Threat Intelligence Applied

Fidelis® Cybersecurity

Intelligence: FuD

"…Our collective ignorance of intelligence has undermined not only our intelligence capabilities, but ultimately the policy makers and citizens served."

-Henry A. Crumpton ,*The Art of Intelligence: Lessons from a Life in the CIA's Clandestine Service*

"[Many] just think you can 'buy intelligence' or 'download intelligence' and don't realize they need to 'develop intelligence'."

-Scott Roberts, Director of Bad Guy Catching GitHub

Intelligence Defined

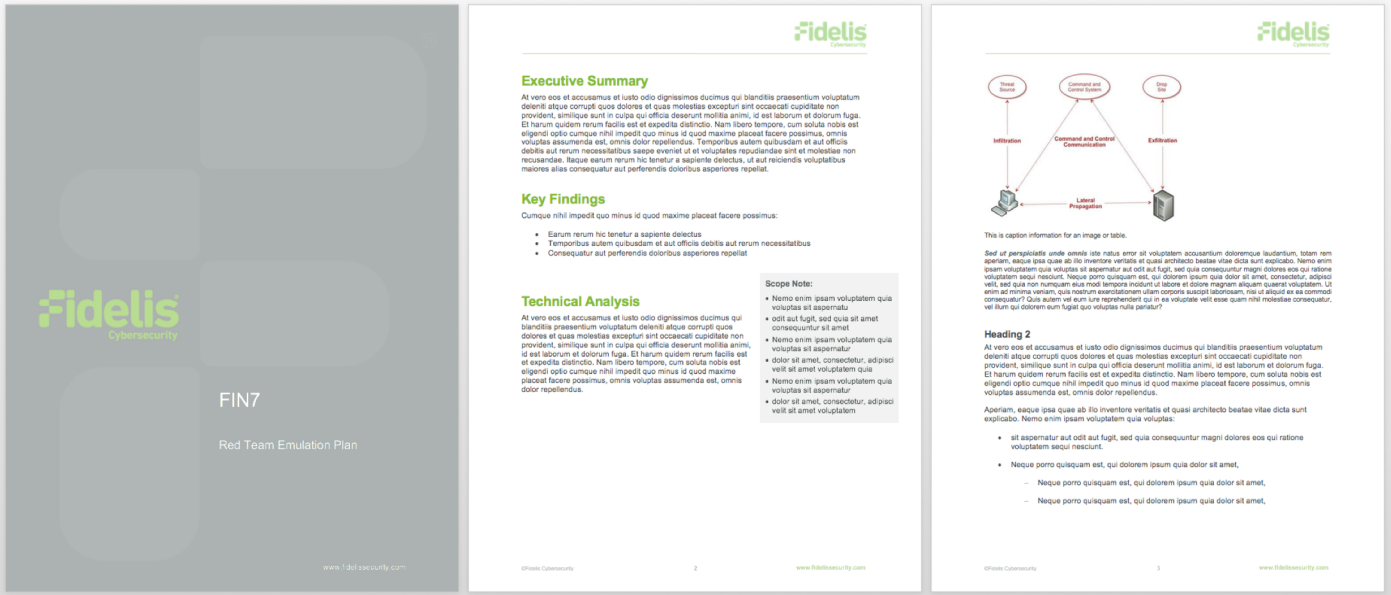
Threat Intelligence is the planning, collection, analysis and dissemination of information and countermeasures concerning threat and vulnerabilities provided to enhance the decision-making process.

Perform situation development
Provisioning of intelligence to support an understanding of the threat landscape.

Support organizational and asset protection
Determining top threats to the organization and providing countermeasures.

Provide indications and warning (I & W)
Used in the identification and prevention of vulnerabilities from being exploited, as well as informing operations of potential attacks.

Types of Intelligence

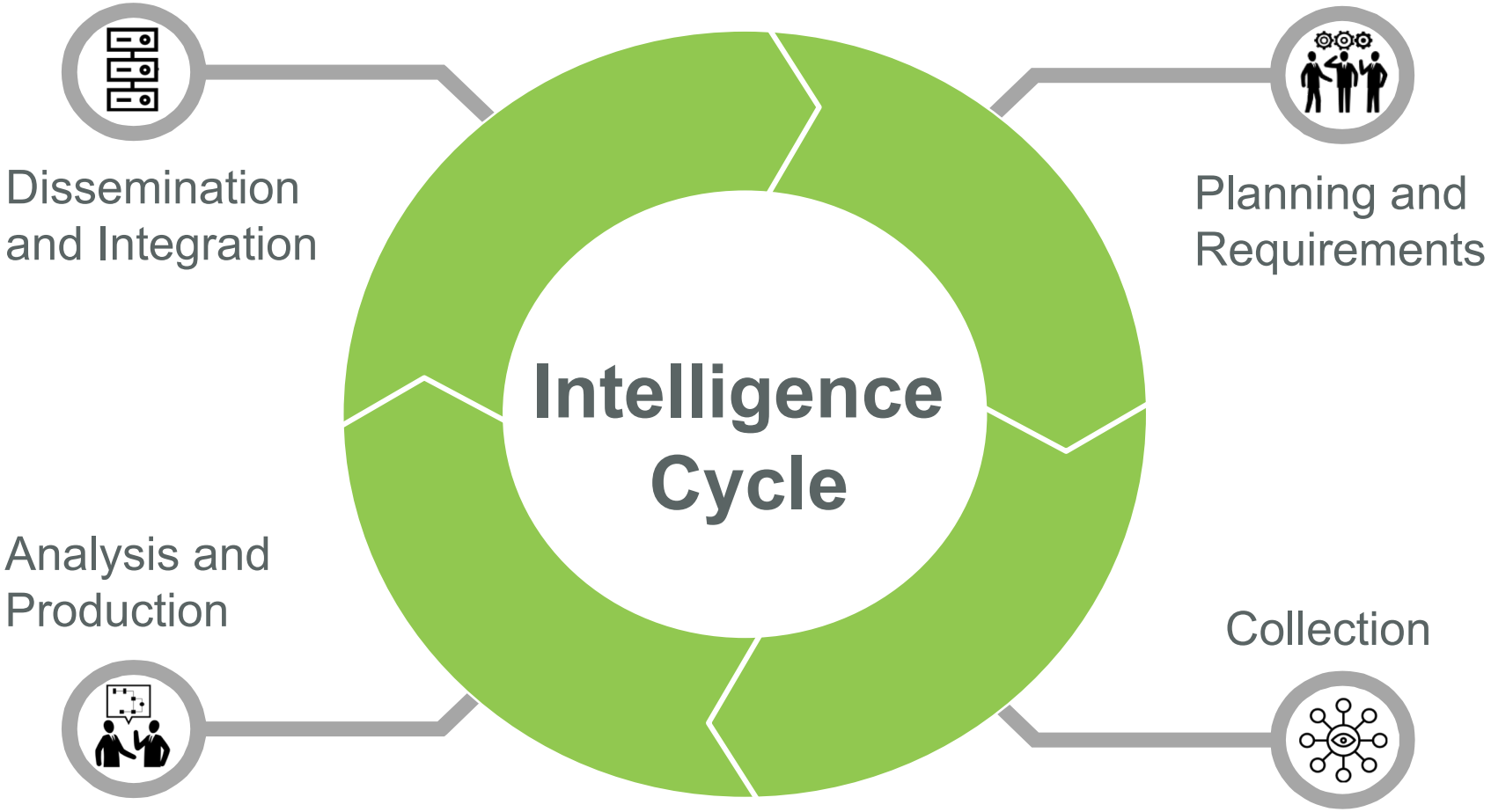


Basic Intelligence:
largely deals with past events and bringing them to present [describes / explains / evaluates / tracks]

Current Intelligence:
situationally designed to get relevant intelligence outbound to decision makers [describes / explains / evaluates current events]

Estimative Intelligence:
used to prepare decision makers for future threats / events [predictive / more strategic]

The Process



Requirements: 4 Qualities

Necessity:
How important is this requirement to supporting the risk reduction of the firm?

Feasibility:
What is the likelihood, in the current environment, that this requirement can be successfully filled?

Timeliness:
What is the likelihood, in the current environment, that this requirement can be successfully filled in a timely manner such that the firm can act on the information to reduce risk?

Specificity:
How specific is the requirement? This refers to the information being asked for and how concrete the request is relative to others.

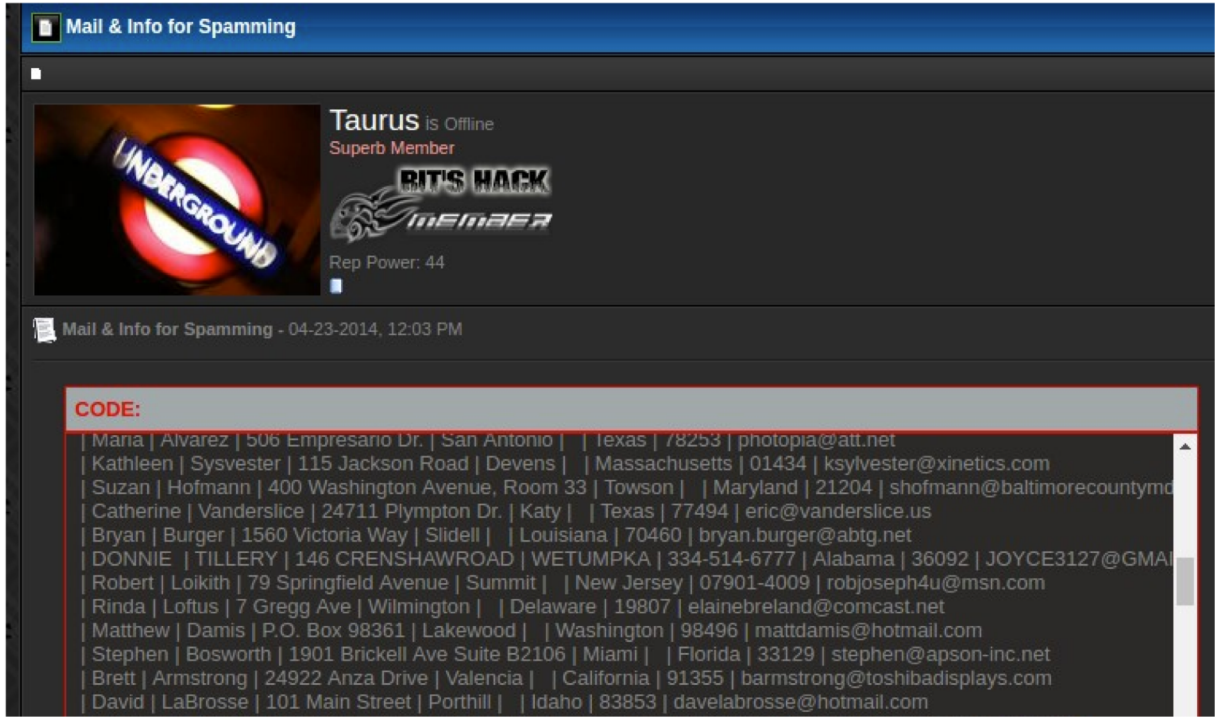
Stakeholder:
IT Support / Security Analyst

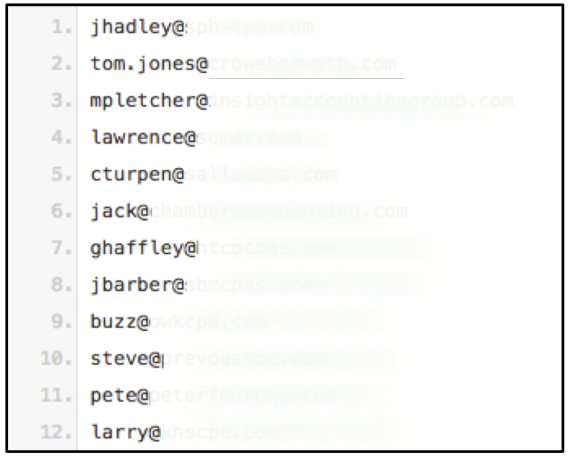
Blue Sky:
"I would like to know when an end user is on a target list so we can better detect when they will be phished to provide extra security awareness training and lower the risk."

Converted:
Are our employees on target lists?

Collect

With or Without Credentials?





Analyze

Analysis and Production

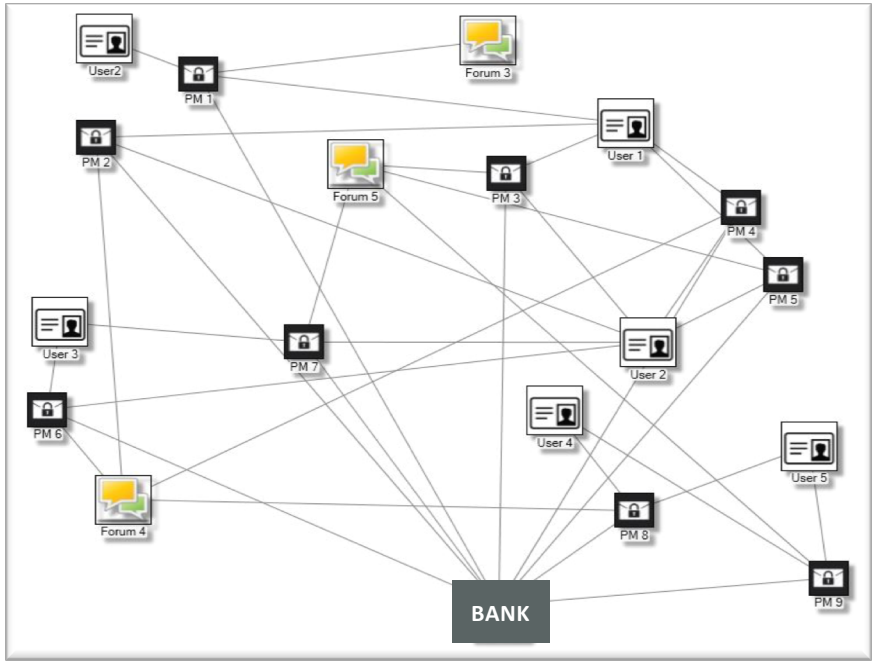
Have sources reported reliably in the past?

Is the collection legitimate?

Who is the consumer?

What templates do we use to disseminate?

Based on severity and timeliness, do we escalate prior to full analysis?



UID/PW

Disseminate

Use the BatPhone

=

Great Success!

CTI Operations

Intelligence Requirement

- Are our employees on target lists?

Collection Requirements

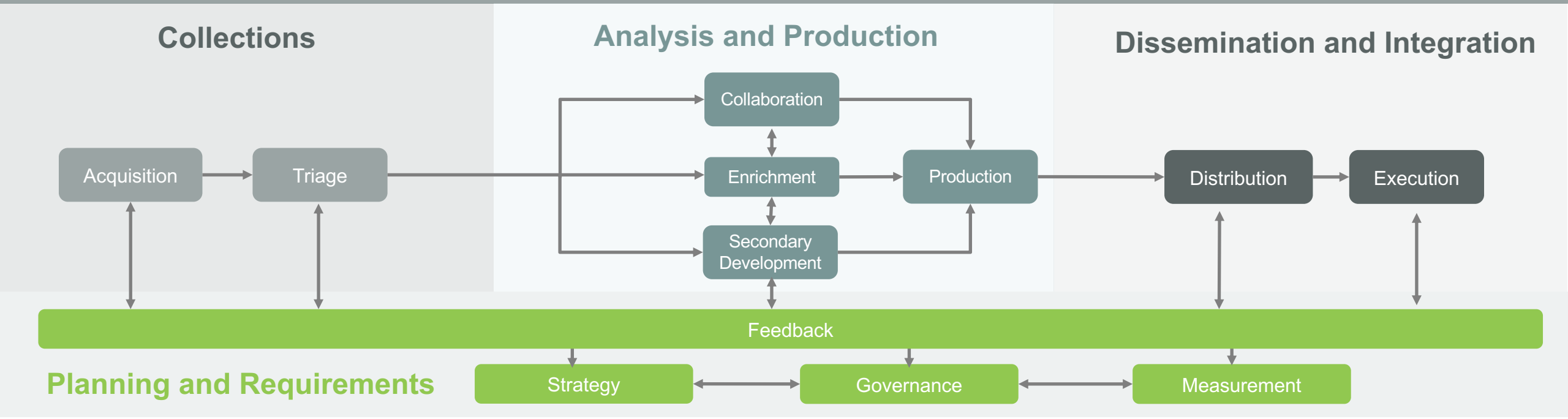
- Which sources collect against paste sites / breach dumps?
- How often are we targeted by phishing?

Production Requirements

Stakeholder:
IT Support / Security Analyst

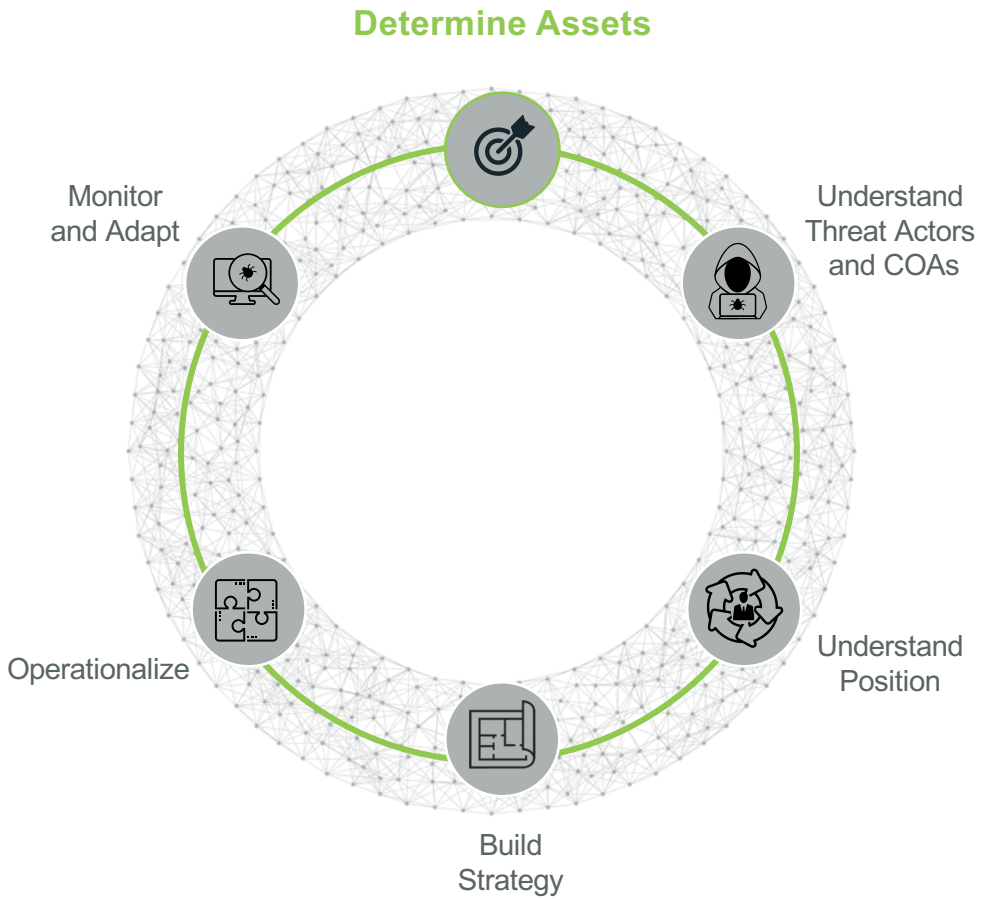
Product:
Direct notifications to IT Support / Security Analyst via ticketing system

Cadence:
Continuous



Intelligence Requirements Define intelligence needed by the decision maker | Example: "*Are our employees on target lists?*"

Let’s Imagine



Who are we?

Large Financial Institution

What type of historic incidents can we pull from?

63% of incidents happen via phishing

CTI Operations

Intelligence Requirements

- Which threat actors target Banking & FinServe within North America?
- What are their tools, tactics and courses of action?

Collection Requirements

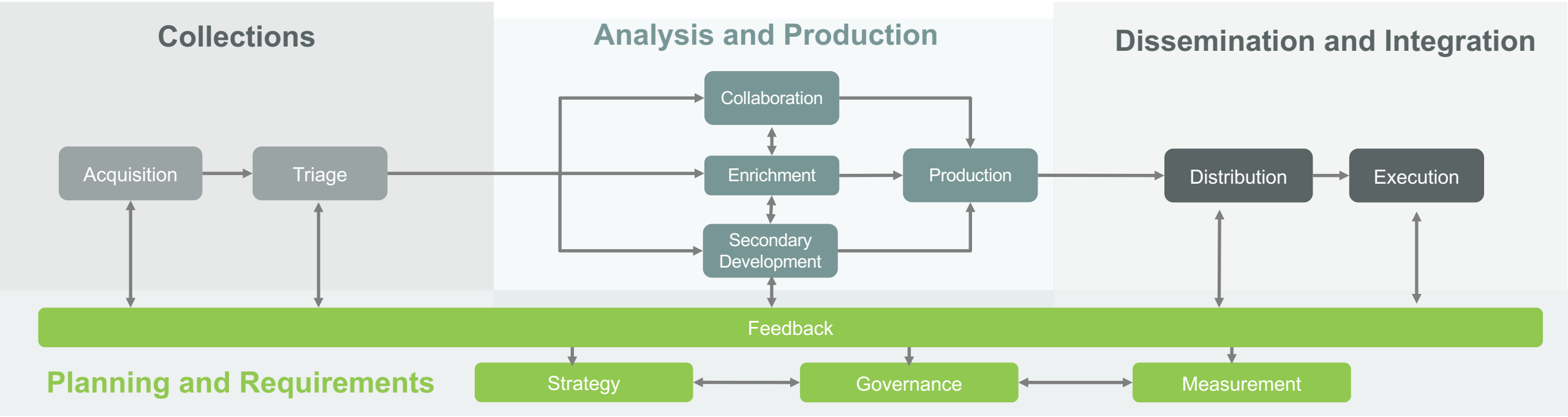
- Sources which collect against threat actors.
- High-fidelity / vetted sources.
- Include TTPs and intent

Production Requirements

Stakeholder:
Red Team

Product:
Finished Intelligence: brief and long form format detailing actor history and known COAs

Cadence:
Upon request



Threat Actor ID

Intelligence Requirements

- Which threat actors target Banking & FinServe within North America?
- What are their tools, tactics and courses of action?

Collection Requirements

- Sources which collect against threat actors.
- High-fidelity / vetted sources.
- Include TTPs and intent

Production Requirements

Stakeholder:
Red Team
Product:
Finished Intelligence: brief and long form format detailing actor history and known COAs
Cadence:
Upon request

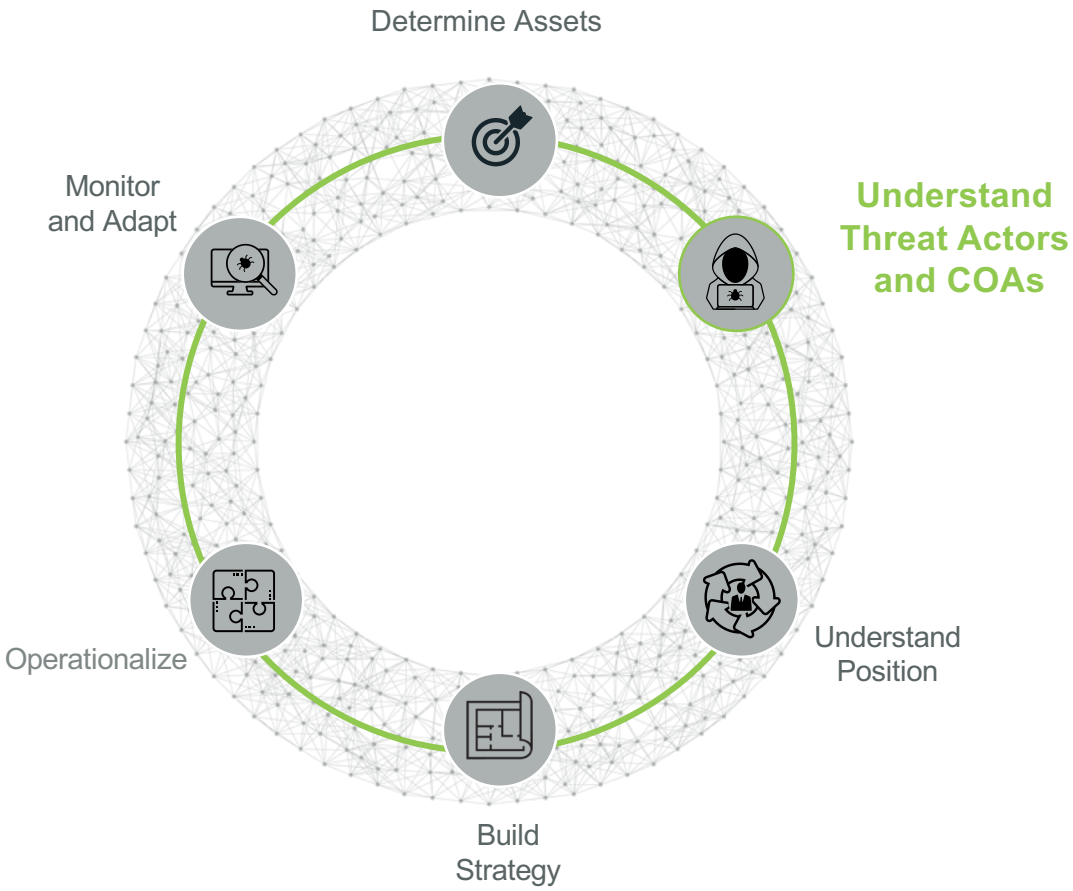
Threat Actors

Group of attackers or an individual actor that has the means, and opportunity to conduct an attack.

Other Considerations

Composition and Strength: can we determine if the threat agent is a group or individual, and if a group, do we have association
Tactics: do we have intelligence on historical courses of action
Logistics: what does their infrastructure look like; command and control servers; potential nation-state sponsored or well funded
Effectiveness: are their previously or historically identified successful attacks; how effective were they

Let's Pontificate



Which well known Threat Actor utilizes phishing for initial compromise?

FIN7

Have they targeted my vertical in the past?

Yes – SEC Filing Campaign (FEB 2017)

Threat Actor ID: FIN7

Intelligence Requirements

- Which threat actors target Banking & FinServe within North America?
- What are their tools, tactics and courses of action?

Collection Requirements

- Sources which collect against threat actors.
- High-fidelity / vetted sources.
- Include TTPs and intent

Production Requirements

Stakeholder:
Red Team
Product:
Finished Intelligence: brief and long form format detailing actor history and known COAs
Cadence:
Upon request

FIN7

FIN7 is an advanced financially motivated group that has been conducting operations since as early as 2015. The group is often combined with the Carbanak Gang due to the shared usage of the Carbanak malware family, but this fact has been disputed due to different TTPs utilized by the groups. The group has historically targeted retail and hospitality companies utilizing specially crafted spear-phishing campaigns for their initial infection. Once inside of a victim's network, the actors utilize APT-like behaviors to maintain and expand their foothold until they have the information or ability to complete their goals. The group has utilized point-of-sale malware in many of their operations as well, scraping credit card data from unsuspecting customers of their targets.

The structure and origination of the group has been heavily debated in the security industry. In some of their most recent campaigns the use of the Cyrillic charset has been used, which may indicate Russian or Eastern European origin. The group appears to be very organized in their operations, and the scale and speed at which they adapt and change their TTPs indicates that FIN7 could be a large-scale cybercrime ring. The group has also been identified running many large campaigns at once indicating possible separation, or operating cells within the group itself.

Key Judgements

- FIN7 is a highly advanced financially motivated group utilizing APT-like techniques
- FIN7 activity will continue and potentially increase based on 2016 & 2017 activity
- FIN7 will continue to evolve and change their TTPs to evade and elude detection techniques in order to maintain footholds within networks

Threat Actor TTPs and COAs

Intelligence Requirements

- Which threat actors target Banking & FinServe within North America?
- What are their tools, tactics and courses of action?

Collection Requirements

- Sources which collect against threat actors.
- High-fidelity / vetted sources.
- Include TTPs and intent

Production Requirements

Stakeholder:
Red Team
Product:
Finished Intelligence: brief and long form format detailing actor history and known COAs
Cadence:
Upon request

Courses of Action

Threat actor courses of action can be described as attack patterns or kill chains. Based off of historical patterns, and actor means and intent, the threat modeler can develop templates for anticipated courses of action that will be undertaken to meet the attacker's objective.

Threat Actor TTPs and COAs: FIN7

Intelligence Requirements

- Which threat actors target Banking & FinServe within North America?
- What are their tools, tactics and courses of action?

Collection Requirements

- Sources which collect against threat actors.
- High-fidelity / vetted sources.
- Include TTPs and intent

Production Requirements

Stakeholder:
Red Team
Product:
Finished Intelligence: brief and long form format detailing actor history and known COAs
Cadence:
Upon request

FIN7: Intent

- Financial Motivation
- Data Theft

FIN7: Malware

- PowerSource
- TextMate
- Carbanak
- HalfBaked

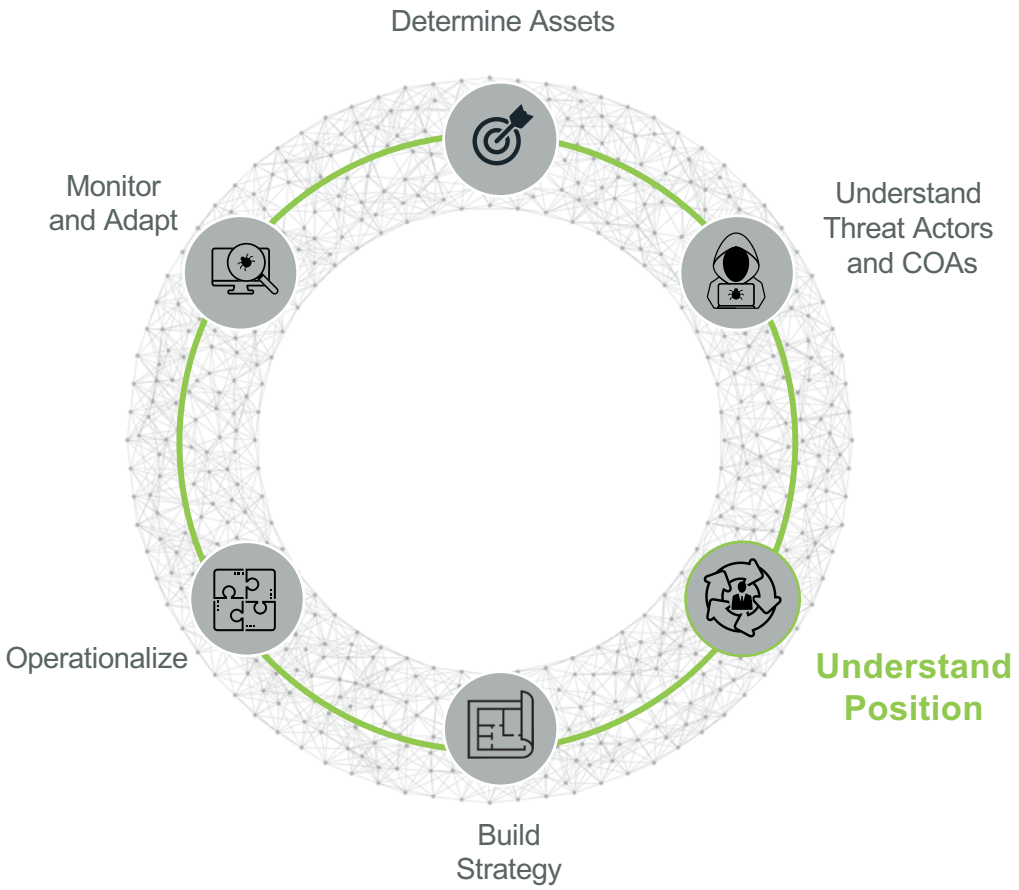
FIN7: Techniques

- **PowerShell** - FIN7 uses a PowerShell script to launch shellcode that retrieves an additional payload.
- **Remote File Copy** - FIN7 uses a PowerShell script to launch shellcode that retrieves an additional payload.
- **Scheduled Task** - FIN7 malware has created scheduled tasks to establish persistence.
- **Registry Run Keys / Start Folder** - FIN7 malware has created a Registry Run key pointing to its malicious LNK file to establish persistence.
- **Masquerading** - FIN7 has created a scheduled task named “AdobeFlashSync” to establish persistence.
- **Application Shimming** - FIN7 has used application shim databases for persistence.
- **Dynamic Data Exchange** - FIN7 spear phishing campaigns have included malicious Word documents with DDE execution.
- **Mshta** - FIN7 has used mshta.exe to execute VBScript to execute malicious code on victim systems.

Threat Actor TTPs and COAs: FIN7

Recon	• Specially crafted emails in a spear-phishing campaign with attached documents
Lure	• Documents contained embedded .LNK files with text to entice users to run the object
Exploit Executed	• Embedded .LNK objects kick off JavaScript chain pulled from a word document object using wscript.exe
Inject Through Backdoor	• File dropped on disk at %HOMEPATH%\md5.txt to be run with wscript.exe
Establish Command and Control	• JavaScript runs to decode the components and schedules a task to maintain persistence in some cases • Once JavaScript has been decoded, a PowerShell script is decoded and placed on disk at %HOMEPATH%\(Randomly generated GUID) along with the JavaScript bot components • PowerShell script is run and spawns a second PowerShell process • Second PowerShell decodes and decompresses a hardcoded DLL in memory and reflectively injects the library into its own process
Explore and Move	• Malware scrapes known directories for usernames and encrypted passwords on disk before decrypting the passwords • Code encrypts the data with a simple obfuscation technique and stores the information at %APPDATA%\%USERNAME%.ini
Data Theft	• The file is uploaded to one of the hardcoded C2 servers

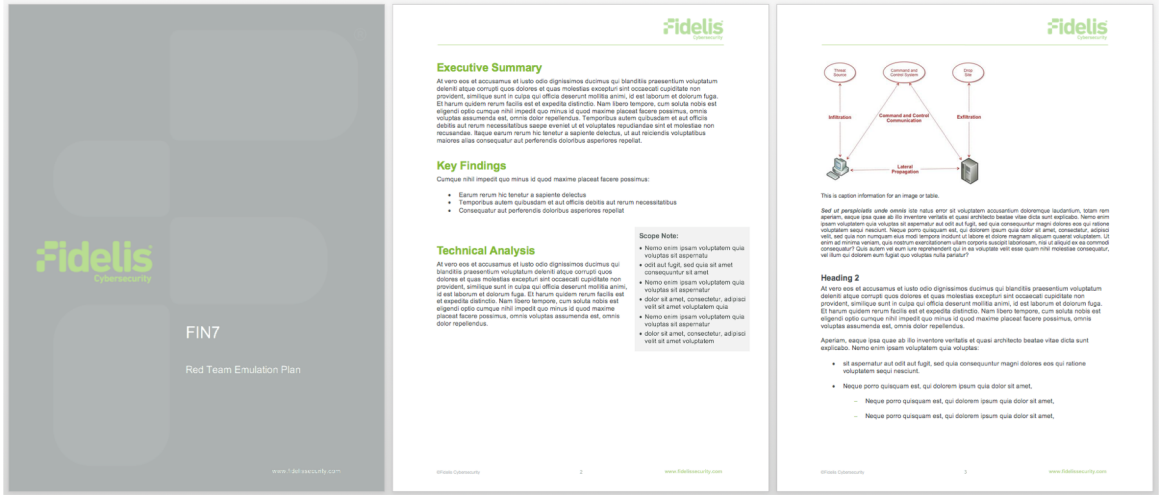
Let's Drive



Production Requirements

Stakeholder: Red Team

Product: Finished Intelligence: brief and long form format detailing actor history and known COAs
Cadence: Upon request



Example Sources

- IntSights RESEARCH module
- MITRE ATT&CK Framework
- FireEye APT Groups
- APT THREAT TRACKING community
- Diamond Model for analysis

Take Away & Questions

Talk To Your Stakeholders

Get Good Requirements

Check Your Collections

Products To The Right Consumers

Danny Pickens
danny.pickens@fidelissecurity.com
@dannypickens

threatgeek.com
fidelissecurity.com

Resources

Professional Resources

- Joint Publication JP 2-01: Joint and National Intelligence Support to Military Operations
- U.S. Army ADRP 2-0: Intelligence
- Intelligence and National Security Alliance (INSA) Whitepapers
- MITRE ATT&CK: Threat Modeling and Controls

Books

- “Psychology of Intelligence Analysis”, Richards Heuer Jr.
- “The Art of Intelligence: Lessons from a Life in the CIA’s Clandestine Service”, Henry A Crumpton
- “Killer Elite”, Michael Smith
- “Silent Warfare: Understanding the World of Intelligence”, Abarm Shulsky
- “Left of Bang: How the Marine Corps’ Combat Hunter Program Can Save Your Life”, Patrck Van Horne
- “Open Source Intelligence Techniques – 3rd Edition”, Michael Bazzell