RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **LAB2-W02**

Put the Analysis Back in Your SOC!

Kristy Westphal

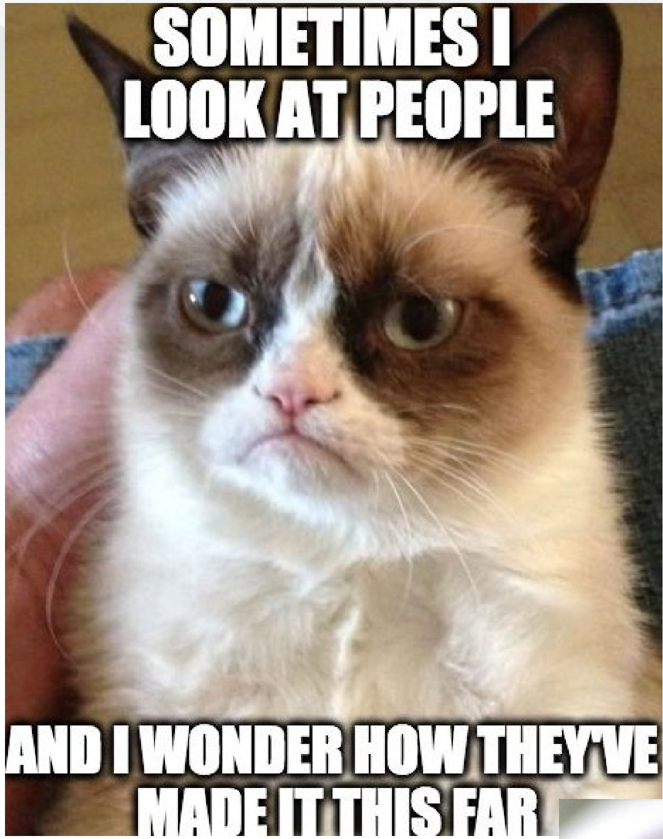
VP, CSIRT
MUFG Union Bank

Disclaimer

- The views, opinions, and material presented by Kristy Westphal at this conference are solely based on her experience and opinions related to incident response.
- The content of this presentation does not reflect the views or opinions of MUFG Union Bank.

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!


SOMETIMES I LOOK AT PEOPLE
AND I WONDER HOW THEY'VE MADE IT THIS FAR

Agenda

- Why we need to train in-house
- Ignorance and importance of analysis (the techniques)
- Lots and lots of practice
  - Log analysis
  - Network forensics
  - Endpoint forensics
  - A quick side journey to Cloud incident response
  - Putting it all together
- How to go back and do this (starting right away)

Why train in-house?

- How well do you sleep at night?
- If you asked your analysts what they do, what would they say?
  - And how happy are they doing it?
- How long did it take you to fill your last open role?
  - Let’s take it upon ourselves to up the game of existing employees
  - And to train good people to become cyber security analysts
- Improve the security posture of your organization by putting the analysis back in your SOC!

Poll the audience

- **How would you rate your SOC's analysis skills today?**
- LAB2-W02

A. Low

B. Medium

C. High

https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1997652731

How do we do that?

- This class is about how to approach analysis techniques
- Not about how to use tools or hack stuff
  - We need to teach thinking, not hacking
- It’s all about understanding what you’ve found
- And most importantly, how to teach it to others

RSA Conference2020

Think about this…

“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***.

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.“

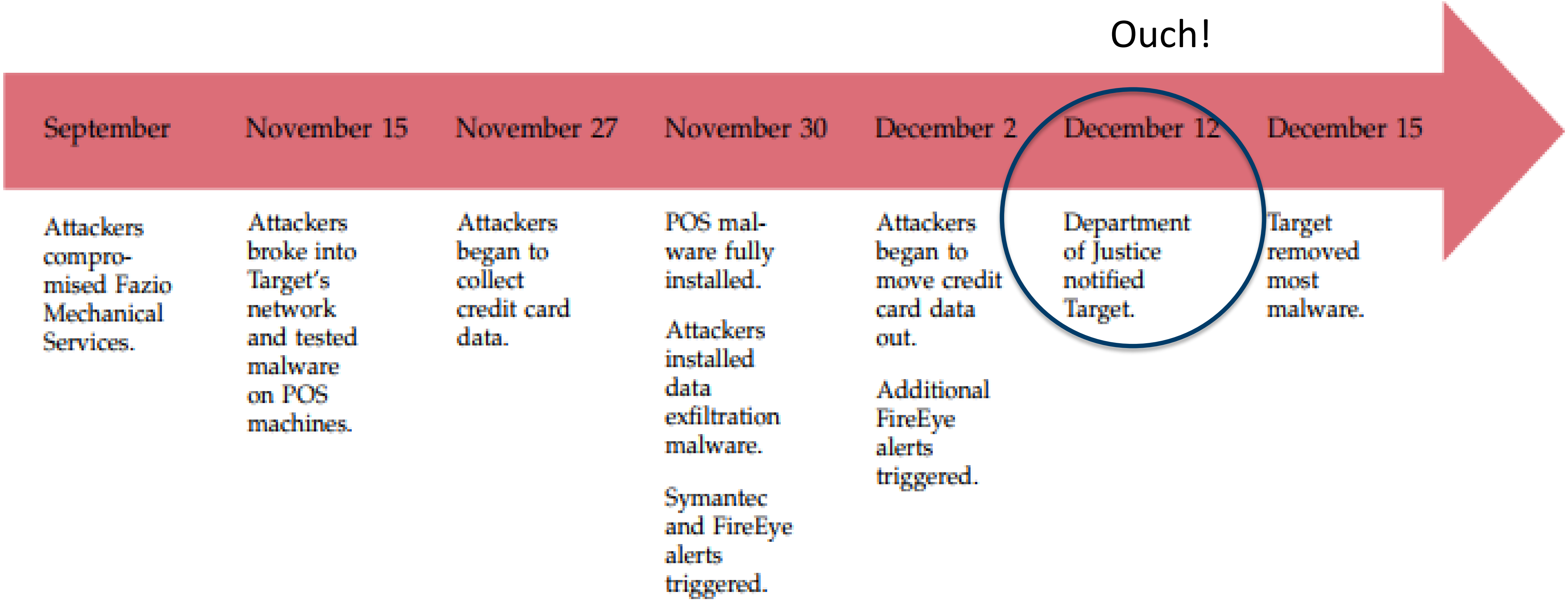
– Damian Menscher

This never happens

- Multiple lockouts from same source
  - Happens to be a development server
- No response from owner
  - No one wants to claim ownership
- Ticket closed as ‘uses vaulted credentials; associate and close’
  - Really? Did anyone check?

Let’s talk about Target (yes, again)

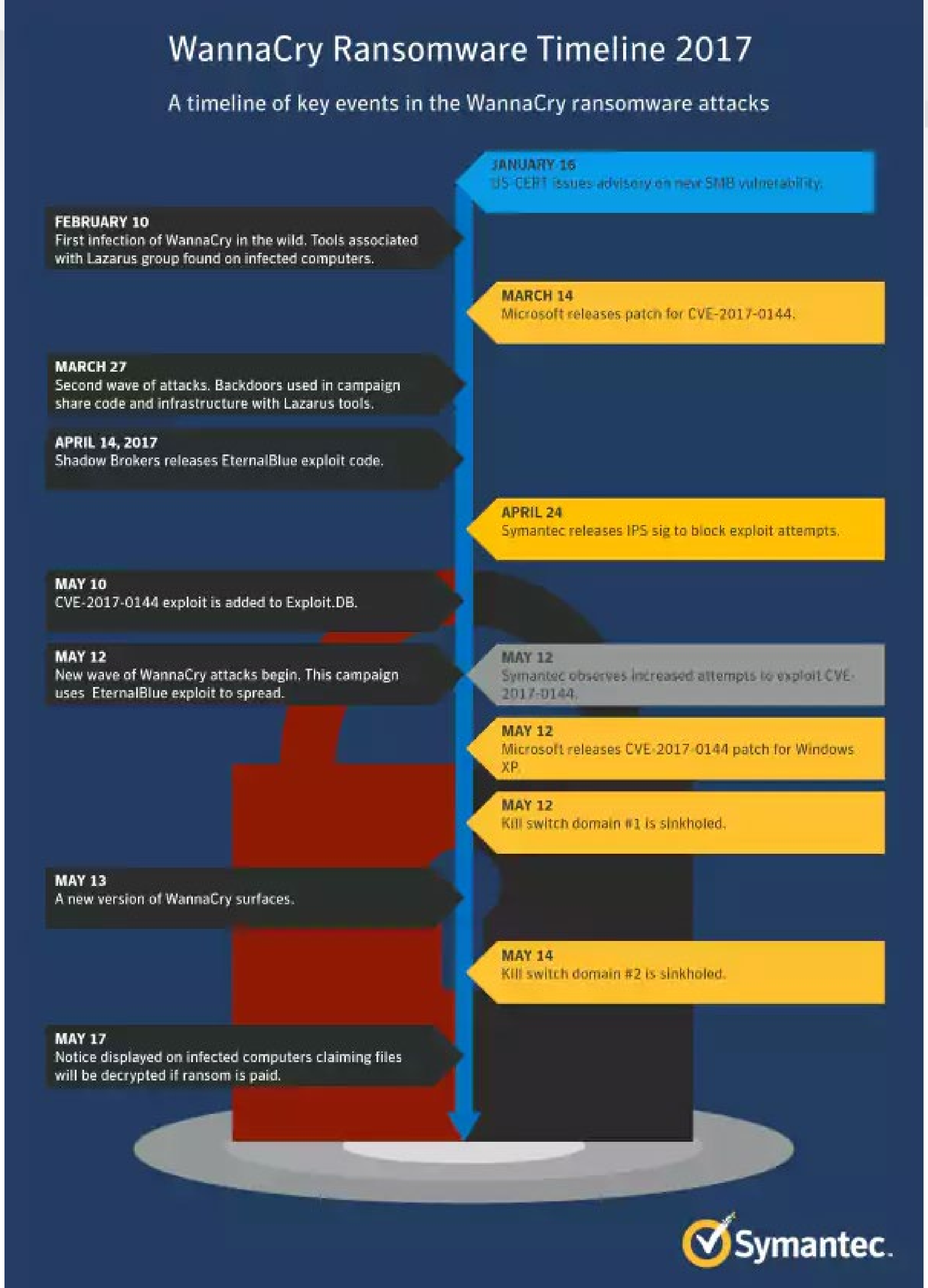
“Predicting or targeting some specific advance is less useful than aiming for deeper understanding.” –Firestein



Ouch!

September	November 15	November 27	November 30	December 2	December 12	December 15
Attackers compromised Fazio Mechanical Services.	Attackers broke into Target’s network and tested malware on POS machines.	Attackers began to collect credit card data.	POS malware fully installed. Attackers installed data exfiltration malware. Symantec and FireEye alerts triggered.	Attackers began to move credit card data out. Additional FireEye alerts triggered.	Department of Justice notified Target.	Target removed most malware.

Wanna Cry?



WannaCry Ransomware Timeline 2017

A timeline of key events in the WannaCry ransomware attacks

JANUARY 16
US-CERT issues advisory on new SMB vulnerability.

FEBRUARY 10
First infection of WannaCry in the wild. Tools associated with Lazarus group found on infected computers.

MARCH 14
Microsoft releases patch for CVE-2017-0144.

MARCH 27
Second wave of attacks. Backdoors used in campaign share code and infrastructure with Lazarus tools.

APRIL 14, 2017
Shadow Brokers releases EternalBlue exploit code.

APRIL 24
Symantec releases IPS sig to block exploit attempts.

MAY 10
CVE-2017-0144 exploit is added to Exploit.DB.

MAY 12
New wave of WannaCry attacks begin. This campaign uses EternalBlue exploit to spread.

MAY 12
Symantec observes increased attempts to exploit CVE-2017-0144.

MAY 12
Microsoft releases CVE-2017-0144 patch for Windows XP.

MAY 12
Kill switch domain #1 is sinkholed.

MAY 13
A new version of WannaCry surfaces.

MAY 14
Kill switch domain #2 is sinkholed.

MAY 17
Notice displayed on infected computers claiming files will be decrypted if ransom is paid.

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

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 vs. 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?

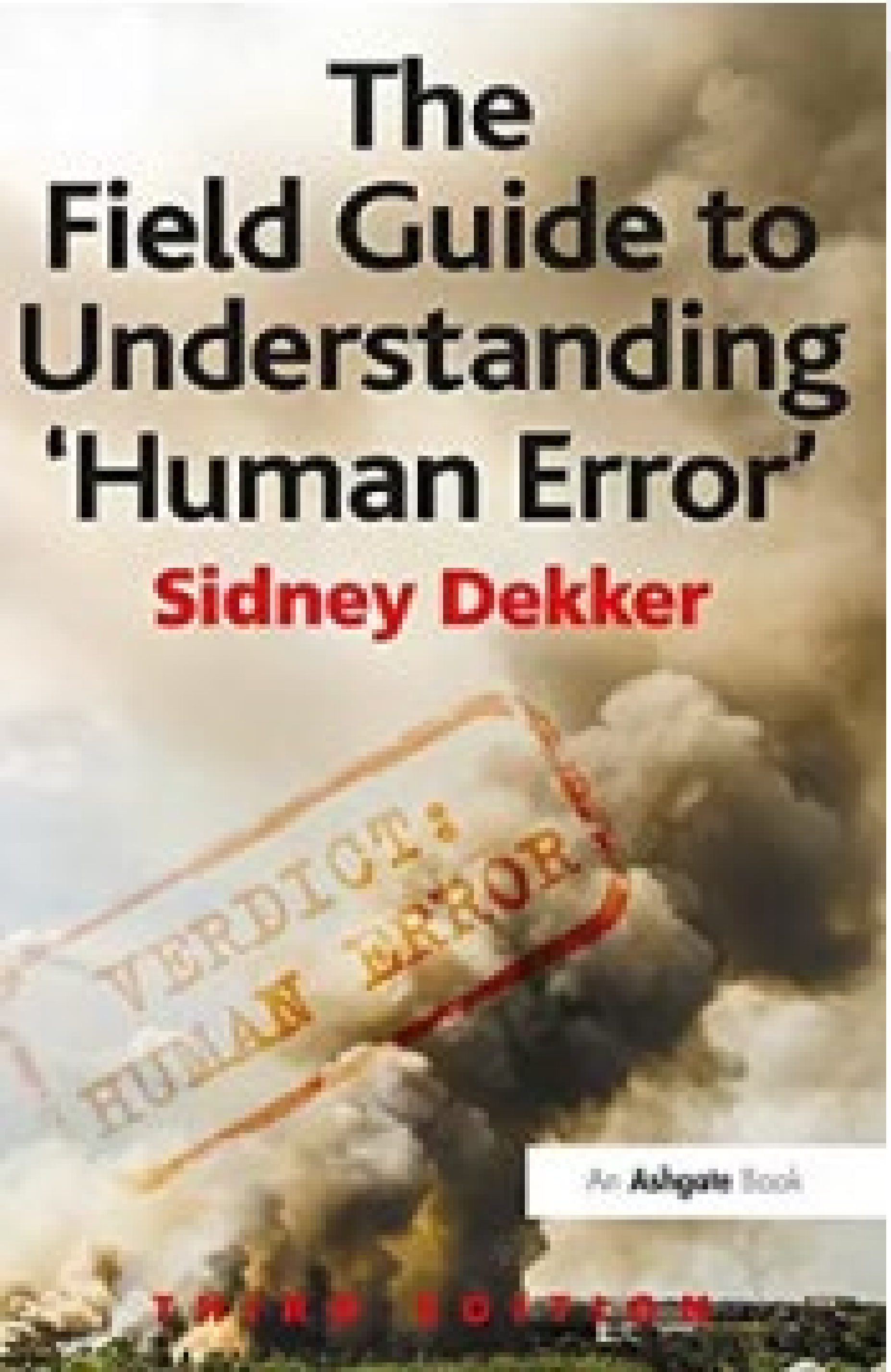
- You put together a timeline/project plan
- You work diligently to achieve it
- Yet the steps you originally map out never end up completed like you originally planned
  - Oftentimes, the end-result isn't what was originally asked for either

Poll the audience

- **Where are the gaps in skill sets in your SOC?**
- LAB2-W02
  A. Network
  B. Operating System
  C. Security Controls

https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1997652731

Maybe a little process



Keep this in mind…

- Getting human factor 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 do you take to analyze?
  - Logs
  - OSINT
  - Threat Intel data
  - Google
  - IOCs
  - Kill Chain

What do you have them look for?

- What is not normal?
- Starting points
  - Odd outbound traffic
  - Strange privileged access behavior
  - Unusual patterns in geographic behavior
  - Log-in anomalies
  - Changes in volumes of database reads
  - Weird changes to the registry

Other tools in your toolbox

- Virustotal.com
- Maltego (Visual analysis)
- FOCA (metadata and hidden in documents)
- Shodan
- Cuckoo
- BURP Suite
- KALI Linux
- OSINT Framework
- And take a look at this crazy site: http://www.onstrat.com/osint/

Other ways to research

- News sites
- Corporate websites
- Government websites
- Blogs
- Social media (Try socialmention.com)
- APIs
- A moment on the Dark Web…
- Don’t always rely on one method

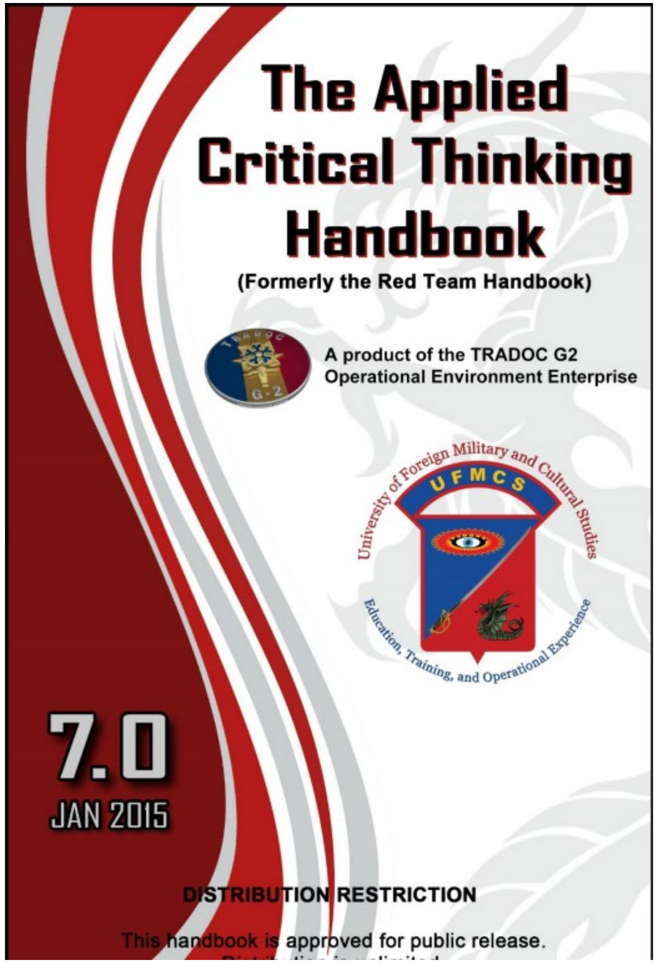
Red teaming?

- Good techniques for decision-making can also be found in poking holes in hypotheses

MICAH ZENKO

RED TEAM

HOW TO SUCCEED BY THINKING LIKE THE ENEMY



The Applied Critical Thinking Handbook

(Formerly the Red Team Handbook)

A product of the TRADOC G2 Operational Environment Enterprise

TRADOC
G-2
University of Foreign Military and Cultural Studies
UFMCS
Education, Training, and Operational Experience

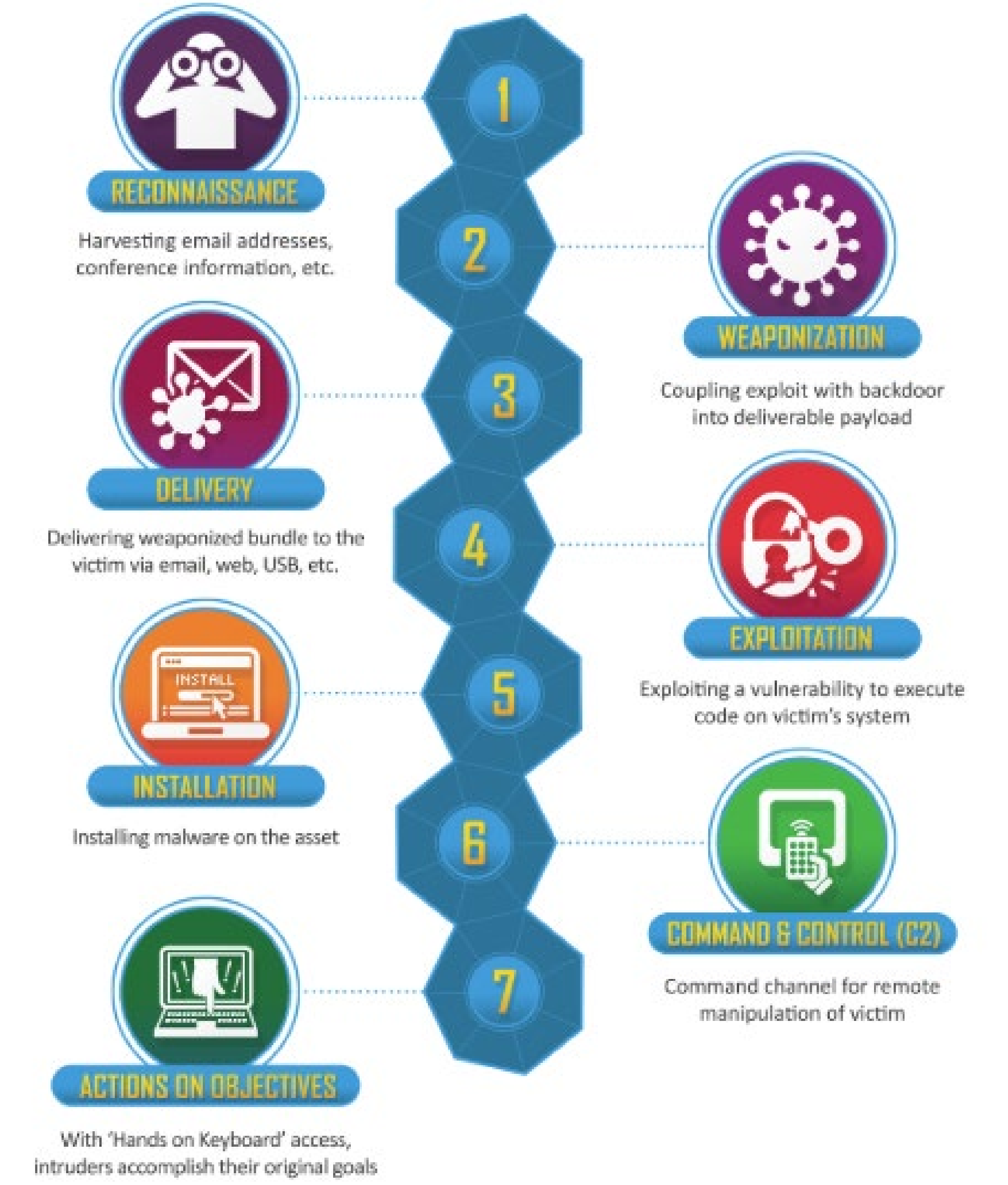
7.0

JAN 2015

DISTRIBUTION RESTRICTION

This handbook is approved for public release.

Apply hypothesis to 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 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

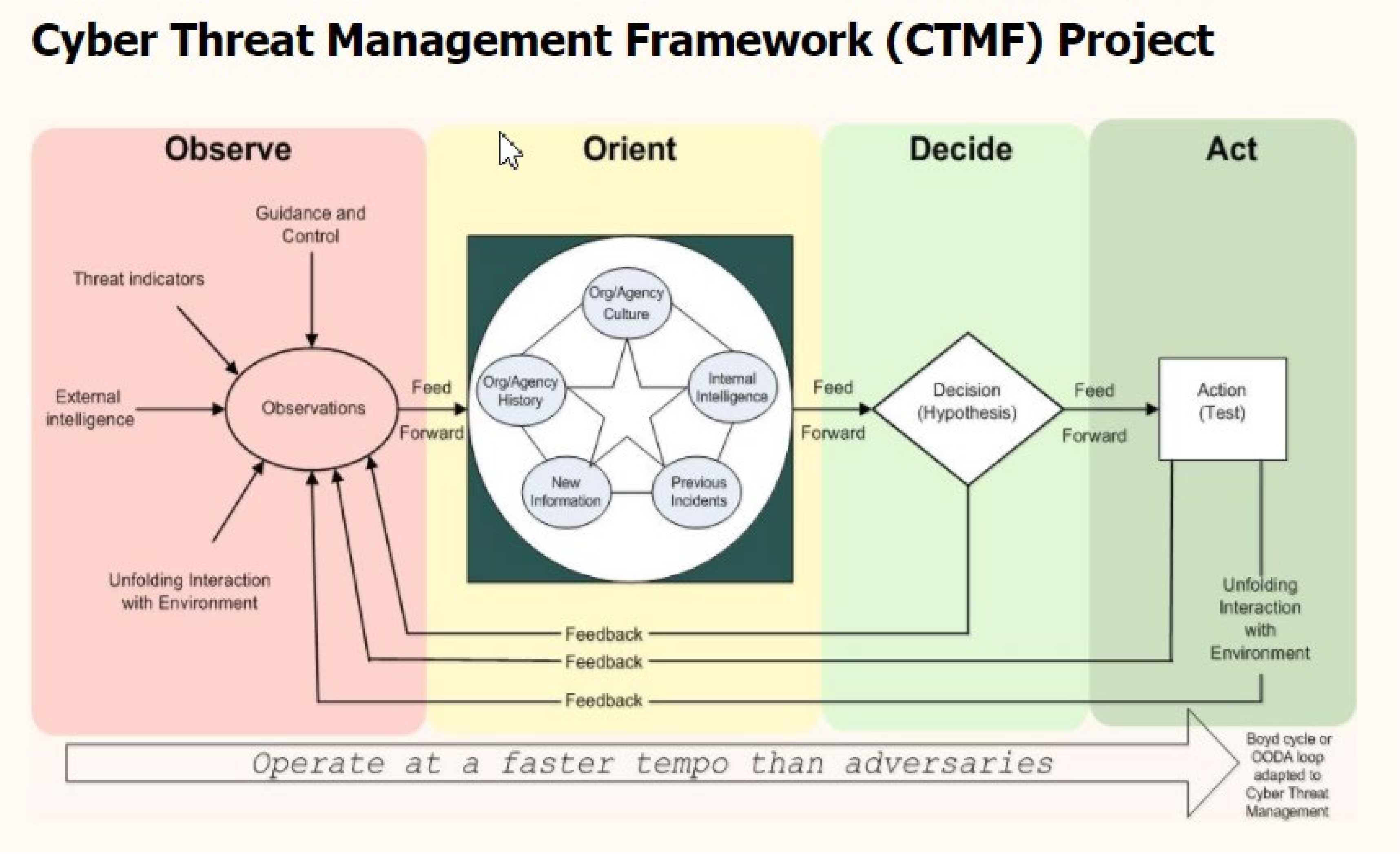
7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

Then maybe apply a little DREAD

- 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

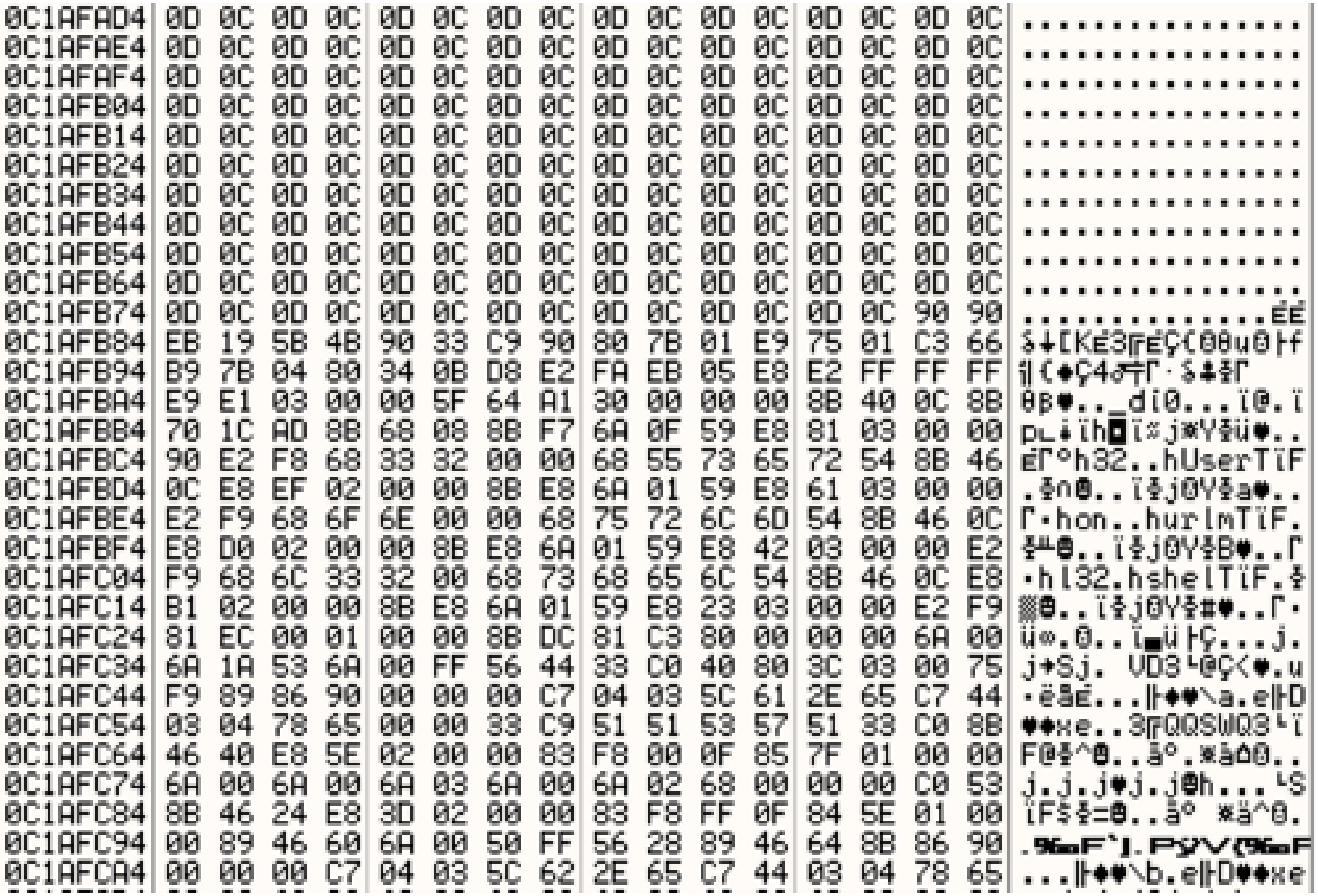


Cyber Threat Management Framework (CTMF) Project

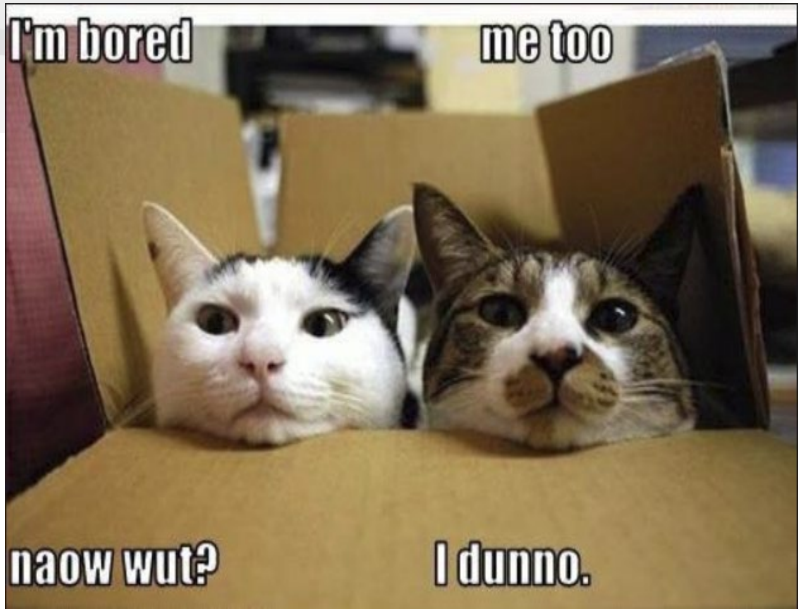
Boyd cycle or OODA loop adapted to Cyber Threat Management

Speed round of samples

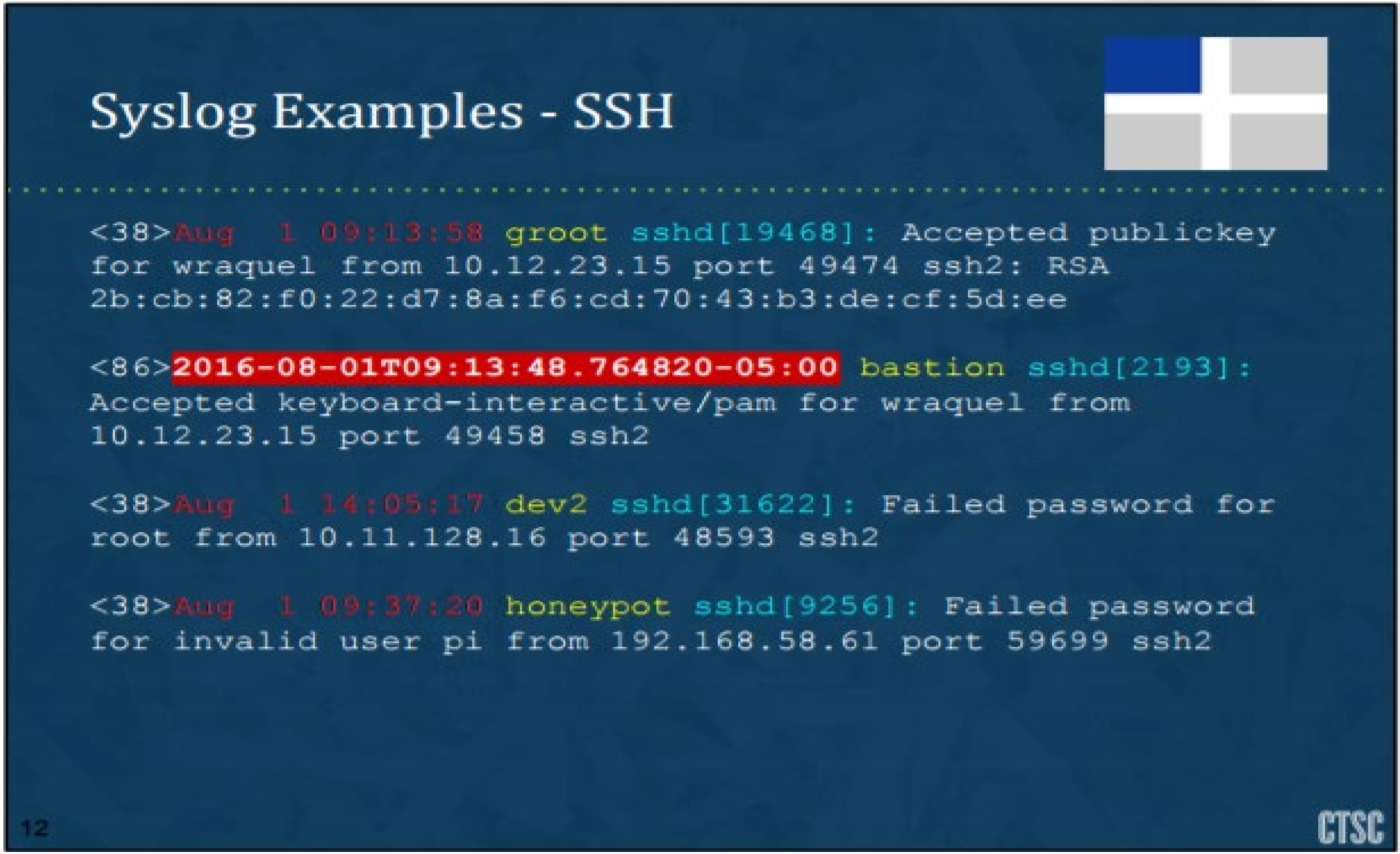
What does this mean?



```
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{☺Θu☺├f
0C1AFB94 B9 7B 04 80 34 0B D8 E2 FA EB 05 E8 E2 FF FF FF ╣{♦Ç4♂╪Γ·δ♣Φ Γ   
0C1AFBA4 E9 E1 03 00 00 5F 64 A1 30 00 00 00 8B 40 0C 8B Θß♥.._dí0...ï@.ï
0C1AFBB4 70 1C AD 8B 68 08 8B F7 6A 0F 59 E8 81 03 00 00 p∟¡ïh◘ï≈j☼YΦü♥..
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 .Φn☻..ïΦj☺YΦa♥..
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 Φ╨☻..ïΦj☺YΦB♥..Γ
0C1AFC04 F9 68 6C 33 32 00 68 73 68 65 6C 54 8B 46 0C E8 ·hl32.hshelTïF.Φ
0C1AFC14 B1 02 00 00 8B E8 6A 01 59 E8 23 03 00 00 E2 F9 ▒☻..ïΦj☺YΦ#♥..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@Φ^☻..â°.☼à⌂☺..
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$Φ=☻..â° ☼ä^☺.
0C1AFC94 00 89 46 60 6A 00 50 FF 56 28 89 46 64 8B 86 90 .ëF`j.P V(ëFdïåÉ
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
- 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

The six step analysis technique

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

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 training?

- Have them ask questions
- Let them feel comfortable not knowing everything
    - What are the facts?
    - What were some ways you found out about the facts?
    - 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?

RSAConference2020

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 = "2193976896017"
     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 = "2193976896017"
     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

RSA®Conference2020

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  000000702141E170 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  000000702141E170 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  000000702141E170 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
```

```
1070236831,0,3175466240,198.32.11.5,1,1500,3175436989,3175436989,0,0,130.74.208.0,169.232.72.0,198.32.11.4,
33,35,1373,4753,6,0,16,16,16,25656,52
1070236831,0,3175466240,198.32.11.5,3,1884,3175408565,3175433201,0,0,130.74.208.0,169.232.72.0,198.32.11.4,
33,35,1373,4753,6,0,24,16,16,25656,52
1070236831,0,3175466240,198.32.11.5,1,628,3175448463,3175448463,0,0,130.74.208.0,169.232.112.0,198.32.11.4,
33,35,1373,3855,6,0,24,16,16,25656,52
1070236831,0,3175466240,198.32.11.5,1,1500,3175442525,3175442525,0,0,130.74.208.0,169.232.112.0,198.32.11.
4,33,35,1373,3864,6,0,16,16,16,25656,52
1070236831,0,3175466240,198.32.11.5,1,1500,3175451974,3175451974,0,0,130.74.208.0,169.232.112.0,198.32.11.
4,33,35,1373,3831,6,0,16,16,16,25656,52
1070236831,0,3175466240,198.32.11.5,6,3768,3175398562,3175449061,0,0,130.74.208.0,169.232.112.0,198.32.11.
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
1070236836,0,3175471250,198.32.11.5,1,92,3175414202,3175414202,0,0,130.18.248.0,165.132.224.0,198.32.11.4,1
8,35,0,0,1,0,0,16,16,10546,4665
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
1070236836,0,3175471250,198.32.11.5,1,92,3175403033,3175403033,0,0,130.18.248.0,211.248.144.0,198.32.11.4,1
8,35,0,0,1,0,0,16,17,10546,9768
```

```
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)
```

RSAConference2020

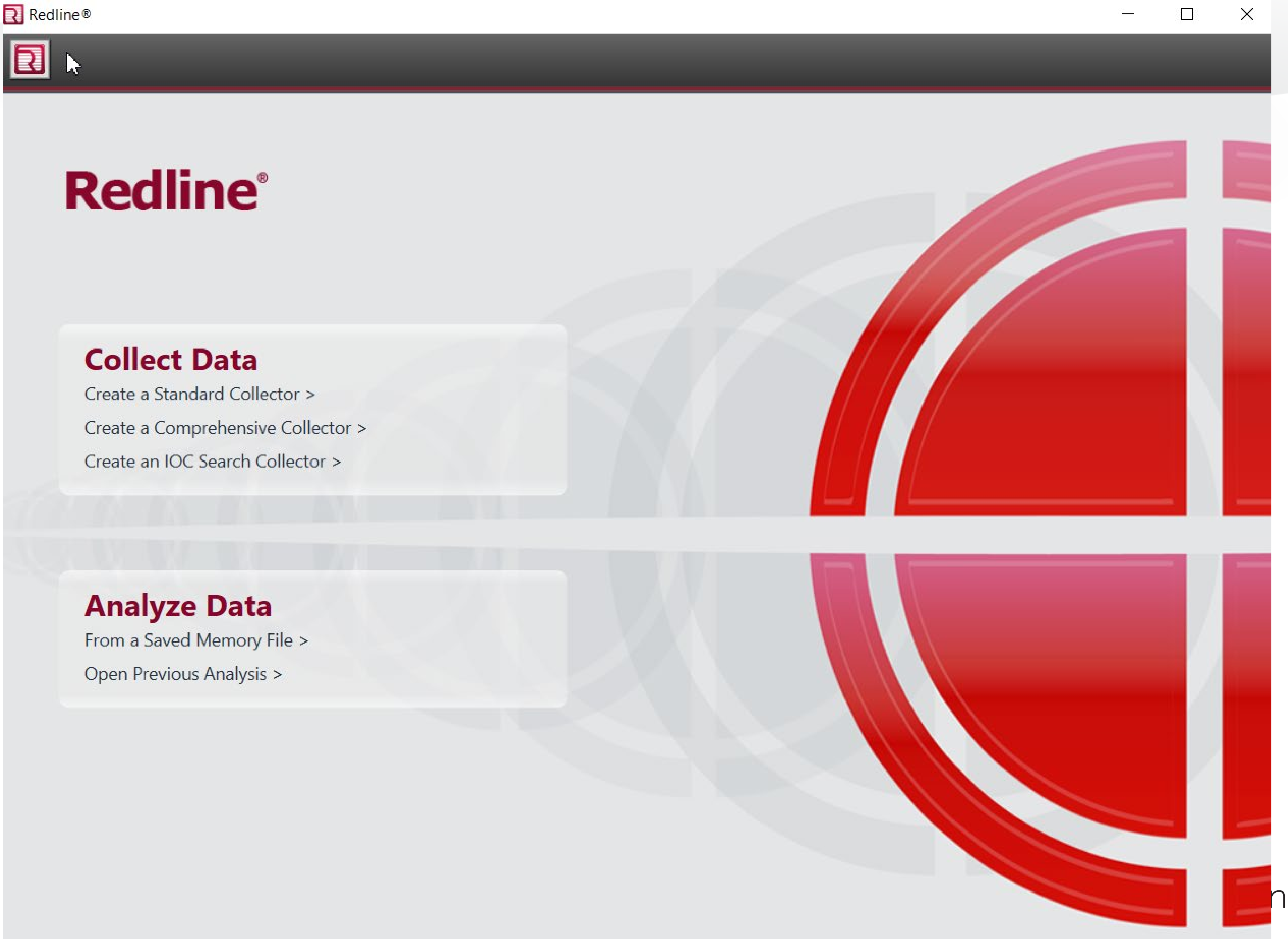
Your turn!

RSAConference2020

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
  - Redline
- If not grab these scripts:
  - Rift



Collect Data

Create a Standard Collector >

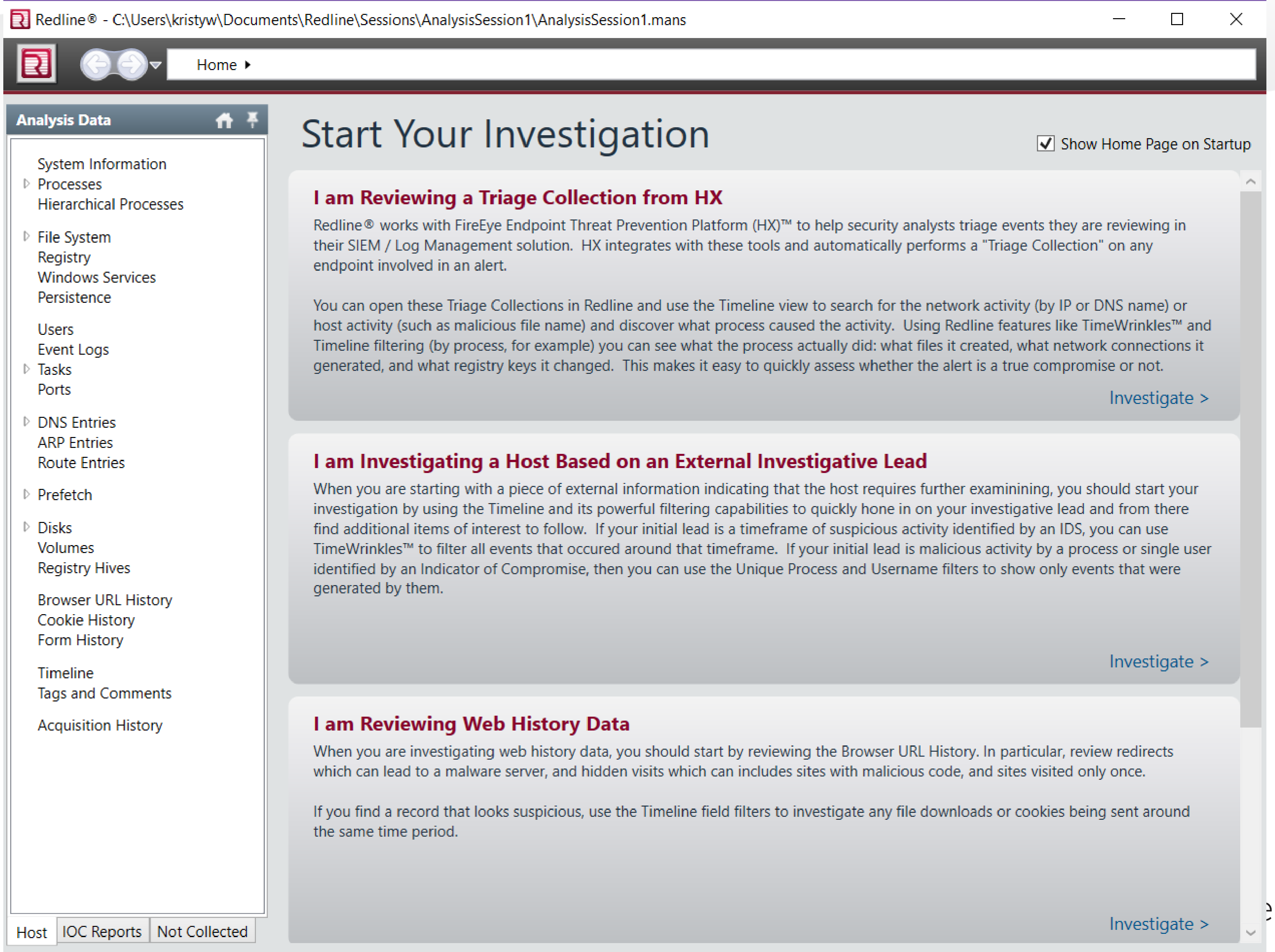
Create a Comprehensive Collector >

Create an IOC Search Collector >

Analyze Data

From a Saved Memory File >

Open Previous Analysis >



Start Your Investigation

☑ Show Home Page on Startup

I am Reviewing a Triage Collection from HX

Redline® works with FireEye Endpoint Threat Prevention Platform (HX)™ to help security analysts triage events they are reviewing in their SIEM / Log Management solution. HX integrates with these tools and automatically performs a "Triage Collection" on any endpoint involved in an alert.

You can open these Triage Collections in Redline and use the Timeline view to search for the network activity (by IP or DNS name) or host activity (such as malicious file name) and discover what process caused the activity. Using Redline features like TimeWrinkles™ and Timeline filtering (by process, for example) you can see what the process actually did: what files it created, what network connections it generated, and what registry keys it changed. This makes it easy to quickly assess whether the alert is a true compromise or not.

Investigate >

I am Investigating a Host Based on an External Investigative Lead

When you are starting with a piece of external information indicating that the host requires further examinining, you should start your investigation by using the Timeline and its powerful filtering capabilities to quickly hone in on your investigative lead and from there find additional items of interest to follow. If your initial lead is a timeframe of suspicious activity identified by an IDS, you can use TimeWrinkles™ to filter all events that occured around that timeframe. If your initial lead is malicious activity by a process or single user identified by an Indicator of Compromise, then you can use the Unique Process and Username filters to show only events that were generated by them.

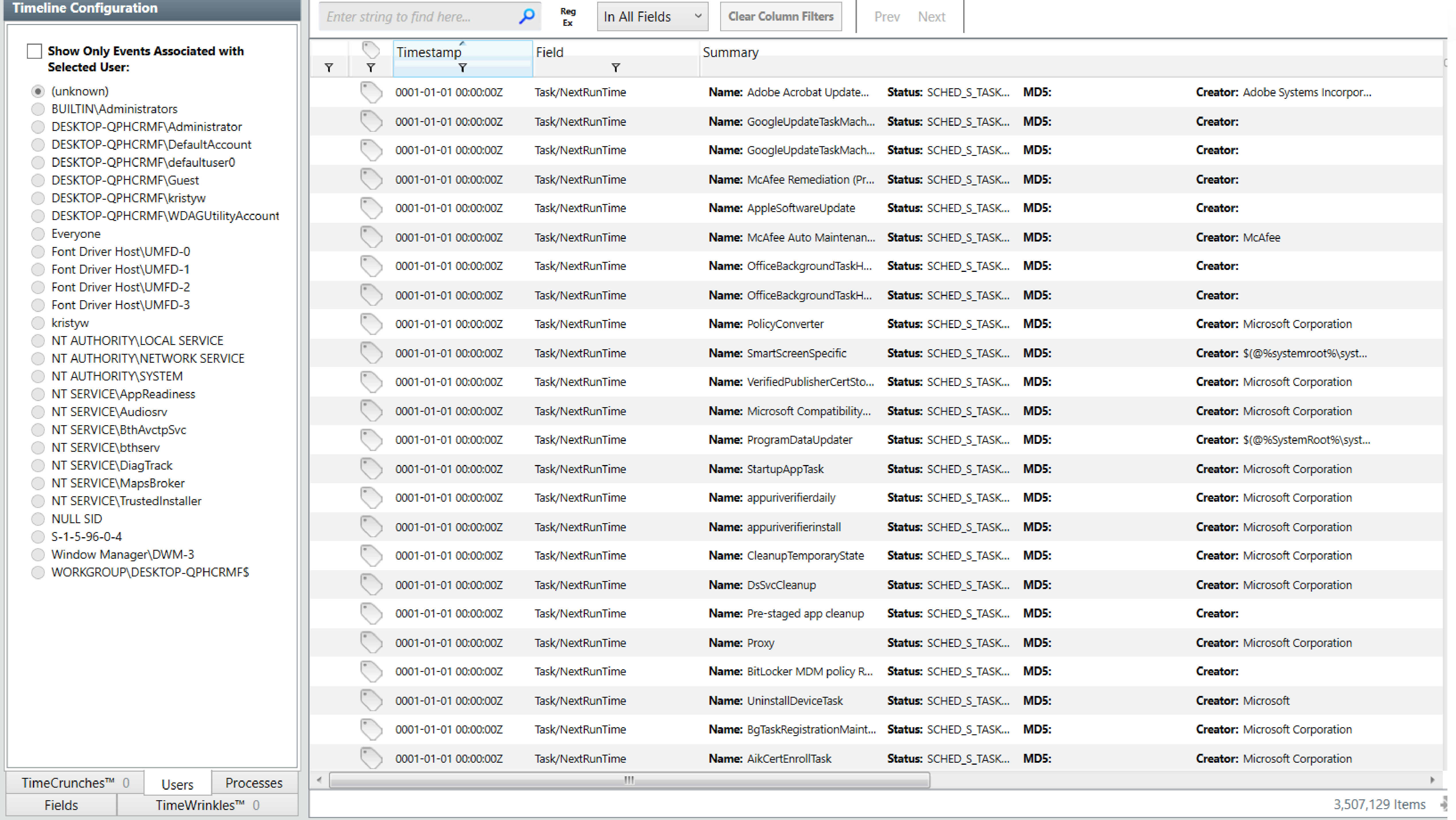
Investigate >

I am Reviewing Web History Data

When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can includes sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.

Investigate >



Timeline Configuration

□ **Show Only Events Associated with Selected User:**

- ● (unknown)
- ○ BUILTIN\Administrators
- ○ DESKTOP-QPHCRMF\Administrator
- ○ DESKTOP-QPHCRMF\DefaultAccount
- ○ DESKTOP-QPHCRMF\defaultuser0
- ○ DESKTOP-QPHCRMF\Guest
- ○ DESKTOP-QPHCRMF\kristyw
- ○ DESKTOP-QPHCRMF\WDAGUtilityAccount
- ○ Everyone
- ○ Font Driver Host\UMFD-0
- ○ Font Driver Host\UMFD-1
- ○ Font Driver Host\UMFD-2
- ○ Font Driver Host\UMFD-3
- ○ kristyw
- ○ NT AUTHORITY\LOCAL SERVICE
- ○ NT AUTHORITY\NETWORK SERVICE
- ○ NT AUTHORITY\SYSTEM
- ○ NT SERVICE\AppReadiness
- ○ NT SERVICE\Audiosrv
- ○ NT SERVICE\BthAvctpSvc
- ○ NT SERVICE\bthserv
- ○ NT SERVICE\DiagTrack
- ○ NT SERVICE\MapsBroker
- ○ NT SERVICE\TrustedInstaller
- ○ NULL SID
- ○ S-1-5-96-0-4
- ○ Window Manager\DWM-3
- ○ WORKGROUP\DESKTOP-QPHCRMF$

Timestamp	Field	Summary
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** Adobe Acrobat Update... **Status:** SCHED_S_TASK... **MD5:** **Creator:** Adobe Systems Incorpor...
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** GoogleUpdateTaskMach... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** GoogleUpdateTaskMach... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** McAfee Remediation (Pr... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** AppleSoftwareUpdate **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** McAfee Auto Maintenan... **Status:** SCHED_S_TASK... **MD5:** **Creator:** McAfee
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** OfficeBackgroundTaskH... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** OfficeBackgroundTaskH... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** PolicyConverter **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** SmartScreenSpecific **Status:** SCHED_S_TASK... **MD5:** **Creator:** $(@%systemroot%\syst...
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** VerifiedPublisherCertSto... **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** Microsoft Compatibility... **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** ProgramDataUpdater **Status:** SCHED_S_TASK... **MD5:** **Creator:** $(@%SystemRoot%\syst...
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** StartupAppTask **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** appuriverifierdaily **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** appuriverifierinstall **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** CleanupTemporaryState **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** DsSvcCleanup **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** Pre-staged app cleanup **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** Proxy **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** BitLocker MDM policy R... **Status:** SCHED_S_TASK... **MD5:** **Creator:**
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** UninstallDeviceTask **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** BgTaskRegistrationMaint... **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation
0001-01-01 00:00:00Z	Task/NextRunTime	**Name:** AikCertEnrollTask **Status:** SCHED_S_TASK... **MD5:** **Creator:** Microsoft Corporation

3,507,129 Items

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
```

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
```

RSA Conference2020

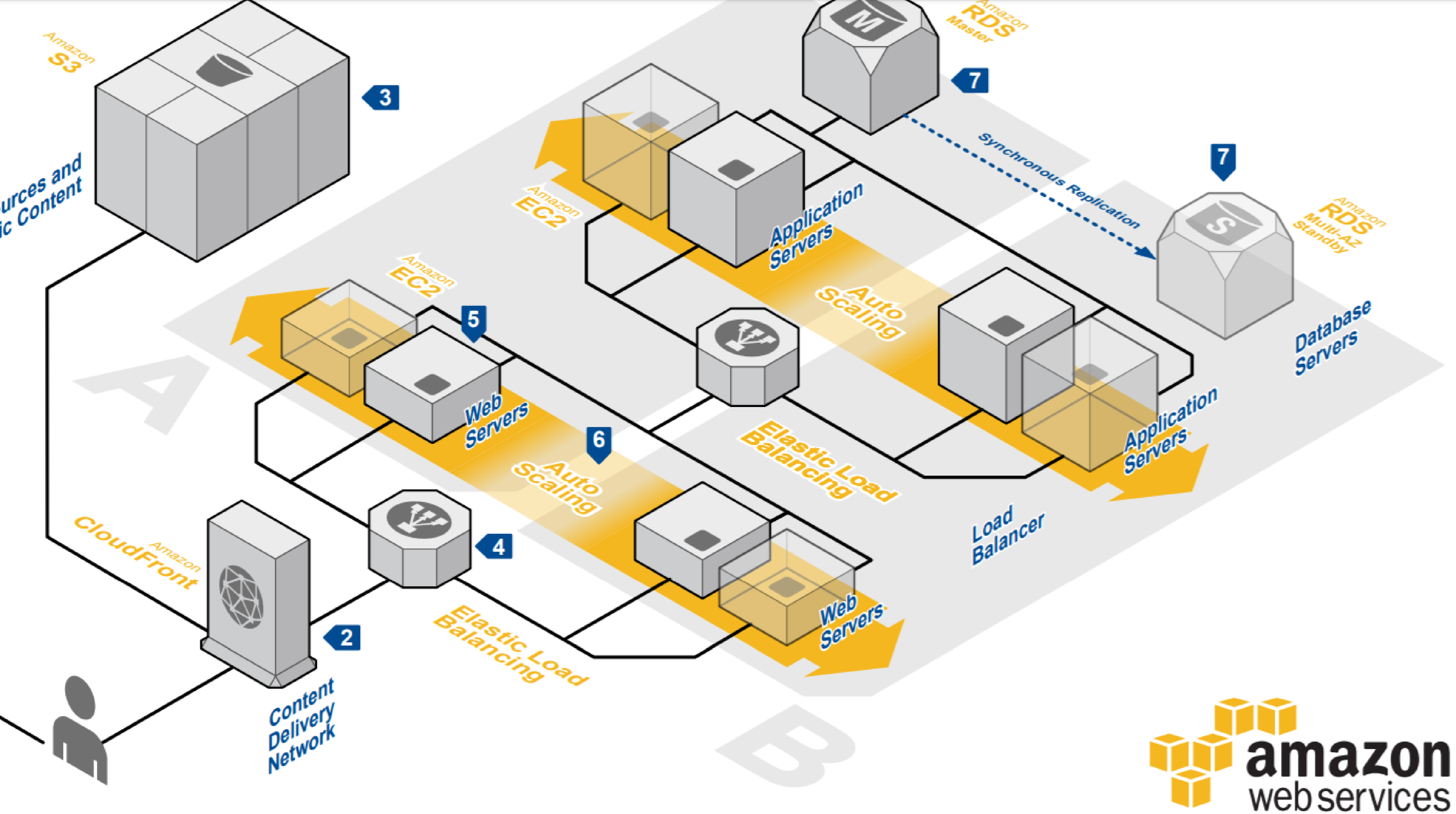
Guess WHAT?

Yep, it’s your turn

To the clouds!

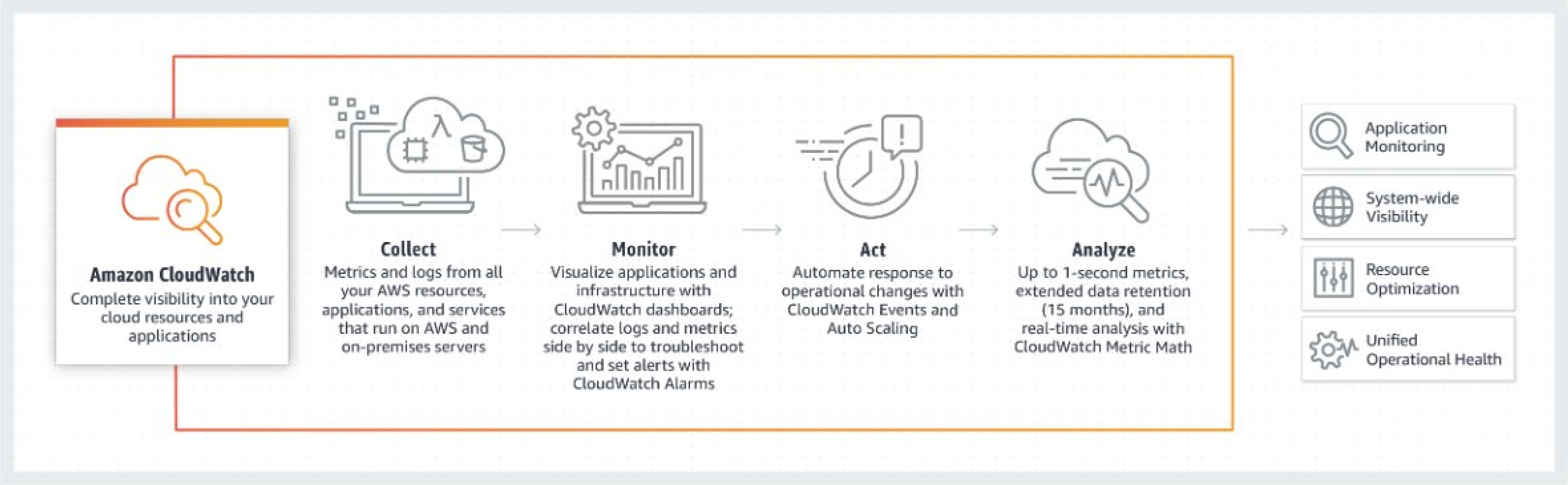
Cloud analysis

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



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

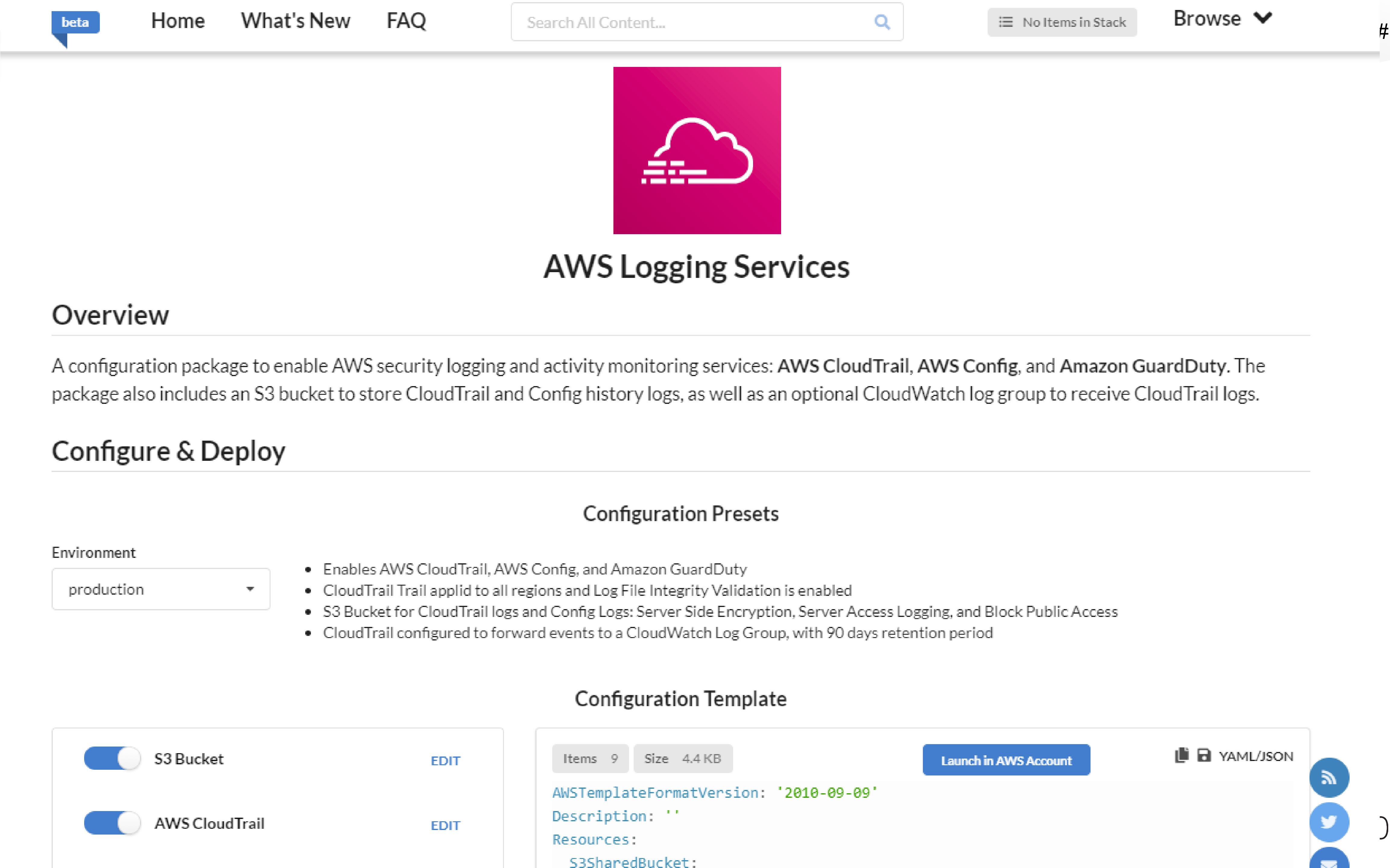
Act
Automate response to operational changes with CloudWatch Events and Auto Scaling

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

```
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"
        }
    }]}}
}]}
```

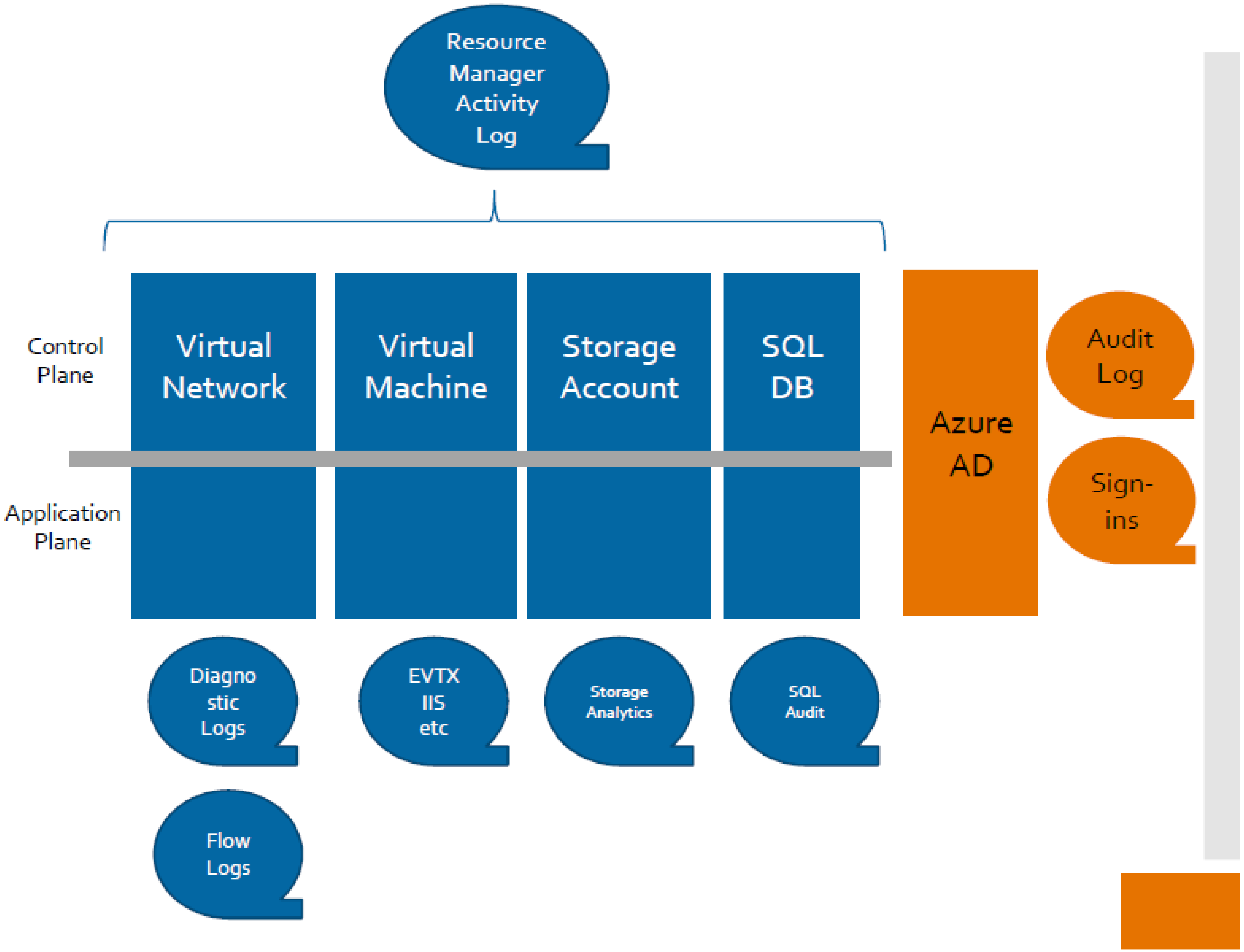
Don’t forget about Azure

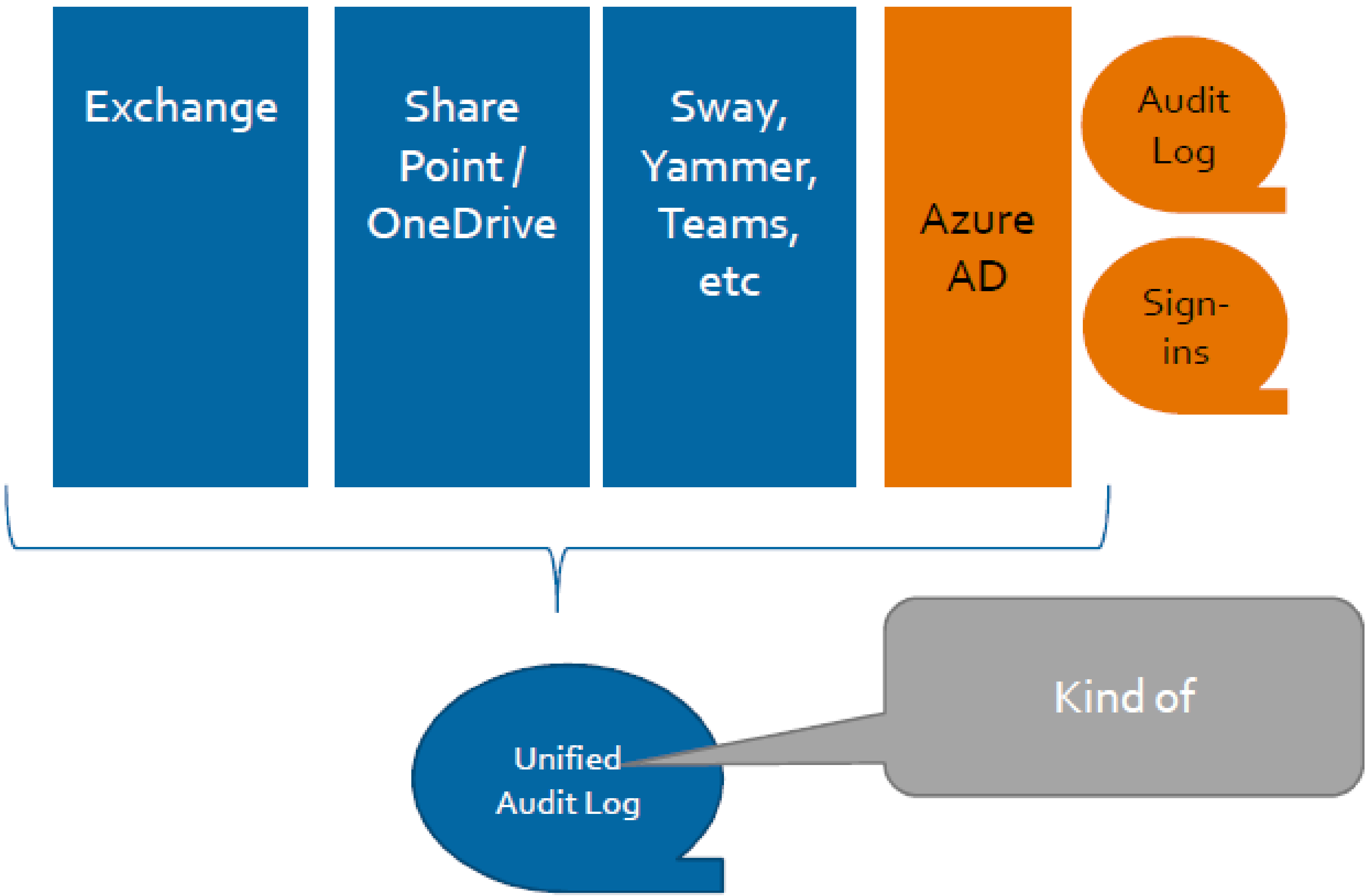
- https://docs.microsoft.com/en-us/azure/security/azure-log-audit
- Very similar in JSON format
- Otherwise tells you different things
- Use Security Center to help
- https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-schema
- https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-overview

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

Azure Logging





Exchange

Share Point / OneDrive

Sway, Yammer, Teams, etc

Azure AD

Audit Log

Sign-ins

Unified Audit Log

Kind of

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

```
{
  "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"
        }
```

RSAConference2020

LAST ROUND!

Wrapping up (you made it!!)

- Definitely use tools to help you with the volume 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…

So what’s the plan?

- 30-day plan
  - Take this presentation, use it for your security operations analysts
  - Plan out more exercises, each more advanced, and schedule them
- 60-day plan
  - Implement the analysis training as part of onboarding
  - Start screening non-traditional cyber analysts who can be taught
- 90-day plan
  - Make this a regular opportunity to learn going forward
  - Recruit senior analysts to start creating and training on their own content

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

RSAConference2020

THANK YOU!!

kmwestphal@cox.net

Keep the conversation going!