Discovering U.S. Government Threat Hunting Processes and Improvements

William “Trey” Maxam

PURDUE UNIVERSITY

Elmore Family School of Electrical and Computer Engineering

Outline

- Introduction
- Background
- Research Questions
- Methodology
- Results
- Discussion and Future Work
- Questions

ELMORE FAMILY SCHOOL OF ECE

Introduction

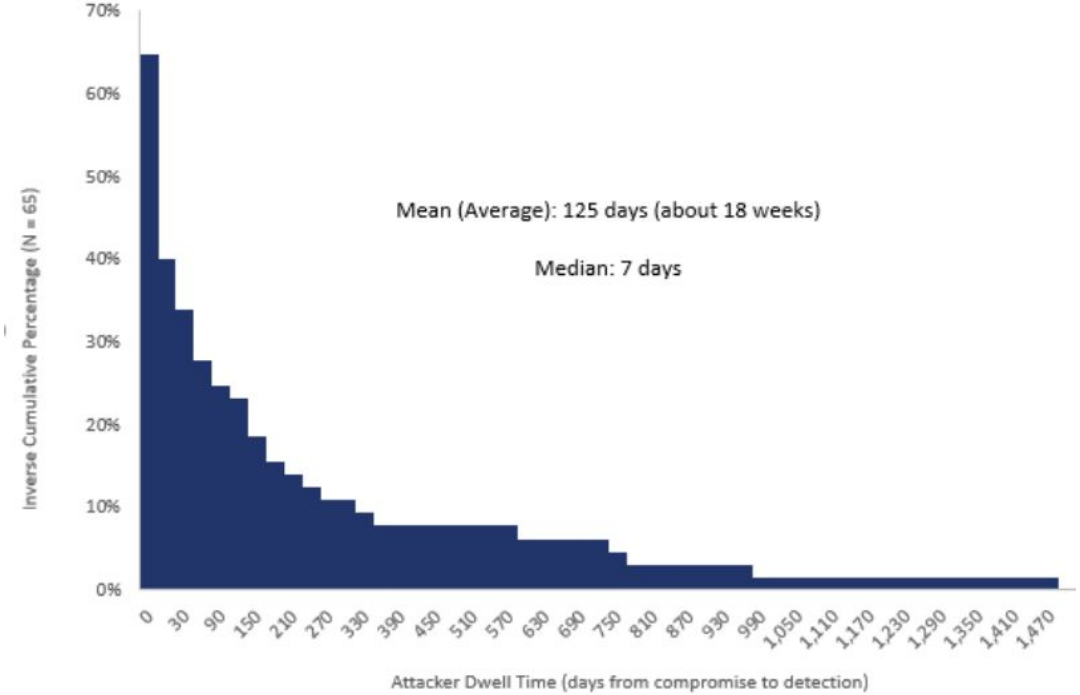
Timeline of an attack

ELMORE FAMILY SCHOOL OF ECE

Timeline of an attack

ELMORE FAMILY SCHOOL OF ECE

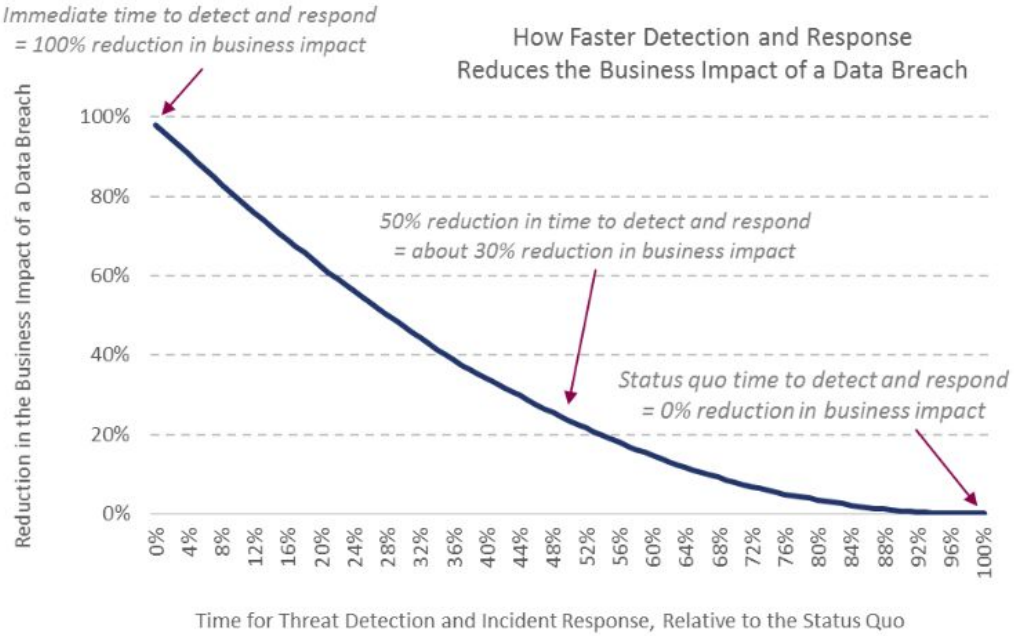
Distribution of Dwell Times



Source: D. E. Brink, “Quantifying the Value of Time in Cyber-Threat Detection and Response,” en, Aberdeen Group, Tech. Rep. 15218, Jan. 2017.

ELMORE FAMILY SCHOOL OF ECE

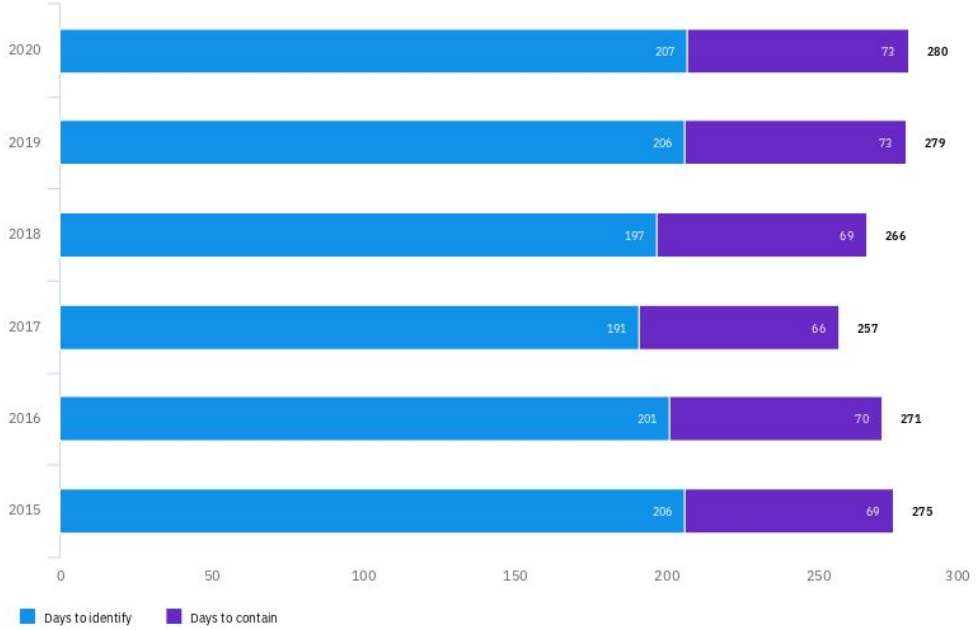
Less Dwell Time = Lower Cost of Intrusion



Source: D. E. Brink, “Quantifying the Value of Time in Cyber-Threat Detection and Response,” en, Aberdeen Group, Tech. Rep. 15218, Jan. 2017.

ELMORE FAMILY SCHOOL OF ECE

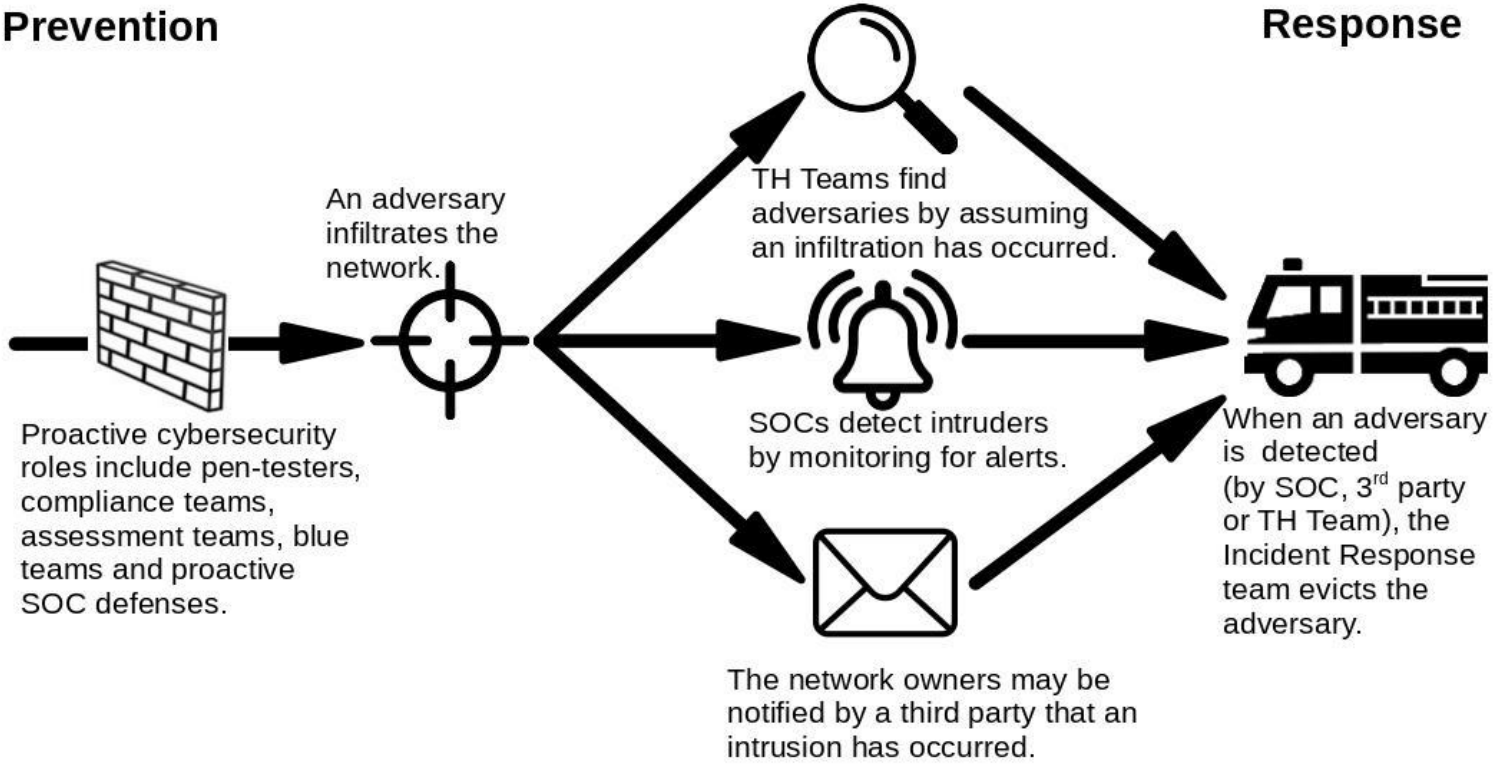
Time to Identify Data Breaches Remains Constant



Source: “Cost of a Data Breach Report 2020,” en, IBM Security, Tech. Rep., Jul. 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf .

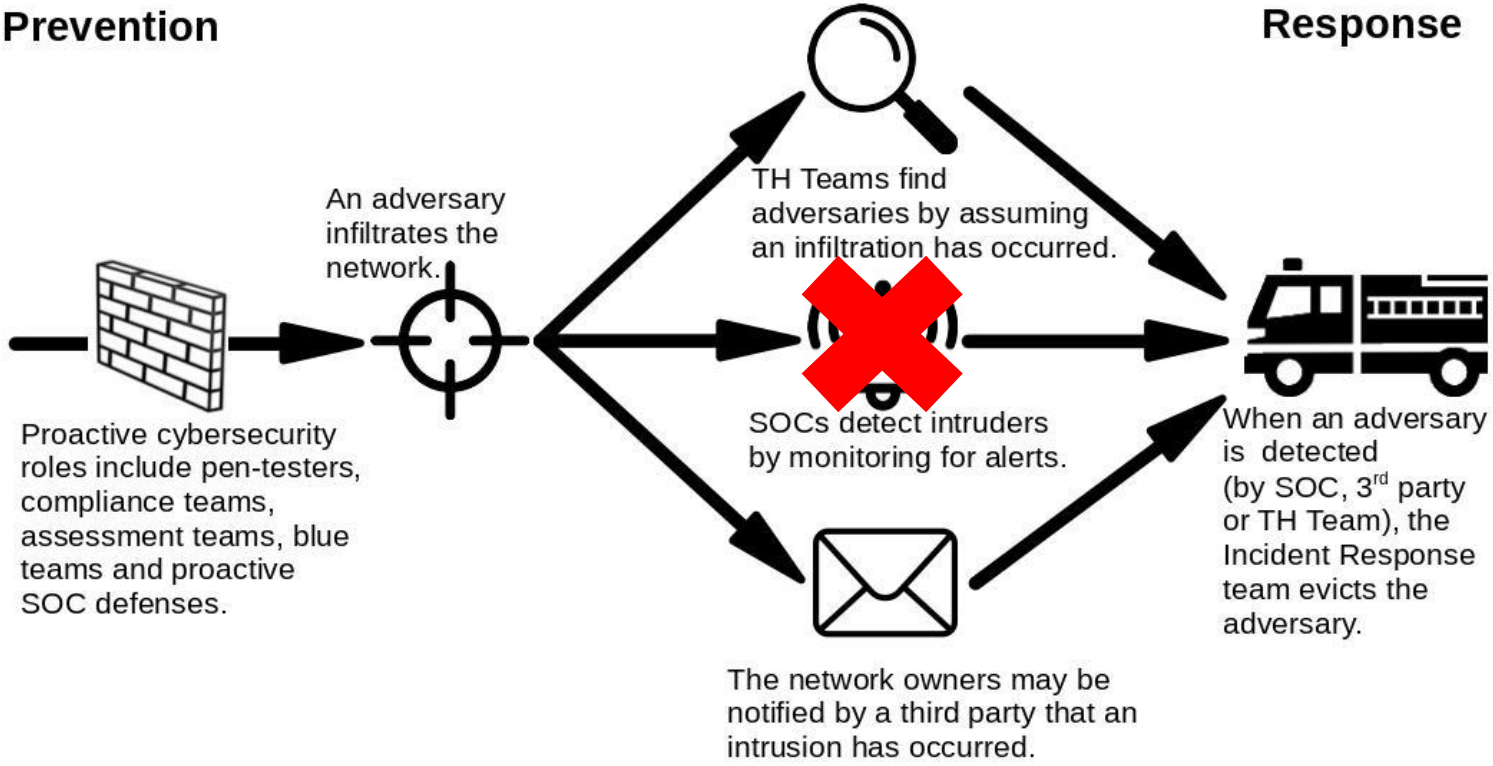
ELMORE FAMILY SCHOOL OF ECE

Three Paths to Adversary Discovery



ELMORE FAMILY SCHOOL OF ECE

Three Paths to Adversary Discovery



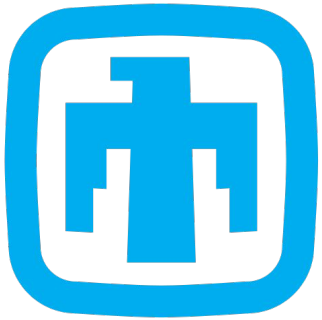
ELMORE FAMILY SCHOOL OF ECE

Private Sector TH teams

Booz | Allen | Hamilton

ELMORE FAMILY SCHOOL OF ECE

Government TH Teams



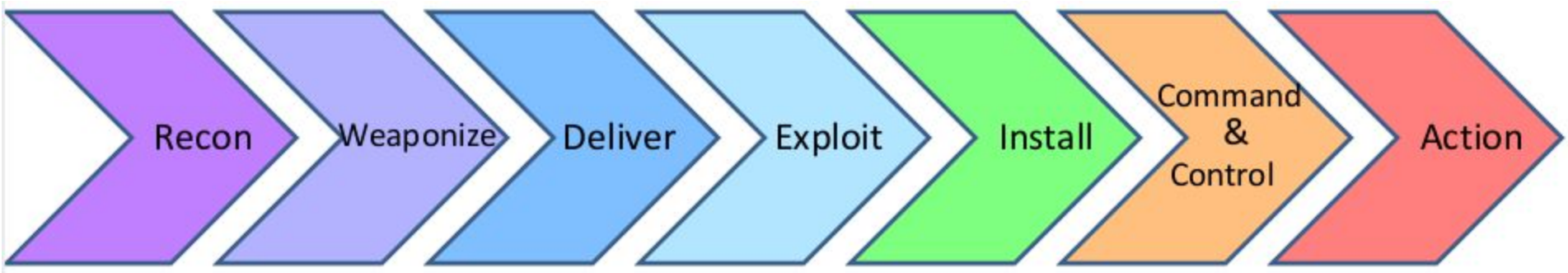
Sandia National Laboratories

ELMORE FAMILY SCHOOL OF ECE

Background

TH Frameworks

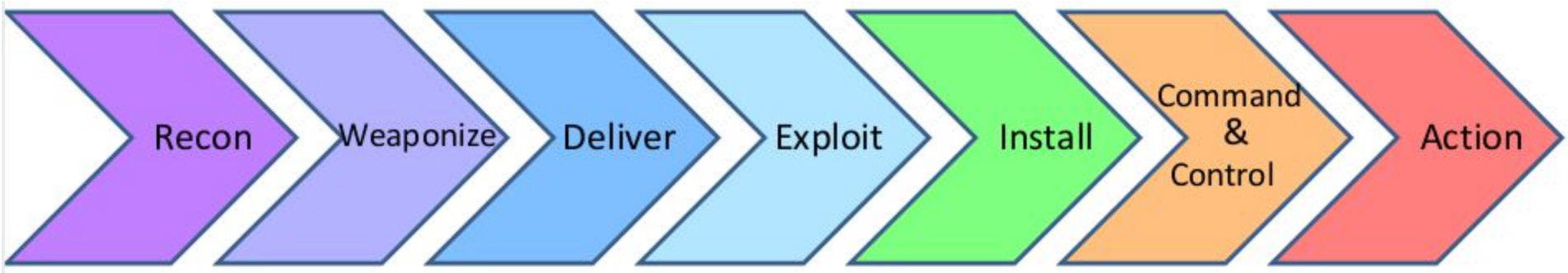
- Lockheed Kill Chain



Source: S. Commerce, “A "Kill Chain" analysis of the 2013 target data breach,” in The Target Store Data Breaches: Examination and Insight, Jan. 2014, pp. 41–60.

TH Frameworks

- Lockheed Kill Chain
- Mitre ATT&CK



Source: S. Commerce, “A "Kill Chain" analysis of the 2013 target data breach,” in The Target Store Data Breaches: Examination and Insight, Jan. 2014, pp. 41–60.

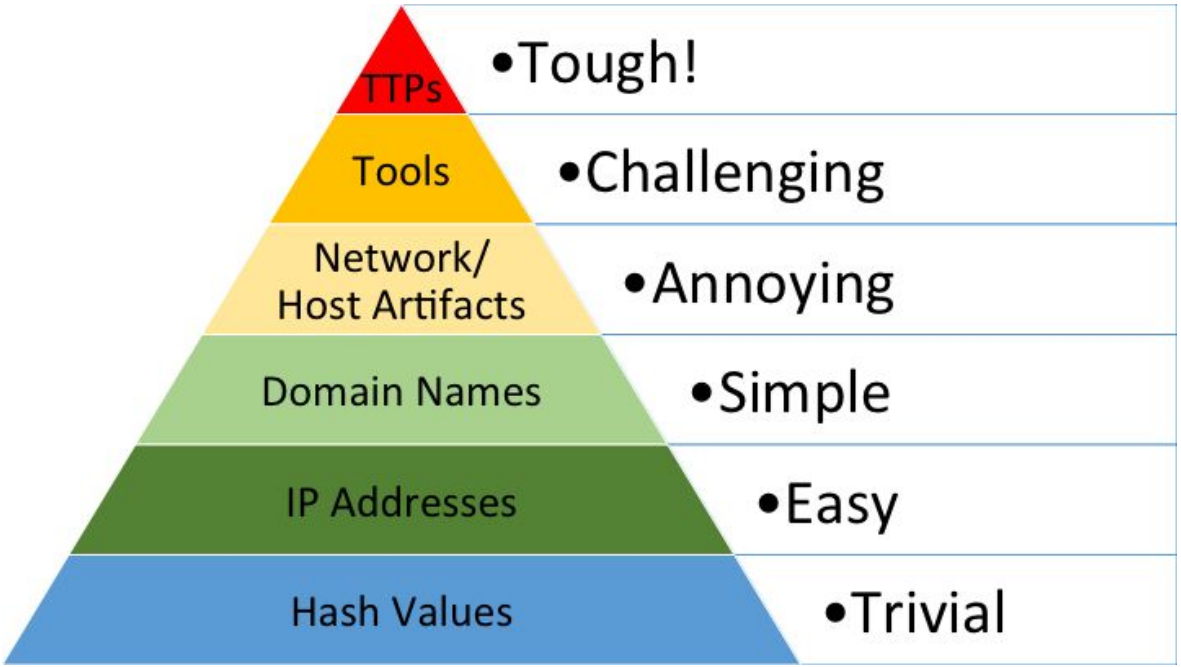
TH Frameworks

- Lockheed Kill Chain
- Mitre ATT&CK
- Hypothesis Checking

Source: R. van Os, M. Bakker, R. Bouman, M. D. van Leeuwen, M. van der Kraan, and W. Mentges, TaHiTI: A threat hunting methodology, Dec. 2018. [Online]. Available: https://www.betaalvereniging.nl/wp-content/uploads/TaHiTI-Threat-Hunting-Methodology-whitepaper.pdf .

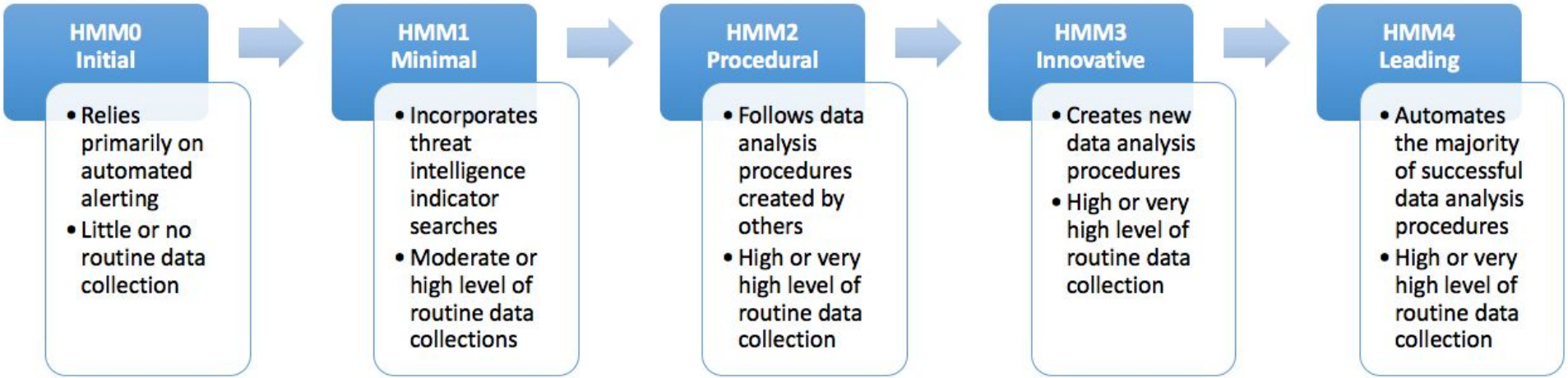
TH Frameworks

- Lockheed Kill Chain
- Mitre ATT&CK
- Hypothesis Checking
- Pyramid of Pain



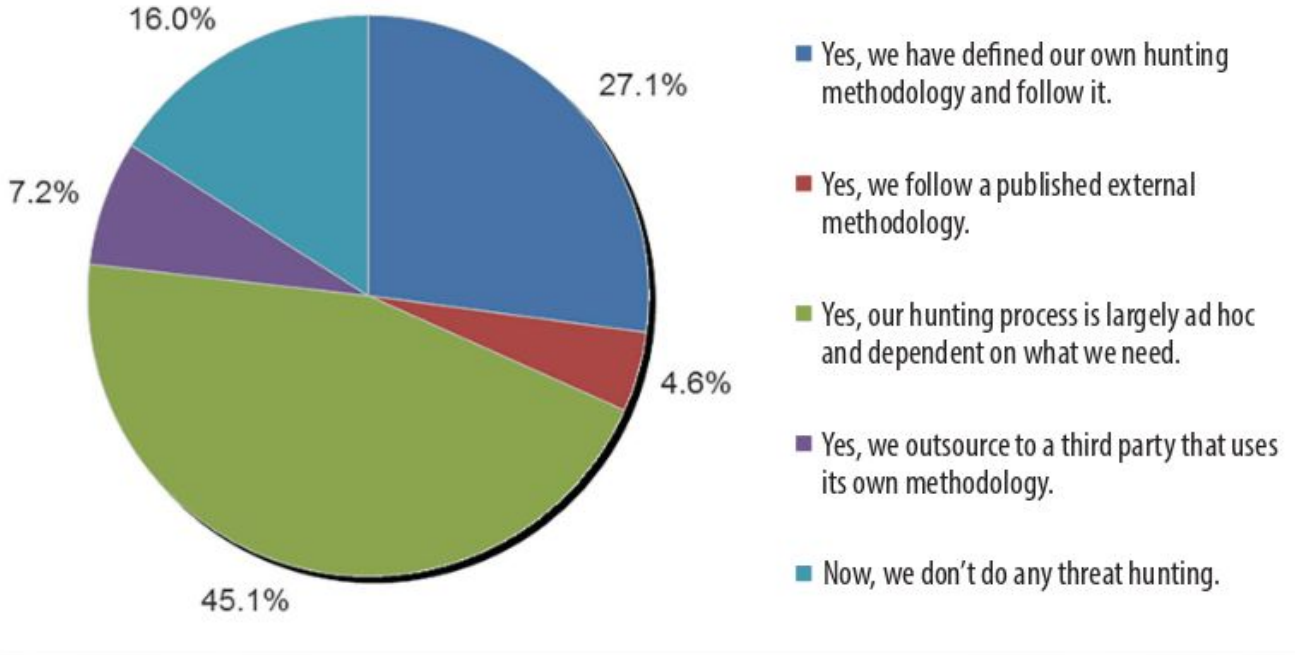
Source: Davidjbianco, Enterprise Detection & Response: The Pyramid of Pain, Mar. 2013. [Online]. Available: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html .

TH Maturity Model



Source: D. Bianco, A Simple Hunting Maturity Model, en, Blog. [Online]. Available: http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html .

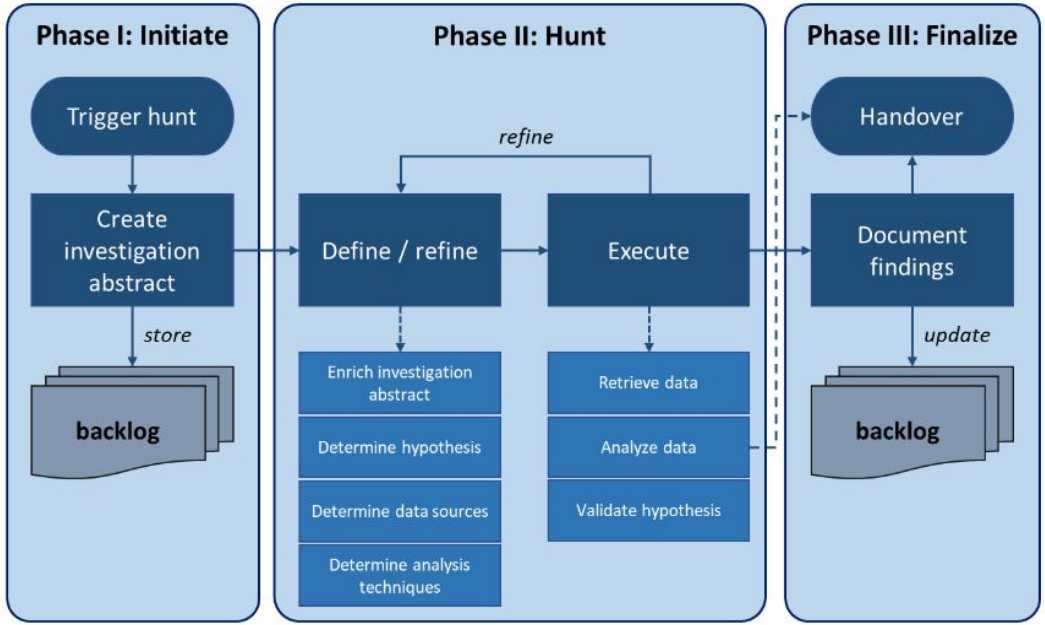
Most TH Teams Operate Ad Hoc



Source: W. R. Lee and R. M. Lee, The Hunter Strikes Back: The SANS 2017 Threat Hunting Survey, en, 2017.

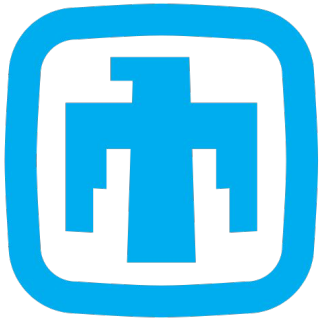
ELMORE FAMILY SCHOOL OF ECE

Targeted Hunting integrating Threat Intelligence (TaHiTI)



Source: R. van Os, M. Bakker, R. Bouman, M. D. van Leeuwen, M. van der Kraan, and W. Mentges, TaHiTI: A threat hunting methodology, Dec. 2018. [Online]. Available: https://www.betaalvereniging.nl/wp-content/uploads/TaHiTI-Threat-Hunting-Methodology-whitepaper.pdf .

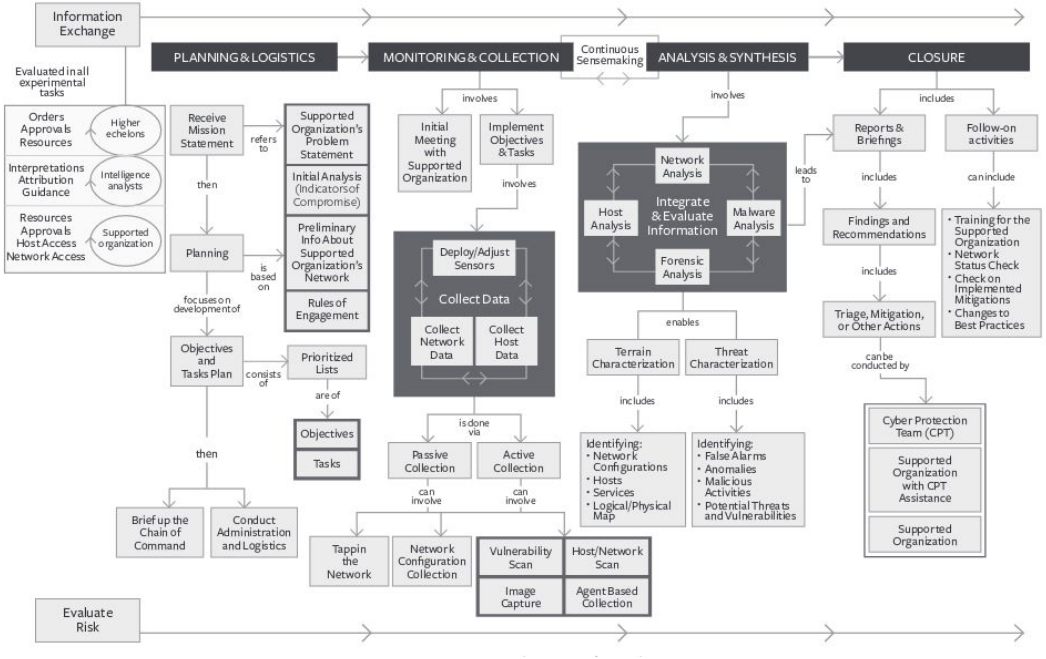
Government TH Teams



Sandia National Laboratories

ELMORE FAMILY SCHOOL OF ECE

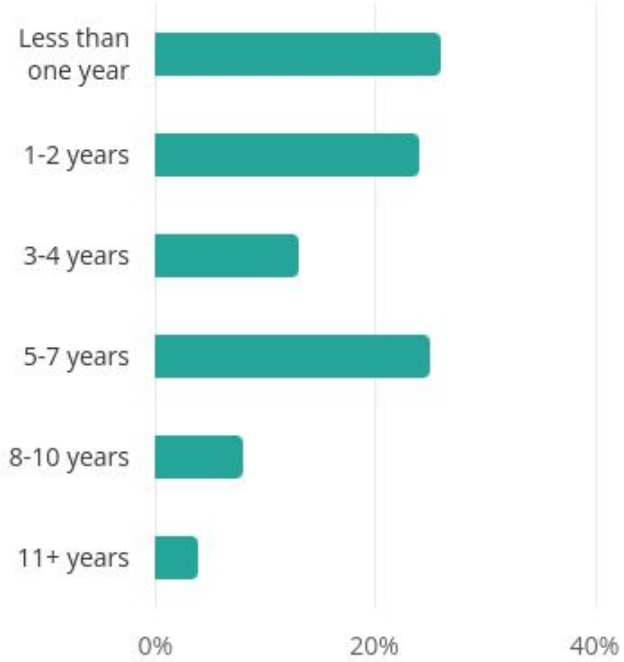
Modelling the Cognitive Work of CPTs (Trent et al.)



Source: S. Trent, R. R. Hoffman, D. Merritt, and S. Smith, "Modelling the Cognitive Work of Cyber Protection Teams," The Cyber Defense Review, vol. 4, no. 1, pp. 125–136, 2019, Publisher: Army Cyber Institute, issn: 2474-2120. [Online]. Available: http://www.jstor.org/stable/26623071 .

ELMORE FAMILY SCHOOL OF ECE

Cyber security turnover



Source: Cyber Security Analyst Demographics And Statistics In The US. [Online]. Available: https://www.zippia.com/cyber-security-analyst-jobs/demographics/ .

ELMORE FAMILY SCHOOL OF ECE

Research Questions

Research Questions

- Theme #1: Process
  - RQ1.1: What processes are currently used by government TH teams?
  - RQ1.2: What shortcomings exist with current government TH processes and what can be done to alleviate these shortcomings?
- Theme #2: New Members
  - RQ2.1: How do newer members fit into government TH processes?
  - RQ2.2: How could government TH process changes facilitate the integration of less expert members?
  - RQ2.3: What features indicate expertise to government TH team members?

Methodology

Methodology

- Semi-structured interviews

Methodology

- Semi-structured interviews
  - Requested hand-drawn process diagrams

ELMORE FAMILY SCHOOL OF ECE

Methodology

- Semi-structured interviews
- Recruitment

Methodology

- Semi-structured interviews
- Recruitment
  - 12 subjects

Position	# Subjects
Leadership	4
Team Leads	4
Analysts	4

ELMORE FAMILY SCHOOL OF ECE

Methodology

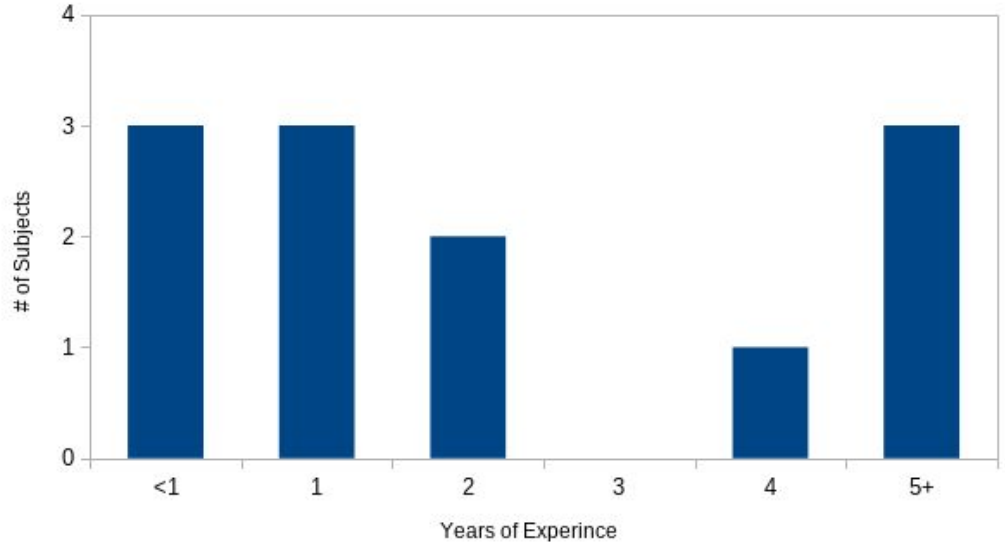
- Semi-structured interviews
- Recruitment
  - 12 subjects

Organization	# of Subjects
Coast Guard Cyber Command	10
CISA	3
Sandia National Labs	1
Private Sector	1

ELMORE FAMILY SCHOOL OF ECE

Methodology

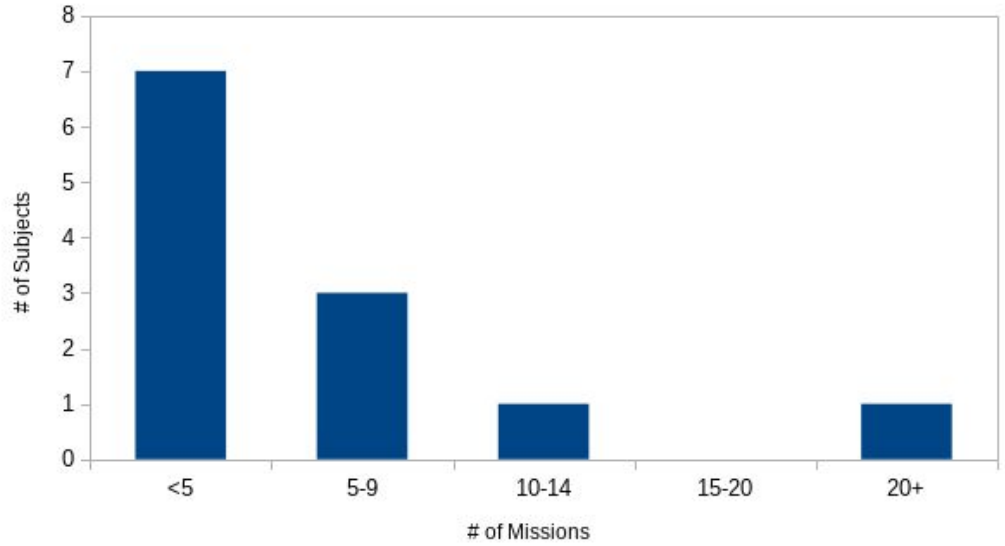
- Semi-structured interviews
- Recruitment
  - 12 subjects



ELMORE FAMILY SCHOOL OF ECE

Methodology

- Semi-structured interviews
- Recruitment
  - 12 subjects



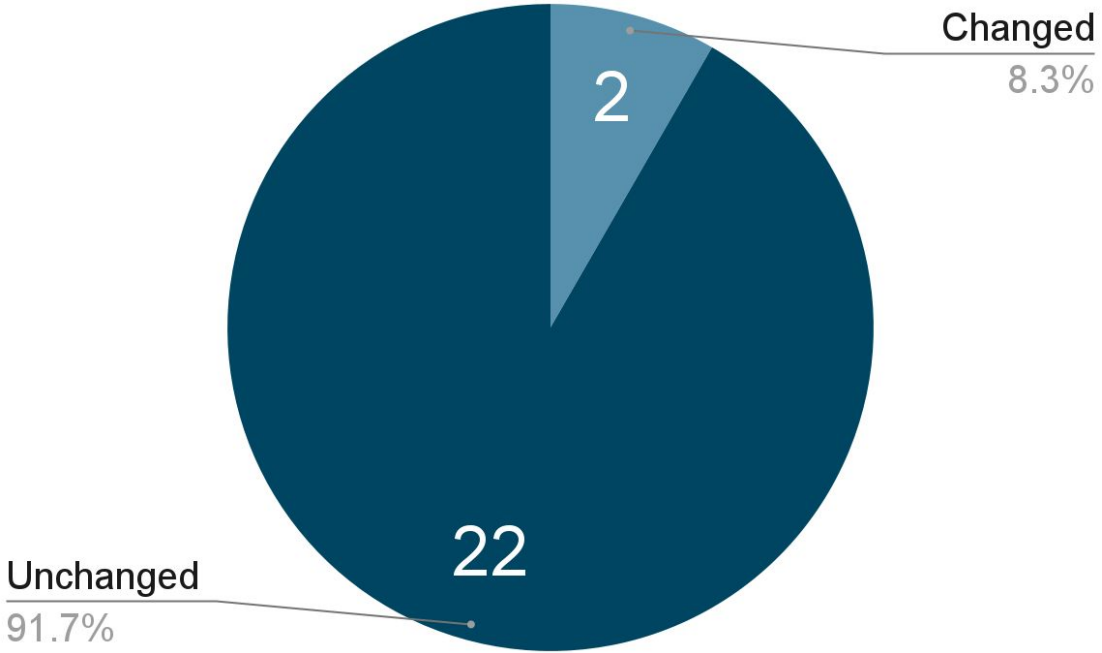
ELMORE FAMILY SCHOOL OF ECE

Methodology

- Semi-structured interviews
- Recruitment
- Interview instrument

Methodology

- Semi-structured interviews
- Recruitment
- Interview instrument
  - 2 internal pilots
  - Iteratively developed



ELMORE FAMILY SCHOOL OF ECE

Methodology

- Semi-structured interviews
- Recruitment
- Interview instrument creation
  - 2 internal pilots
  - Iteratively developed
  - 9 follow up questions added

- What is a good measure of a member's expertise?
  - Experience?
  - Certifications?
  - Personality?
  - Willingness to put in own time?
  - Is this different for potential?

ELMORE FAMILY SCHOOL OF ECE

Methodology

- Semi-structured interviews
- Recruitment
- Interview instrument creation
- Conduct interviews

Methodology

- Sanitization

Methodology

- Sanitization
  - National Security/Classification
  - Anonymization

Methodology

- Sanitization
- Thematic Coding

Methodology

- Sanitization
- Thematic Coding

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer.

ELMORE FAMILY SCHOOL OF ECE

Methodology

- Sanitization
- Thematic Coding
  - 636 Memos

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

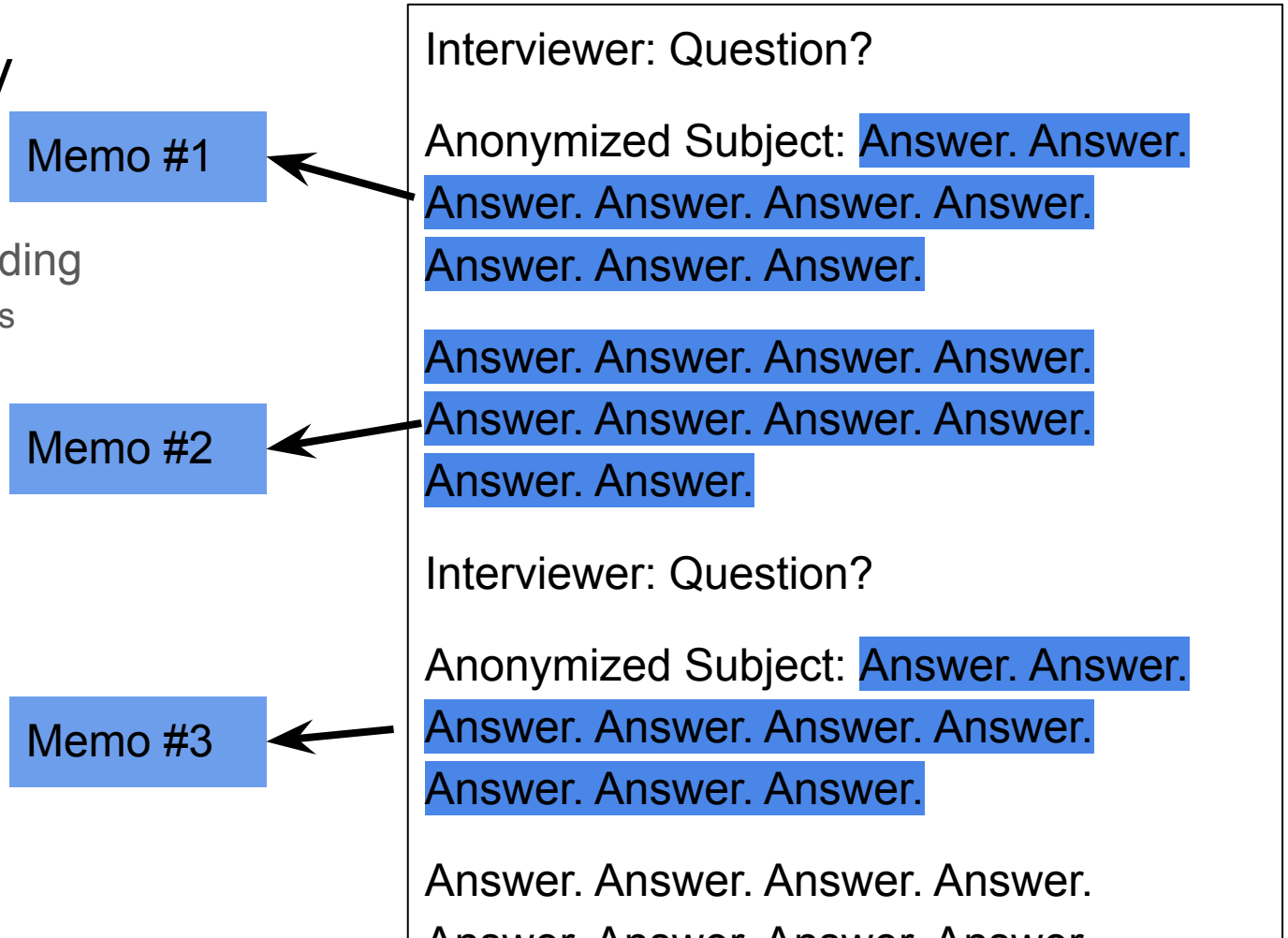
Answer. Answer. Answer. Answer.

Memo: If there is Intel then the CPT has a focus when beginning the process

ELMORE FAMILY SCHOOL OF ECE

Methodology

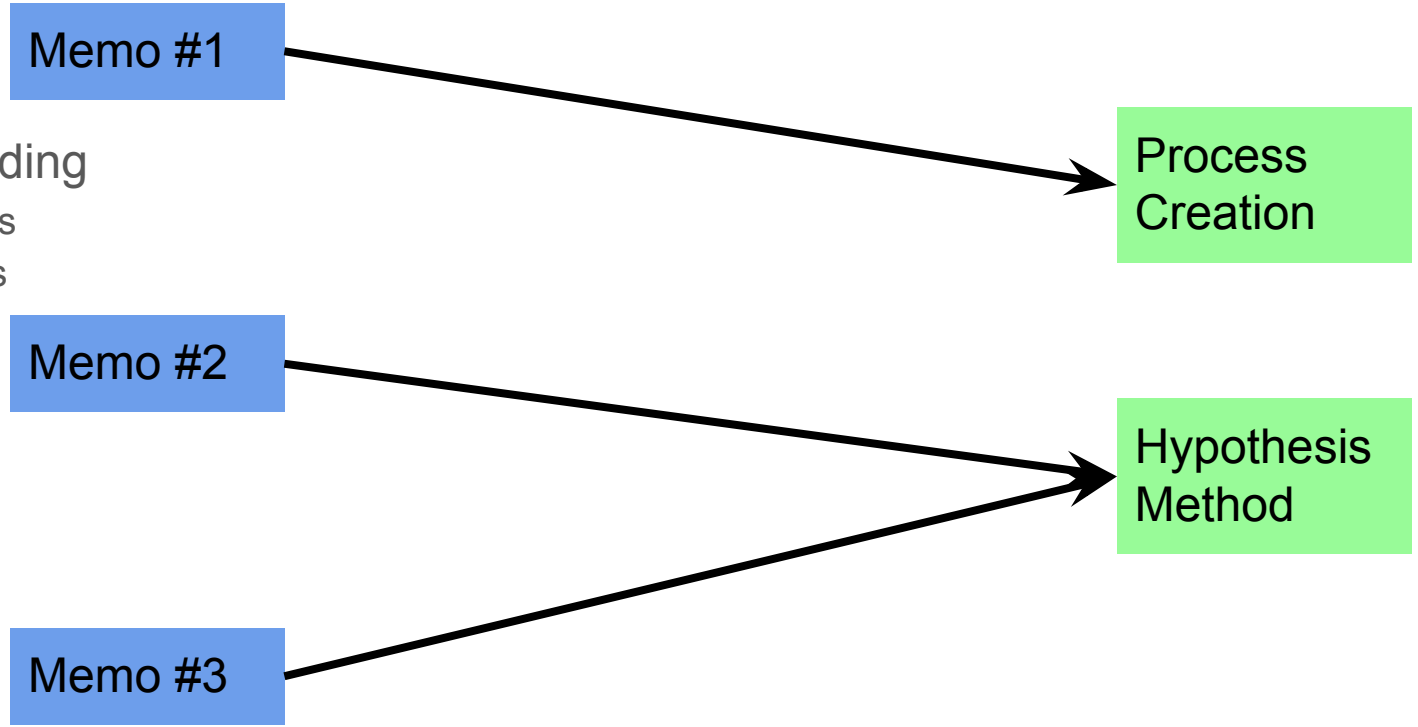
- Sanitization
- Thematic Coding
  - 636 Memos



ELMORE FAMILY SCHOOL OF ECE

Methodology

- Sanitization
- Thematic Coding
  - 636 Memos
  - 58 Themes



ELMORE FAMILY SCHOOL OF ECE

Methodology

- Sanitization
- Thematic Coding
  - 636 Memos
  - 58 Themes

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer.

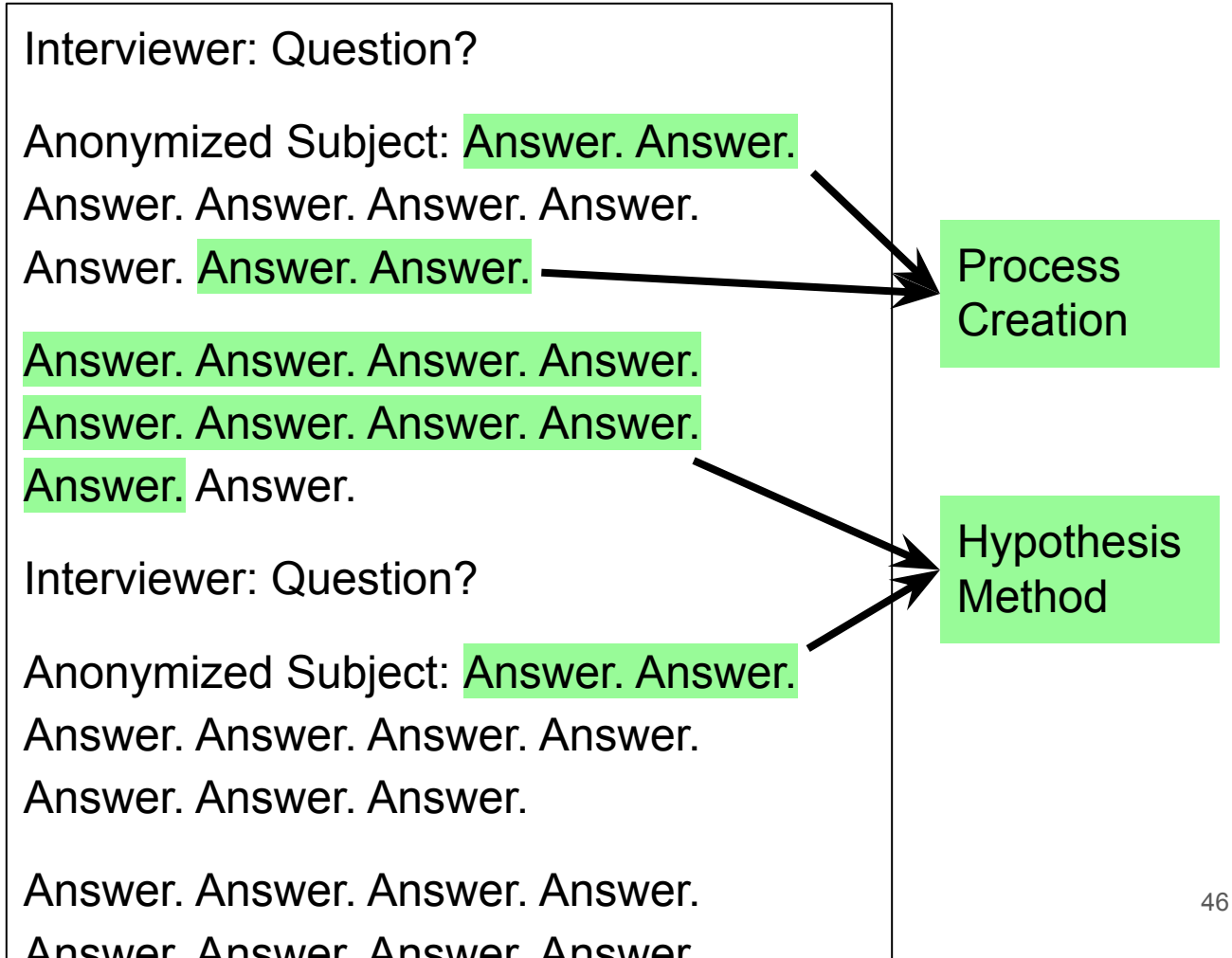
Process Creation

Hypothesis Method

ELMORE FAMILY SCHOOL OF ECE

Methodology

- Sanitization
- Thematic Coding
  - 636 Memos
  - 58 Themes



ELMORE FAMILY SCHOOL OF ECE

Methodology

- Sanitization
- Thematic Coding
- Process Coding

Methodology

- Sanitization
- Thematic Coding
- Process Coding

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer.

ELMORE FAMILY SCHOOL OF ECE

Methodology

- Sanitization
- Thematic Coding
- Process Coding

Code #1

Code #2

Not in TaHiTI

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer.

ELMORE FAMILY SCHOOL OF ECE

Methodology

- Sanitization
- Thematic Coding
- Process Coding

Code #1

Code #2

Not in TaHiTI

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer.

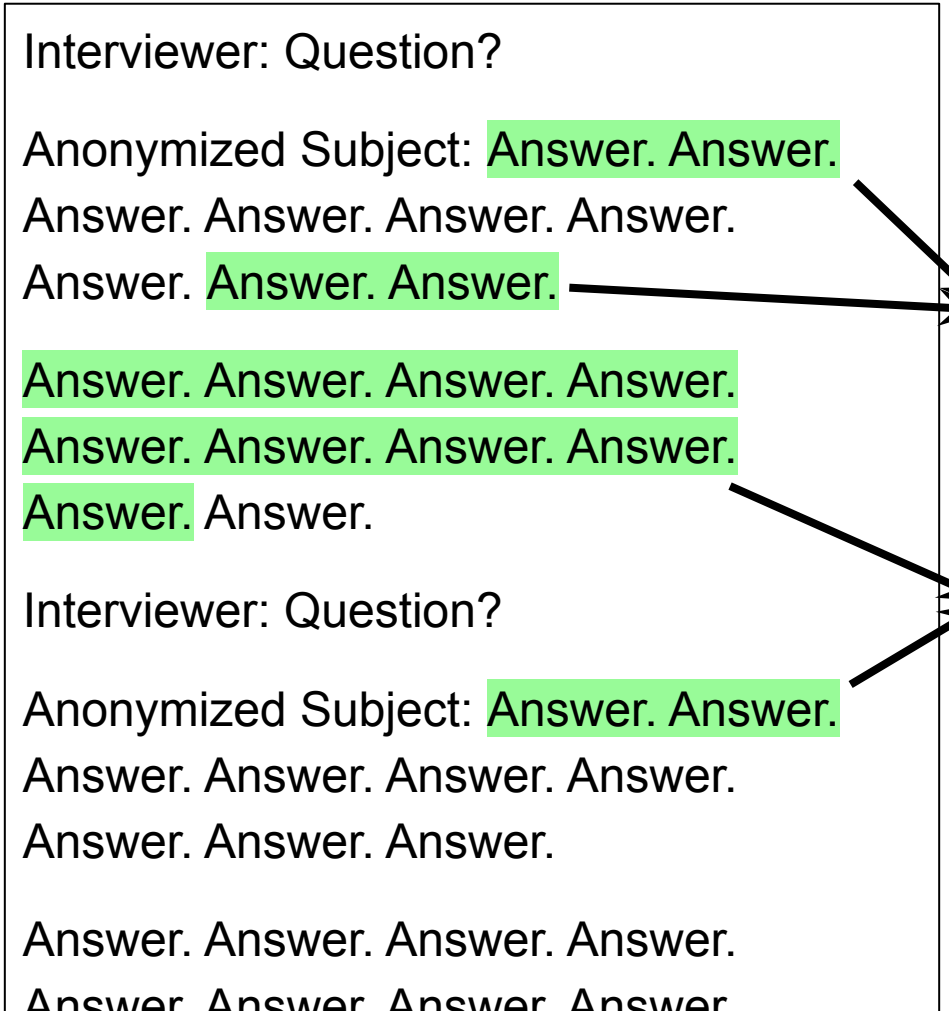
ELMORE FAMILY SCHOOL OF ECE

Methodology

- Sanitization
- Thematic Coding
- Process Coding
- Interrater Agreement

Methodology

- Sanitization
- Thematic Coding
- Process Coding
- Interrater Agreement
  - Kappa .82



ELMORE FAMILY SCHOOL OF ECE

Methodology

- Sanitization
- Thematic Coding
- Process Coding
- Interrater Agreement
  - Kappa .82

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

?

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Process Creation

Hypothesis Method

ELMORE FAMILY SCHOOL OF ECE

Methodology

- Sanitization
- Thematic Coding
- Process Coding
- Interrater Agreement
  - Kappa .82

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

?

Interviewer: Question?

Anonymized Subject: Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer. Answer.

Answer. Answer. Answer. Answer.

Code #1

Code #2

Code #3

Code #4

Code #5

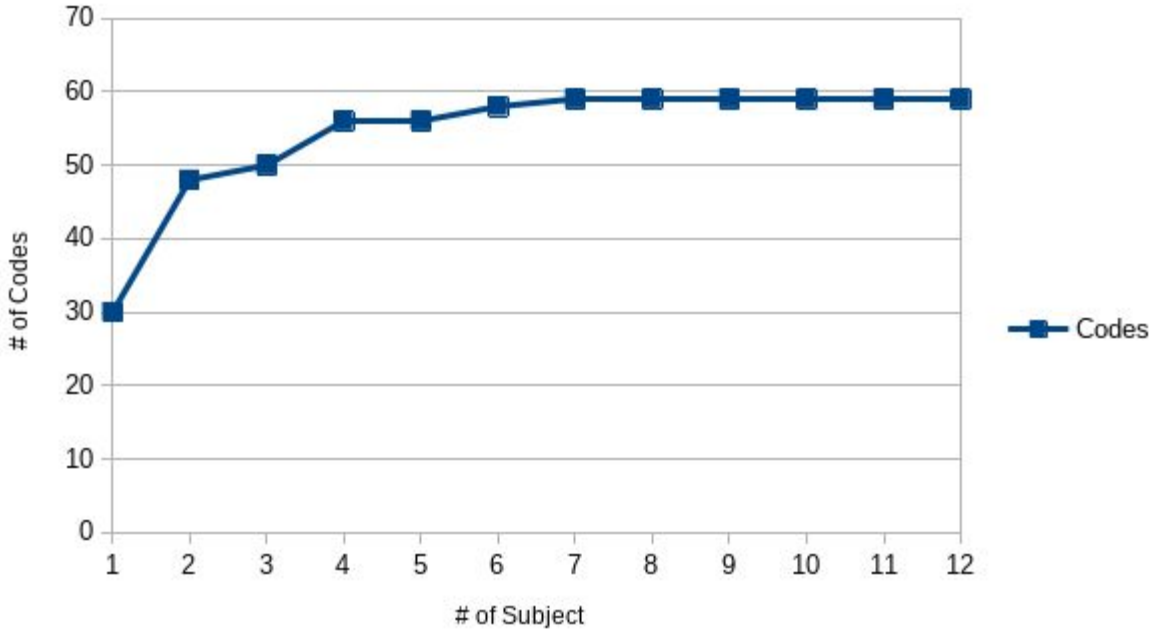
Code #6

Code …

Code #58

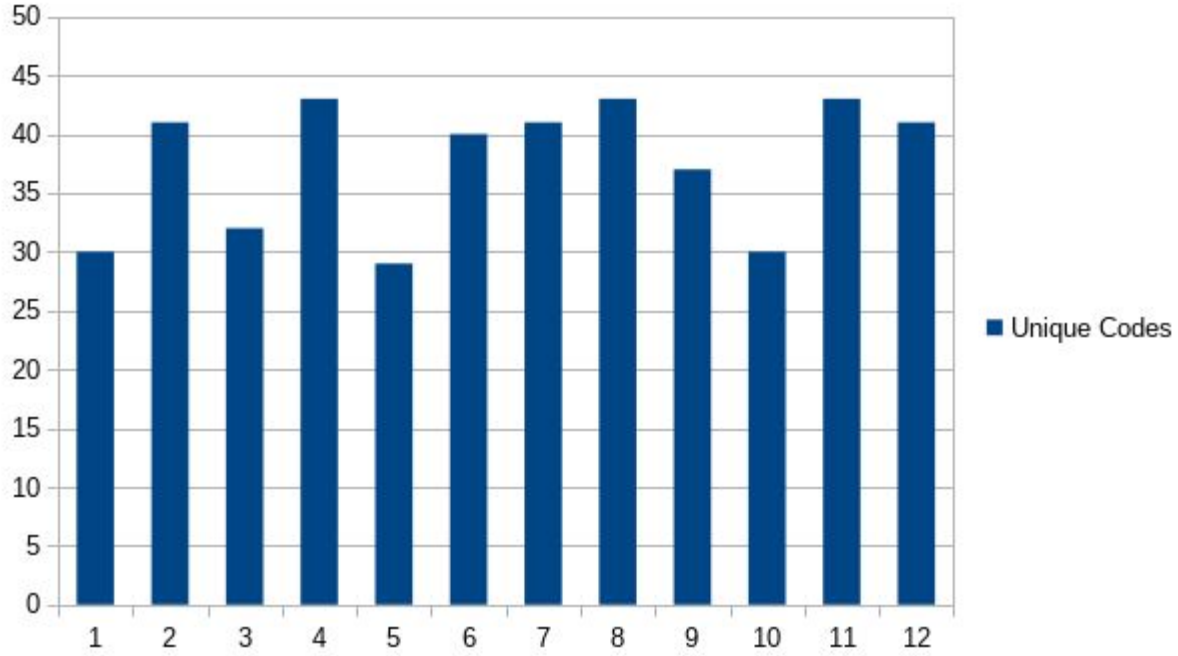
ELMORE FAMILY SCHOOL OF ECE

Cumulative Number of Codes After Each Interview



ELMORE FAMILY SCHOOL OF ECE

Unique codes observed at each interview



ELMORE FAMILY SCHOOL OF ECE

Limitations

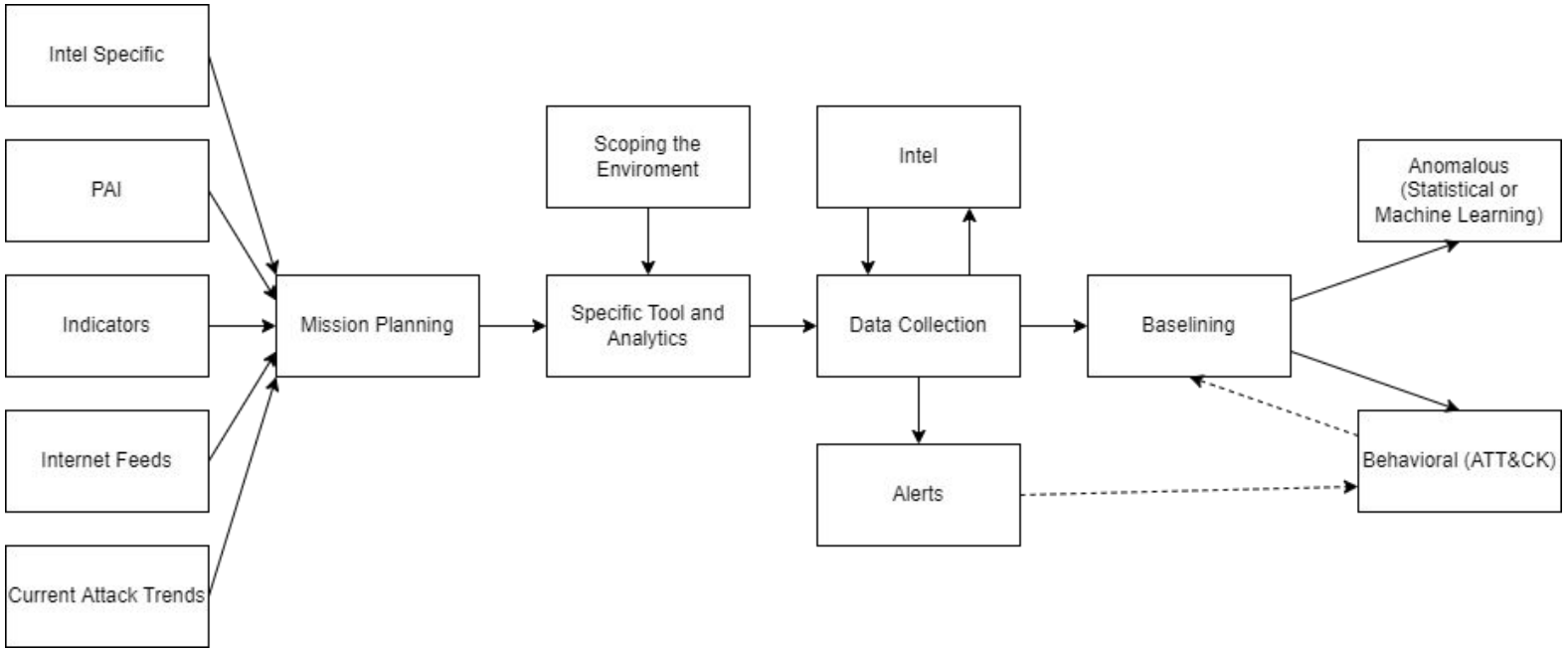
- A sample size of 12 is small
  - Not uncommon
  - Sufficiently large for homogenous populations
- One researcher did most of the work
  - Kappa .82
- Self reported
  - Used best practices
- Limited generalizability
  - Only seeking to describe what was observed within government teams

ELMORE FAMILY SCHOOL OF ECE

Results

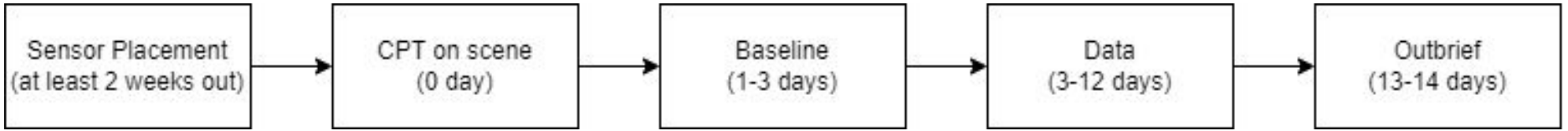
RQ1.1: What processes are currently used by government TH teams?

Detailed Diagrams



ELMORE FAMILY SCHOOL OF ECE

Linear Diagrams



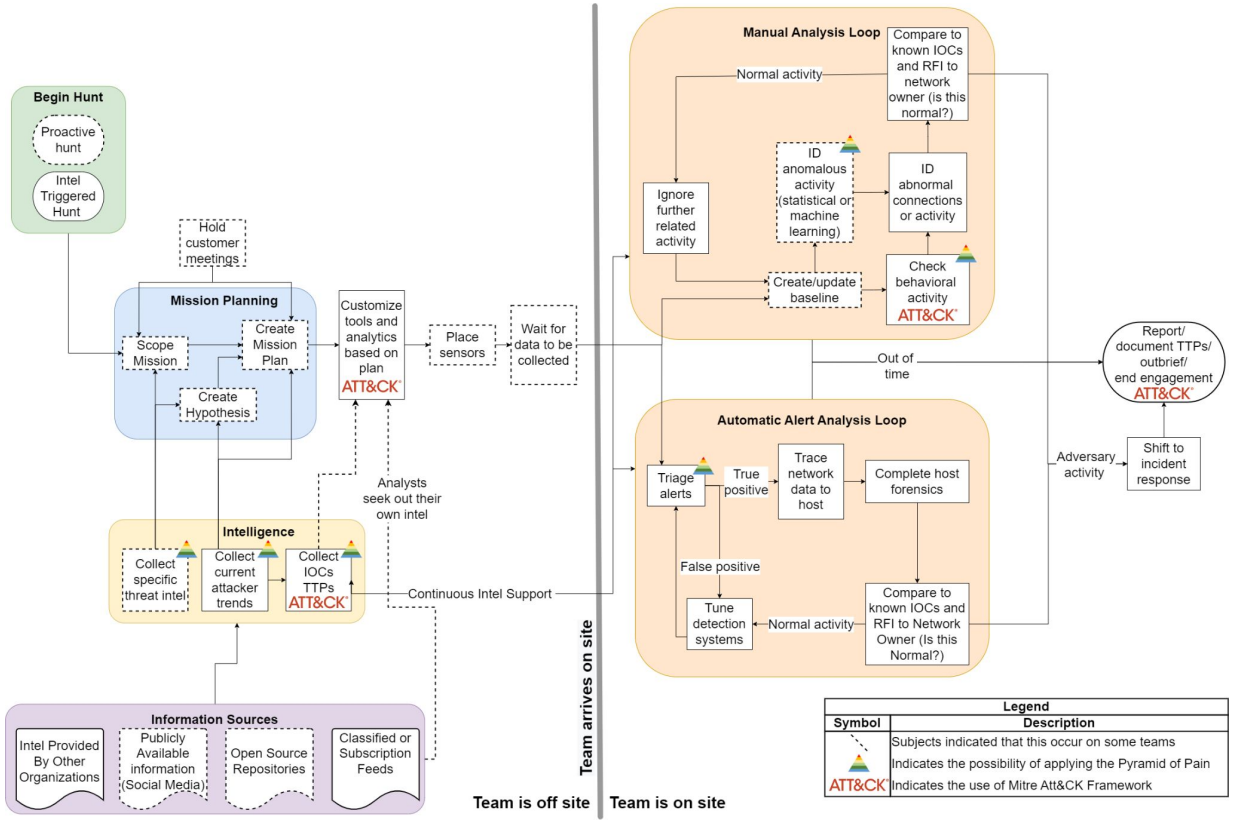
ELMORE FAMILY
SCHOOL OF ECE

The Simplest Diagram

The Simplest Diagram

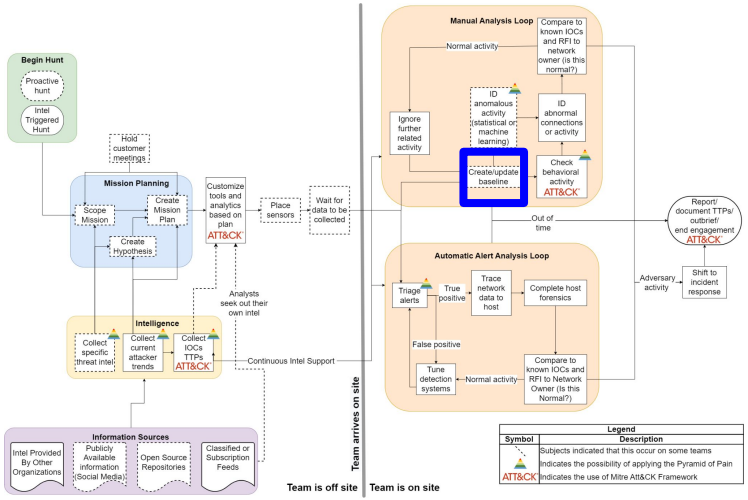
“Then, for the hunt section, the reason why it’s just a nebulous cloud is because that’s kind of what it is right now. We just hunt.”

The Observed Process



ELMORE FAMILY SCHOOL OF ECE

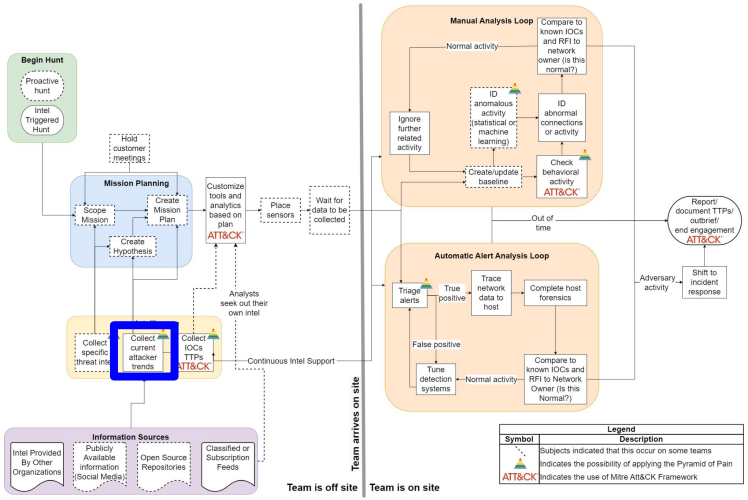
From Data to Process

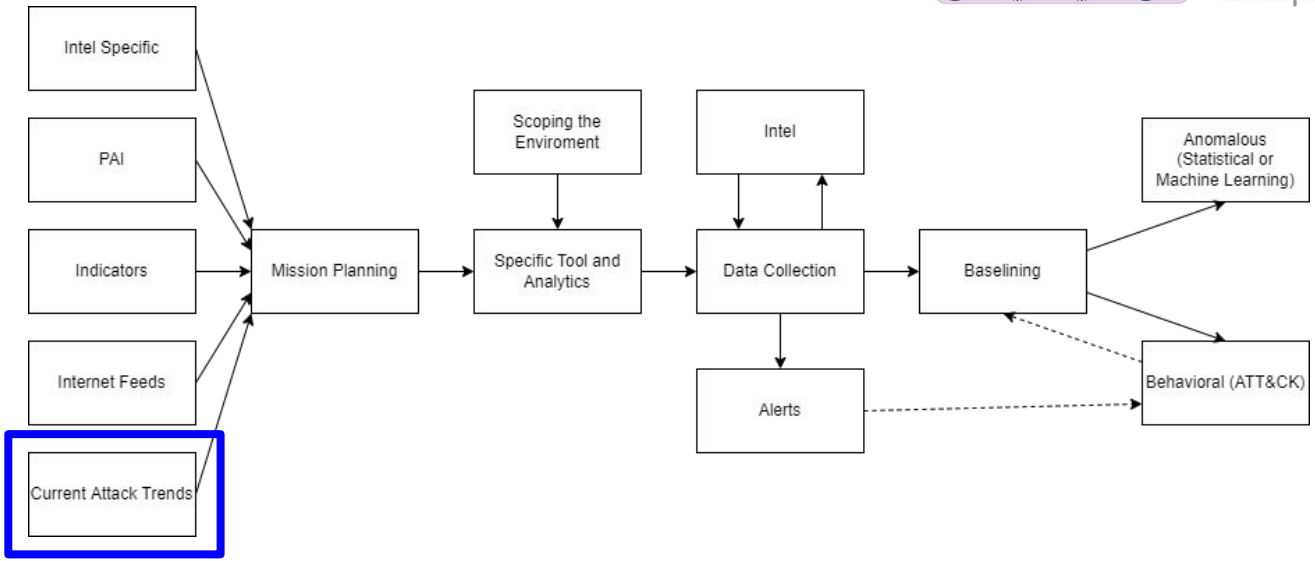


ELMORE FAMILY SCHOOL OF ECE

From Data to Process

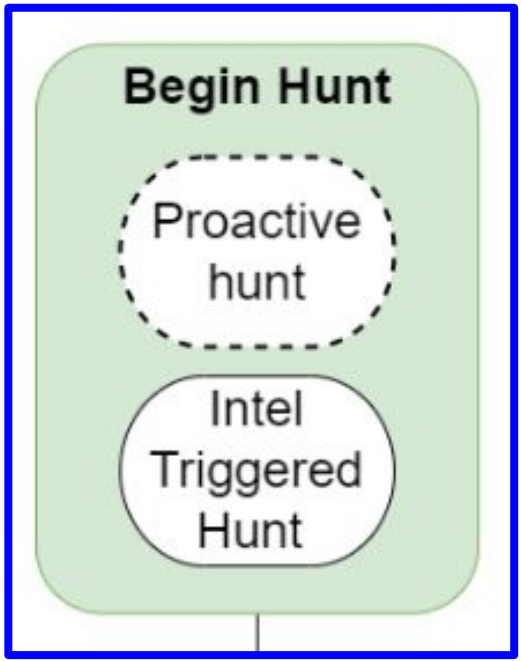
We may have Intel … like current events, if there's like a current prevalent, exploit that's being used, that you're seeing in the news, something that everyone would know about.

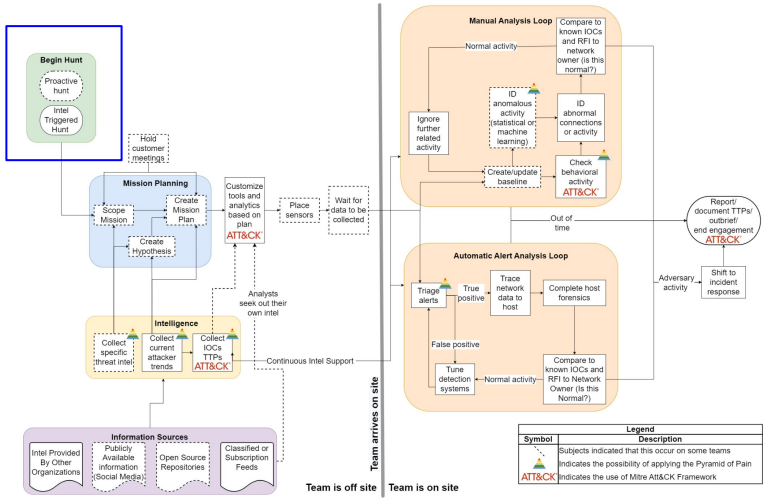




ELMORE FAMILY SCHOOL OF ECE

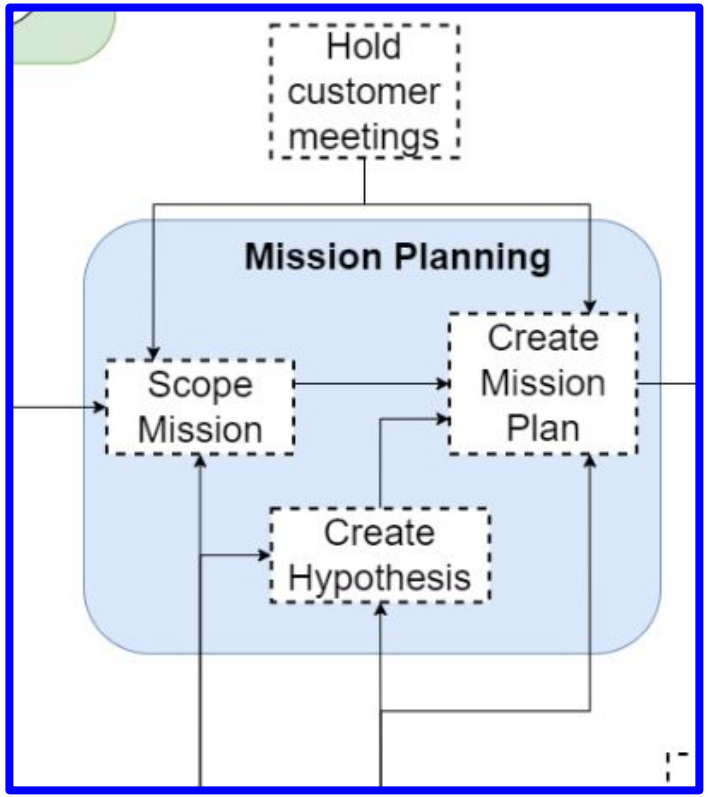
The Observed Process

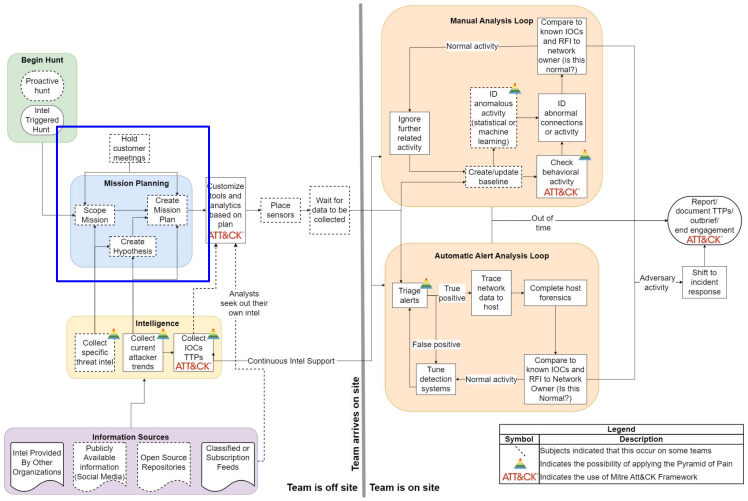




ELMORE FAMILY SCHOOL OF ECE

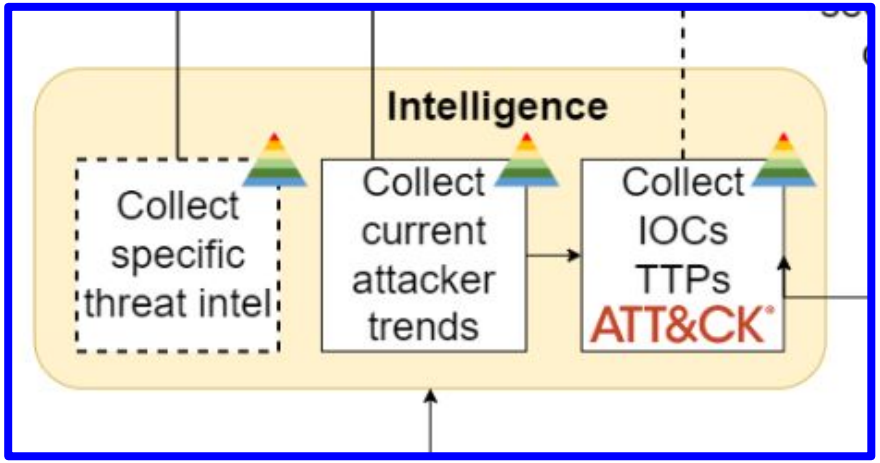
The Observed Process

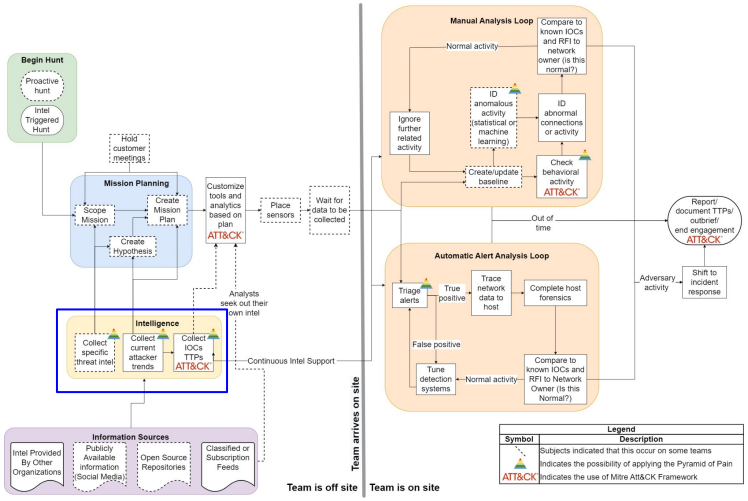




ELMORE FAMILY SCHOOL OF ECE

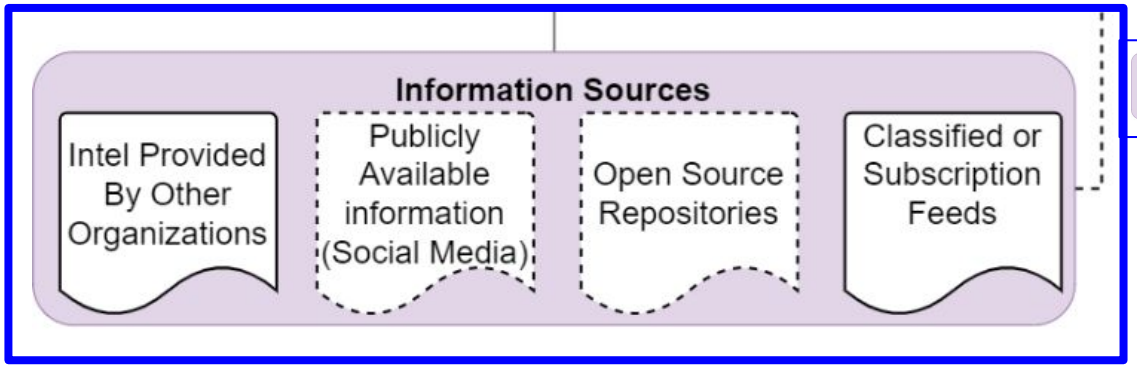
The Observed Process

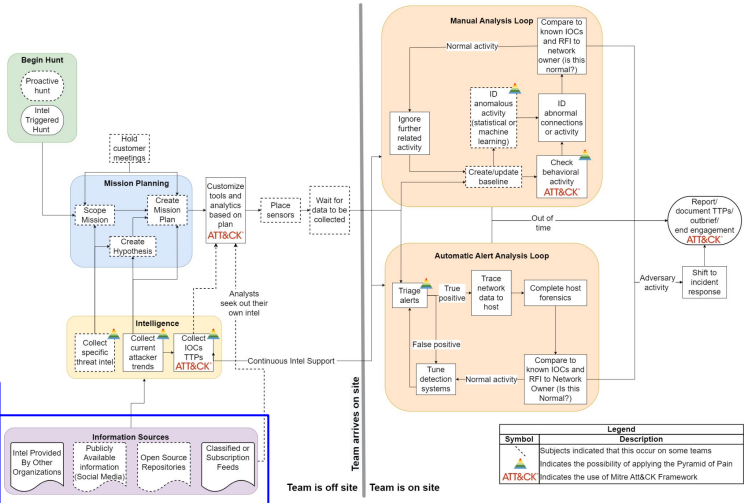




ELMORE FAMILY SCHOOL OF ECE

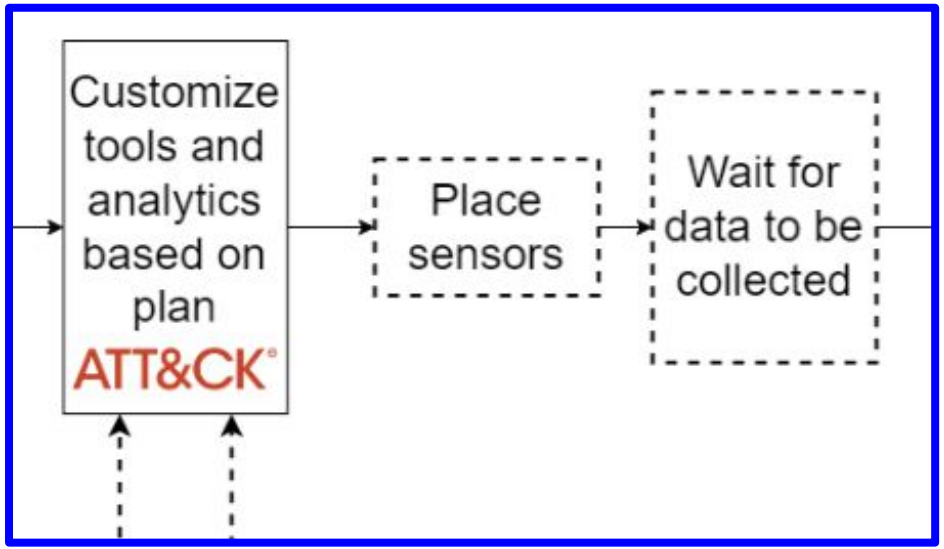
The Observed Process

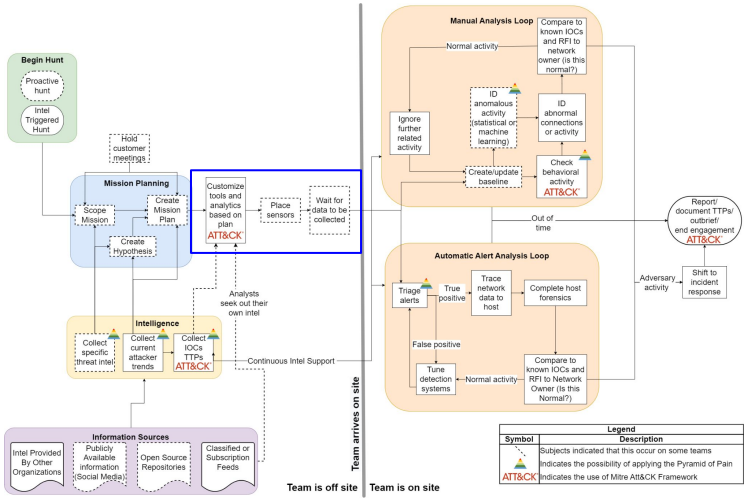




ELMORE FAMILY SCHOOL OF ECE

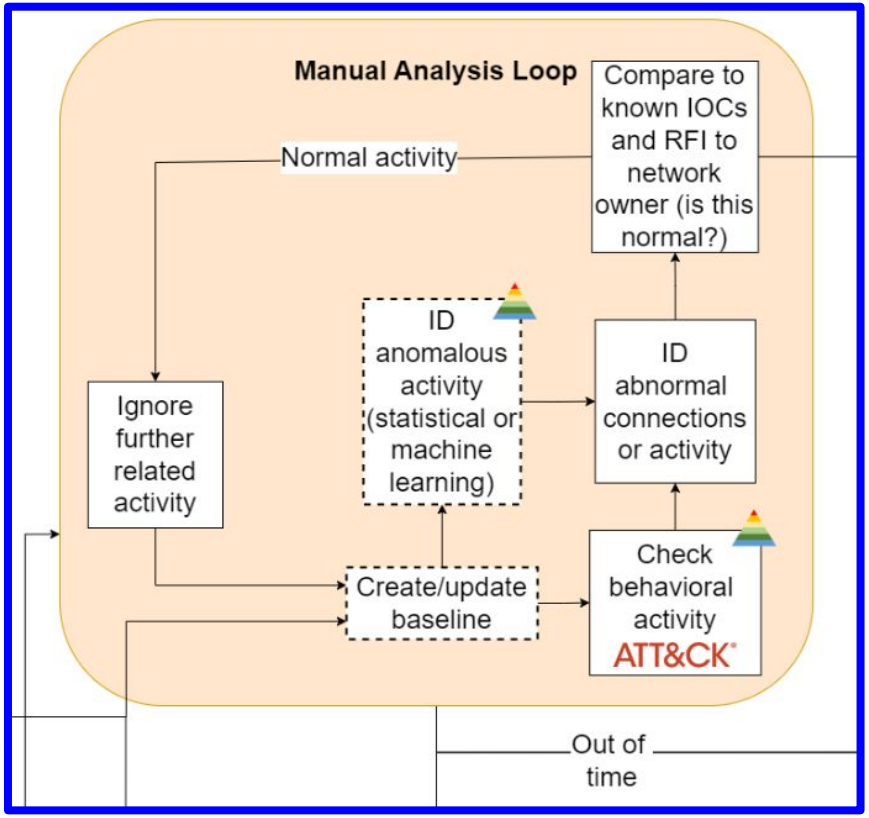
The Observed Process

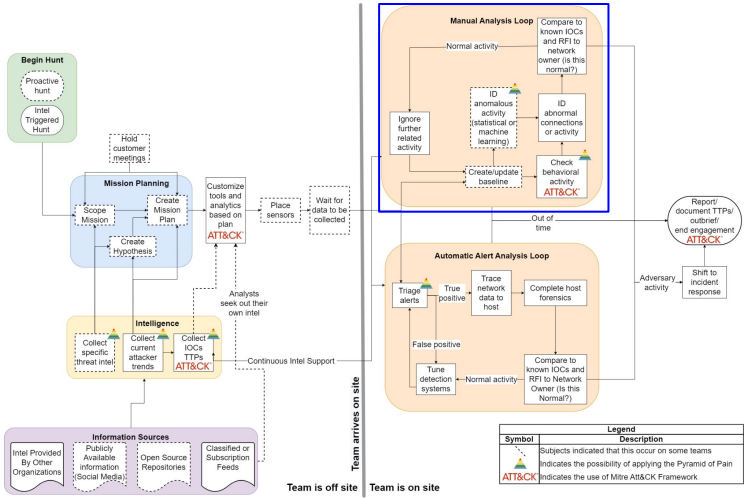




ELMORE FAMILY SCHOOL OF ECE

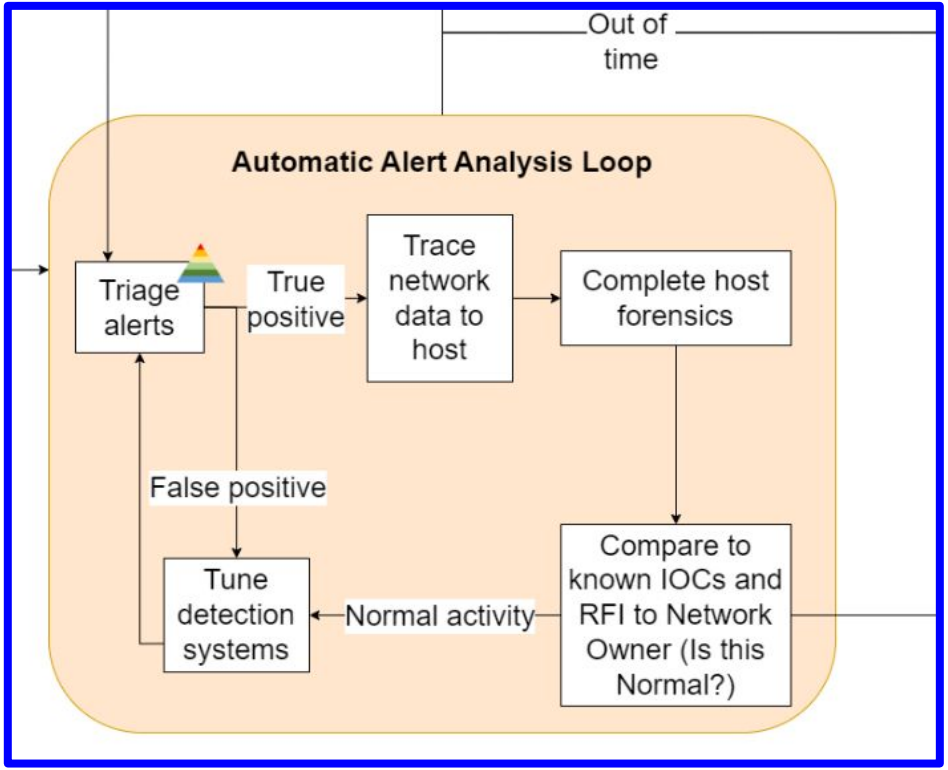
The Observed Process

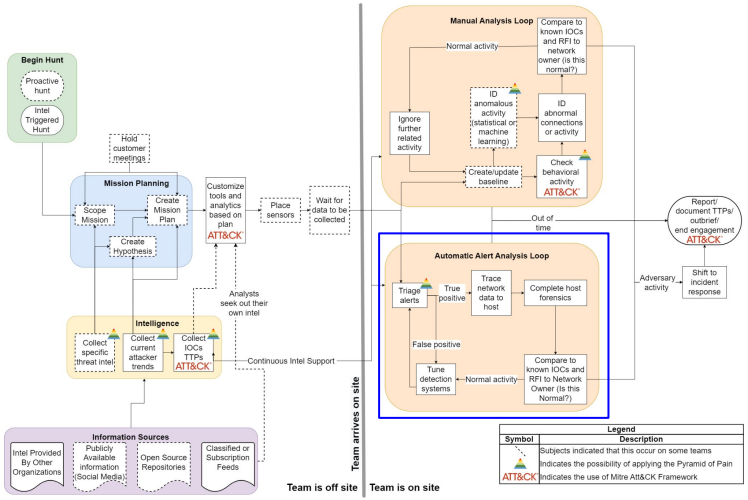




ELMORE FAMILY SCHOOL OF ECE

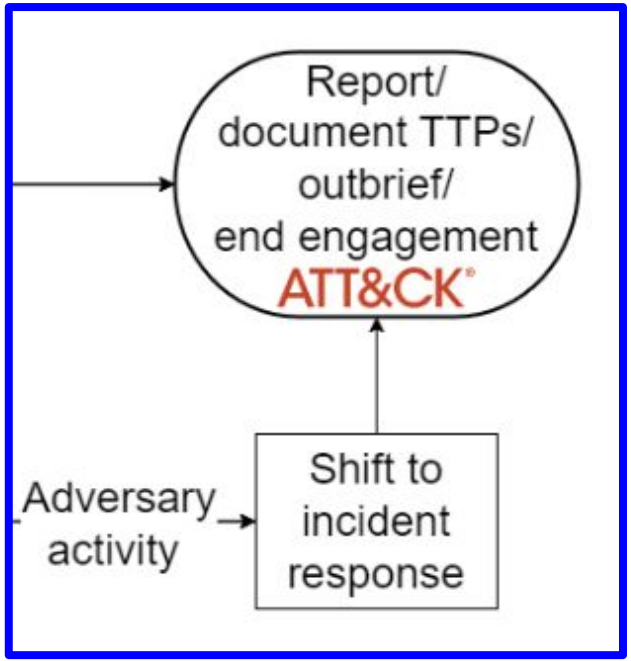
The Observed Process

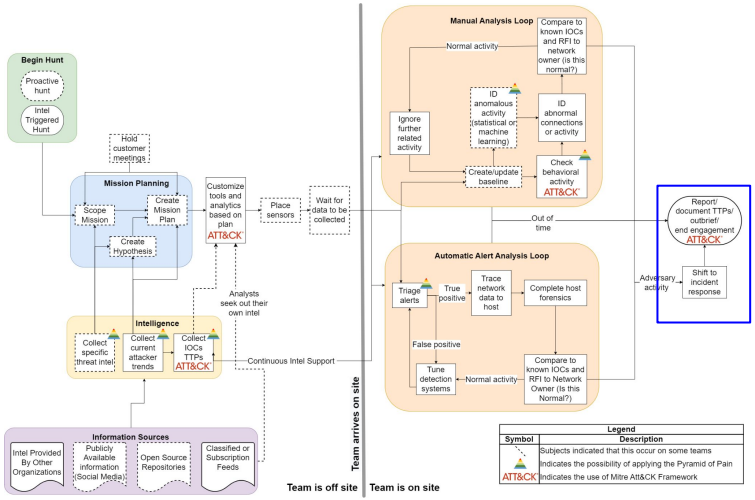




ELMORE FAMILY SCHOOL OF ECE

The Observed Process





ELMORE FAMILY SCHOOL OF ECE

Frameworks incorporated

TH Frameworks	# Subjects who used the framework (# of organizations)
Mitre ATT&CK	11 (3)
Hypothesis Checking	8 (3)
Lockheed's Kill Chain	3 (2)
Pyramid of Pain	2 (2)

RQ1.2: What shortcomings exist with current government TH processes and what can be done to alleviate these shortcomings?

RQ1.2: Process shortcomings

Shortcoming	# Subjects (# organizations)
Too little automation	7 (3)
Poor threat intelligence	5 (2)
Teams lack needed data	5 (2)
Insufficient process detail	5 (2)
Side-tracked analysts	4 (2)
High turnover	4 (2)
Inaccurate task tracking	4 (1)

Too little automation

- 7 subjects had this complaint
- 2 subjects were hesitant
  - Tasks should not be automated
  - TH cannot be automated

“Hunting in general should start where automation stops. … Because you have these SOC automation tools … but with threat hunting, the premise, the fundamental assumption, is that the sophisticated adversary already bypassed all that and now you have to apply the manual technique to be able to find them. … I think to some point it’s good to automate some things that are repetitive, … But I think most of the analytical work should still be relying on [the] human factor.”

Poor threat intelligence

- 5 subjects had this complaint
  - Intel was not helpful (3 subjects)
  - Intel seemed random (2 subjects)
  - Intel personnel did not understand the mission (1 subject)
- 5 subjects mentioned intelligence and did not complain

“We have the [intelligence component] gather the Intel for us before we go on a mission. Usually, I honestly don’t know how they do it because it doesn’t make sense. ... It seems like they just randomly pick out APTs [Advanced Persistent Threats] to go after.”

RQ2.1: How do newer members fit into government TH processes?

RQ2.1: How new members fit into the process

- Simple Tasks (3 subjects)
- Used for feedback (3 subjects)
- Sometimes a hindrance (1 subject)

RQ2.1: How new members fit into the process

- Simple Tasks (3 subjects)
- Used for feedback (3 subjects)
- Sometimes a hindrance (1 subject)

Recommendation	# Subjects (# Organizations)
Cybersecurity Education & Experience	5 (3)
Computer & Networking Basics	5 (1)
Number of missions	4 (1)

ELMORE FAMILY SCHOOL OF ECE

RQ2.2: How could government TH process changes facilitate the integration of less expert members?

RQ2.2: Facilitating the integration of less expert members

Recommendation	# Subjects (# Organizations)
Pairing Members	7 (3)
Process Documentation	6 (3)
Task Separation	4 (1)
Training	3 (2)
Personnel Issues	2 (1)

Pairing Members

- 7 subjects recommended this practice
- 2 critical subjects
  - Slows down the process
  - Must be interactive

“One of the things we did ... that I thought was really useful is doing a threat hunt with fellow [team] member. They kind of had experience looking a lot of the data and the host forensic side things and so I was able to learn a lot from them ... so I thought that was really useful. I think like a lot of shoulder surfing kind of experiences, I think that would be useful.”

Process Documentation

- 6 subjects recommended this practice
  - Ensuring a standard quality of work (2 subjects)
  - Providing guidance (4 subjects)
- 1 critical subject
  - Concerned about coverage

“I think having the [documentation] will help them be more effective, faster, because it will give them a guideline of what to do. … So instead of sitting there: ‘I don’t even know where to start.’ It’s: ‘I’m looking for connections on odd ports. That’s my first thing. And that’s how I’m gonna learn to build my first queries.’”

RQ2.3: What features indicate expertise to government TH team members?

RQ2.3: Features that indicate expertise

Feature	# subjects who spoke positively (# orgs)	# subjects who spoke negatively (# orgs)
Experience and number of missions	6 (3)	5 (2)
Certifications	2 (1)	7 (3)
Doing cybersecurity work in personal time	7 (2)	1 (1)
Training	3 (2)	4 (2)
Personality	5 (2)	2 (1)

ELMORE FAMILY SCHOOL OF ECE

Experience and number of missions

- 6 subjects spoke positively of this as a metric for expertise
  - Spoke hesitantly - indicating a general rule not an unbreakable law
- 5 subjects were critical
  - Often gave examples of individuals

“You … have people who’ve been on a hundred missions and they just don’t have the aptitude or the thought ability. You also have people who have never been on a mission who have the aptitude and who are gonna outperform people who have been on 20 missions. … The biggest <hesitates> there is a correlation between number of missions and analyst success. I would say there’s very little correlation between … [lists other factors]“

ELMORE FAMILY SCHOOL OF ECE

Certifications

- 2 subjects spoke positively of this as a metric for expertise
  - As a baseline only
- 7 subjects were critical

“Certifications I think are a good baseline, but not what should necessarily be used beyond that. It’s good to know people have, you know, your [name of cert] or [name of cert] or at least some sort of "coming in baseline" where they understand a little bit, but experience actually being on a network, threat hunting [is] more valuable once you’ve gotten that baseline. ”

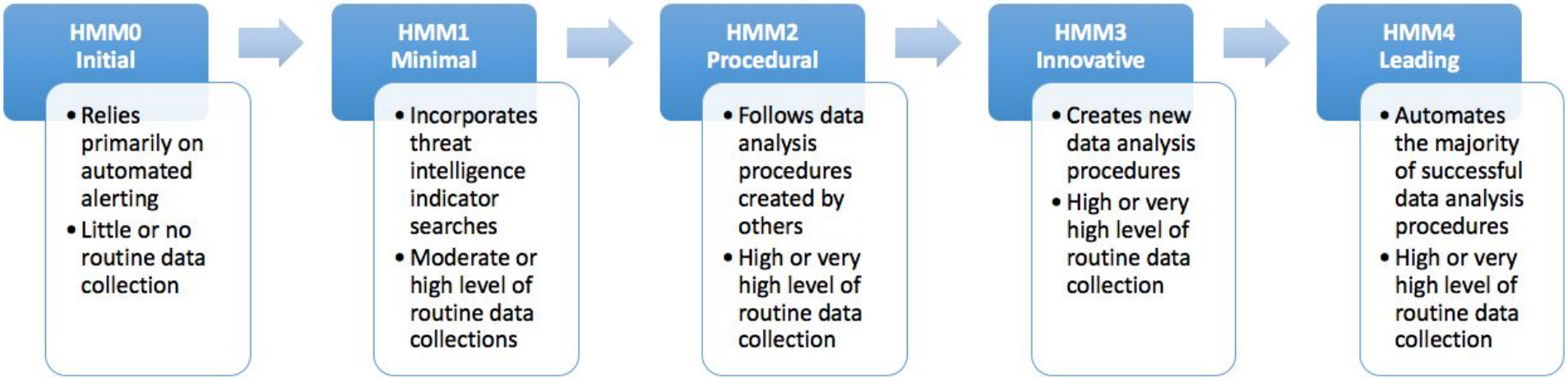
Doing cybersecurity work in personal time

- 7 subjects spoke positively of this as a metric for expertise
  - 4 potential expertise
  - 2 actualized expertise
  - 1 both potential and actual expertise
- 1 subject was critical of off the clock work **as a measure for expertise**

“I think it’s a good metric for passion. ... I think passion means you can go faster or advance faster. ... The person that’s just sitting on their computer, researching networks all night might get there faster than somebody that does it on clock. ”

Discussion and Future Work

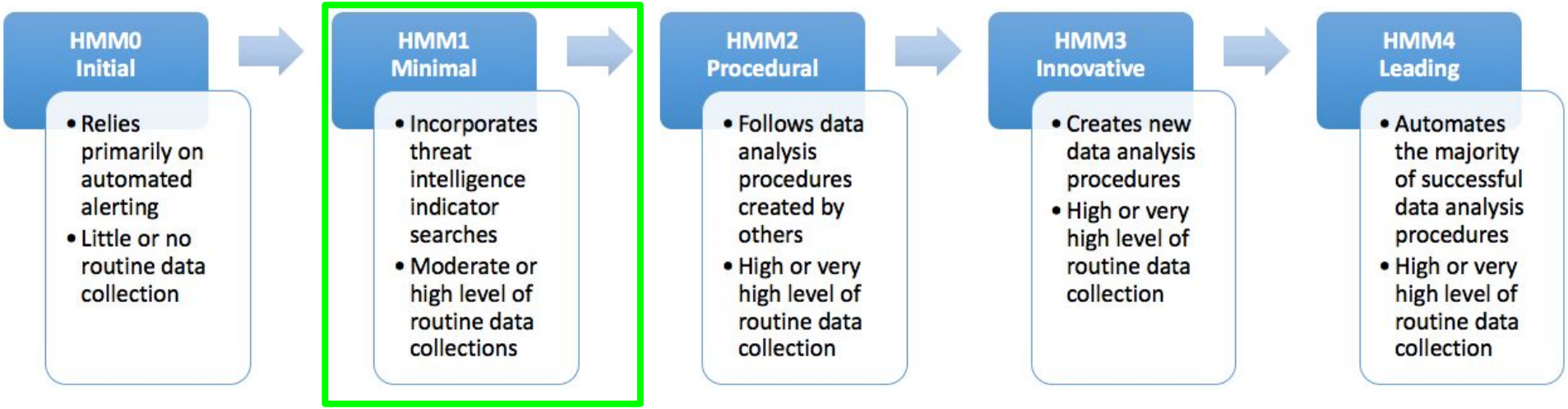
For Researchers: Process Evaluation



Source: D. Bianco, A Simple Hunting Maturity Model, en, Blog. [Online]. Available: http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html .

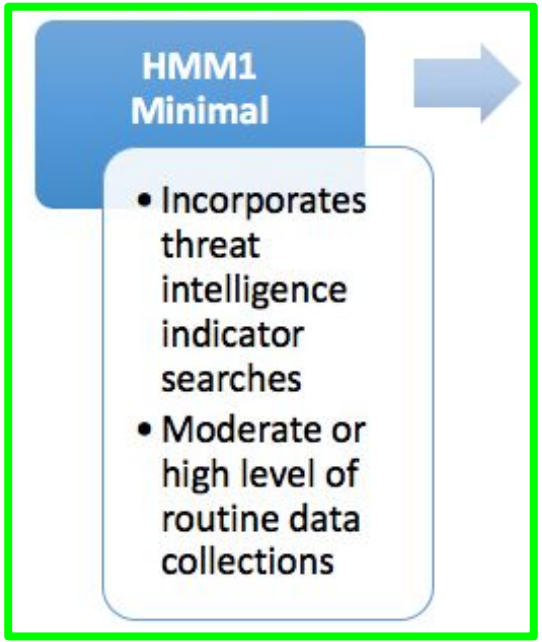
ELMORE FAMILY SCHOOL OF ECE

For Researchers: Cyber Threat Intelligence



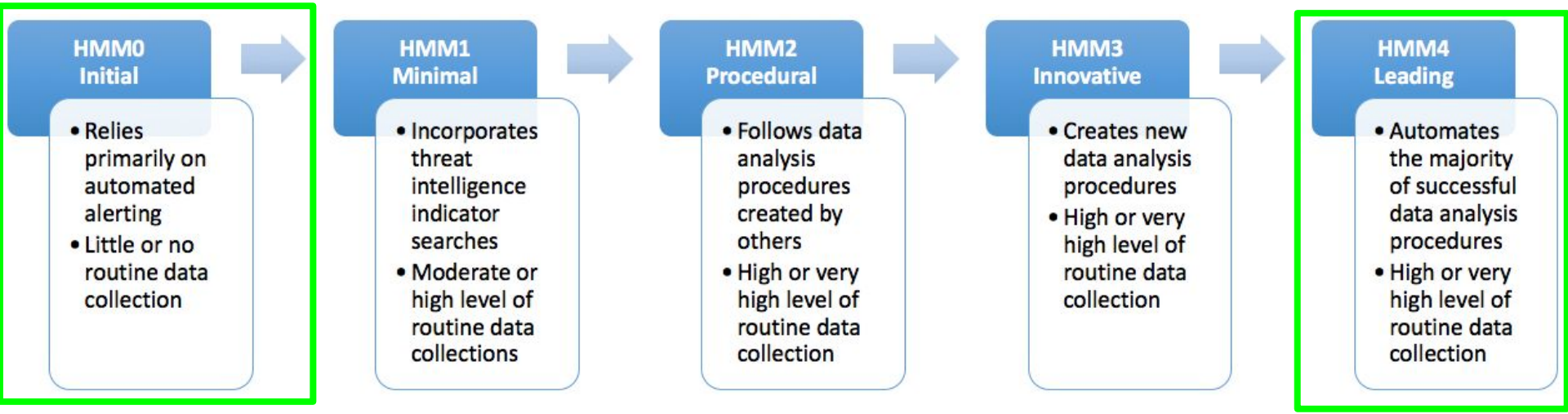
Source: D. Bianco, A Simple Hunting Maturity Model, en, Blog. [Online]. Available: http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html .

For Researchers: Cyber Threat Intelligence



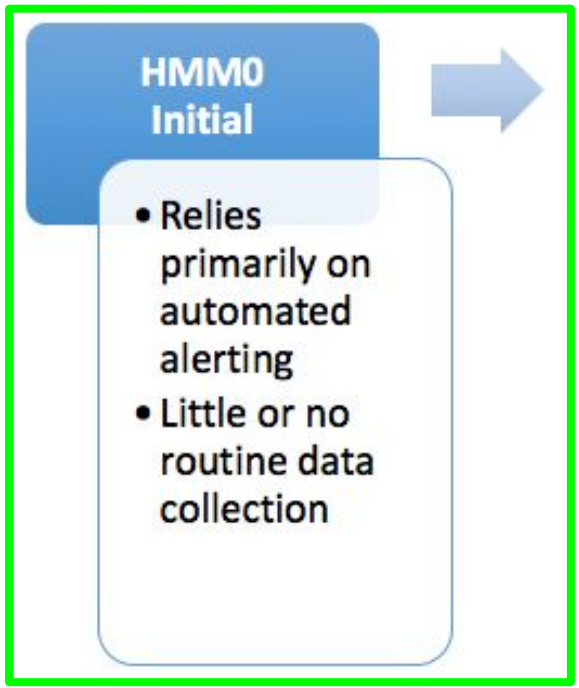
Source: D. Bianco, A Simple Hunting Maturity Model, en, Blog. [Online]. Available: http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html .

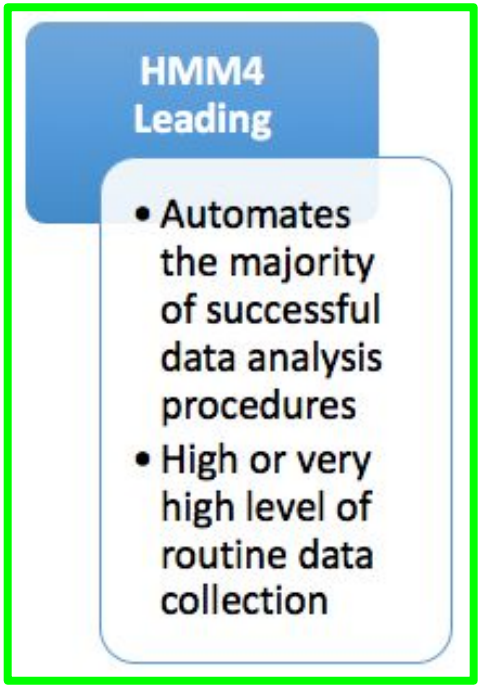
For Researchers: Develop Automation



Source: D. Bianco, A Simple Hunting Maturity Model, en, Blog. [Online]. Available: http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html .

For Researchers: Develop Automation





Source: D. Bianco, A Simple Hunting Maturity Model, en, Blog. [Online]. Available: http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html .

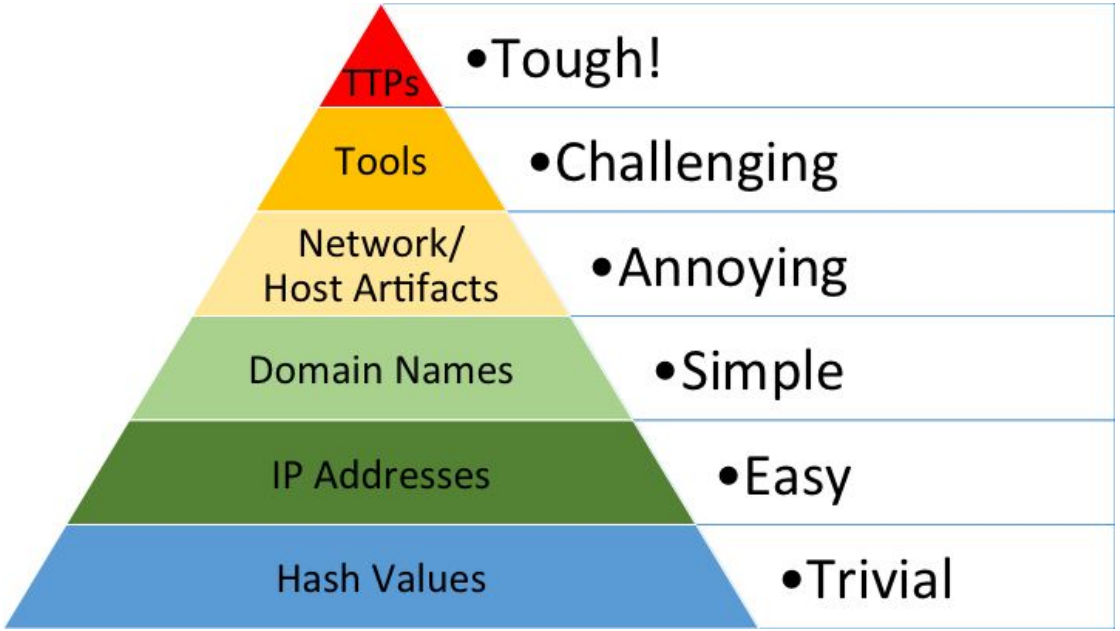
For Practitioners: Use TH Frameworks

TH Frameworks	# Subjects who used the framework (# of organizations)
Mitre ATT&CK	11 (3)
Hypothesis Checking	8 (3)
Lockheed's Kill Chain	3 (2)
Pyramid of Pain	2 (2)

For Practitioners: Use TH Frameworks

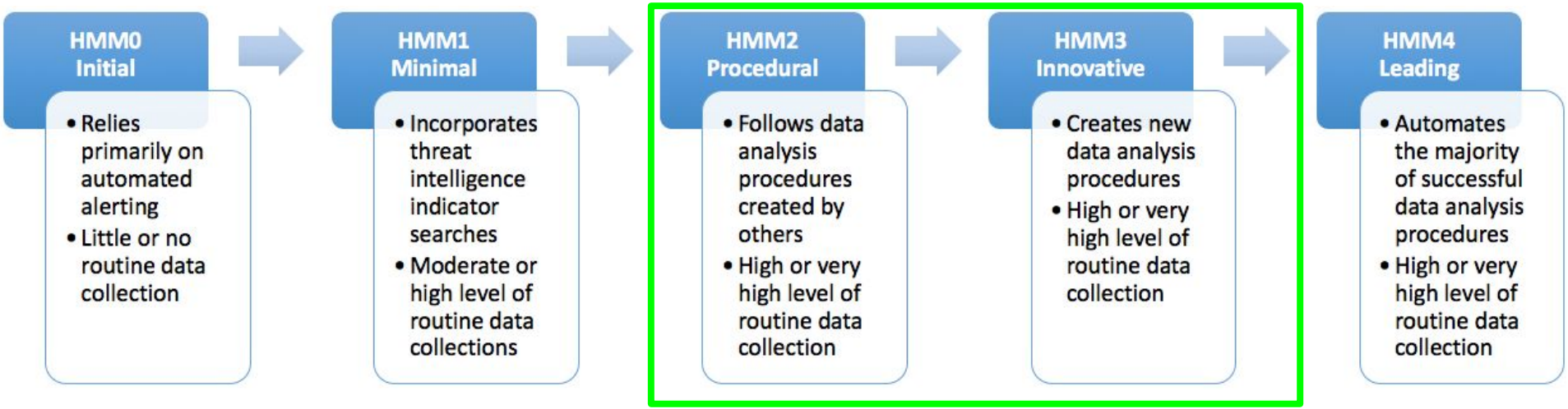
TH Frameworks	# Subjects who used the framework (# of organizations)
Mitre ATT&CK	11 (3)
Hypothesis Checking	8 (3)
Lockheed's Kill Chain	3 (2)
Pyramid of Pain	2 (2)

For Practitioners: Use TH Frameworks



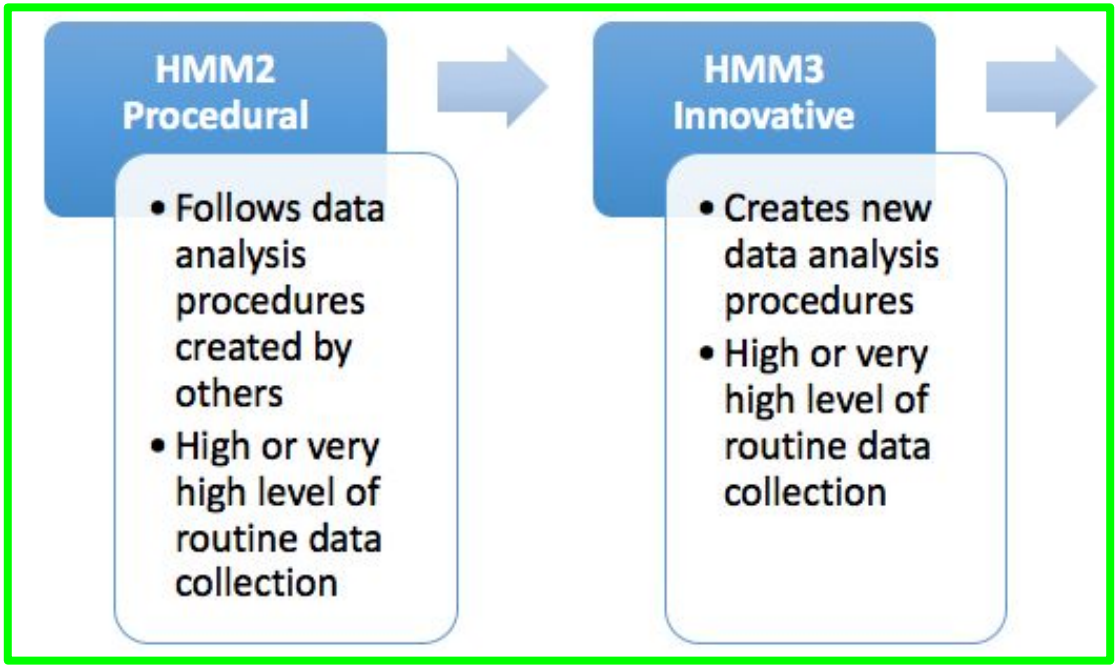
Source: Davidjbianco, Enterprise Detection & Response: The Pyramid of Pain, Mar. 2013. [Online]. Available: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html .

For Practitioners: Use TH Frameworks



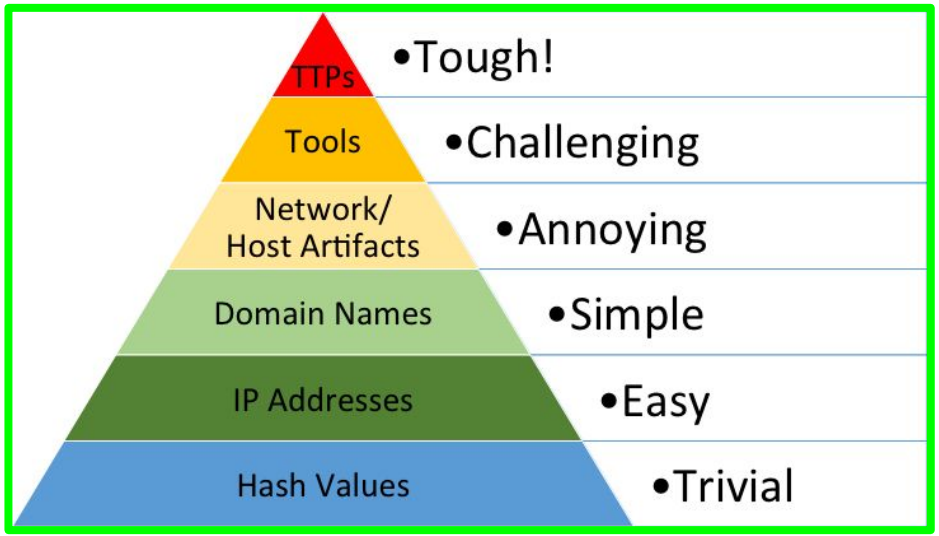
Source: D. Bianco, A Simple Hunting Maturity Model, en, Blog. [Online]. Available: http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html .

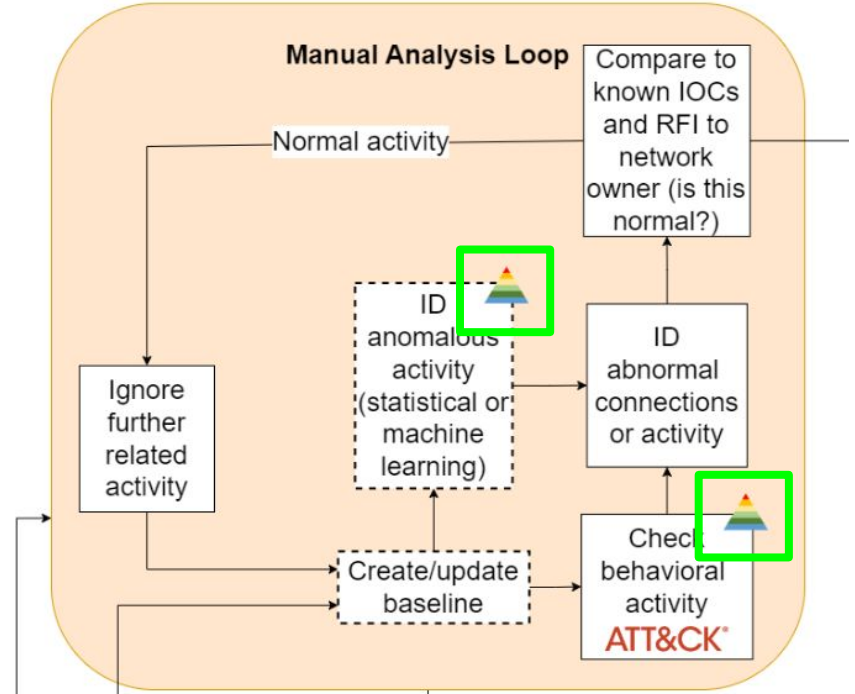
For Practitioners: Use TH Frameworks



Source: D. Bianco, A Simple Hunting Maturity Model, en, Blog. [Online]. Available: http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html .

For Practitioners: Use TH Frameworks

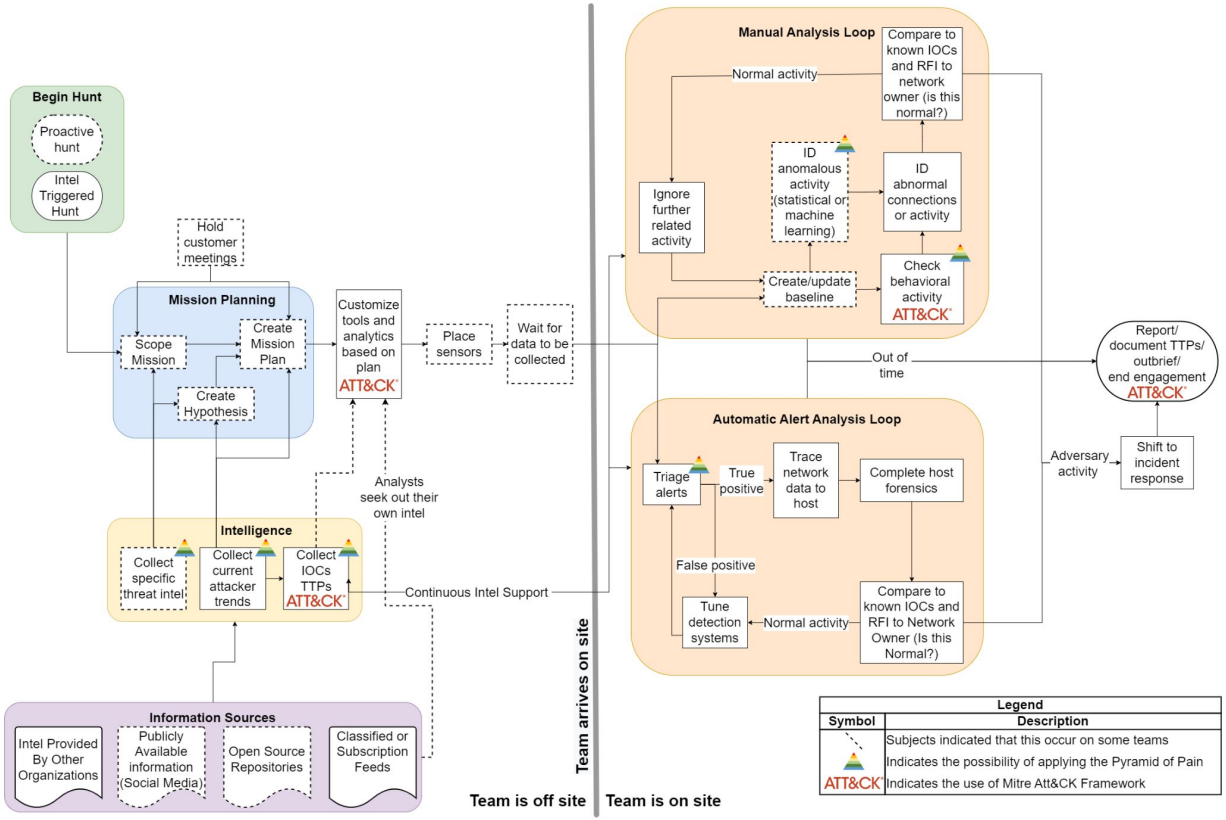




Source: Davidjbianco, Enterprise Detection & Response: The Pyramid of Pain, Mar. 2013. [Online]. Available: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html .

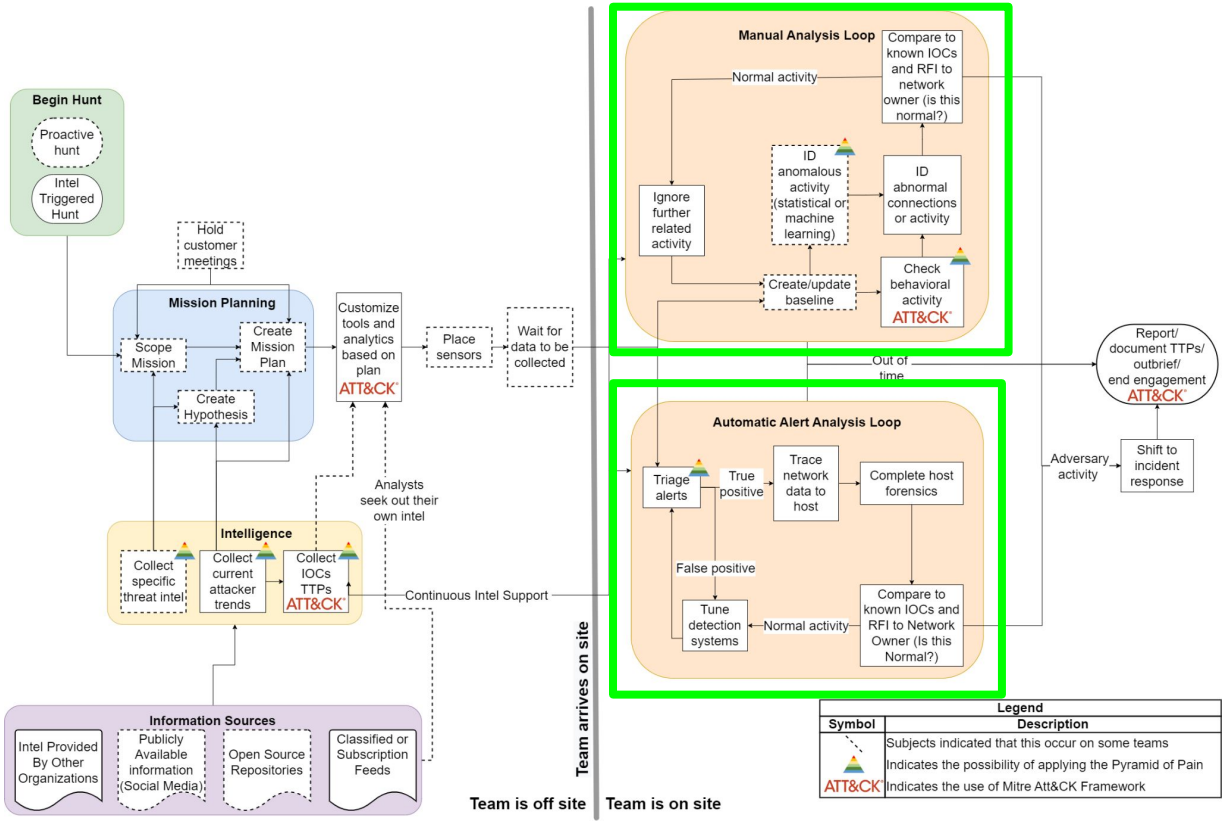
ELMORE FAMILY SCHOOL OF ECE

For Practitioners: Balance Resources



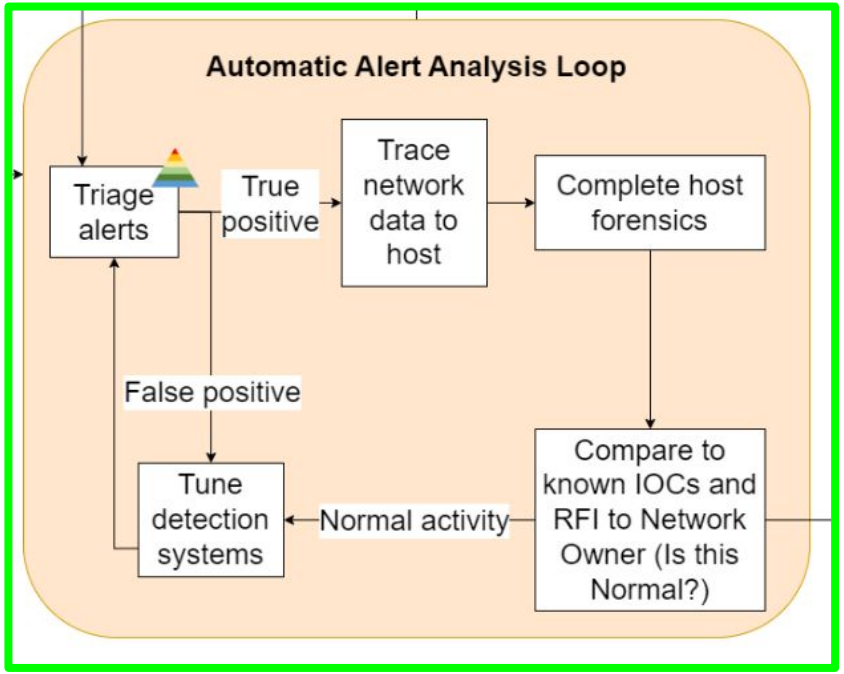
ELMORE FAMILY SCHOOL OF ECE

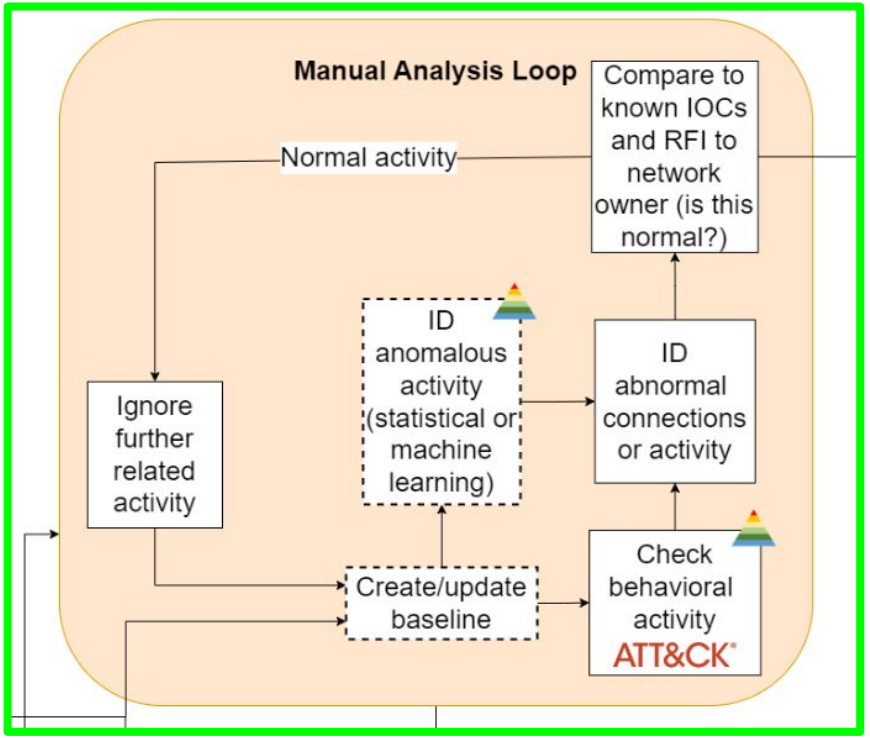
For Practitioners: Balance Resources



ELMORE FAMILY SCHOOL OF ECE

For Practitioners: Balance Resources



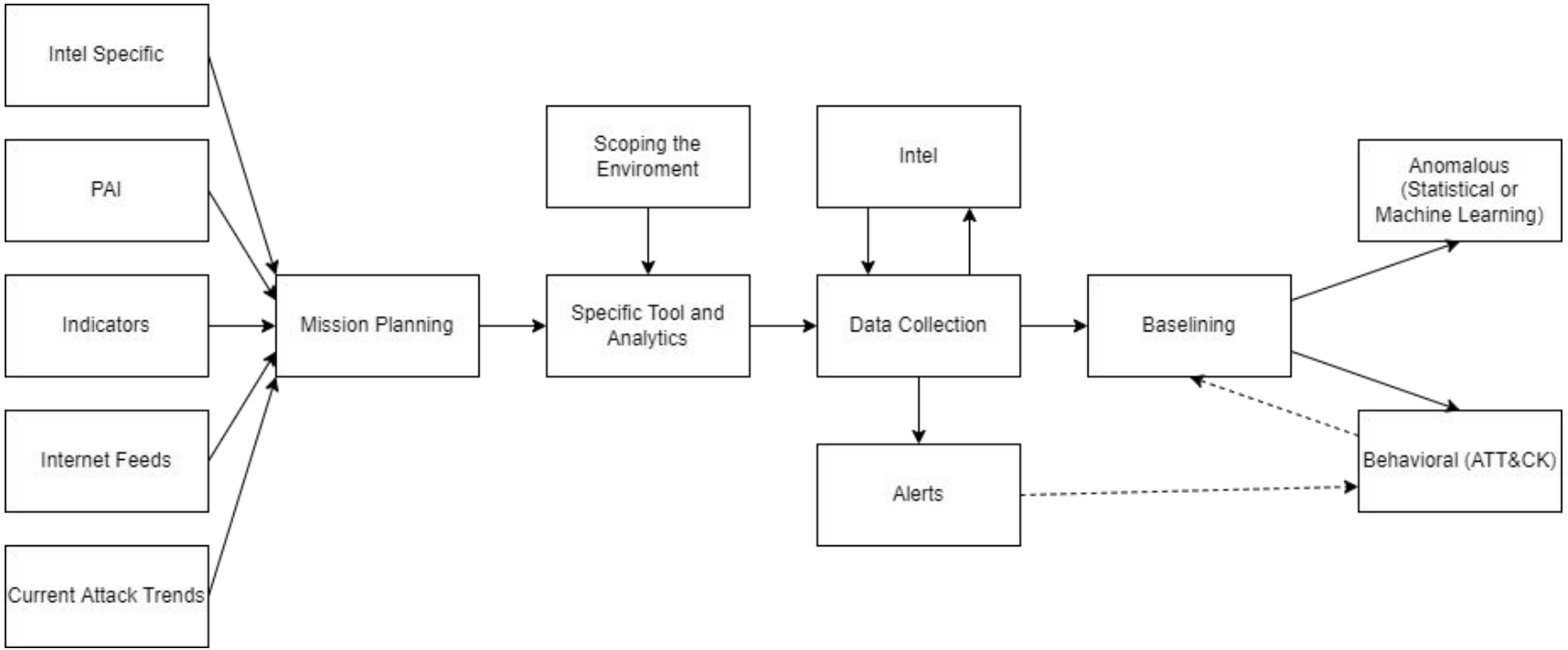


ELMORE FAMILY SCHOOL OF ECE

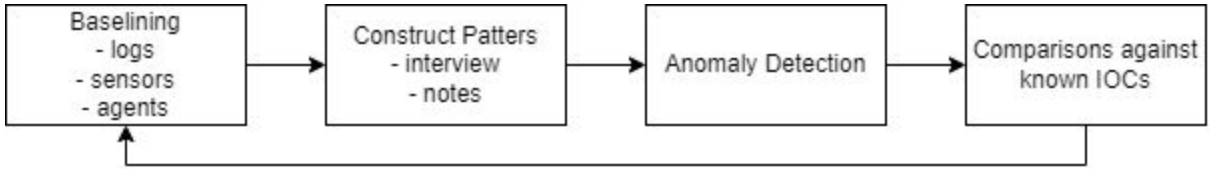
Questions?

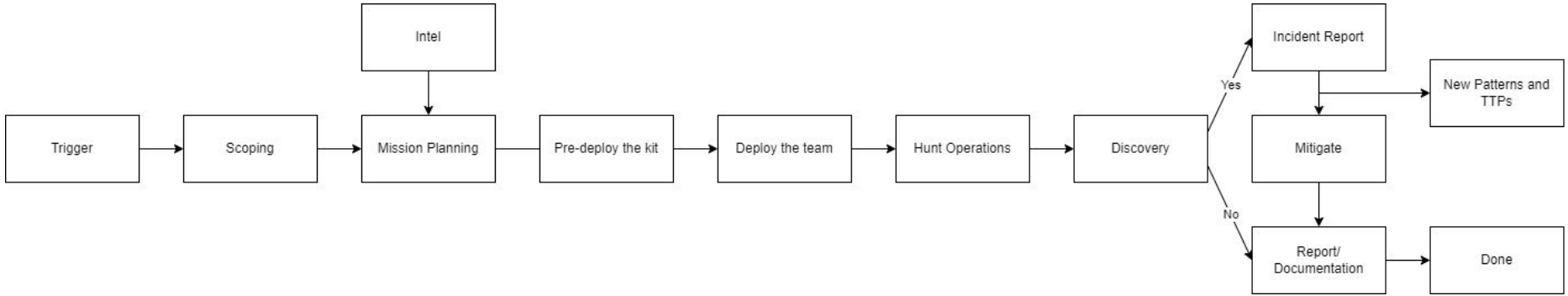
Thank you for your attention

Elmore Family School of Electrical and Computer Engineering

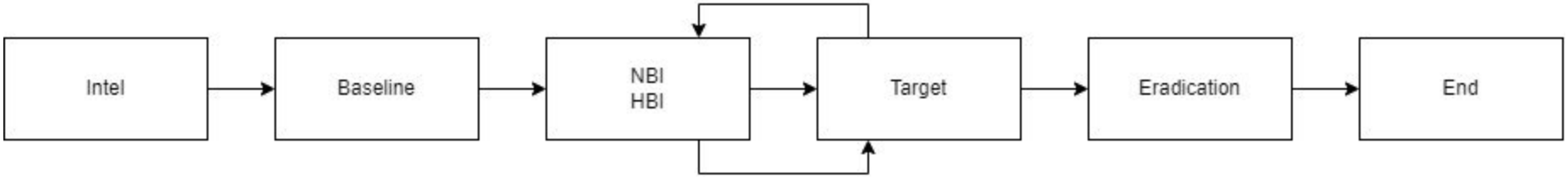


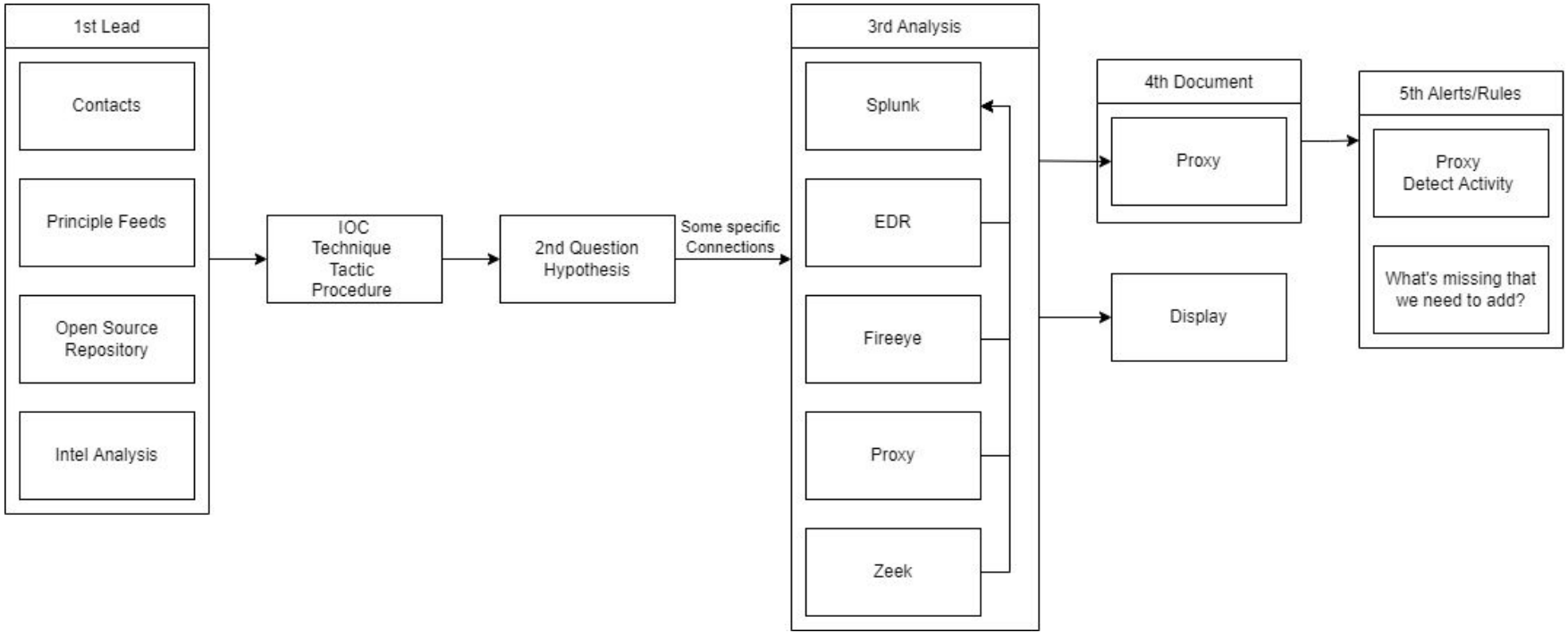
ELMORE FAMILY SCHOOL OF ECE


Baselining
- logs
- sensors
- agents
Construct Patters
- interview
- notes
Anomaly Detection
Comparisons against known IOCs

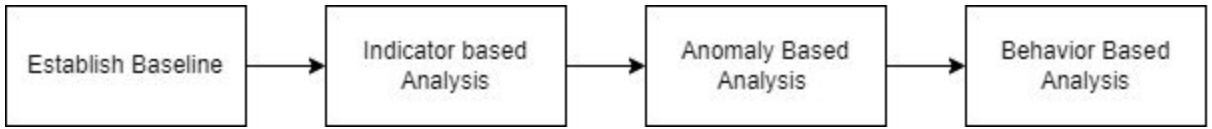


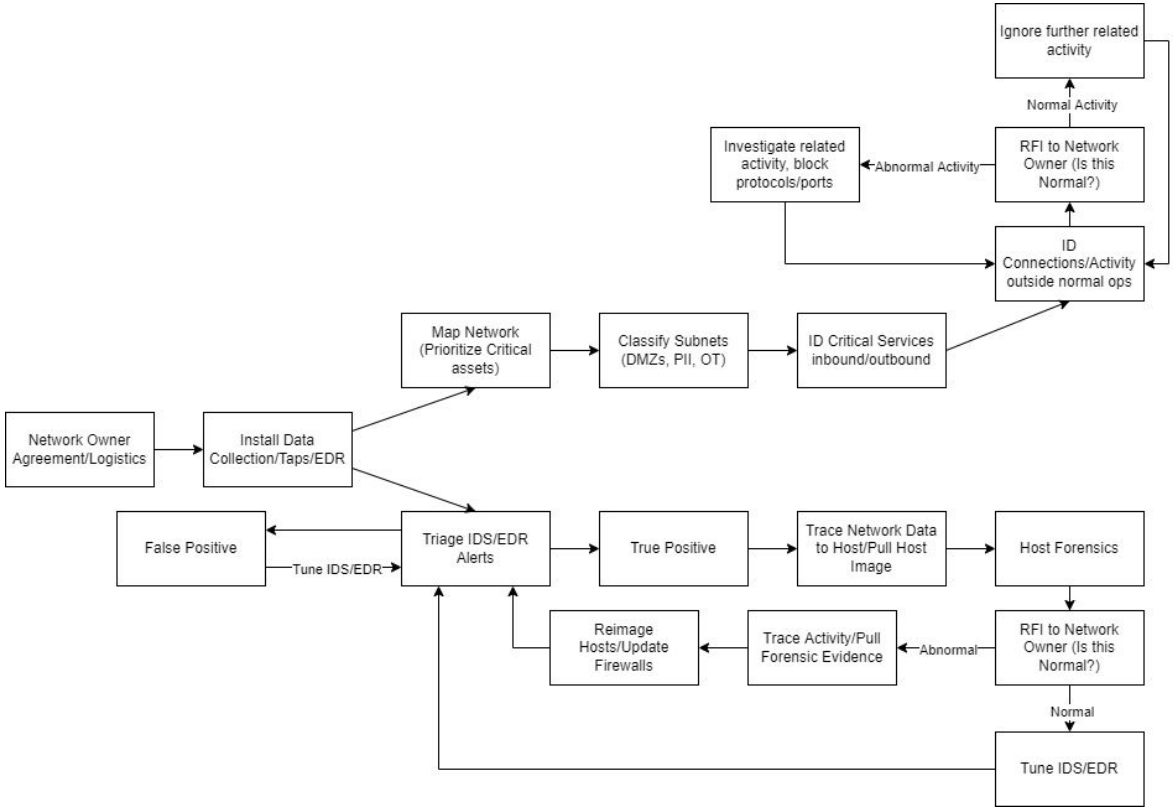
ELMORE FAMILY SCHOOL OF ECE


Intel
Baseline
NBI
HBI
Target
Eradication
End

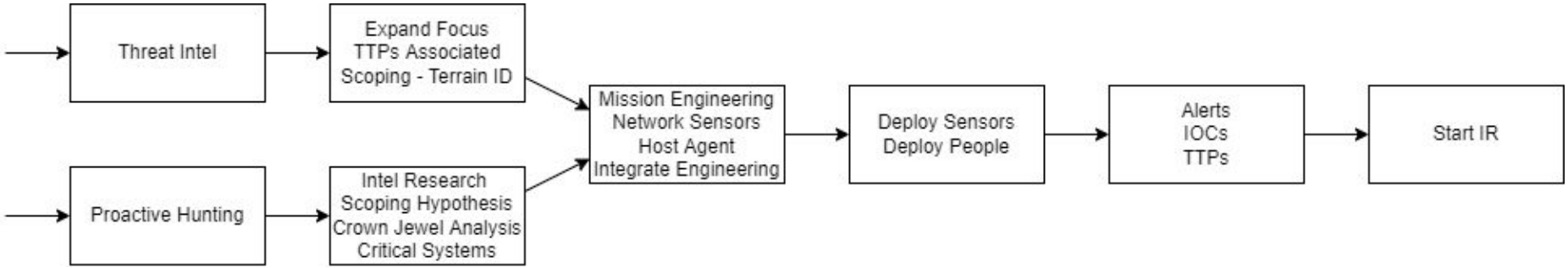


ELMORE FAMILY SCHOOL OF ECE


Establish Baseline
Indicator based Analysis
Anomaly Based Analysis
Behavior Based Analysis



ELMORE FAMILY SCHOOL OF ECE


Threat Intel
Expand Focus
TTPs Associated
Scoping - Terrain ID
Proactive Hunting
Intel Research
Scoping Hypothesis
Crown Jewel Analysis
Critical Systems
Mission Engineering
Network Sensors
Host Agent
Integrate Engineering
Deploy Sensors
Deploy People
Alerts
IOCs
TTPs
Start IR


Intel
APT
Past Activities
Customer Meetings
MTS Open Source Research/ Mitre
Sus. Processes/ Spreadsheet related to Mitre
End

ELMORE FAMILY
SCHOOL OF ECE


Baseline
Hunt and Report
Write Report