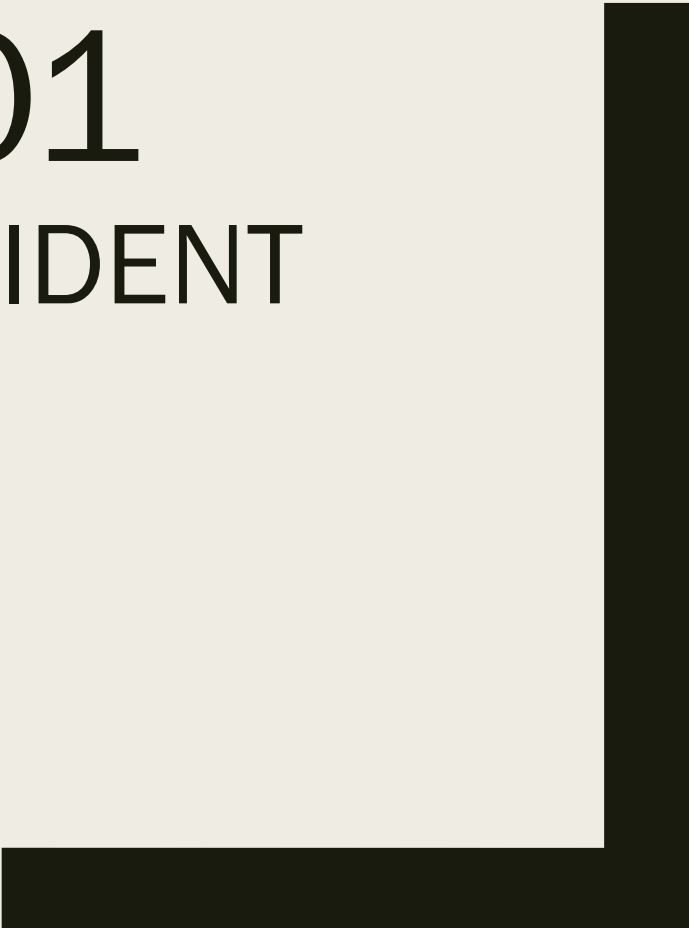


ANALYSIS 101

FOR HACKERS AND INCIDENT RESPONDERS

Kristy Westphal
SANS Cyber Defense Forum
October 9, 2020



Agenda

- Ignorance and Importance of Analysis
- What is Analysis?
- A Little Process
- Critical Thinking
- Resources
- **Disclaimer:** 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!



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.

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...

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

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*

Cyber Kill Chain®

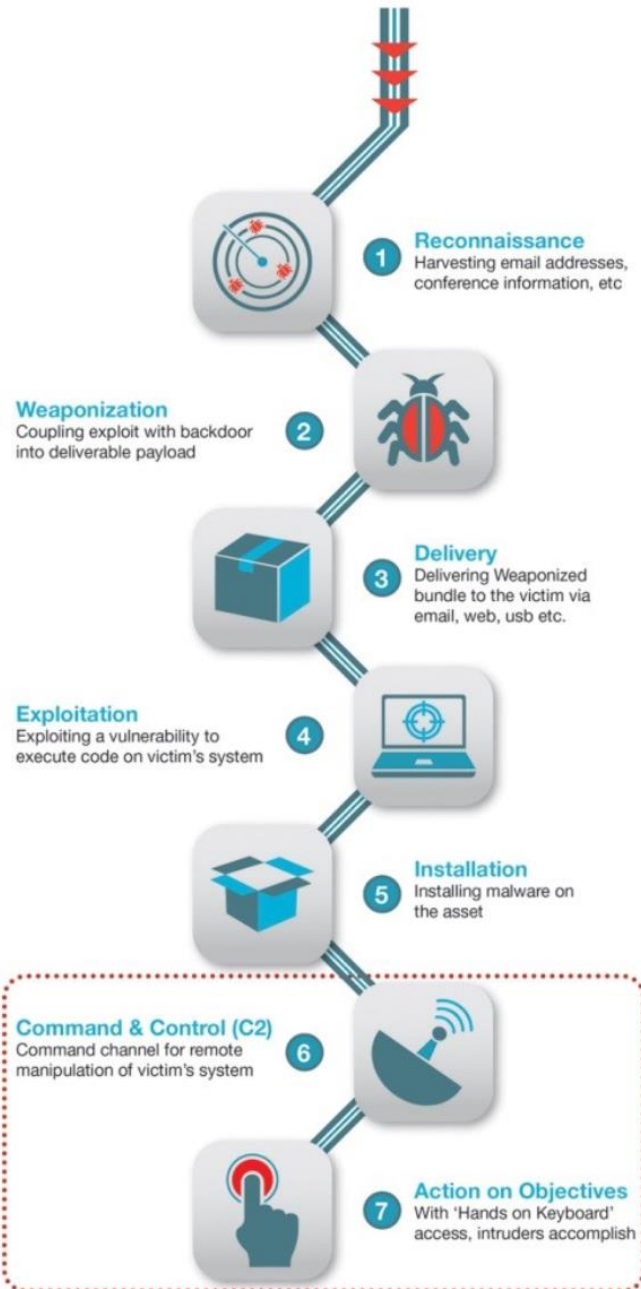


Timeline

Hours to Months

Seconds

Months



Based on Lockheed Martin's Cyber Kill Chain

Preparation

Intrusion

Active Breach

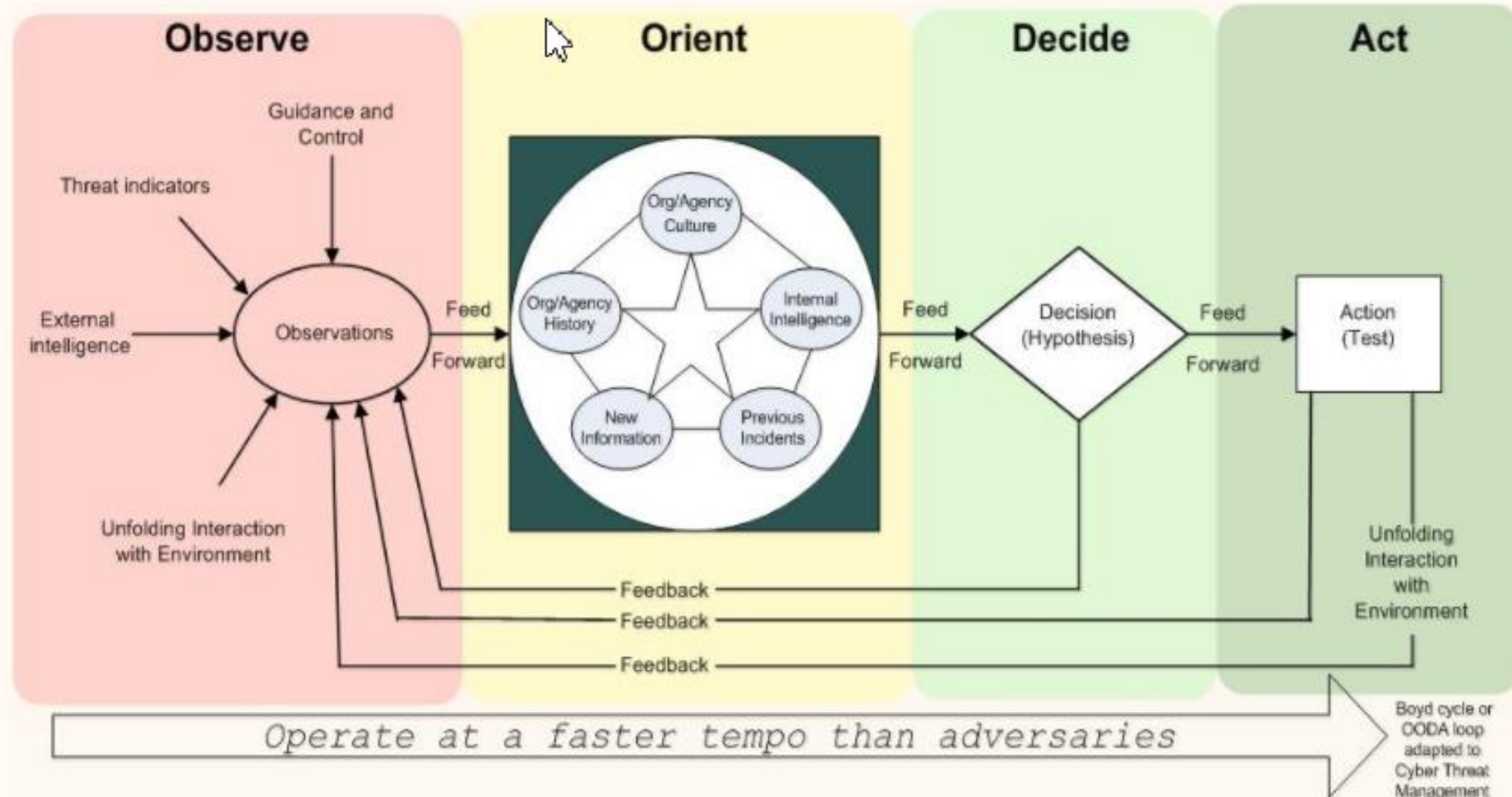
https://socprime.com/wp-content/uploads/2016/03/blackenergy-p3_2.jpg

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

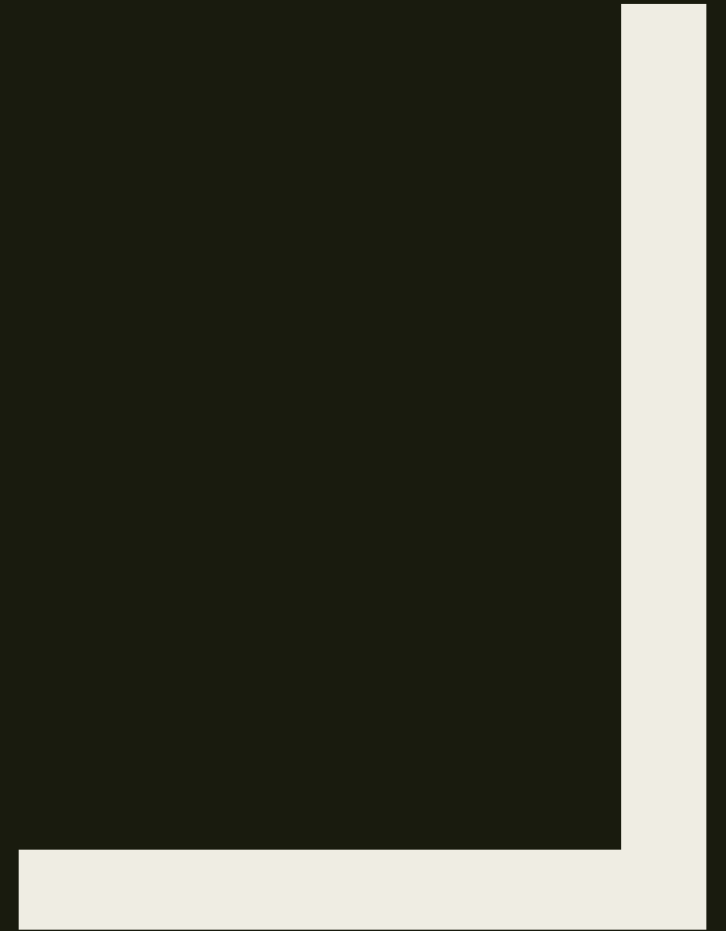
Cyber Threat Management Framework (CTMF) Project



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.”
- “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.”

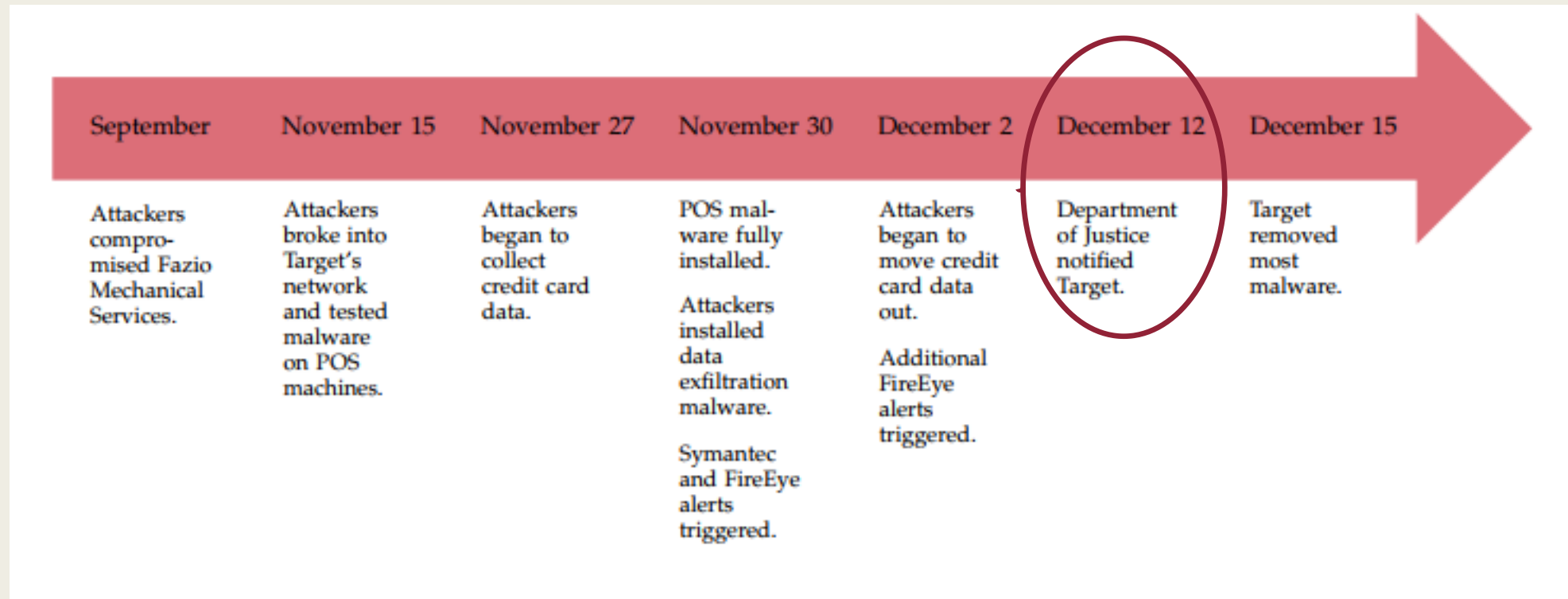
The six step analysis technique

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!



But how do I start?

- By asking questions
- Always assume (yes, you have permission) that you don't know everything
 - What are the facts?
 - What 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?

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



CYBER DEFENSE
FORUM & TRAINING
—
Live Online

THANK
YOU!!

Keep the conversation going!

kmwestphal@cox.net