sysmon/Operational
  Computer DESKTOP-QPHCRMF
  - Security
  [UserID] S-1-5-18

Second part of the event log

- EventData

RuleName
UtcTime 2019-06-21 17:49:33.034
ProcessGuid {404F8C83-18AD-5D0D-0000-0010951EC630}
ProcessId 30664
Image C:\Program Files\Splunk\bin\splunk-optimize.exe
FileVersion 7.3.0
Description splunk-optimize
Product splunk Application
Company Splunk Inc.
CommandLine splunk-optimize -d "C:\Program Files\Splunk\var\lib\splunk_internaldb\db\hot_v1_4" -x 40290210304 --log-to--splunkd-log --write-level 1
CurrentDirectory C:\WINDOWS\system32\
User NT AUTHORITY\SYSTEM
LogonGuid {404F8C83-5448-5D05-0000-0020E7030000}
LogonId 0x3e7
TerminalSessionId 0
IntegrityLevel System
Hashes SHA1=9EACAE222E8B87066B98061A57E3E9986D8C7317
ParentProcessGuid {404F8C83-5459-5D05-0000-0010FD270400}
ParentProcessId 4596
ParentImage C:\Program Files\Splunk\bin\splunkd.exe
ParentCommandLine "C:\Program Files\Splunk\bin\splunkd.exe" service

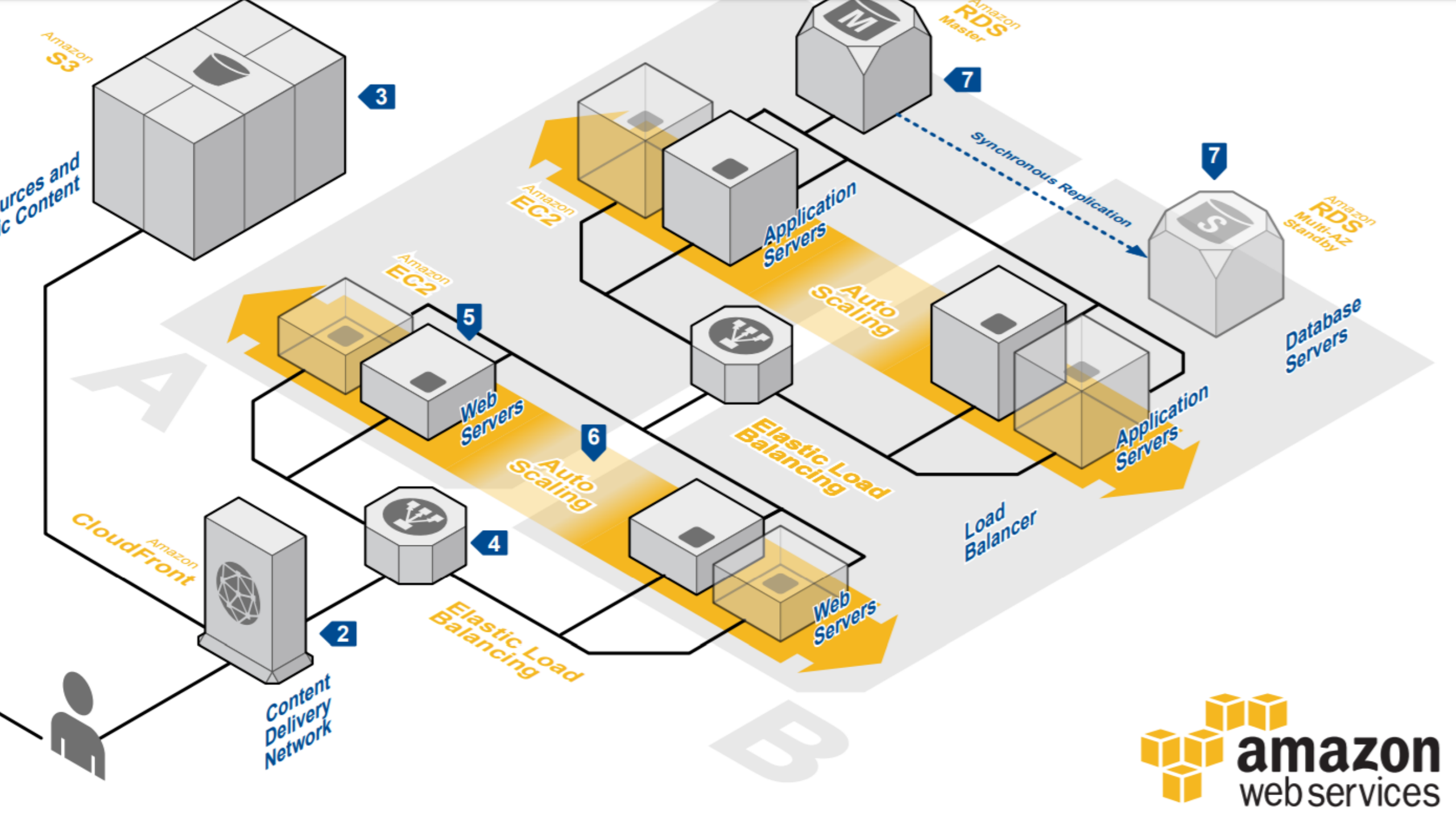
GUESS WHAT?

Yep, it's your turn

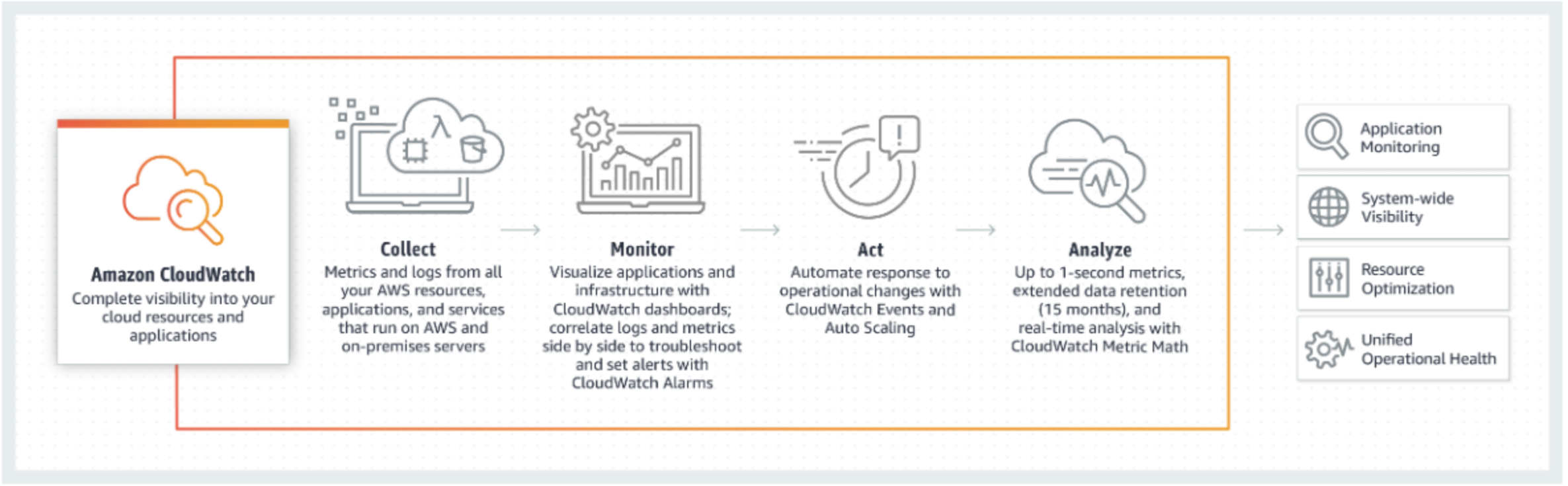
TO THE CLOUDS!

CLOUD ANALYSIS

- How is cloud response/analysis different?
- How might it not be different?
- Couple of AWS examples
- And one Azure (just for fun)


Amazon S3
urces and
ic Content
3
Amazon RDS
Master
7
Synchronous Replication
7
Amazon RDS
Multi-AZ
Standby
Amazon EC2
Application Servers
Auto Scaling
Database Servers
Amazon EC2
5
Web Servers
6
Auto Scaling
Elastic Load Balancing
Application Servers
Load Balancer
Amazon CloudFront
4
Elastic Load Balancing
Web Servers
2
Content Delivery Network
A
B
amazon
web services

How it works


Amazon CloudWatch
Complete visibility into your cloud resources and applications
Collect
Metrics and logs from all your AWS resources, applications, and services that run on AWS and on-premises servers
Monitor
Visualize applications and infrastructure with CloudWatch dashboards; correlate logs and metrics side by side to troubleshoot and set alerts with CloudWatch Alarms
Act
Automate response to operational changes with CloudWatch Events and Auto Scaling
Analyze
Up to 1-second metrics, extended data retention (15 months), and real-time analysis with CloudWatch Metric Math
Application Monitoring
System-wide Visibility
Resource Optimization
Unified Operational Health

COMPONENTS OF INTEREST

- Shared Responsibility Model- tells you what you can access and what you can't
- IAM
- Host
- Data
- Applications
- (Sound familiar?)

AWS Logging Services

Overview

A configuration package to enable AWS security logging and activity monitoring services: **AWS CloudTrail**, **AWS Config**, and **Amazon GuardDuty**. The package also includes an S3 bucket to store CloudTrail and Config history logs, as well as an optional CloudWatch log group to receive CloudTrail logs.

Configure & Deploy

Configuration Presets

Environment

production

- Enables AWS CloudTrail, AWS Config, and Amazon GuardDuty
- CloudTrail Trail applid to all regions and Log File Integrity Validation is enabled
- S3 Bucket for CloudTrail logs and Config Logs: Server Side Encryption, Server Access Logging, and Block Public Access
- CloudTrail configured to forward events to a CloudWatch Log Group, with 90 days retention period

Configuration Template

S3 Bucket EDIT

AWS CloudTrail EDIT

Items 9 Size 4.4 KB Launch in AWS Account YAML/JSON

```
AWSTemplateFormatVersion: '2010-09-09'
Description: ''
Resources:
  S3SharedBucket:
```

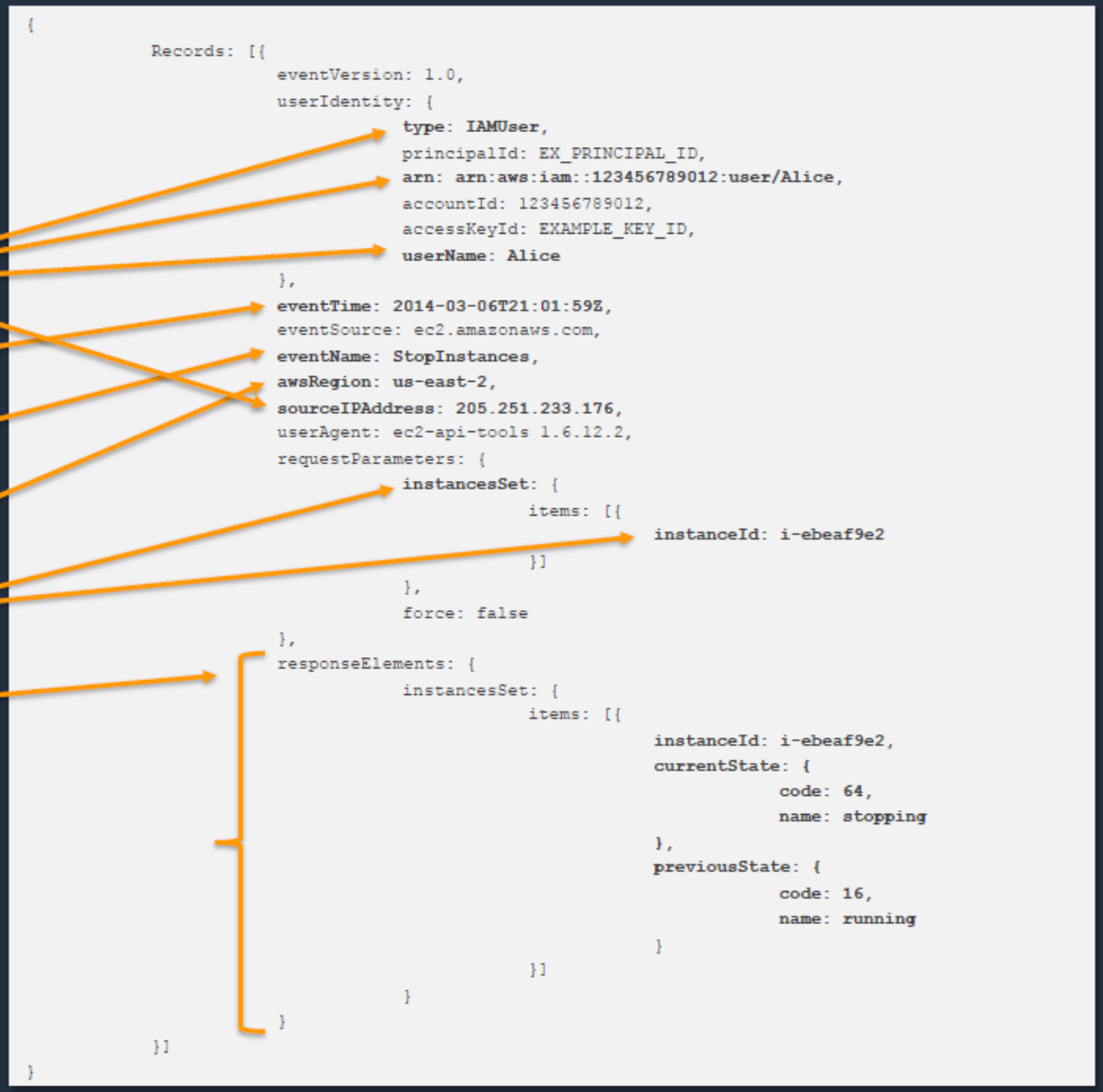
```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "accountId": "123456789012",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:22:54Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]}},
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 0,
            "name": "pending"
        },
        "previousState": {
            "code": 80,
            "name": "stopped"
        }
    }]}}
}]}
```

AWS Services for Incident Response

AWS CloudTrail

`StopInstances`
API Call (Example)

Who
When
What
Where
Which
Result

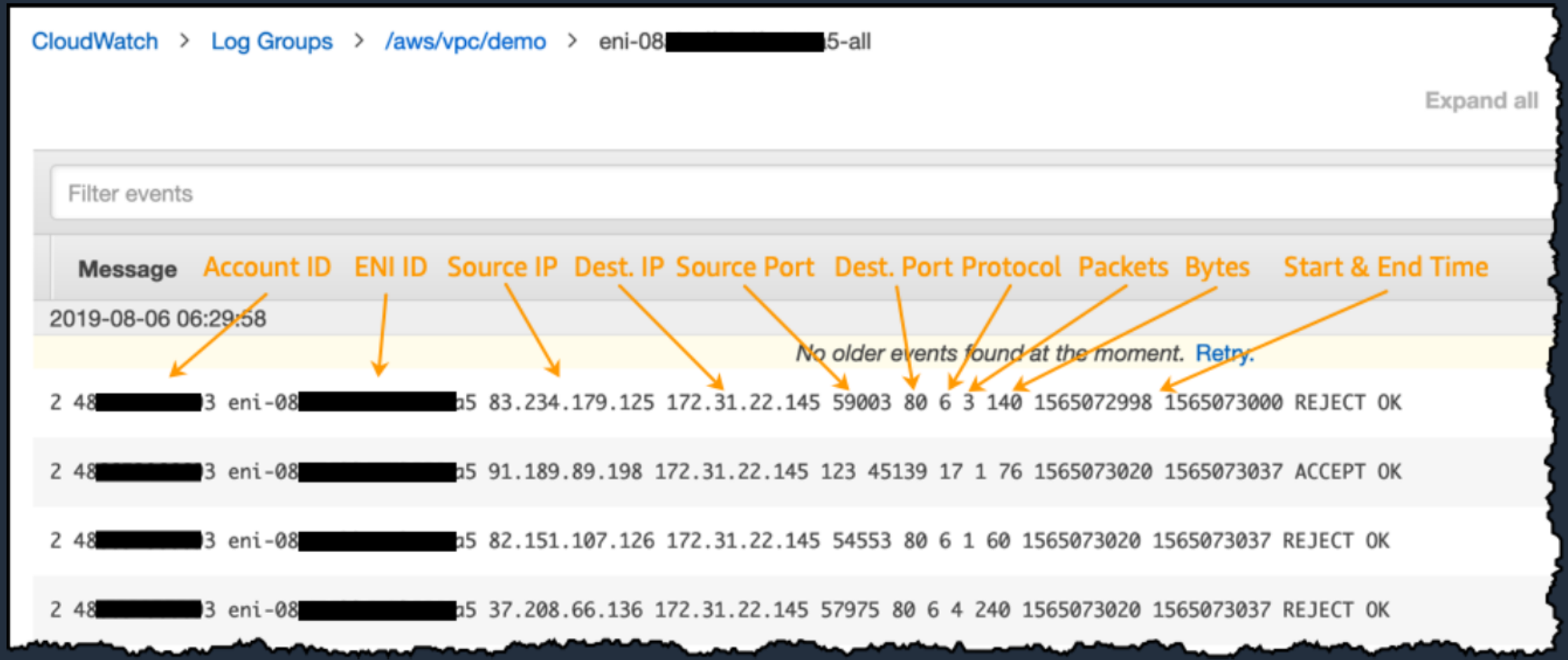


```
{
        Records: [{
                eventVersion: 1.0,
                userIdentity: {
                        type: IAMUser,
                        principalId: EX_PRINCIPAL_ID,
                        arn: arn:aws:iam::123456789012:user/Alice,
                        accountId: 123456789012,
                        accessKeyId: EXAMPLE_KEY_ID,
                        userName: Alice
                },
                eventTime: 2014-03-06T21:01:59Z,
                eventSource: ec2.amazonaws.com,
                eventName: StopInstances,
                awsRegion: us-east-2,
                sourceIPAddress: 205.251.233.176,
                userAgent: ec2-api-tools 1.6.12.2,
                requestParameters: {
                        instancesSet: {
                                items: [{
                                        instanceId: i-ebeaf9e2
                                }]
                        },
                        force: false
                },
                responseElements: {
                        instancesSet: {
                                items: [{
                                        instanceId: i-ebeaf9e2,
                                        currentState: {
                                                code: 64,
                                                name: stopping
                                        },
                                        previousState: {
                                                code: 16,
                                                name: running
                                        }
                                }]
                        }
                }
        }]
}
```

AWS Services for Incident Response

VPC Flow Logs

Version 2 Log Sample (CloudWatch Console)



DON'T FORGET ABOUT AZURE

- https://docs.microsoft.com/en-us/azure/security/azure-log-audit
- Very similar in JSON format
- Otherwise tells you different things
- Use Security Center to help
- https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-schema
- https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-overview

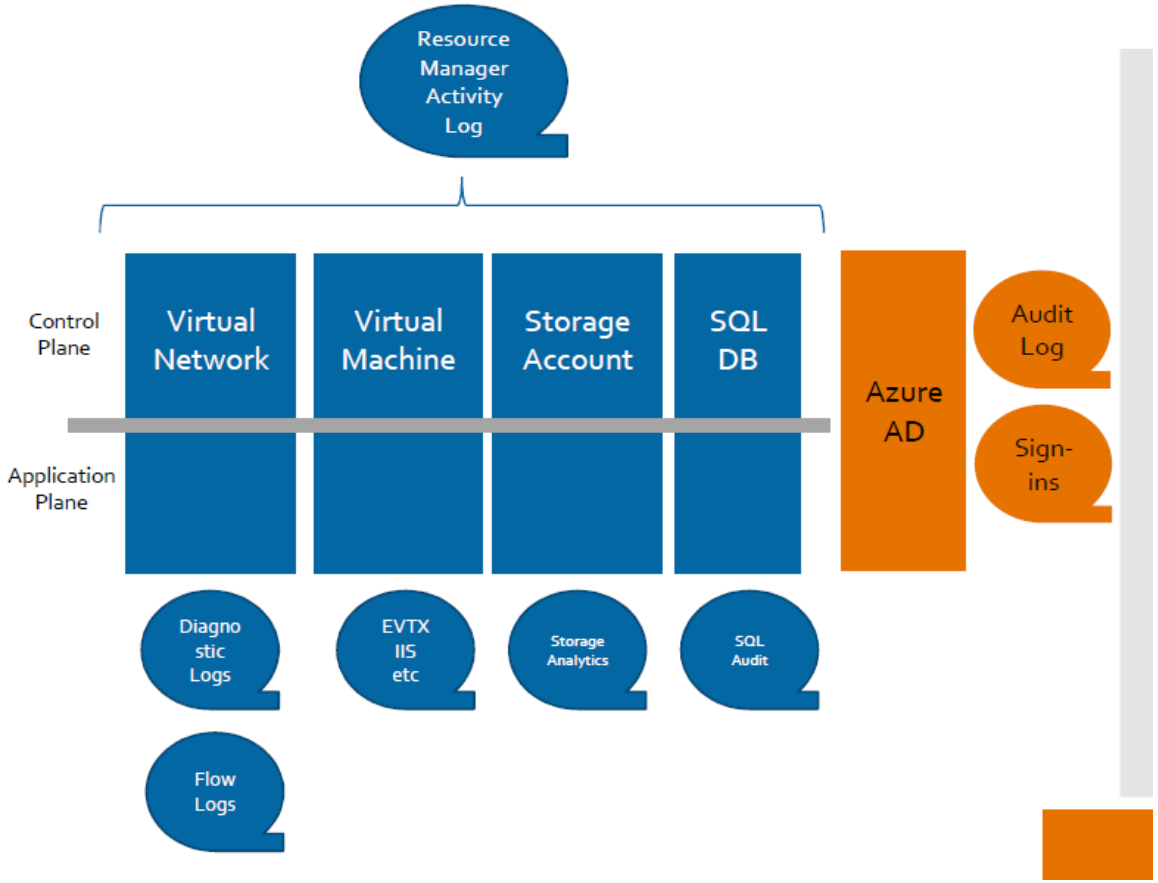
TYPES OF AZURE LOGS

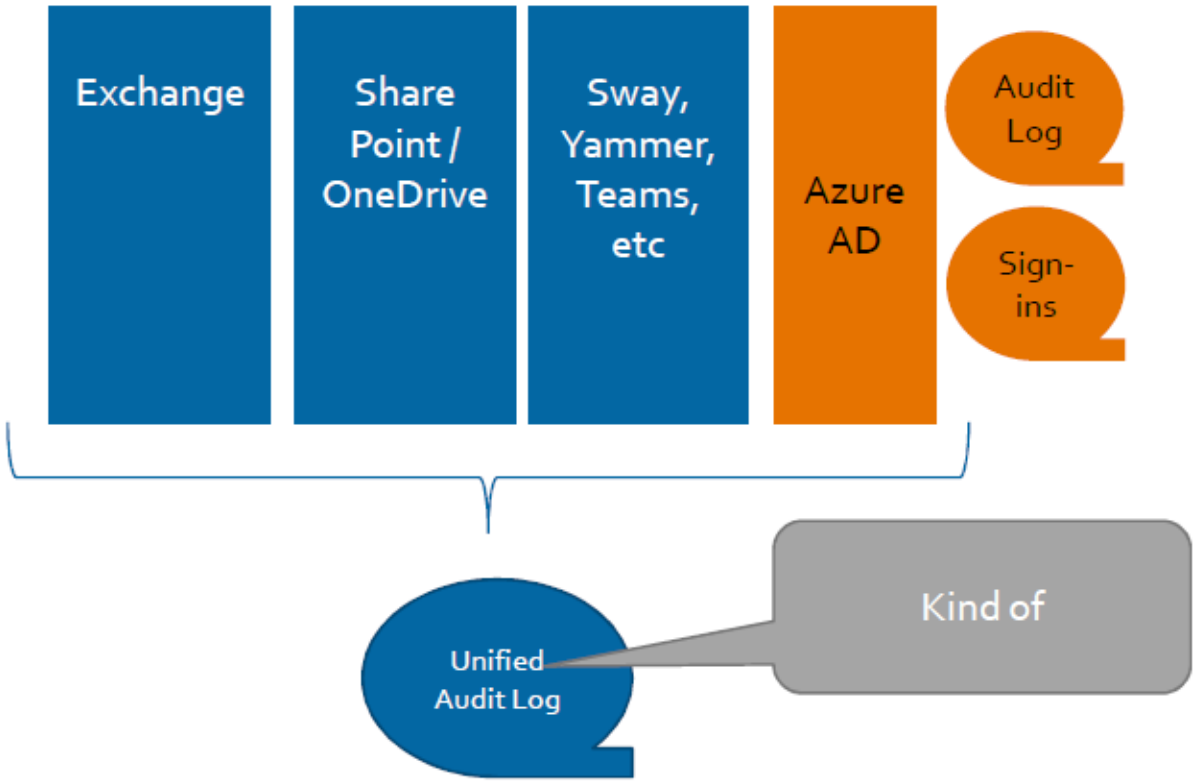
- Activity logs
- Diagnostic logs
- AD reporting
- Virtual machines and cloud services (event and syslog)
- Storage analytics
- Network security group flow logs
- Application
- Process data/security alerts

ULTIMATE IT SECURITY .COM

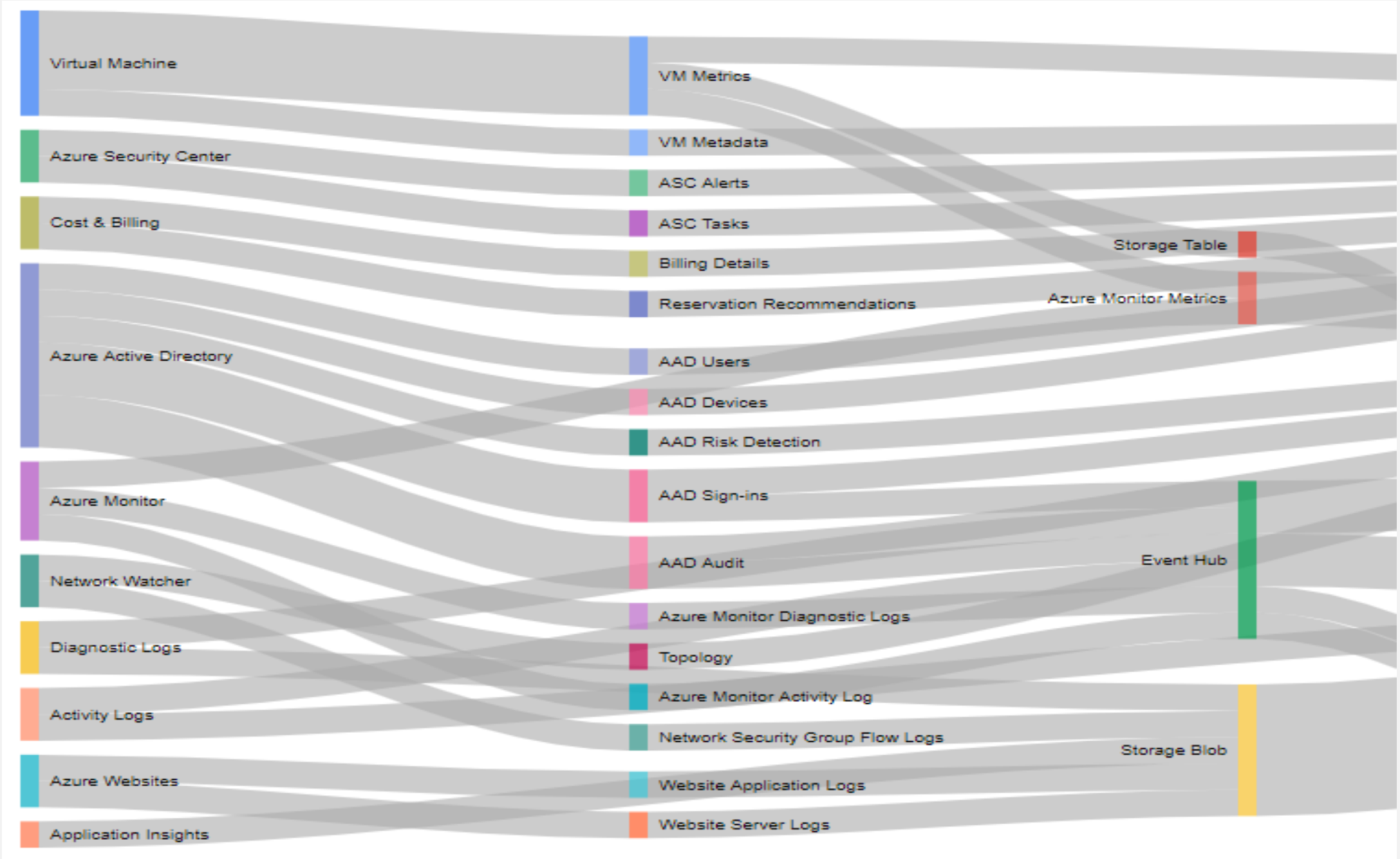
RAPID7

Azure Logging





https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema


Virtual Machine
Azure Security Center
Cost & Billing
Azure Active Directory
Azure Monitor
Network Watcher
Diagnostic Logs
Activity Logs
Azure Websites
Application Insights
VM Metrics
VM Metadata
ASC Alerts
ASC Tasks
Billing Details
Reservation Recommendations
AAD Users
AAD Devices
AAD Risk Detection
AAD Sign-ins
AAD Audit
Azure Monitor Diagnostic Logs
Topology
Azure Monitor Activity Log
Network Security Group Flow Logs
Website Application Logs
Website Server Logs
Storage Table
Azure Monitor Metrics
Event Hub
Storage Blob

```
{
    "records": [
        {
            "time": "2015-01-21T22:14:26.9792776Z",
            "resourceId": "/subscriptions/s1/resourceGroups/MSSupportGroup/providers/microsoft.support/supporttickets/115012112305841",
            "operationName": "microsoft.support/supporttickets/write",
            "category": "Write",
            "resultType": "Success",
            "resultSignature": "Succeeded.Created",
            "durationMs": 2826,
            "callerIpAddress": "111.111.111.11",
            "correlationId": "c776f9f4-36e5-4e0e-809b-c9b3c3fb62a8",
            "identity": {
                "authorization": {
                    "scope": "/subscriptions/s1/resourceGroups/MSSupportGroup/providers/microsoft.support/supporttickets/115012112305841",
                    "action": "microsoft.support/supporttickets/write",
                    "evidence": {
                        "role": "Subscription Admin"
                    }
                },
                "claims": {
                    "aud": "https://management.core.windows.net/",
                    "iss": "https://sts.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/",
                    "iat": "1421876371",
                    "nbf": "1421876371",
                    "exp": "1421880271",
                    "ver": "1.0",
                    "http://schemas.microsoft.com/identity/claims/tenantid": "1e8d8218-c5e7-4578-9acc-9abbd5d23315 ",
                    "http://schemas.microsoft.com/claims/authnmethodsreferences": "pwd",
                    "http://schemas.microsoft.com/identity/claims/objectidentifier": "2468adf0-8211-44e3-95xq-85137af64708",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn": "admin@contoso.com",
                    "puid": "20030000801A118C",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier": "9vckmEGF7zDKk1YzIY8k0t1_EAPaXoeHyPRn6f413zM",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname": "John",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname": "Smith",
                    "name": "John Smith",
                    "groups": "cacfe77c-e058-4712-83qw-f9b08849fd60,7f71d11d-4c41-4b23-99d2-d32ce7aa621c,31522864-0578-4ea0-9gdc-e66cc564d18c",
                    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": " admin@contoso.com",
                    "appid": "c44b4083-3bq0-49c1-b47d-974e53cbdf3c",
                    "appidacr": "2",
                    "http://schemas.microsoft.com/identity/claims/scope": "user_impersonation",
                    "http://schemas.microsoft.com/claims/authnclassreference": "1"
                }
```

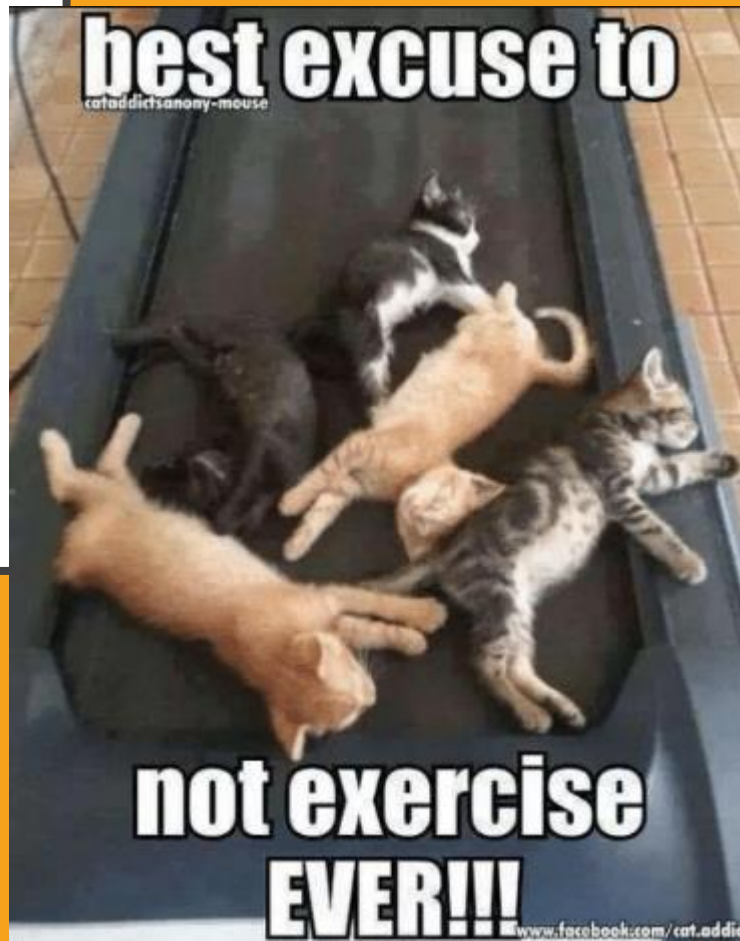
PUTTING IT ALL TOGETHER

LET'S TALK ABOUT THE THREE CS

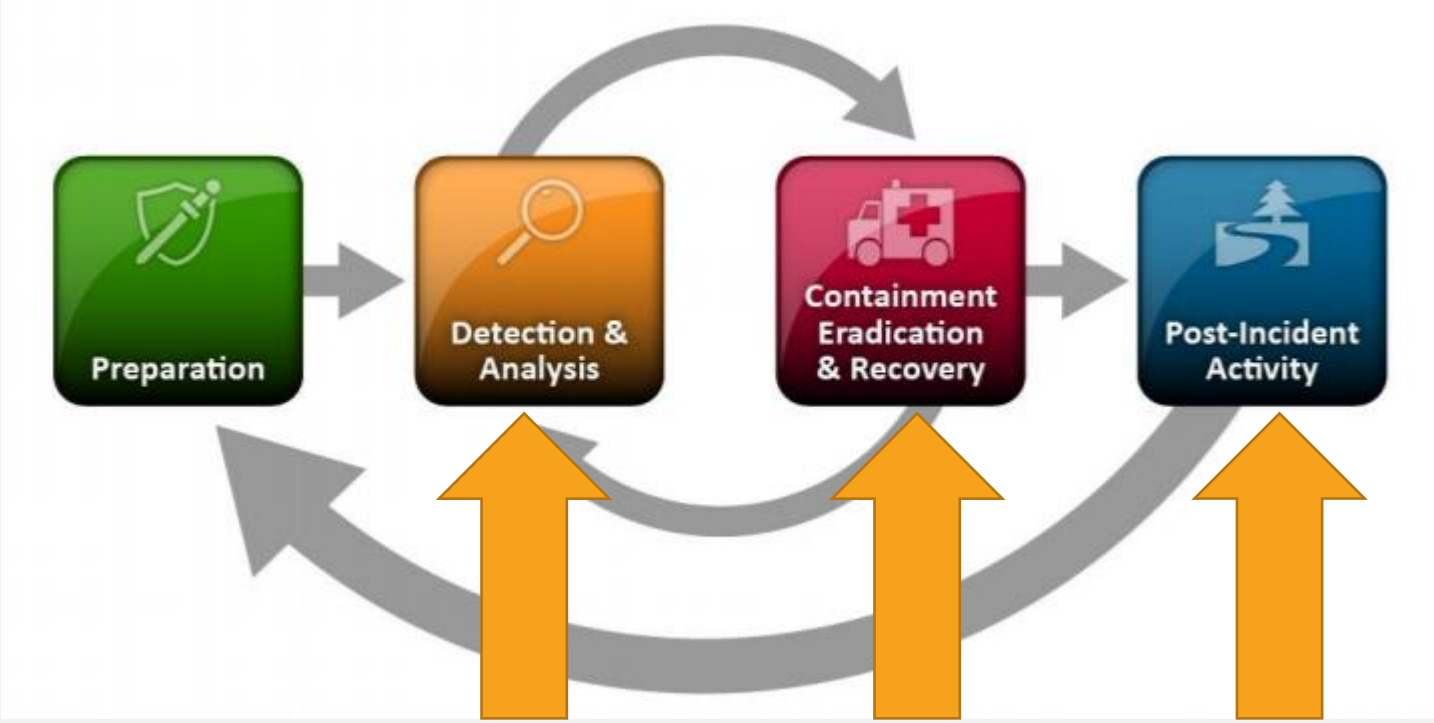
- Critical Thinking
- *Communication*
- *Control of the Message*

Why are these important to incident response?

COMMUNICATION: LET'S GET VISUAL



AT WHAT POINT DOES VISUAL INCIDENT RESPONSE HELP?

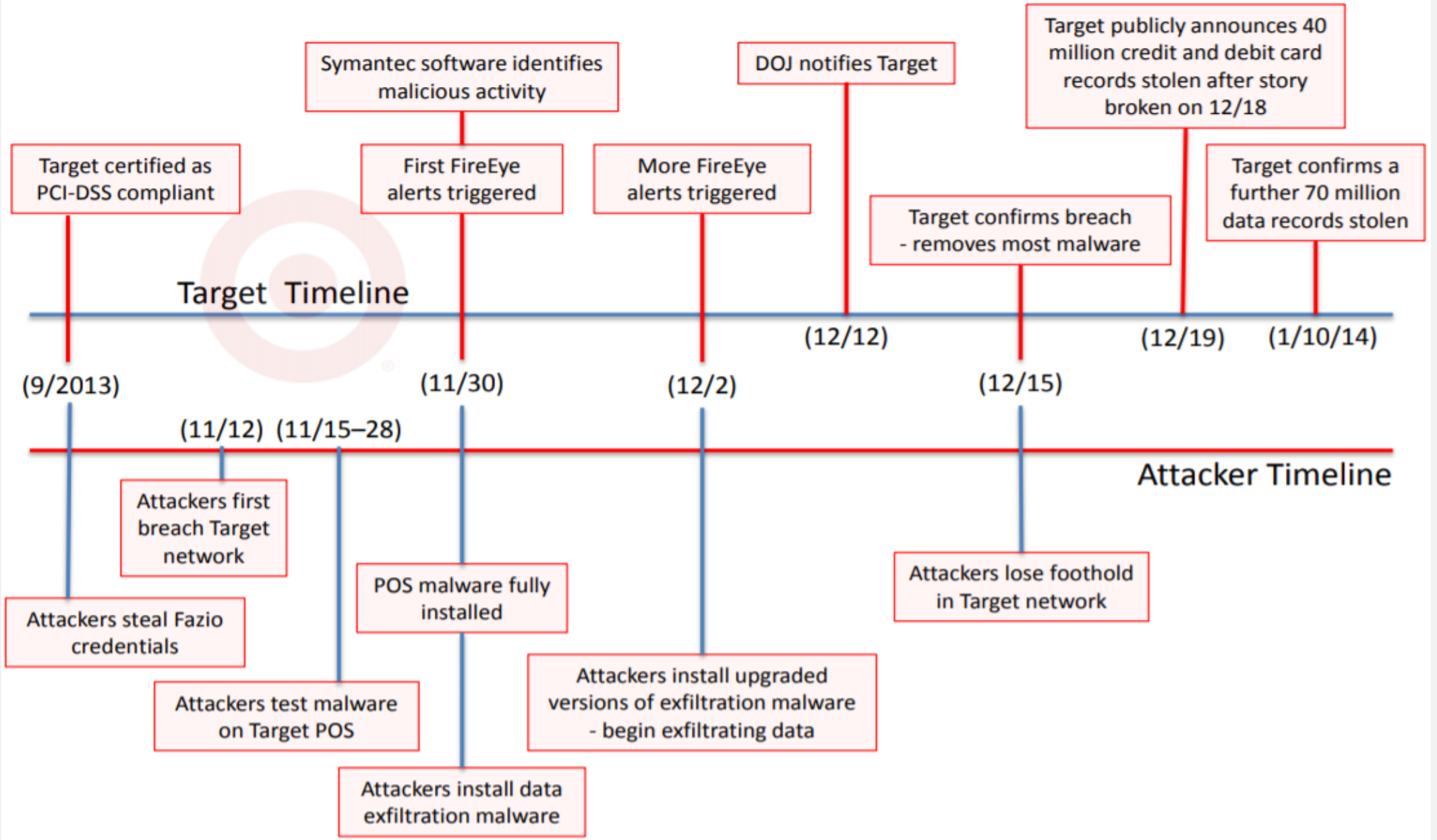


Here for sure

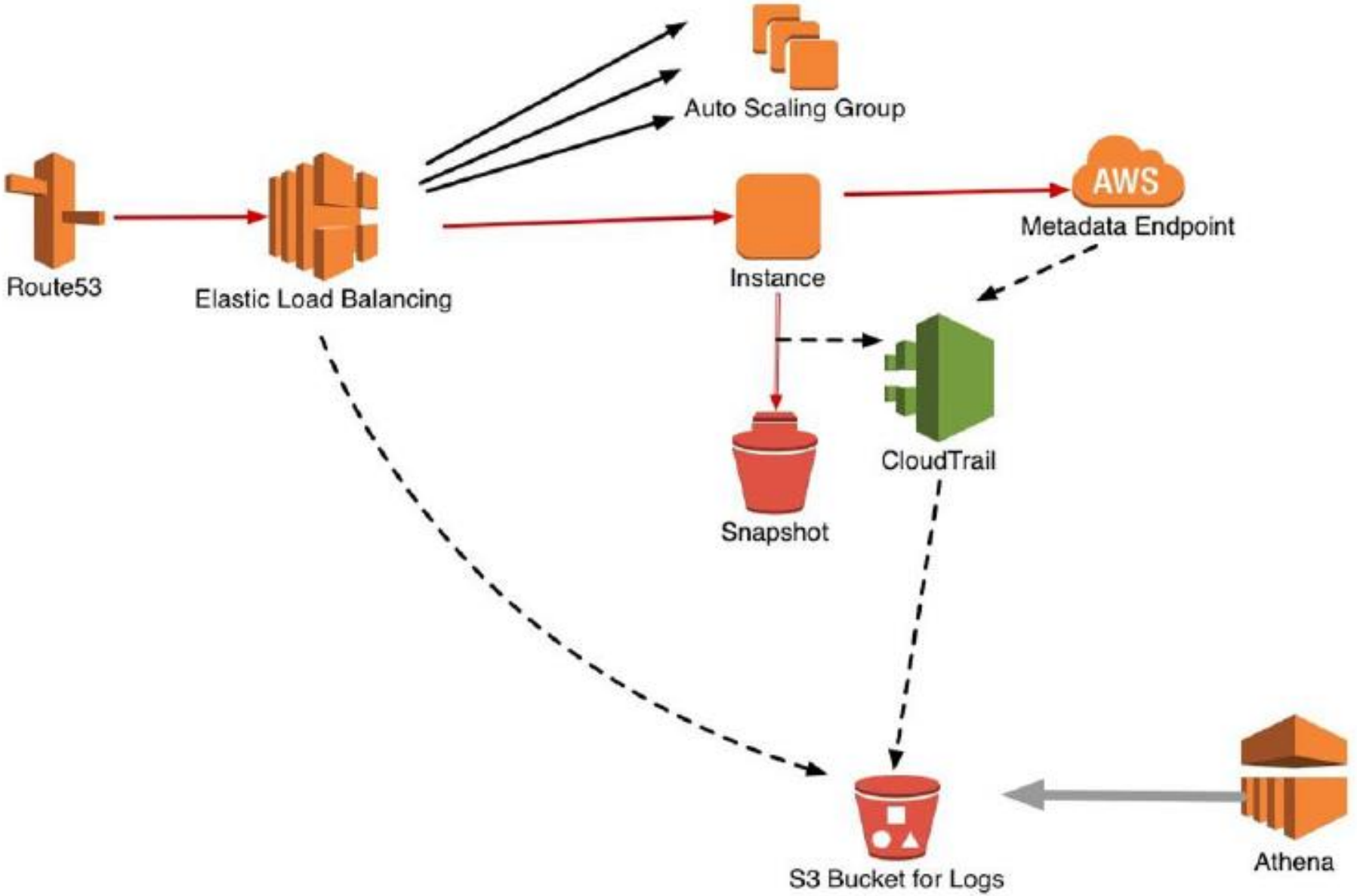
Sometimes here too

For sure here

A Timeline of the Target Data Breach



CLOUD TRAIL


Auto Scaling Group
Route53
Elastic Load Balancing
Instance
AWS
Metadata Endpoint
Snapshot
CloudTrail
S3 Bucket for Logs
Athena

NEED HELP WITH VISUALIZATION?

- Check out the Information is beautiful Facebook page
  - You know pretty quickly what this is saying….

ALSO PRETTY EASY TO UNDERSTAND

WRAPPING UP (YOU MADE IT!!)

- Definitely use tools to help you with the tonnage of data you have to deal with
- But understand what feeds the tool
  - And how the tool may present it
- Why didn't I cover application logs?
- Don't go it alone….

RESOURCES

- https://github.com/chaoticmachinery/frac_rift Endpoint Collection Tools
- https://d1.awsstatic.com/whitepapers/aws-security-best-practices.pdf AWS Security
- http://www.onstrat.com/osint/
- https://www.hybrid-analysis.com/
- https://inteltechniques.com/
- https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- https://www.fireeye.com/services/freeware/redline.html

RESOURCES, PART DEUX

- Malware Forensics: Investigating and Analyzing Malicious Code Cameron H. Malin, Eoghan Casey, James M. Aquilina
- Eagle, Chris The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler. No Starch Press.
- Eilam, Eldad Reversing: Secrets of Reverse Engineering. Wiley.
- http://www.reddit.com/r/ReverseEngineering/
- http://www.virusign.com/
- https://zeltser.com/malware-sample-sources/
- https://zeltser.com/malicious-software/
- Yurichev, Dennis. An Introduction to Reverse Engineering for Beginners. http://beginners.re/RE_for_beginners-en.pdf

WELCOME TO ANALYSIS 102

NOW WHAT?

- Now we talk about Threat Hunting
- And then we do Use Case-A-Palooza!

THREAT HUNTING

- A Definition:

Threat hunting is aptly focused on threats. And to be a threat, an adversary must have three things: the intent, capability and opportunity to do harm. Threat hunters focus their search on adversaries who have those three characteristics and who are already within the networks and systems of the threat hunters' organization, where they have authority to collect data and deploy countermeasures.

- The interesting thing: most Organizations do not do this. Why?

HOW TO SCOPE AN INVESTIGATION

1. Hypothesis-driven investigation
2. Investigation based on known Indicators of Compromise or Indicators of Attack
3. Advanced analytics and machine learning investigations

THREAT MODELING

- DREAD scores five categories, which are summed together and divided by five, the result is a score from 0-10 where 0 indicates no impact and 10 is the worst possible outcome:
- Risk = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5
- **Damage Potential**
- If the vulnerability is exploited, how much damage will be caused?
  - 0 = Nothing
  - 3 = Individual user data is compromised, affected or availability denied
  - 5 = All individual tenant data is compromised, affected or availability denied
  - 7 = All tenant data is compromised, affected or availability denied
  - 7 = Availability of a specific cloud controller components/service is denied
  - 8 = Availability of all cloud controller components is denied
  - 9 = Underlying cloud management and infrastructure data is compromised or affected
  - 10 = Complete system or data destruction, failure or compromise
- **Reproducibility**
- How reliably can the vulnerability be exploited?
  - 0 = Very hard or impossible, even for administrators. The vulnerability is unstable and statistically unlikey to be reliably exploited
  - 5 = One or two steps required, tooling / scripting readily available
  - 10 = Unauthenticated users can trivially and reliably exploit using only a web browser
- **Exploitability**
- How difficult is the vulnerability to exploit?
  - 0 = N/A We assert that every vulnerability is exploitable, given time and effort. All scores should be 1-10
  - 1 = Even with direct knowledge of the vulnerability we do not see a viable path for exploitation
  - 2 = Advanced techniques required, custom tooling. Only exploitable by authenticated users
  - 5 = Exploit is available/understood, usable with only moderate skill by authenticated users
  - 7 = Exploit is available/understood, usable by non-authenticated users
  - 10 = Trivial - just a web browser

Affected Users

•How many users will be affected?

- •0 = None
- •5 = Specific to a given project
- •10 = All users impacted

Discoverability

•How easy is it to discover the threat, to learn of the vulnerability (By convention this is set to 10 even for privately reported vulnerabilities)

- •0 = Very hard to impossible to detect even given access to source code and privilege access to running systems
- •5 = Can figure it out by guessing or by monitoring network traces
- •9 = Details of faults like this are already in the public domain and can be easily discovered using a search engine
- •10 = The information is visible in the web browser address bar or in a form

Describing Vulnerability Scores

We expect the impact of a vulnerability to be described in the following way:

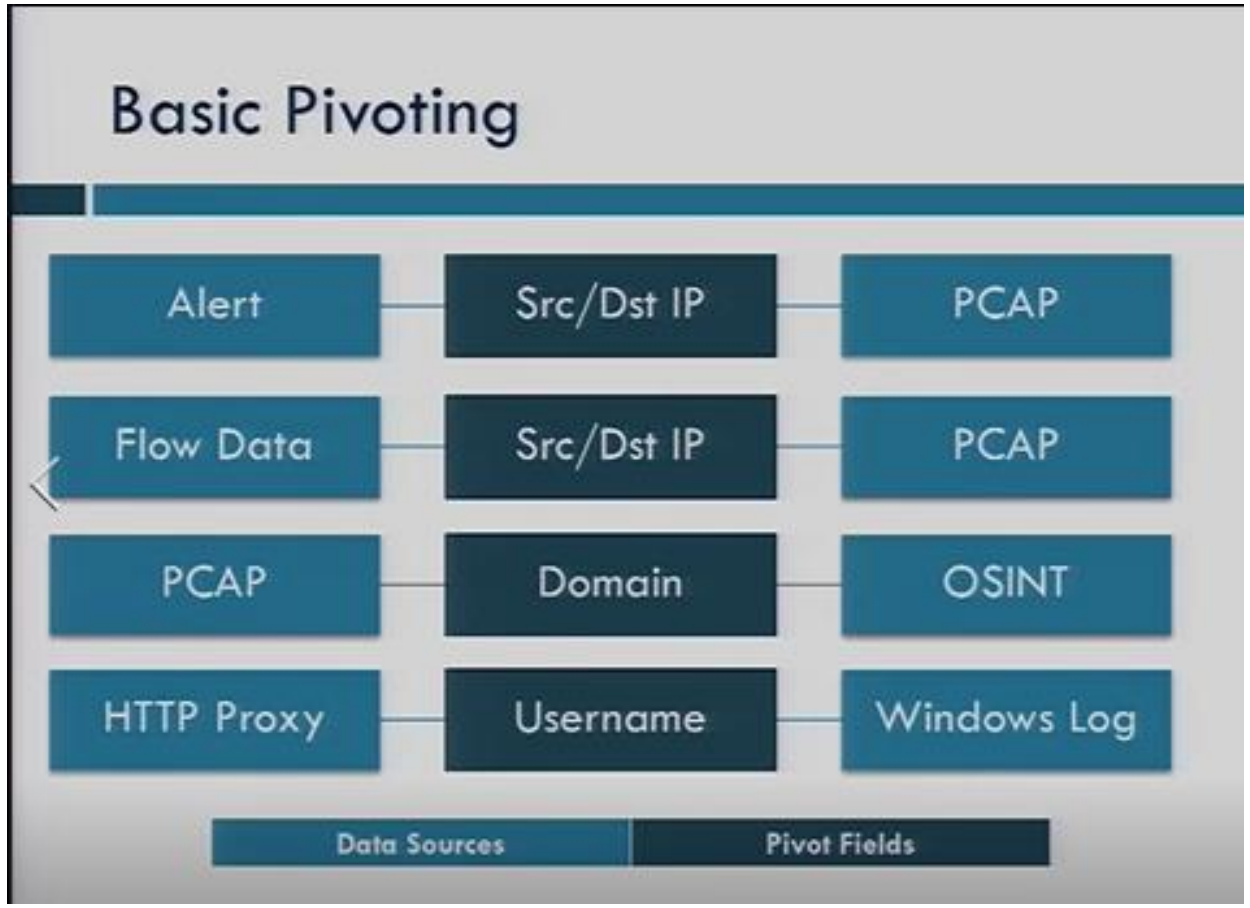
Potential for: Tampering, Escalation				
Category	Score	Rationale		
Damage	6	Significant Disruption		
Reproducability	8	Code path is easily understood, condition exists as standard		
Exploitability	2	Very hard to exploit without specific conditions		
Affected Users	8	All cloud compute users		
Discoverability	10	Discoverability always assumed to be 10		
DREAD SCORE: 31/5 = 6.2 - Important, fix as a priority				

SOME HINTS FROM A VENDOR

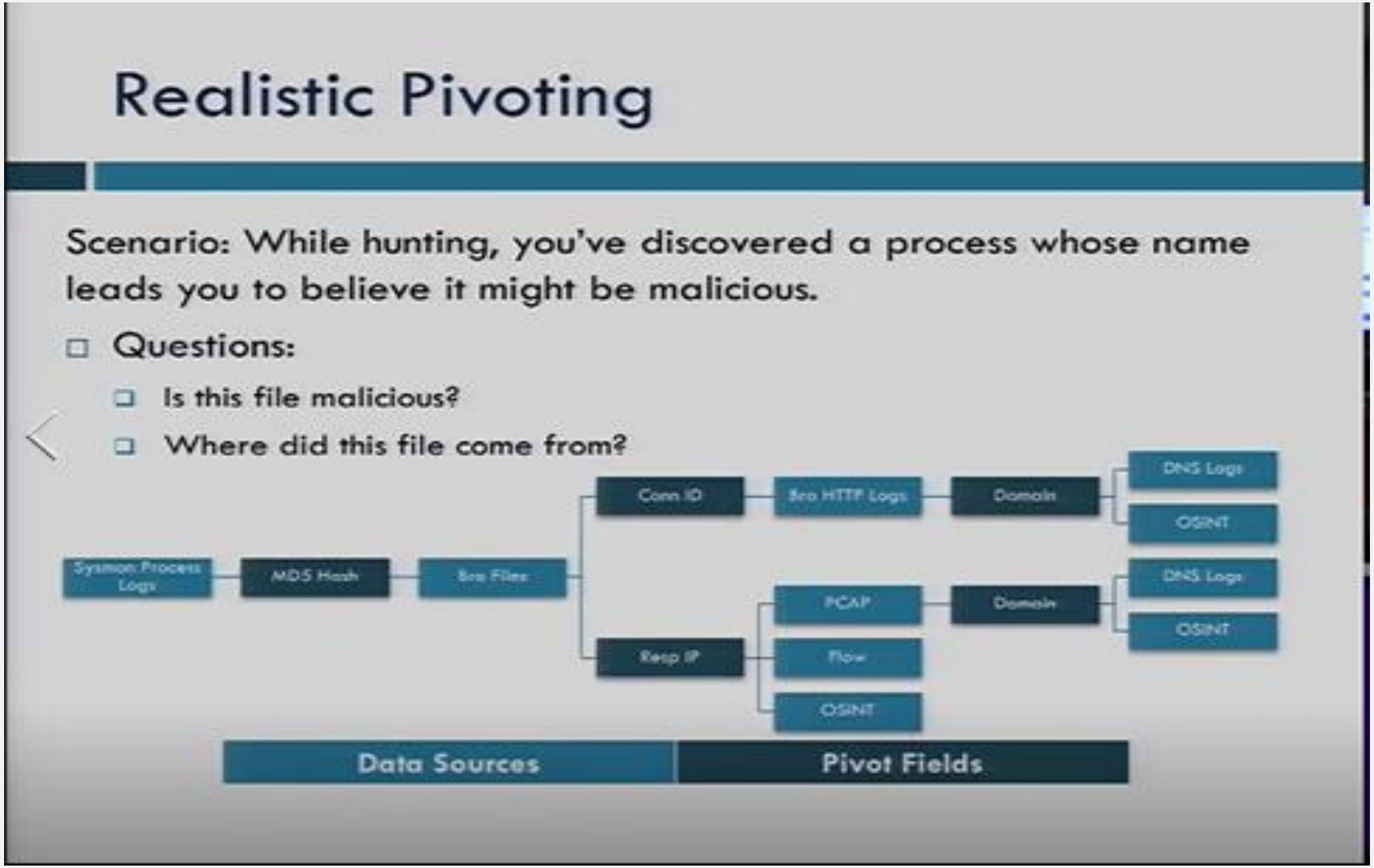
- Collect the right data!
  - Duh! The question is: is this on the endpoint?
- Analyze Relationships
- Incorporate Reputation and Classification Information
- Automate as much as possible!
- Understand attacker motives and tactics
- Know what normal looks like

HOW ABOUT A DIFFERENT WAY TO THINK OF THINGS?

- Abstract Tools
  - What Question am I trying to Answer?
  - Can I find anything in my data that looks like it Doesn't belong?
  - TTP Driven observations
    - What things are suitable for things that aren't Suitable for alerting?
    - Am I seeing pivoting Techniques like these:



PERHAPS IT'S MORE LIKE THIS



WAIT, HOW DO I MAP LIKE THAT?

- Make an Investigative Pivot chart
  - List every data source that you have
  - List every field in that Data source
  - Print, Laminate, Keep close
  - Use a format that makes sense for you
    - Table?
    - Bubble Chart?

SLICE AND DICE YOUR DATA

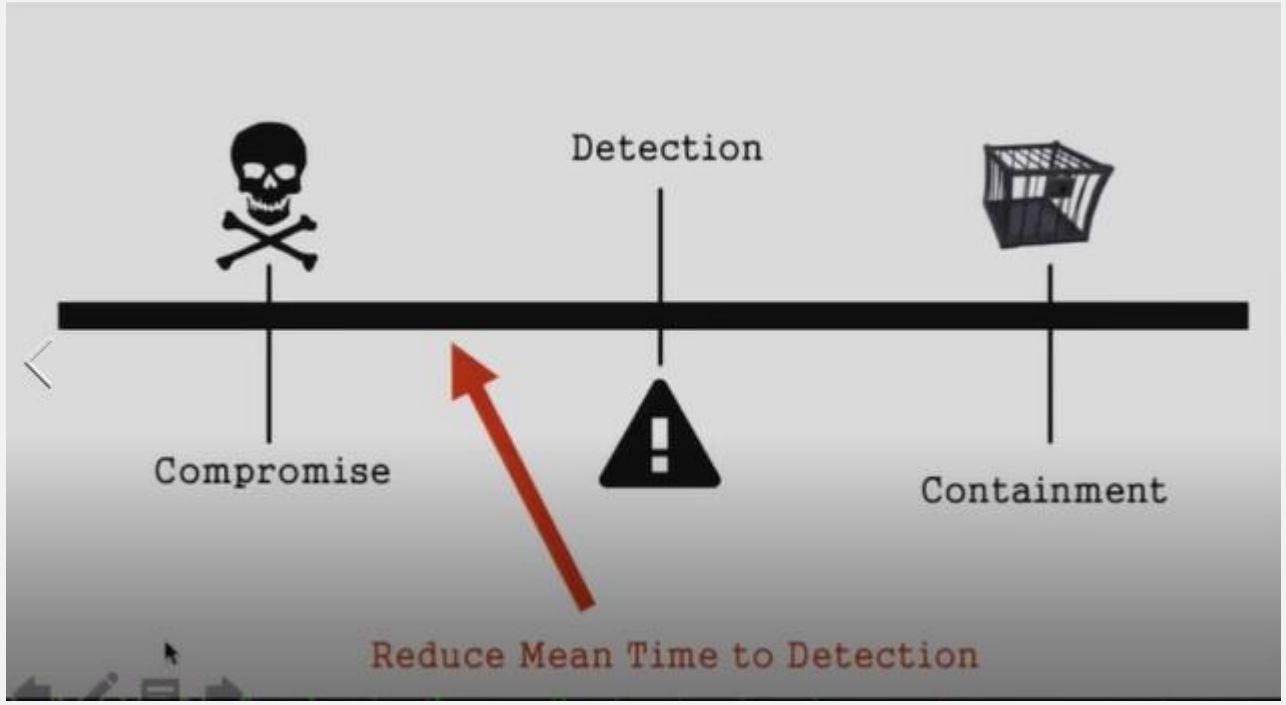
- Aggregation techniques
  - Most occurrences of things
  - LEAST Occurrences of THINGS
  - BYTES Communicated
  - Process names
  - HTTP user agent
  - HTTPS Server Certificate
  - SERVER Authentication User Names
  - Web server access logs
  - CLI Commands executed

OH, AND A BIT OF PROCESS

- Minimize Movement
- Waste nothing- start small not large
- Clean as you go
- Be flexible

VISUALIZATION

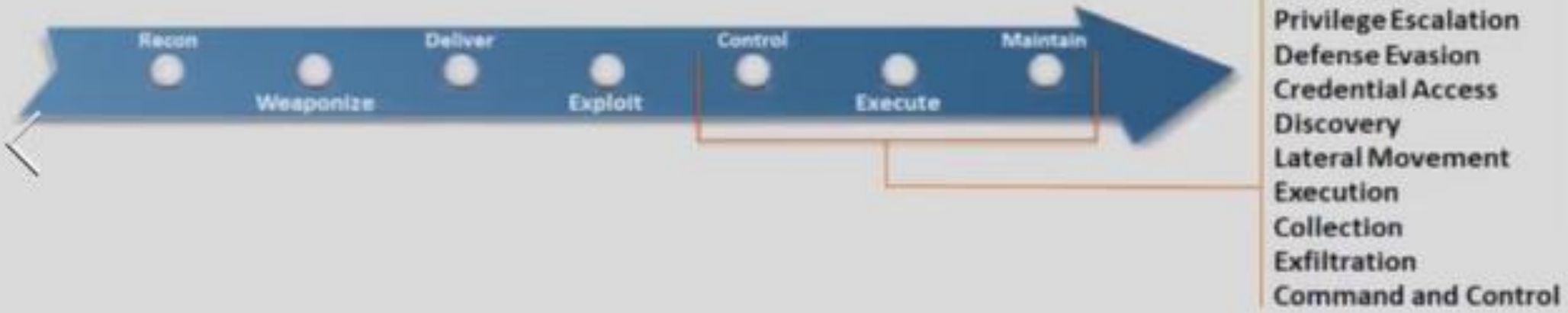
- An over-used word?
- Sometimes it helps!



How Do We Get There?

- Tighter integration between Red & Blue
- Threat Hunting (Blue)
  - Knowing what normal looks like for the environment
  - Looking for anomalous behavior, least frequency of occurrence
- Threat Injection (Red)
  - Execution detection of a single detectable threat in an environment
  - Prioritized ATT&CK techniques based on your organization's threat model

MITRE ATT&CK™ Framework



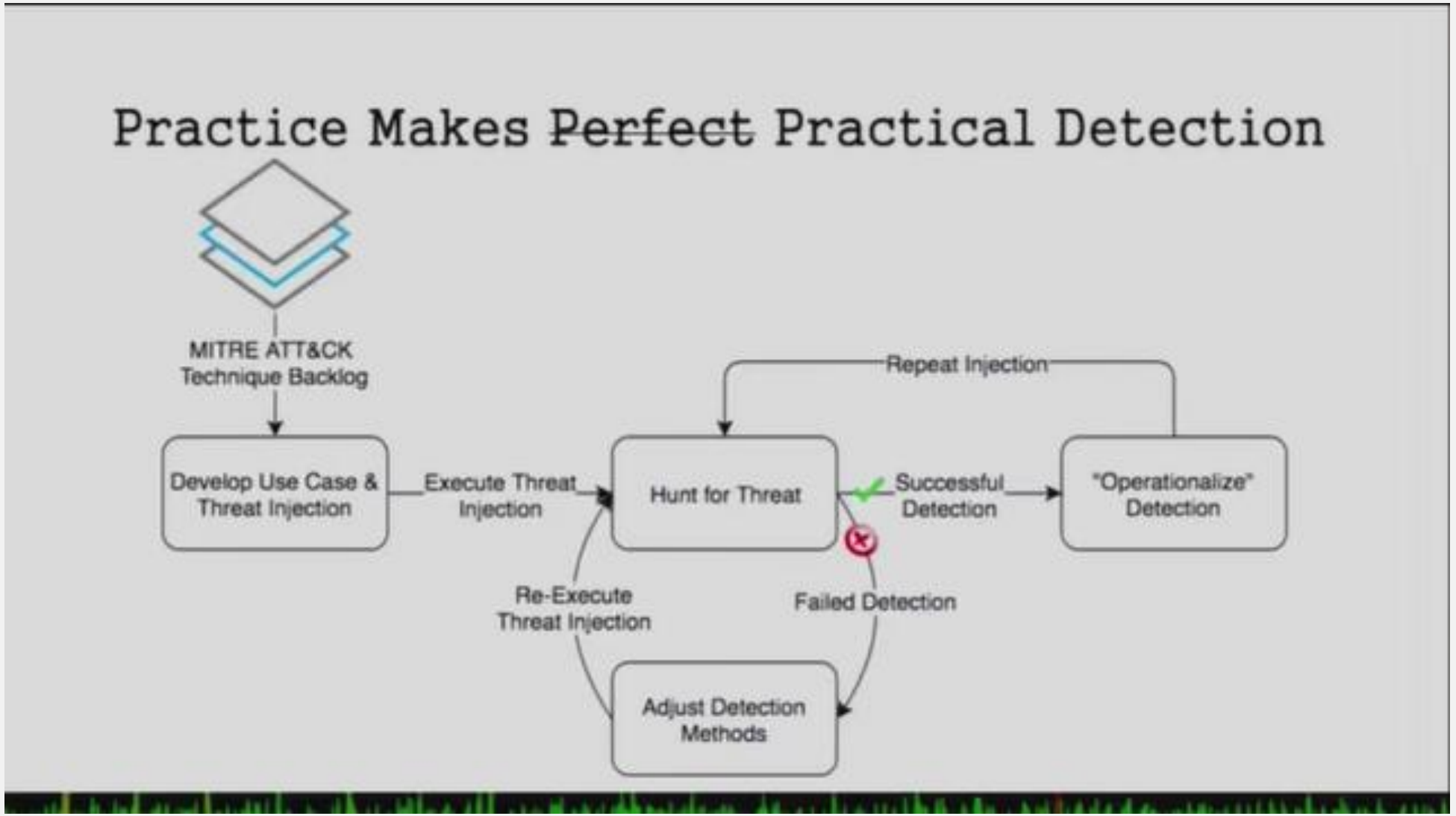
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control

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

Windows ATT&CK for Enterprise Matrix

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Application Shimming	Audio Capture	Automated Exfiltration	Commonly Used Port
AppInit DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Exploitation of Vulnerability	Command-Line Interface	Automated Collection	Data Compressed	Communication Through Removable Media
Application Shimming	AppInit DLLs	Bypass User Account Control	Create Account	File and Directory Discovery	Logon Scripts	Execution through API	Clipboard Data	Data Encrypted	Connection Proxy
Authentication Package	Application Shimming	Code Signing	Credential Dumping	Network Service Scanning	Pass the Hash	Execution through Module Load	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Bootkit	Bypass User Account Control	Component Firmware	Credentials in Files	Network Share Discovery	Pass the Ticket	Graphical User Interface	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Change Default File Association	DLL Injection	Component Object Model Hijacking	Exploitation of Vulnerability	Peripheral Device Discovery	Remote Desktop Protocol	InstallUtil	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding

Practice Makes ~~Perfect~~ Practical Detection



SOME SIMPLE TECHNIQUES

- Searching
- Clustering
- Grouping
- Stack counting

WHAT DOES IT ALL BOIL DOWN TO?

- Just start looking!
- Build a list of indicators
- This takes a lot of time

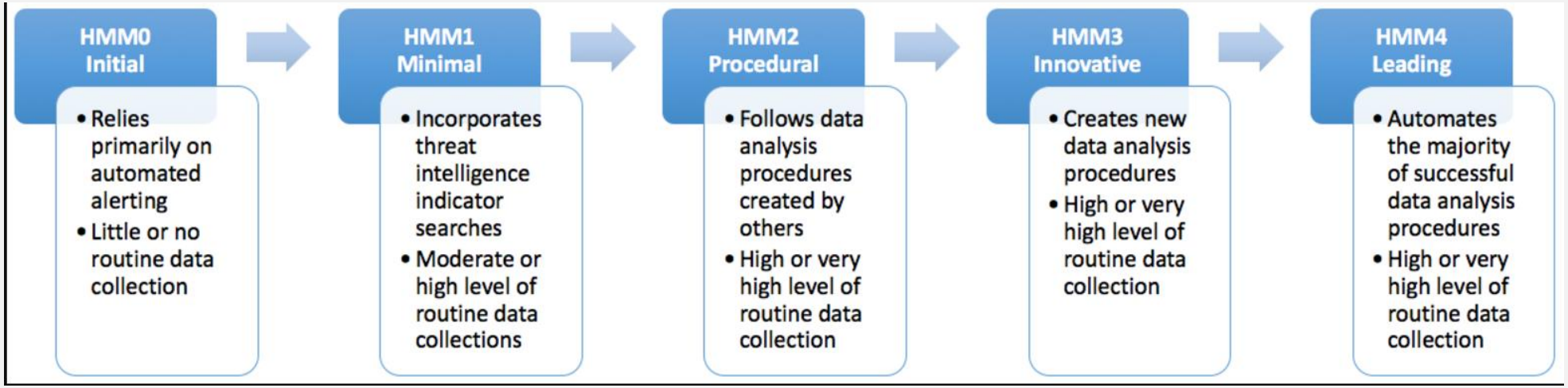
ARE THERE SPECIFIC TECHNOLOGIES?

- Mayyyyyyyyybe
- Depends on the indicator and where that might take place along the Kill Chain (yes that)
- Endpoint data is definitely nice, if you have it
- Netflow data is also handy
- Threat Intel data is priceless!

GOOD SOURCES OF DATA

- Proxy logs
- Windows logs
- Anti-Virus Logs
- What else?

THREAT HUNTING MATURITY MODEL

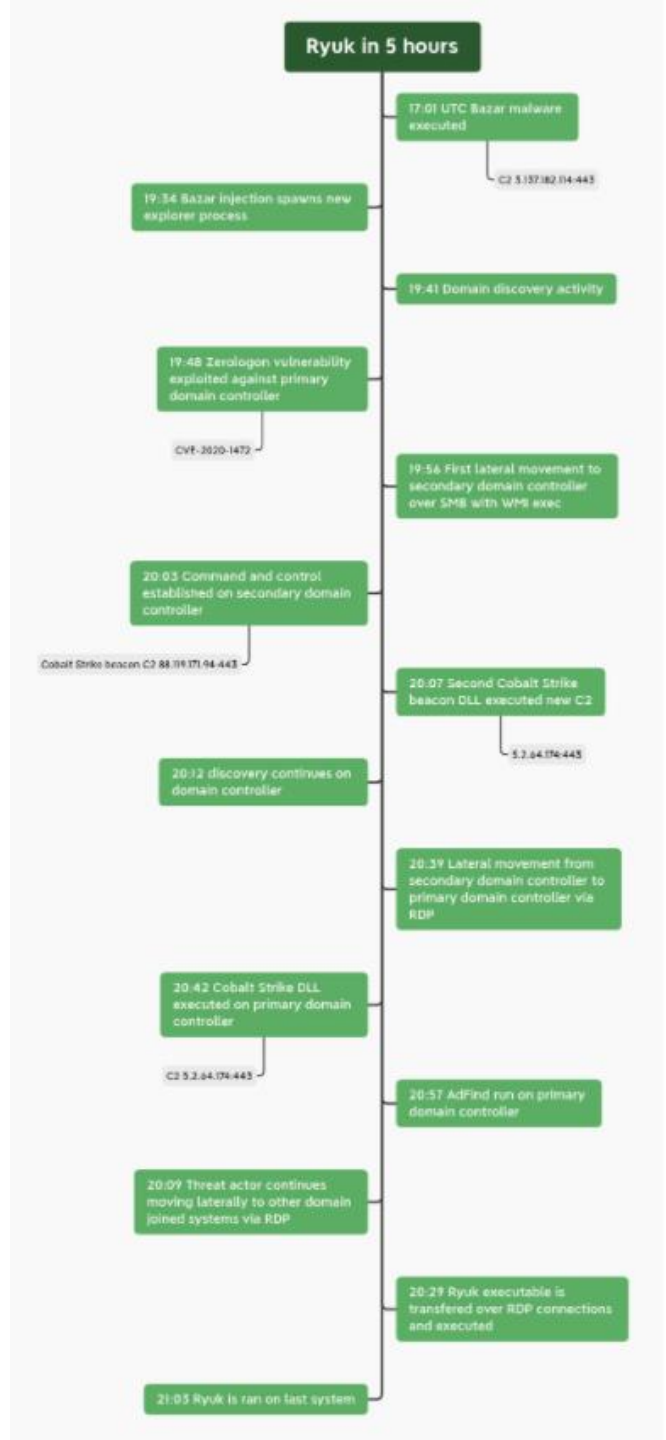


WHICH MEANS YOU…

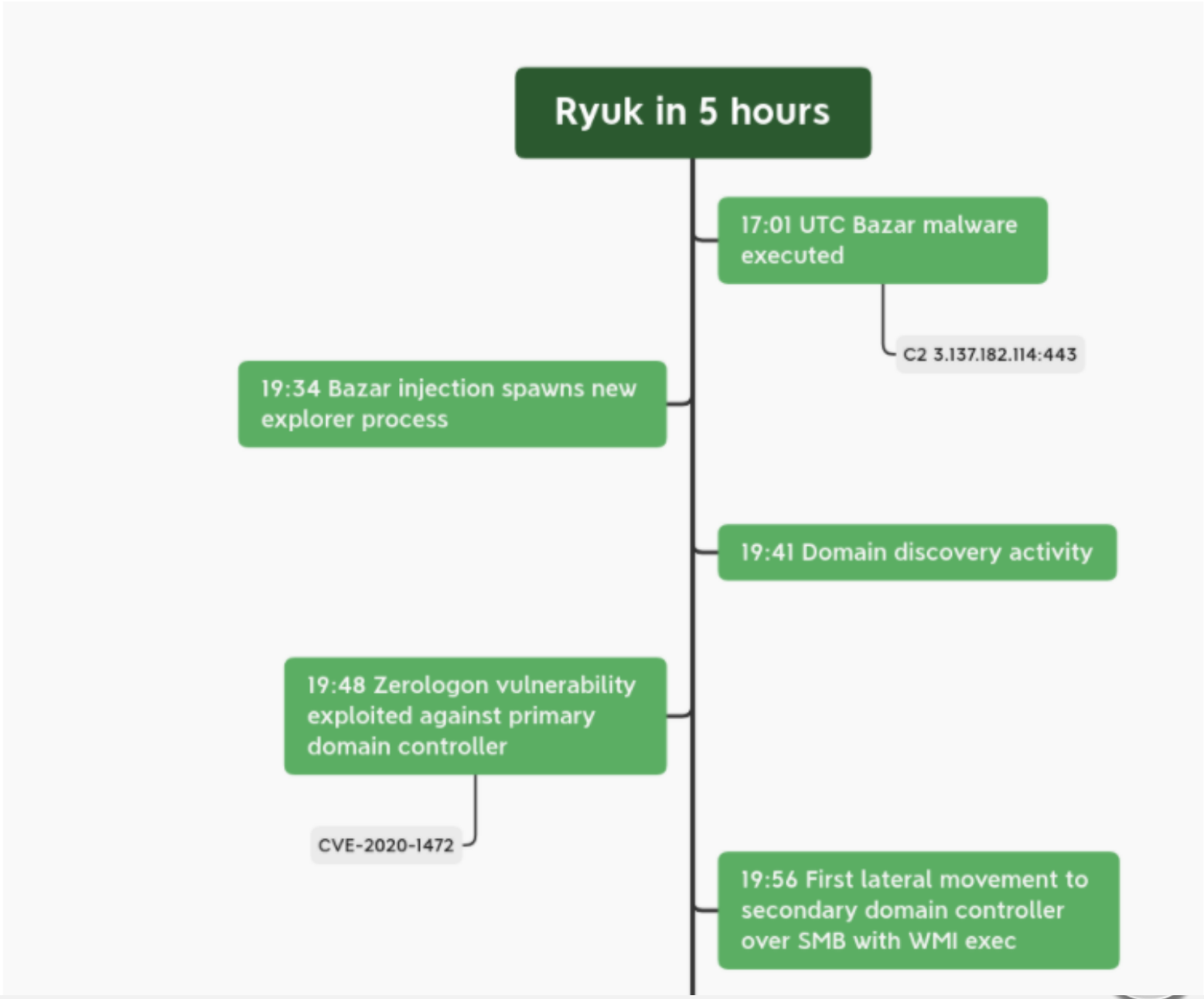
- Embrace BIG Data
- Ask questions
- Pivot…then pivot again (datasets)
- Always have a strategy
- Get your data science on

BUT WE NEED AN EXAMPLE

MEET RYUK



Timeline


Ryuk in 5 hours
17:01 UTC Bazar malware executed
C2 3.137.182.114:443
19:34 Bazar injection spawns new explorer process
19:41 Domain discovery activity
19:48 Zerologon vulnerability exploited against primary domain controller
CVE-2020-1472
19:56 First lateral movement to secondary domain controller over SMB with WMI exec

20:03 Command and control established on secondary domain controller

Cobalt Strike beacon C2 88.119.171.94:443

20:07 Second Cobalt Strike beacon DLL executed new C2

5.2.64.174:443

20:12 discovery continues on domain controller

20:39 Lateral movement from secondary domain controller to primary domain controller via RDP

20:42 Cobalt Strike DLL executed on primary domain controller

C2 5.2.64.174:443

20:57 AdFind run on primary domain controller

20:09 Threat actor continues moving laterally to other domain joined systems via RDP

20:29 Ryuk executable is transfered over RDP connections and executed

21:03 Ryuk is ran on last system

USE CASE-A-PALOOZA!

- Four use cases:
- First is file based
- Then logs
- Then network
- Then a really difficult one

ANALYSIS CHALLENGE #1

- We got a request from HR to review a USB drive that was seized from an employee.
- The employee allegedly has a side business in pizza trading, which is illegal.
- Do a review of the files in the ‘flashdrive’ directory and see if there is any evidence that should be turned over to law enforcement for further examination.

ANALYSIS CHALLENGE #2

We received an alert that a Unix host potentially compromised. Take a look at the files in 'server logs' and try to answer the following questions.

1. Was the system compromised and when? How do you know that for sure?
2. If the was compromised, what was the method used?
3. Can you locate how many attackers failed? If some succeeded, how many were they? How many stopped attacking after the first success?
4. What is the timeline of significant events? How certain are you of the timing?
5. Anything else that looks suspicious in the logs? Any misconfigurations? Other issues?

ANALYSIS CHALLENGE #3

It's a post-holiday problem: Rudolph the Red Nosed Reindeer is being accused of being responsible for Grandma's disappearance. Review the 'reindeer' pcap and see if you can answer the following questions:

1. According to the packet capture file, what was Grandma's grand plan for Christmas day?
2. Why did the geo-location information on Rudolph's computer, synced from his cell phone, show that Rudolph was in Central Park during the attack?
3. Where should the authorities look for Grandma?
4. Based on the evidence in the packet capture file, who is guilty in this story?

ANALYSIS CHALLENGE #4

- You receive an alert from a windows host that malware has been installed.
- Through the various tools available to you, you get a memory capture.
- Analyze the memory capture call ‘fuzzy.img’ and report back what suspicious activity you find. You are allowed to use tools that you may not immediately have installed right now, but you can also simply use strings or a text editor.
- HINT: The profile you seek is WinXPSP3x86

ARE WE THERE YET?

YES! You made it all the way to the end!

To sum it up: Practice, Practice, Practice!

Discuss hypothesis with your peers

Don’t give up!!

KEEP THE CONVERSATION GOING!

KMWESTPHAL@COX.NET