RSAConference2019
San Francisco | March 4–8 | Moscone Center


SESSION ID: HUM-R03

# Don’t Hand Me That! The Art of Incident Analysis

**Kristy Westphal**

Vice President, CSIRT
A Large Financial Institution

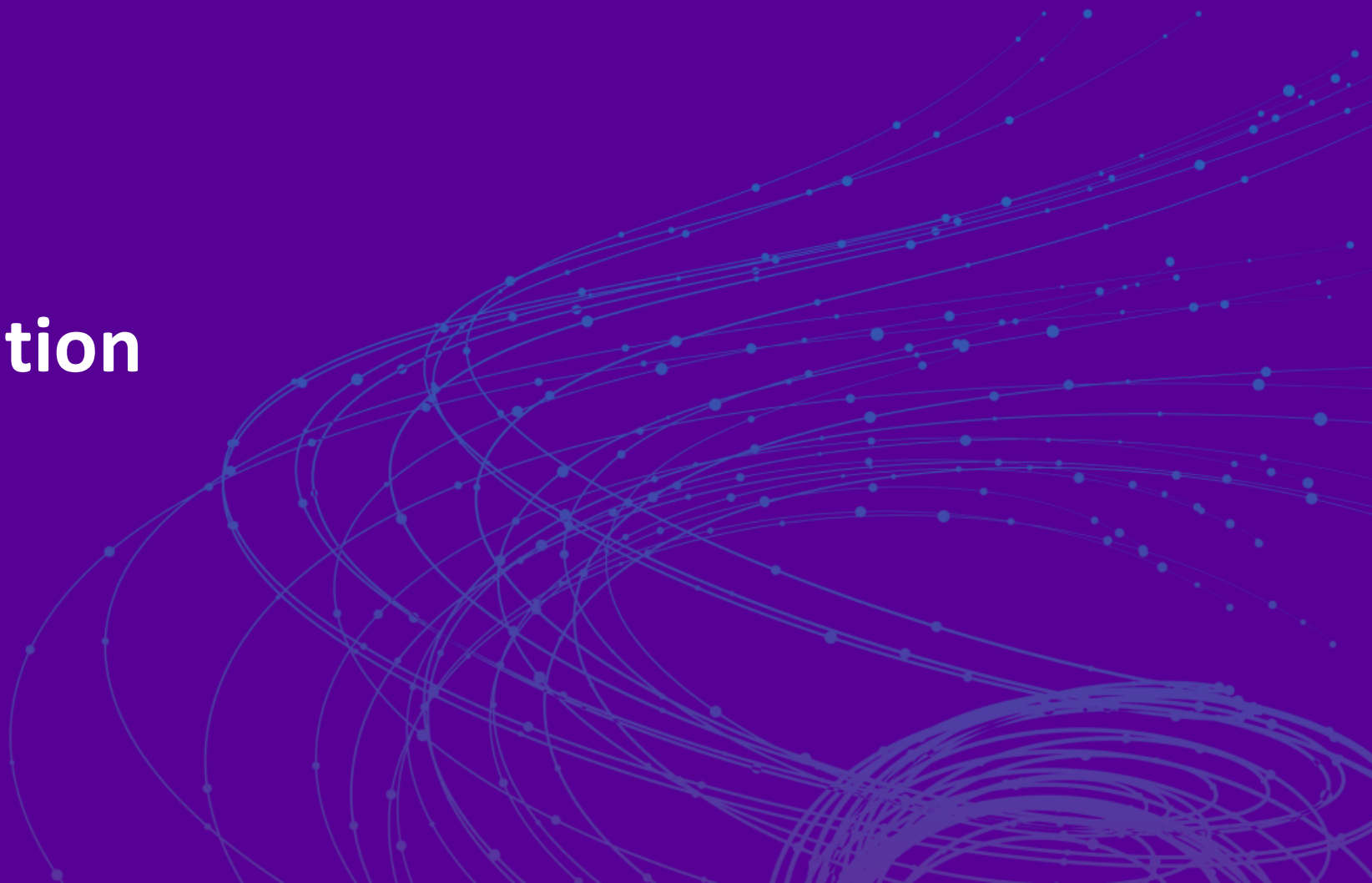
*The views and opinions in this presentation are my own and do not represent the views of MUFG.*

# Agenda

- My inspiration for this talk
- The problem:  Is your SOC doing effective incident analysis?
- All about the three ‘C’s
- What can we do?
  - Right now and longer term

RSAConference2019

# Some inspiration

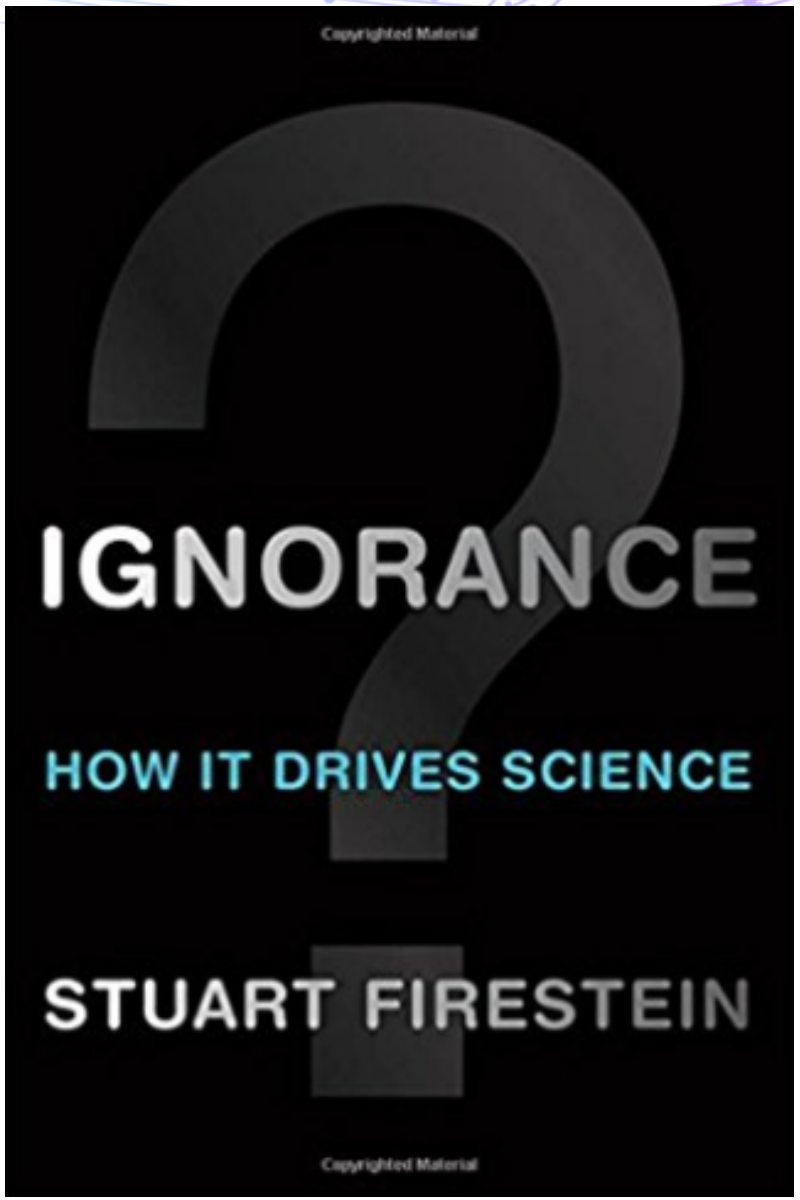


# Why am I here?


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

# So I heard about this book

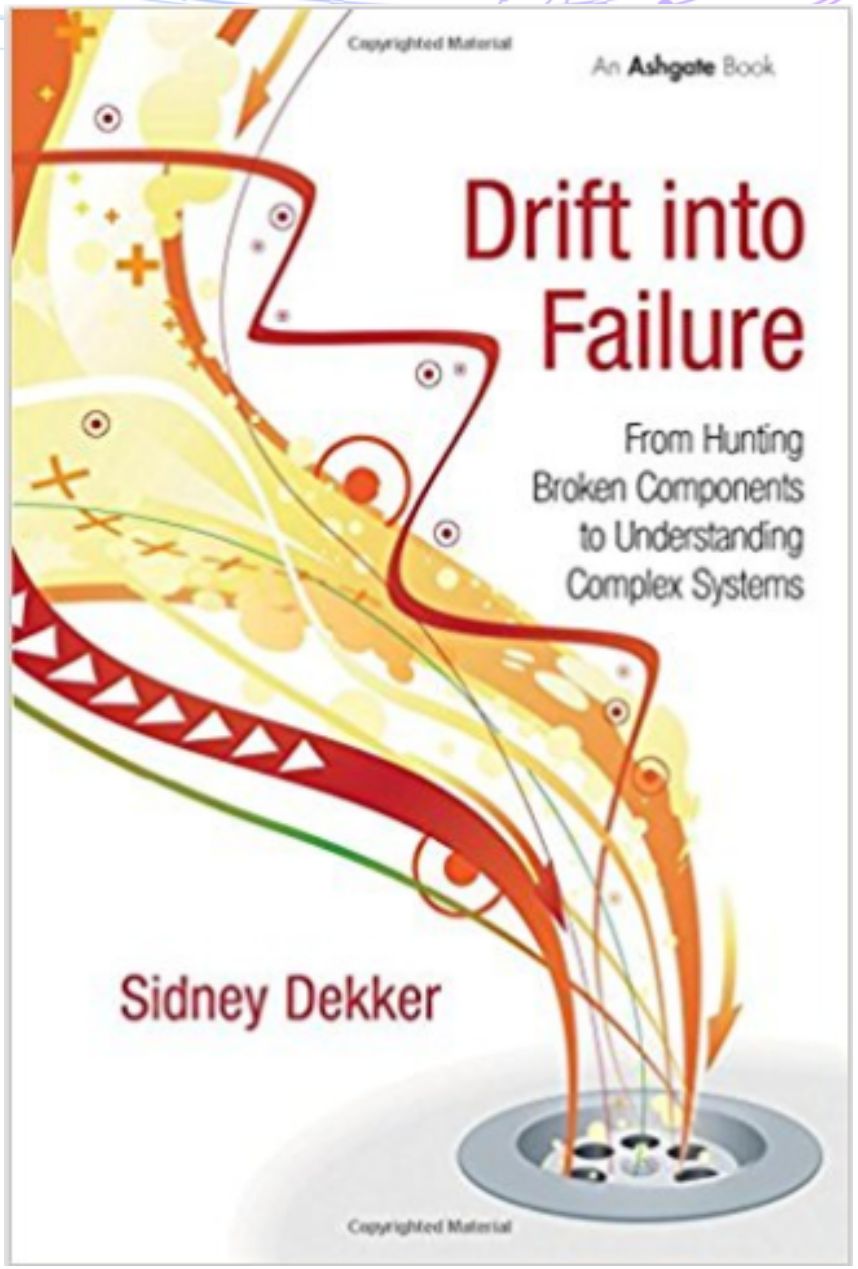
- It’s not about Information Security
- Let’s take a closer look…



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

# And then there is this book…

- "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."



# Analysis is Like Solving a Mystery… A good example of solving a mystery:

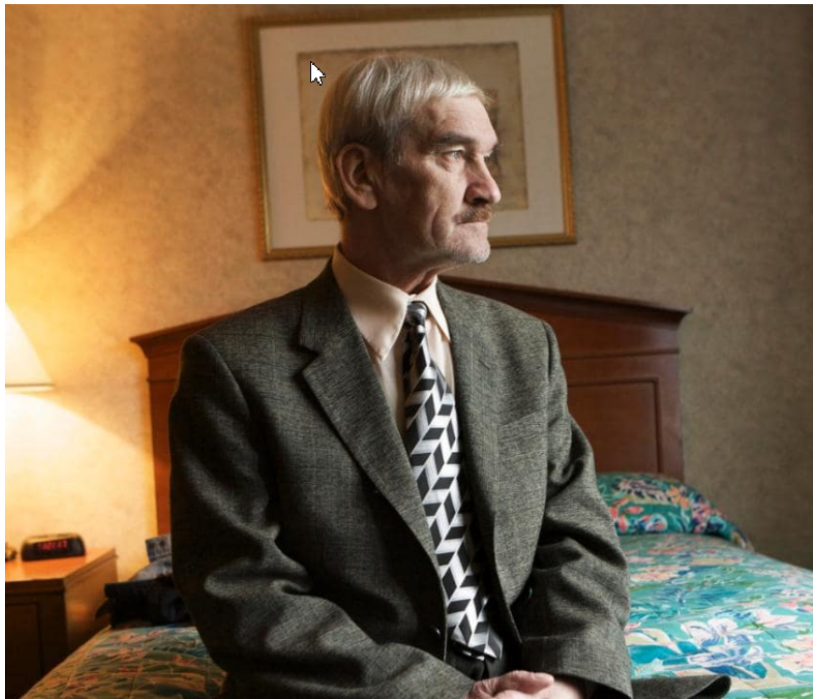
"I was trained as a physicist, and in physics we're always trying to figure out how the world works," he explained. "But you have to ask the right questions. You have to investigate things. You always have to be willing to question your assumptions. DDoS defense is very similar. You can't just look at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

RSAConference2019

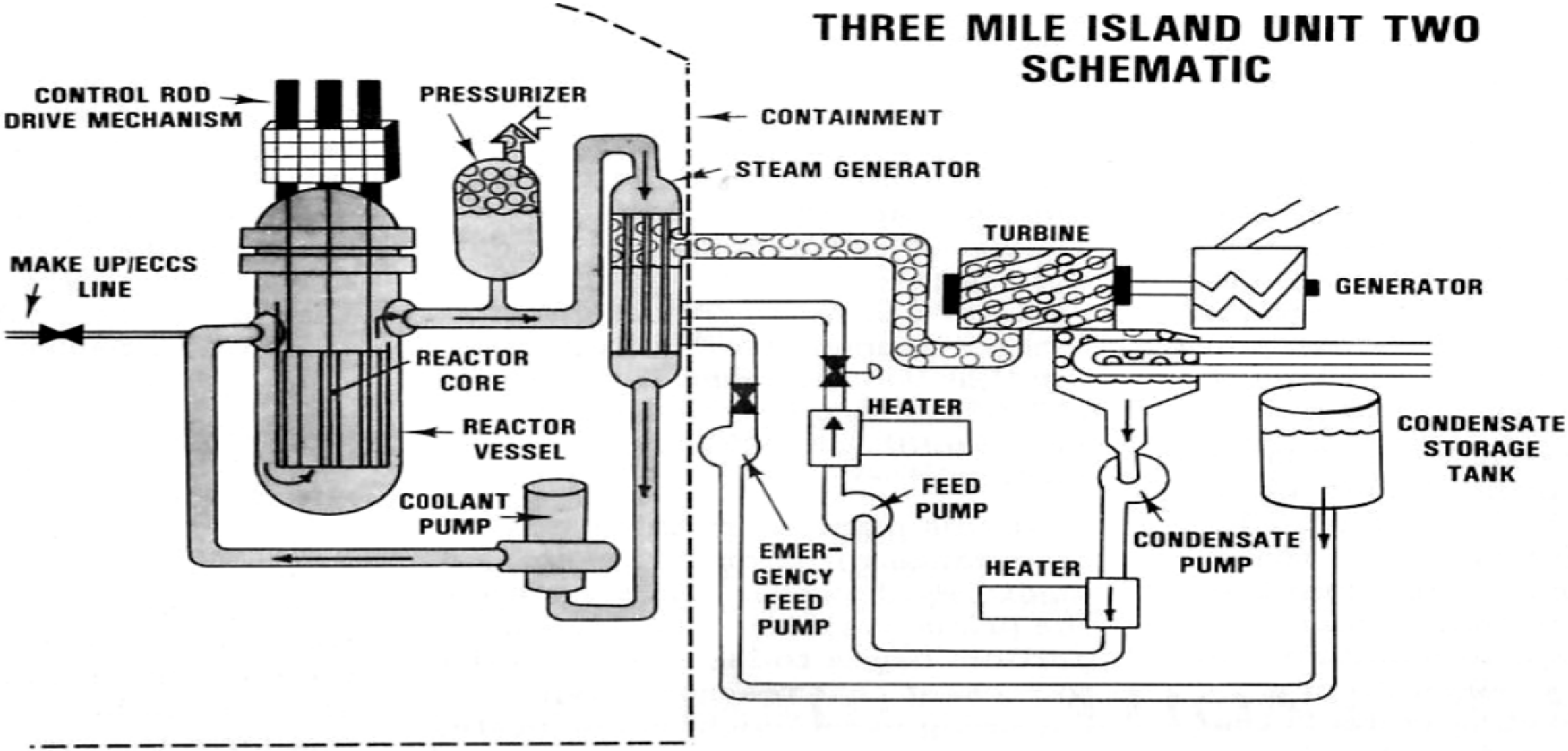
# Incident analysis is also a world of uncertainty

# How to save the world

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

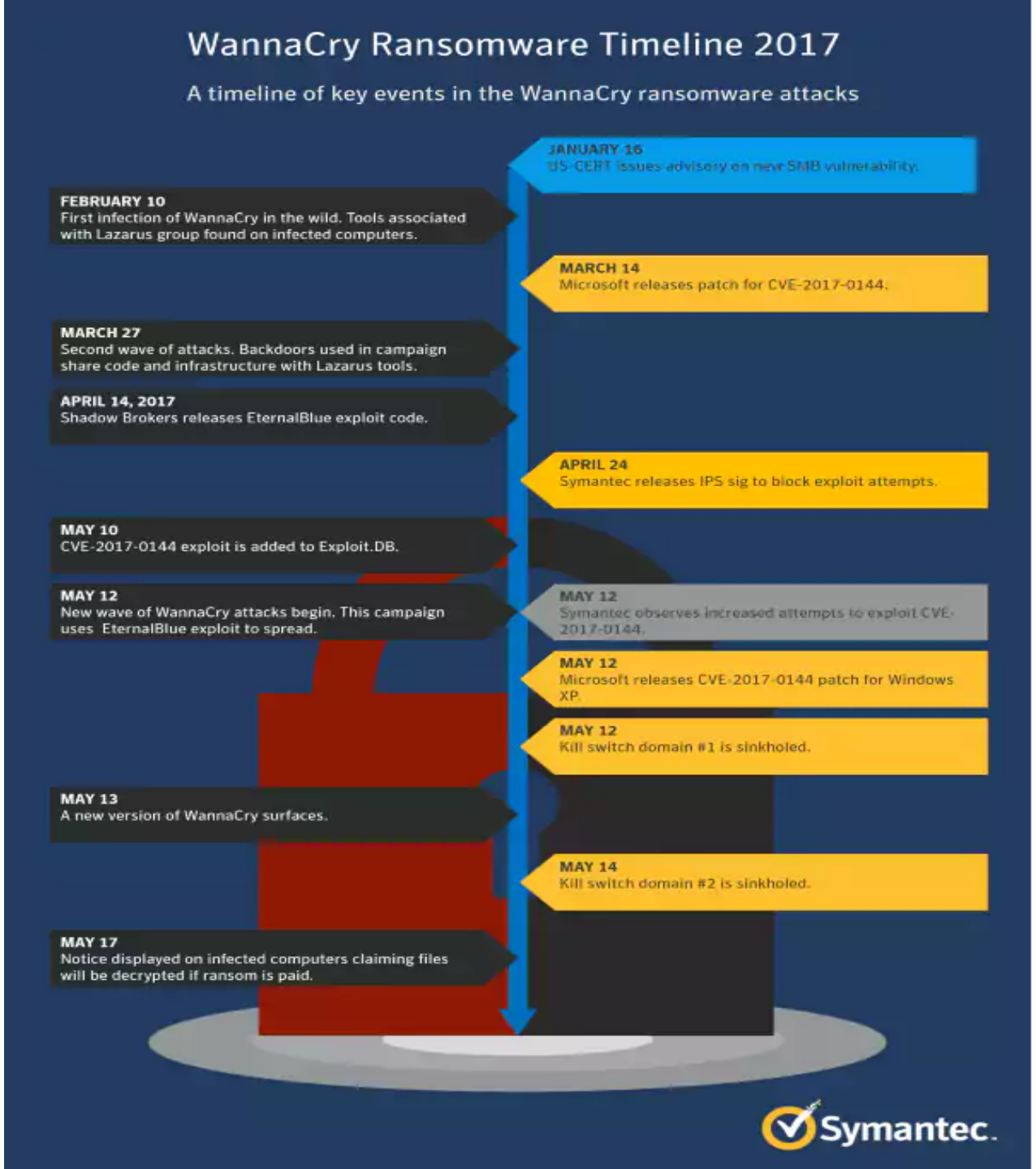


# What's broken here?




Drawing from Metropolitan Edison Co. "A Report to the Met-Ed Community" May 30, 1979

# 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.
Symantec.

RSAConference2019

# Is your SOC doing effective analysis?

# Polling Question #1

- How would you currently rate your incident handling analysis quality?
- https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3868

# 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 ë↓[KÉ3╔ÉÇ{☺ëu☺├f
0C1AFB94 B9 7B 04 80 34 0B D8 E2 FA EB 05 E8 E2 FF FF FF ╣{♦Ç4♂╪┌·§♣ë┌
0C1AFBA4 E9 E1 03 00 00 5F 64 A1 30 00 00 00 8B 40 0C 8B ΘÞ♥..._dí0...ï@.ï
0C1AFBB4 70 1C AD 8B 68 08 8B F7 6A 0F 59 E8 81 03 00 00 pL¡ïh◘ï≈j☼Yèü♥..
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 .èn☻..ïèj☺Yèa♥..
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 èпL☻..ïèj☺YèB♥..Γ
0C1AFC04 F9 68 6C 33 32 00 68 73 68 65 6C 54 8B 46 0C E8 ·hl32.hshelTïF.è
0C1AFC14 B1 02 00 00 8B E8 6A 01 59 E8 23 03 00 00 E2 F9 ▒☻..ïèj☺Yè#♥..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@è^☻..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$è=☻..â° ☼ä^☺.
0C1AFC94 00 89 46 60 6A 00 50 FF 56 28 89 46 64 8B 86 90 .ëF`j.PÿV(ëFd
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
```

# 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*

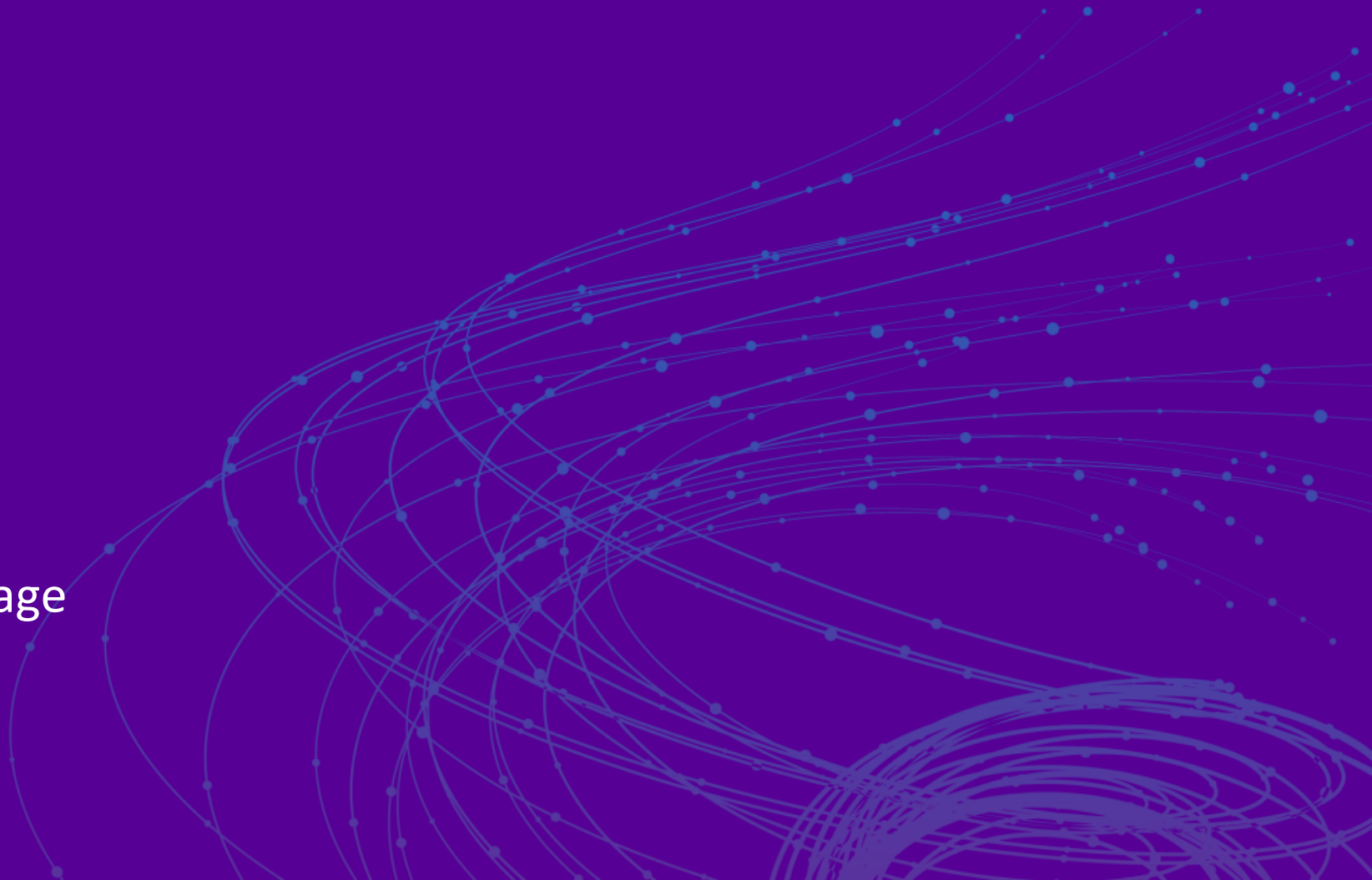
# Think about a task you are given- how do you analyze it?

- 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

RSAConference2019

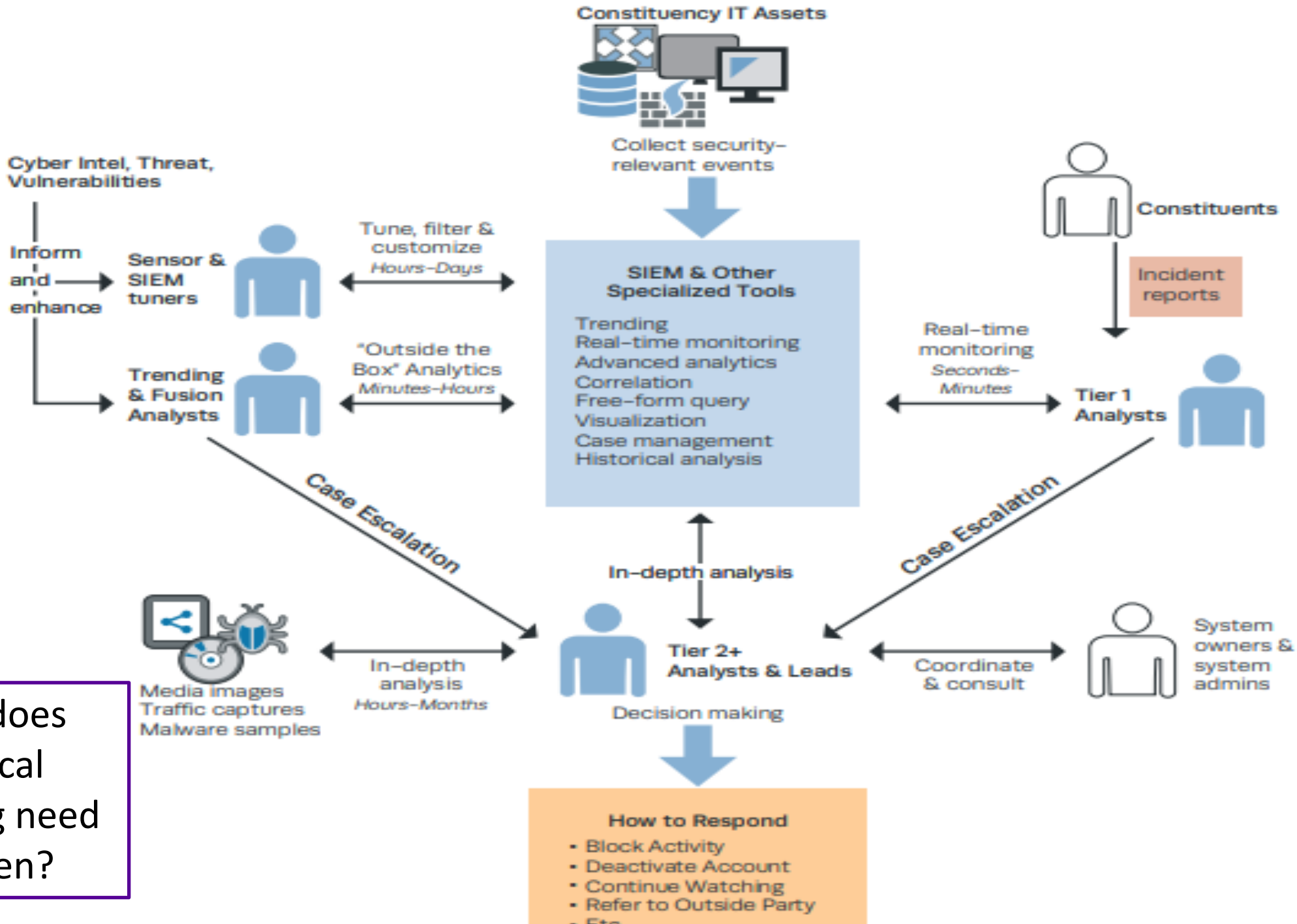
# The three Cs

Critical Thinking
Communication
Control of the Message



# *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




Where does the Critical Thinking need to happen?

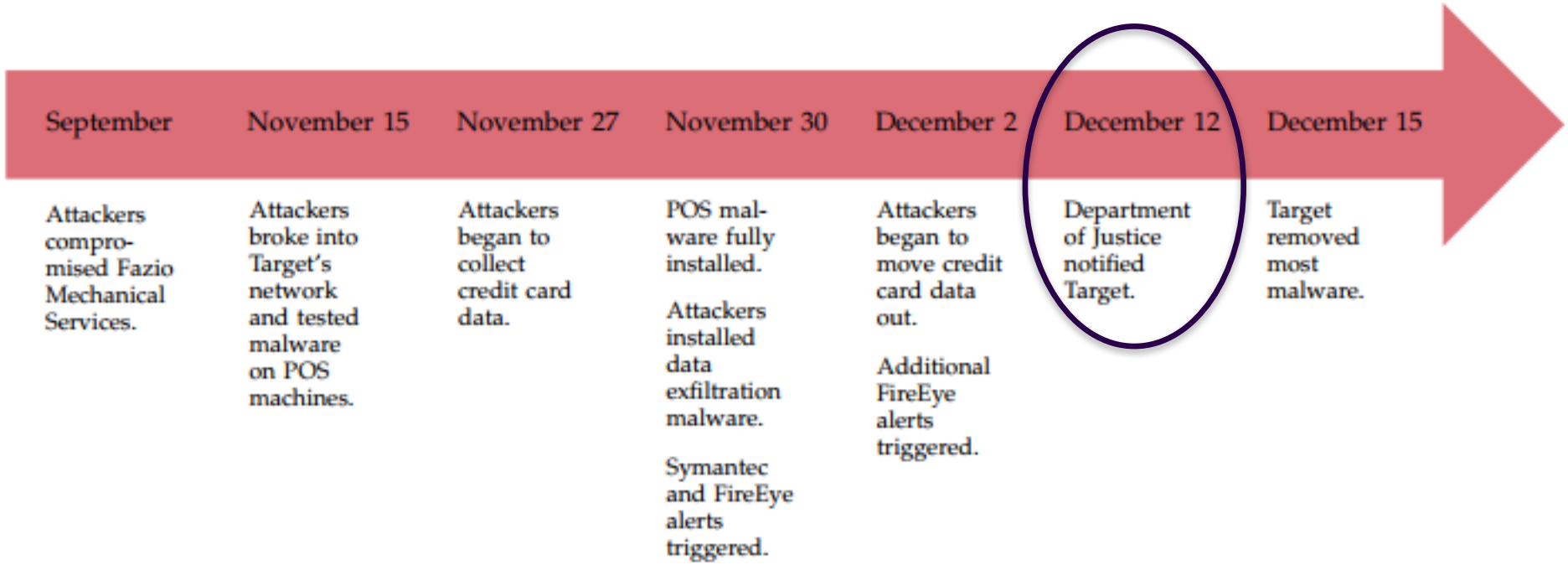
# Critical thinking applies to InfoSec analysts, too

*"Being a scientist requires having faith in uncertainty, finding pleasure in mystery, and learning to cultivate doubt."* -Firestein

# 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

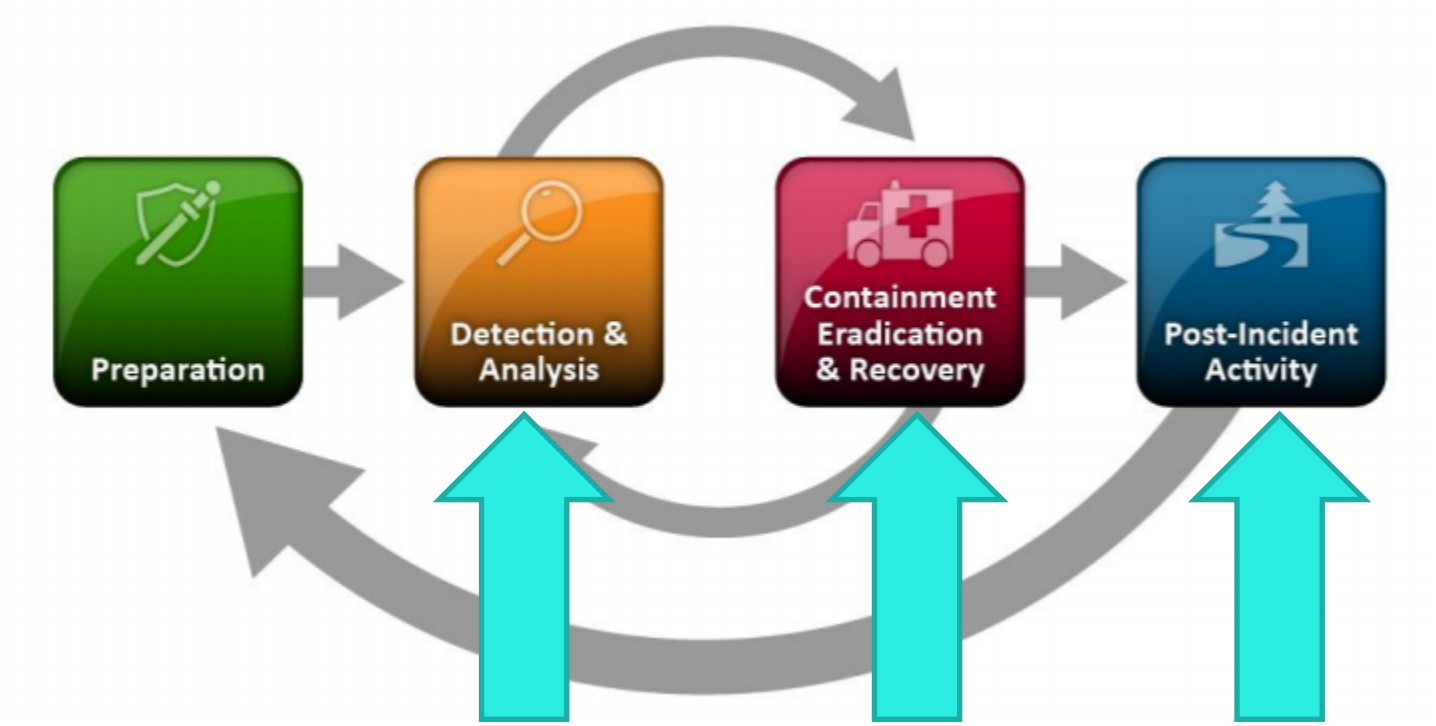
RSAConference2019

# Communication, communication, communication

# Polling question #2

- How would you rate your communication process for incidents?
- https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3869

# At what point does Visual Incident Response help?

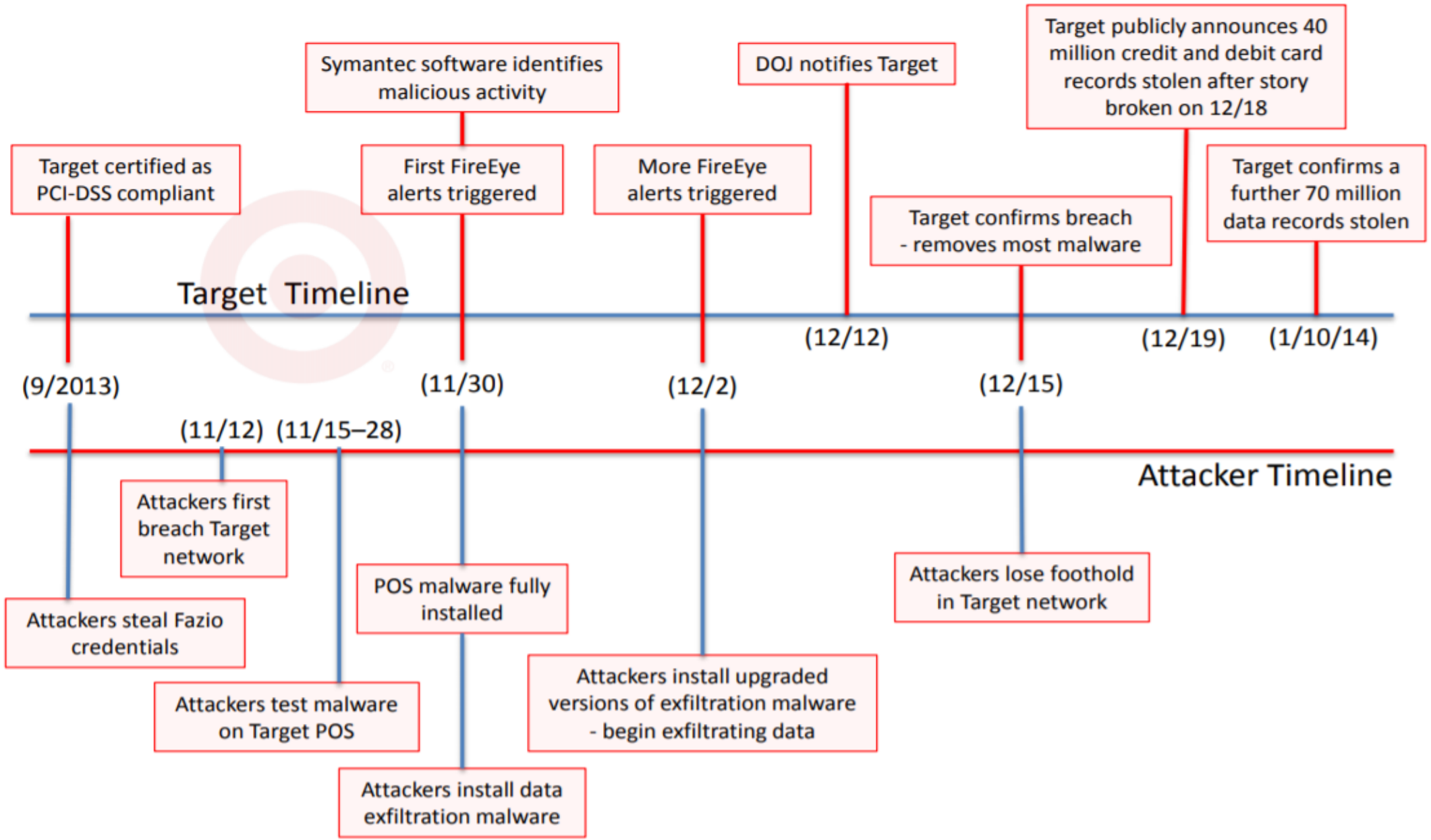



Here for sure

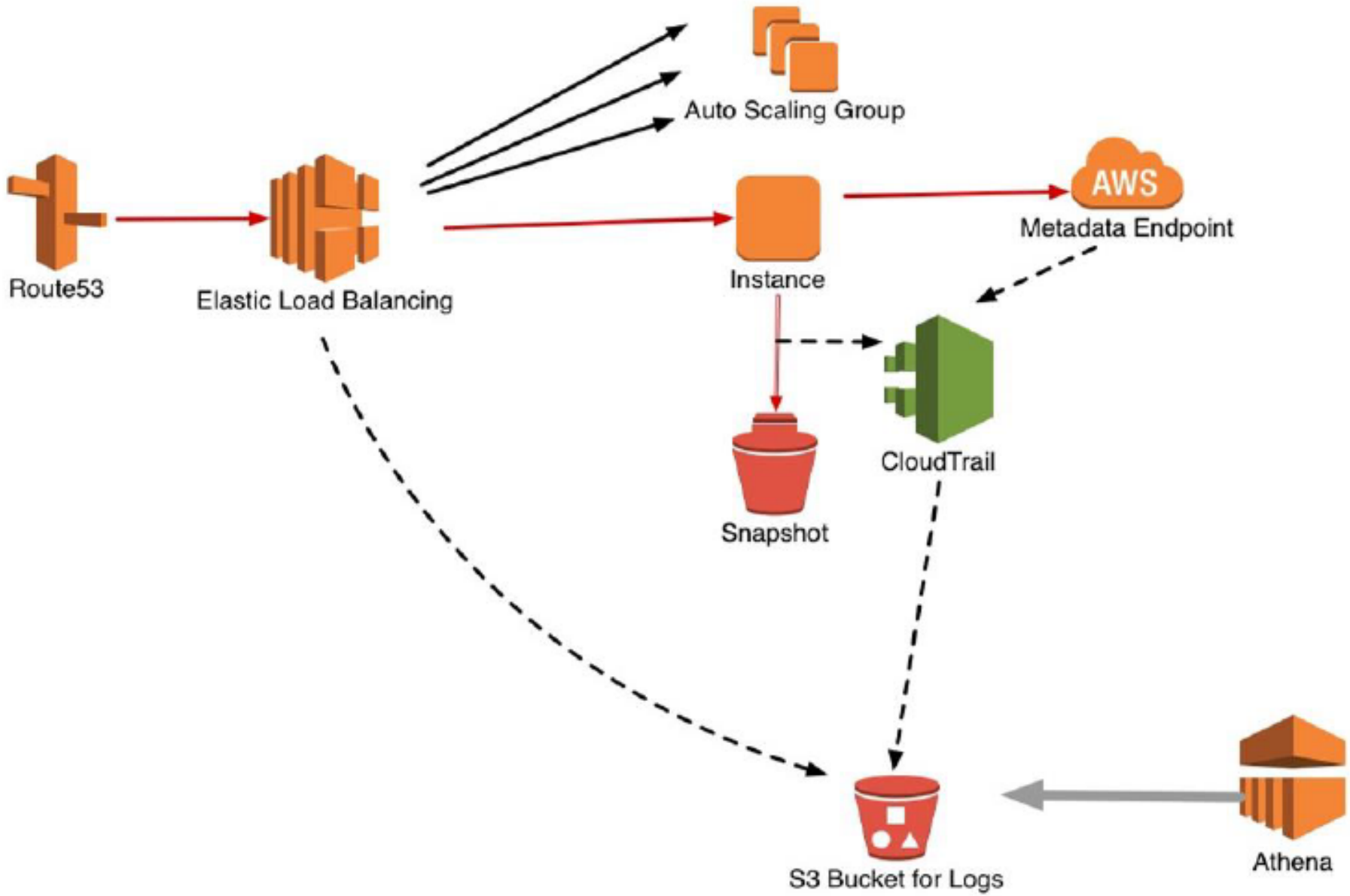
Sometimes here too

For sure here

# A Timeline of the Target Data Breach



# CLOUD TRAIL

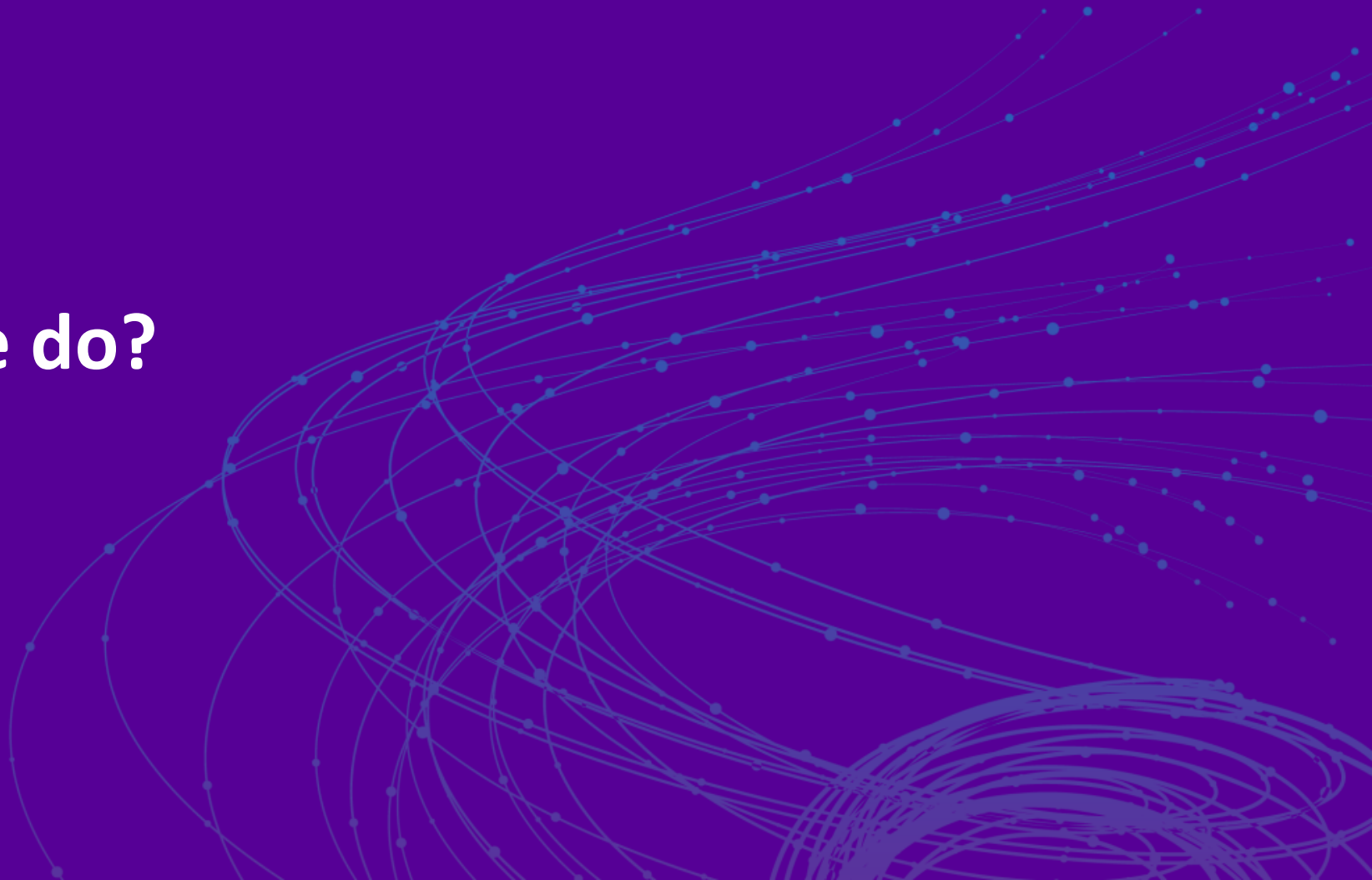

Auto Scaling Group
Route53
Elastic Load Balancing
Instance
AWS
Metadata Endpoint
Snapshot
CloudTrail
S3 Bucket for Logs
Athena

# Controlling the message

- What's going on
- Impacts of the event
- Actions
- Communication considerations

RSAConference2019

# What can we do?



# So what should you focus on?

*“The lesson here is to recognize the value of the observable and to leave the unmeasurable stuff for later.” -Firestein*

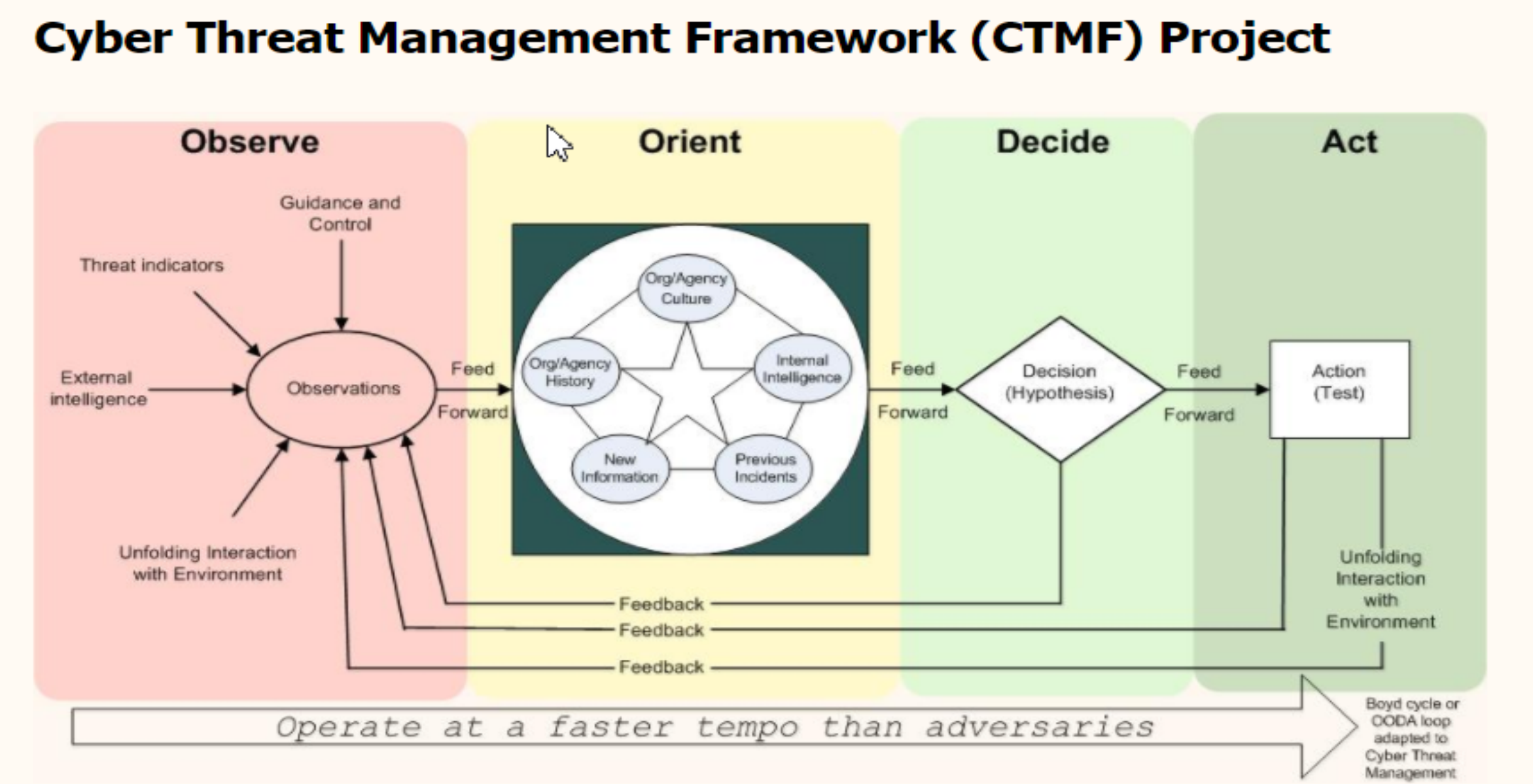
# OK, so what do you do now?

- Start asking questions (as soon as you get back)
  - Always assume (yes, you have permission) that you don't know everything
- Take a look at your incident handling SOPs (longer term)

# Then maybe apply a little DREAD (longer term)

- We need to think a little differently
- Having a framework for your questions can be helpful
- So use as you see fit

# Another way to go



*“In an honest search for knowledge you quite often have to abide by ignorance for an indefinite period.”*

*-Erwin Schrodinger*

# In summary

- Need more analysis
- Careful automation
- Practice, practice, practice!
- There are a lot of resources listed in this presentation (use them!)
- Ignorance drives science…so why not InfoSec as well?

RSAConference2019

# Thank you!
# Keep the conversation going

kmwestphal@cox.net