578.1
Cyber Threat Intelligence and Requirements

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

578.1
Cyber Threat Intelligence and Requirements

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

Author Information:

Robert M. Lee (Lead Author)

Robert M. Lee is the CEO and Founder of the critical infrastructure cyber security company Dragos, Inc. where he and his team develop ICS cyber security products, ICS threat hunting and incident response, and produce cyber threat intelligence for the industrial industry. He is a SANS Certified Instructor and the course author of SANS ICS515 - "Active Defense and Incident Response" and the co-author of SANS FOR578 - "Cyber Threat Intelligence." Robert is also a non-resident National Cyber Security Fellow at New America focusing on policy issues relating to the cyber security of critical infrastructure and a PhD candidate at Kings College London. For his research and focus areas, he was named one of Passcode's Influencers, awarded EnergySec's 2015 Cyber Security Professional of the Year, and inducted into Forbes' 30 Under 30 in 2016 as one of the "brightest entrepreneurs and change agents" in technology.

Robert obtained his start in cyber security in the U.S. Air Force where he served as a Cyber Warfare Operations Officer in the U.S. Intelligence Community. He has performed defense, intelligence, and attack missions in various government organizations including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles in publications such as Control Engineering and the Christian Science Monitor's Passcode and speaks at conferences around the world. Lastly, Robert is author of the book "SCADA and Me" and the weekly webcomic http://www.LittleBobbyComic.com

Robert may be found on Twitter @RobertMLee or contacted via email at RLee@Dragos.com

Be Social!

#FOR578

Use the hashtag to communicate about the class, cool new findings, reports, tools, and more to share with your growing community

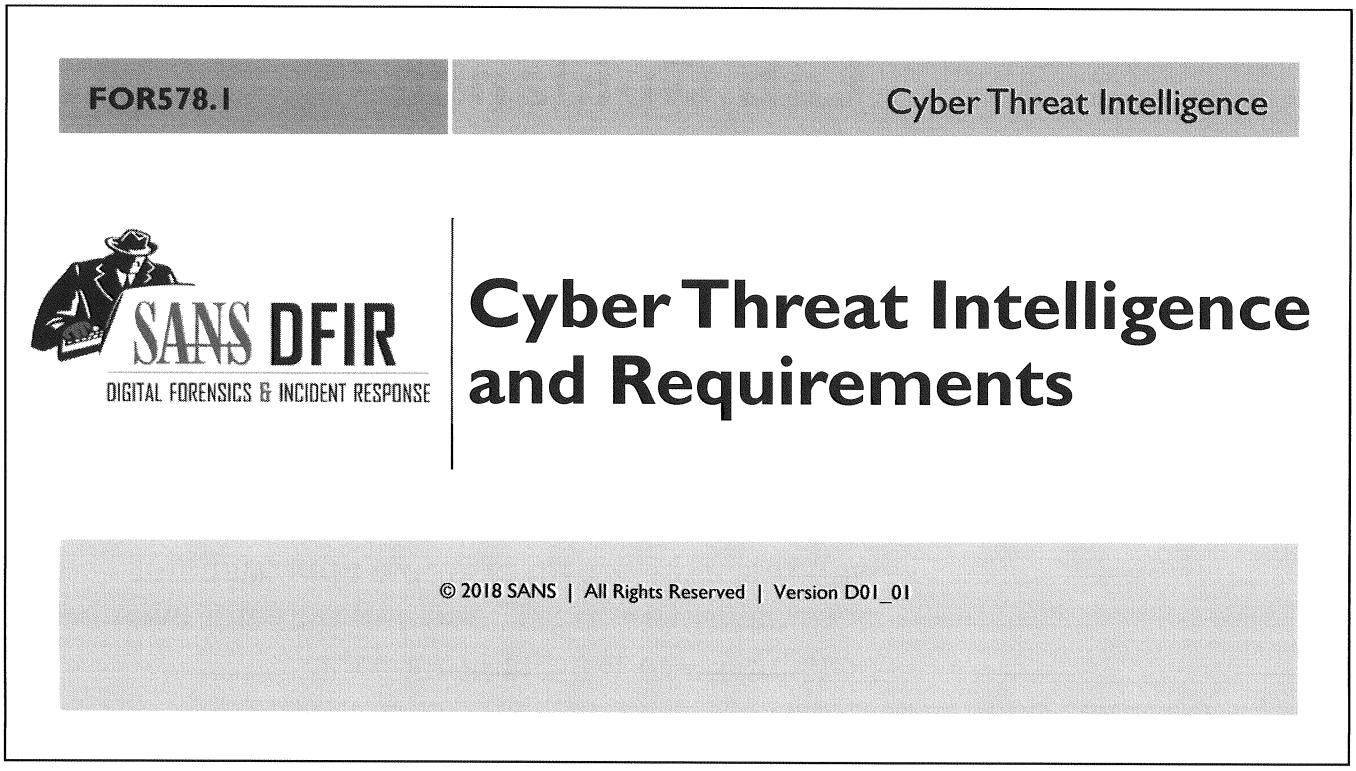
Also, each SANS event has a hashtag to communicate about evening events and socials

This page intentionally left blank.

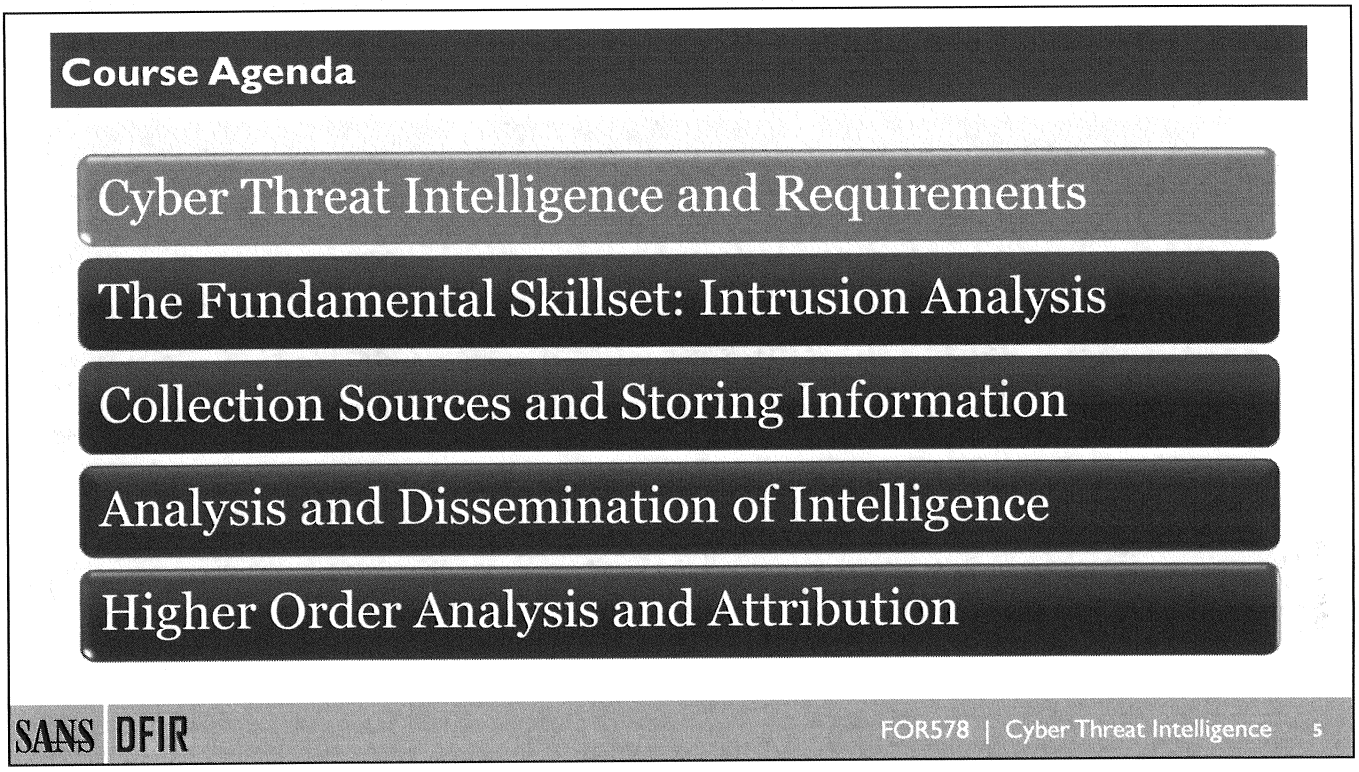
Lab Guidance

This is a course to help develop your analyst skills; the point of the labs are to provide structured analysis training more than learning specific tools. There are some labs that query or use online data/tools. In those labs you will likely not get the same answer as the one in the book. You do not need to. The point of the lab is in the type of skillset or thought process, the walkthroughs are an example approach not necessarily the "right" one and may not even be possible given the changing data.

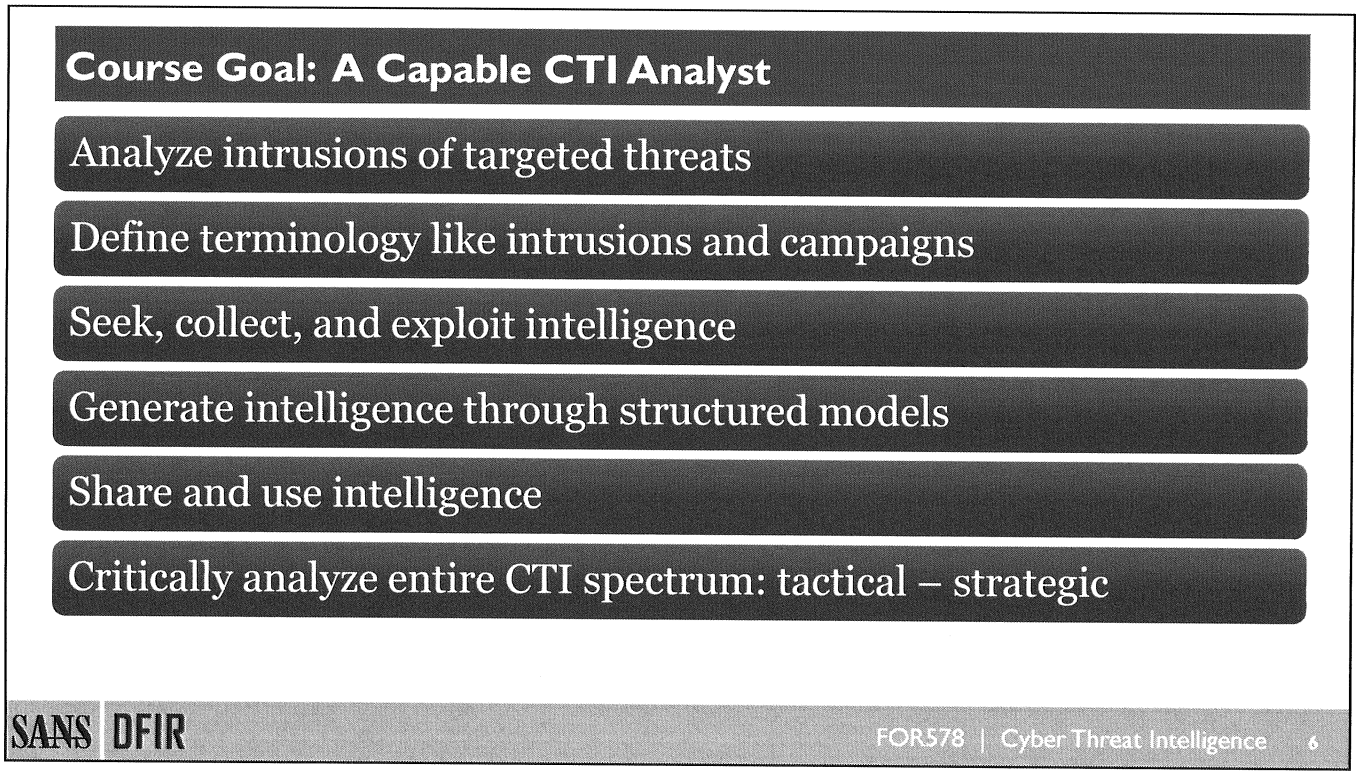
This page intentionally left blank.



Before we begin, please make sure you have completed Exercise 0, "SIFT Lab Installation."



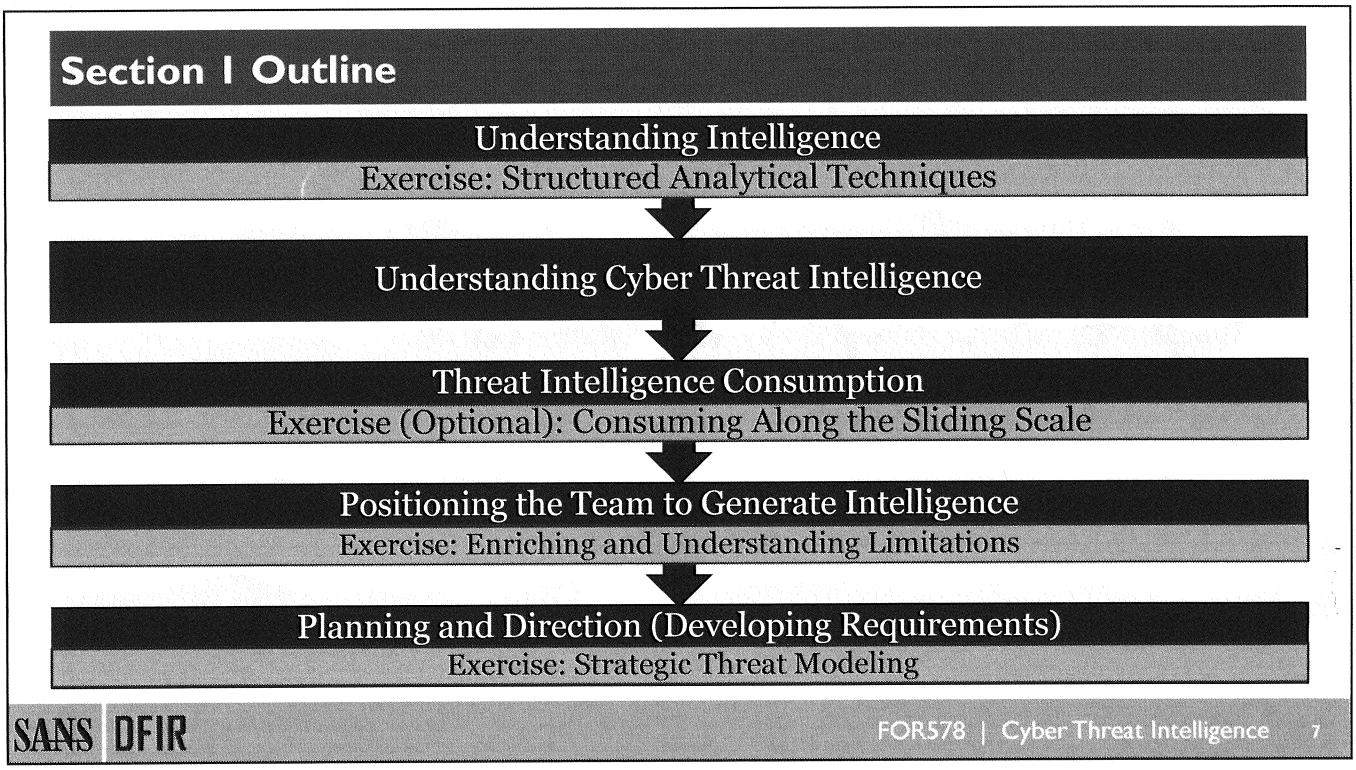
This page intentionally left blank.



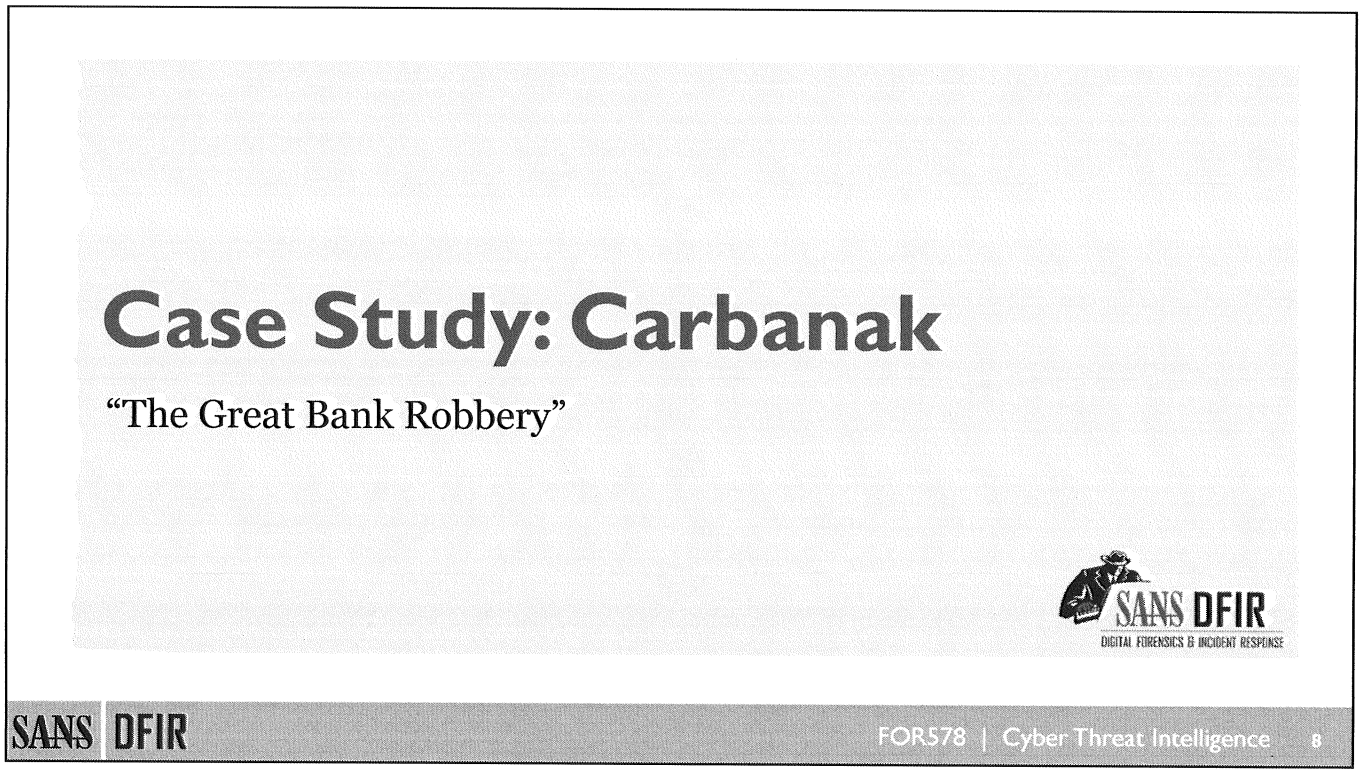
Now that we've gotten the juices flowing and framed the next few days, let's discuss the theory behind CTI. What we hope to do over the next few days is create a capable CTI analyst. We hope students leave this course with an understanding of what to do when provided CTI, how to fully analyze the actions that an adversary takes, how to leverage that knowledge to support a mission of organizational defense or intelligence collection, and how to become fully self-sufficient in the generation and exploitation of CTI.

What defines a capable CTI analyst? A CTI analyst can:

- Fully analyze successful and unsuccessful intrusions by targeted threat actors
- Construct descriptions of campaigns, actors, and organizations
- Seek out, collect, and properly exploit intelligence from others
- Generate intelligence from their own data sources and share it accordingly
- Manage intelligence to further the objectives of their organizations



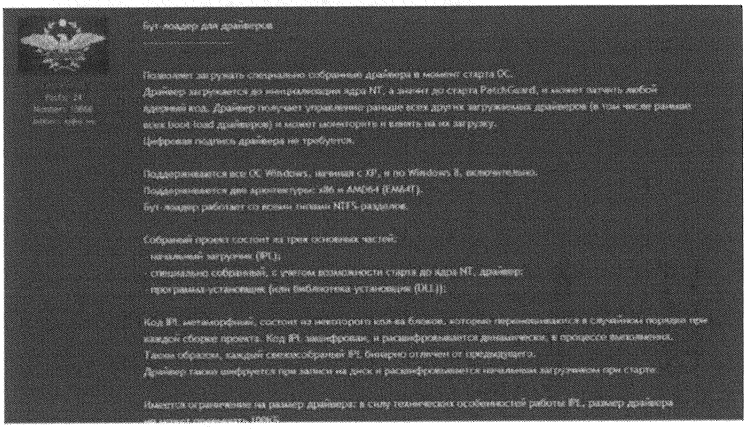
This page intentionally left blank.



This page intentionally left blank.

Carberp

- Cybercrime toolkit (first appeared Fall 2010) sold on Russian fraud forums with traditional capabilities such as VNC, RDP, sniffers, and keyloggers
- Source code sold in 2013 for $50,000 USD with a Master Boot Record rootkit



SANS DFIR FOR578 | Cyber Threat Intelligence 9

Carberp

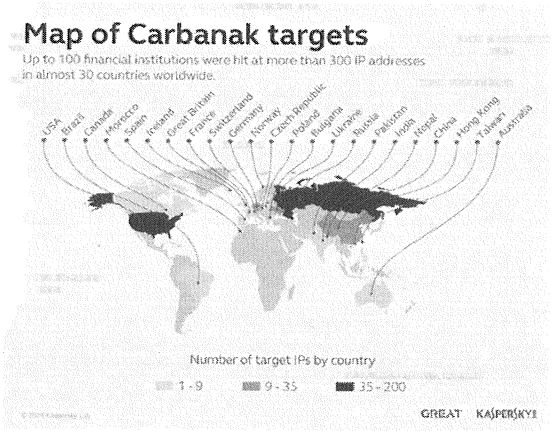
In 2010 a piece of malware identified as Carberp began to emerge from the Russian cyber crime scene. The piece of malware was fairly capable including some capabilities to steal certificates, sniff traffic, and perform keylogging functionality. At its basic components, it was a run of the mill, but highly effective, cyber crime tool. Eventually, likely due to some disputes with the creator, the source code of the malware was sold. Selling malware is nothing new but selling the full source code is still seen as fairly rare.

Reference:

https://securityintelligence.com/carberp-source-code-sale-free-bootkit-included/

Carbanak

- Malware based on Carberp discovered by Kaspersky Labs that was used in an Advanced Persistent Threat (APT) cyber crime campaign against banks
- Targeted over 100 banks in various countries:
  Ukraine, Russia, China, United States, Kuwait, Nepal, Malaysia, etc.
- Ongoing campaign showing flexibility of cyber crime groups

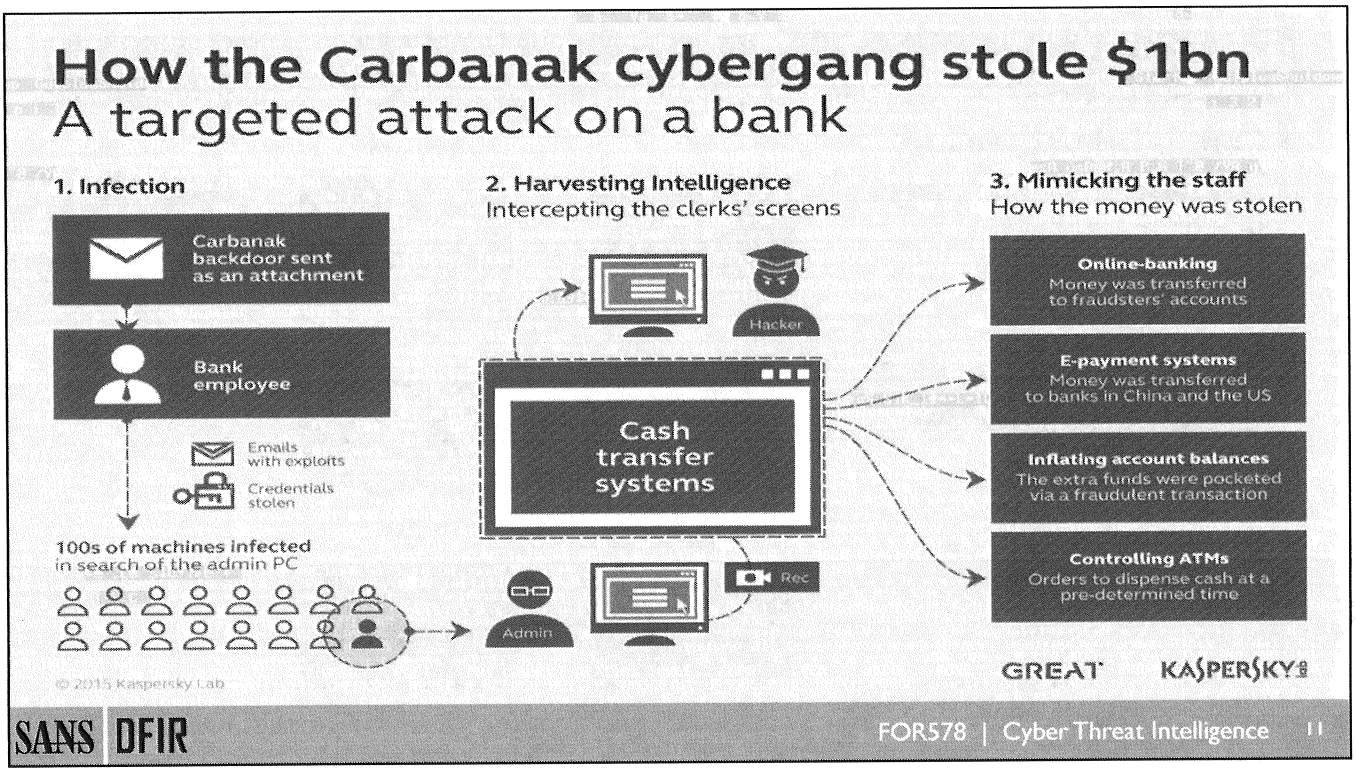


Carbanak

A cyber crime group acting in true APT fashion took Carberp and heavily modified it to create Carbanak. The Carbanak campaign was identified by Kaspersky Labs after a bank in Ukraine reported some odd activity to them. Eventually, another customer in Russia reported millions of US dollars in loss. The campaign ended up targeting over 100 banks, and is still active today, in various countries.

Reference:

https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf



How the Carbanak Cybergang Stole $1B

This is a good reference model that Kaspersky Labs made identifying the flow of the adversary intrusion. The core elements are similar to many campaigns: phishing emails with a malicious attachment, users open them, credentials are stolen off of the network, and information is gained about it. Eventually, the adversaries stole money in a variety of forms including ATM compromises and fake accounts.

Reference:

https://blog.kaspersky.com/billion-dollar-apt-carbanak/7519/

Carbanak Evolution

- Continued to target banks but moved to also target hotels, restaurants, and retail stores
- In 2017, was seen using Google for Command and Control (C2)

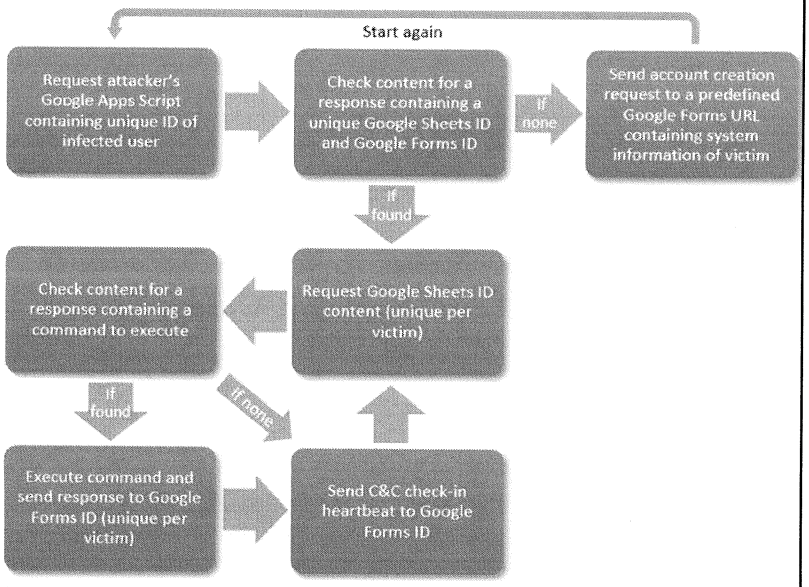


Image credit: Forcepoint

SANS DFIR FOR578 | Cyber Threat Intelligence 12

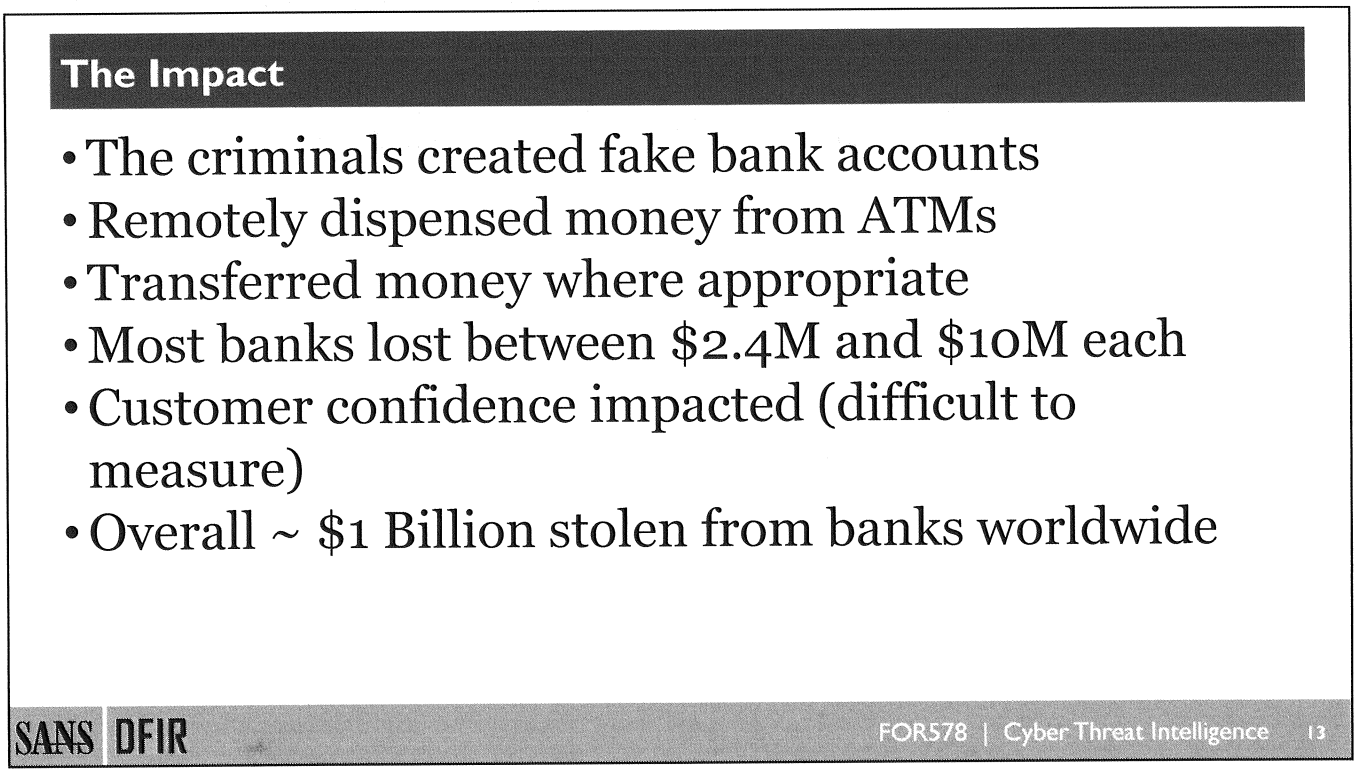
Carbanak Evolution

Carbanak seemed to evolve its operations in late 2016 to begin target hotels, restaurants, and retail stores instead of just banks. What was once seen as "crimeware" evolved into a campaign against banks and then evolved into a far-reaching campaign against numerous locations where financial motive could be sought.

Interestingly, Forcepoint identified a clever way that the adversaries were doing command and control (C2). The malware contained a script that leveraged Google Apps such as Google Sheets and Google Forms. The malware would beacon to a pre-determined and hardcoded Google Apps Script URL and determine if the victim was already registered with the adversary in the form of a unique Google Sheet or Google Form ID. If the victim did not have one yet, one was assigned and a unique Sheet or Form was leveraged to store information about the victim.

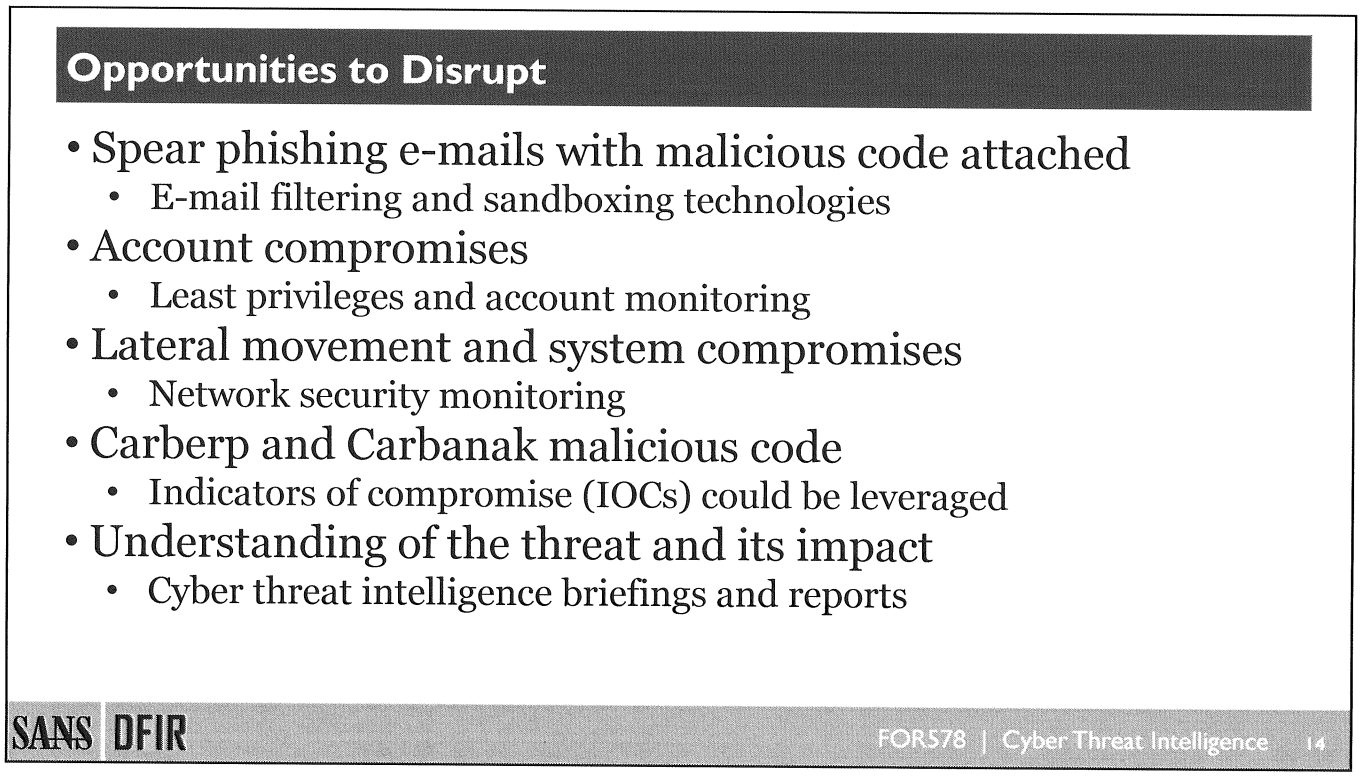
The threat is human – not malware. And humans are predictable in many ways. As an example, information management is a challenge for everyone. Unique files dedicated to individual victims is great for information management purposes.

Reference: https://blogs.forcepoint.com/security-labs/carbanak-group-uses-google-malware-command-and-control



The Impact

The various adversary efforts led to $2.4M to $10M being stolen from each targeted bank. At that point, the adversaries moved on, likely trying to avoid detection as much as possible. Ultimately the numbers have placed the campaigns haul at around $1Billion USD. This makes this campaign the larger cyber heist in history.



Opportunities to Disrupt

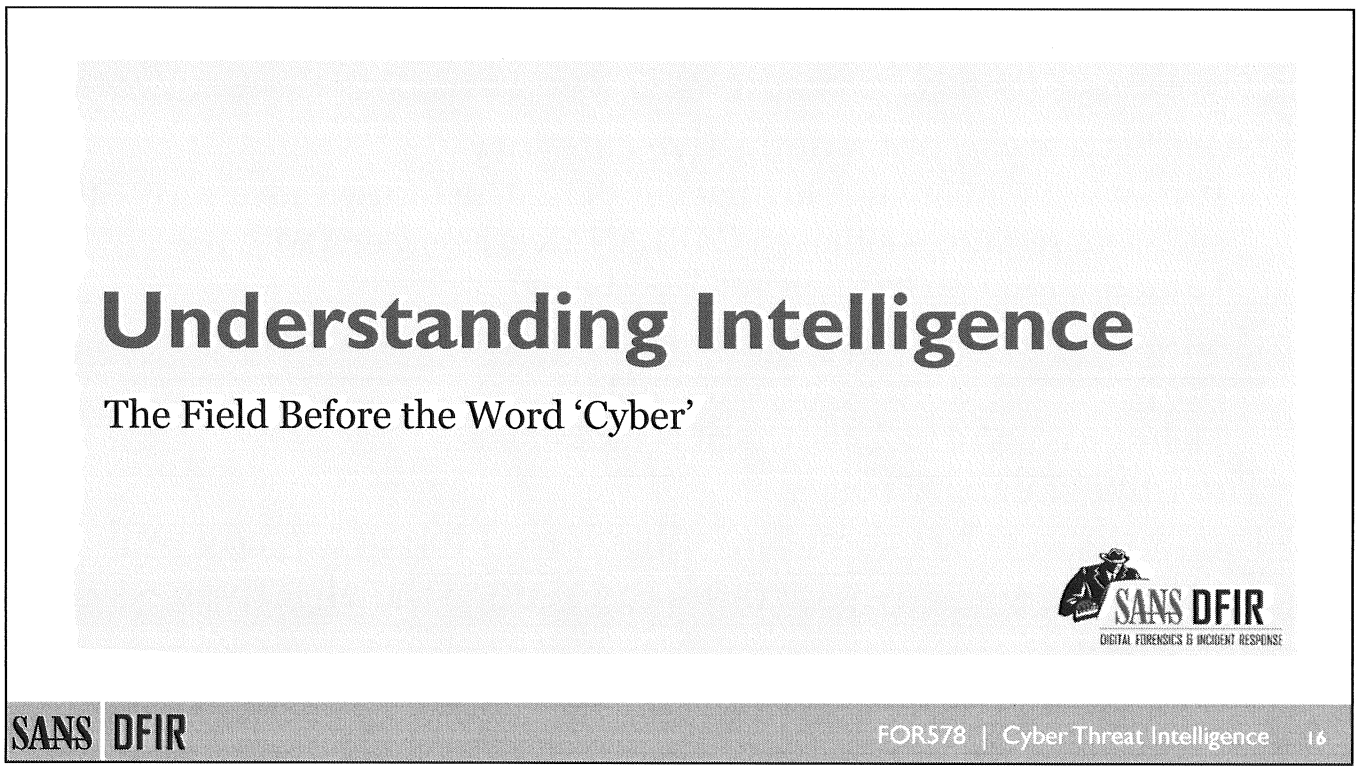
What is important here is noting that many of your classic security solutions and safeguards would have significantly helped in this campaign. Nothing about the "APT" actor was "advanced" only persistent and well-funded. It is important for organizations to understand models such as the SANS 20 Critical Controls significantly reduce attacker opportunities. Eventually though, understanding the threat and its impact while also identifying the threat actor's campaign is the role of cyber threat intelligence. We will discuss the role of cyber threat intelligence throughout this course.

Lessons Learned

- "APT" is a style, not a definitive category
  - It's not just for nation-states but any persistent focused adversary with sufficient resources although CARBANAK is associated with the Lazarus Group (to be discussed later today)
- "Commodity malware" in the form of Carberp was repurposed by a more capable actor
  - Malware is just a tool; the threat is the human
- The impact can be costly
- Increases in cyber threat intelligence on top of already well-functioning security programs can reduce the effectiveness of the threat

Lessons Learned

Many organizations think in concepts of "advanced" as exceptionally new and tailored exploits, cool vulnerabilities, and tactics we haven't seen before. Advanced is really just a qualification of funded operations and logistics though. It is also important to note that the adversary's malware was based on commodity malware. Malware is just a tool. We will focus in this course on focusing on the human threat. Ultimately cyber threat intelligence should influence well-functioning security programs to operate more effectively and efficiently—it should not act as a silver bullet for security issues.

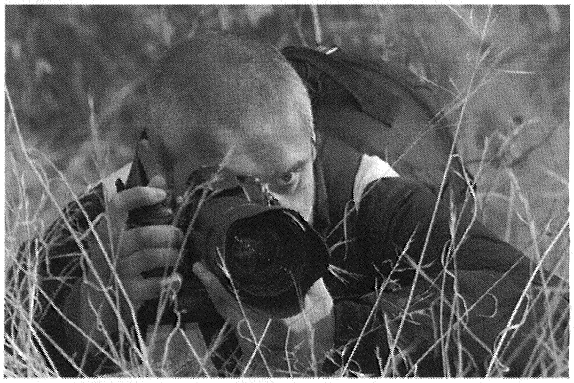


This page intentionally left blank.

Intelligence

Intelligence is the collecting and processing of information about a competitive entity and its agents, needed by an organization or group for its security and well-being.

Intelligence is both a product and a process



Before we begin diving into the depths of Cyber Threat Intelligence, it behooves us to engage in a discussion about what intelligence is, in a traditional sense. Primitives in the traditional intelligence domain form the basis around which CTI has evolved and apply to our domain as it is a subset of traditional intelligence analysis.

So, what is intelligence? This is a broad question with many answers, but in the context of intelligence analysis, we seek a definition that captures the essence of the information we desire in furtherance of our nation-state objectives (be they military, economical, or geopolitical). A fantastic now-declassified discussion is provided by CIA analyst Martin T. Bimfort who pulls together a variety of definitions to formulate one that describes intelligence in the context of classic intelligence analysis:

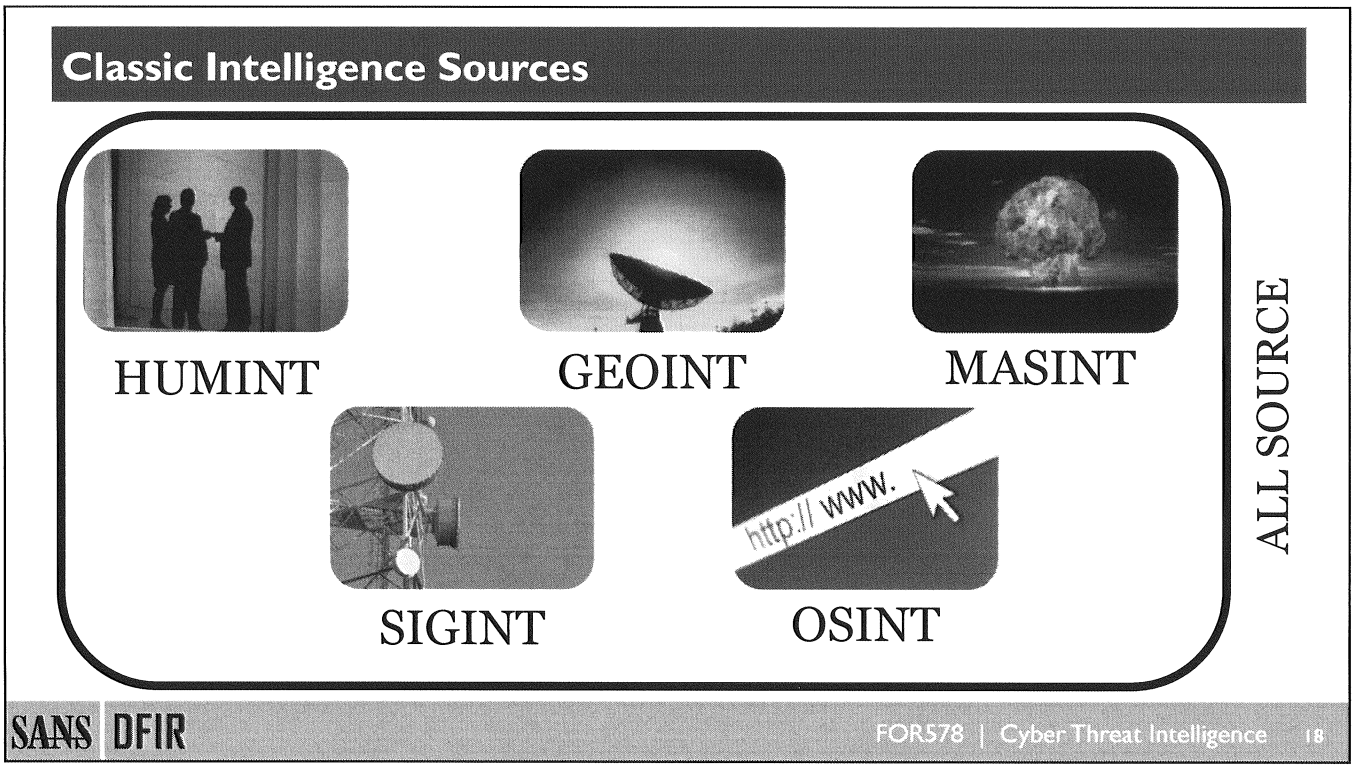
> *"Intelligence is the collecting and processing of that information about foreign countries and their agents that is needed by a government for its foreign policy and for national security, the conduct of non-attributable activities abroad to facilitate the implementation of foreign policy, and the protection of both process and product, as well as persons and organizations concerned with these, against unauthorized disclosure."*

I recommend you read the discussion provided in the paper cited for this definition.

["A Definition of Intelligence" (https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm). Martin T. Bimfort. Central Intelligence Agency. Declassified 18 Sept 1995. Retrieved 4 Oct 2014.]

From Bimfort's definition, a generalized definition of intelligence can be formed:

> *Intelligence is the collecting and processing of information about a competitive entity and its agents, needed by an organization or group for its security and well-being.*



Classic intelligence has abbreviations associated with the sources of intelligence. Generally speaking, these can be broken out by collection and analysis (or derivative intelligence) using human and technological means. Common acronyms are:

- **HUMINT**: Human intelligence collection (interpersonal).
- **GEOINT**: Geospatial intelligence collection (from satellites).
- **MASINT**: Measurement and signature intelligence (from radar signatures, nuclear detonation signatures, and so on).
- **OSINT**: Open-source intelligence collection (from libraries, public records, or the Internet).
- **SIGINT**: Intelligence derived from signal intercepts (cell phone communications or tapping of communication lines).
- **ALL SOURCE**: Intelligence derived from every available source on a subject or topic.

Classically intelligence was bifurcated into the areas to which you collected it. However, cyber threat intelligence does not get this luxury; we often do not deploy HUMINT agents or have SIGINT operations. Instead, our focus is one of all source: identifying various sources of data that can meet our requirements and fusing it together.

It is important to note that different focuses on collection generated different biases in the intelligence communities around the world. HUMINT analysts are often more at odds with SIGINT analysts than they are conjoined. This divide is often seen between intelligence agencies in countries around the world even when working for the same government. A dedication towards types of collection can be very important when trying to derive specific, and varying, intelligence requirements based on those collection sources that support national objectives such as going to, or avoiding, war. In the digital domain, our choices are often not designed for those types of objectives. A malware analyst may be very biased towards appreciating what malware is able to say about an adversary just like a HUMINT analyst will be biased towards human collection tactics. Try to avoid those biases and leverage data for one it is – one data point to make an overall intelligence assessment.

Counterintelligence

Counterintelligence is:

- Identification of intelligence activities of adversarial entities
- Assessment of intelligence activities of adversarial entities
- Neutralization of intelligence activities of adversarial entities
- Exploitation of intelligence activities of adversarial entities

We derive a definition of counterintelligence from a CIA paper on Strategic Counterintelligence that states:

"It is the job of U.S. counterintelligence to identify, assess, neutralize, and exploit the intelligence activities of foreign powers, terrorist groups, and other entities that seek to harm us." ["Strategic Counterintelligence" (https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/strategic- counterintelligence.html). Michelle Van Cleave. Central Intelligence Agency. 12 Jun 2007. Retrieved 4 Oct 2014]

To generalize this statement, **counterintelligence** is the identification, assessment, neutralization, and exploitation of intelligence activities of adversarial entities.

It's worth noting at this point that although we call this course "Cyber Threat Intelligence," the focus is on the intelligence activities of others; in other words, counterintelligence. Unfortunately, by the time we realized this error, the term had caught on and we were unable to get in front of it. So just know that CTI is really cyber threat *counter*intelligence.

Case Study: Operation Bodyguard

- Allied initiated operation to counter German intelligence efforts
- Positioned that the D-Day invasions would take place later than reality and at different locations than Normandy
- Used fake armament positioned along England
- Employed double agents and leaked false info
- Offensive styled counterintelligence
  - The focus of this course is defensive counterintelligence

Case Study: Operation Bodyguard

During World War II the Allied states initiated Operation Bodyguard. The purpose of this operation was to perform counterintelligence operations for the purpose of confusing the Germans and causing faulty strategic choices about where the D-Day landing would take place. This more offensive version of counterintelligence required active deception to include the creation and leaking of strategies and plans where the supposed Ally invasion would take place in locations such as Pas De Calais, the Balkans, southern France, and Norway with additional attacks from the Soviets in Bulgaria and northern Norway. The operation was also meant to fool the Germans into believing the attack would take later than anticipated.

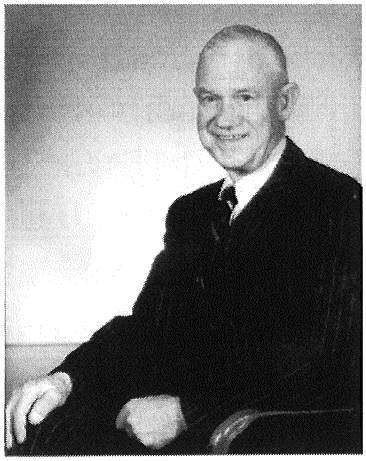
This case study is a great one to understand more offensive techniques. In this course, we will be talking about passive techniques; the analysis of adversary actions that have taken place and the countering of them early into espionage efforts. In Operation Bodyguard, many of the more offensive techniques included double agents sending back misinformation while decrypting German transmissions to evaluate the success of the operations. There were also fake military armament deployed along locations in England to pretend a staging effort for an invasion that never came.

Image Reference:

https://en.wikipedia.org/wiki/File:DummyShermanTank.jpg (inflatable Tank)

Sherman Kent

- Yale University history professor
- During World War II and 17 years during the Cold War served in the Central Intelligence Agency (CIA)
- Considered the father of intelligence analysis
- Authored: *Strategic Intelligence for American World Policy*



Sherman Kent, 1903-1986

Sherman Kent

Sherman Kent is often considered the father of intelligence analysis. As a Yale professor, he was inspired during World War II to join the Office of Strategic Services (OSS) which would eventually become the Central Intelligence Agency (CIA). During his time as an analyst, he focused heavily on a combination of history (something for all threat analysts to think heavily upon and learn from) and a way to professionalize analysis instead of allowing rash decisions and judgments. Due to the mistreatment of intelligence analysts at the time compared with the "operators" who were the collectors of information directly from sources he was inspired to write *Strategic Intelligence for American World Policy* and set out to formalize an understanding of analysis.

Reference:

https://en.wikipedia.org/wiki/Sherman_Kent

https://www.cia.gov/library/kent-center-occasional-papers/vol1no5.htm

Kent's Analytic Doctrine

1. Focus on Policymaker Concerns
2. Avoidance of a Personal Policy Agenda
3. Intellectual Rigor
4. Conscious Effort to Avoid Analytic Biases
5. Willingness to Consider Other Judgements
6. Systematic Use of Outside Experts
7. Collective Responsibility for Judgement
8. Effective Communication of policy-support Information and Judgements
9. Candid Admission of Mistakes

Kent's Analytic Doctrine

Based on his encounters and for his book Kent set forth on specific insights into analysis. The list on the slide was made from an analysis of and understanding of Kent's doctrine. As you read the list think about what Kent was trying to get across and how it translates to what we as analysts in cyber threat intelligence do on a daily basis. First, Kent notes that the focus is on policymaker concerns. In your organization, this may be your decision makers especially related to the board of executives and C-suite members. This begs the question about the role of forms of intelligence that are more tactical in nature. In truth, though, it all fits nicely; the concerns of the executives should represent the needs of the organization and whether that is of a strategic or tactical nature it does not matter as it should support something. This also highlights an important concept though: intelligence must be useful. The words "actionable intelligence" are often abused because intelligence is always meant to be actionable.

Many of the other points standalone in understanding them. However, focus on the need to have an intellectual process, break your biases, and admit your mistakes. Also, the focus of this list is on clearly communicating information and judgments. Or in other words, skip the technical jargon and communicate clearly about the needs of the decision-makers. It is in this way we can best represent our field and the security community.

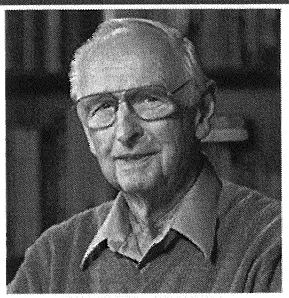
These topics will all be explored in some part across the five sections of this course.

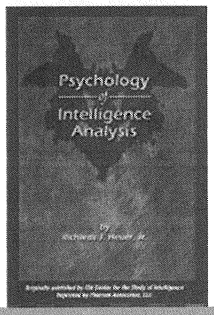
Reference:

https://www.cia.gov/library/kent-center-occasional-papers/vol1no5.htm

Richards J. Heuer Jr.

- 45-year veteran of the CIA and author of the *Psychology of Intelligence Analysis*
- Work primarily focused on analysis types, critical thinking models and approaches, and overcoming biases that hinder analyst thought processes
- Also co-wrote *Structured Analytic Techniques for Intelligence Analysis*
  - Contains 55 structured analytic techniques in step-by-step processes to assist analysts
- Often cited for his work developing the Analysis of Competing Hypotheses





Richards J. Heuer Jr.

Richards is one of the most well-known intelligence analysts and focused his work on structuring analysis. As a 40-year veteran of the CIA, he lived through good and bad analysis and the impacts it caused including life and death situations. His books *Psychology of Intelligence Analysis* and *Structured Analytic Techniques for Intelligence Analysis* could be courses in of themselves and are often course books in collegiate intelligence courses. In this course, we will highlight core concepts needed for good structured CTI work including the defeating of biases. Much of this will be dived into during Section 5 of this course.

Reference:

https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf

http://www.analysis.org/structured-analytic-techniques.pdf

Analysis

(a) Detailed examination of the elements or structure of something
(b) Breaking something down into its constituent parts so as to understand its operation

We analyze:
- Observed activity
- Adversary intent

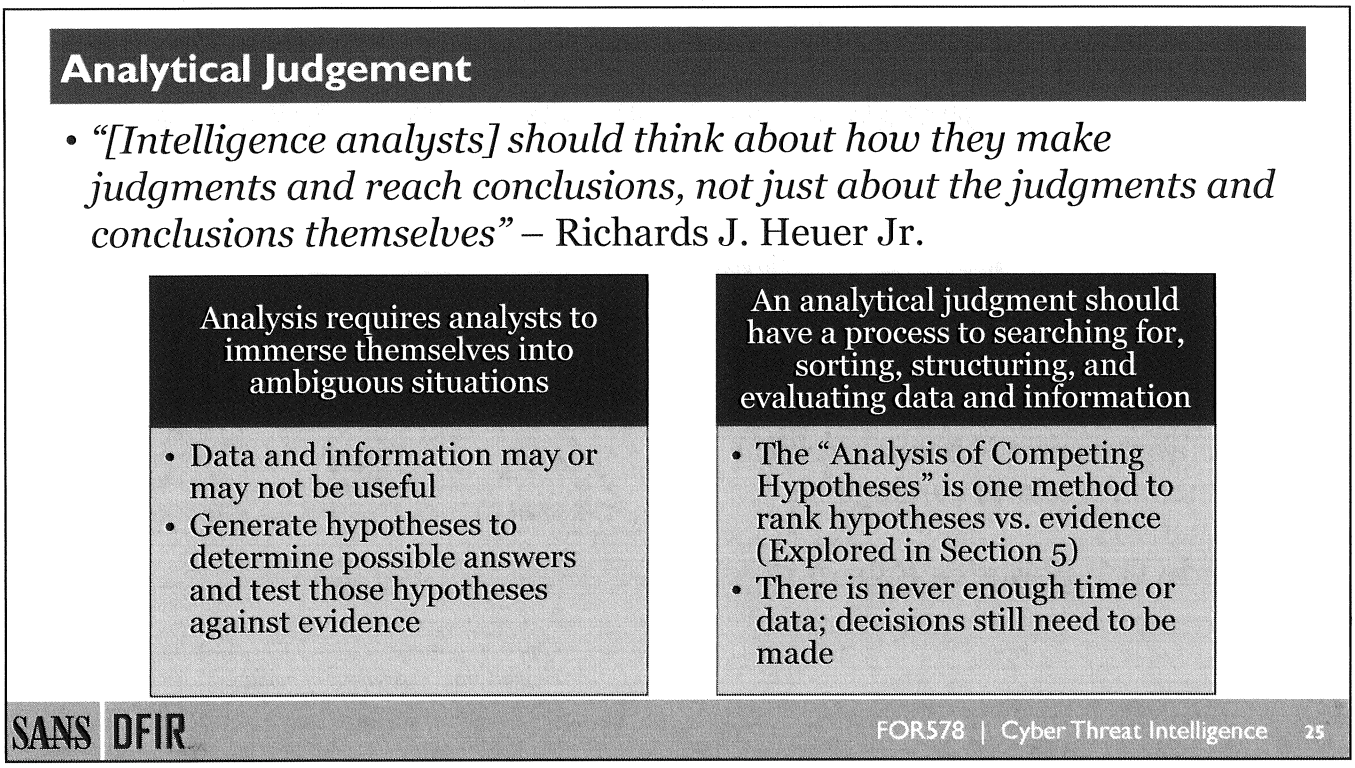
We synthesize:
- Mitigated activity
- Profiles
- Campaigns

Analysis

Analysis is derived from the Greek primitives "ana" (up) and "luein" (loosen). It is the act of taking something apart so as to understand it. This is what we do for intrusions and threat actors: analysis. We deconstruct intrusions to understand how they operate. We perform one other action not covered by *analysis* in the literal sense, which is somewhat the opposite of analysis, yet still essential for the understanding of how adversaries operate: We synthesize unsuccessful intrusions. Synthesis is the act of constructing an object. We also synthesize profiles of adversaries based on intelligence we collect from our available sources, and we synthesize campaigns (which you will learn more about later). Although malware analysis is quite literally analysis in the conventional sense, what we will often take part in is the analysis of an unsuccessful intrusion, therefore *synthesizing* the rest of the intrusion so as to enhance our understanding of it. You will learn more about the analysis-synthesis duality when we discuss completing the Kill Chain and constructing campaign, persona, and organization profiles.

In short, although we use the term analysis to describe classic intelligence analysis as well as CTI, what we are really doing is a combination of taking apart what we have, as well as synthesizing that which we don't have, all to enhance our understanding of our adversaries.

[Source: Google, https://www.google.com/search?q=analysis+etymology]



Analytical Judgements

In many ways, an analysts' role in intelligence analysis comes down to making judgments. It is simple enough to understand that a conclusion may not be fully supported or to structure data to help support a conclusion or detract from it, but action is required. Take for example an analyst that understands that an adversary may not actually have a malicious capability to disrupt the company's operations. However, most of the data available indicates that the adversary does indeed have a capability to harm the organization. Yet the analyst also understands they do not have enough information yet, would need more time to reach a better conclusion, and could be wrong ultimately impacting the organization if it decides to act or not act in response to this capability. Yet the organization's head requires an answer. Is it appropriate for the intelligence analyst simply to respond that there is a low to moderate confidence assessment but they cannot recommend an action one way or another? Being a purist about analysis is important to our processes but at the end of the day, judgments have to be made in many situations. Understanding when judgment is needed, when it is not, and how to facilitate the best judgment possible to meet those requirements is an important and stressful requirement.

Analysts will always find themselves wanting more time and information. But we must make the best of what we have and approach it with as much structure and intellectual rigor as possible while still returning results and value to the organizations that depend on us.

Reference:

https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf

Thinking About Thinking and Perception

- Good intelligence analysts think about how they think
  - Deriving a conclusion should be much like a forensic process: defensible, repeatable, and understandable to others
- All people view the world in different ways
- Perception should be an active process instead of a passive one
  - Do not let your views jade your analysis especially because critical situations are often ambiguous situations
- How do you perceive Figure 1?

Figure 1

Figure 1 from *Psychology of Intelligence Analysis*

Thinking About Thinking and Perception

The first two chapters of Richards J. Heuer Jr.'s book *Psychology of Intelligence Analysis* are "Thinking about Thinking" and "Perception: Why Can't We See What Is There to Be Seen?". In these two chapters Richards masterfully lays out a simple expectation for analysts: we are required to think about how we arrive at conclusions instead of just accepting what others would see, else we miss important things during critical times. Richards helped showcase this with the first figure in his book. This very simple figure, shown in the slide, helps most analysts understand that they have expectations of how the world works and thus miss important details. If we can stop to think about how we see the world and structure our analysis appropriately we can pick up on what others do not. Perception is not simply a passive process, as Richards stated, but is instead something we can train ourselves on and can demonstrate by actively striving to be aware of what is around us. As an example, did you see in Figure 1 that the word "the" and "a" is written twice whenever used? Re-look at Figure 1 and note that it should not say "the the spring" "a a lifetime" and "the the hand" but because we as analysts expected an outcome we perceived it to be there. Most people allow their expectations of reality and views of the world to drive their perception inappropriately.

Reference:

https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf

Example Types of Analysis

- Data-Driven Analysis
  - Accuracy is based on the dataset's accuracy and completeness
  - Logically driven and easily understood by other analysts observing it
  - Requires good datasets and straightforward problems
- Conceptually Driven Analysis:
  - Numerous unknowns and undefined variables and relationships
  - Often immediate interpretation of complex concepts
  - Accuracy is driven by mental models and feedback over time
- Mosaic Theory of Analysis
  - Disparate information comes together to tell the right story
  - Rarely practical and heavily based on analyst interpretation
  - Inappropriate belief that there is only 1 mosaic to make
- Many Types of Analysis Exist:
  - Descriptive, Explanatory, Evaluative, Estimative, etc.

Example Types of Analysis

To give some examples of types of analysis we can look at three types that Richards laid out in his first book. There is no definitive choice on types of analysis and there is no one model that works for all situations; Richards showed disdain for the mosaic theory but there are many types of analysis out there.

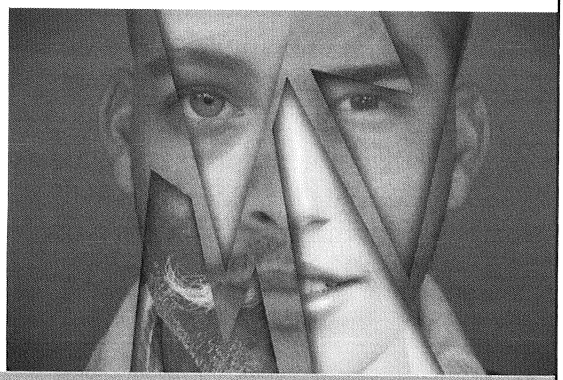
As an example, there is Descriptive Analysis where analysts simply describe the elements of the data or information they are observing. Explanatory Analysis tries to structure the "why" of the situation where Evaluative Analysis tries to understand the information actually means. Estimative Analysis and to a greater extent Predictive Analysis tries to give a "what will happen next?" type approach to situations. It is important to try to understand what types of analysis is being done and the impact of each.

Reference:

https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf

Hindrances to Good Analysis

- Everyone has biases
- Bias is difficult to understand and impossible to eliminate
  - Understanding our biases is important for us to do analysis
- The human brain tries to simplify things around us
  - Shortcuts and simplicity can drive mistakes
  - Cognitive bias, those resulting from the mind, will be explored in-depth in Section 5
- Good intelligence teams should strive to limit bias through structured analytical approaches and diversity on the team and in their analysis



SANS DFIR FOR578 | Cyber Threat Intelligence 28

Hindrances to Good Analysis

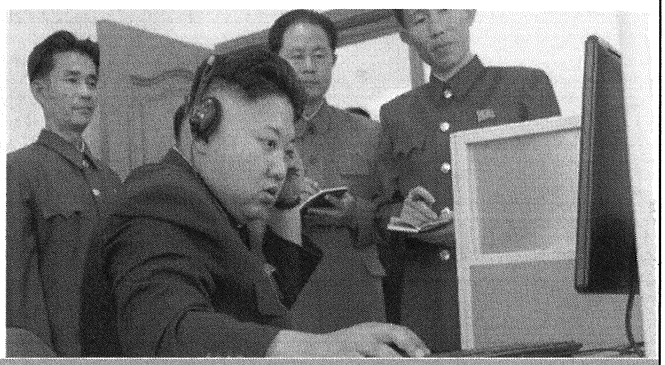
Bias is a complicated matter. It is both the human aspect of intelligence (why can't a machine simply do intelligence analysis? One potential answer is bias.) and the error that hinders how we analyze situations. Put simply, the mind wants the world to be simple. It helps simplify things around us so we can make quick decisions especially when it is important to our self-interest and survival. But bias jades the way we look at the world and it is impossible to remove all of our biases.

Cognitive biases, mental errors, will be explored in-depth in Section 5 of this course. For now though, we will explore some types of analysis and structured analytical techniques. Another awesome opportunity for teams to expand their analysis and avoid group think and bias is to ensure diversity on the team. Diversity should exist as much as possible in the form of ethnicity, sex, creed, background, upbringing, etc. just as it applies to skills. If you have 10 malware analysts as your intelligence analysts, they will likely view the world of intelligence focused around malware. If you have 10 international relations theorists as intelligence analysts the world will be more likely viewed through international messaging and norm setting. It is important to include different make-ups and backgrounds in analysts.

Image Ref: Diversity.com

Bias Example - Adversary Intent: North Korea and WannaCry

- Early 2017 WannaCry ransomware worm infected 300k+ computers
- The National Security Agency (NSA) assessed that the adversary behind WannaCry was North Korea
  - Many in the community supported this with their own analysis
- Despite the attribution (right or wrong) questions formed
  - Why did North Korea do this?
  - Would North Korea do this?
  - What was their intention?
- Adversary intent is one of the most difficult intelligence challenges
  - It is also often not at all helpful
- Instead focused on perceived adversary intent or possible motives as long as they help structure defense



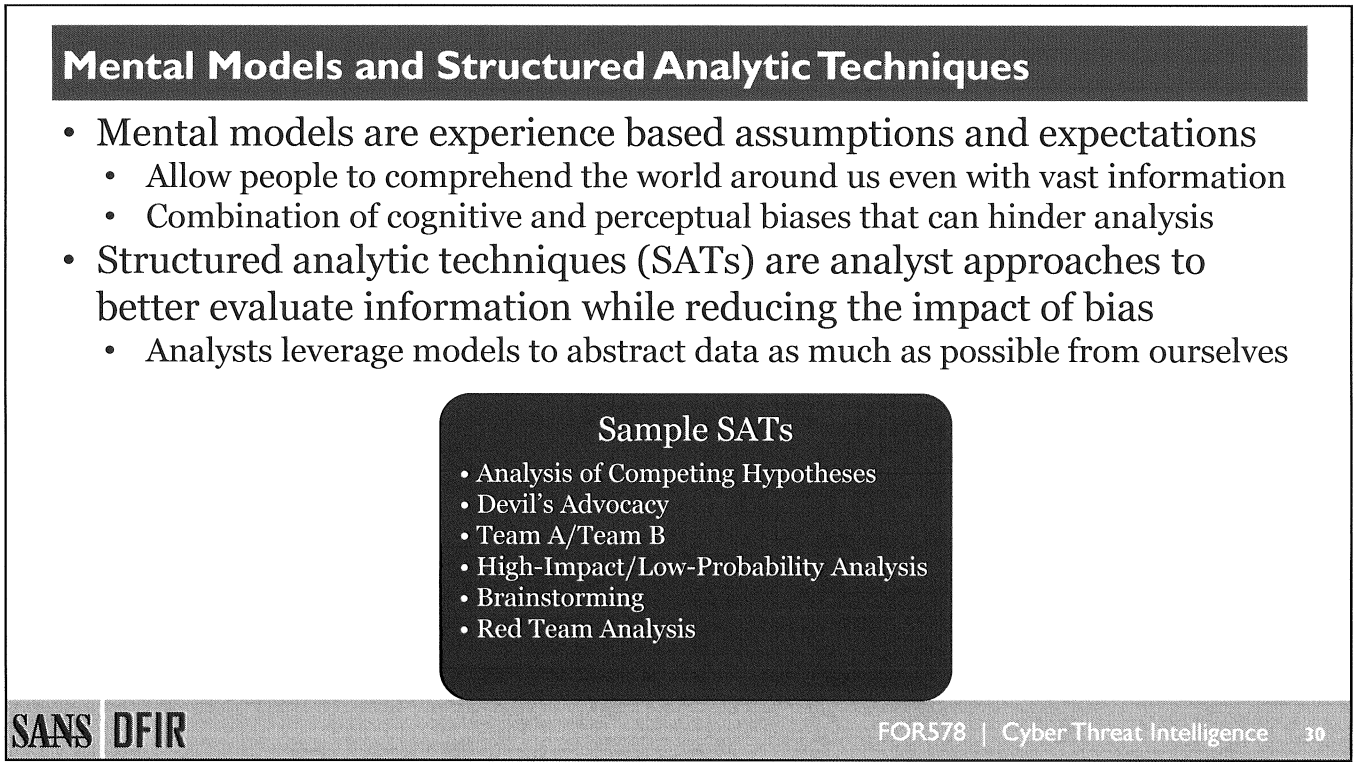
Bias Example: North Korea and WannaCry – Adversary Intent

In early 2017 an outbreak of a worm that leveraged stolen National Security Agency (NSA) exploits occurred. This malware was called WannaCry. Unlike previous worms that the world had seen—such as Conficker—this malware was also ransomware. Yet it seemed to not be that effective in earning money (estimates around $120k USD in total) whereas it infected hundreds of thousands of computers around the world. The NSA and the United Kingdom's Government Communications Headquarters (GCHQ) made the assessment that WannaCry originated in North Korea by government-aligned operators. This matched much of the analysis done in the private sector community as well. Regardless of the validity of the attribution though it is a useful case study to explore bias. In the weeks and months following many journalists and security professionals had a simple question: why did North Korea do this?

There were plenty of claims such as "obviously this wasn't North Korea because a nation-state wouldn't release something so powerful and profit so little" or "obviously this was North Korea and they didn't intend for the malware to get out." But all these claims look at adversary intent. Adversary intent is one of the most difficult goals in intelligence analysis. How many of us in the security community have previously been North Korean government operators/hackers? (Hopefully, none taking this course). Removed from that, how many of us have been raised in North Korea? Is there a "single" North Korean thought process as well? People are diverse anywhere in the world, thought processes are diverse, and it is truly difficult to think like the adversary for a variety of cultural differences. Thinking like an attacker might be useful in discussing pentests but truly thinking like an attacker and understanding their intent is outside the scope of what most intelligence analysts will ever do. Instead, it may be important to understand a perceived intent and how we wish to respond to that event. Also understanding if our actions change at all based on intent is important.

Reference:

https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.141acddb027c



Mental Models and Structured Analytical Techniques

Mental models are different frames of reference or mindsets that people adopt. These are the combination of perception and cognitive biases formed through experience. It is important for people to have these mental models so that we can digest vast amounts of information that we receive each day. Mental models allow us to get into habits and quickly work. Think about the security analyst who responds quickly to incidents she's seen dozens of times before. This is the experience that people get paid for that makes them senior responders. However, that same quick approach could lead the responder to miss key details of change. Instead of seeing what was important for analysis to answer new or challenging questions the responder may be responding to what they perceive as important or taking place instead of the small subtle change that has occurred.

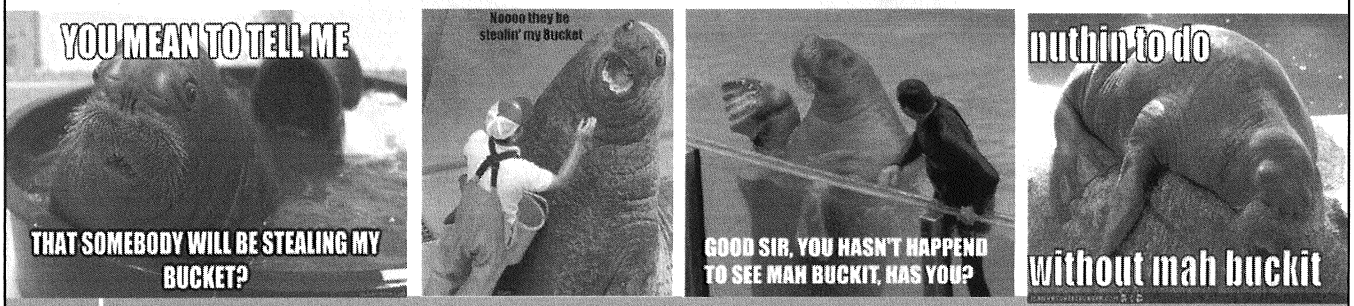
Structured analytic techniques (SAT) are there to assist analysts at deriving better analysis through the abstraction of their biases. This can be in very simple approaches (such as playing devil's advocate where you argue against the accepted assumptions or explanations) to more complex approaches (such as analysis of competing hypotheses). SATs are not perfect and analysts that use them still may not derive a better answer than those that do not. However, over time and leveraged appropriately they can help each analyst achieve a better approach and consistency in their analysis. As an example, Devil's Advocacy is where an analyst(s) challenges a strongly held assumption, position, or explanation. This can be more complex in a Team A/Team B situation where two teams do their own individual analysis on strongly held views or competing hypotheses. Even more complex is Red Team Analysis where analysts try to think about how an adversary would think about a situation or event. This is one of the most difficult SATs because it is impossible for analysts to truly understand the mindset, SATs, and biases of the adversary. However, it can be very useful.

Reference:

http://www.analysis.org/structured-analytic-techniques.pdf

Kill Chains and Other Models – Data into Buckets

- Structured models are useful to analysts for many reasons but a chief reason is simply: data into buckets
  - Data into buckets allows for the abstraction of the analyst and identification of patterns
- "Kill Chain" is a military concept to understand the individual elements of an attack for offensive or defensive purposes dating to at least 1973
  - The "Cyber Kill Chain" is an example in cybersecurity and will be explored in Section 2



SANS DFIR FOR578 | Cyber Threat Intelligence 31

Kill Chains and Other Models – Data into Buckets

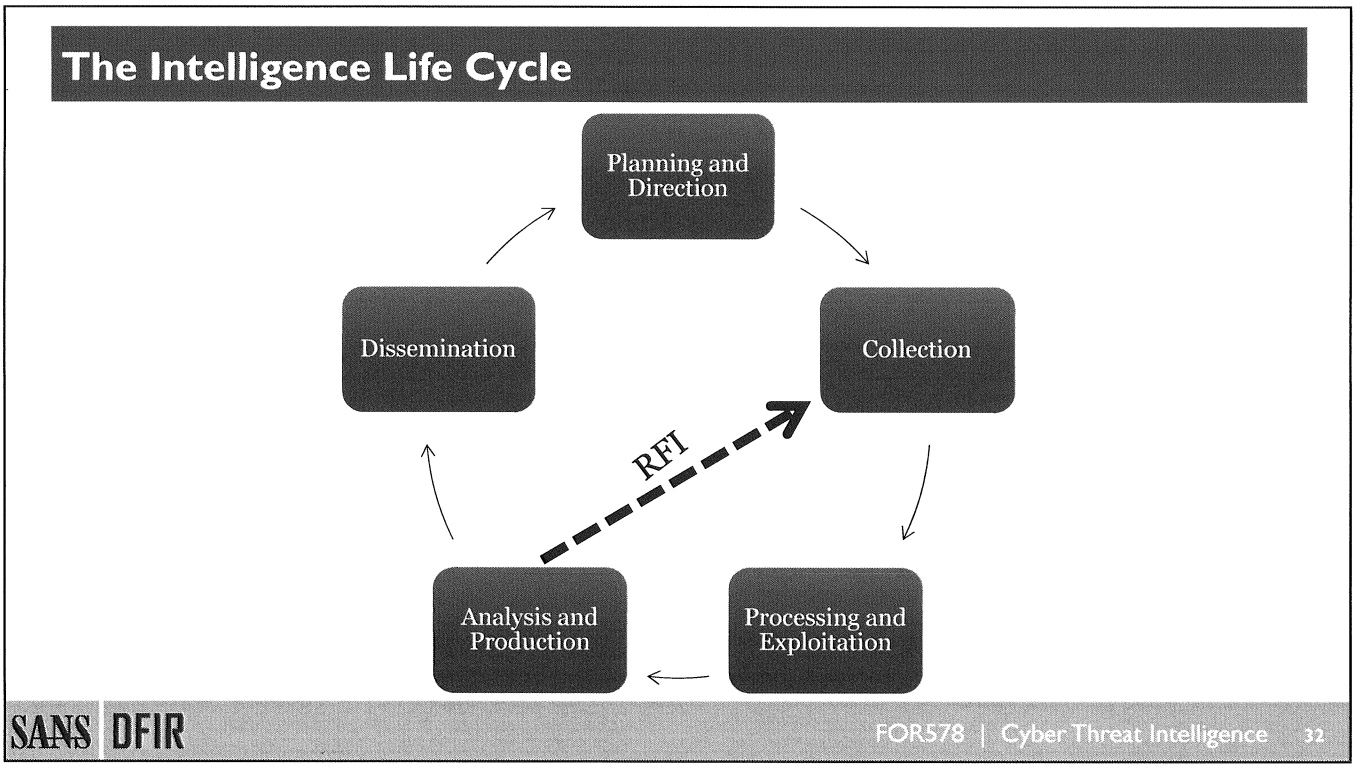
One unavoidable topic in cyber security is the cyber kill chain. This model is often abused and many times used incorrectly, but it is extremely valuable and will be covered in Section 2. But the cyber kill chain (or "intrusion kill chain") is not the first kill chain. Kill chains do not have a definitive origin but the earliest mentions can be found as far back as 1973 when used in discussion of the Vietnam war and air warfare. The idea behind a kill chain was simple: what are the individual elements or actions that the adversary must do to be successful. Understanding what actions they have to take before some sort of mission, success or impact helped the military understand where defenses were needed and how to posture correctly against different types of attacks. It also aided analysts in understanding how to identify patterns and early indications and warning in adversary behavior.

Models are not necessarily SATs but they can be leveraged in many the same ways such as trying to reduce our biases while observing information for what it is and trying to make it more useful. It's all about putting data into buckets (building a structured schema) and enforcing it in your analysis and in your team's.

Reference:

US Defense Strategy from Vietnam to Operation Iraqi Freedom, Robert R. Tomes

Image Ref: Outdated memes and too much time on the Internet



The Intelligence Life Cycle

One example of a model used heavily in the intelligence community is the Intelligence Life cycle. This is a general process with five stages (and an assumed, always present sixth element of "Evaluation and Feedback"). These five stages are:

- Planning and Direction
- Collection
- Processing & Exploitation
- Analysis & Production
- Dissemination

Why does this matter? As analysts, intelligence analysis is what we do. Some of you may be guided by this cycle as network defenders, while others of you who work for the government will be participating in this exact cycle.

During the *Planning and Direction* stage, intelligence gaps are identified and prioritized, and methods for filling those gaps are developed. A plan is set forth to where and how analysts will get the data and information they need. This drives collection.

The *Collection* stage: The plan is executed and data is collected to fill the intelligence gap. In CTI, this might be the act of instrumenting a network with a tap or enabling enhanced logging on certain devices.

Processing and Exploitation refers to any preparation needed for the raw data collected. This might be filtering, transformations of the data from one format to another, or extraction of key indicators collected.

Dissemination is the act of distributing the requested intelligence to the "customer" (note: you may be your own customer). This, of course, is then used by the customer to further their objective (improved defenses, better information on the location of a suspect for Law Enforcement (LE), a greater understanding of an adversary's social or computer network for counterintelligence, and so on). Once intelligence is disseminated, more questions are raised, which leads to additional planning and direction of future collection efforts.

Request for Information (RFIs) generally describe a request by analysts focusing on one phase of the cycle for more information from analysts in another phase of the cycle. This could include subject matter expertise in areas unfamiliar to the requesting party, a clarification on processed data, or tasking to collect additional data, to amplify analysis.

This process is generally followed by many of the U.S.'s 14 intelligence community (IC) entities, such as the NSA and CIA, as well as the Department of Defense.

["Joint Publication 2-0, Joint Intelligence," http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf. *Defense Technical Information Center (DTIC)*. Department of Defense. 22 June 2007. pp. GL–11. Retrieved 10/1/2014.]

Field of View Bias from Collection

Operational Environment (location of collection) and Intelligence Requirements yield a "field of view"

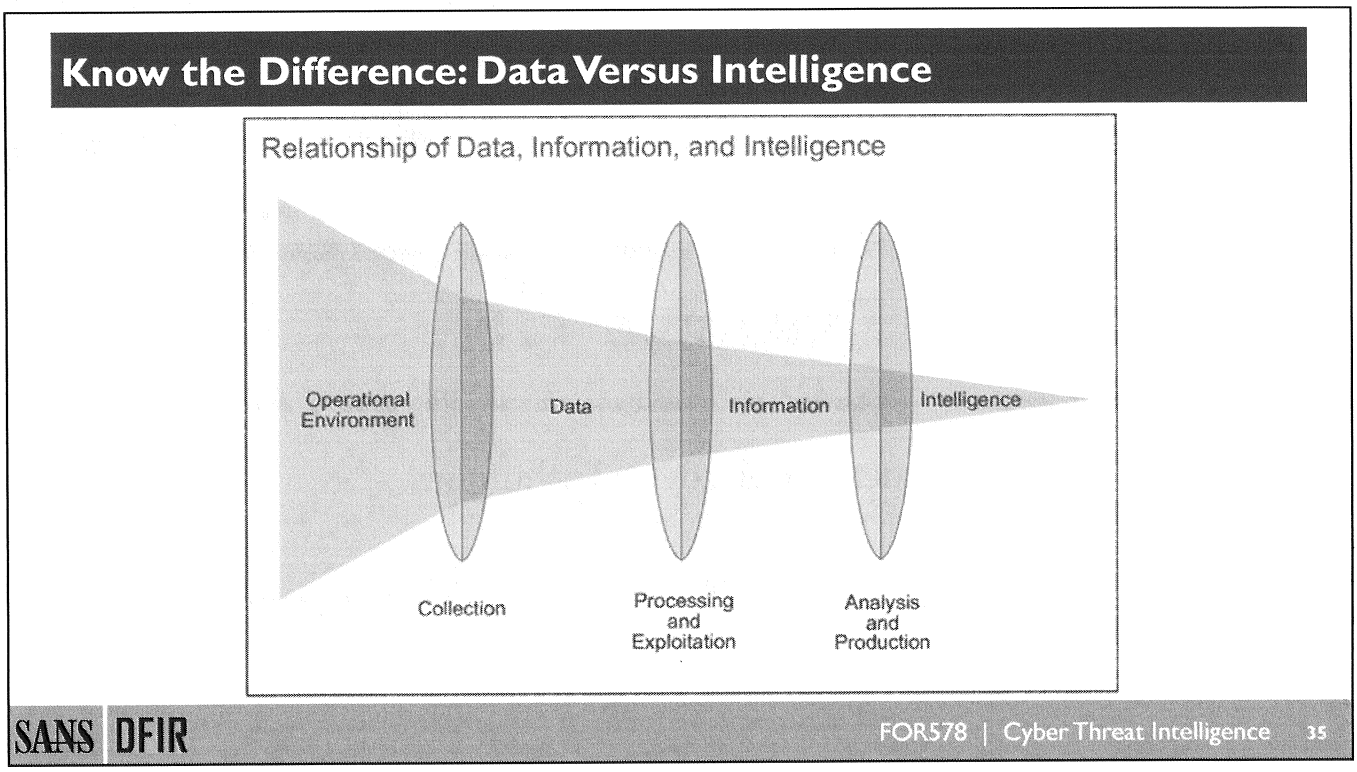
The security firm collecting from customers in the U.S. will see different data, threats, etc. than the security firm in Iran

Of the ~320 known targeted cyber activity groups worldwide, it is estimated only ~60 ever operate in any given region

Field of View Bias from Collection

Each person and organization has a limited field of view into threats. This is determined by the operational environment and intelligence requirements that govern each of us. As an example, the California based electric utility is going to see different cyber threat activity groups than the Germany based financial firm. This over the years has led to a perception that security vendors play favorites to their host countries. While there may be some of that the reality is more centered around collection. As an example, the Russian based antivirus company likely sees more U.S. and European based threats targeting their customers in Russia and the Middle East than the U.S. based security company would. Yet they report on those groups. The U.S. based security company likely sees Chinese, Iran, and Russian based threats targeting their customers.

All intelligence firms, security companies, analysts, etc. have methods and sources of data collection that drive how they perceive the world. This perception is not necessarily good or bad but should be considered when doing more strategic intelligence analysis.



Know the Difference: Data Versus Intelligence

Intelligence, as noted previously, is analyzed information. However, it is important to understand that to get intelligence requires lots of information and information requires lots of data. Each of us is able to collect data from whatever our operational environment is. The network defender in an oil company in Saudi Arabia has a different operating environment than the network defender at a financial company in New York. Systems, supply chain, geopolitical events, culture, personnel, point in time, mission focus, etc. all play a role in what our operational environments are not just the different types of data that can exist.

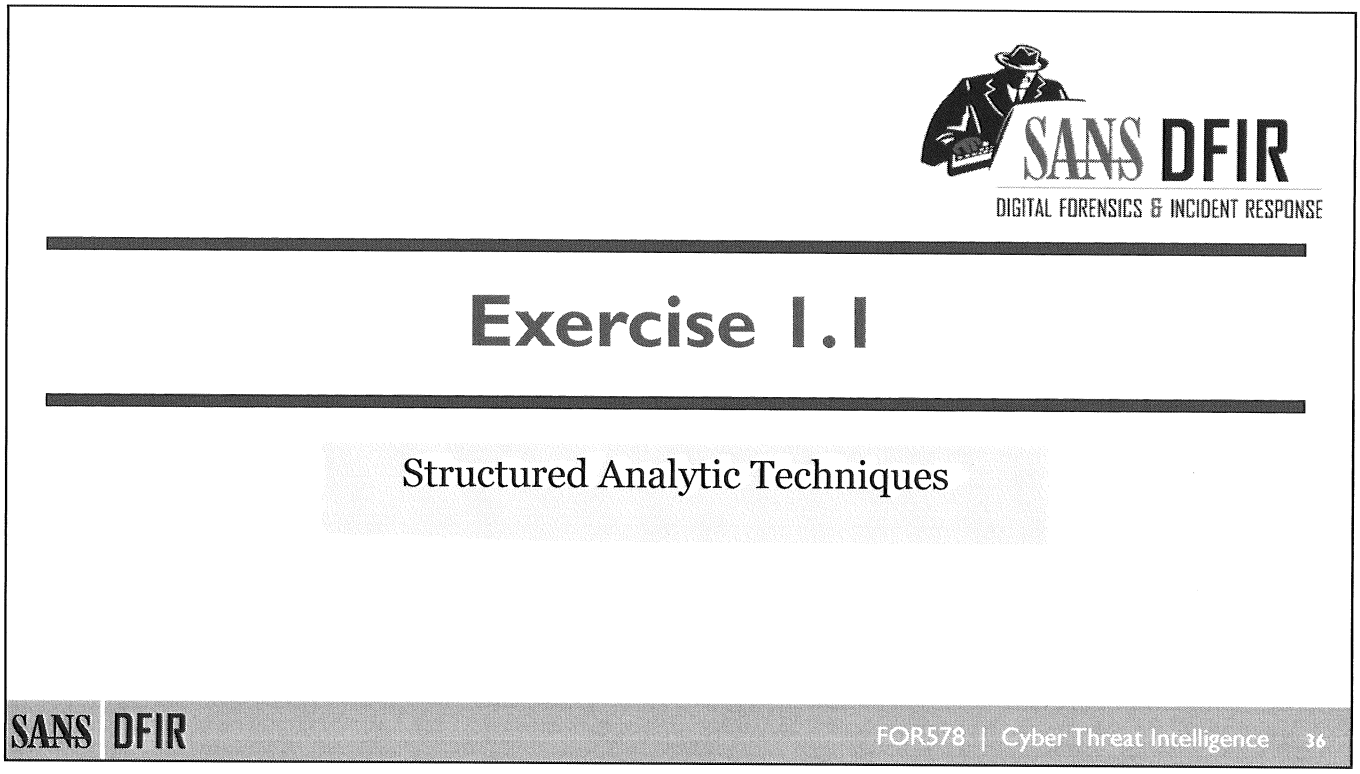
Data is simply sets of values and individual elements of what makes up information. Information is simply stated as the collection of data that can answer yes or no questions. Intelligence though really does not answer yes or no questions. It may be important to give a yes or no answer and intelligence customers want that, but ultimately, we all operate from the understanding that we never have all the data. You can never collect all the data from the operating environment meaning we will never have all the information needed to know anything for certain when it comes to an intelligence assessment.

Examples in cyber threat intelligence:

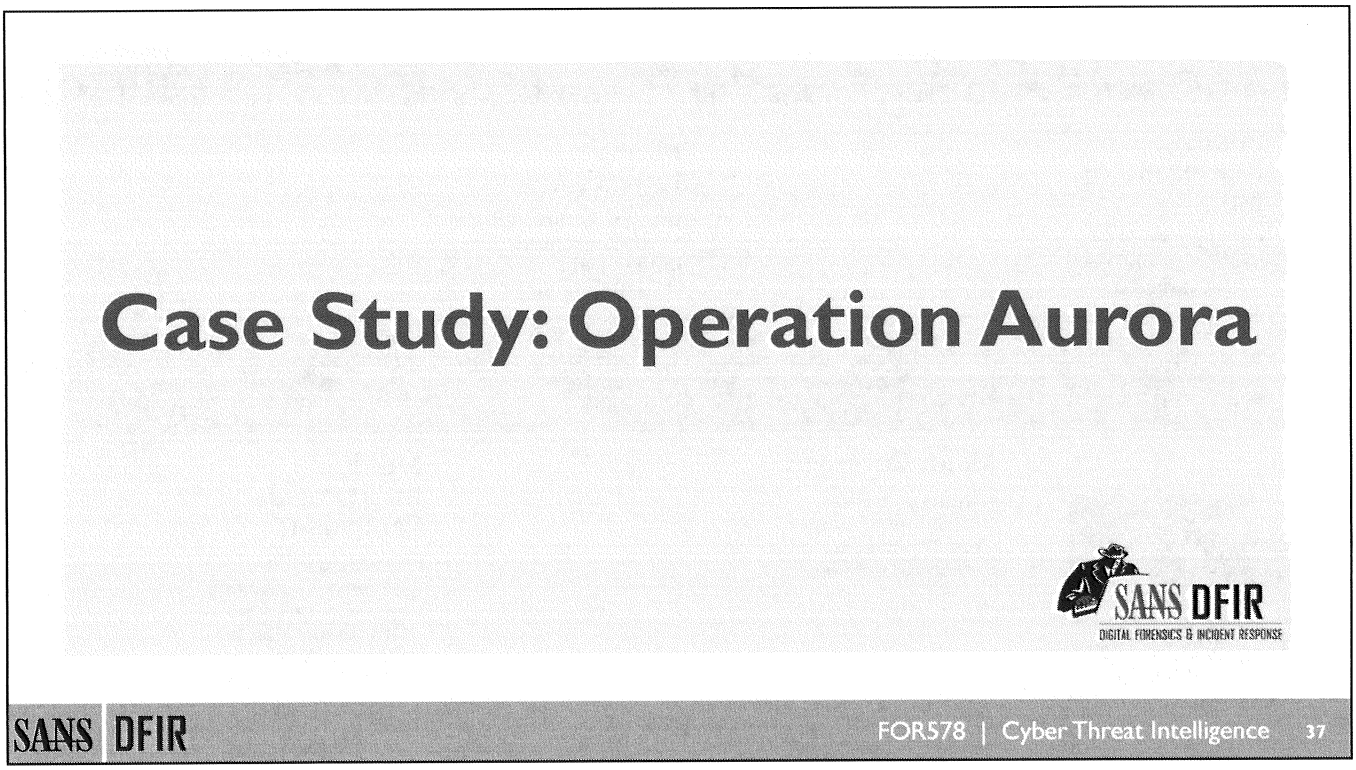
- This is an IP address (Data)
- This IP address is command and control for this malware (information)
- The malware is on our systems (information)
- We assess that the adversary is not purposely targeting our systems and that this is an incidental infection (Intelligence)

Image Ref: DoD JP 2-0

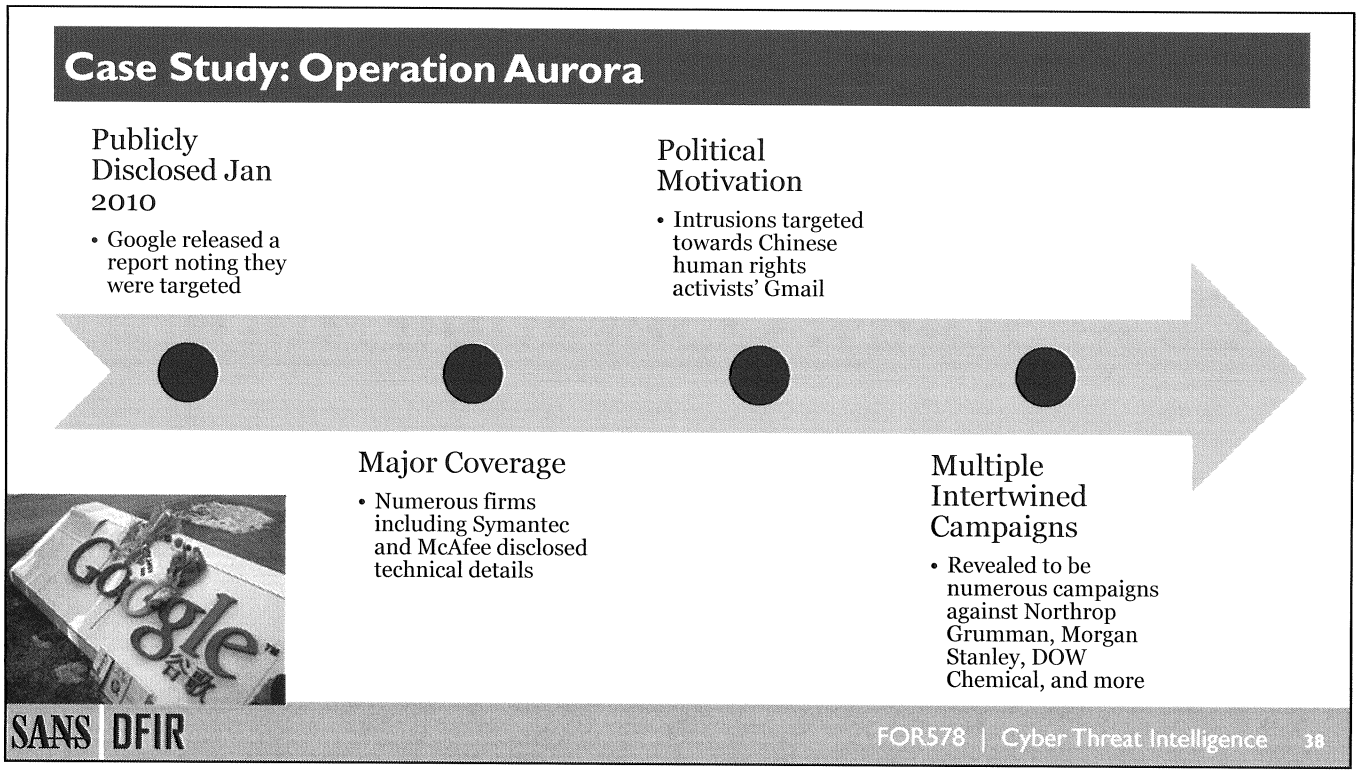
Reference: https://digital-forensics.sans.org/blog/2015/07/09/your-threat-feed-is-not-threat-intelligence/



Please refer to your workbook for Exercise 1.1.



This page intentionally left blank.



Case Study: Operation Aurora

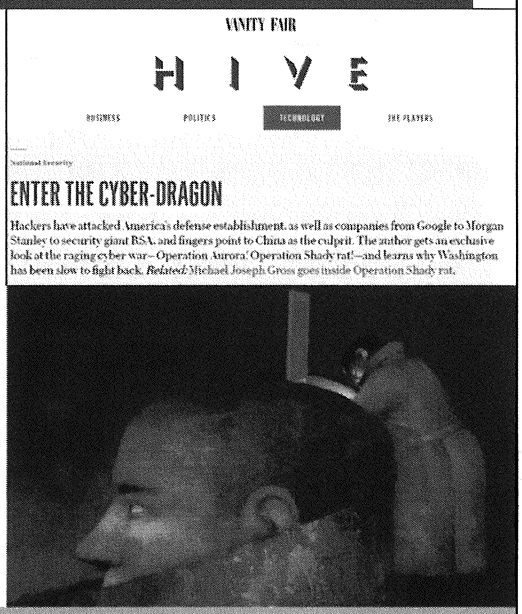
In many ways, Operation Aurora kicked off an industry. There were plenty of targeted threats long before Aurora and there were security firms tracking them but none grabbed as much public media attention up until that point as Operation Aurora. Operation Aurora was publicly disclosed by Google in 2010 after they detected the campaign targeted against them in December of 2009. Google, of course, had access to their own datasets though and were able to search through their own infrastructure to find that Gmail was a primary target of the intrusions. The main victims were the Gmail accounts of Chinese human rights activists and dissidents. However, the public information released by numerous firms including McAfee and Symantec revealed a much farther-reaching campaign linked to other campaigns as well.

Reference: https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

Image Ref: Wikipedia. Interestingly the Chinese government originally positioned the entire disclosure as staged by the US as a strategy to deny China access to Google.

"Enter the Cyber-Dragon"

- By 2011 it was understood that groups operating since around 2006 were all linked to Operation Aurora
  - The Elderwood Project
  - Operation Shady RAT
  - Operation Night Dragon
  - Breach of RSA SecurID
- Victims ranged from oil, gas, and petrochemical companies to defense contractors to banks
- Analysis across the campaigns and groups placed the attribution on China's PLA Unit 61398


VANITY FAIR

H I V E

BUSINESS POLITICS TECHNOLOGY THE PLAYERS

National Security

ENTER THE CYBER-DRAGON

Hackers have attacked America's defense establishment, as well as companies from Google to Morgan Stanley to security giant RSA, and fingers point to China as the culprit. The author gets an exclusive look at the raging cyber war—Operation Aurora, Operation Shady rat!—and learns why Washington has been slow to fight back. *Related:* Michael Joseph Gross goes inside Operation Shady rat.

"Enter the Cyber-Dragon"

The headline "Enter the Cyber-Dragon" captured readers' attention in Vanity Fair September 2011. The Washington Post, New York Times, and other major news sources also covered the breaches and the campaigns targeted towards a wide range of industries in the United States. It was in many ways the first significant attention given to the fact that companies were being targeted by foreign militaries and intelligence services. Cybersecurity started to become more of a household topic and the threat intelligence industry started to grow rapidly in response in the United States.

Reference:

https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf

https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html
https://www.vanityfair.com/news/2011/09/chinese-hacking-201109

https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf

Tools and Tradecraft

- Numerous zero-day exploits (initially 8) across the intrusions
  - Initially, the unique exploits bridged numerous malware families including PoisonIvy and Hydraq
- Combination of phishing emails and watering hole styled exploitation
- "Aurora" was a common file folder referenced in the malware used
- Attackers compromised Virtual Private Server hosting firms in California for Command and Control (C2) servers
  - Forensics of the compromised systems unraveled a string of C2 leading to consistent source IP addresses of Chinse government owned infrastructure
- OpSec failures by the Chinese operators were common such as using call signs that they also leveraged in social media and gaming
- Intercepted and then leaked communications showed Chinese government officials directed the campaign

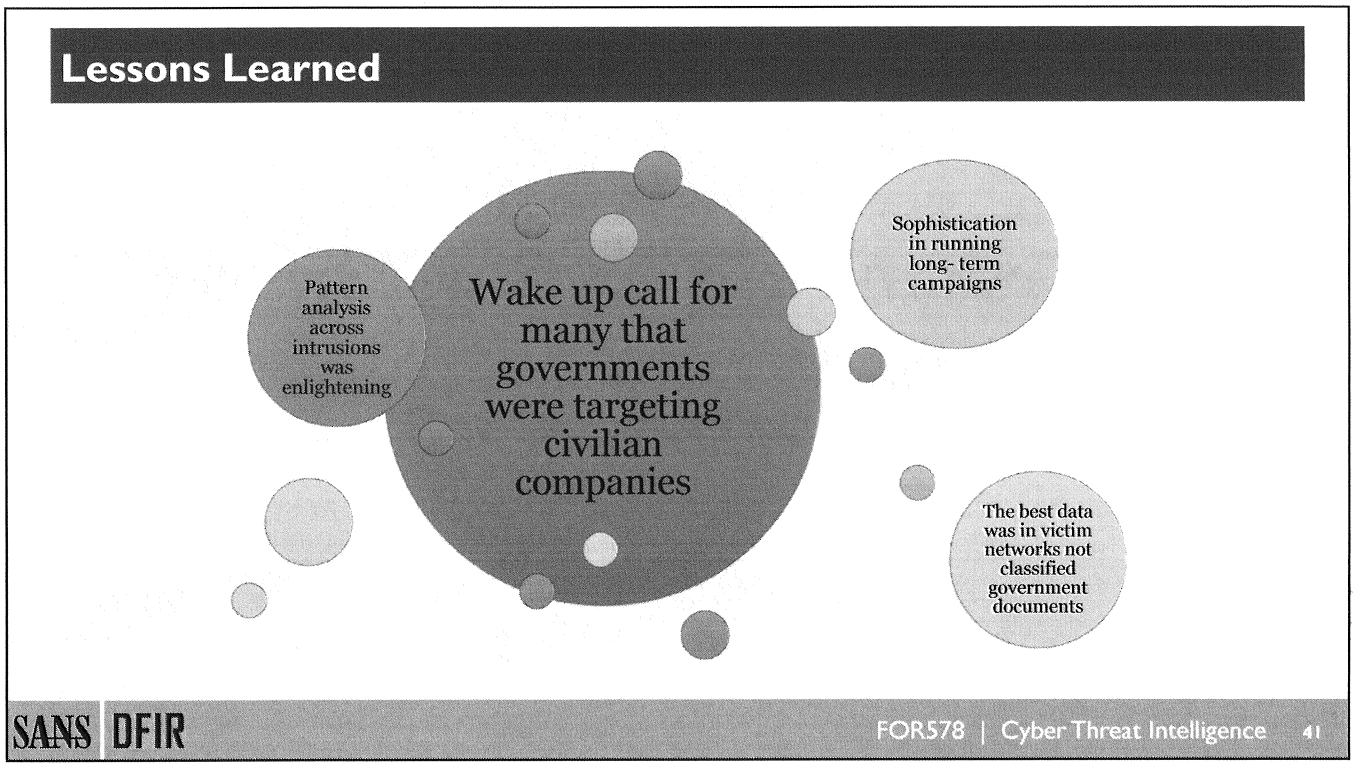
Tools and Tradecraft

The most impressive thing at the time was the sheer number of zero-day exploits leveraged in the campaigns. Zero-day exploits are not entirely uncommon but finding good zero-day exploits can be a challenge and in 2010 it was not so common to see them (in 2009 only 8 were identified and patched the entire year). The Chinese based campaigns through leveraged numerous zero-day exploits, the Elderwood Project group leveraged 8 alone giving them remote code execution on systems through Internet Explorer and Adobe vulnerabilities.

The campaigns were coordinated across different tactics including phishing emails and watering hole attacks. Interestingly, there was infrastructure and capability overlap between most of the intrusions observed helping to bridge the intrusions into campaigns. Shared datasets between companies and researchers helped to unite a singular view on the overall campaign being coordinated against over 30 U.S. companies. Opsec failures, leaked intercepted cables, and consistent patterns in infrastructure choices helped attribute the intrusions to the Chinese government.

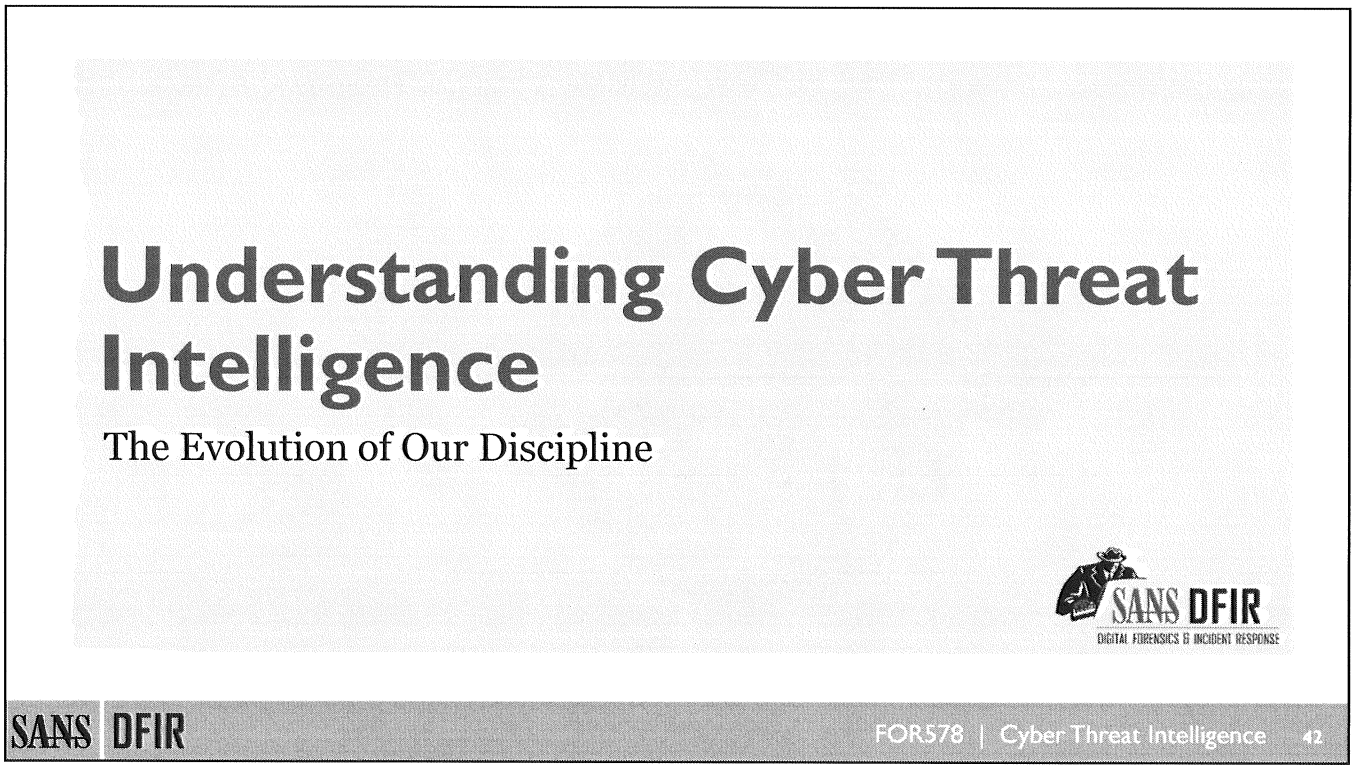
Reference:

http://www.nytimes.com/2010/11/29/world/29cables.html?_r=1&hp



Lessons Learned

As the cyber threat intelligence industry started to come into its full stride there were numerous lessons learned from Operation Aurora and related campaigns. First, many of the campaigns were cross-sector meaning that sharing simply inside of one's industry vertical would not be enough to understand the full scope of adversary efforts. Second, at the time, it was considerable to note that an ongoing effort by an adversary would be so well coordinated and have access to highly sophisticated tool sets and exploits. Third, it was a wake-up call to most of the industry that foreign governments were targeting civilian companies; a fight that definitely did not seem fair to most. Lastly, all of the best data for the identification of these campaigns were not held within the government but in the private sector; it was eye-opening for many to realize that incident response and intrusion data in these datasets could lead to discoveries that would otherwise be classified if gathered differently.

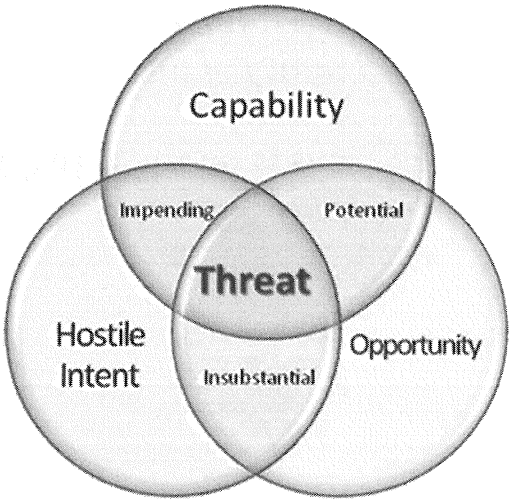


"Tell me what you know.
Tell me what you don't know. Then tell me what you think. Always distinguish which is which."

-Colin Powell

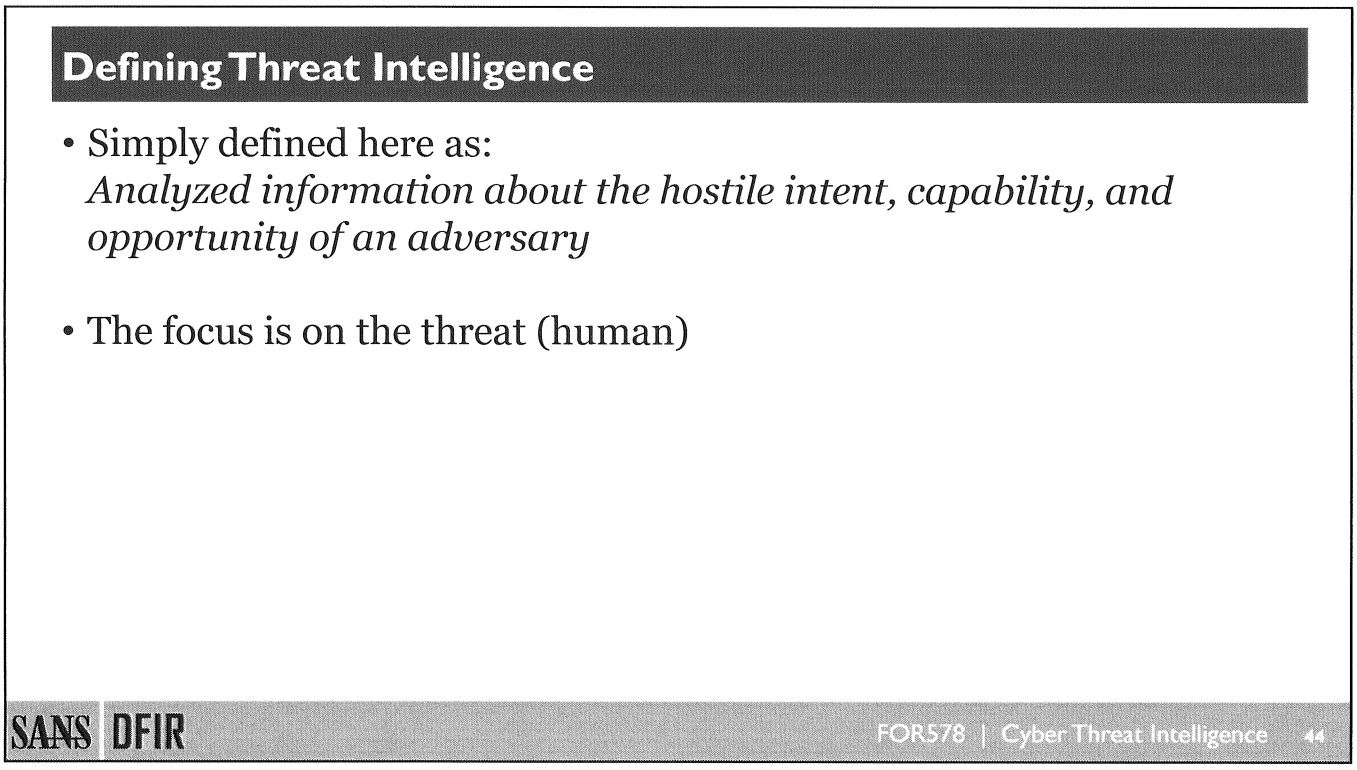
What Is a Threat?

- Organizations must know what their threats are to accurately collect and use threat intelligence
- Threats can be established by evaluating Capability + Intent + Opportunity



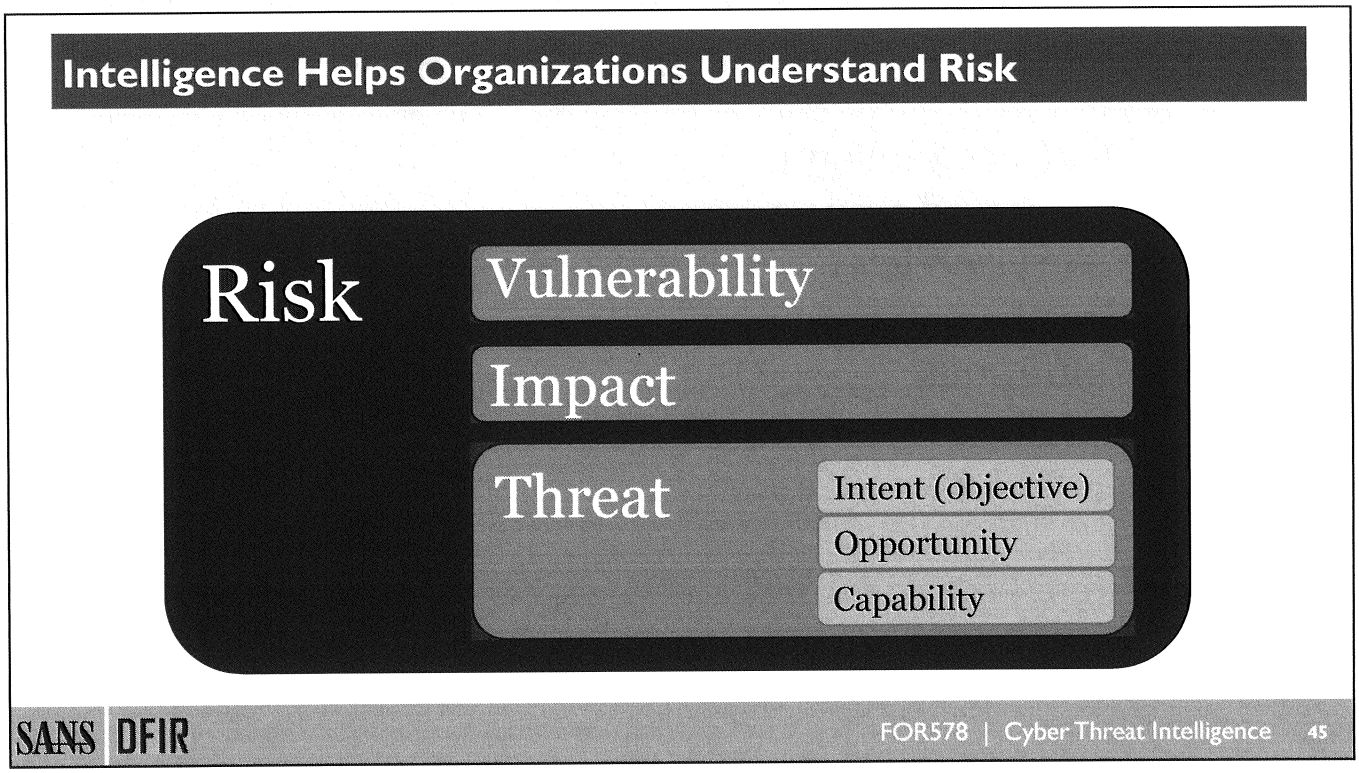
What Is a Threat?

Organizations must understand themselves before they can understand what constitutes a threat to them. This is one of the most significant pitfalls in the Threat Intelligence Community. Without good knowledge of the business operations and goals, network and its assets, and information such as software versions and hardware choices, it is difficult to identify what constitutes a threat. Just because something is a piece of malware or a vulnerability does not mean it is something that can impact an organization. If the vulnerability is for Windows XP but the organization you are at only has Windows 7 and Windows 8 systems, then that vulnerability is not of concern. The UK signals intelligence agency (GCHQ) has the capability and opportunity to pose a significant threat to U.S. intelligence operations. However, there is no hostile intent, so they are not a threat. Getting an organization to the security maturity that it can truly understand what constitutes threats to it should be a major goal of any threat intelligence program. Having that maturity and all the components that go along with it is significantly "ahead of the curve" in terms of average organizational security.



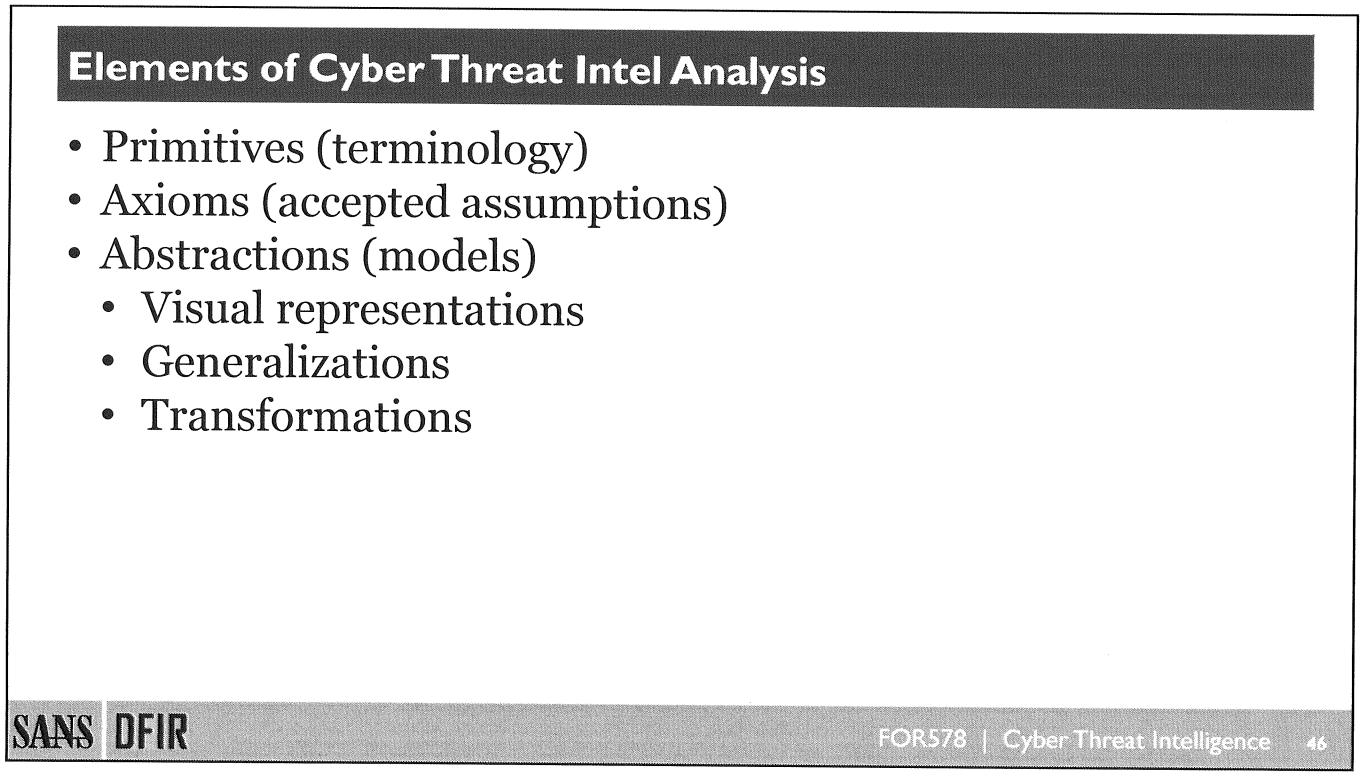
Defining Threat Intelligence

There are a number of definitions for threat intelligence available. However, in understanding what intelligence is and what threats are a simple definition can be crafted. This definition is presented for the purposes of this course and is not meant for canonical presentations. Differing definitions are fine as long as it is understood that the focus is on the threat – the human. The focus is not on activities such as identifying vulnerabilities and patching them faster. Vulnerabilities represent an opportunity to the adversary but alone are not threats just as malware alone is not a threat.



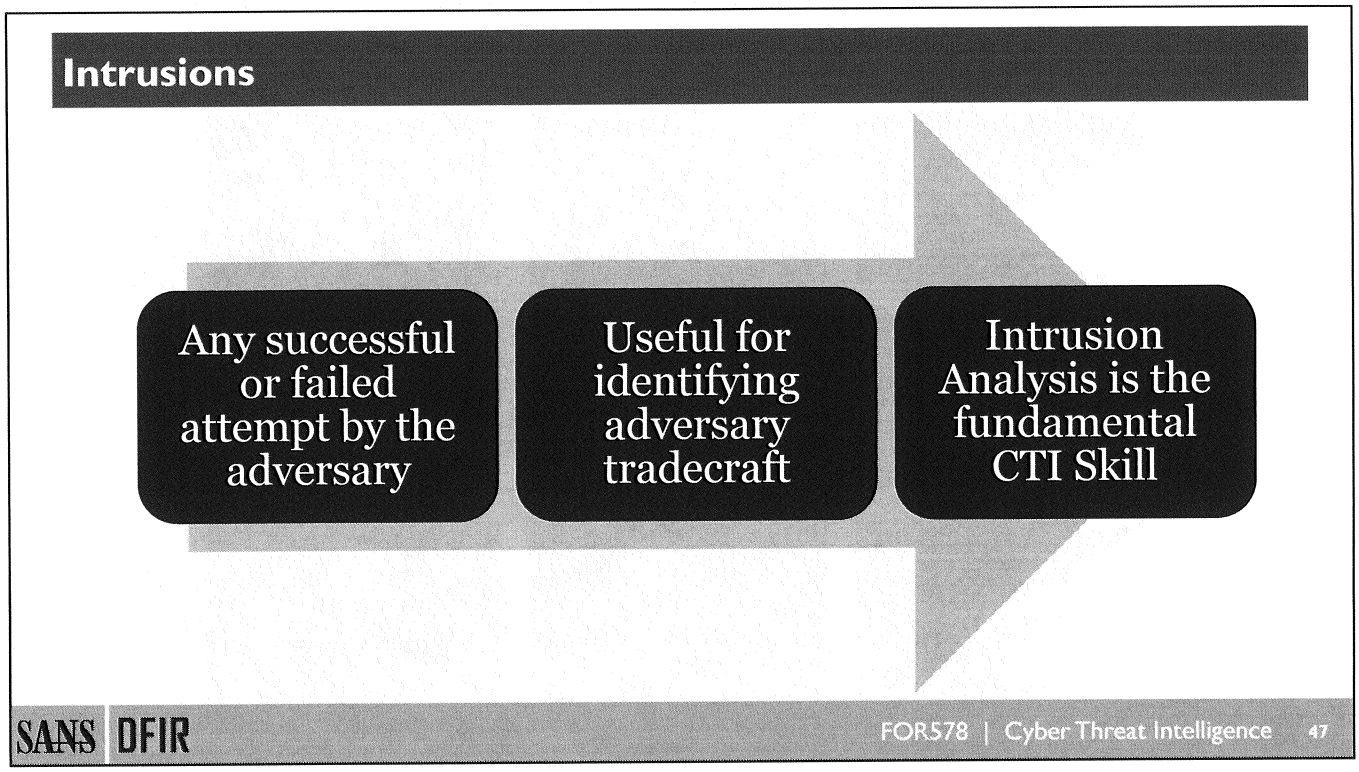
Risk is defined many ways, depending on the subject matter. For this course, we use the definition illustrated in the chart here. What these words mean will be articulated in more detail:

- Vulnerability: The susceptibility of an organization to a compromise of confidentiality, integrity, or availability.
- Impact: The effect of a compromise on an organization.
- Threat: Various attributes of the actor seeking to compromise an organization, which is further broken down into:
  - Intent: What the actor seeks to achieve.
  - Opportunity: Conditions (technical, logistical, legal, etc.) necessary to achieve the threat's objectives.
  - Capability: The degree to which the adversary can succeed in accomplishing his or her objectives.



Cyber Threat Intel Analysis is all about a way of thinking—about adversaries, about intrusions, about defense, intelligence, and so on. One primary takeaway for students is the ability to think within a certain framework. The human brain devotes an incredible percentage of its capacity to the task of communication—from parsing symbolic primitives such as words and pictures all the way to the establishment of semantic meaning. As a result, how we think is deeply affected by how we communicate—from the syntactic use of written and spoken language through lexicon to the data visualized in more abstract shapes and layouts. Clarity and consistency in communication, it follows, foments the same in thought just as they do in the exchange of ideas. They also enable further abstraction of ideas, providing broader semantic meaning and interpretations of what begins, in our case, as extraordinarily detailed and highly-dimensional data.

In light of these biologically-mandated (yet philosophical) realities, capably operating in the CTI domain necessitates explicit agreement on fundamental terms, axioms, and prescriptive abstractions (that is, models). We construct abstractions, or models, by finding new ways of generalizing, transforming, or visualizing certain primitive ideas in our domain, subject to a certain set of axioms. It is these primitives, axioms, and abstractions that provide the definition of Cyber Threat Intel Analysis.

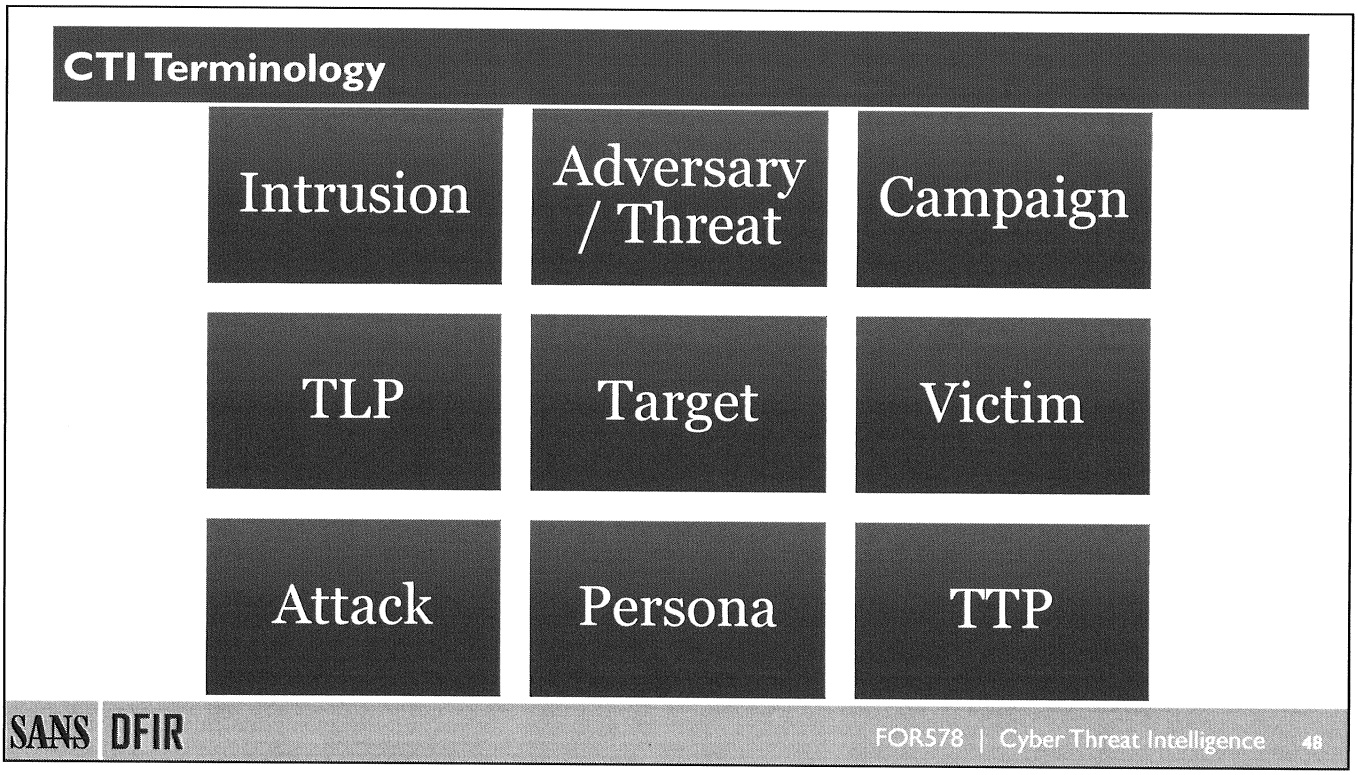


Intrusions

The core of all cyber threat intelligence is intrusion analysis. Intrusions are any attempt, successful or failed, that the adversary makes to compromise or attack systems. Even failed intrusions have a lot of information that we can gather for analysis. As an example, failed intrusions often represent the adversary's first methods to compromise an organization which might have commonality with first methods used against other organizations or even overlaps with future tradecraft leveraged.

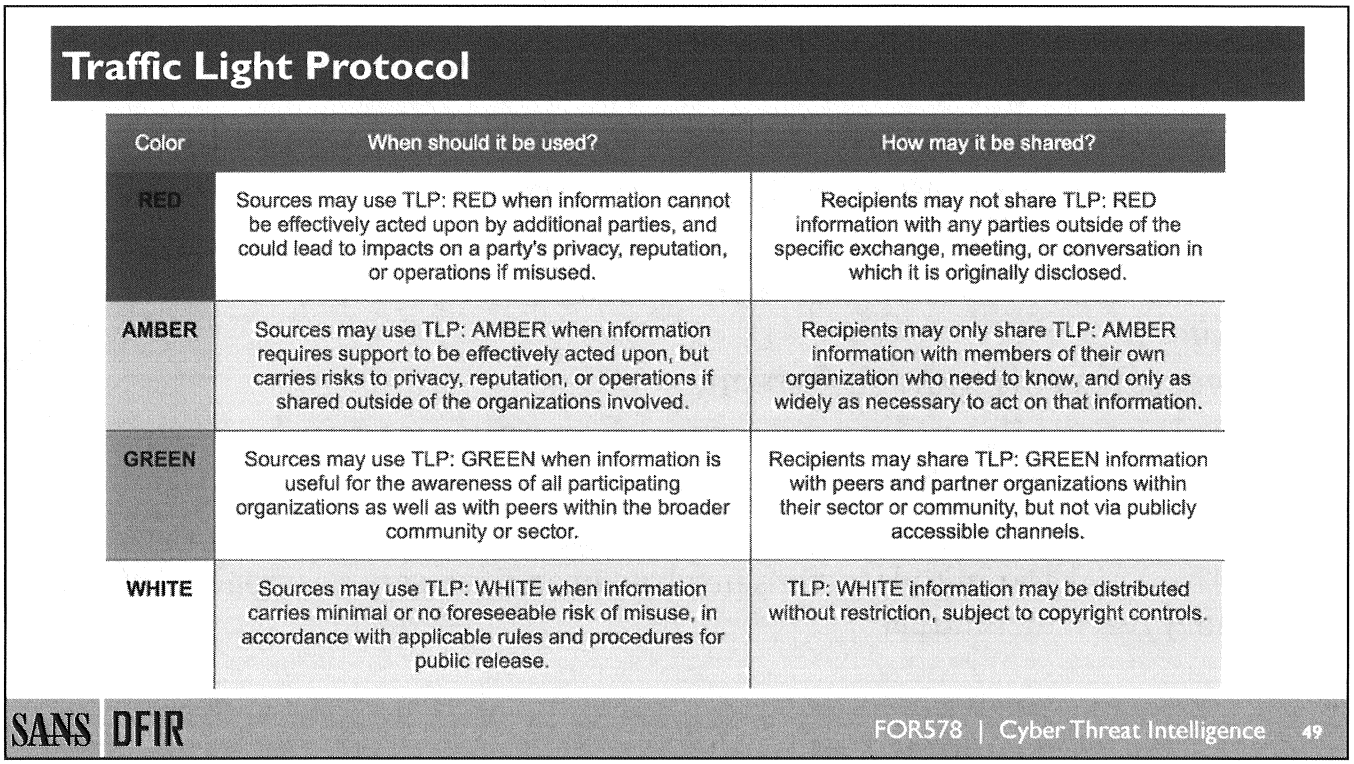
Ultimately, regardless of the level of threat intelligence being examined, it all begins with intrusions. If a national-level government wants to understand the threat landscape and its impact on a global trade agreement, there were likely thousands of intrusions analyzed across large portions of time to understand all the adversaries that made up that threat landscape and their potential impact.

Intrusion analysis will be explored in-depth in Section 2. It is the aspect of cyber threat intelligence that most gloss over and yet it is the underpinning of everything we do and the reason that the best threat intelligence is often the threat intelligence inside your own organization.



These terms are used loosely throughout our industry, so they are often misunderstood. In this course, we strictly adhere to the following definitions:

- An **intrusion** is any successful or failed attempt by the adversary to compromise a system
- A **Campaign** is the adversary's mission focus, such as a malicious group of adversaries targeting financial networks.
- An **adversary** or **threat** is an individual who is involved in the execution of an intrusion. We use the term *threat* interchangeably with *adversary*. Note that a threat is *not* a vulnerability (as used in Microsoft's "threat modeling," which really is modeling vulnerabilities), nor is it a tool (such as a piece of malicious code).
- A **compromise** is the *successful* violation of data confidentiality or integrity that was the intent of the adversary. Keep in mind that CTI is a threat-oriented discipline, and as such, a compromise is the successful execution of an intrusion in accomplishing the objectives of the adversary. The term "breach" is also commonly used, and functionally synonymous with "compromise" for our purposes.
- A **pivot** is leveraging intelligence to identify additional intelligence. We cover this later when we discuss the Indicator Lifecycle.
- A **victim** is an individual, network, or system compromised in the course of achieving an objective.
- A **target** is the intended victim of an intrusion.
- An **attack** is an intrusion executed with the intent of catastrophic data corruption, or, a denial of service. This falls more into the realm of sabotage. Attacks are a different sort of intrusion, and the convoluting terms intrusion and attack can have dangerous consequences, particularly with policymakers who see an attack much differently than a compromise of data confidentiality.
- A **persona** is the fake name or identifier that an adversary takes; it can be operated by one or more adversaries operating on the same or different groups.
- A **TTP** stands for Tactic, Technique, and Procedure. A Tactic is the higher-level tradecraft that the adversary intends to use to reach an objective (e.g. compromise a domain controller to get passwords to target accounts). A Technique is the manner to which the adversary is going to accomplish that Tactic (e.g. leveraging a specific exploit to gain access to the domain controller). A Procedure is the more granular approach to accomplishing the Technique (e.g. the commands typed to launch the exploit).



Usually when governments are involved there are classification systems for the data shared. As an example, in the U.S, Canadian, and several other communities there is the Traffic Light Protocol (TLP). The TLP is built along a spectrum, where TLP Red is very sensitive data at one end and TLP White is completely free to share on the other. TLP Amber permits the sharing of information within an organization, and TLP Green allows for sharing with partners and peers but not via publicly accessible channels such as the internet. The TLP standard will be discussed more in Section 4.

Reference:

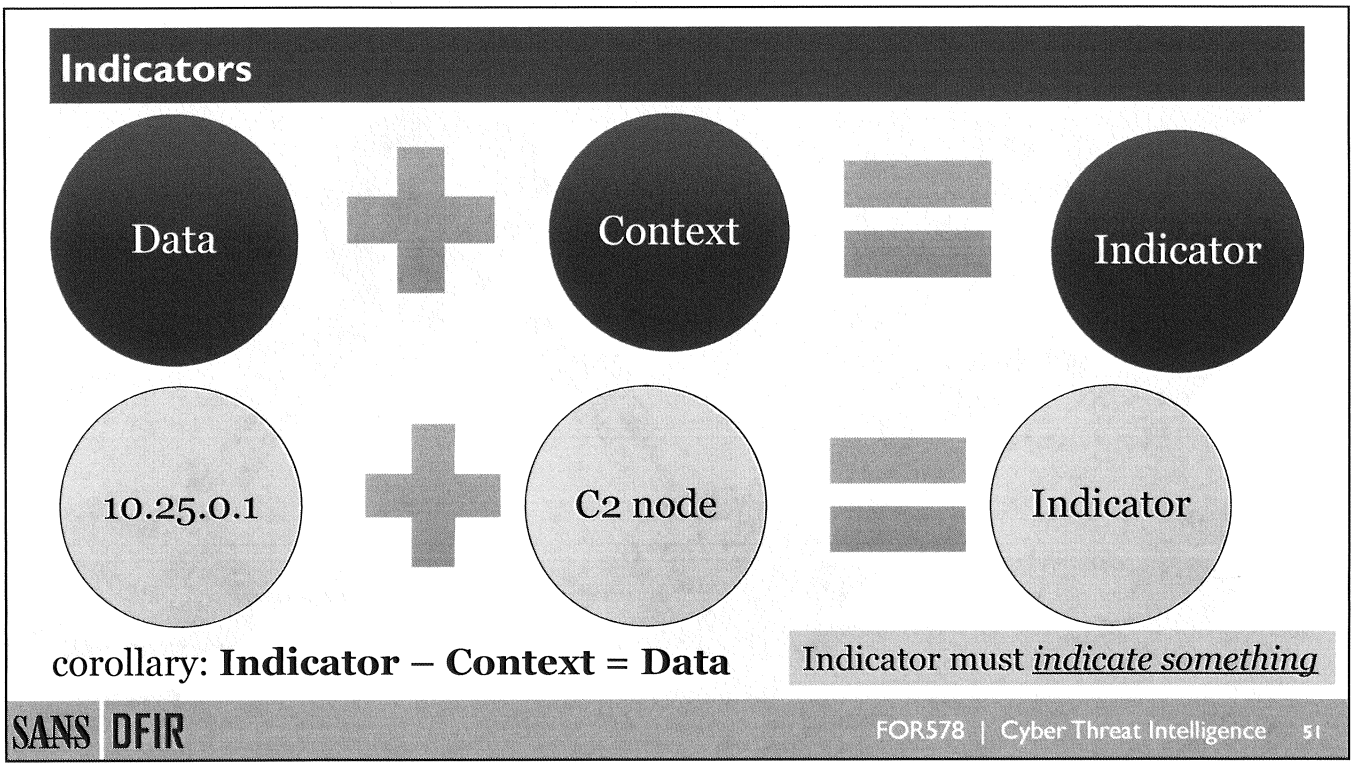
https://www.us-cert.gov/tlp

Adversary/Threat and Personas

- Adversaries are your threat when they have the opportunity, intent, and capability for doing you harm
- Adversaries initiate intrusions which may lead to a compromise
  - An adversary's series of intrusions is their campaign or focus of their efforts
- Adversaries often have Personas
- Personas are the online presence of an adversary and adversaries often have multiple
- The goal of the adversary is their target
  - There may be multiple victims involved in an adversary's campaign before they reach their target

Adversary/Threat and Personas

Adversaries initiate intrusions. When the adversary can initiate an intrusion on you based on intent, opportunity, and capability they are a threat to you. Those threats may fail in their intrusion attempts or succeed – when a successful intrusion takes place it is a compromise. Adversaries often leave a fingerprint behind within the code, their tactics, or their presence. That figurative fingerprint is the focus of threat intelligence. The adversary may also have multiple personas depending on how they structure their intrusion.



Indicators

Debates over what makes an indicator, and what breakdown of indicator types—if any—is useful to the CTI domain. For the purposes of this course, we will use the general definition that an indicator is data, in addition to some context describing an aspect of intrusions.

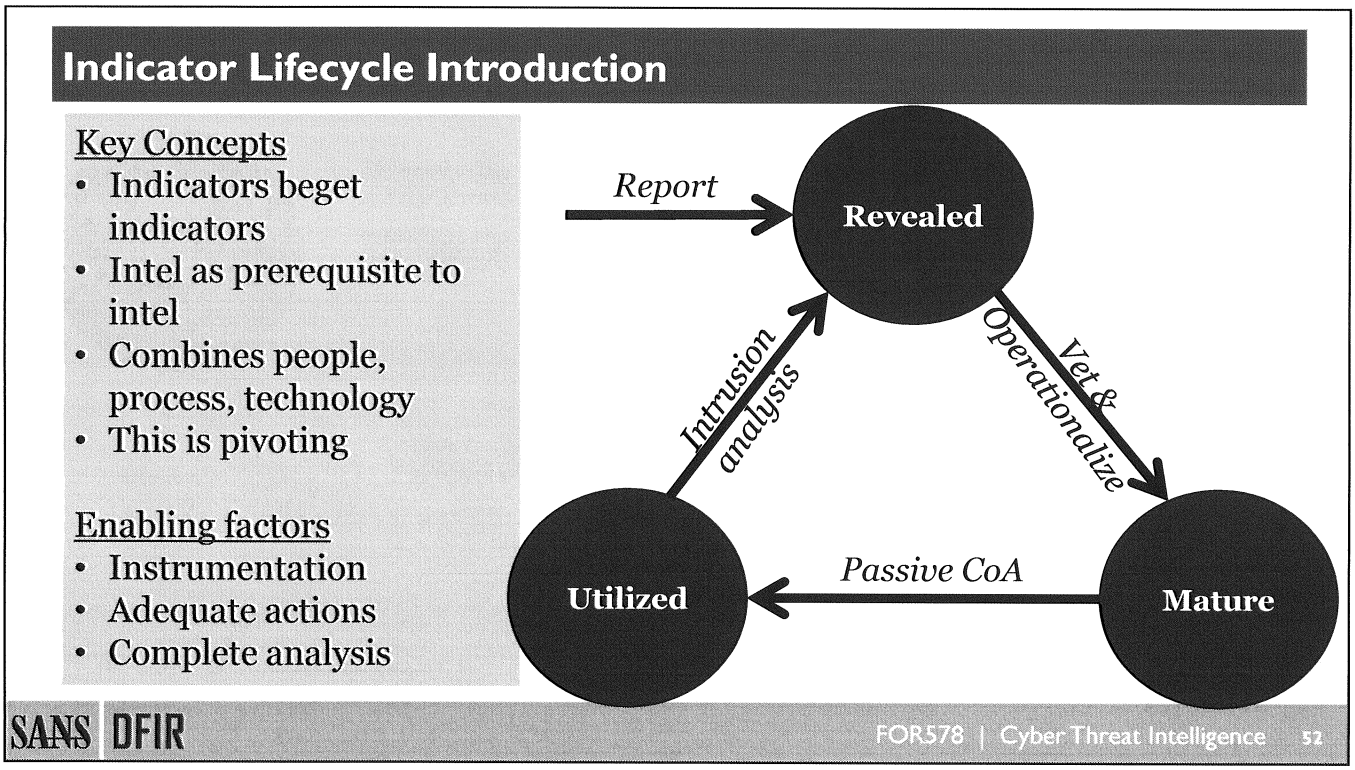
The indicator we were provided with earlier, 10.25.0.1, was described as an IP address involved in remote command-and-control of victim systems. This may not seem like much, but as you'll see later, it meets the minimum criteria to be useful. The data is the address 10.25.0.1. The context is that this is an adversary's infrastructure utilized for command-and-control of victim systems.

If all that was provided was the IP address, that is just data. **An IP address is not an indicator.** It has to be an indicator of *something* related to intrusions to qualify as a CTI indicator. Otherwise, it is *indicating* nothing. It is simply an address. The same goes for an e-mail address, a domain name, a file name, a hash, and so on.

Indicators of compromise (IOCs) are artifacts that are useful in identifying indications of threats on the network or system.

Historically, IOCs have been maintained and used by Antivirus (AV) companies as signatures:

- Malware often bypasses AV detection by modifying or obfuscating these signatures
- AV signatures needed to be created with extremely high confidence
- IOCs can be created giving a lower confidence to give an initial analysis



If you'll recall from the beginning of the last section, you are provided with notification that one of your organization's IP addresses is talking to another known-bad address on the Internet. The bad address is 10.25.0.1, and the type of activity is command-and-control (C2).

We now need to take this paltry amount of information and pivot from within our available data sources to identify what, if any, malicious activity is occurring and how to respond. Guiding these actions is a model we call The Indicator Lifecycle

The **Indicator Lifecycle** describes how indicators (or intelligence, if you will) beget indicators. It is a true cycle, enabled by people, process, and technology of discovery, maturation, and exploitation. The Indicator Lifecycle can be represented as a directed-graph *state diagram* describing the states and transitions that move an indicator between states. That diagram is illustrated here with each action and state discussed in the subsequent slides.

The Indicator Lifecycle is a powerful reality of CTI, but it also suggests—correctly—that one must have intelligence in the first place in order to acquire more intelligence. This is true in a general sense, and in a specific sense with respect to the campaigns that will be discussed later in this course. A large amount of intelligence about one adversary may not help at all against another adversary for whom an organization has no intelligence whatsoever. This is, of course, a shortcoming of the CTI approach that must be addressed in ways other than analysis and network defense; intelligence sharing, in particular, helps fill this void.

We start our discussion of the indicator life cycle at revealed. This state is straightforward. An indicator, some intelligence, has been revealed to us about a specific threat to the assets we intend to defend. Another way to name this state could be simply *known*.

This may have come to us through our own analysis of a past intrusion (which we can call *Detected/Discovered By Us,* or DBU). These indicators will be the most reliable, and those which may be the easiest to make actionable. Alternatively, the indicator may have come from some partnership such as a collaborative information-sharing arrangement (ISAC) protected by an NDA, so-called "threat intelligence feeds," and so on,

which we can call *Reported To Us,* (RTU). These indicators will typically have less context, may be difficult to operationalize, and simply by their nature will have less context around them than internally-derived indicators.

Indicator or intelligence in hand, we must now do something with it. We must determine whether it is actionable and if so, execute the appropriate course of action.

In order for an indicator or piece of intelligence to become mature, it must be vetted. This vetting process involves determining the viability of using the information in hand either alone, or in some context, to detect the malicious activity in the specific environment one is defending. It also involves assessing whether the intelligence is reliable and whether it is good intelligence and adequately represents the malicious activity from which it was derived in a way that is actionable in a particular environment.

The best way to make this decision is to first leverage the indicator for the discovery course of action (remember when we said the CoA matrix connects to the indicator life cycle?). This action is research-oriented; it will not adversely impact an environment in the form of overly aggressive mitigating actions, nor will it bury analysts in false positives as it could if we jump straight to detect (be patient, that's next). What must first be done is historically searching available data sources to discover whether or not this was observed in the past, and if so, investigate further to determine whether the activity was malicious or benign.

At the point where vetting and discovery have been completed and the indicator is determined appropriate for additional actions, it should be applied to two other CoAs: detect and the best available mitigating action, if any exists. After this point, it is considered mature.

All of this brings up an important reality and implication for subscription threat intelligence feeds: Indicators that are viable in one environment may not be viable in another. Additionally, it's often not possible to automagically vet indicators *en masse*.

Once a vetted indicator is assigned to a course of action and deployed, and that course of action matches network and/or system activity, it is considered **utilized**. This could manifest as a positive finding in log searching (that "eureka!" moment) as a **discovery** course of action, or an IDS rule firing on real-time activity as a **detection** action.

This applies to every course of action, but the passive courses of **detect** and **discover** are of particular importance to transition away from at this state. In fact, if neither passive course of action are applied to an indicator, one will never know whether or not this state is reached, and the Indicator Lifecycle is broken for those indicators. They will never beget additional indicators. This is why earlier we stressed the importance of applying both to an indicator; otherwise, we have a bit of a cyber Schrödinger's Box scenario.

Once an indicator is in the utilized state, analysts have a lot of work to do. At this point, there is malicious activity that must be analyzed. An indicator will rarely, if ever, represent a complete set of malicious activity on its own. What this means is that starting with the activity against which an indicator is utilized, one must build a complete picture of the intrusion. This process of articulating each phase of the Kill Chain beginning with the utilized indicator will reveal many, many more indicators, each of which will then begin the life cycle anew.

It's important to note: All intrusions, regardless of their degree of success, potentially have additional indicators to be revealed once identified.

Execution of the Indicator Lifecycle can be tedious and time-consuming, particularly when vetting and operationalizing revealed indicators. Doing so during response to an incident where adversaries were able to proceed to the latter Kill Chain phases is particularly challenging. In such a case, revealed indicators can get lost, or vetting and operationalizing indicators may be assigned a lower priority than, say, determining impact through forensic analysis of compromised systems. When possible, it is advisable to assign one analyst the responsibility of building detections off of indicators revealed in an IR effort.

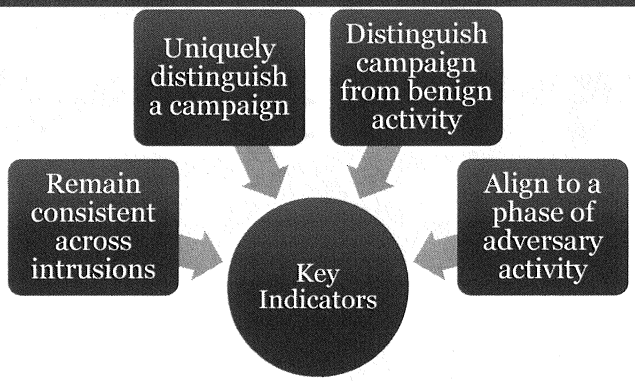
The Indicator Lifecycle isn't particular about how useful an indicator is to identifying intrusions, and certainly not distinguishing between APT-caliber intrusions for which a full intel-driven CND treatment is appropriate versus broad-based threats well mitigated by conventional defenses like antivirus software that don't necessitate the same due diligence. For this reason, it is important to only mature indicators through the life cycle selectively; only those that are with high confidence useful to an intelligence-driven paradigm should be subject to the level of analytical rigor and instrumentation we discuss here.

Because of the cyclical nature of this process, a set of indicators is often imagined as a snowball rolling downhill. The analogy is valid in many different respects: The longer the snowball rolls downhill, the larger it gets and the faster it rolls. Its mass increases nonlinearly. The same is true of indicators. The more an organization has, the more it detects and the more it accrues, with the rate of indicator accrual increasing over time. One might even say *indicator acceleration increases over time.*

This analogical and theoretical fact is played out in reality on networks around the world, and importantly, it is indifferent to the validity of the indicators in the snowball. Bad indicators will beget bad indicators just as good will beget good, and this stream of bad indicators will increasingly accelerate once they've been utilized. Another aspect of the snowball analogy that extends to indicators is the "yellow snowball." Have you ever tried to make a yellow snowball white again? It can be that difficult, or even impossible, to extract bad indicators from the intel snowball once they've been utilized; so, for the sake of everyone in your organization *and those with whom you share*, please, don't pee in the intel snowball.

Considering intelligence applied to the Indicator Lifecycle comes from other organizations as well, there's an external risk to your set of indicators. The consequences for shared CTI are that the risk of pollution is high when the inevitable pressure from management to automate CTI ingestion occurs. This is exacerbated with the common perception that all external indicators must be processed, and proliferation of multiple (often highly-redundant) sources of external intelligence become available. Just remember that this is not risk management; it's risk *avoidance* and is in contradiction to one of the axioms of Cyber Threat Intelligence.

Key Indicators



- Identify as many as possible
- Ideally at least two in different KC phases to define campaign
- Ideally across three or more intrusions

Arguably the most important characteristics of a campaign are its key indicators. Key indicators are those that meet all the following criteria:

- Remain consistent across multiple intrusions.
- Uniquely distinguish a campaign from other campaigns.
- Distinguish a campaign from benign activity.
- Align to a single category of adversary action (such as Exploitation)

How many key indicators define a campaign? As many as possible. Ideally, at least two key indicators exist in two different phases of the Kill Chain for a given campaign.

The key indicators are the most important pieces of intelligence to leverage in a detective and mitigating course of action! Key indicators for which an optimal mitigation, or detection, is available prioritize most highly those categorical courses of action that need investment.

Analysts occasionally debate in general terms the value of certain data types as indicators (or key indicators). The truth is that no such statement can be made in general terms about the value of an e-mail address, an IP address, and so on as an indicator because *it all depends*.

What does it depend on? By now, hopefully, you know the answer: As with most things in CTI, it depends on the adversary. Some campaigns reuse the same delivery and C2 infrastructure over a period of years. Others change infrastructure in these two phases every single intrusion. So, what is the value of an IP address as an indicator? It depends. In the first case, extremely valuable. In the second, pretty much worthless (on its own).

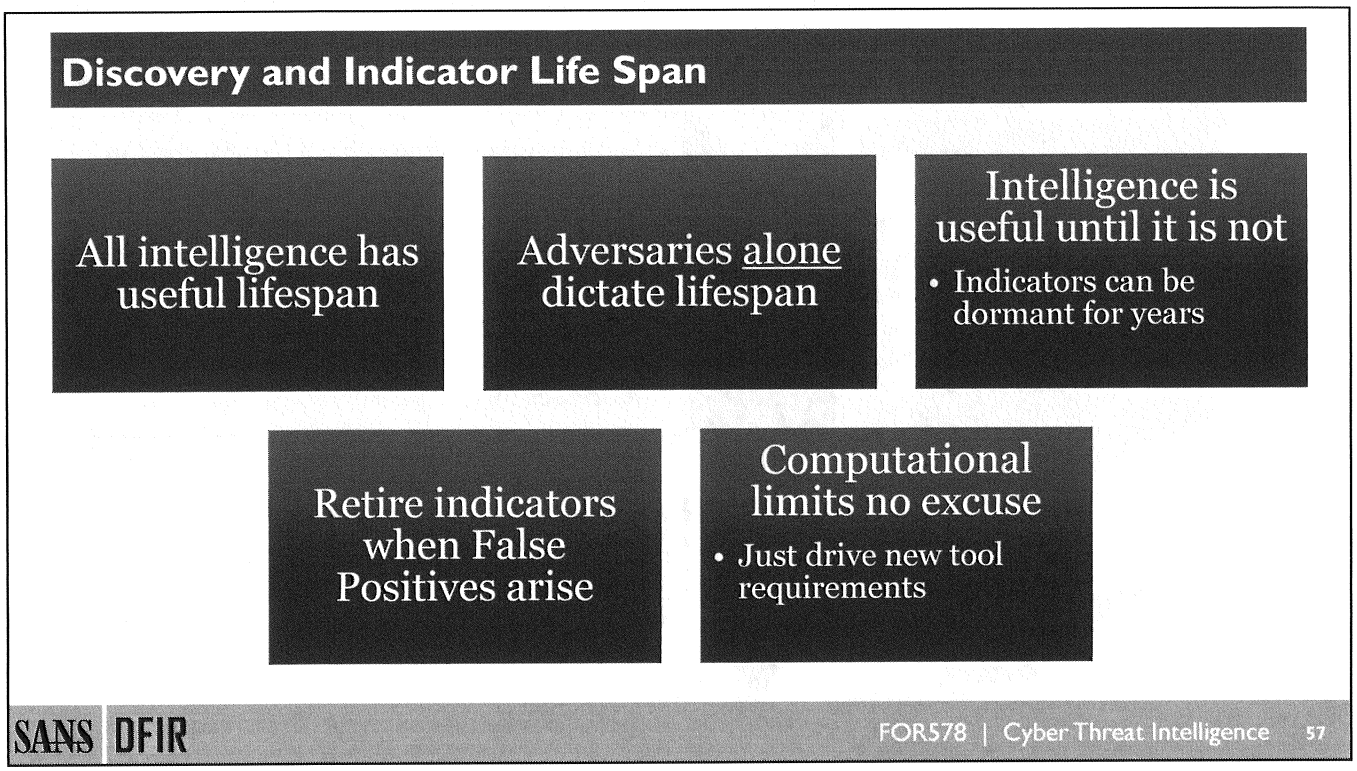
The ideal key indicator is *any* observable that meets the criteria of a key indicator. It could even be a string in a dropper or encoded C2 channel, the meaning of which is totally unknown to the analyst. The bottom line is that it can be used as a key indicator.

Key Indicator Examples

Indicator	Kill Chain Phase	Diamond Vertex
ihijackedyourdomain@cloppert.org	Delivery	Infrastructure
Customized *gsecdump*	Actions on Objectives	TTP
Plug-X DNS variant w/mutex *pWn3d*	C2	TTP
Domain registered by badguy@ene.my	C2	Infrastructure
Carrier PDF author *Benson Hedges*	Weaponization	TTP
google.co.uk referrer w/ "inurl:.jsp" and Polish language setting	Reconnaissance	TTP

Some example key indicators are provided here; these would not necessarily work for anyone else either but could be key for you distinguishing intrusions of similar capabilities or infrastructure from each other:

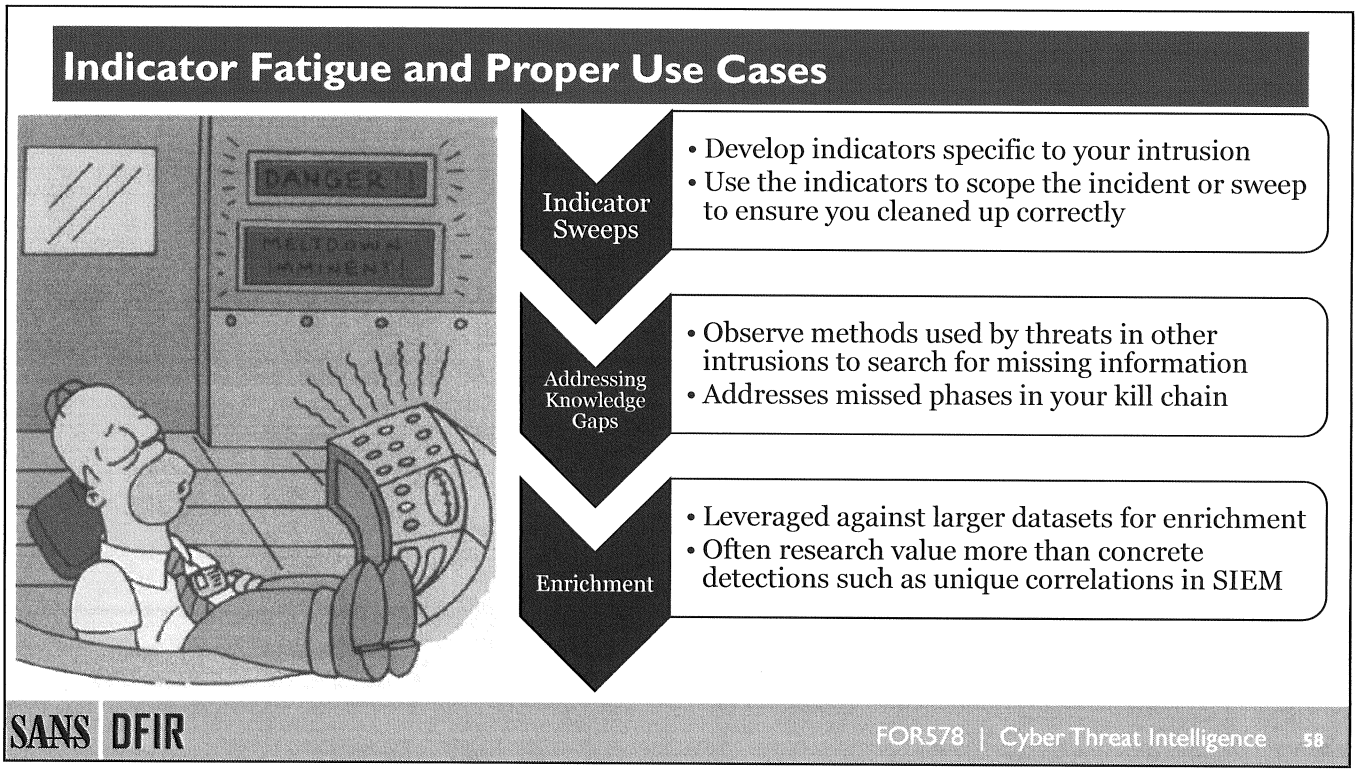
- ihijackedyourdomain@cloppert.org (Delivery, infrastructure)
- Customized version of *gsecdump* (Actions on Objectives, TTP/tool)
- Plug-X variant with mutex *pWn3d* with DNS as the carrier protocol (C2, TTP/tool)
- Domain registered to badguy@ene.my (C2, Infrastructure)
- Carrier PDF with "author" metadata field set to *Benson Hedges* (Weaponization, TTP/tool)
- Google.co.hk referrer string with "inurl:.jsp" in web request with Polish language setting (Reconnaissance, TTP/tool)



All intelligence has a useful lifespan, and that lifespan may be almost literally any length of time. Battlefield intelligence is useful for the duration of the battle. Intelligence on the capabilities of the B-2 Stealth Bomber would have a useful lifespan of 28 years and counting.

Many analysts have tried to classify CTI as "better" or "worse" depending on the type of the intelligence alone, such as domains being more valuable than IP addresses, and so on. This will always fail. As with everything else, the adversary alone dictates this variable. For some actors with great abilities to acquire and move infrastructure, the lifespan of an IP address is so short as to be completely useless for the purposes of analysis or network defense. Other actors, either on account of ignorance, laziness, lack of awareness, or any number of other factors, will change IP infrastructure more slowly. In one case, a C2 IP address had a useful lifespan as a high-fidelity identification of an APT actor for over two years. The only general statement supported by observation about indicator (and therefore detection) lifespan is that those "closer" to the adversary will tend to be less volatile than those further away.

Some organizations get very concerned with "de-tasking" indicators or detections. When they ask if they "age out" a detection or indicator, the most precise answer, as you can surmise, is complex and rife with uncertainty. Even if you can develop inferential statistics on a per-adversary, per-Kill-Chain and per-Diamond-vertex basis, in reality, there is great risk that you will detask a useful indicator or detection. As is often the case, the best advice is the simplest: Keep all of your detections and all of your indicators until their presence causes a problem. When computational bandwidth becomes a problem, redesign, replace, or re-engineer how your detections and the frameworks they ride on operate.



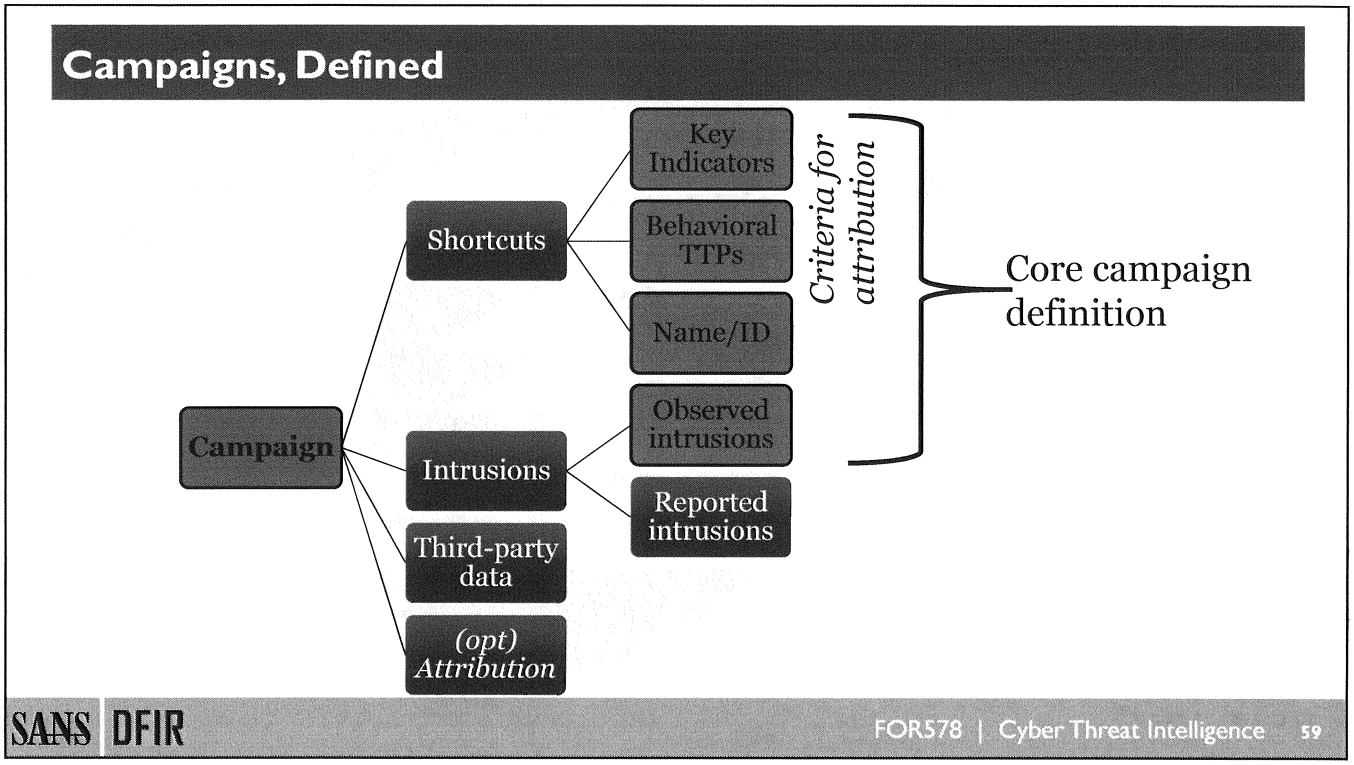
Indicator Fatigue and Proper Use Cases

Indicator and alert fatigue is a real issue for security personnel. If we have 10k critical alerts to go through a day it is unlikely that we will treat each of them as critical. Over the years indicators have been largely abused and positioned as a good detection type for new threats. But really, they are atomic elements of past intrusions. They might be useful to run as indicator sweeps or to fill in our knowledge of adversary intrusions based on what others have seen, but they are not the most effective detection tools.

The value of indicators is when we create them ourselves to scope incidents inside our environment. Most indicators are unique to the victims the intrusion was observed in; it is not as common for indicators to be able to be used across many organizations in an effective manner although some key indicators do exist.

Other value can exist with enrichments on larger datasets in tools such as System Information and Event Management (SIEM) tools but this is often of little value and is used when other starting places aren't available to analysts. This has been abused as a starting place for analysts and leads to high false positive and alert/indicator fatigue – be very cautious with this use case. The most significant value of indicators is in knowledge gap filling.

Image source: The Simpsons

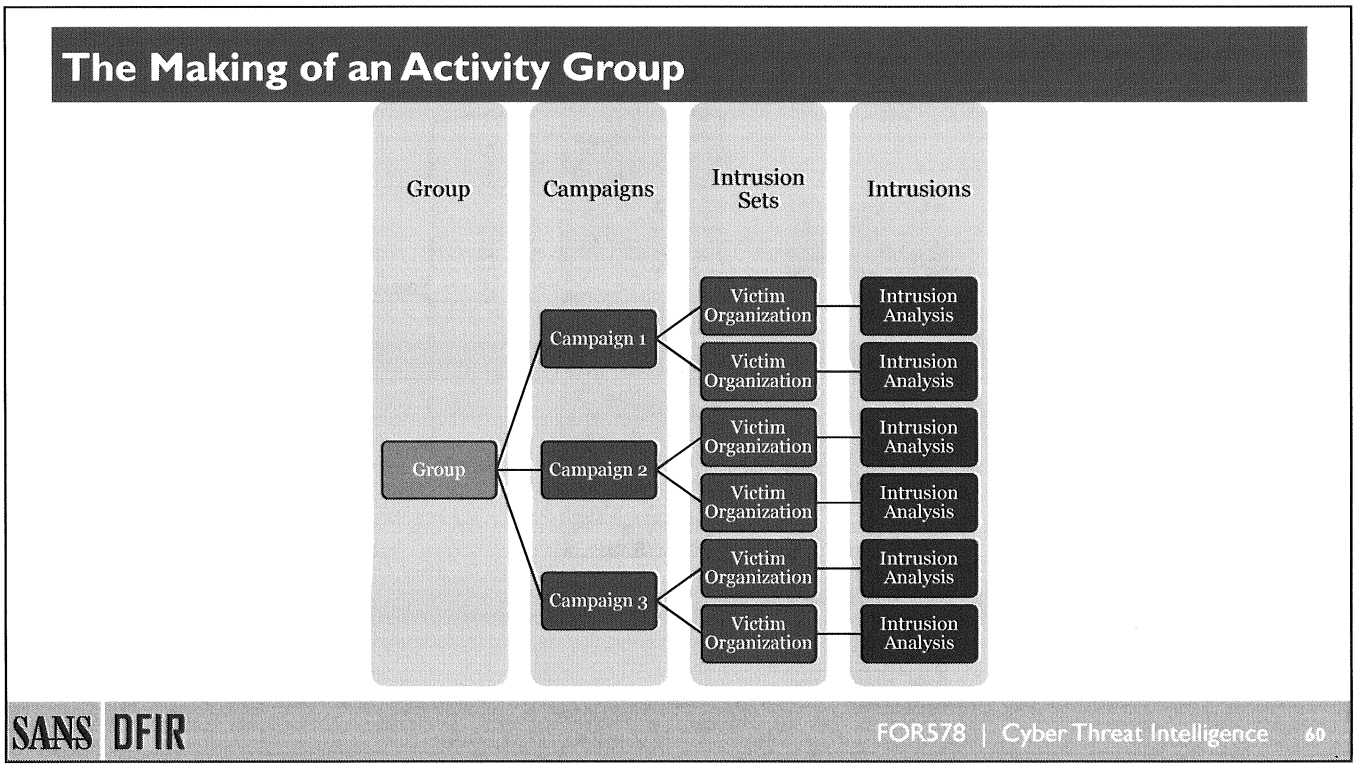


Campaigns are essentially behavioral profiles formulated from trends in intrusion activity. A campaign consists of:

- "Shortcuts" to the campaign to facilitate detection and communication:
- Key indicators:
  - Behavioral TTPs or profile
  - Name/identifier
  - Intrusions that have been attributed to the campaign by:
    - Ourselves—directly observed intrusions
    - Others—not directly observed intrusions
      - Related third-party, non-intrusion research and pivoting
    - Sometimes individual—group, or nation-state attribution

The principle criteria for attributing an intrusion to a campaign are the key indicators and behavioral TTPs. For this reason, their selection is the most critical element of a campaign.

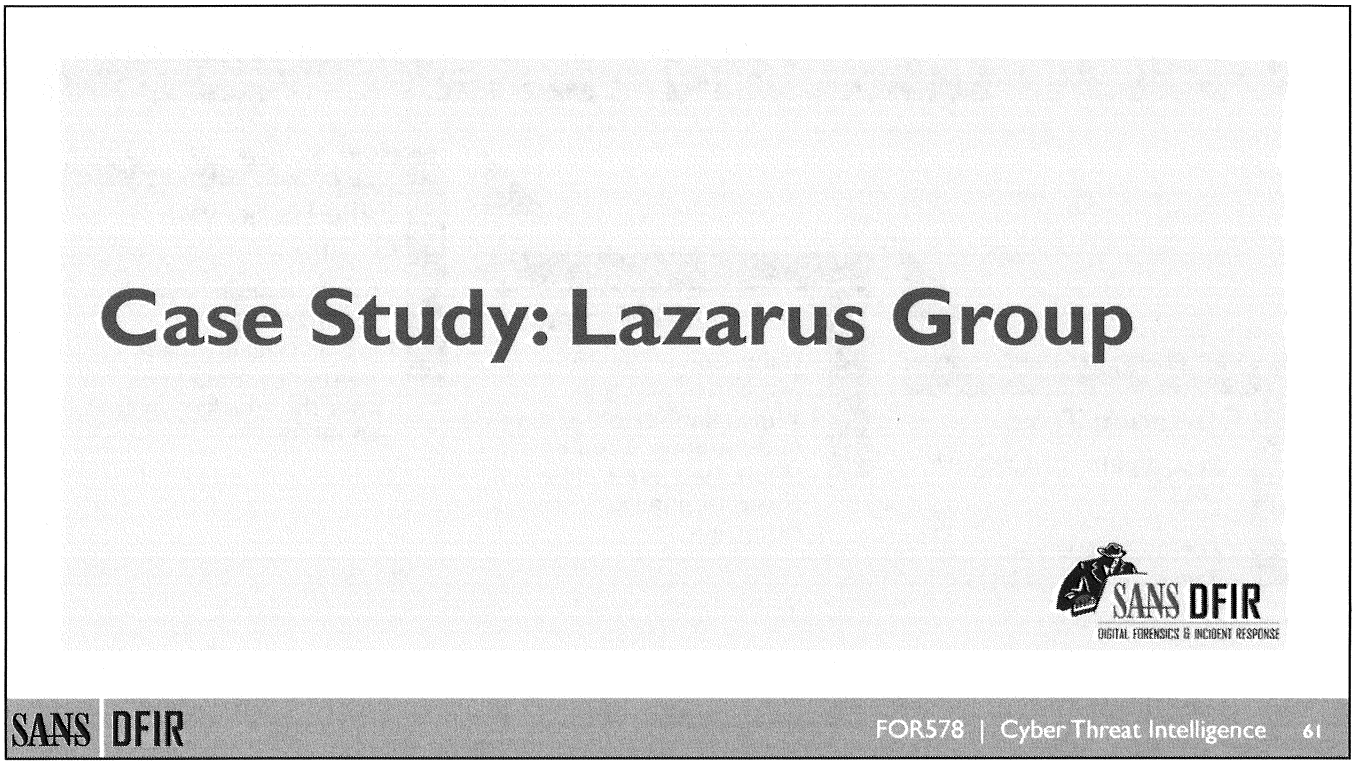
We go into each of these in more depth in the following slides.



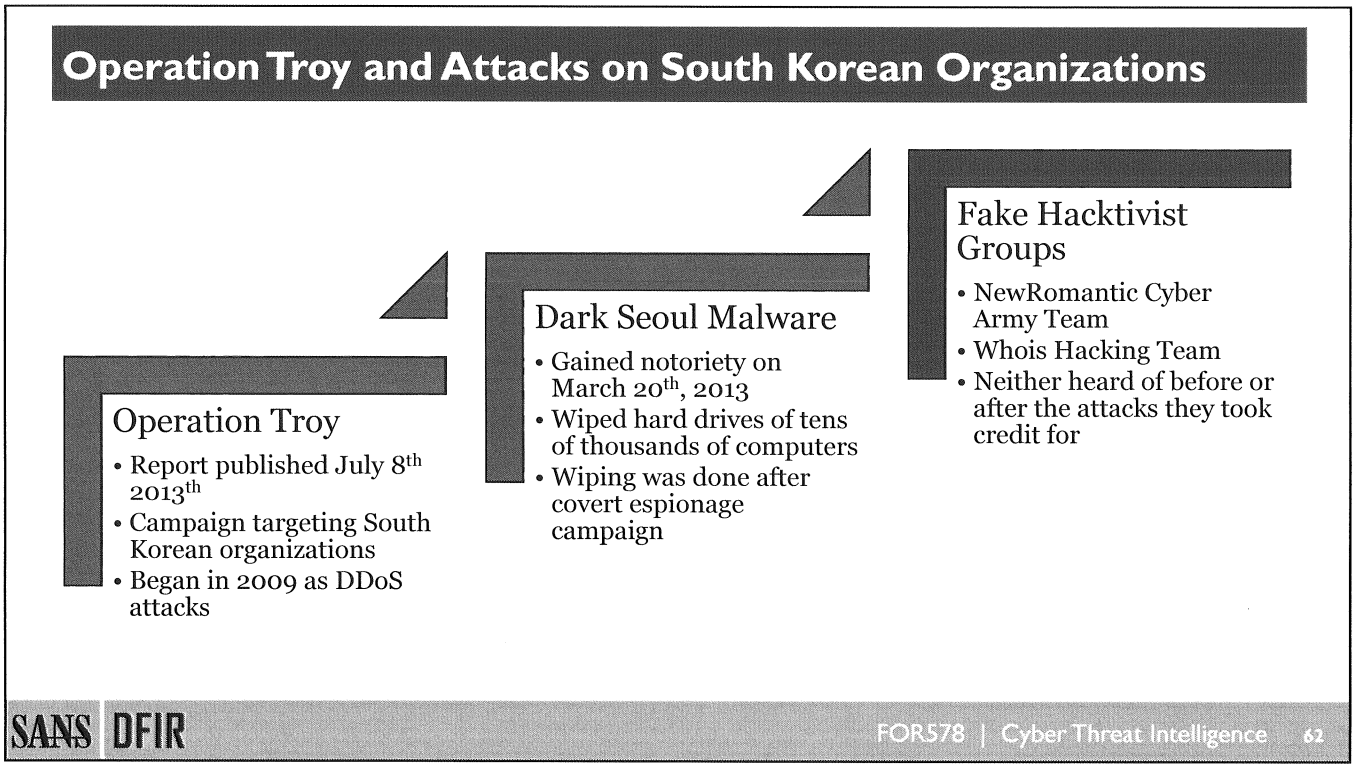
The Making of an Activity Group

Just as we saw during Operation Aurora, there is a difference between intrusions, campaigns, and groups. In fact, there is another classification called an intrusion set that often was leveraged as a term in the U.S. government circles. Ultimately, everything comes down to intrusion analysis. Victim organizations are able to identify singular intrusions into their organizations. Over time those singular intrusions in the organizations are easily identified as a set of intrusions (intrusion set) of a focused effort by an adversary to compromise the organization. At some point though most organizations (unless they are considerable in size such as the Fortune 500) will need to go outside of their networks and understand other intrusion sets in other victim organizations. Through the analysis of these numerous intrusion sets, we can learn that there is a focused effort not just against one company but against numerous. This effort may fit a certain profile or objective of the adversary. Campaigns can be thought of the adversary's mission. As an example, if an adversary wanted to target energy companies that would be one campaign, a different effort by the same adversary to target banks could be seen as a different campaign. The adversary that conducts the campaigns though is identified as a group. The most commonly referred to name for this is an activity group since we are not always sure (and we don't always care) who the adversary is.

An activity group can be thought of as the human team or organization conducting the campaigns. These terms are mixed and matched and abused in the larger security industry but getting our teams and the industry to use a consistent language can help us all understand what analysis has been done and what analysis is left to be done. As an example, to get to an activity group there's a lot of campaigns, intrusion sets, and a whole lot of intrusions that need to be analyzed fully.



This page intentionally left blank.



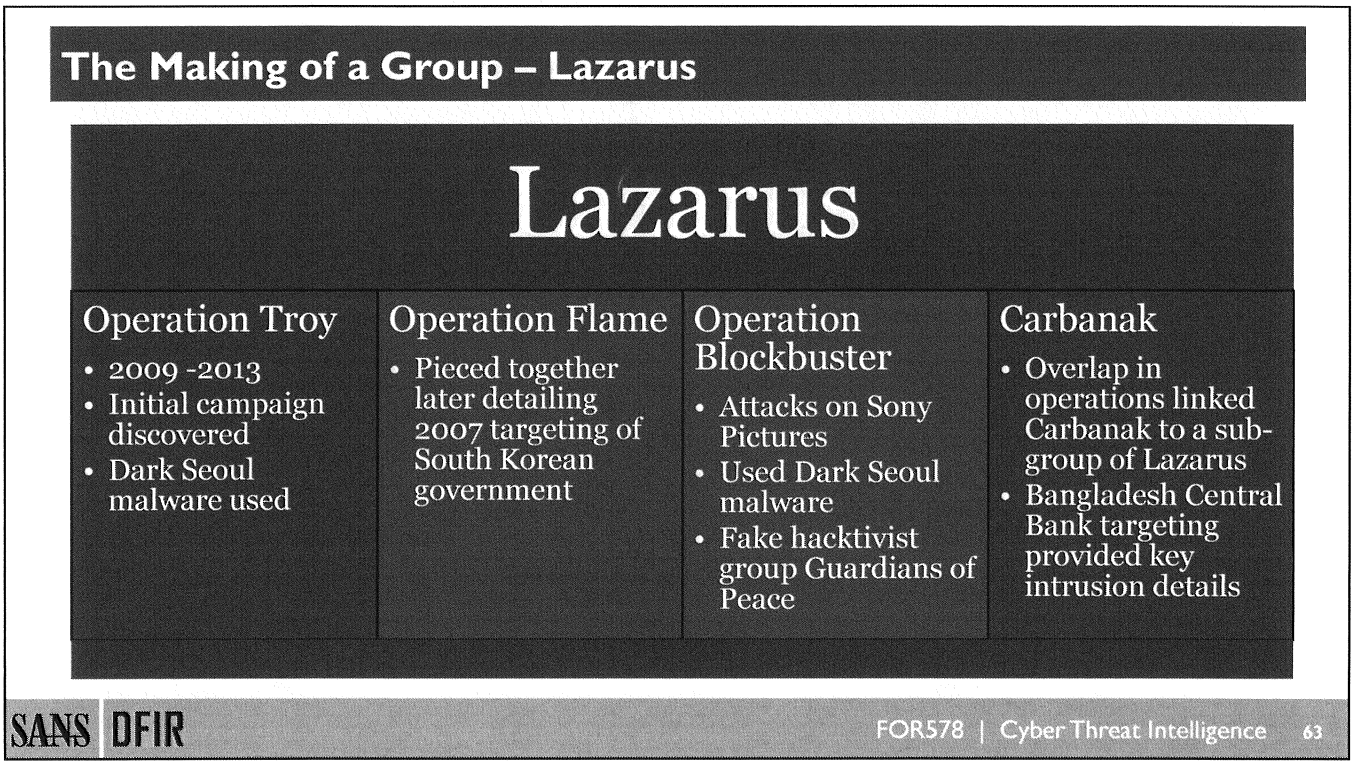
Operation Troy and Attacks on South Korean Organizations

In 2013 McAfee published a whitepaper covering the Dark Seoul malware that was leveraged against South Korean organizations. The paper dubbed the campaign Operation Troy and detailed how the master boot record (MBR) wiping malware was first leveraged as a sophisticated espionage campaign. The Dark Seoul malware contained remote access Trojan (RAT) functionality which allowed the adversaries to espionage after infecting the organization through spear phishing emails. The targets of the attack were largely banks and media organizations as well as government networks. Interestingly, the attackers took credit for the attacks as "NewRomantic Cyber Army Team" and on other occasions "Whois Hacking Team." Neither of those hacktivists groups were ever heard of before each attack nor were they active following the attacks. Each seemed to be made up hacktivist groups designed to take credit for the attacks.

Although 2013 was the first major public attention paid to the malware the analysis of Operation Troy detailed that there were numerous attacks going back to DDoS efforts in 2009 against other South Korean targets.

Reference:

https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/dissecting-operation-troy.pdf



The Making of a Group – Lazarus

As the individual intrusions were analyzed across numerous targets and years' worth of data, there were distinctive patterns that formed. There was a commonality in the malware, in the style of the intrusions, and even in the naming convention of fake hacktivist groups each time an attack was orchestrated. But Operation Troy was simply one look at what would become known as the Lazarus Group. Over the course of a few years, there were various campaigns orchestrated by what appeared to be a single group. This group consistently targeted South Korean media and financial companies and eventually began targeting other organizations such as the Bangladesh Central Bank and Vietnamese Tien Phong bank.

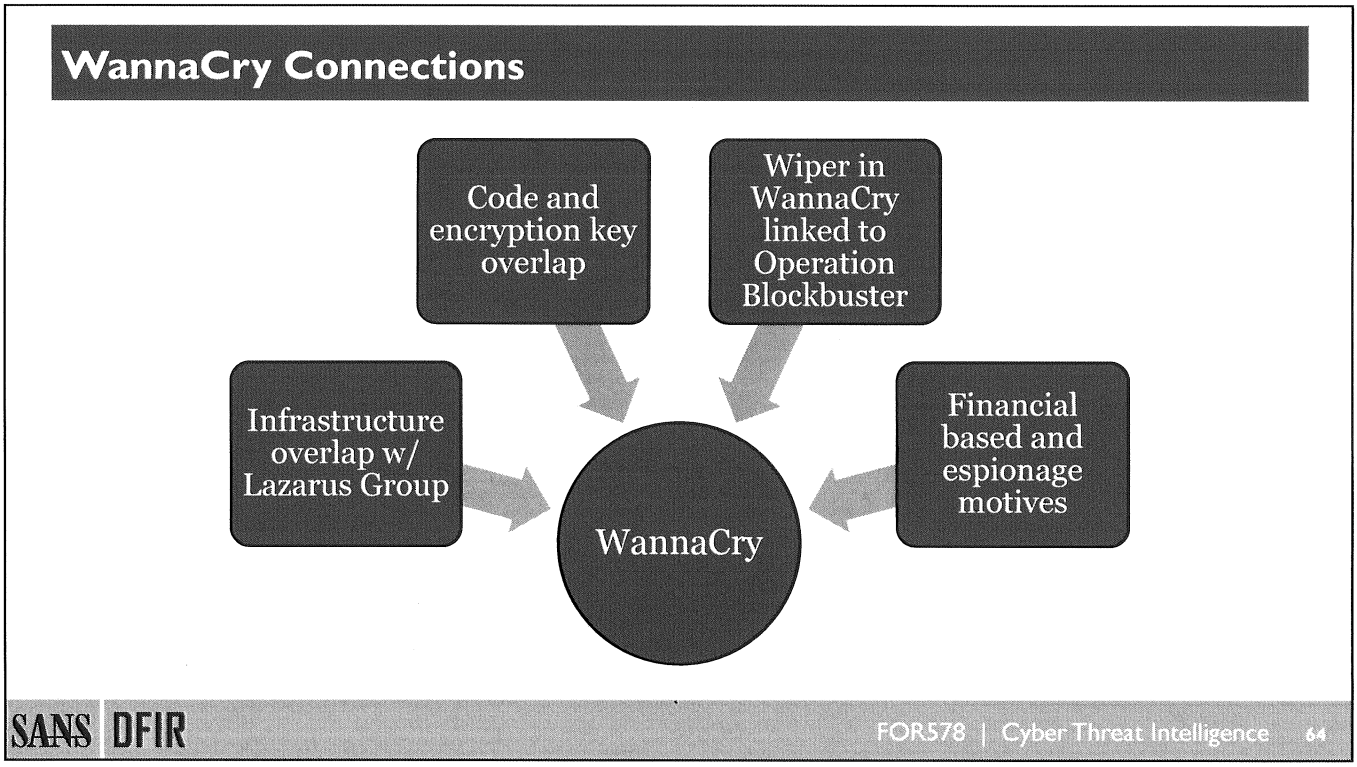
Interestingly enough, the analysis helped tie together an even earlier campaign than Operation Troy called Operation Flame. This was the first generation of the Dark Seoul malware leveraged against the South Korean government for a long-term espionage program.

Reference:

https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/

https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf



WannaCry Connections

Following the WannaCry infections of 2017 multiple security companies including BAE and Kaspersky Labs performed code analysis between the Lazarus Group samples and the WannaCry malware. There was particular overlap including specific encryption key usage between the malware samples unique to the adversary group. More important than just code overlap was also command and control (C2) overlap between the infrastructure the adversaries were using to distribute WannaCry and infrastructure sites the Lazarus group has used before.

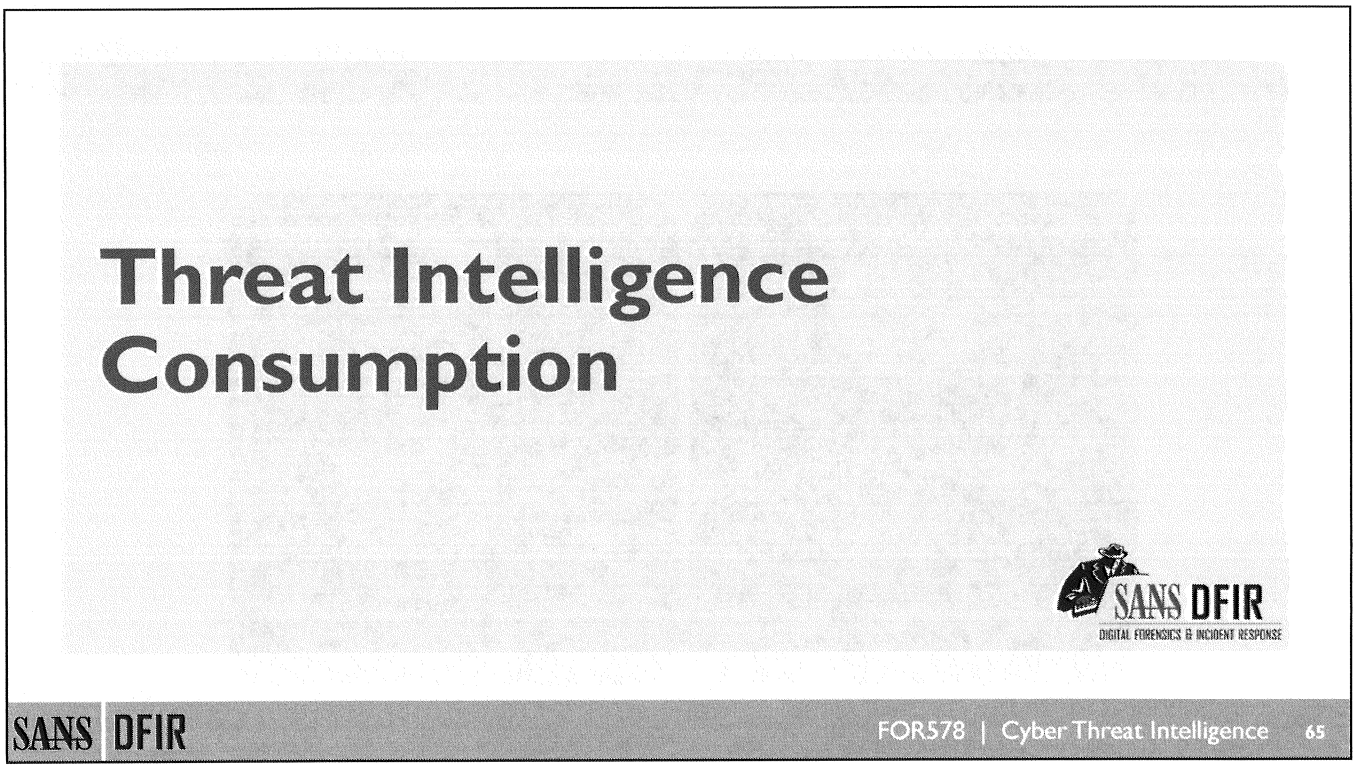
There were many theories around WannaCry and why it worked like it did—including how poorly the ransom component was orchestrated—but as analysts, we have to be careful not to let ourselves be overly-biased. The ransomware functionality of the malware could have been a disguise like the wiper component of DarkSeoul after the espionage program. It could have been a mistake as well though letting it loose on the Internet. Additionally, maybe it was simply handled very poorly and one team worked on the malware while another team inside the Lazarus group worked, less successfully, on the ransom portion.

As organizations try to piece together the ties to the group though it is important to think about whether or not the Lazarus group represents a threat to your organization, what you would do as cyber threat intelligence analysts, and to use structured analytical techniques to help in your analysis.

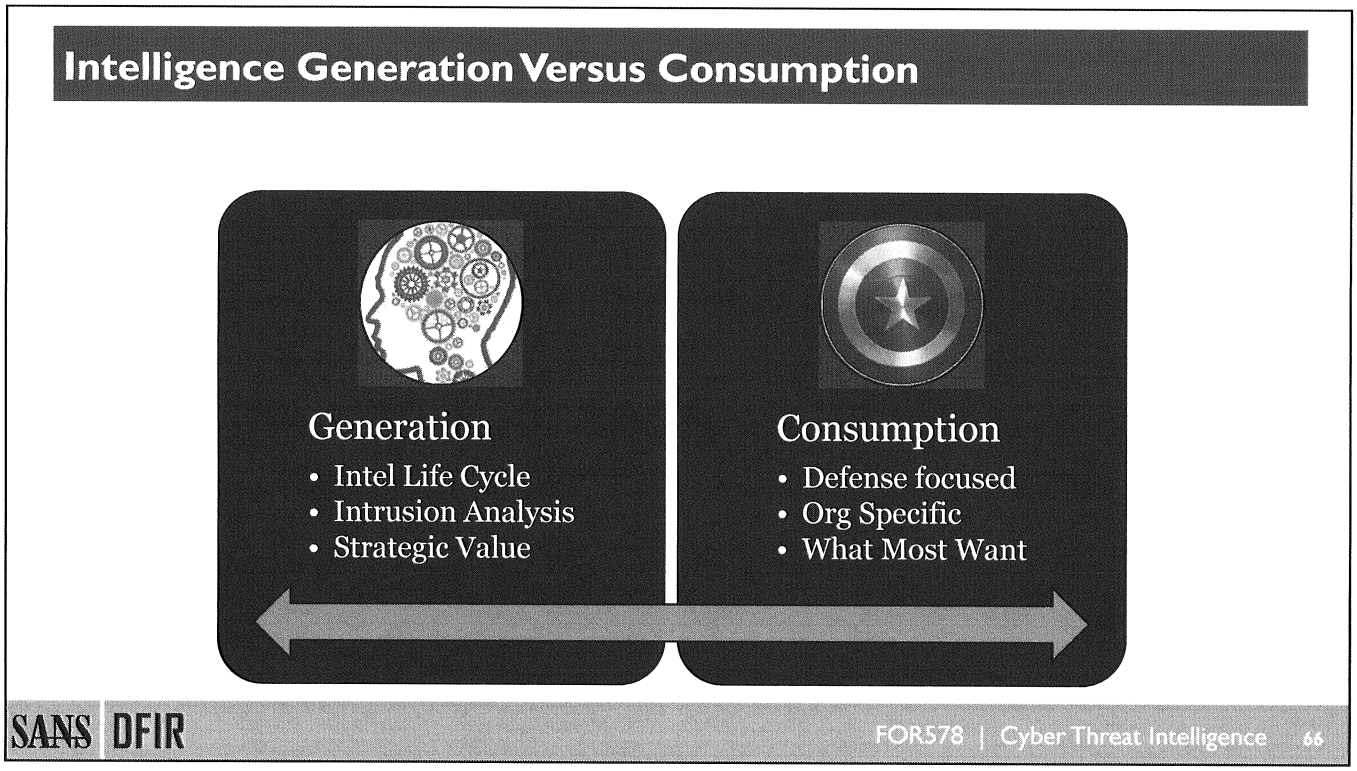
Reference:

https://securelist.com/wannacry-and-lazarus-group-the-missing-link/78431/

https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group



This page intentionally left blank.

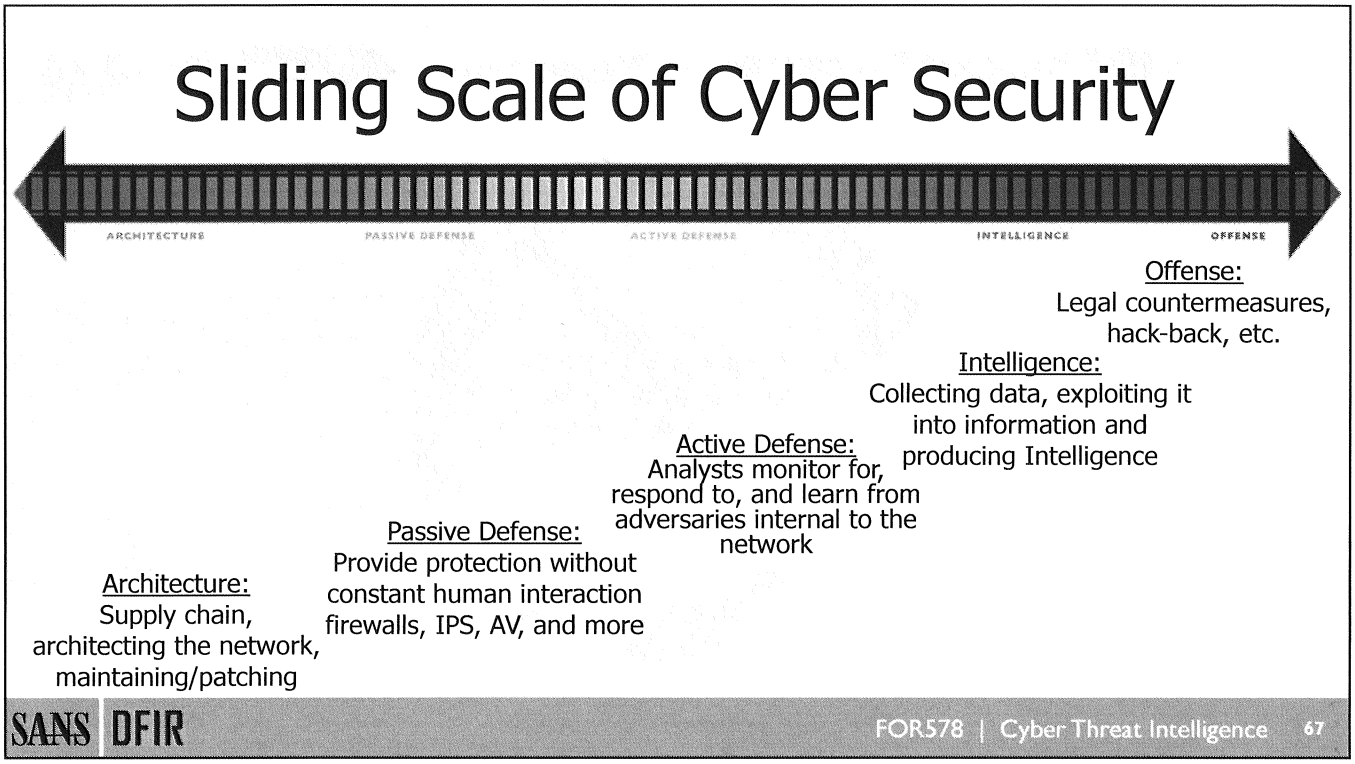


Intelligence Generation Versus Consumption

When trying to understand the audience, it is important to remember if it is generating intelligence or consuming it. Right now, there is little separation in the Threat Intelligence Community with regard to the difference between generating and using threat intel. This has led to the buzz terms "actionable intelligence" and confusion on the role of threat intelligence analysts. As the community matures this meaningful separation will become more important. Organizations and teams can either focus intelligence for the purposes of actuating it or they can produce threat intelligence. A single team may bounce back and forth between these two concepts but should not be doing both at the same time. Analysts should focus on producing intelligence or structuring it in formats so that security personnel can quickly use it.

Generally speaking, intelligence generation focuses on creating intelligence through the models and processes we've discussed already. The Intelligence life cycle, the Cyber Kill Chain, and the diamond model are the important concepts and pieces required to create intelligence, analyze intrusions, and understand the larger campaigns of the adversary. Intelligence consumption is how defenders use that information. Intelligence consumption is important because it still requires analysts who understand intelligence and who understand the organization's environment. (Know thyself and know the adversary.) Intelligence and the indicators it begets can be placed into passive defenses (those that do not require direct and constant human interaction) such as firewalls, antimalware solutions, IDS/IPS, and so on, and it can be used by active defense mechanisms such as network security monitoring analysts, malware analysts, incident responders, and teams such as security operations centers. We discuss threat intelligence consumption more in-depth later today.

Note: The arrow at the bottom of the graphic is important to keep in mind. Those that consume intelligence, such as incident responders, are some of the best to provide the data required for generating threat intelligence. It is a back-and-forth process that requires the best out of every analyst to truly understand, learn from, and respond to advanced adversaries.

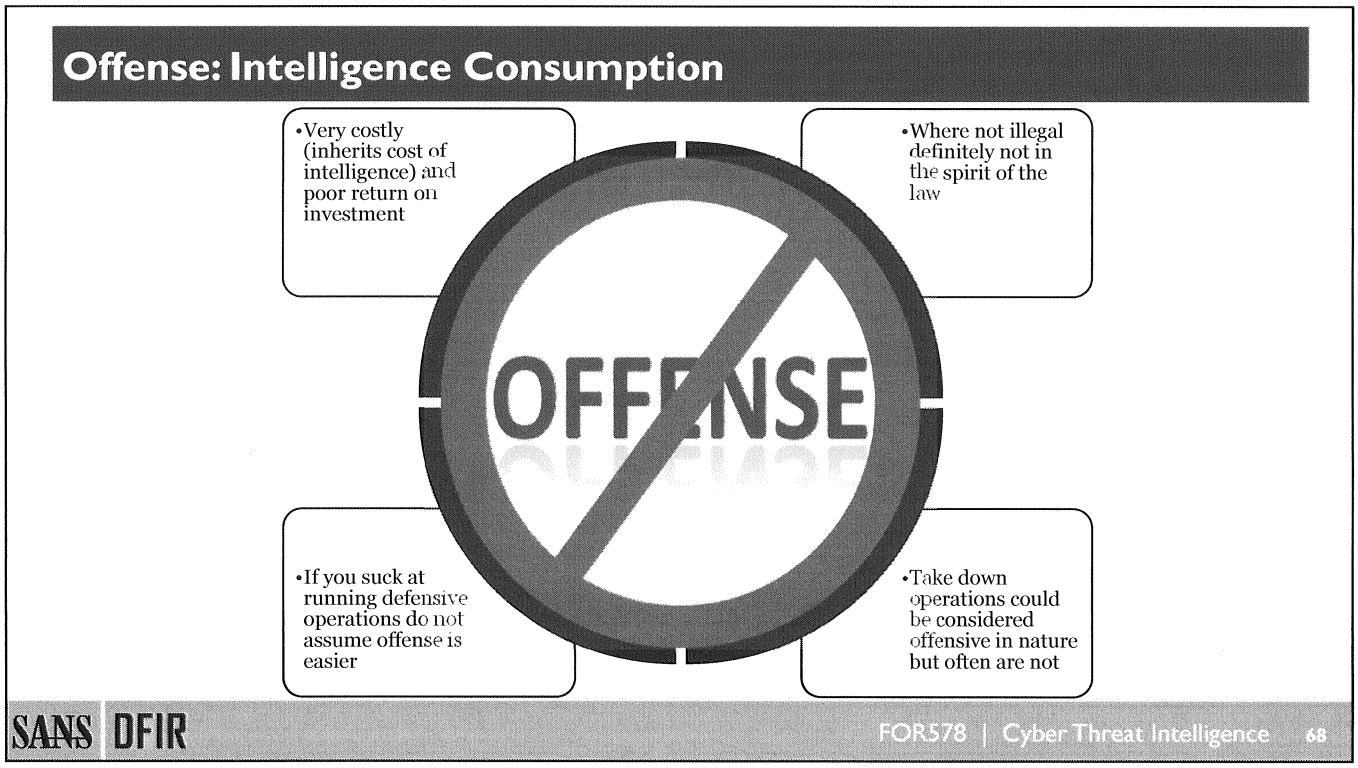


Sliding Scale of Cyber Security

The Sliding Scale of Cyber Security is a theoretical framework developed by Robert M. Lee in the pursuit of his Ph.D. at Kings College London and built upon his experiences in the U.S. Intelligence Community and Air Force. It is entirely meant to simply be a way to frame the discussion regarding actions that contribute to cyber security without getting overly technical. It is a nuanced discussion beyond doing "defense" and is more of a learning tool than a model that should be used. It is important to note here as we move to explore actuating threat intelligence that the production of threat intelligence falls into the Intelligence category. It is an intelligence act and process to create threat intelligence; this can be done internal or external to your environment (that is, incident response data internal to the environment through the Kill Chain and Diamond Model versus collecting information from adversary networks). Actuating threat intelligence, or otherwise using an intelligence-driven defense, is the process of consuming threat intelligence. Although intelligence can be used in a number of areas, the focus on the analyst is a heavy focus of this course and of what is required; therefore, consuming threat intelligence will be placed into the context of an active defense. To discuss active defense, it needs to be effectively defined.

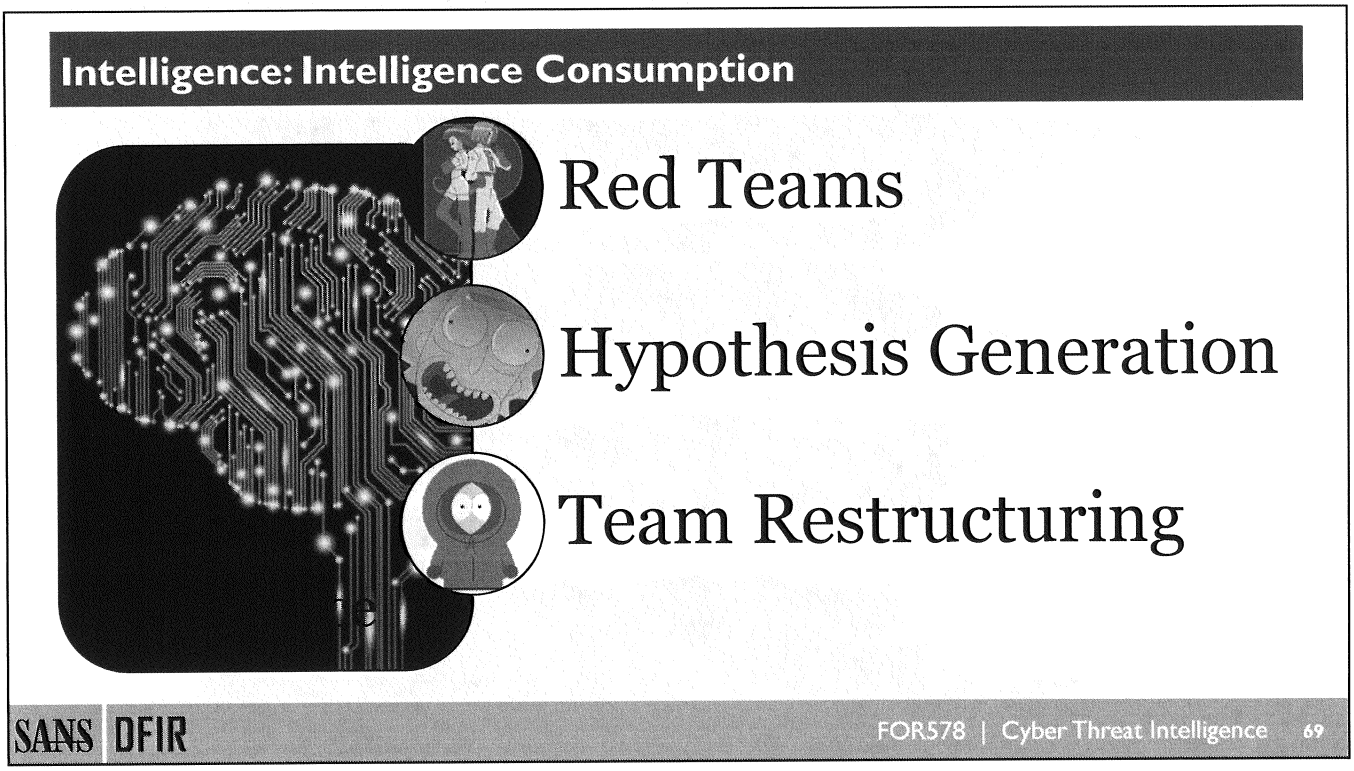
The paper covering this topic may be found in the SANS Reading Room here:

https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240



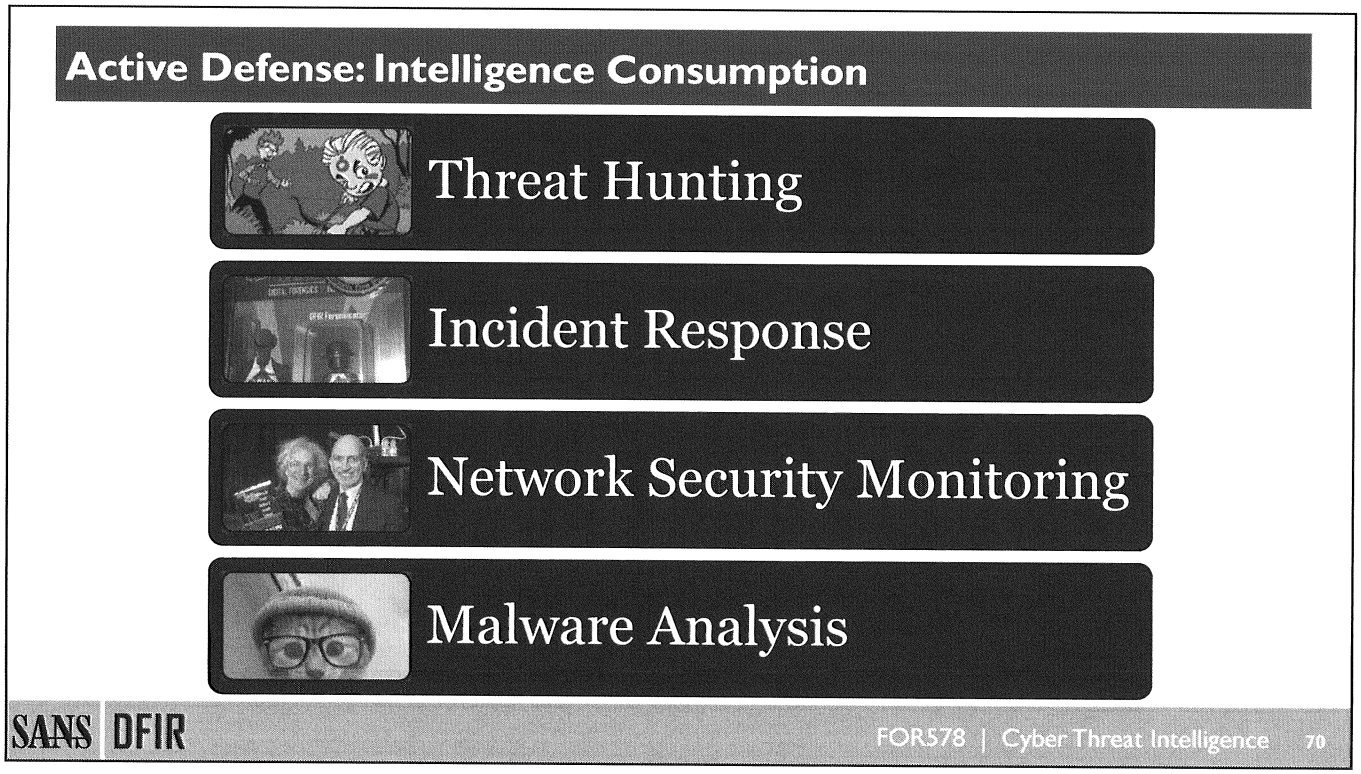
Offense: Intelligence Consumption

We will first look at offense from an intelligence consumption perspective. Intelligence drives the ability to do offense. Especially for anything related to security (and not just espionage or military attack), there is a critical need for good intelligence to ensure the offensive operations being undertaken are against the right target and will have the right effect. As an example, teams have to worry not only about operational planning and coordination but also damage assessments and mission effectiveness calculations. Additionally, coordination with others must be done to ensure multiple teams are not converging on a target and impacting each other. Offense is a lot harder than people make it out to be; it's not simply about profiling an adversary, logging in with their password, or gathering a command and control address to sink hole. However, many take down operations actually relate to the patching of vulnerabilities at the same time someone is updating passive defenses to start blocking malware and eliminating adversary access to command and control. Very rarely are offensive actions ever taken and they are always poor return on investment for organizations.



Intelligence: Intelligence Consumption

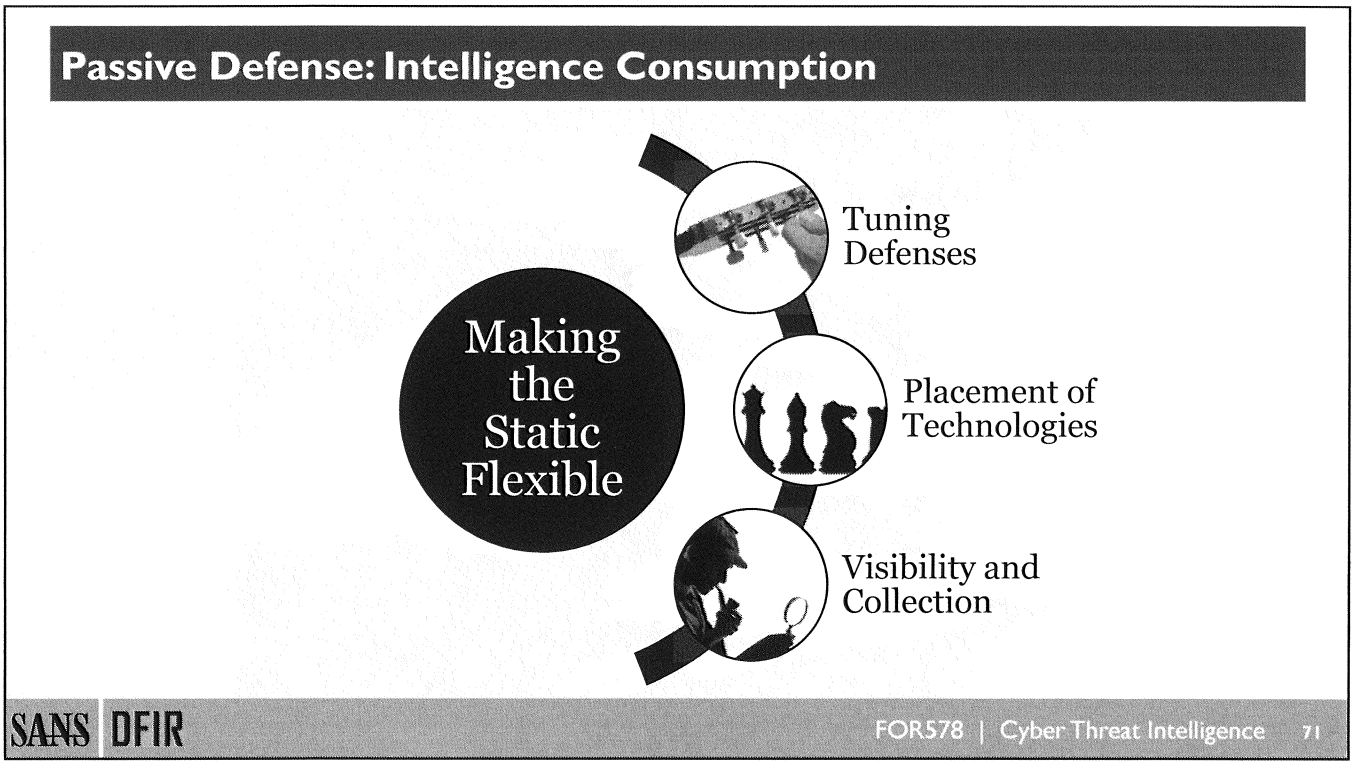
It may seem odd but you can absolutely consume intelligence for the purpose of influencing the intelligence category of the sliding scale. As an example, red teams emulate the adversary (whereas pentesting would be an architecture phase category because it is meant to validate architecture and vulnerabilities). Consuming intelligence can ensure that red teams are emulating the tradecraft and techniques employed by adversaries your organization should be concerned with instead of just what the latest and coolest tricks and tools are. Additionally, hypothesis generation is vital to hunting, later generating intelligence, and thinking about how to defense overall. Hypothesis generation is a skillset in and of itself but falls into the intelligence category. Understanding how adversaries operate and what it took to catch them can lead to generating hypotheses that are useful for the other phases of the sliding scale. Lastly, you may find that your policies or even team structure itself are not well suited to take on the adversary. Understanding how the adversaries are postured with relation to your organization can help you consume intelligence to ensure that your team is restructured, re-sized, or trained to face the threat that it needs to face.



Active Defense: Intelligence Consumption

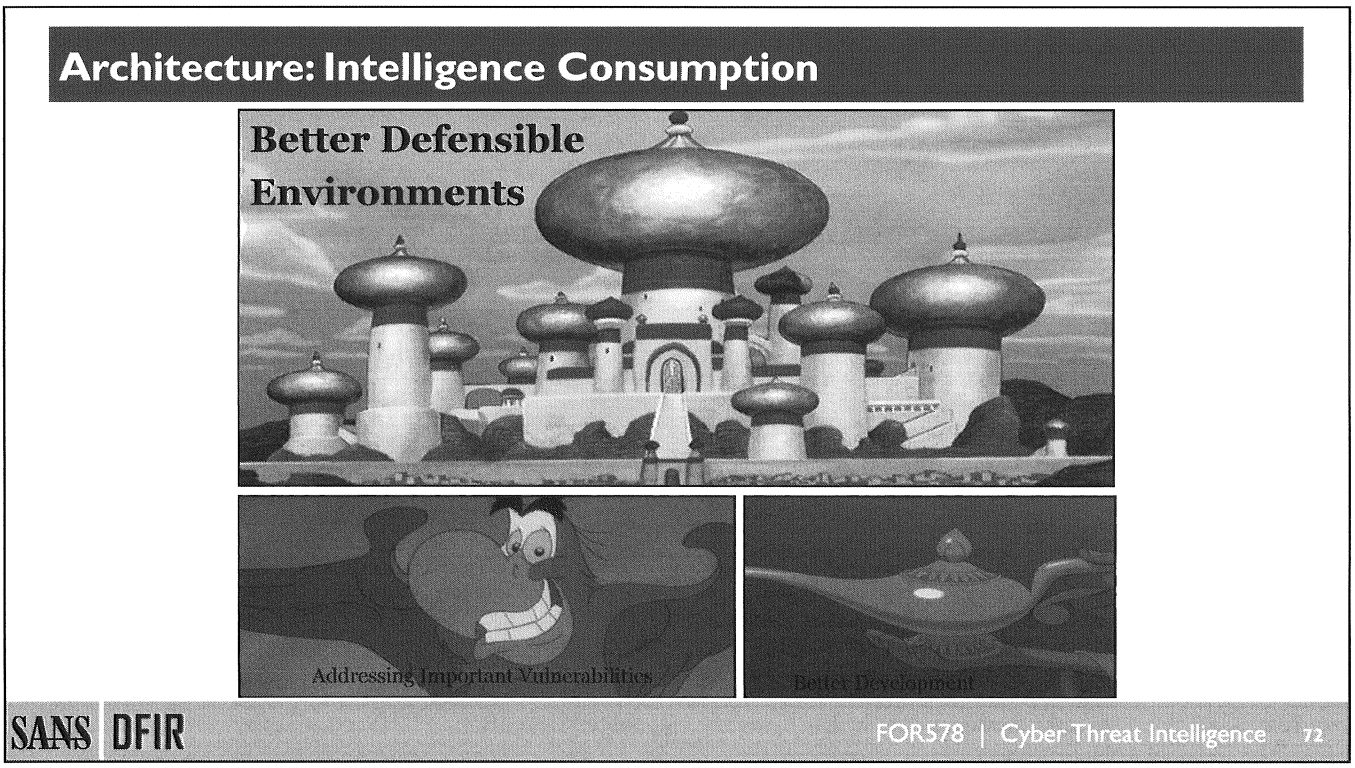
Active defense is the focus for most of us. It is the essential human component of defense in pursuit and countering of the adversary. Models exist such as the Active Cyber Defense Cycle (ACDC) (covered in SANS ICS 515) for how to do an active defense in different environments but the key thing to note with regards to intelligence is that intelligence should drive how we all do defense. Threat hunting is the human focus on hunting out and countering threats in one's environment. It is linked in many ways to how we do incident response (not just more IOCs but in understanding adversary tradecraft in general), how we perform tactics such as network security monitoring, and ultimately how we analyze the adversary's capabilities so that we can better learn and posture against them.

There are many ways to consume intelligence at the active defense phase; these are just some of the more common. Most of the SANS classes folks talk in the Forensics and many in the Security track deal with active defense and how to empower the human defender against the human adversary.



Passive Defense: Intelligence Consumption

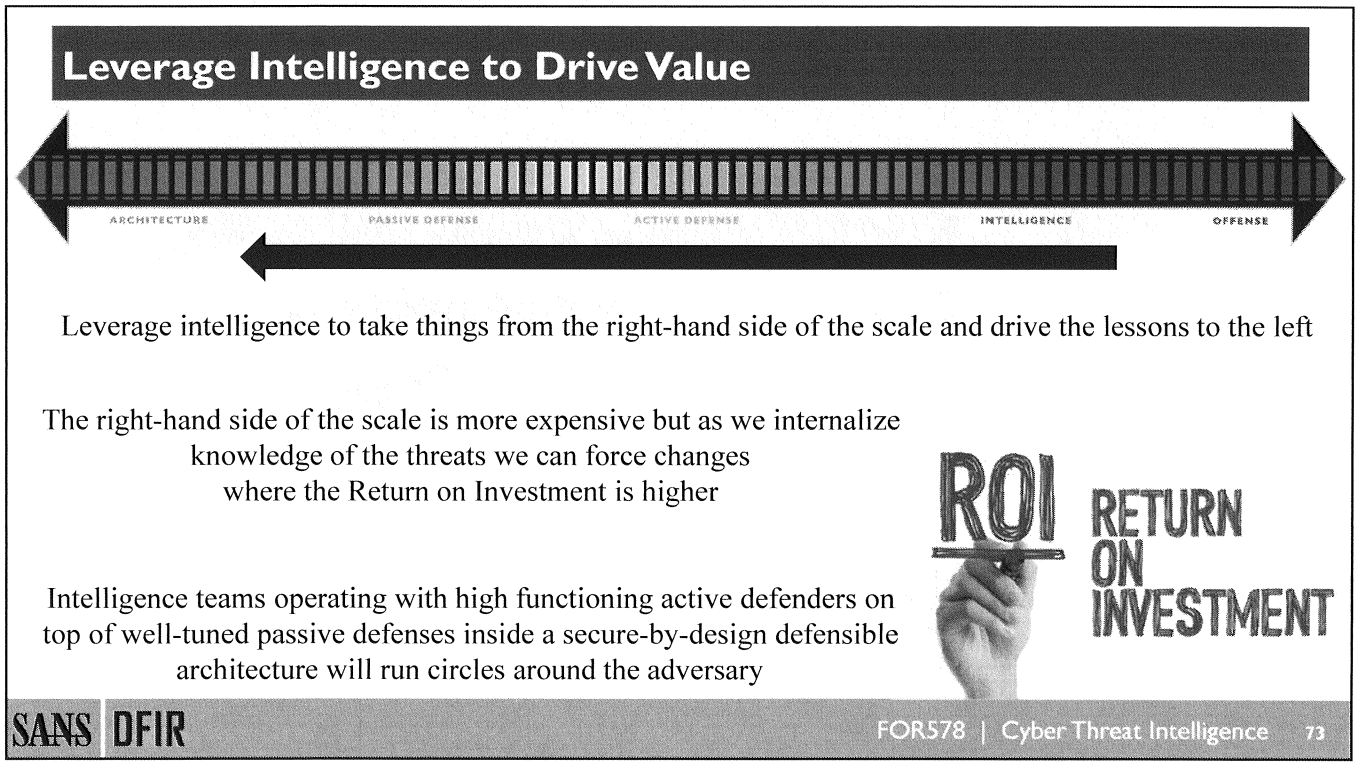
Much of what is done in defense is done through passive defenses such as antivirus, intrusion detection systems, system information and event managers (SIEMs), endpoint security technologies, and more. These once static tools (Firewalls never being updated are a good example) have become more flexible over the years especially with the addition of threat intelligence and insights from that intelligence. We now have tools that are more adaptive, collect better data for us to make defensive decisions on, are better tuned, and placed in environments where we understand there is no perimeter anymore. Threat intelligence has been abused by tools (mindlessly inserting IOCs into a proxy server is not proper usage) but there is a lot of value for how we adapt over time. These focuses can help ensure that our active defense (humans) can focus on more sophisticated threats instead of playing whack-a-mole against every issue on the network.



Architecture: Intelligence Consumption

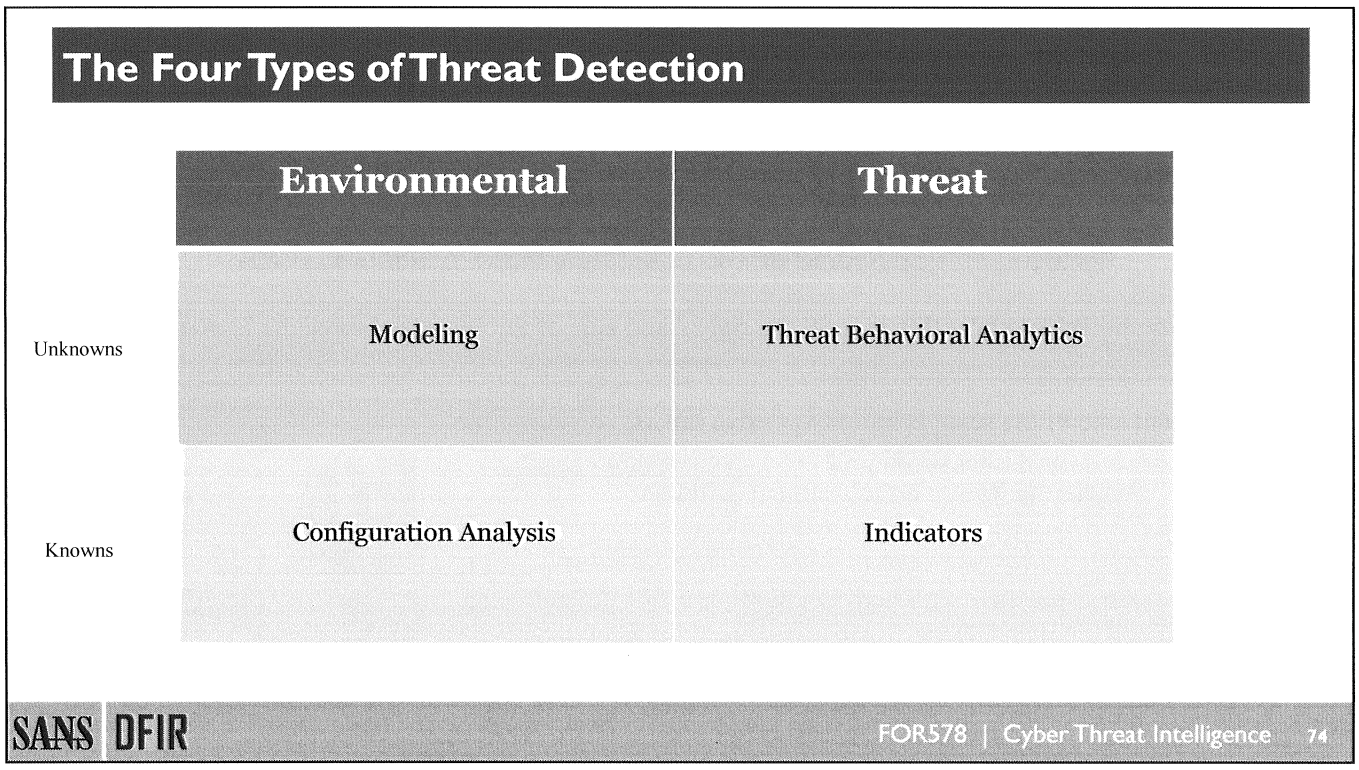
Intelligence for the purpose of the architecture phase should be focused around making our architecture more defensible (humans make it defended but it is in the architecture, design, and sourcing of that architecture that we are able to have a defensible environment). Those defensible environments always have vulnerabilities, though, and addressing them are important; however, there are always more vulnerabilities to find and patching across large organizations is not a simple matter. Yet, when intelligence is able to help us understand that some vulnerabilities are in active use by threats we are concerned with they become more important for us to address. Additionally, the hope is that over time intelligence forces better development of systems, networks, and their architectures.

All images and rights of Disney images are owned solely by Disney…don't sue me, Disney.



Leverage Intelligence to Drive Value

Consuming intelligence is ultimately all about driving change to organizations. Intelligence teams should focus on driving as much change to as far right of the scale as possible. This does not mean to ignore the fires that we are all fighting each day, but instead, to ensure that we make changes in the future that keep giving us advantages against threats. Each engagement with the adversary should drive lessons learned that, over time, help us to make better architectures, tune and place better passive defenses, hone our active defenders better, and leverage intelligence to ensure we stay ahead of threats. Ultimately intelligence practitioners should understand the return on investment various actions give to the organization and try to maximize value.

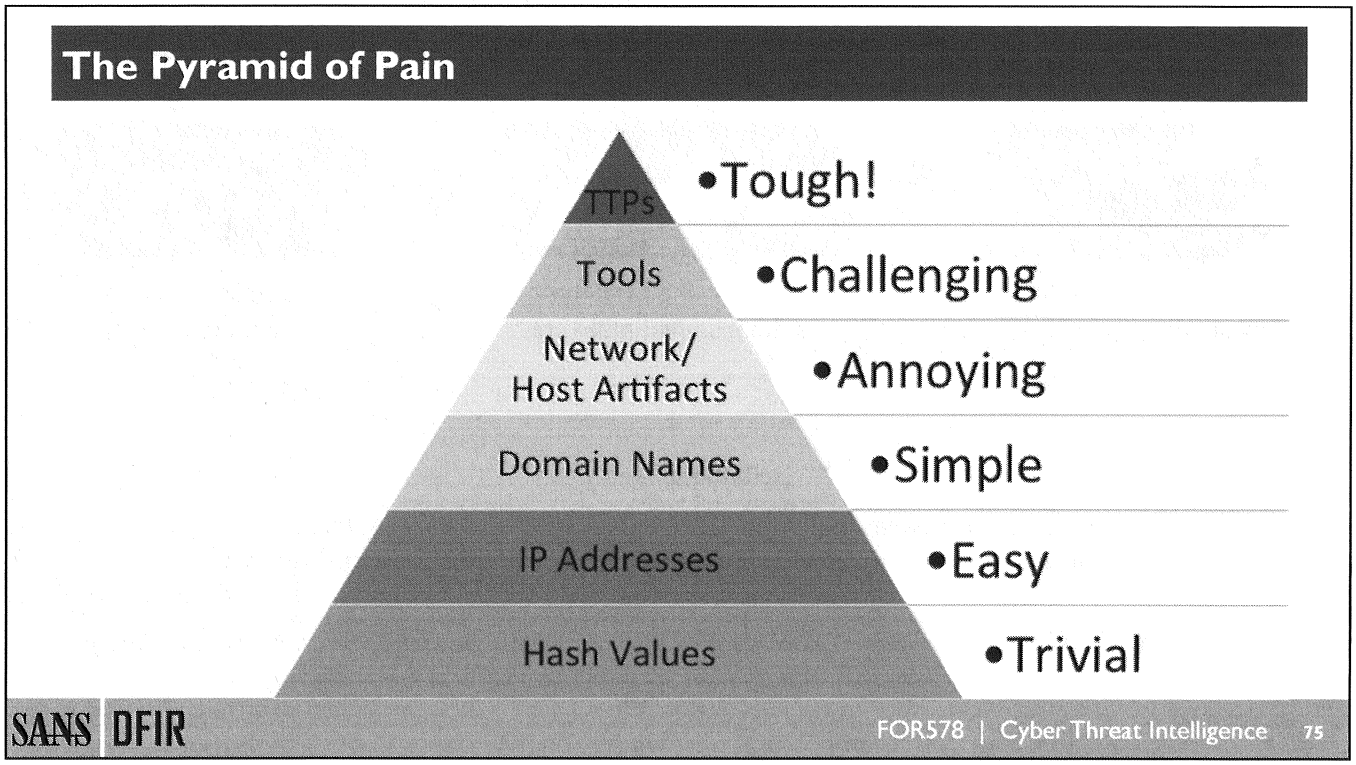


The Four Types of Detection

Threat intelligence analysts need to understand the ways to which threat detection is done. There are truly only four categories of threat detection: configuration analysis, modeling, indicators, and threat behavioral analytics. Configuration analysis and statistical modeling are an environmental based approach which means organizations need to understand themselves or develop models and systems to help understand deviations from normal activity. These environmental based approaches are great at applying knowledge of the environment to catch activity. These anomalies can be threat-based but they are also sometimes simply configuration issues, maintenance issues, or other non-threat-based activity. It can catch threat-based activity as well but the downside is there is no way for an environmental based approach to have context as to what is being analyzed. In other words, it's good at generating alerts and potentially with information for the analyst to investigate but it's not going to give you context.

Threat-based approaches such as indicators and behavioral analytics are not good at catching everything. You must program knowledge into them focused on the adversary. They become highly scalable and effective when done correctly though. However, they instantly can deliver context as to what is being alerted upon. A single behavioral analytic may fire instead of thousands of anomalies and give you the appropriate context and what to do about it.

We will explore the threat-based approach more in depth as this is exactly what threat intelligence analysts should be focused on: leveraging their knowledge of the adversary to help improve true positive detections in their organizations.

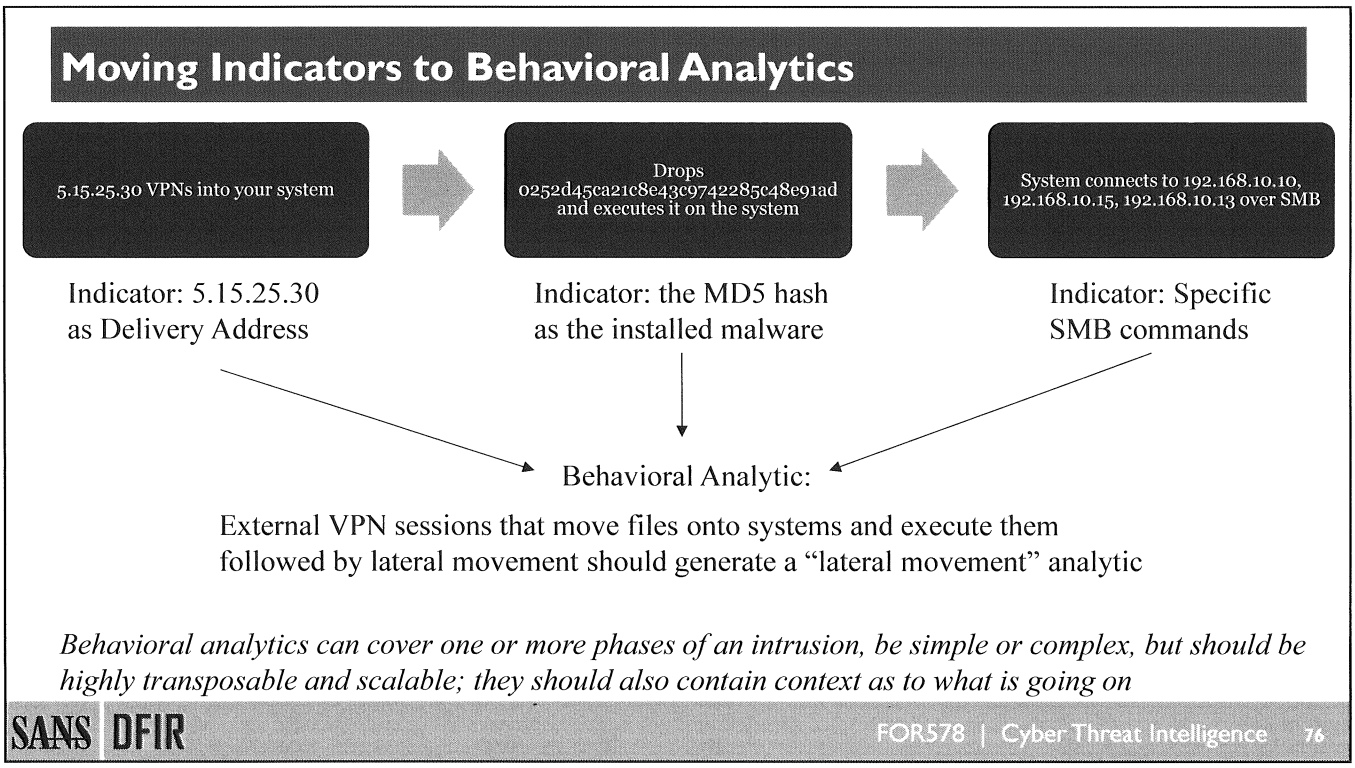


One way to categorize indicators is by using the pyramid of pain, a model that is used to show how much pain it causes the adversary when indicators at different levels are identified and alerted upon. Hashes are easy to alert upon with high confidence; however, they are also easy to change, and therefore, it causes them a trivial amount of pain. Changing IP addresses is more difficult than changing hashes; however, most adversaries have disposable infrastructure and can also change the IP addresses of their hop points and command and control nodes once they are compromised.

Indicators such as network and host artifacts and tools are more difficult for adversaries to change once they are detected, which is why they are higher up on the pyramid. At the top of the pyramid are tactics, techniques, and procedures, which if identified, require that an attacker change nearly every aspect of how they operate. It is more difficult to alert on network and host artifacts and TTPs as well; however, when it is possible to alert on these indicators, it will have a lasting impact on the attackers.

Reference and Image:

http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html



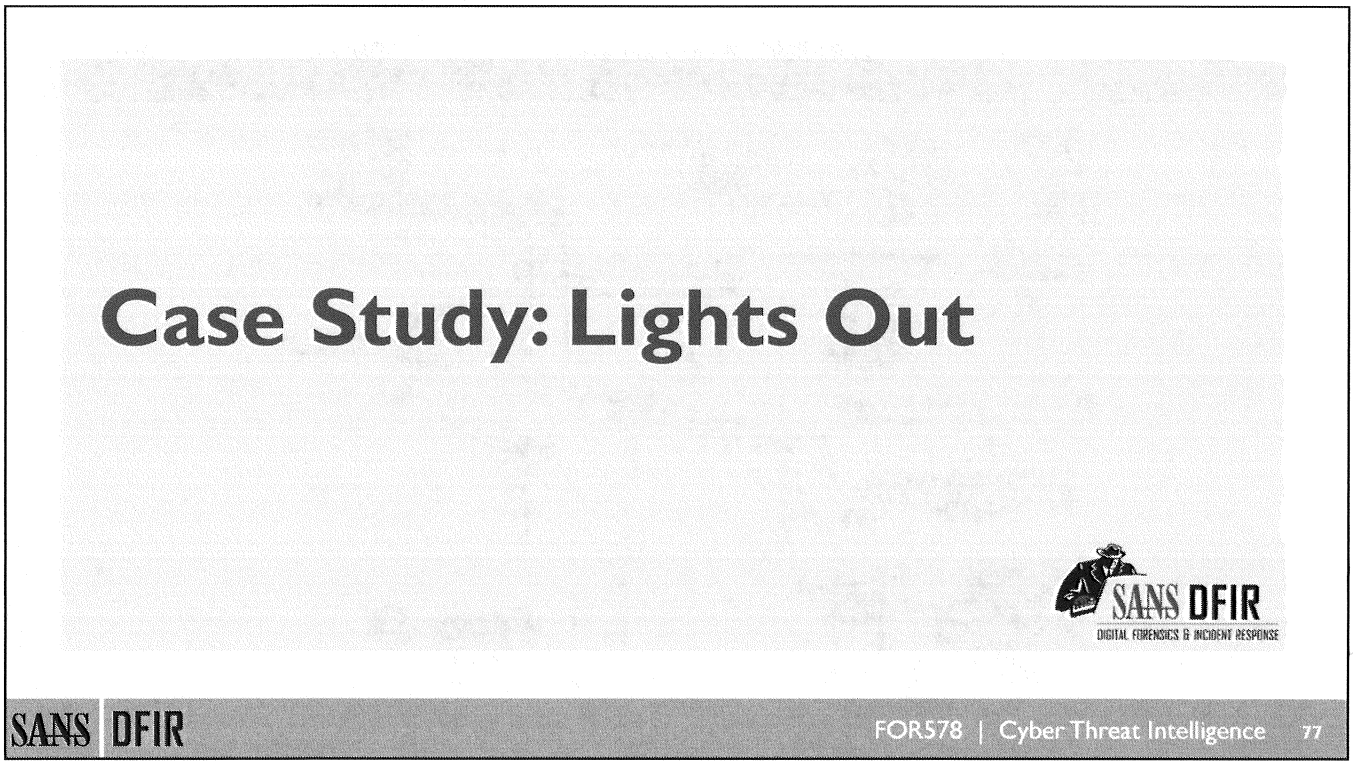
Moving Indicators to Behavioral Analytics

Signature has become a dirty word in the security industry. Really when most people are referring to signatures they mean indicators. Complex and chained signatures addressing behaviors observed across other atomic elements such as indicators though can be very valuable.

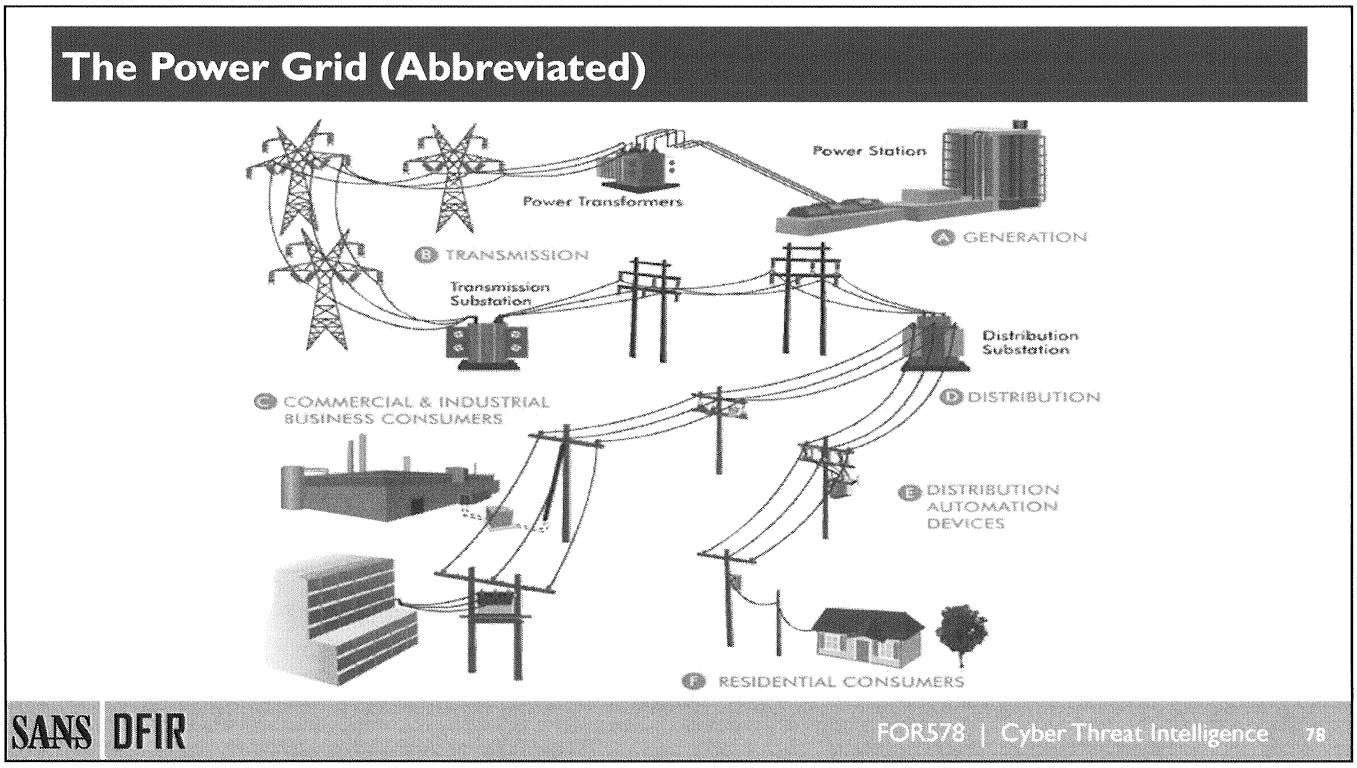
As an example, you may not care what the IP address of the adversary is (indicator) that comes across the VPN nor would you care what the MD5 hash of the malware is (indicator) or what other systems it then connects to internal to your environment (indicator) but you care that any time any IP address connects to your systems via VPNs, moves over a file, and performs lateral movement you want to know that potentially malicious behavior occurred (behavioral analytic).

Indicators and past events should be leveraged to think about the behaviors exhibited and security should leverage behavioral analytics to identify whole swaths of new malicious activity even the unknown intrusions or to determine high true positive behaviors that we then adapt our defenses or systems to mitigate or prevent them in the future.

Behavioral analytics can be simple: any file that drops into the TEMP directory and then elevates privileges is an analytic to identify common malware installation and privilege escalation behaviors. They can be complex linking together various phases of the intrusion and adversary activity. But they must be highly scalable and not bound to individual atomic elements like indicators are. They should also contain context as to what the malicious activity is; really good analytics can also suggest appropriate follow on actions and queue up workflows that incident responders or security personnel should follow as a result of the analytic firing.



This page intentionally left blank.



The Power Grid (Abbreviated)

This image by "DisasterMan" gives a great quick understanding of a standard grid implementation. The key points to notice is that there are often generation stations, transmission substations, and distribution substations. Impacting generation and transmission can impact a lot of folks whereas distribution substations are important to protect but have less potential impact. There are also regional control centers that monitor everything that is going on through a supervisory control and data acquisition (SCADA) implementation. These SCADA systems contain workstations for the operators of the power grid to view the process and what's going on, these stations are human machine interfaces (HMI)s. In short, operators have a Windows system that shows them a picture of what the power grid is doing. It is mostly automated but if you want you can switch to "manual" control to operate portions of the grid without the automation or the SCADA server; it's not ideal but doable. Additionally, outside the SCADA system, in many areas, the only other way to know the power is out is the telephone call center for customers to report the power is out.

Image Reference:

https://disastermanblog.wordpress.com/2012/05/25/how-secure-is-our-power-grid/

Ukraine Power Outage

- On December 23, 2015, Ukrainian energy providers and the Ukrainian government reported outages in the Ivano-Frankivisk Oblast region
  - Reports concerned technical issues where "central dispatch was blinded"
  - Multiple substations disconnected
  - Ukrainian state security service (the SBU) attributed a "virus" and Russia state security services
- Impact lasted around 6 hours
  - Around 60 substations disconnected across three regions of Ukraine leaving 150,000+ customers (each building/apartment/etc. is one customer) without power
  - Biggest impact was no automated systems for grid control for ~8 months
- First cyber attack on a power grid that resulted in loss of operations (power outage)

Case Study: Ukraine Power Outage

On December 23, 2015, Ukrainian energy providers and the Ukrainian government reported outages in the Ivano-Frankivisk Oblast region. Reports were immediately about technical issues where "central dispatch was blinded" and the disconnecting of multiple substations. Soon the Ukrainian state security service (SBU) reported that they had stopped a "virus" and an attack that would have impacted more of the grid if it had not been stopped. Their reports contained information also concerning a DDoS of the telephone call center. The power outage was immediately reported as impacting 80,000 people but that number has reached as high as 150,000 customers. The interesting part though is that the Ukrainian grid (this portion) is entirely distribution and not transmission sites; the regional control centers impacted showed an adversary's ability to cripple the entirety of this region and its control. So, regardless of the number count, it was an entire system failure.

Initial summary of reporting: https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage

SANS ICS Reporting and Analysis

- Jan 1 the SANS ICS team (Michael Assante, Robert M. Lee, and Tim Conway) first reported on the malware sample recovered from the Ukrainian network ("killdisk")
- Jan 9 confirmed the outage was due to a coordinated cyber attack
  The "KillDisk" component though was not responsible for the outage
- "KillDisk" taking down the SCADA server would have blinded the operators and made it difficult to recover but wouldn't have caused the power outage
- SANS ICS released full report at https://ics.sans.org/duc5

SANS ICS Reporting Analysis

A few days after the event the SANS ICS team was passed a malware sample that was recovered from the impacted Ukrainian networks by trusted sources. The malware was analyzed and determined to be the "KillDisk" component found in BlackEnergy3. BlackEnergy3 is a piece of malware used by the Sandworm team which has previously been reported to have had ties with Russia. However, the SANS ICS team (Robert M. Lee, Michael Assante, and Tim Conway) specifically strayed away from attribution and focused instead on the defense lessons learned. They were the first to report on the malware being uncovered which added credibility to Ukraine's claim of a cyber attack.

With more first-hand data and analysis of the systems themselves (the control systems not just the 'cyber' components) the SANS ICS team was able to determine that there was, in fact, a coordinated attack on the Ukrainian power grid. They have been mostly tight-lipped other than the confirmation of the attack and the focus on defense lessons learned.

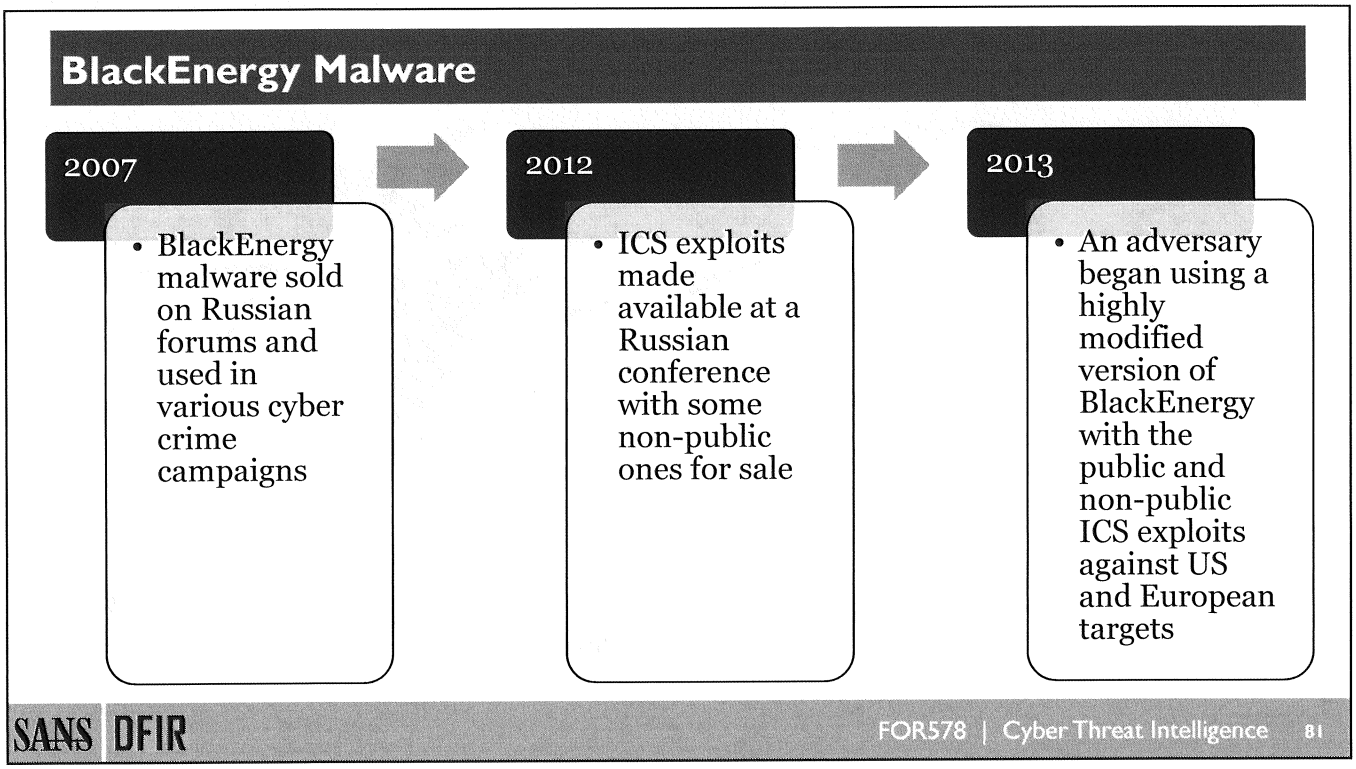
With an understanding of the KillDisk component and SCADA systems, it's clear that the component couldn't have caused the outage. It was much more likely that BlackEnergy3 enabled access to the environment and KillDisk made it more difficult to recover after the attack.

Series of webcasts and blogs from the SANS ICS team kept the community informed on the evolving analysis but SANS stayed away from attribution. Others including iSight performed great analysis and noted that the attribution was Russian actors but not necessarily Russian government.

Reference:

https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered

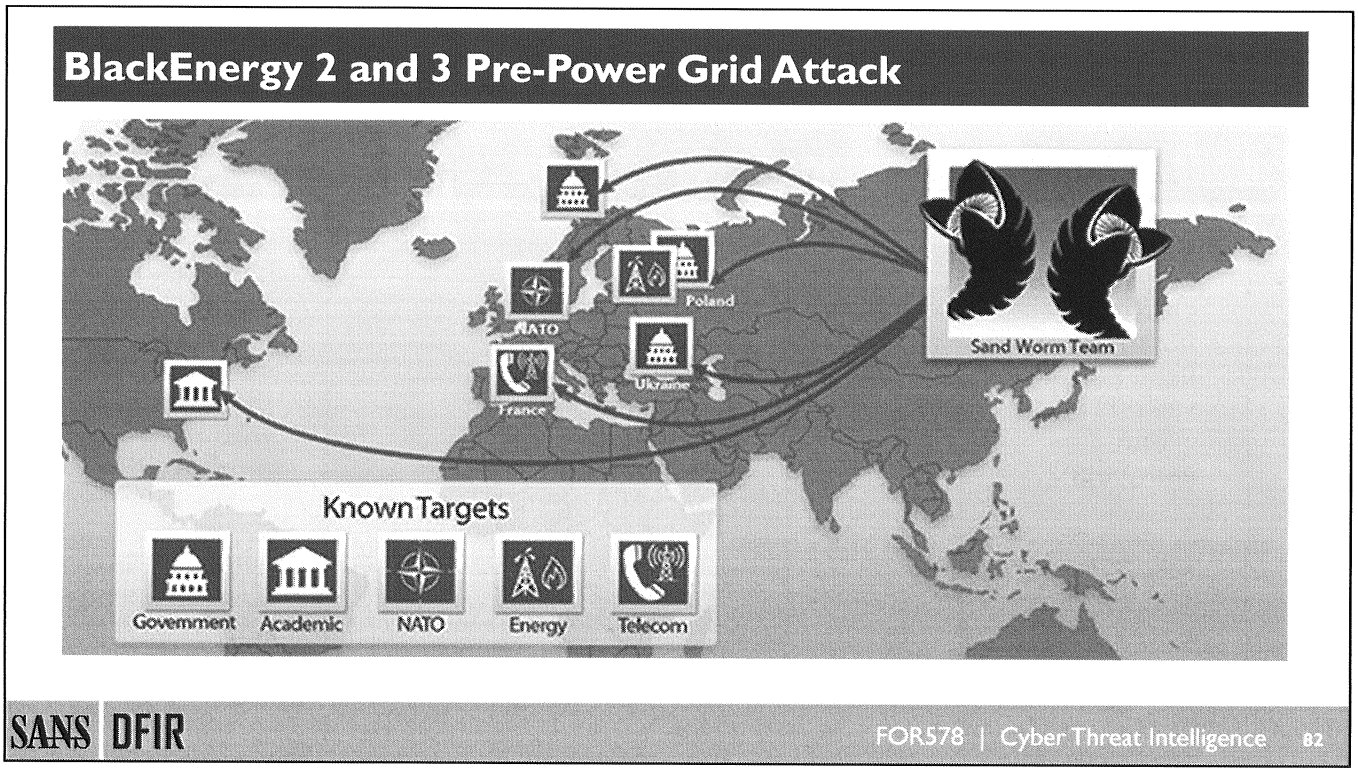
https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid



BlackEnergy Malware

The BlackEnergy malware was originally a piece of malware sold on forums for crime purposes including DDoS and credit card scraping. The malware was available for purchase by a large number of people and groups. Separately, there was a conference in Moscow, Russia where researchers released ICS tailored exploits that allowed remote exploitation of Internet-connected Human Machine Interfaces (HMIs) (HMIs are the systems used to operate industrial control systems used by human operators). Interestingly, the researchers noted that 2 of the exploits were public but the other 3 they would not release and were available for sale.

In 2013 and 2014, following the availability of the exploits and the malware, a group known as Sandworm leveraged a highly customized and enhanced version of BlackEnergy, the public exploits, and the non-public exploits to target industrial sites in the U.S. and Europe.



BlackEnergy 2 and 3 Pre-Power Grid Attack

BlackEnergy was a common Russian underground piece of malware for DDoS styled attacks back in 2007. However, an advanced actor co-opted the malware and added the "Sandworm exploit" to it to leverage it in a campaign. BlackEnergy3 was identified as the version that targeted companies and BlackEnergy2 targeted ICS locations (different exploits and modules and will be discussed in the next slide).

The Sandworm Exploit report by iSight Partners (https://www.isightpartners.com/2014/10/cve-2014-4114/) led to the identification of multiple C2 servers. TrendMicro analysts pivoted off of the C2 servers to find a file that had been seen communicating to one of the IP addresses. The file was identified as config.bak which is a type of file that goes with GE's CIMPLICITY SCADA software. From this, the analysts were able to identify other files related to the config.bak file including files that were downloaded from the C2 server. These other files were additional types of CIMPLICITY related malicious files as well as non-CIMPLICITY related malware. The other files were useful in identifying e-mail addresses, follow on files, C2 servers, and targets.

The work by the TrendMicro analysts off of the iSight report allowed the iSight analysts to revisit the data in a follow-up report (http://www.isightpartners.com/2014/10/sandworm-team-targeting-scada-systems/) and identify additional files such as CCProjectMgr.exe that were being used – which are related to SIMATIC and Siemens WinCC software. This helped developed new indicators useful for analysts to identify infected systems.

Reference:

https://threatpost.com/sandworm-apt-team-found-using-windows-zero-day-vulnerability/108815/

http://www.isightpartners.com/2014/10/cve-2014-4114/

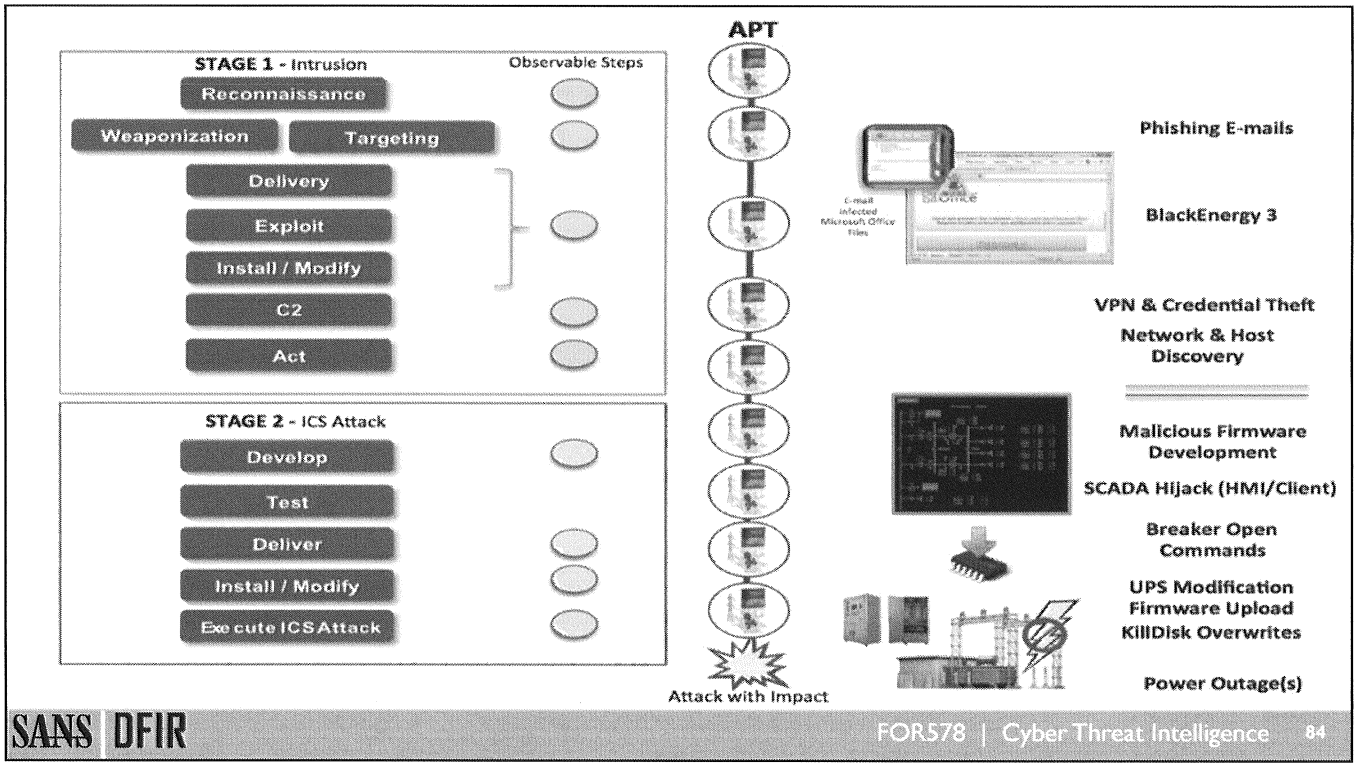
Image Ref: iSight

BlackEnergy3 in Ukraine

- BlackEnergy3 was identified in the Ukrainian power grid network
  - Previously BE3 did not target ICS only BE2 which showed an evolution of the campaign
  - Cybersecurity companies originally misreported that a spear phishing e-mail and XLS document was the initial infection vector when it was actually a Word document with macros enabled

BlackEnergy3 in Ukraine

Information about the event is still evolving but the links between BlackEnergy3 and the Ukraine attack are growing and very interesting. First, the threat was still the human, not the malware; the malware itself likely did not impact the power but enabled the attack and made cleanup more difficult. The indicators, the network traversal, etc. were all great case studies for threat intelligence analysts. For those doing tactical defense the active cyber defense cycle demonstrates the pattern of using indicators, searching in traffic, responding to the systems impacted, and analyzing/documenting the threat and internal information collected. The case study helps bring together the concepts in a manageable way.



Ukraine Kill Chain

The full report is available here: ics.sans.org/duc5

In the event of an attack, the adversary infiltrated the business network with BE3 via phishing emails and gathered credentials such as the VPN credentials into the ICS. They then accessed the ICS and learned the environment. From there they developed malicious firmware for serial to Ethernet devices (bridges between the SCADA environment and the remote substations), learned the SCADA environment, and ultimately opened up the breakers, bricked the serial to Ethernet devices with the malicious firmware, used killdisk malware to delete information off of systems and render them inoperable, reconfigure the UPS so that the center would lose power when the electric grid went down, and launch a telephone denial of service attack to add to the confusion.

It's important to note that the attack took place across the business and industrial networks and that in the business networks it was only a matter of days, but in the industrial networks, adversaries existed for months before the attack took place.

The ICS Cyber Kill Chain

The ICS Cyber Kill Chain was written by Robert M. Lee and Michael Assante as a method to analyze attacks on industrial control systems (ICS). Specifically, the analysis was for attacks (not espionage, theft, or breaches) and for those type of high confidence process effects that can damage infrastructure or cause physical effects such as power outages. It was an adaptation of the Kill Chain from Lockheed Martin to show an extended kill chain is required in ICS attacks – thus highlighting defenders have more time and opportunities to defend and counter adversaries.

The ICS Cyber Kill Chain Stage 1

The full paper is available here: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

In the ICS Cyber Kill Chain, much of Stage 1 is similar to the Kill Chain identified previously in the course. The main difference is that there is also an optional targeting phase instead of weaponization. Internet-connected control systems do not need anything weaponized to target as an example.

The focus on the ICS Cyber Kill Chain is analyzing high confidence attacks on ICS; not any intrusion and not any attack. Specifically, the attacks we are concerned most within the ICS community. Stage 1 is only the beginning part though to be able to learn the ICS.

The ICS Cyber Kill Chain Stage 2

Phase Two:

Tailored Capability

With the appropriate exfiltrated data and network access adversaries, if they desire to have a physical impact or to posture to impact the infrastructure later, they will have to create a tailored capability. Simply creating a DoS is a sloppy and uncertain method of creating physical impacts in an environment. The more tailored a capability, the more certain it is to have the desired impact, but the less likely it is to be useful against other targets. That is, more specific = more impact = less targets. In this stage, adversaries will conduct research back in a mock environment, test lab, or other areas in which the defender is unlikely to detect the research.

2nd Stage Delivery

Adversaries must deliver the tailored capability to the target environment. This can be done through the already established C2 server or through the same method as the 1st Stage Delivery. However, it can appear entirely unrelated. The adversary may choose another attack vector so that if the capability is detected, they do not also alert defenders to their original access. This helps the adversary remain persistent.

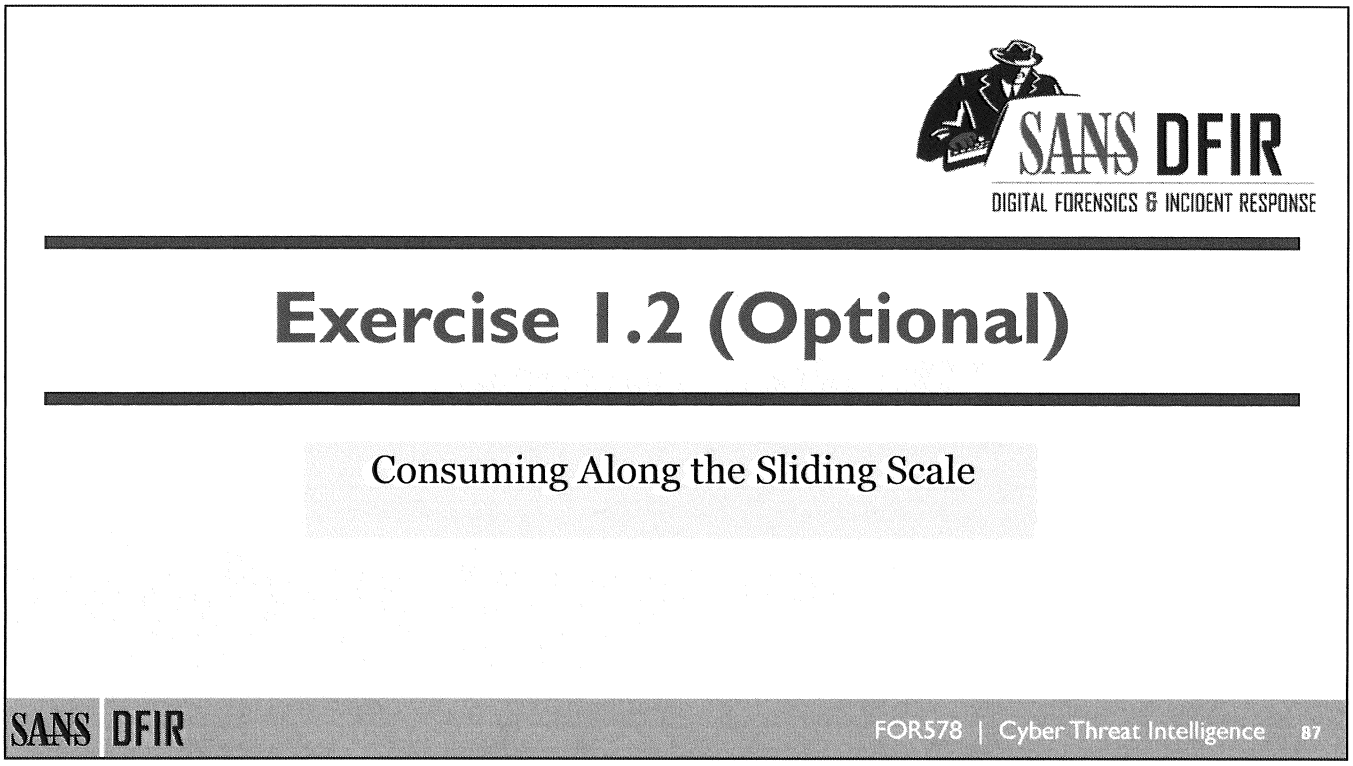
Impact

At this point, it is too late for the defender to counter the adversary. This stage is when the tailored capability has its desired impact. Likely, the tailored capability will not work perfectly regardless of the research because there are always unknown variables, even to the adversaries. Therefore, in this stage, although the defender cannot counter the adversary, the defender can initiate incident response procedures to ensure the safety of personnel and civilians. Time is of the essence, and incident response is not limited to information security incident response at this point.

Exercise 1.2 (Optional After Class) Lead In

- One of our subsidiary companies is Acme Power
- You are on the security team
- Consume intelligence from the 2015 attack
  - Make recommendations for better security
  - Identify useful indicators from the case
  - Identify useful behaviors to identify past indicators

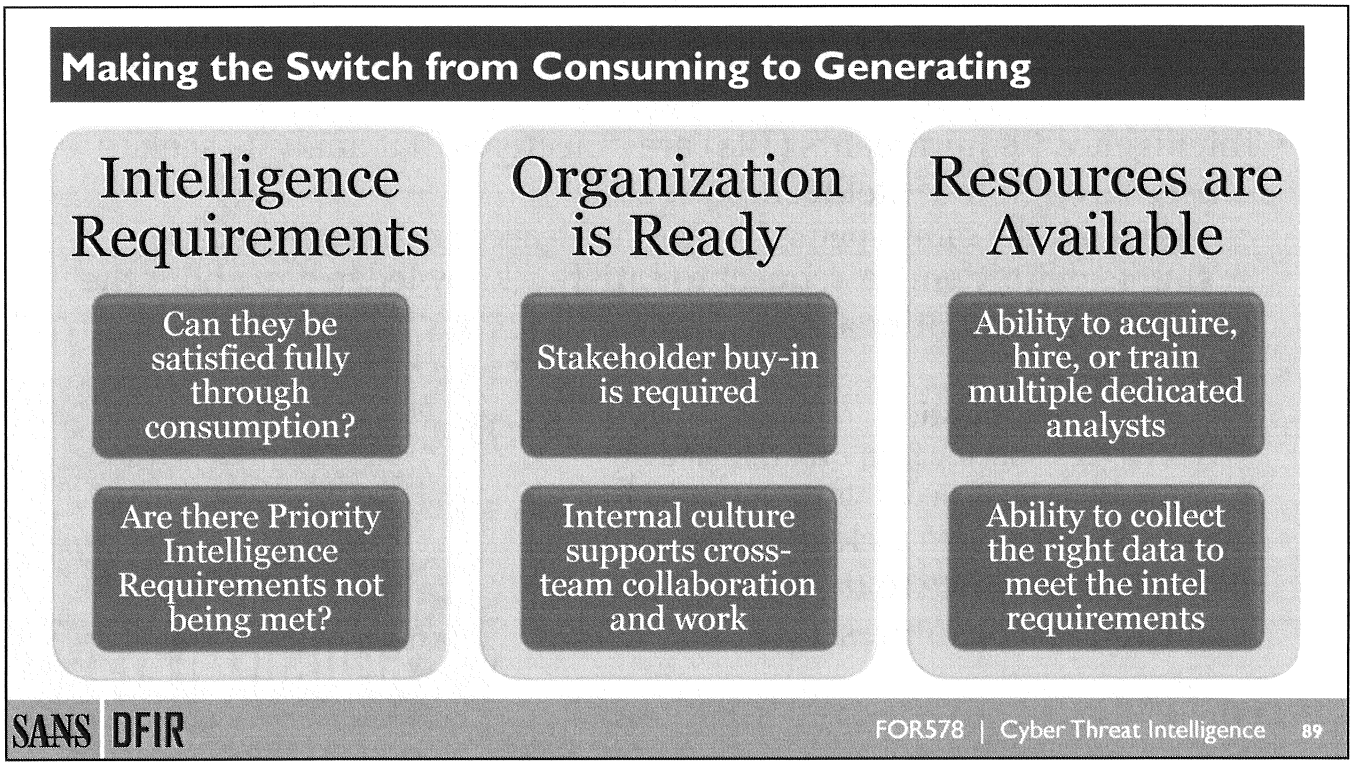
This page intentionally left blank.



Please refer to your workbook for Exercise 1.2.

Preparing the Team to Generate Intelligence

This page intentionally left blank.



Making the Switch from Consuming to Generating

In truth, generating and consuming intelligence are very closely linked and the line between those two functions is gray at best. However, there is a distinctive difference in consuming intelligence to meet an objective vs. generating intelligence in terms of the skills, analysis, and focus needed. In intelligence consumption, you want to validate what you are looking at is legitimate and try to apply it to your use cases. In generation, you are analyzing adversary activity to identify information that can meet a requirement. Many intelligence teams in the private sector will find themselves performing both actions back and forth. Many security operations analysts and incident responders can be fully trained to be great at consuming intelligence. However, having a dedicated team that generates intelligence can be very costly – so it must be justified.

An easy way to justify if an intelligence team is needed is to determine your requirements and see if you can fully satisfy them from just consuming intelligence. If you cannot, you then should determine if you have the resources available (people, systems, organization, data, etc.) to meaningfully satisfy your intelligence requirements. One of the worst things that you can do though is establish an intelligence team without any clear objectives. It will be largely a waste of money and time.

Intelligence Requirements

- Intelligence Requirements (IRs) are objectives that analysts seek to satisfy through the intelligence process
  - They guide the entire approach to the intelligence process and life cycle
- A simple definition: "A request to satisfy a knowledge gap about the threat or the operational environment"
- Best practices:
  - Ask only one question
  - Focus on a specific fact, event, or activity
  - Support a single decision
- Teams should have a clearly articulated list of IRs available to the intelligence team and its consumers

Intelligence Requirements

Intelligence requirements are the objectives that analysts seek to satisfy through the intelligence process. Our finalized intelligence products should meet those requirements and guide how we do the process such as collection, exploitation, and analysis of the data. Simply defined (drawing from JP 2-0) an intelligence requirement is "A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment of threat forces." That's a bit intense and very militarized. So instead we'll use the definition: a knowledge gap that needs addressing to enable action

Intelligence requirements need to be simple and support a single decision by decision makers. The focus on specific events, facts, and activity will also help avoid nebulous requirements such as "will we be attacked?" It is a best practice to keep intelligence requirements visible to everyone on the team and make them visible to the consumers as well. We want our consumers to have direct input into the intelligence requirement process because it is a bad habit to let the intelligence team define these on their own – we are not the consumers of our own intelligence.

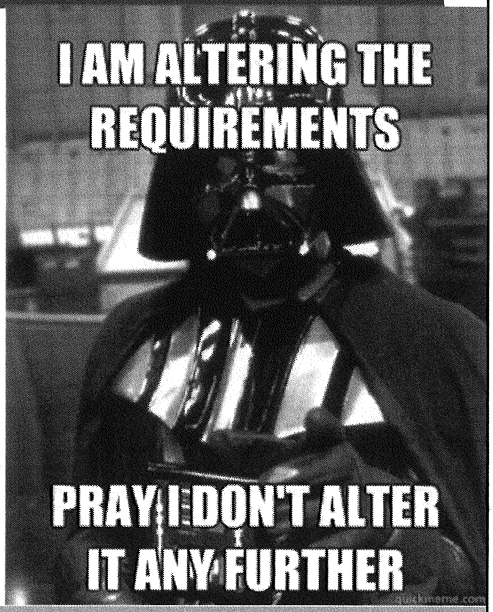
Reference:

http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

https://medium.com/@sroberts/cti-squadgoals-setting-requirements-41bcb63db918

Priority Intelligence Requirements

- Priority Intelligence Requirements (PIRs) are those IRs that are seen as critical to mission success
- They follow the same best practices as IRs
- In addition, they will often change over time
  - Many IRs will be standing requirements
  - PIRs are often tied to specific events or times
  - Require highest level of buy in to be effective
- Recommendation:
  - Do not let consumers input PIRs without conversation or mapping it to specific mission-critical decisions facing the organization
  - Not everything is critical



Priority Intelligence Requirements

Priority Intelligence Requirements (PIRs) are those intelligence requirements that are key to the mission of the organization. Satisfying the PIRs should be seen as paramount to mission success. Because of this, it is common for PIRs to be highly fluctuating. It would make sense that PIRs would be very static and stable IRs that do not get changed often, but the reality is that our decision makers are most concerned with the immediate future regarding threats or situations. As an example, "will the acquisition of $X company open us to targeting by new threat actors?". This is going to be bound by a timeline of the acquisition of the company. However, that decision may weigh very heavily on the acquisition of the company to our decision makers and thus be a priority intelligence requirement.

PIRs follow the same best practices as IRs in terms of their simplicity and focus but also should often come as the result of thorough interaction between the intelligence team and the consumer. Intelligence teams should map PIRs to significant events or risks facing the organization and there should be buy in from the senior level decision-makers that will use the PIRs else they will be ineffective.

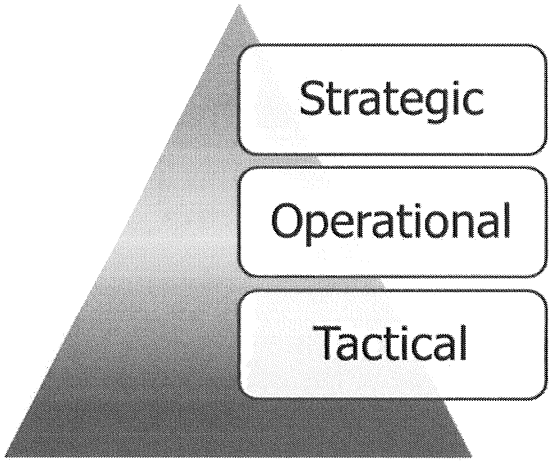
Reference:

http://www.dtic.mil/dtic/tr/fulltext/u2/a234157.pdf

http://www.globalsecurity.org/intell/library/policy/army/fm/34-8-2/34-8-2ap-d.pdf

Intended Audience

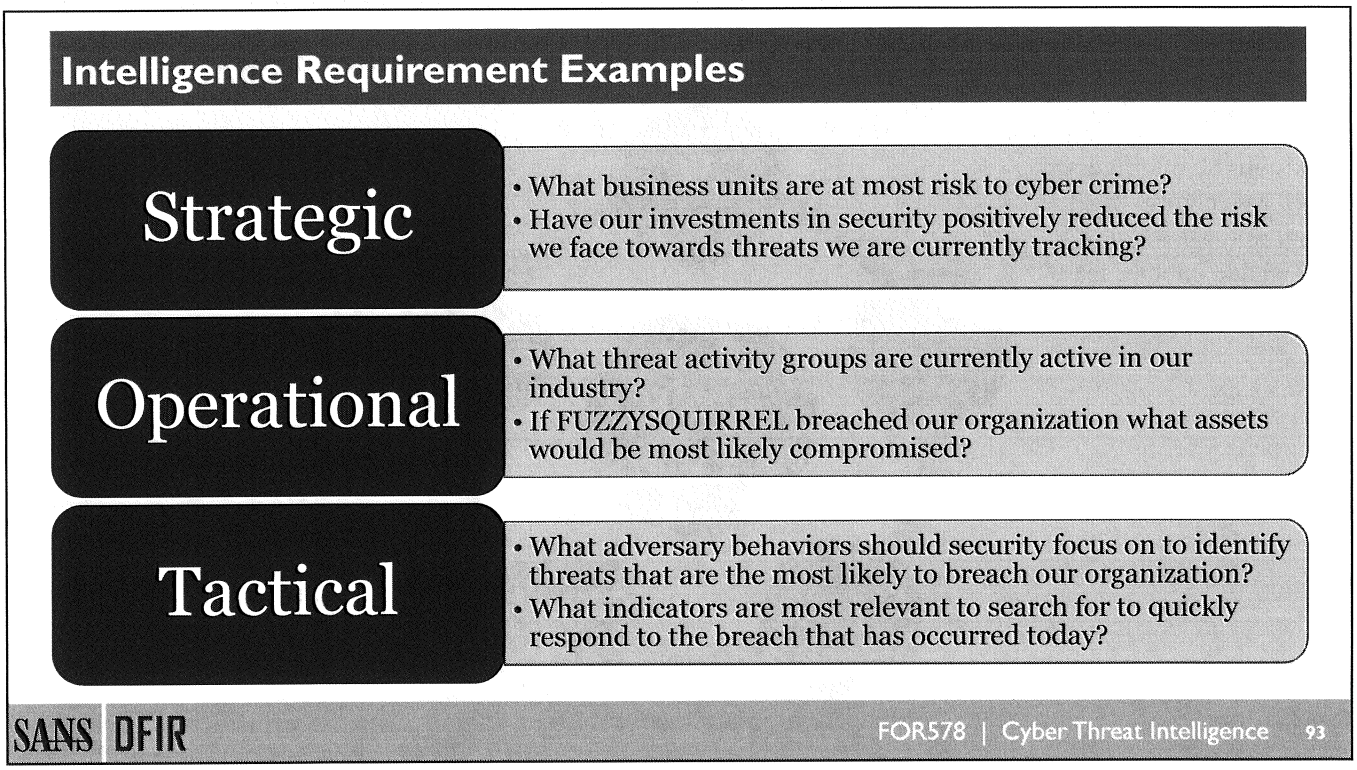
- The intended audience and their goals determine the type of threat intelligence generated and how it is to be used



Intended Audience

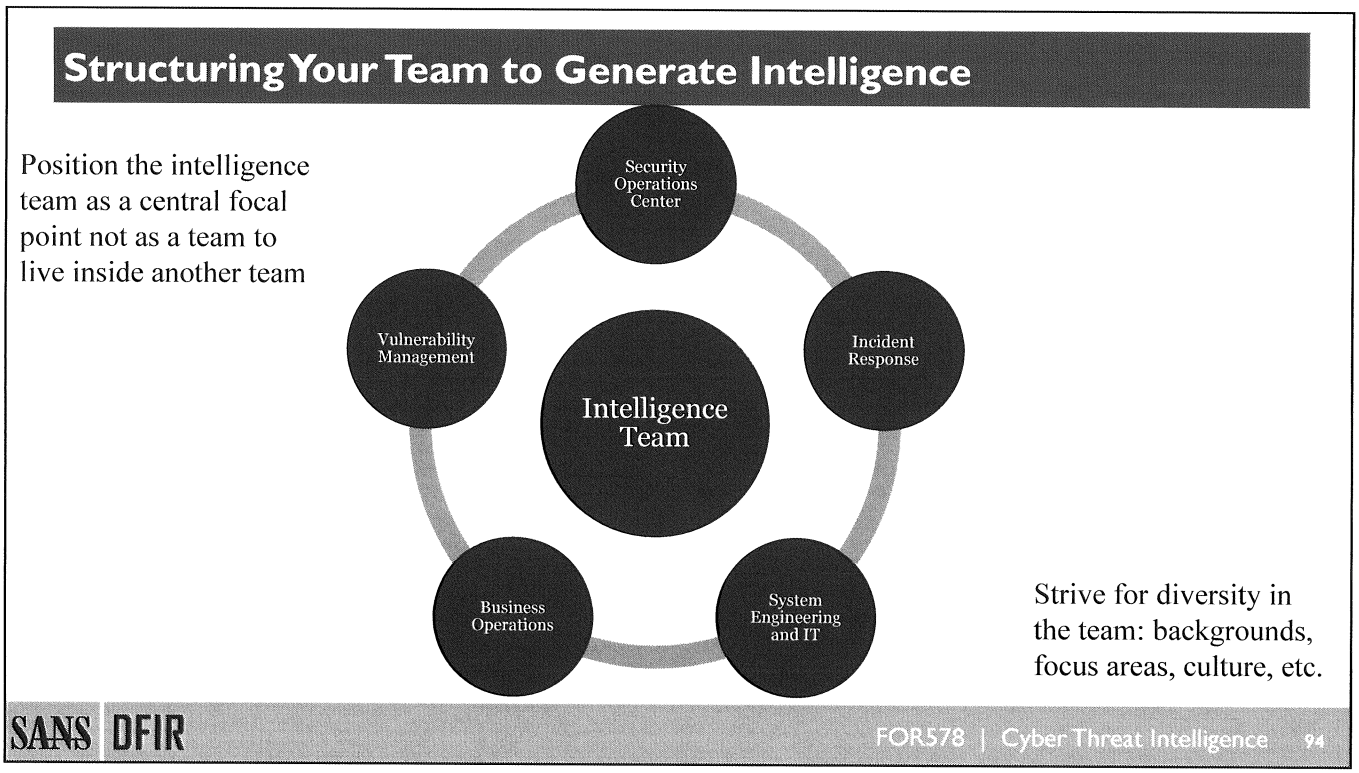
It is important to identify the audience's needs. Are they executives that need more strategic understanding? Or are they technical folks who need more tactical level information? Understand these audience types and what they need helps drive the goals of the intelligence process. In addition, it helps drive how the intelligence is presented and in what manner the audience needs the intelligence to consume it quickly and effectively. Through the rest of the day, we'll discuss the three general types of audience members for threat intelligence: Strategic, Operational, and Tactical. These three groups are not the only way to identify threat intelligence audiences but are useful for structuring how threat intelligence is shared and ultimately used.

Good intelligence analysts should be able to operate across this spectrum; they may have a specialty or one they like more but they should be able to do the work across tactical-operational-strategic.



Intelligence Requirement Examples

It is not required to break intelligence requirements down into strategic, operational, and tactical categories but it can be a useful thought exercise and also shape our understanding of how the audience needs to consume the intelligence. As an example, the indicators that the tactical folks need will be delivered in an entirely different approach by the intelligence team than the understanding of cyber crime risk to our executives. Intelligence requirements should be achievable goals to important questions to enable others. While it seems like a simple process you will find a lot of your most challenging initial work is working with consumers to develop good intelligence requirements. Often, our consumers do not understand exactly what they need out of intelligence because they are not aware of what all intelligence can provide. It is important in these cases to lean on our own understanding of defense, our threat model (to be covered later), and pain points in the organization.



Structuring Your Team to Generate Intelligence

To set your team up for success you will need to think long and hard about where it goes in the organization. There is no right or wrong answer so long as your team satisfies the intelligence requirements levied to it. However, your intelligence team will absolutely take on the focus of those that have the most access to you. As an example, if the intelligence team lives inside the Security Operations Center (SOC) it is very likely most of the IRs will be SOC-related. The PIRs will take a SOC focused approach and many teams outside that organization may not ever levy appropriate requirements. However, without access to the SOC and Incident Response teams, the intelligence team will likely never get the intrusion data to analyze and satisfy intelligence requirements of other teams.

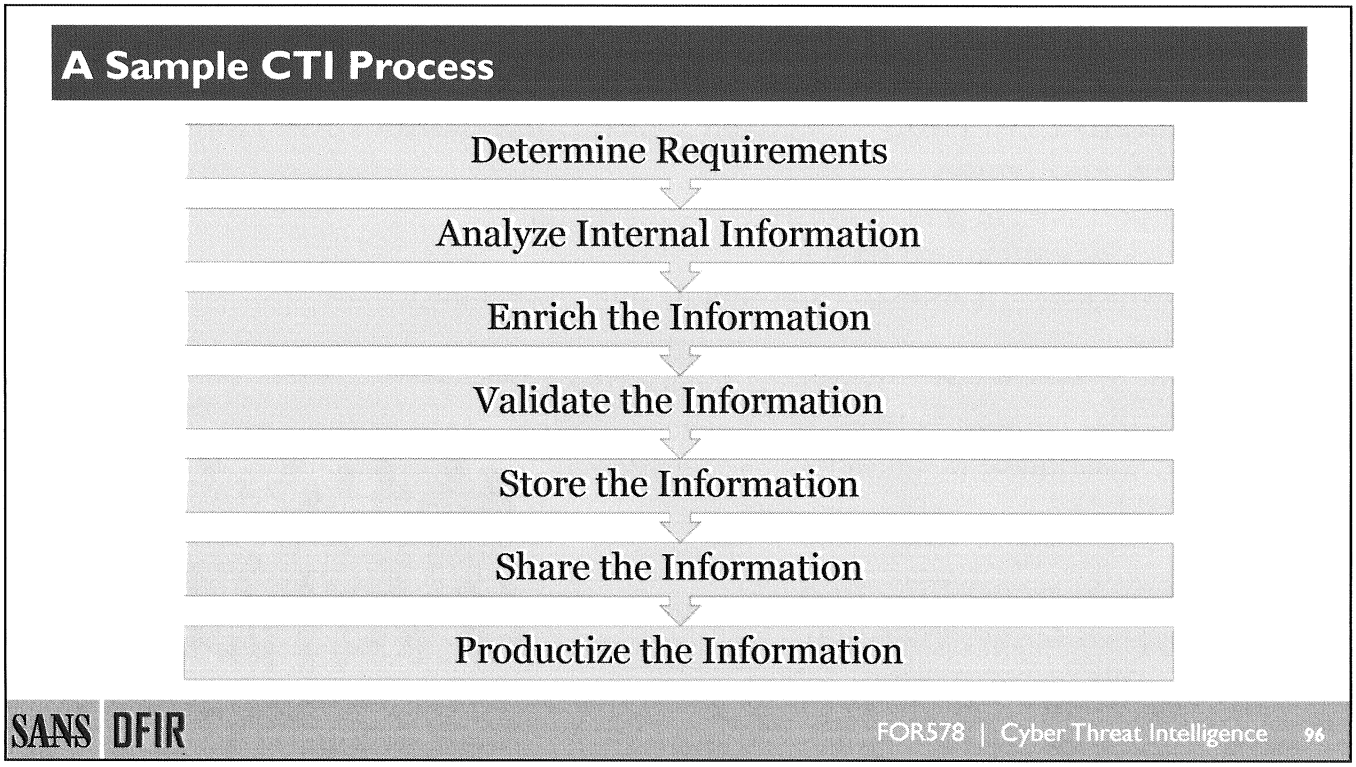
For this reason, it is suggested to treat the intelligence team as an independent team with direct ties to different organizations. In a perfect world, it would be in the center of all the security-related teams with a direct tie to other teams even outside of security and a direct reporting line to as high in the organization as suitable (CISO or CSO would be appropriate in most cases).

A Few Sample Purposes of a Cyber Threat Intelligence Team

- Preventative Function – Security Operations Center (SOC) support, alerting, and triage
  - Support SOC in generating and triaging alerts
  - Provides enrichment on IOCs
  - Provides information to vulnerability and risk management
- Response Function – Incident Response support
  - Provides support to IR team on engagements
  - Provides Enrichment on IOCs and artifacts
  - Facilitates information sharing
- Strategic Support Function
  - Supports business decisions
  - Informs resource prioritization

SANS DFIR FOR578 | Cyber Threat Intelligence 95

Cyber threat intelligence teams can support various roles within an organization, from the SOC to vulnerability management to the CISO and the board of directors. The role of the CTI team within an organization will depend on the needs of that particular organization. If you have trouble deciding where the intelligence team should sit in the organization think about the requirements it is attempting to satisfy and what type of function the intelligence team is taking. Use that to guide the organizational chart much more closely than any best practices issued elsewhere. As an example, it is often considered a poor organizational choice to put the intelligence team in a vulnerability management group. However, if that is the most important thing to your organization and consumes a majority of your intelligence requirements it could be a good choice for your organization.



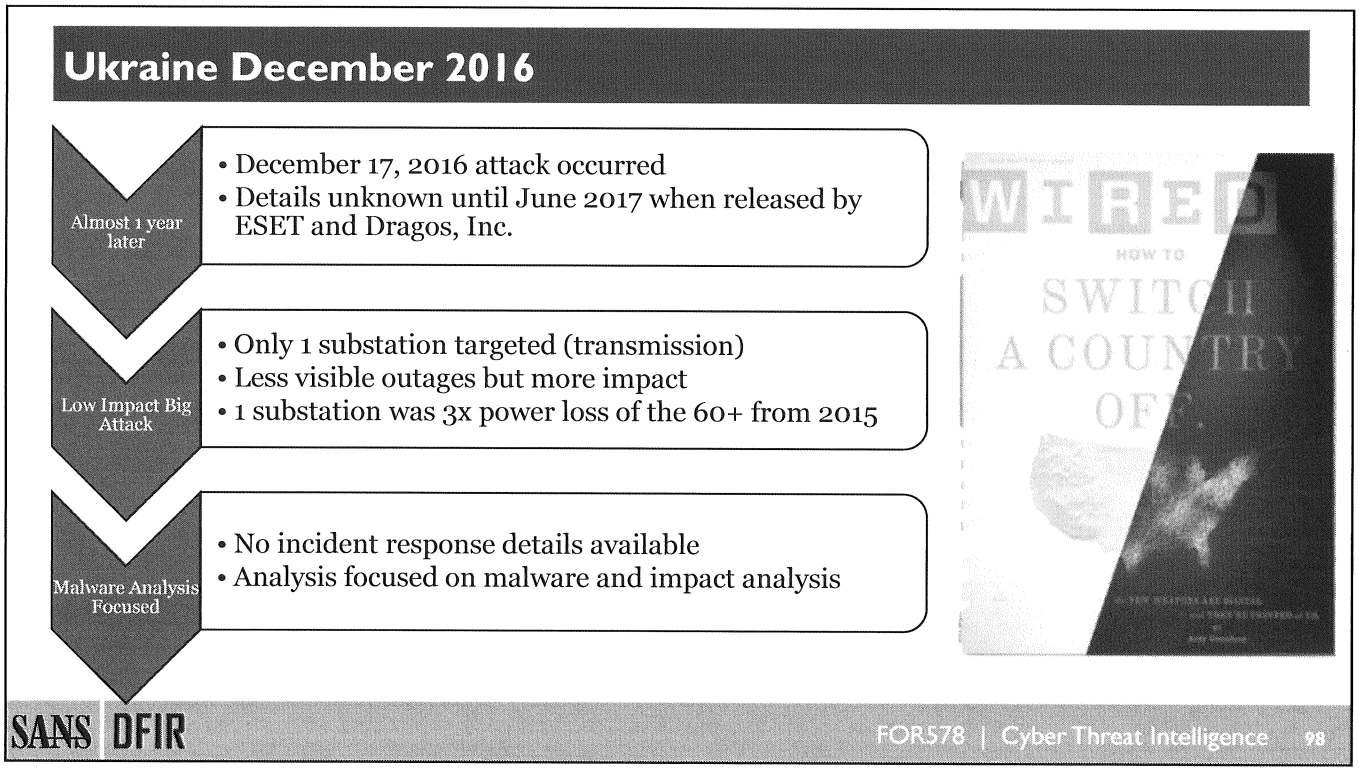
A Sample CTI Process

This is one sample process on how to perform cyber threat intelligence. It takes from the intelligence life cycle and applies the current focuses of cyber threat intelligence today. It will act as a model for the class – it is only one way to proceed but will help focus our skills throughout the course.

Determining requirements ensure that the intelligence produced fits some goal that we set forth for it such as incident response efficiency or understanding of a specific threat. Analyzing internal information ensures that we always focus on the best threat data possible – what is available in our organizations. Then analysts should enrich that information usually using peer-to-peer relationships that currently exist or open-source data sources. Then that information should be validated as false positives are one of the most expensive aspects of cyber threat intelligence. Then that information should be stored appropriately so that it is made available to us and is useful in the future. Once that information is stored appropriately in a structured way it should be shared out to others and we should receive information back in return for sharing. Eventually, the intelligence should be productized into reports, briefings, or models such as threat modeling (which will be explored later today).

Case Study: The First Ever Electric Grid Focused Malware

This page intentionally left blank.



Ukraine December 2016

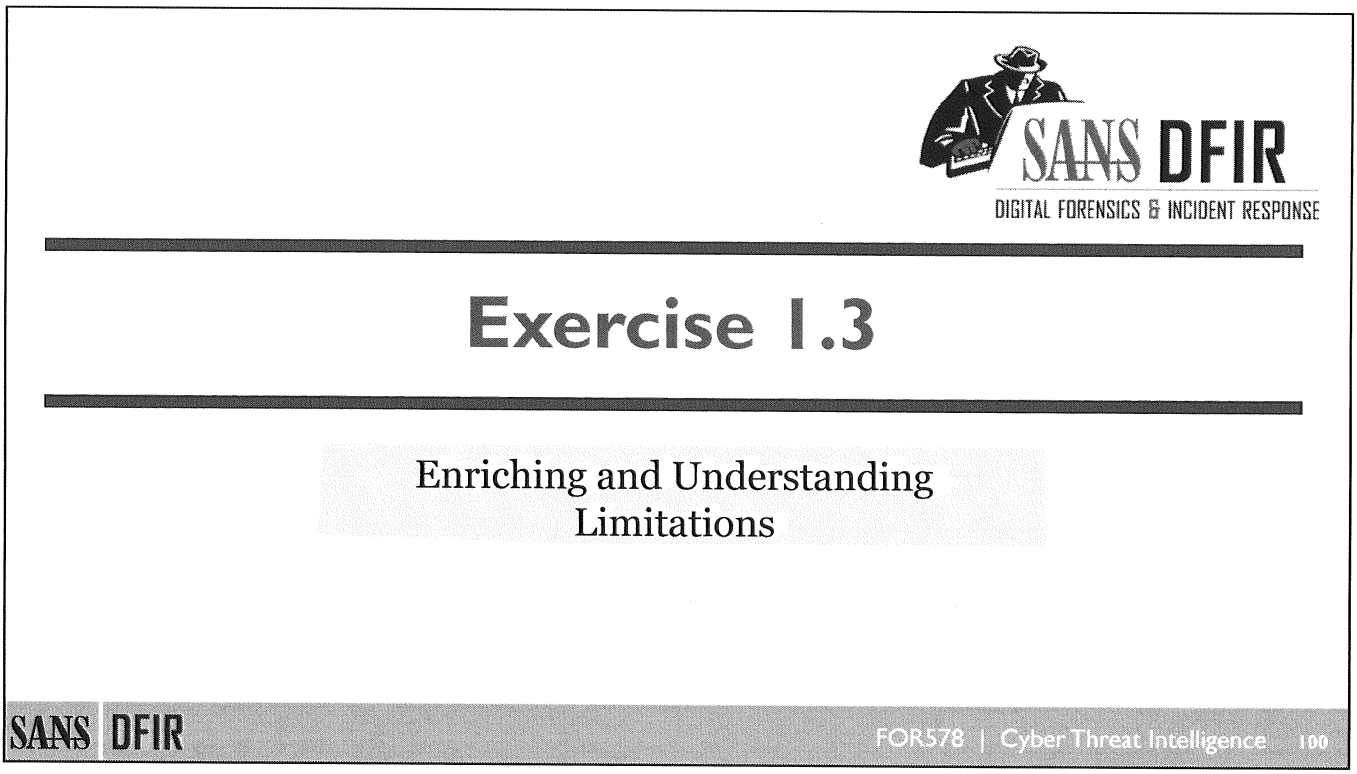
On December 17, 2016, almost 1 year after the 2015 attack, the Ukrainian power grid was attacked again. This time the attack took place only at 1 substation but it was a transmission level substation in Kiev. The total power loss was over three times the amount of all the power loss in 2015 but the impact was not very visible to most citizens as it was an impact on the bulk grid which was able to take the blow. In many ways, the attack appeared to be a proof of concept of a new, highly scalable, and grid focused malware that could be used to target other power grid sites.

The firms ESET and Dragos, Inc. did not have access to the incident response details but were able to get samples of the malware which they released in June 2017. ESET had decided to release the details when Dragos, Inc. was notified about it with less than 96 hours from notification until announcement. In the 96 hours, the Dragos team reverse-engineered the malware, identified the adversary group, performed responsible disclosure to the industry before they would have to learn about it from the press, notified CERTs around the world, and did an impact analysis that also confirmed the malware was used in the 2016 attack.

Exercise 1.3: The Evolving Situation

- Fast forward past the 2015 and 2016 attacks, Acme Power wants to know if this new malware can impact them
- Additionally, our organization also has subsidiary companies that deal in manufacturing and they want to know if they are potentially impacted as well

This page intentionally left blank.



Please refer to your workbook for Exercise 1.3.

Planning and Direction (Developing Requirements)

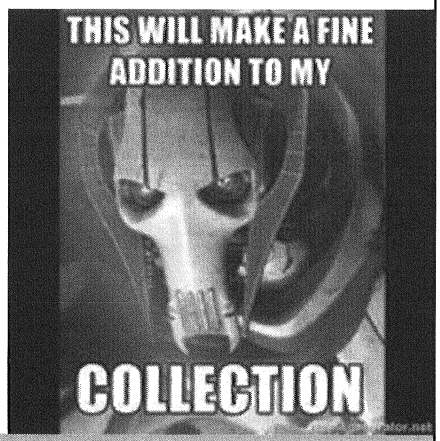
"Take time to deliberate, but when the time for actions comes, stop thinking and go in." – Napoleon Bonaparte

This page intentionally left blank.

Planning: Collection Management Framework

- Intelligence requirements cannot be satisfied if the data or information does not exist to properly fill the knowledge gap
- Analysts must understand where they are getting data, how it is processed and delivered to them, and what questions they can reasonably ask of the data
- A Collection Management Framework is a view of sources of data, what is available in the data, and how that data is processed and exploited

- Analysts who do not understand their collection on a technical level cannot satisfy IRs against it or realize the limitations



Planning: Collection Management Framework

As part of your overall planning to perform the intelligence work required of your team you need to have a good collection management framework (CMF). A CMF is the plan for how you collect data, where you collect it from, and what type of data you collect. Ultimately, this helps you understand what questions can be asked by understanding what data you have access to. Prior to trying to satisfy intelligence requirements, an analyst should understand if that IR is even possible given their CMF or if they need to work on their CMF first.

As an example, do you have a requirement to extract adversary behaviors from intrusions that occurred 3 months ago? And do you only have system logs and intrusion data from 2 months ago? Then that IR is not going to be possible to satisfy and it's important to identify the limitation so that it can be addressed in the future. Do your executives want attribution on a specific threat group but you do not have first-hand experience on the team with that group or actual intrusion data? That too would be an impossible intelligence requirement to confidently satisfy.

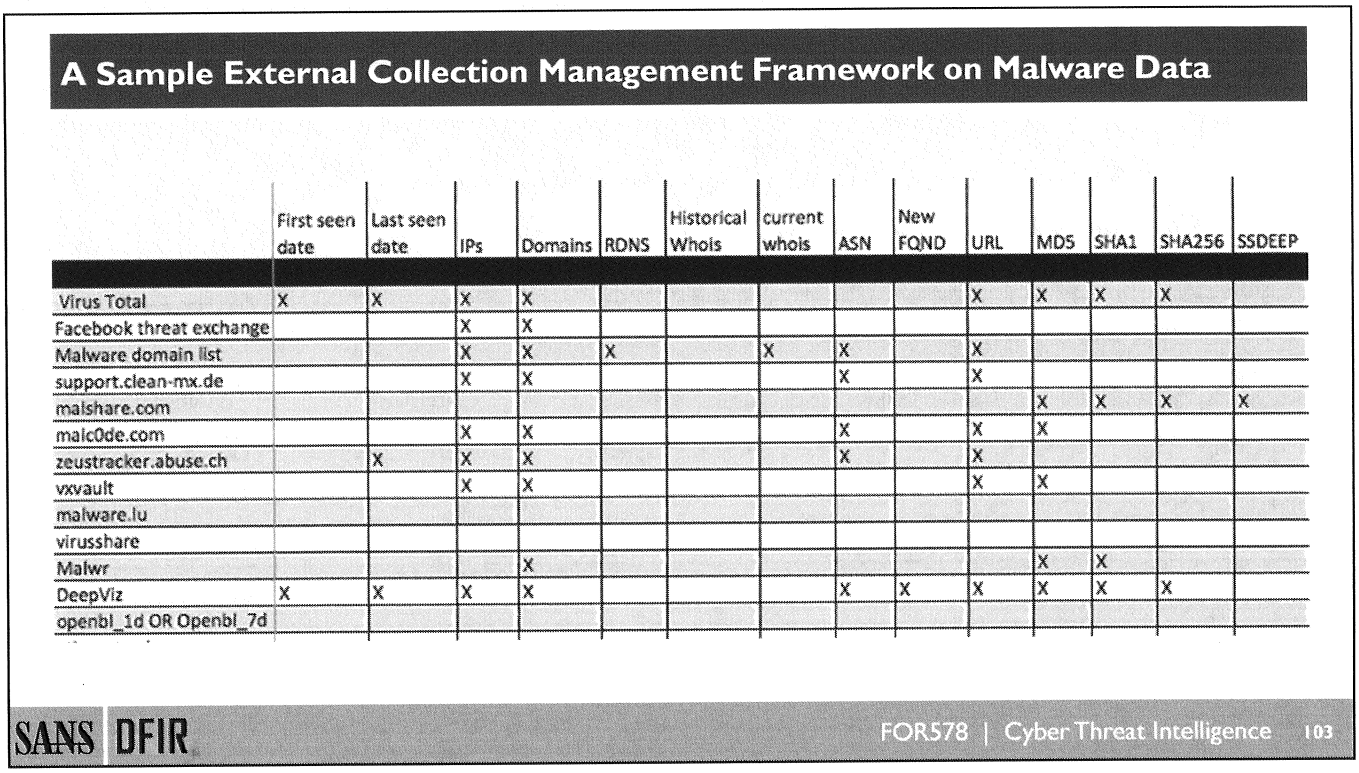
Intelligence analysts in our field can come from many backgrounds from policy to malware analysis. However, it is vital that all intelligence analysts fully understand their CMF and what questions can and cannot be answered. You should be able to ask very well-structured questions of your data and CMF to be successful.

Reference:

http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf

http://326gtd123dbk1xdkdm489u1q.wpengine.netdna-cdn.com/wp-content/uploads/2016/10/Collections-Management-Framework.pdf

https://www.cia.gov/library/reports/general-reports-1/unclass_sip/chapter-6-interacting-with-collectors.html



A Sample External Collection Management Framework on Malware Data

This is an example collection management framework for malware based data. Data is most useful when it meets a specific requirement that an organization needs. A collection plan helps to identify the best data sources for an organization based on their needs and what data they can act on. To build a collection plan, first determine what types of information you need, based on what you can act on. This may include indicators you can alert on, such as IP addresses, hashes, etc., but can also include enrichment information to help with your understanding of threats when something generates an alert.

Next, identify which threat feeds have the information that you need. This includes not only types of indicators, but also their sources. Data comes from somewhere, after all, and the details on what types of threats it captures can help make sure that the feeds or data that you are collecting meets your needs. It can take a bit of research to find out where the data comes from, but it is well worth the effort.

In short, this process helps you understand what questions you can ask of your data.

A Sample Internal Collection Management Framework

	Endpoint Protection System	Windows Systems	Network	Firewall
Data Type	System Alert	Host Based Logs	Netflow	System Alert
Kill Chain Coverage	Exploitation & Installation	Exploitation, Installation, and Actions on Objectives	Internal Reconnaissance, Delivery, and C2	Internal Reconnaissance, Deliver, and c2
Follow on Collection	Malware sample	Files and timelines	Packet Capture	Netflow
Typical Storage in Days	30 days	60 days	23 days	60 days

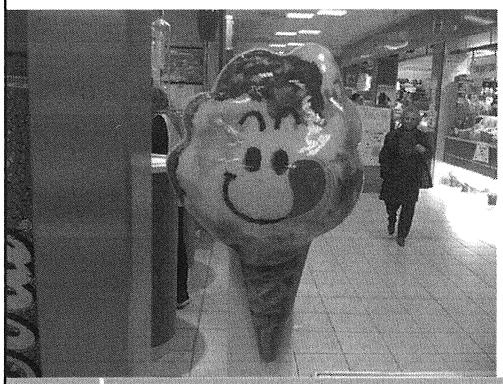
A Sample Internal Collection Management Framework

Instead of structuring your sources and including what they can get for you via types like hashes or IP addresses, you might also approach your collection management framework for the phase of data according to the kill chain the source might be able to get you. Going more in depth to understanding the technical information can also be useful as well.

There is no one way to make a collection framework just make sure it helps answer your questions .

Generating Intelligence Requirements

- Seek input from intelligence consumers
- Formulate intelligence requirements you think they'd need and position it with them for review; offer sample expected results
- Leverage the threat model and pain points in the org as a starting place



Intelligence Requirements help to avoid the self-licking ice-cream cone problem (Useless Intelligence)

Generating Intelligence Requirements

When generating intelligence requirements, it'd be great if consumers could articulate great IRs but often it will not be the case. It is often good practice to open up the dialogue and request IRs but to plan on creating your own for the consumer. Position these back to them for feedback and offer a sample output of what you think you might be able to generate for them based on the requirement. I.e. a report, a briefing, a recommendation, indicators, behavioral analytics, etc. and talk them through how you think they'd use it. You will find that most consumers will nicely correct you and inform you on how they'll actually use the output which goes back into your understanding of their problems. Ultimately, you're addressing pain points for the consumer (tied to knowledge gaps).

These pain points are going to be one of your biggest opportunities to generate intelligence requirements. However, one of the better starting points is your organization's threat model.

Threat Modeling

- Threats are not always equally distributed
- A model is a representation of an idea, an object, or a system
- Identify knowledge gaps to generate IRs

- It can show:
  - Structure
  - Relationships
  - Behaviors

One of the most asked strategic questions is "what threats do we need to be worried about?" Different organizations or individuals will face different threats. There are some threats, such as commodity malware and indiscriminate spamming or phishing that have the potential to impact anyone who is on the internet, however, there are some threats that are more likely to target certain organizations. Understanding those targeted threats: how they operate, what information they are after, and how you are likely to identify their actions.

A model is a replica or representation of an idea, object, or system. It can show form, structure, relationships, or behaviors of the subject that is being modeled. Models are critical to understanding complex targets, or complex sets of targets.

Threat modeling is important for a variety of reasons. There are many different threats that can impact organizations, and there is some sort of threat intelligence available on just about all of these threats. Ingesting and analyzing all the available information on cyber threats is an impossible task, so there needs to be a way for CTI analysts to identify which threats are likely to impact them.

Many people have a rough idea that threats that impact them, and a threat model can help formalize and document those threats, which will give an organization a better understanding of the threats facing you. Understanding what threats are most likely to impact you can help prioritize security efforts, allowing you to focus on the things that are most relevant to you. This allows you to generate intelligence requirements, avoid becoming overloaded with intelligence that isn't relevant to you, and identify where there are gaps in your intelligence collection that need to be addressed.

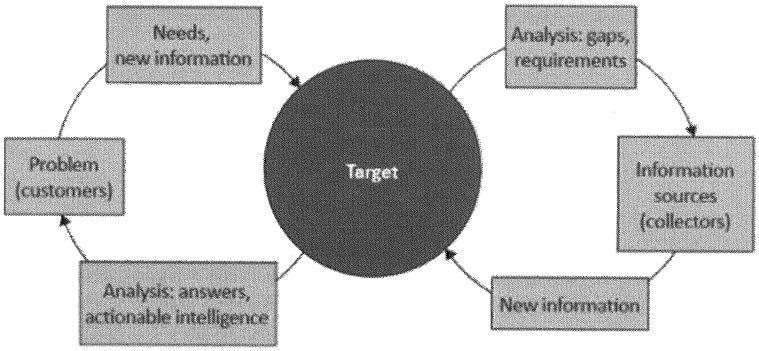
Threat modeling is an art, not a science. When you build a threat model, remember that the threats will not always stay exactly the same over time. It will be necessary to reevaluate and update the threat model periodically.

In addition, while we can analyze what we know about an attacker's behavior to predict future behavior, there is no guarantee that the attacker will behave in that way. Attackers are humans, and they have the option to do things that don't align with a behavior pattern, regardless of how good the analysis of their actions are.

Finally, it is also possible, and more recently it is even likely, that multiple attackers or actor groups use similar tools and tactics which can make it difficult to identify who the attacker is. An example is that if you see a lot of Poison Ivy malware on your system, and you know that Poison Ivy malware was developed by Chinese threat actors, you should not automatically assume that China is targeting your network and change your threat model based on that.

Target-Centric Intelligence Analysis

- Non-linear approach to the intelligence cycle
- Builds a conceptual model of a "target"
- Used as a foundation for further analysis



SANS DFIR FOR578 | Cyber Threat Intelligence 108

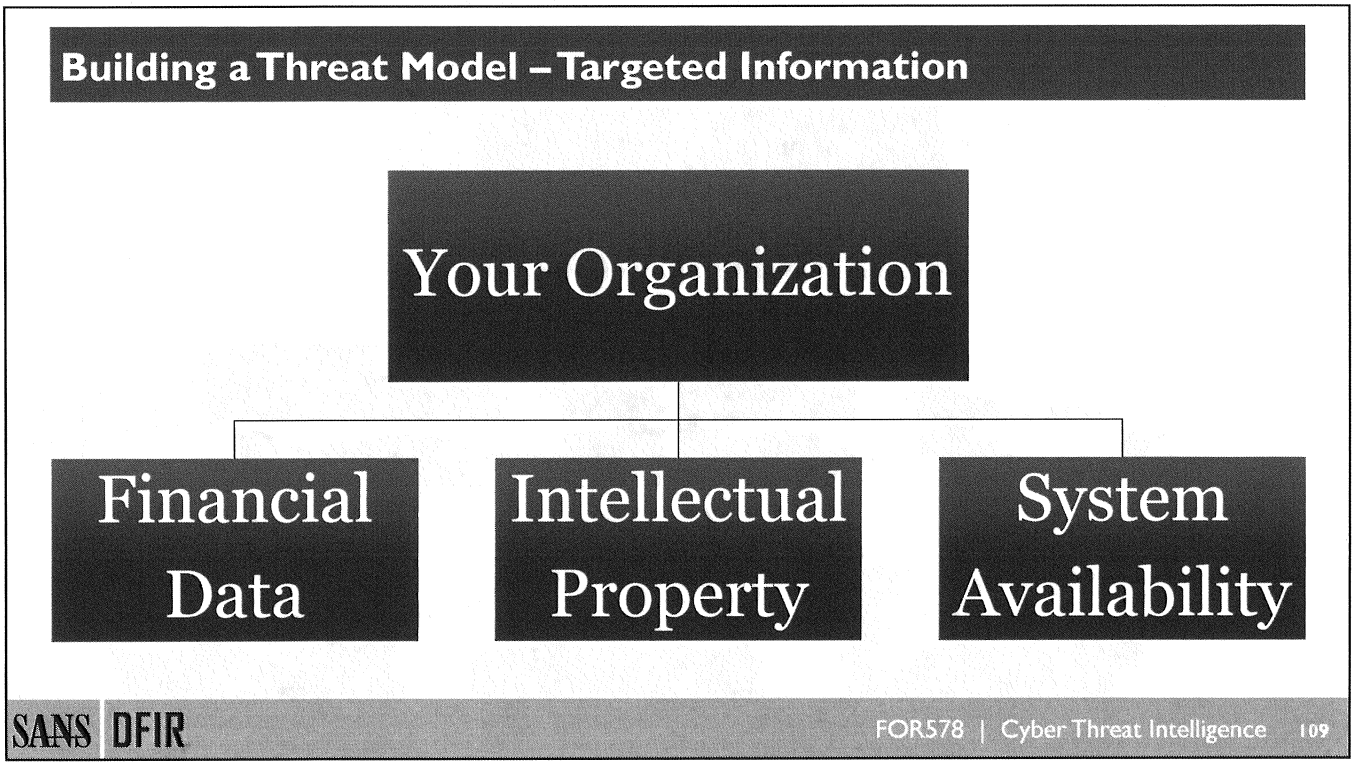
Robert Clark—a former CIA analyst, group chief, and teacher—developed a concept known as "target-centric intelligence", which takes a nonlinear approach to the intelligence cycle. It treats intelligence analysis as a living, changing process that involves many different parties all of which can contribute to the understanding of the analysis. The target-centric approach was meant to get rid of the stove-piping that often occurs in intelligence work.

This process creates a conceptual model that is used as the foundation for further analysis of the target. A conceptual model is extremely flexible, it can detail the hierarchy and structure of a threat group, or can describe a network intrusion.

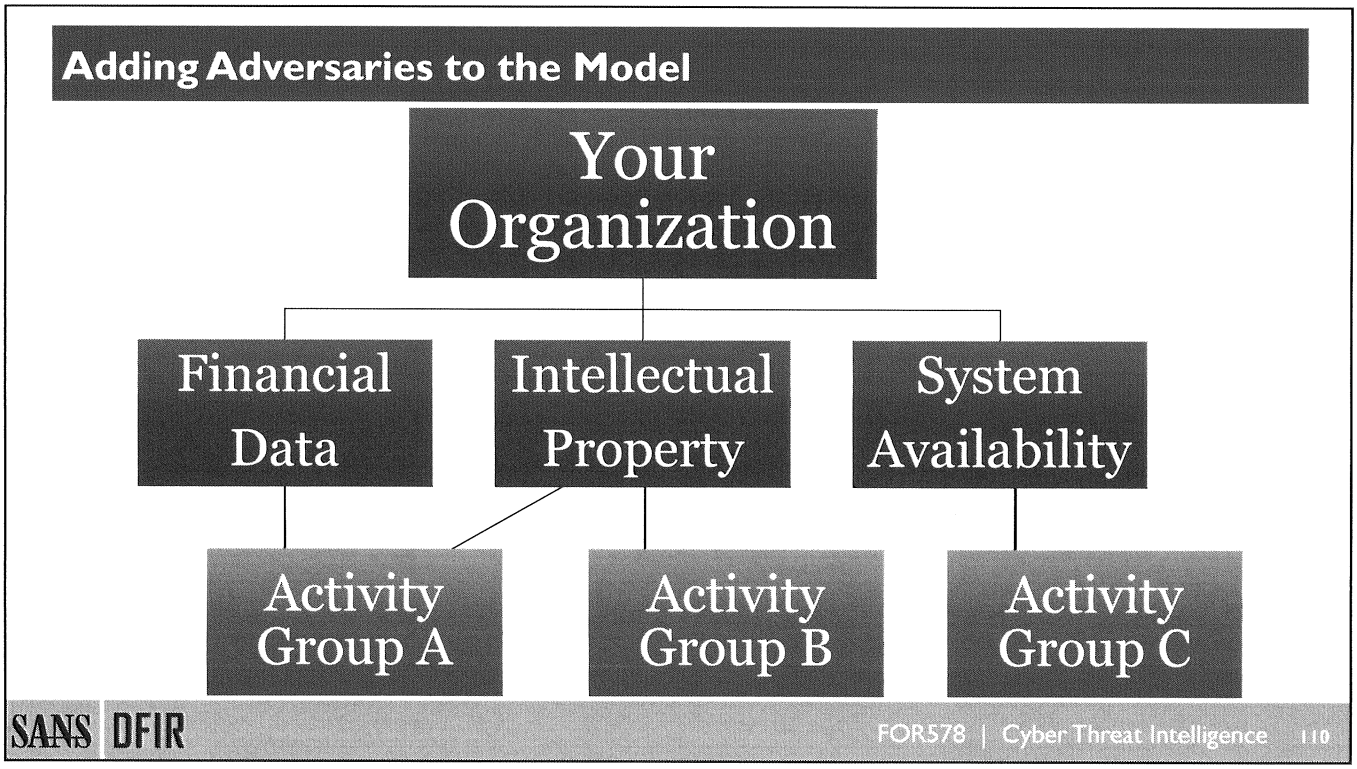
Targets can be individuals, groups, formal organizations or companies, governments, or facilities. There are many different types of targets, it is just important that they are something that can be analyzed and understood in a systematic way.

Image reference:

http://www.journal.forces.gc.ca/vol15/no1/eng/images/44-WILSON-fig1-2-large.jpg



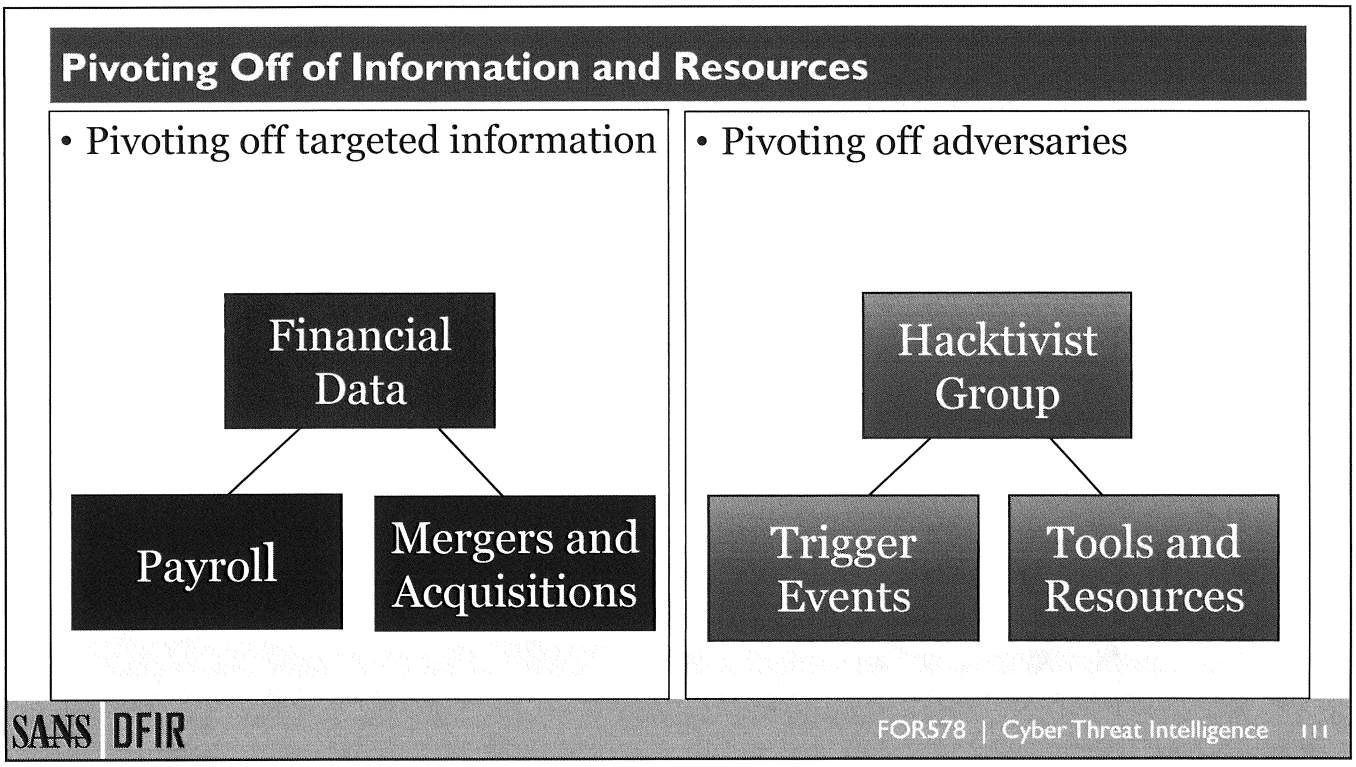
When you build a threat model of your organization, you become the first target in the threat model. At this stage, you need to identify what information or resources you have that could be targeted by an adversary. Do you have financial information? Customer or client information? Personally Identifiable Information of employees? Do you have proprietary information or intellectual property? Do you or others rely on your system's availability or operations? All of these things could be targeted by different adversaries for different reasons, and once you understand what you have you can start to understand your threat profile and which adversaries may target you for what reason.



In many cases, different adversaries target different types of organizations and different types of data for specific reasons. There has been extensive work done in this space, and it is possible to use the different assessments of actors and campaigns to understand what adversaries could potentially target you. In many cases adversaries align to industry verticals, target a specific type of information or in the case of hacktivists or other socially-motivated actors may target based off of events or incidents.

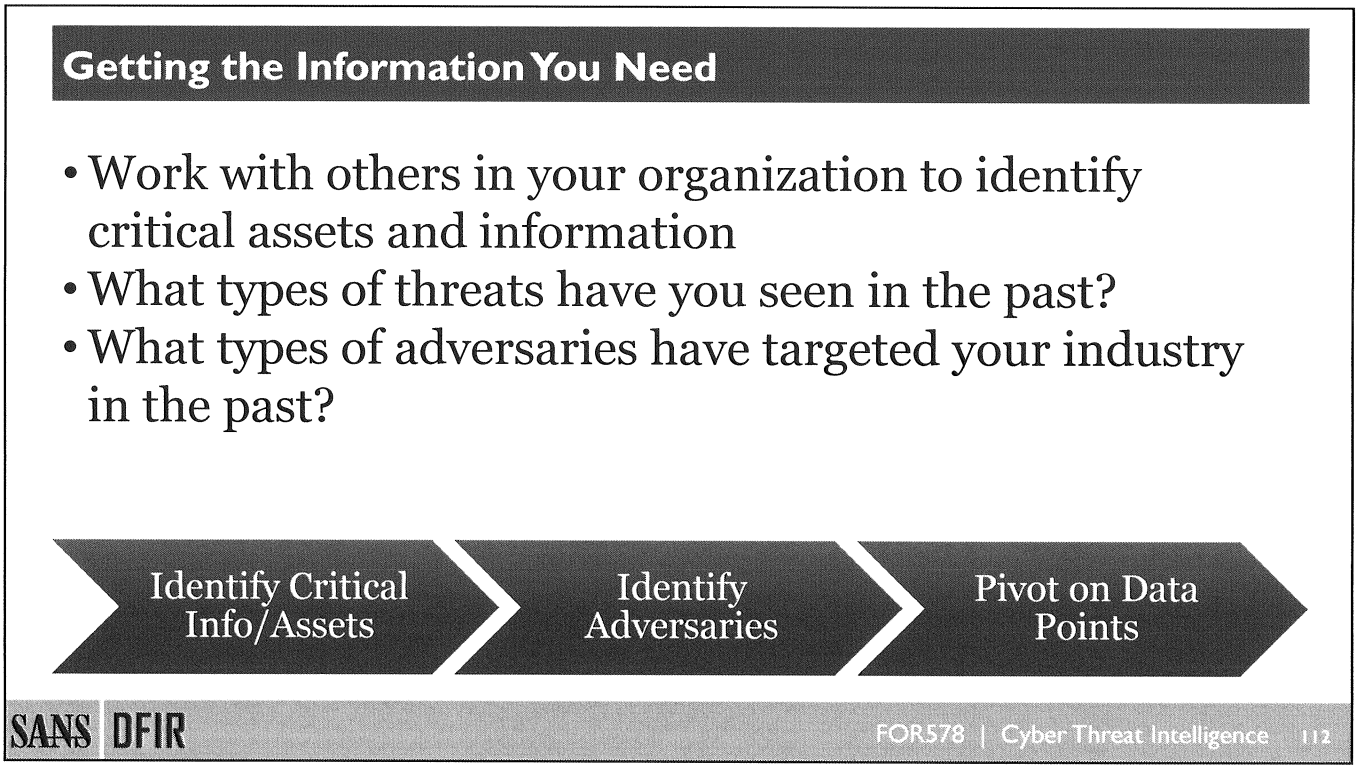
Again, it can be impossible to guarantee that you have captured every threat actor and what information they may target; like we mentioned previously, the attacker has a say as well, but this will serve as a general guideline for what information may be targeted by what actor type.

There are several ways to model details, this is one example of how to capture important details. In these charts, the same organization may be targeted by different actors for different reasons, which are outlined in the first two bullets. The "details" section can include any significant pieces of information about them; however, the more specific and tailored it is to the specific organization the more useful it will be moving forward.



Once you have mapped out a basic threat model of your organization, capturing the information and resources that may be targeted and then the threat actors who may target that data, you can continue to build out the model by pivoting off of several different aspects of your model. One way is to pivot off of the information and resources you have identified. These will become the new "targets" of the target-centric model. You can deep dive into the various types of information within each category, understanding at a more granular level where this information is, what the risk is it if it is exposed, and which actors may be interested in just some of the information in this category but not others.

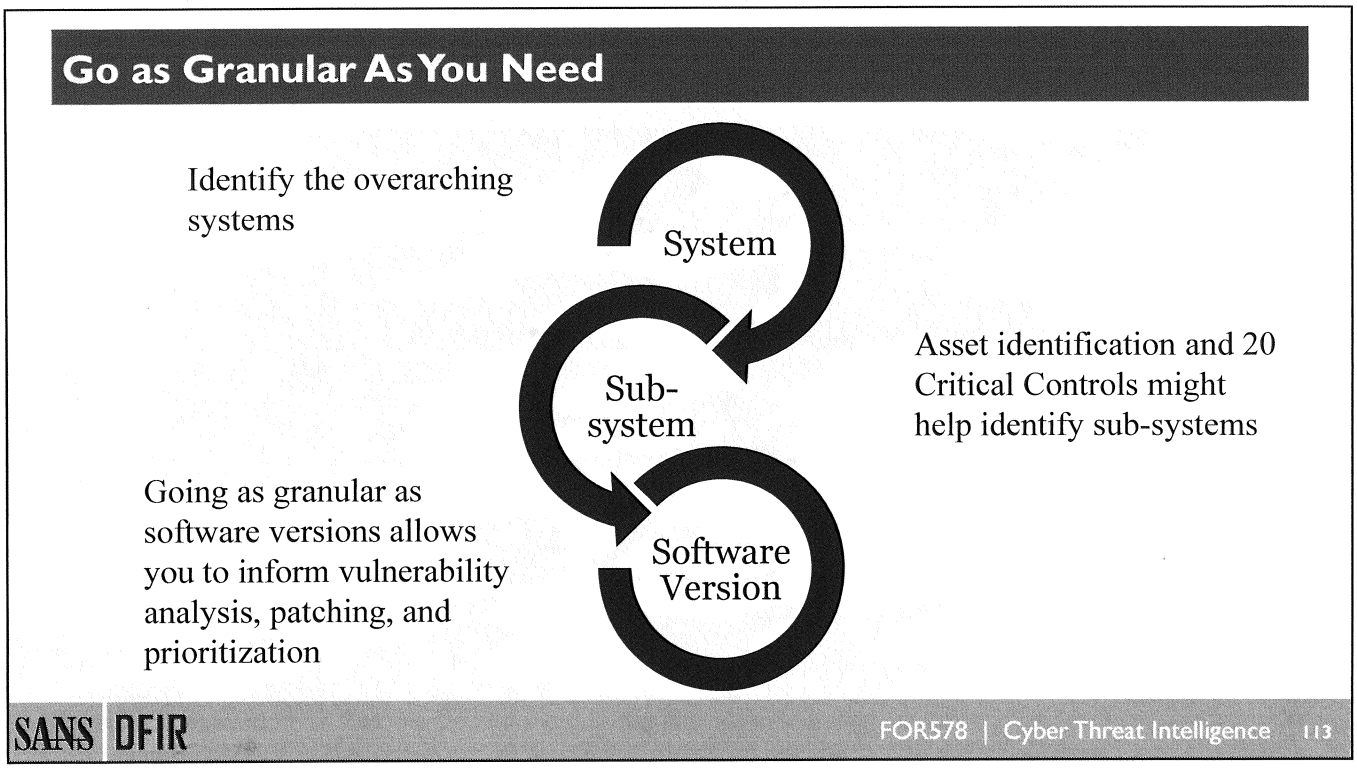
You can also pivot off of the adversaries that you have identified, focusing on the tools they use, their support or operational dependencies, and triggers that may cause them to target your organization. Each of these new categories can be further broken down. It is important to not just identify what you know about each of the new targets, but also what additional information you need, where you can get it, and how you would identify any of the tools or activities that are identified.



One of the key tenants of target-centric modeling is reducing stove-pipes. This means that when you are building out your threat model and identifying the information and resources that an attacker may target, make sure that you are working with others within your organization so that you can get a full picture of what could potentially be targeted. We often tend to think of things from an information security perspective and focus on systems, servers and other technical resources that an attacker may target. Talking to others will bring a new perspective and may reveal additional assets or information that we would not have thought of.

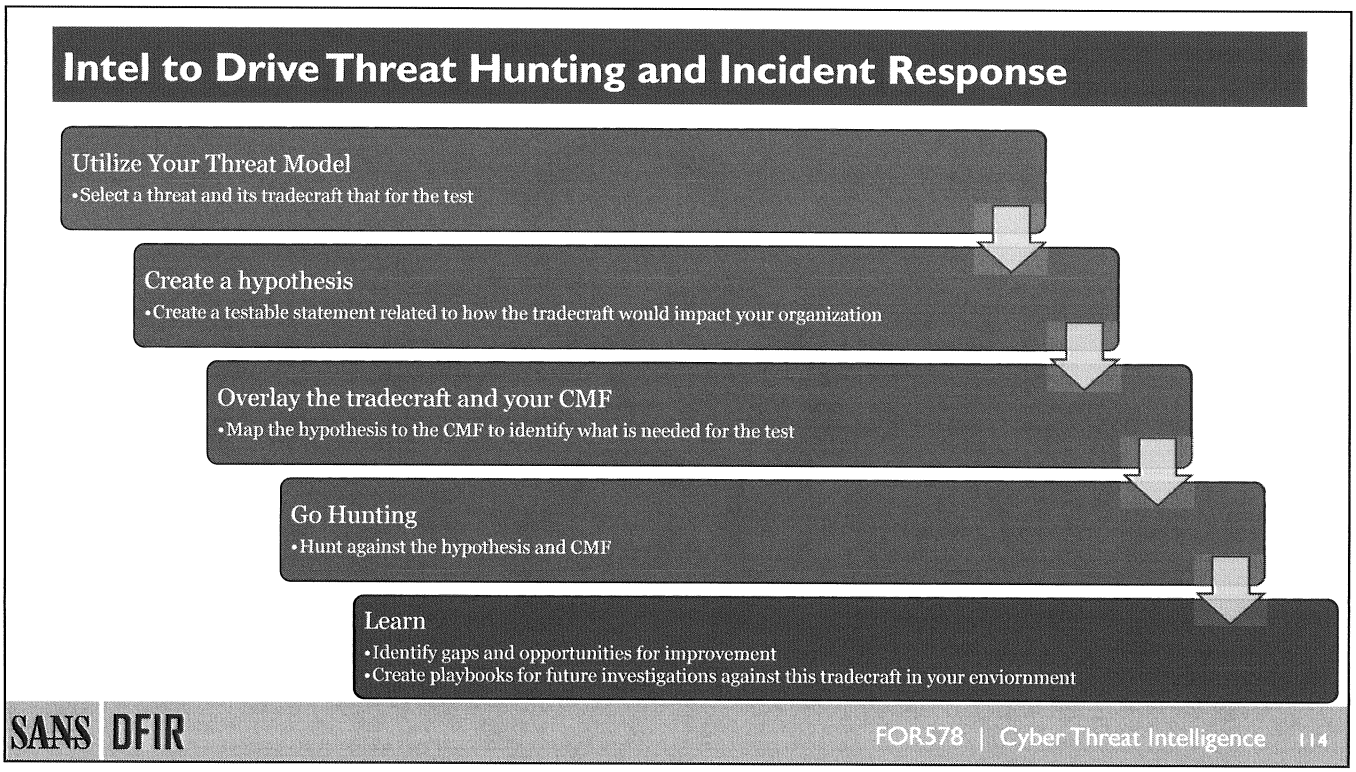
Information or resources that an attacker may target can include systems, information, or personnel. Working with a diverse team to understand everything that an organization has that could be a target for an attacker can reduce the risk of overlooking something because of our own analytic biases.

Once you have identified what information or resources you have that may be targeted, you can start identifying what types of threat actors may target that information. You can begin to identify adversaries by looking first at what types of threats you have seen in the past. Your own threat intelligence will always be the most relevant to you. You do not have to have attribution to a particular actor in order for the information to be useful, it is helpful to simply understand what information they targeted, which can give you an idea of the category they fit into and their motivation.



Go As Granular as You Need

You might find your needs are related to campaigns and threat actors; from there you might be able to satisfy your intelligence requirements. You might find though that you have intelligence requirements to help the vulnerability management group. You could continue to go more granular and identify each major grouping of assets and software versions and have that in a centralized location that you can pull from or have RFIs to the teams that own that information. Software versions and understanding of your environment can make sure that you can prioritize vulnerabilities as important if they are for particularly critical systems or there is a likelihood (or observed activity) that threats you care about are leveraging those vulnerabilities.



Intel to Drive Threat Hunting and Incident Response

Threat hunting serves the purpose of not necessarily finding threats (that would be a bad outcome) but instead on helping to identify gaps in your internal collection and ability to deal with threats. It also is used to help encourage more automation including the types of detection and correlation that are helpful in dealing with threats. In many ways, threat hunting, when done correctly, is working the incident response ahead of the incident and ensuring you will be successful while identifying areas for improvement.

By combining your threat model and your internal collection management framework (CMF) you can guide threat hunting and incident response in your organization as an intelligence analyst. You should select a threat from your threat model and identify key tradecraft. Take that tradecraft and create a hypothesis for your threat hunters where the hypothesis is a testable question or statement relating to how that threat and its tradecraft would compromise your organization. The hunters then map out their process using the CMF and then test the hypothesis. The hunters should also develop playbooks along the way of what an analyst doing the incident response should do in the future. I.e. develop a step by step guide in how to run the investigation while searching for this specific tradecraft against your specific environment.

The VERIS Framework

- The Vocabulary for Event Recording and Incident Sharing (VERIS)
- Captures metrics on events and incidents
- Strategic-level counterpart to indicator sharing
- Most well-known use case is the Verizon Data Breach Investigations Report (DBIR)

The Vocabulary for Event Recording and Incident Sharing (VERIS) is framework that provides a common language for describing security incidents in a structured and repeatable manner. Unlike data formats such as STIX and OpenIOC, VERIS is designed as a set a metrics that allows you to capture entire incidents rather than patterns of observables or behaviors. VERIS can be thought of as the strategic-level counterpart to other indicator sharing formats.

VERIS is used by numerous organizations to capture metrics on their own incidents; however, the most well-known example of VERIS in use is the Verizon Data Breach Investigations Report, or the DBIR, which uses VERIS to capture and analyze data breach information from companies and organizations around the world.

Reference:

http://veriscommunity.net/

Fundamentals of VERIS

- Incident Details
- Four A's
  - Action
  - Asset
  - Actor
  - Attribute

Variable	Value
timeline.incident.year	2014
schema_version	1.3
incident_id	1
security_incident	Confirmed
discovery_method	Unknown
action	Unknown
asset	Unknown
actor	Unknown
attribute	Unknown

VERIS has the potential to be very complex, capturing numerous in-depth details about an event or incident; however, it doesn't take much information to start. At very basic levels, VERIS captures details about the incident such as the date, an incident ID for tracking purposes, whether the incident was confirmed, and how it was discovered. In addition, VERIS captures the four "A's", action, asset, actor, and attribute. These are four data types that are present in every security incident, from the loss of a laptop to a denial of service attack. We are going to do more in-depth on these four aspects in the next slides.

For each data enumeration field within VERIS there are two options, either a yes/no or true/false answer simply identifying the presence of activity in a given field, or you can actually provide details on the field and provide more details about a specific data field.

The actions field is used to answer the question "what actions affected the asset?" It is possible that there is more than one action that occurred during an event, so it is possible that there will be multiple actions per incident or event. The primary actions that can be captured under "actions" are malware, hacking, social, misuse, physical, error, and environmental. Malware covers any type of malicious files or software that is part of an incident, hacking involves the exploitation of a vulnerability, social includes a social engineering actions including phishing or call center hoaxes. Misuse most often involves someone who has been given access to a system who abuses or misuses their access. Physical involves gaining physical access to a system, such as through a USB drive. Errors include things such as problems in software or configurations that resulted in an incident. Environmental includes things such as storms or natural disasters.

Just like we mentioned before, all of these can include a simple yes or no answer or they can have additional enumerations such as variety, vector, or vulnerability.

The asset category identifies the asset or assets that were involved in an incident or event. In most incidents, there was not a single asset that was affected, and VERIS allows you to capture data on all of the various assets that may have been involved. It can capture a variety of information about an asset, including its variety – server, desktop, laptop, appliance, etc. It can also capture information on the owner of the asset, such as whether it was owned by the company, by an employee, a contractor, or a customer. It also captures information on who managed the asset, namely whether it was internally managed by the organization or managed by someone else, either an external party such as a hosting provider or an employee in the case of Bring Your Own Device policies. There are additional asset enumerations that deal with hosted assets or assets in the cloud.

In VERIS, an actor is an individual or an entity that contributes to an incident or an event. They are not always malicious, an actor could be an employee who loses a laptop or a contractor who accidentally misconfigures a firewall, resulting in an incident. VERIS breaks the actor categories down into Internal, External, Partner, or Unknown. At the very basic level, each of these types could be answered with a yes or no. For example: Is it an internal actor? No. Is it an external actor? Yes. Is it a partner? No. The next level would be to add detail using VERIS's enumerations. One enumeration that crosses all four categories is motivation and includes things such as espionage, financial, ideology, or convenience, which is seen in a lot of situations where the event occurs as a result of a mistake or misconfiguration. Another enumeration is variety, and this also includes enumerations for internal, external, and partners such as auditor, competitor, end-user, etc.

Attributes answer the question "how was this asset affected?" It follows the traditional CIA triad, Confidentiality, Integrity, and Availability. It needs to be answered as best as possible for each asset that was affected, at the basic level it can be a yes or no answer, or unknown in many cases, but it can also include details on how the data was affected, what type of data was impacted, or in the case of availability how and for how long the system's availability was compromised. This will help identify the impact that the threat had on the asset and can contribute to things such as loss analysis moving forward.

If you are able to capture the various information on incidents and events in your environment then you will have a rich resource to tap into when you are trying to understand trends and threats to your own environment. Using VERIS will also enable you to share more strategic-level information with peers and partners, and allow you to contribute to large-scale reports such as the DBIR. It will also enable you to produce your own internal reports on the threats that are facing you, which will allow you to provide greater awareness of your threat profile.

Reference:

ttp://veriscommunity.net/howto.html

https://www.youtube.com/watch?v=k9OFoSdyLsg

Using VERIS to Track Threats

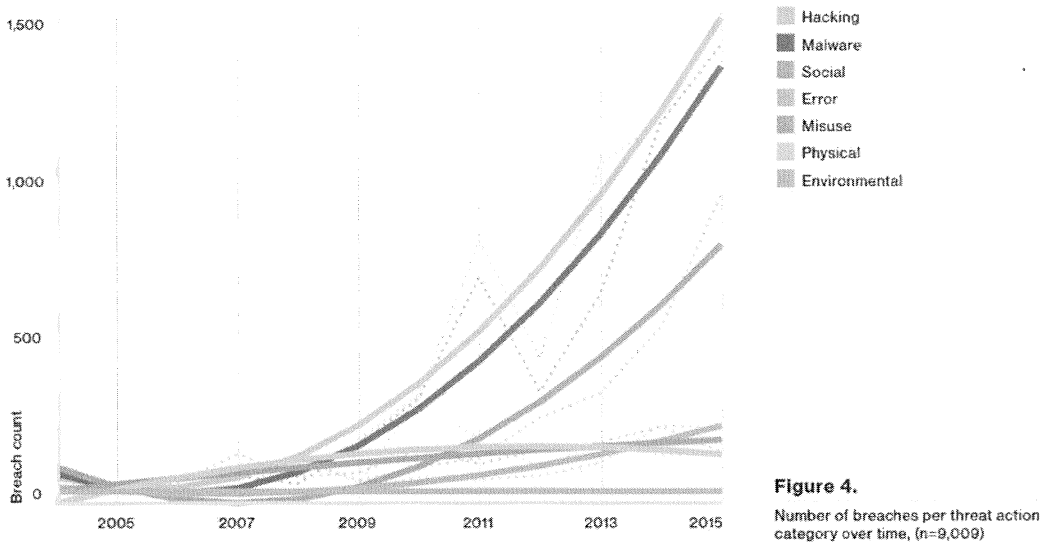


Figure 4.
Number of breaches per threat action category over time, (n=9,009)

One of the benefits of using a framework like VERIS to capture strategic level data is that it allows you to track and conduct trend analysis on threats, which in turn helps to update threat profiles. A specific benefit of VERIS is that you can also track your internal data against the external data that is presented in the Verizon DBIR to help understand how you compare to others.

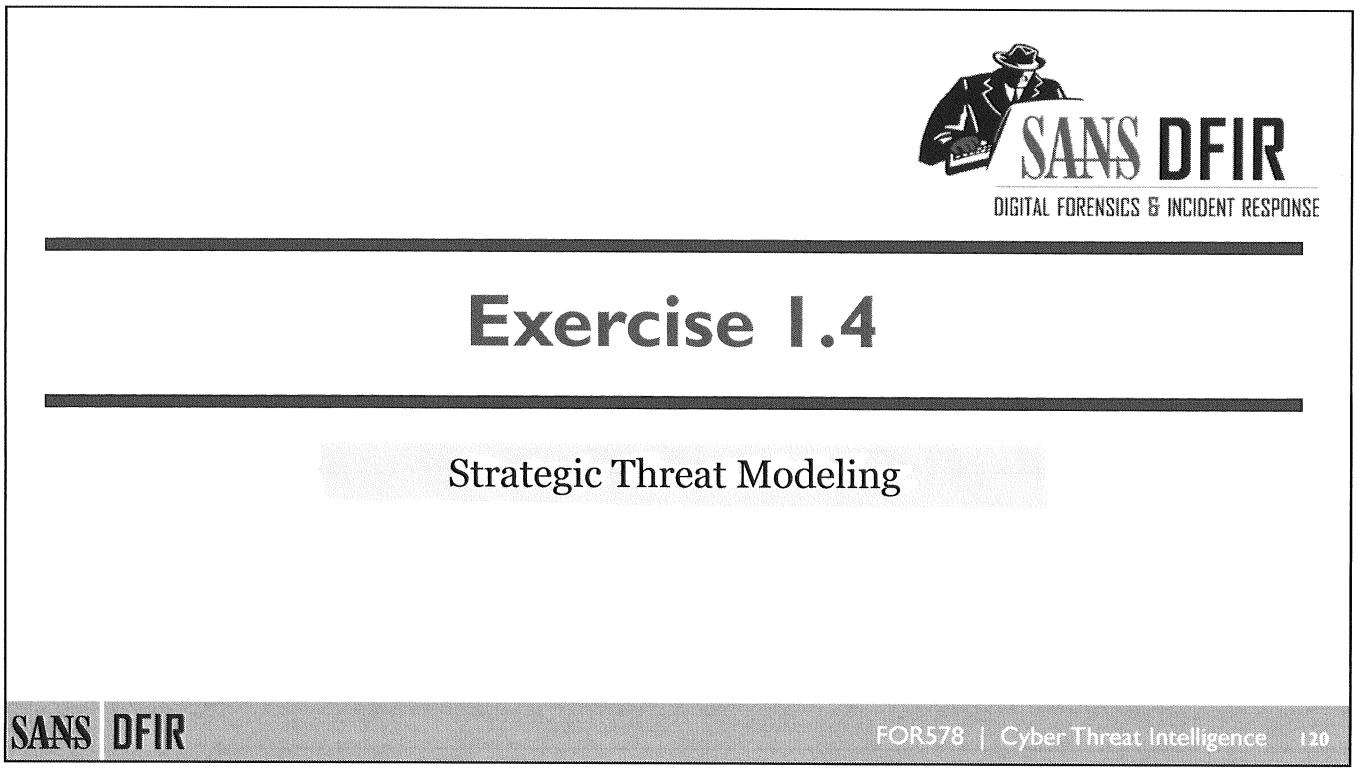
Image reference:

2015 Verizon DBIR

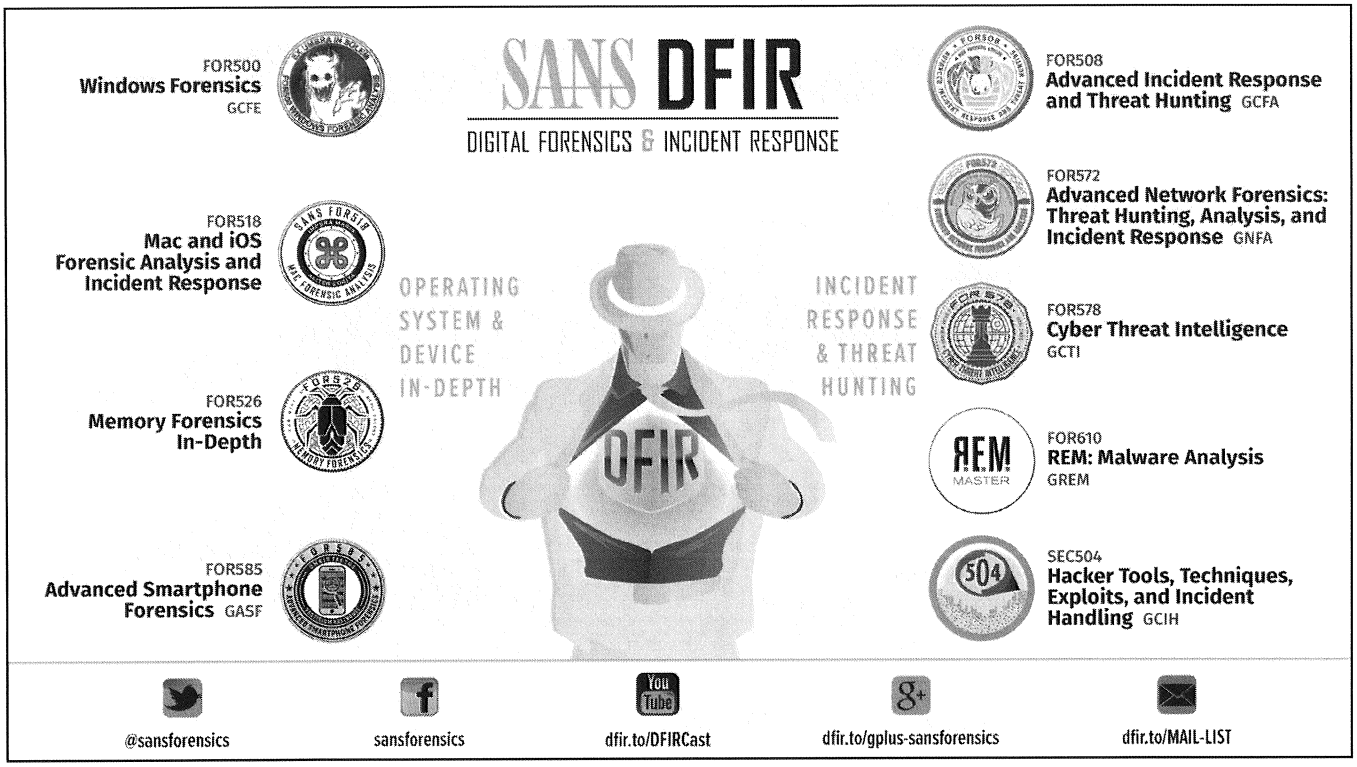
Exercise 1.4: Positioning for the Future

- Acme Power is concerned about the growing threat to the electric power industry following the 2015 and 2016 cyber attacks on the Ukraine power grid
- They have requested your team to develop a threat model so that they can better understand their threat landscape and articulate questions for IRs

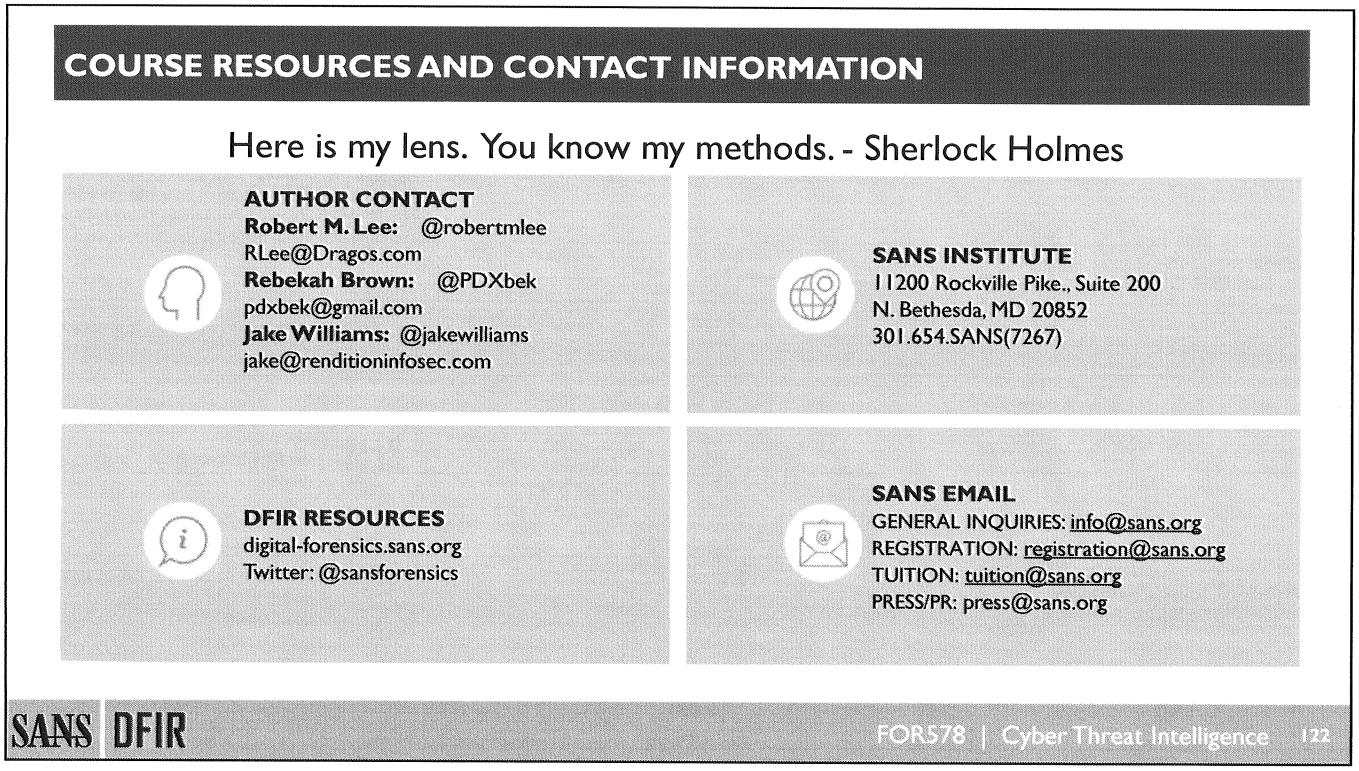
This page intentionally left blank.



Please refer to your workbook for Exercise 1.4.



This page intentionally left blank.



This page intentionally left blank.

"As usual, SANS courses pay for themselves by Day 2. By Day 3, you are itching to get back to the office to use what you've learned."
Ken Evans, Hewlett Packard Enterprise - Digital Investigation Services

SANS Programs
sans.org/programs

GIAC Certifications
Graduate Degree Programs
NetWars & CyberCity Ranges
Cyber Guardian
Security Awareness Training
CyberTalent Management
Group/Enterprise Purchase Arrangements
DoDD 8140
Community of Interest for NetSec
Cybersecurity Innovation Awards

Search SANSInstitute

SANS Free Resources
sans.org/security-resources

- E-Newsletters
  NewsBites: Bi-weekly digest of top news
  OUCH!: Monthly security awareness newsletter
  @RISK: Weekly summary of threats & mitigations
- Internet Storm Center
- CIS Critical Security Controls
- Blogs
- Security Posters
- Webcasts
- InfoSec Reading Room
- Top 25 Software Errors
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- 20 Coolest Careers
- Security Glossary

SANS Institute
8120 Woodmont Avenue | Suite 310
Bethesda, MD 20814
301.654.SANS(7267)
info@sans.org