Study Guide

Advanced Cyber Threat Intelligence

Created By: David Davor, Teaching Assistant

Instructor: Alyssa Berriche

Module 1: Introduction

Lesson 1.1: Course Introduction

Skills Learned From This Lesson: Course prerequisites, course structure, Course overview, Course objective.

Who should take this course

- Security Practitioners
- SOC Analysts
- Threat Intelligence Analysts
- Threat Hunters
- Incident Response Teams
- Digital Forensic and Malware Analysts

In general, cybersecurity professionals who want to enrich their skills and knowledge in the field of Cyber Threat Intelligence.

Course Prerequisites

- Networking essentials
- Security terminologies (Firewall, SIEM, IPS, ….)
- Complete the “Introduction to Cyber Threat Intelligence” course
- Basic OSINT knowledge
- Basic Understanding of the Cyber Kill Chain
- Basic understanding of Data Analysis
- Willingness to learn something new

Course Objective

The following will be learnt in this course;

- The different collection sources
- The importance of data collection in Cyber Threat Intelligence program
- The processing and management of the collected evidence/data/feeds
- Examples of Threat Intelligence Platforms
- Methodologies used for intrusion analysis
- Methodologies used for campaign analysis
- One of the challenges facing Threat Intelligence Analysis: biases
- Dissemination of Threat intelligence based on the intended audience

Course Structure

- **Advanced Cyber Threat Intelligence**
  - ➔ Presentations/Videos
  - ➔ Assessments
  - ➔ Supplemental Materials

Course Overview

- Module 1: Data collection
  - ➔ Introduction to data collection
  - ➔ Internal data acquisition
  - ➔ External data sources/ Feeds types
  - ➔ Leveraging OSINT

- Module 2: Data management and processing
  - ➔ Introduction to processing
  - ➔ CTI common standards
  - ➔ Integration and storage
  - ➔ Threat Intelligence Platforms (TIP)

- Module 3: Analysis
  - ➔ Introduction to analysis phase
  - ➔ Analysis of competing hypotheses
  - ➔ Cyber Kill Chain and Diamond Model
  - ➔ Cyber Kill Chain and course of Actions

- Module 4: Campaign analysis
  - ➔ Defining campaigns
  - ➔ Heatmap analysis
  - ➔ Visual analysis
  - ➔ MITRE ATTACK & MITRE threat group tracker
  - ➔ Recommendations for campaign naming

- Module 5: Attribution
  - ➔ Introduction to attribution
  - ➔ Cognitive bias
  - ➔ Logical errors
  - ➔ How to manage biases
  - ➔ Nation-state biases

- Module 6: Dissemination & Feedback
  - ➔ Introduction to dissemination
  - ➔ Dissemination: Tactical
  - ➔ Dissemination: Operational
  - ➔ Dissemination: Strategic

Lesson 1.2: Introduction to the Intelligence Lifecycle

Skills Learned From This Lesson: Data, Information,Intelligence.

Data and Intelligence (Relationship)

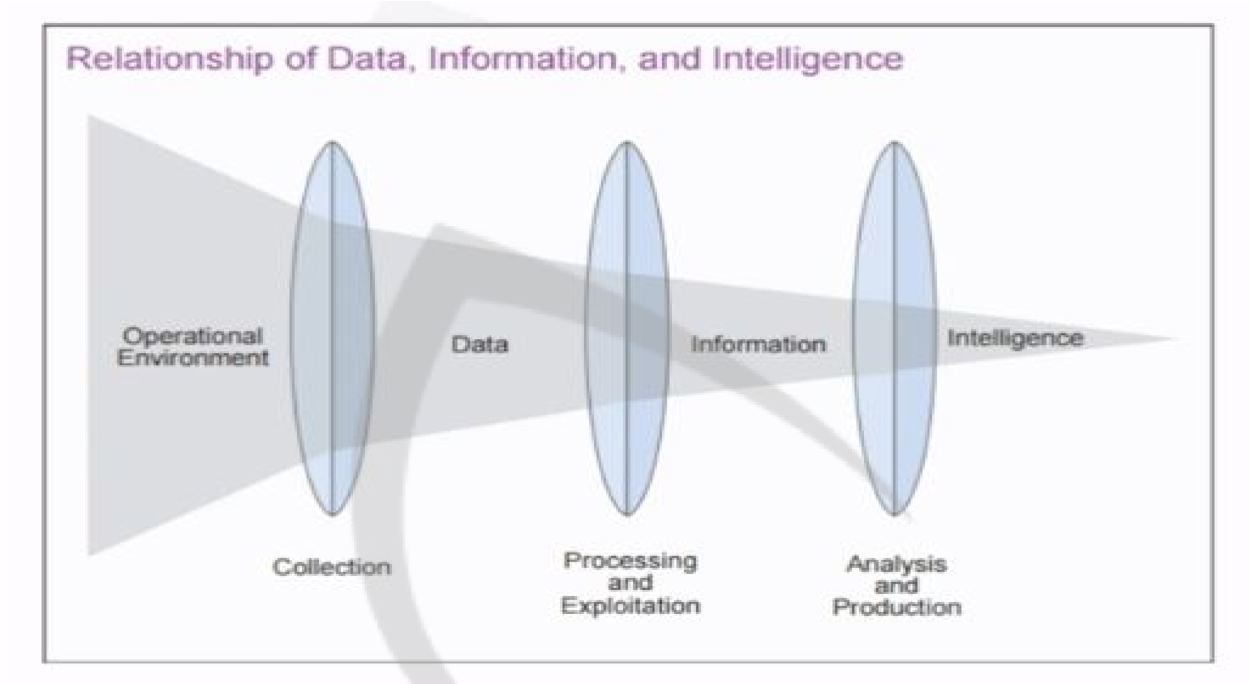
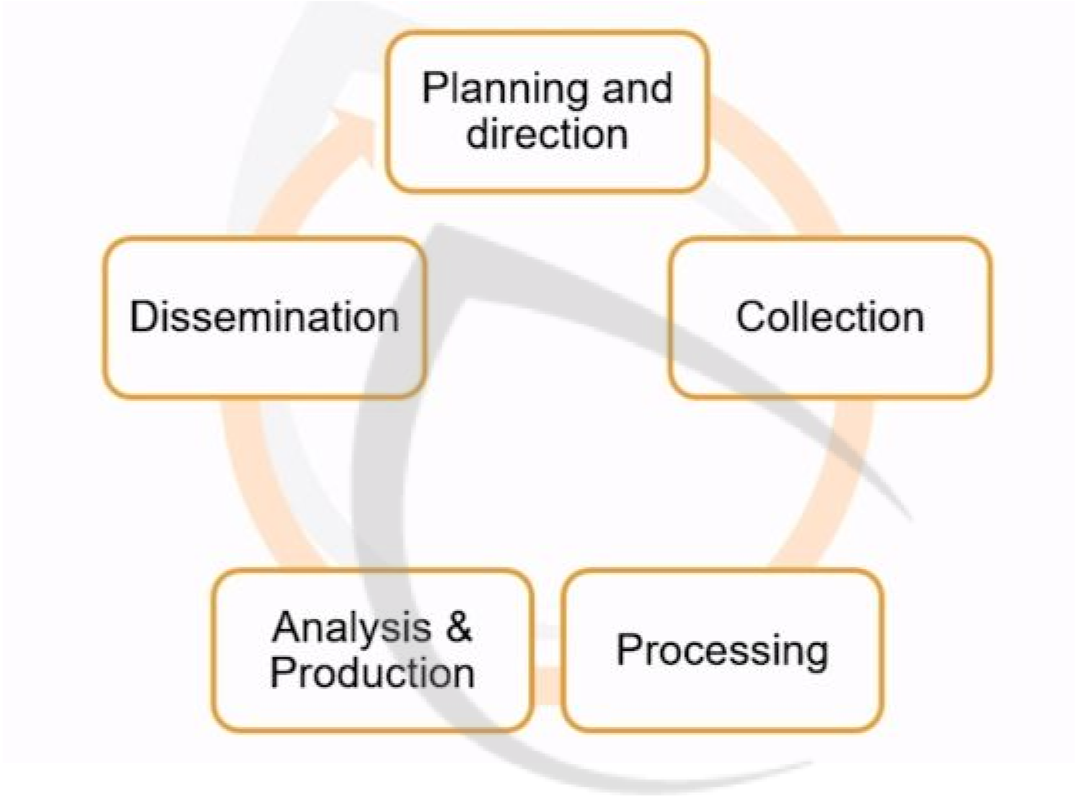


Image taken from the U.S Department of Defence's "Joint Publication 2.0: Joint Intelligence" report.

What is the Intelligence Lifecycle

- According to the Federation of American Scientist*, "The Intelligence Cycle is the process of developing raw information into finished intelligence for policy makers to use in decision making and action."*
- It is also called the Intelligence Process by the U.S Department of Defence (DoD) and the uniformed services

Steps of the Intelligence cycle



- **Planning and direction**
  - ➔ Involves setting goals for the threat intelligence program
  - ➔ It is the beginning and the end of the cycle
    - ➢ Beginning because it consists of defining the requirements for the collection
    - ➢ End because finished intelligence, will support decision makers to generate new requirements.
  - ➔ Also includes setting priorities.

- **Collection**
  - ➔ Gathering of “data” to produce intelligence
  - ➔ Data gathering can occur from a variety of sources

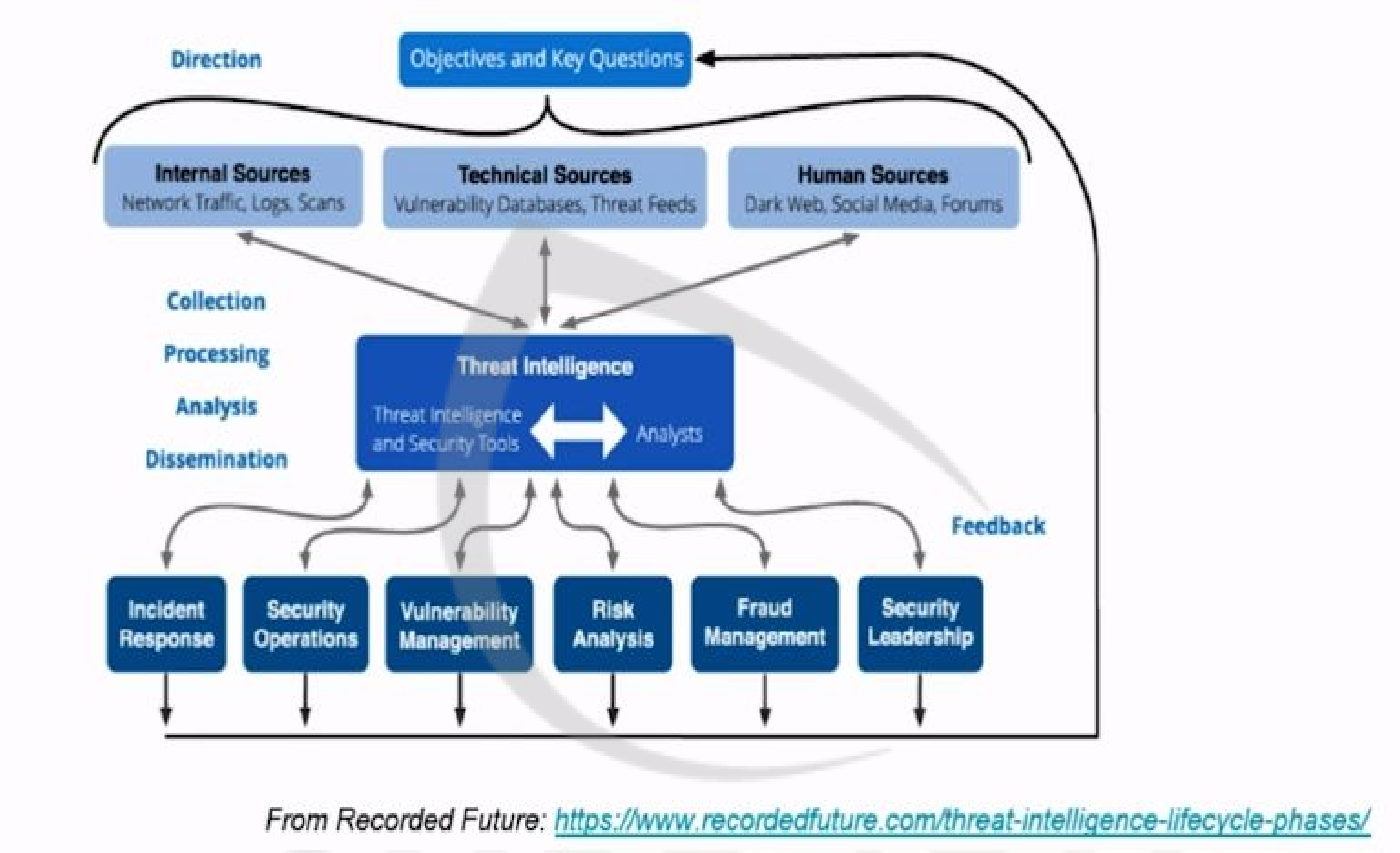
- ➔ Logs from internal IT infrastructure
- ➔ Threat data feeds from the industries
- ➔ Publicly available information

- **Processing**
  - ➔ Processing is the transformation of collected data into a format usable by the organization
  - ➔ In some cases, collecting data from different sources requires different ways of processing to get a normalized set of information**.**
  - ➔ Technically, processing will require extracting IOCs (Indicators of Compromise) from threat reports or emails or threat feeds.

- **Analysis and Production**
  - ➔ Involves the evaluation and enrichment of the processed information to understand it
  - ➔ This phase involves, thinking about the information collected and applying different lenses to derive meaning.
  - ➔ It draws conclusions from the available information and providing assessments in the form of advice and recommendations.

- **Dissemination**
  - ➔ Dissemination involves getting the finished intelligence and assessment distributed to the appropriate audience
  - ➔ It includes the frequency in providing this output

Why are we introducing the Intelligence Cycle?



From Recorded Future: https://www.recordedfuture.com/threat-intelligence-lifecycle-phases/

Module 2: Collection

Lesson 2.1: Introduction to Data Collection

Skills Learned From This Lesson: Data collection, Sources, Recommendations

What is data collection in CTI context?

Collection is the process of gathering data and information to address intelligence requirements and objectives that were defined in the planning and direction.

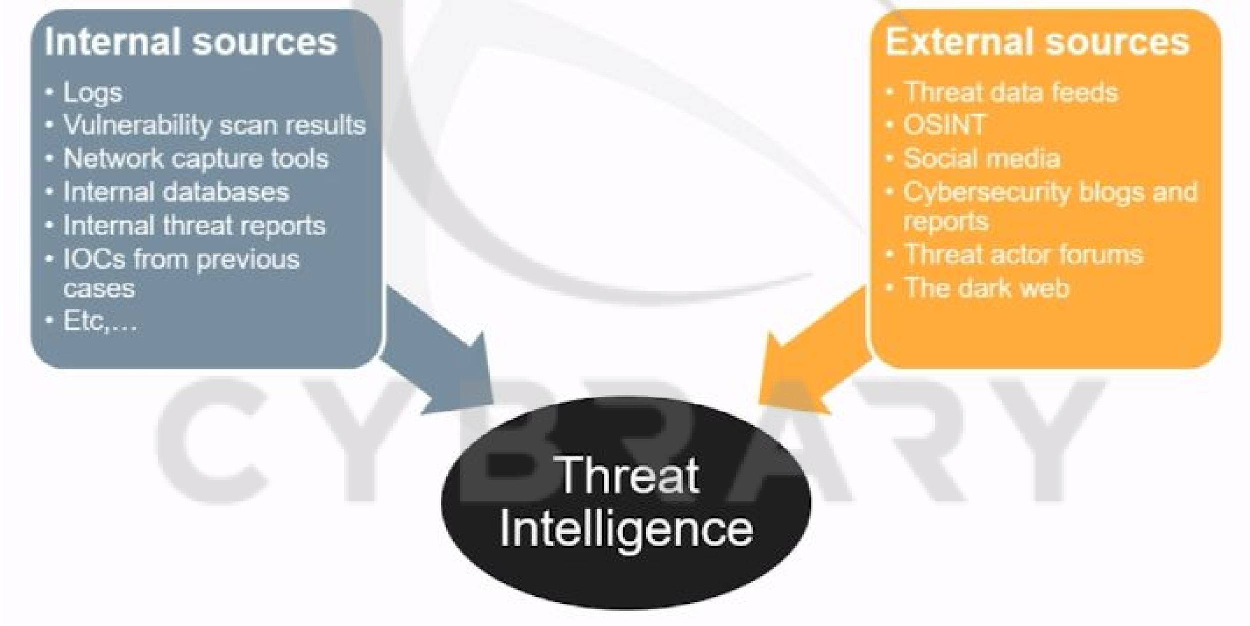
The data collected can be:

- Finished intelligence (intelligence reports from vendors)
- Raw data (firewall logs)
- Dump (paste websites)

Recommendations about data collection

- Collecting data from one end is not sufficient
- Quality matters as much as quantity
- Don't waste much time on collection. Automation may help

Types of collection sources.



Internal sources

- Logs
- Vulnerability scan results
- Network capture tools
- Internal databases
- Internal threat reports
- IOCs from previous cases
- Etc,...

External sources

- Threat data feeds
- OSINT
- Social media
- Cybersecurity blogs and reports
- Threat actor forums
- The dark web

Threat Intelligence

Lesson 2.2: Internal Data Acquisition

Skills Learned From This Lesson: Network data source, Endpoint data source, Threat intelligence sources.

Internal data sources

- There are literally hundreds of possible types of data sources around your environment
- By leveraging threat data data from your own network, you can detect and stop threats
- Understanding all the log types and sources available for selection can be pretty difficult
- It is practically impossible to cover every source of logs, this is why it needed to identify what may be more valuable

What data are we collecting internally?

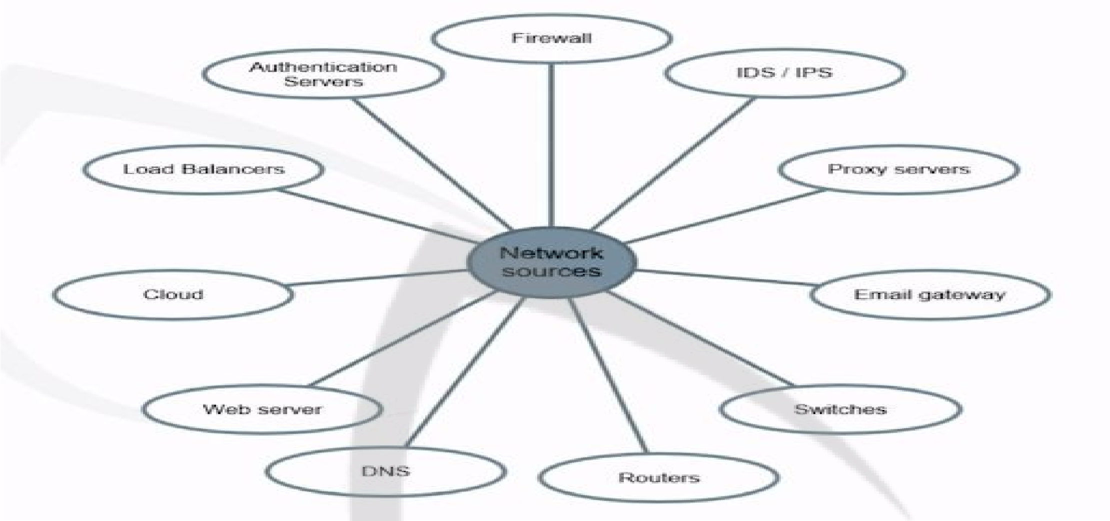
- Host/ Endpoint data
- Network data
- Finished intelligence

Endpoint data

- Process execution metadata: processes running on endpoints
- Registry access data: registry objects, including key and value metadata on windows-based endpoints
- File data: includes dates, size, type and location
-
- Network data: network connections

Network data

It involves collecting data from network and security devices available in your IT environment



Threat Intelligence data

You can leverage intelligence from your own network like:

- Threat intelligence reports
- Incident response reports
- Indicators of compromise stored in your threat intelligence platform
- Vulnerability scan reports
- Vulnerabilities exploited
- Forensic reports
- Malware analysis reports

<u>Lesson 2.3</u>: External Data Sources

Skills Learned From This Lesson: Data sources, External sources, Right approach

What are the external data sources?

- Security reports from vendors or cyber security experts
- Security blogs and articles about trending threats

- Malware analysis results
- Indicators of compromise (IOCs)
- Open source intelligence
- Advisories about new vulnerabilities
- Social media feeds
- Yara rules
- IDS alerts
- Dumps of credentials

External data sources

- External sources can be pretty varied with various degrees of trustworthiness
- These sources can provide indicators in:
    - ➔ Structured data report formats such as STIX, CSV, JSON, XML, etc
    - ➔ Unstructured reports such as PDF and word documents, emails from sharing groups etc.

What's the right approach on selecting your sources

- An assessment of what is going to have the greatest impact and the likelihood of that against your organization has to be done
    - ➔ For example, all organizations are aware that a ransomware that gets in the right spot can shut the business for weeks or permanently in some cases, so must be considered a priority.
    - ➔ No need to fully focus on a trendy APT that is not even interested in your organization.
    - ➔ During Wannacry case: Patches were available and advisories were published prior to the attack but it wasn't prioritized

Effective threat intelligence role is to keep defenders informed of common threats by providing up-to-date IOCs

Types of external data sources

- Public data source
- Community data source
- Private or commercial data source

Lesson 2.4: Private Data Sources Part 1

Skills Learned From This Lesson: Data sources, Threat intelligence feeds

Private data sources

Private or commercial data sources provide:

- Vetted and enriched intelligence
- Up-to-date intelligence
- Some vendors can send relevant and customed intelligence to their customers
    - ➔ Relevance matters
- Some vendors are more focused on rule based engines while others add human analysis capabilities.

Narrative-based reports

- Finished intelligence
    - ➔ Multiple organizations are using threat intelligence from finalized reports
    - ➔ They describe a series of events related to an intrusion or incident
- Threat reports include:
    - ➔ TTPs
    - ➔ Campaign investigations
    - ➔ Attribution
    - ➔ ATT & K mapping

CTI teams need to ensure they are properly staffed.

Advantages:

- Reports are usually rich in data and full of indicators
- They give full picture
- They sometimes include recommendations

Disadvantages

- Takes considerable time to produce
- Difficult to make reports actionable
- Require custom tools to automate processing

Threat Intelligence Feeds

- Threat intelligence feeds are real-time and continuous streams of data
- Feeds are usually made up of simple indicators or artifacts
- For example a feed might represent a stream of information on:
    - ➔ Malware hashes
    - ➔ Suspicious domains
    - ➔ IP associated with malicious activity
- Feeds provide an easy way to get a quick, real-time look at the external threat landscape
- Cyber threat intelligence feeds get their data from different sources
- Paid feeds should generally produce more unique data, like data gathered from closed sources.
- For feeds to be actionable, they generally need to be integrated into SIEM
- Feeds can be aggregated in one solution to add context to evidence
- Feeds can be used to blacklist communications and requests originating from malicious sources

Advantages

- Feeds are actionable and easy to integrate
- Up-to-date intelligence
- Vetted information

Disadvantages

- Lack of context compared to reports
- Big volume of data to ingest
- Sometimes lack relevance.

Lesson 2.5: Private Data Sources Part 2

Skills Learned From This Lesson: Data sources, Threat intelligence feeds

Threat intelligence platforms

- A piece of software, or provider's portal
- Organizes one or more feeds into a single stream of threat intelligence
- Can be used to get alerts and manipulate data.

Most platforms offer a set of benefits:

- Combines feeds into a single location
- Receives alerts in real time
- Normalizes feed data
- Integrates with SIEM, firewall logs etc.
- Creates reports
- Might include a sandbox (optional)

Advantages

- Indicators with context, and actionable
- Useful for enrichment
- Aggregate multiple feeds and sometimes finished intelligence
- Integrates with SIEM solutions

Disadvantages

- Expensive especially if they include premium feeds

Lesson 2.6: Community Data Sources

Skills Learned From This Lesson: Data sources, ISACs, ISAOs

Intelligence sharing communities were created to make best practices and cyber threat information more accessible to companies so organizations are no longer alone in this hostile environment

ISACs: History

- Information Sharing and AnalysisCenters (ISACs) were first established in the US in 1998.
- Created to address US' critical infrastructure vulnerabilities and facilitated the sharing of actionable cybersecurity intelligence among trusted organizations within an industry and between sectors.
- Many ISACs are well resourced, come with membership fees and have infrastructure and full-fledged security operations centers for monitoring threats on a global scale
- The National Council of ISACs currently lists 21 member ISACs including those for the financial, automotive, energy, aviation, communication and defense industrial base sectors.

ISACs: Types

- There are three common types ISACs
    - ➔ Sector-based
    - ➔ Country-based
    - ➔ Internation

Why join ISACs

Services provided by ISACs include:

- Risk mitigation
- Rapid response
- Analysis on relevant threats, vulnerabilities, and incidents

- Training
- Curated reporting

ISAOs: history

- Information Sharing and Analysis Organizations (ISAOs) are the results of a White House directive to promote voluntary cyber threat information sharing within industry sectors.

What is an ISAO?

- A group created to gather, analyze, and disseminate cyber threat information.
- Offer a more flexible approach to self-organized information sharing activities amongst communities of interest.
- The ISAO standard organization currently lists more than 70 groups that it describes as being engaged in some level of information sharing activity.

Lesson 2.7: Public Data Sources Part 1

Skills Learned From This Lesson: Data sources, Public feeds, Feed aggregators.

Public Threat intelligence Sources

- Are available with no cost
- Public data collection sources include: threat bulletins, feeds and platforms
- Huge databases are available and concern many types of threats.

Issues with public intelligence sources

- It has a low level of trustworthiness
  - Indicators are rarely curated
  - Generates noise
- Lack of context is another problem
- Some indicators may be mentioned in lists involved with malicious activities without fully explaining their rules

- Keeping outdated data for years
- Association with malicious activity may change as time goes by

Examples of public feeds

- Cybercrime tracker
- URL haus
- Ransomware tracker
- Openphish
- I-Blocklist
- Cyber cure

Examples of Feed Aggregator:

- LIMO
- HAIL A TAXII

Lesson 2.8: Public Data Sources Part 2

Skills Learned From This Lesson: Data sources, TIPs

Threat Intelligence Platforms (TIPs)

Lesson 2.9: Leveraging OSINT Part 1

Skills Learned From This Lesson: OSINT, Tools, Framework

OSINT Definition

Open-source intelligence, mostly called OSINT is defined by both the U.S. Director of National Intelligence and the U.S. Department of Defense (DoD) as:

"*Produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement"*

Advantages of OSINT

- Has unlimited potential in any topic
- Relatively low cost
- Generally up to date
- Can be shared with anyone.

Disadvantages

- It could be disinformation or simply inaccurate

Usage of OSINT

- Threat actors use open source intelligence tools and techniques to identify potential targets and exploit weaknesses in target networks
- OSINT provide information about the IT systems, networks, and individuals working with these organizations.
- Can be used by CTI teams to:
    - ➔ Identify your exposed attack surface

- ➔ Collect information about your adversaries

Identifying your attack surface using OSINT

- Public IP ranges and open ports
- Company domains and subdomains
- Technologies used in your websites
- Employee emails and phone numbers
- Exposed servers or databases
- Public documents
- Public source code
- Social media

Knowing your adversaries using OSINT

- Adversaries leave their evidence that you can collect to create a context and help decision making
- Monitoring social media, reddit forums.

OSINT Tools and Framework

- OSINT framework
- SHODAN
- Cencys
- Binary edge

Lesson 2.10: Leveraging OSINT Part 2

Skills Learned From This Lesson: OSINT, google dorts, Account verification

Accounts / Email verification

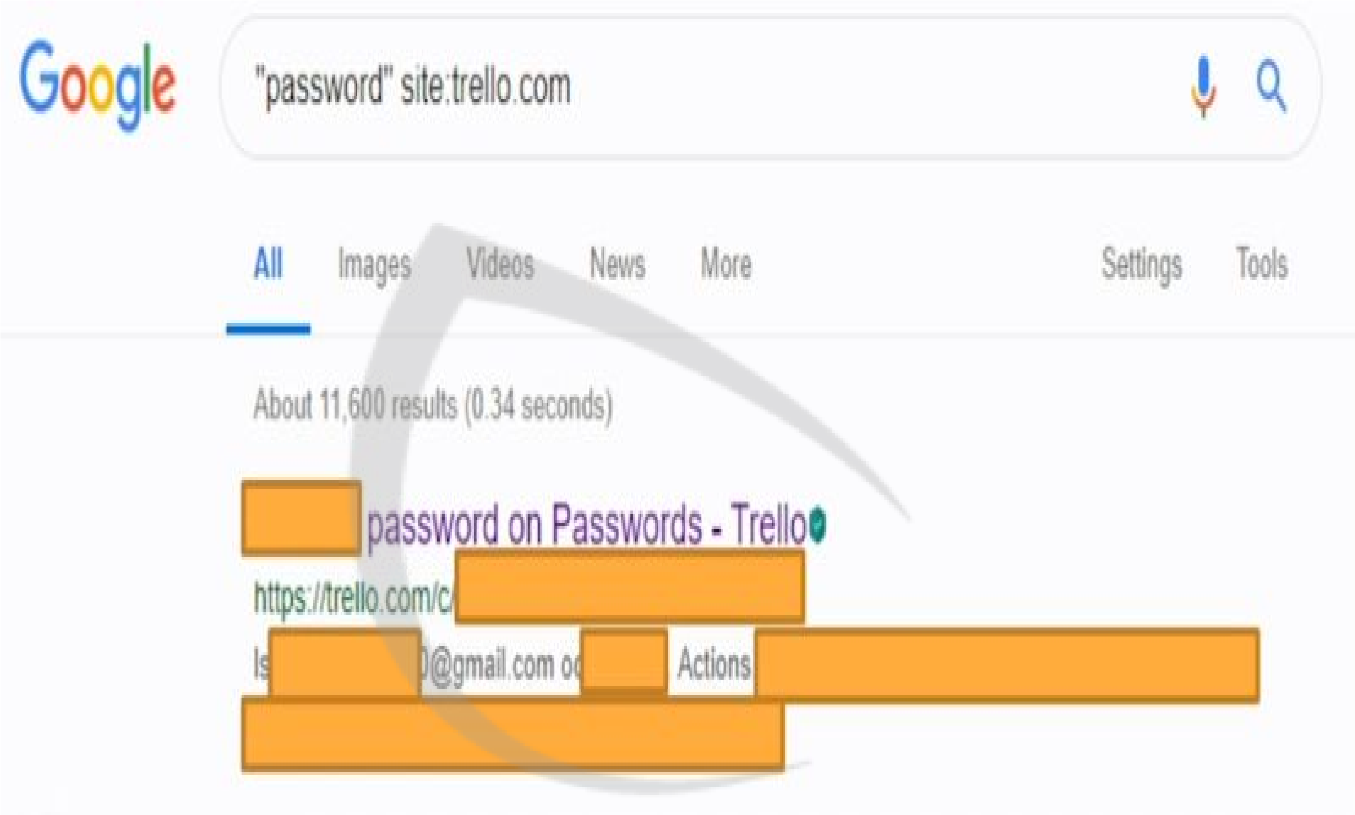
The following tools can be used to verify if a mail has been compromised.

Google dorks

- Are queries that use advanced search operators to find information that is not readily available on a website
- Example:
  - <searchterm> site:example.com, filetype:pdf
  - List of google dorks can be found in the link below https://gbhackers.com/latest-google-dorks-list/

Example:

- *We are going to search for the term "password" within a website. Example taken from TRELLO which is a project management platform*
- ***"Password" site:trello.com***



"password" site:trello.com

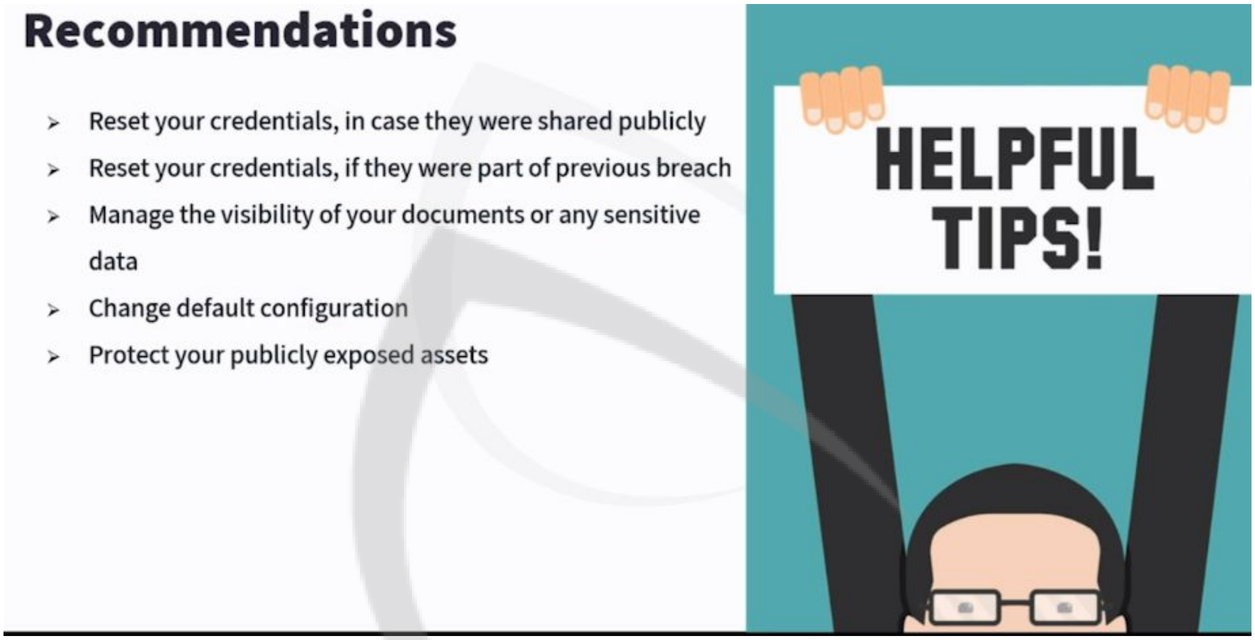
About 11,600 results (0.34 seconds)

[redacted] password on Passwords - Trello

https://trello.com/c/[redacted]

Is[redacted]@gmail.com o[redacted] Actions [redacted]

[redacted]



Recommendations

- Reset your credentials, in case they were shared publicly
- Reset your credentials, if they were part of previous breach
- Manage the visibility of your documents or any sensitive data
- Change default configuration
- Protect your publicly exposed assets

HELPFUL
TIPS!

Module 3: Data Management and Processing

Lesson 3.1: Introduction to Data Processing

Skills Learned From This Lesson: Data processing, Stages, Approaches.

What is data processing

- Data processing is the conversion of data into usable and desired format. Data can be processed through automation or manual (relying on humans)
- Different collection methods often required different means of processing
- The time consumed in obtaining the desired result is dependent on the operations and the nature of the output required.

Approaches of automated processing

The most common approaches today include:

- Identification based on basic patterns
- Statistical or probability algorithms
- Machine learning algorithms
- Natural language processing of human produced text

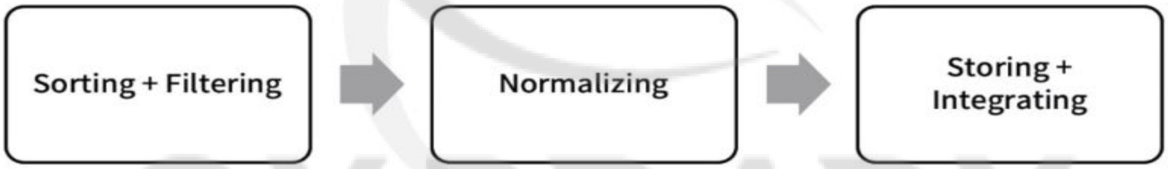
Limitation:

- No total replacement of the human analyst

Human based approach

- Manual method of data processing
- Some types of collected data (eg finishes reports) are difficult to process using automated tools
- Analysts are able to go beyond what any fully automated system can do today.

Stages of processing



What makes processing important

- Dealing with non-processed data is time consuming and sometimes difficult or even impossible for analysts to correlate events and make assessment only based on raw data.

<u>Lesson 3.2</u>: Common CTI Standards Part 1

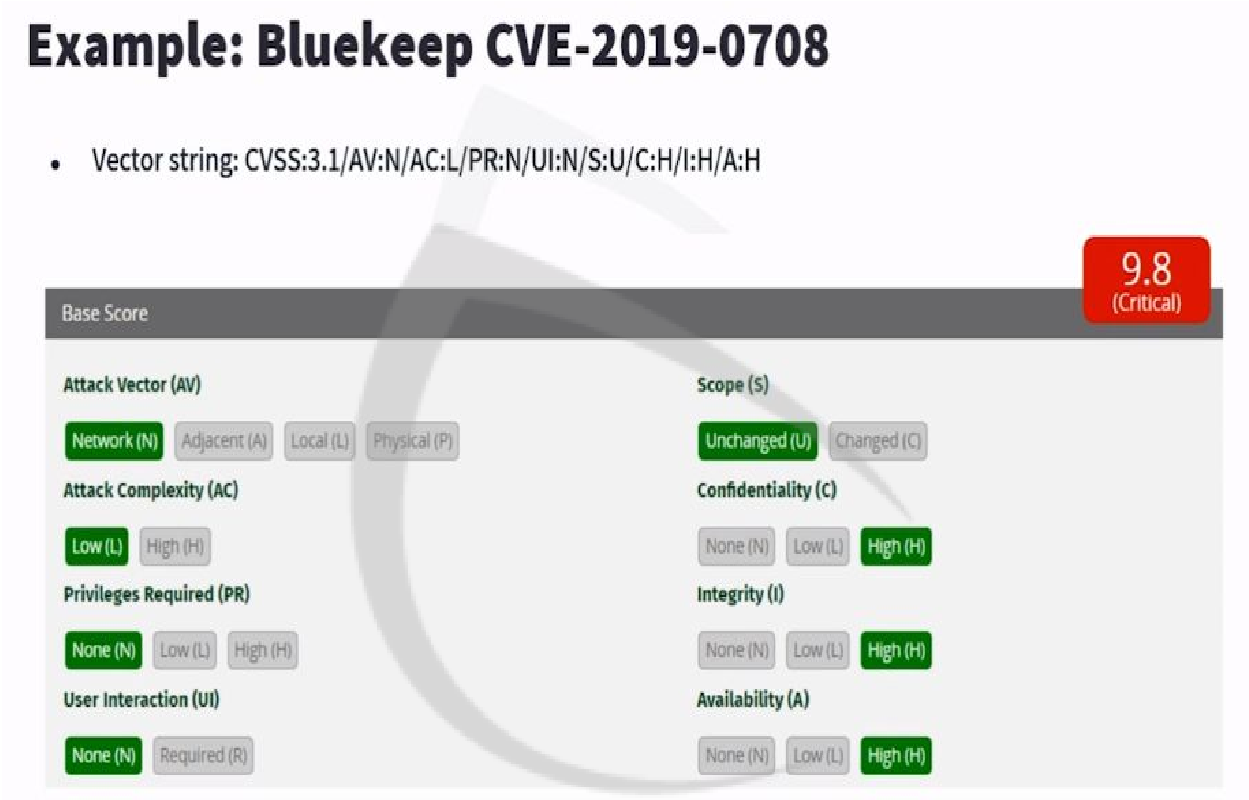
Skills Learned From This Lesson: OpenIOC, Cybox, STIX

Advantages of using standards

- Use of existing tools built to support the standard
- Reduced percentage of misinterpretation
- Ease of sharing and integration

Scoring standards

- CVSS**:** Common Vulnerability scoring System
  - CVSS is a scoring system for describing and rating IT vulnerabilities
  - The current version of CVSS (CVSSv3.1) was released in June 2019
  - CVSS measures 3 areas of concern:
    - ➔ Base metrics (obligatory)
    - ➔ Temporal metrics (optional)
    - ➔ Environmental metrics (optional)
  - The numerical score can then be translated into a qualitative representation (such as low, medium, high and critical)



Example: Bluekeep CVE-2019-0708

- Vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score

9.8 (Critical)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

None (N) Low (L) [✓ High (H)]

Threat description/ Taxonomy standards: OpenIOC

OpenIOC

- OpenIOC (open indicators of Compromise) was introduced by Mandiant in 2011.
- OpenIOC provides definitions for specific technical details including over 500 indicator terms.
- XML schema

An online example can be found on the website below

https//www.iocbucket.com/openioceditor

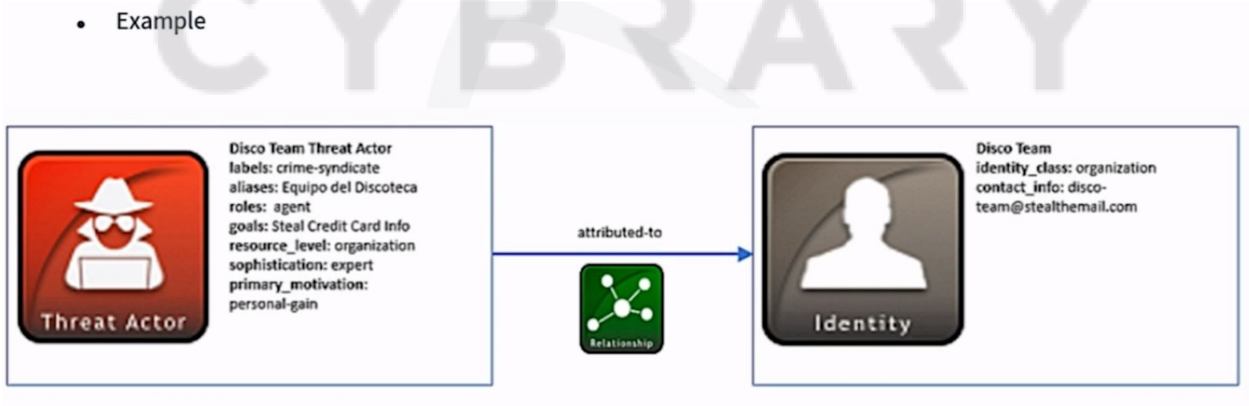
Cyber Observable eXpression (Cybox)

- A standardized language to represent observables
- Introduced by MITRE in 2012 and now maintained by OASIS
- Cybox is now integrated into STIX 2.0 standard
- Types of indicators: OS artifacts, APIs, X509 certificates, network flows, network artifacts, files, SMS messages, images, email messages
- XML schemas

STIX

- Structured Threat Intelligence Expression (STIX) is a structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner with current version 2.0
- JSON schemas

STIX 2 defines twelve STIX domain objects including : Campaign, Course of action, Identity, Malware, Threat actor, Tool, Vulnerability, and others…
STIX 2 defines two STIX relationships objects: Relationship, Sighting.



- Example

Disco Team Threat Actor
labels: crime-syndicate
aliases: Equipo del Discoteca
roles: agent
goals: Steal Credit Card Info
resource_level: organization
sophistication: expert
primary_motivation: personal-gain

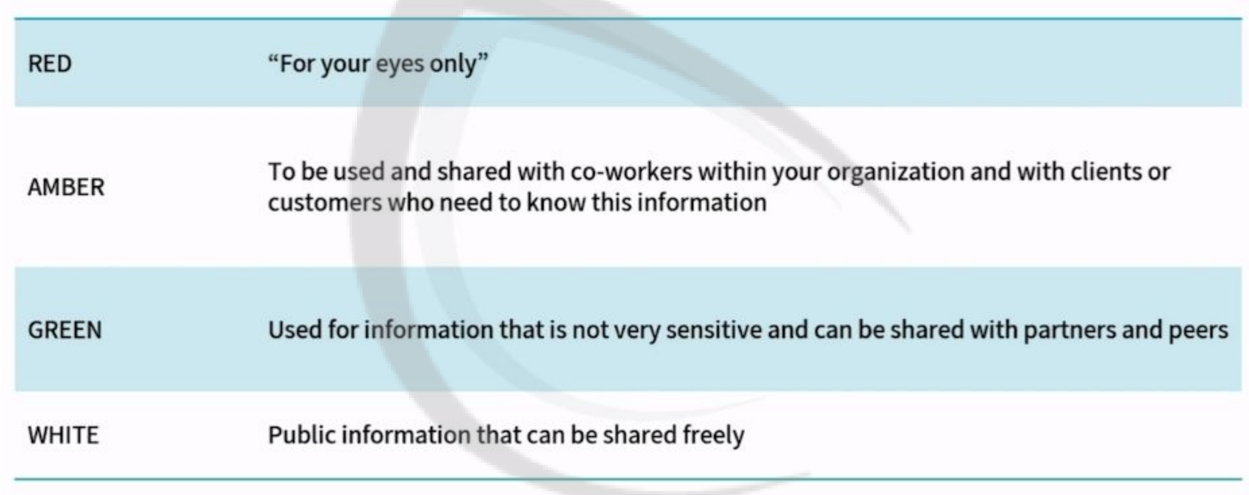
Disco Team
identity_class: organization
contact_info: disco-team@stealthemail.com

Lesson 3.3: Common CTI Standards Part 2

Skills Learned From This Lesson: TLP, TAXII

Transport standards and protocols

TLP - Traffic light protocol



RED	"For your eyes only"
AMBER	To be used and shared with co-workers within your organization and with clients or customers who need to know this information
GREEN	Used for information that is not very sensitive and can be shared with partners and peers
WHITE	Public information that can be shared freely

TAXII - Trusted Automated eXchange of Indicators Information

- Supports sharing of CTI data
- Current version is TAXII 2.0
- In particular, TAXII was design as the transport protocol for STIX
- TAXII uses HTTPS for transport

Lesson 3.4: Storage and Integration

Skills Learned From This Lesson: Storage, Integration.

Storage and integration

- The output information should be conserved to be consumed in the future
- The processed data could be integrated within security products
- Most of threat Intelligence Platforms allow all processing stages by the same software

Importance of storage

- Storage is the final stage of data processing
- Stored intelligence is useful for future usage including temporal analysis and campaign analysis
- Properly stored data is necessary for compliance
- Properly stored information is easier to access and query when needed

Importance of integration

- Integrations are a key requirement for threat intelligence
- Actionable indicators need to find a way back into the security tools and products used by an organization
- Avoid integrating non-curated feeds into active security devices

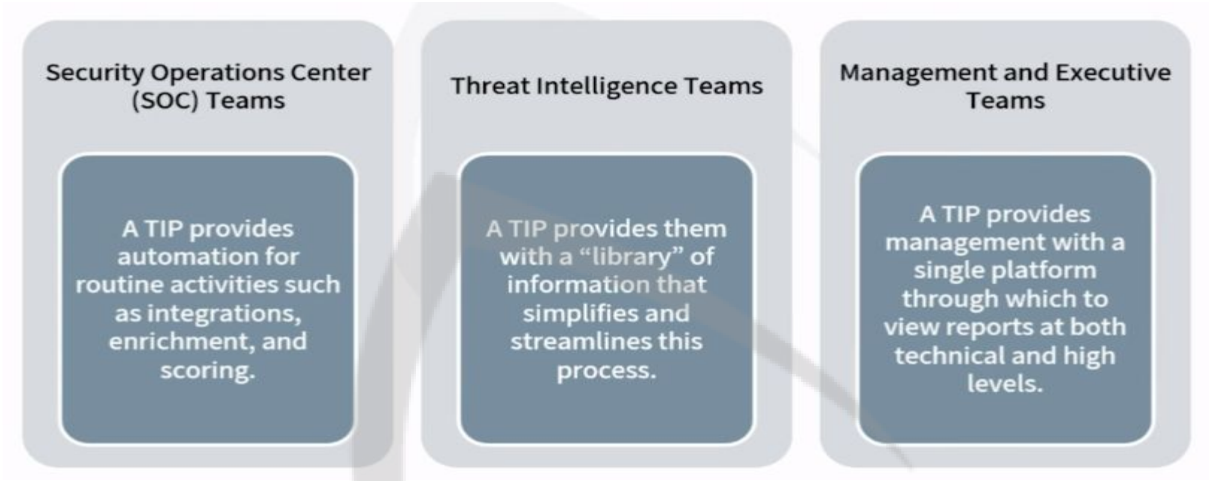
Lesson 3.5: Threat Intelligence Platforms

Skills Learned From This Lesson: Threat Intelligence, Features of TI, Products of TI

Definition:

"A threat intelligence platform is defined as a piece of software where you can organize one or more feeds into a single stream of threat intelligence and that you can use to get alerts and manipulate data"

Who uses Threat Intelligence Platforms



Security Operations Center (SOC) Teams

A TIP provides automation for routine activities such as integrations, enrichment, and scoring.

Threat Intelligence Teams

A TIP provides them with a "library" of information that simplifies and streamlines this process.

Management and Executive Teams

A TIP provides management with a single platform through which to view reports at both technical and high levels.

Common features of Threat Intelligence Platforms

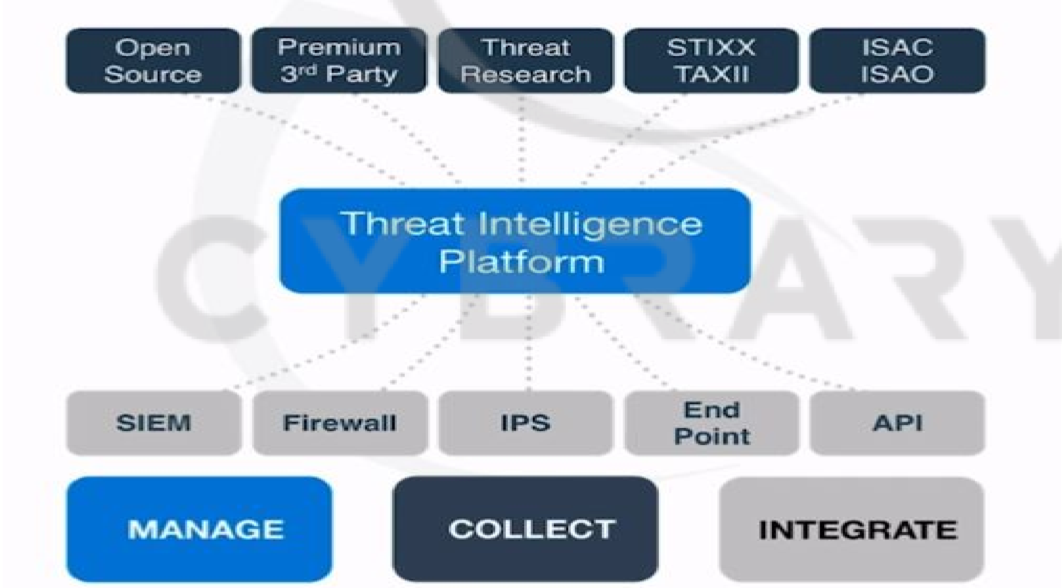


Image Copyright at Anomali.com

Examples of products:

OTX

- Open Threat Exchange is a platform developed by Alienvault
- More than 80,000 collaborators who share more than 19 million potential threats daily
- OTX can act as a TAXII server
- Easy to integrate with other Threat Intelligence platforms

MISP

- A threat intelligence platform for sharing, storing and correlating Indicators of Compromise
- A repository of malware, IOCs and cyber threat related technical information
- Each package of information is called an “Event”
- Receive alerts of other users publishing events

CRITS

- Collaborative Research into Threats is an open source malware and threat repository
- It gives analysts a better way of storing, enriching and discovering threat data
- CRITs can be installed locally for a private isolated instance or shared among other trusted organizations

ThreatConnect

- Offers a free cloud based TIP via: https://app.threatconnect.com
- Big community
- Includes orchestration through the platform

STAXX

- Anomali STAXX provides an easy way to subscribe to any STIX/TAXII feed

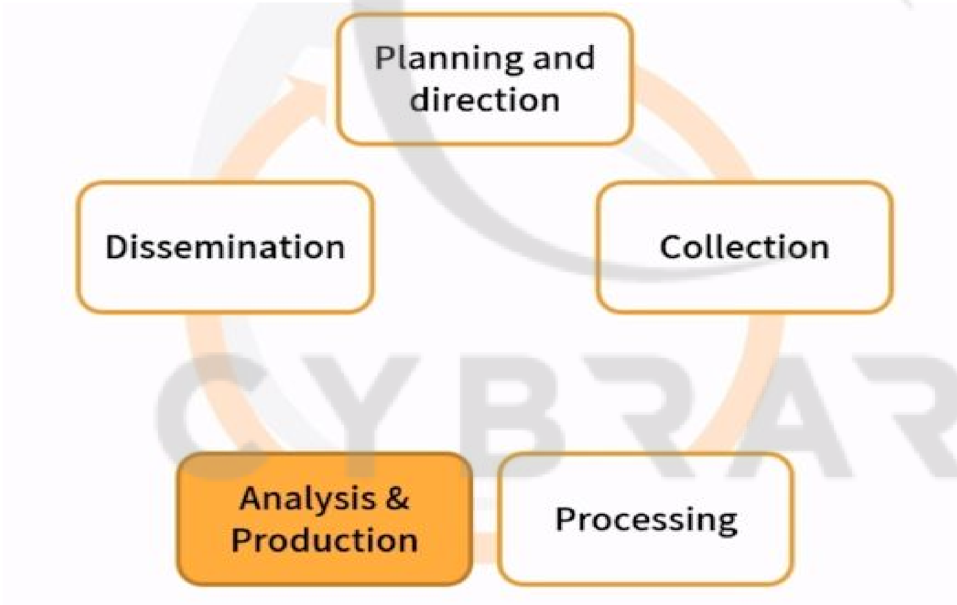
- It comes configured with free TAXII feed LIMO
- It offers enrichment for the indicators (confidence, severity, passiveDNS and WHOIS information)

Module 4: Analysis

Lesson 4.1: Introduction to Analysis

Skills Learned From This Lesson: Analysis, Approaches, techniques.

Analysis and Production



Common analysis approaches, techniques and skills

The main reason to use techniques for analysis is to reduce analyst biases.

- Structured Analytics Techniques

- Analytics of Competing Hypothesis
    - Devil's Advocacy
    - Team A/ Team B
    - Red Team Analysis

- Modelling techniques
    - Attack Graph or Tree
    - Cyber Kill Chain
    - Diamond Model
    - Att&ck Model

Lesson 4.2: Analysis of Competing Hypothesis

Skills Learned From This Lesson: ACH, Wannacry

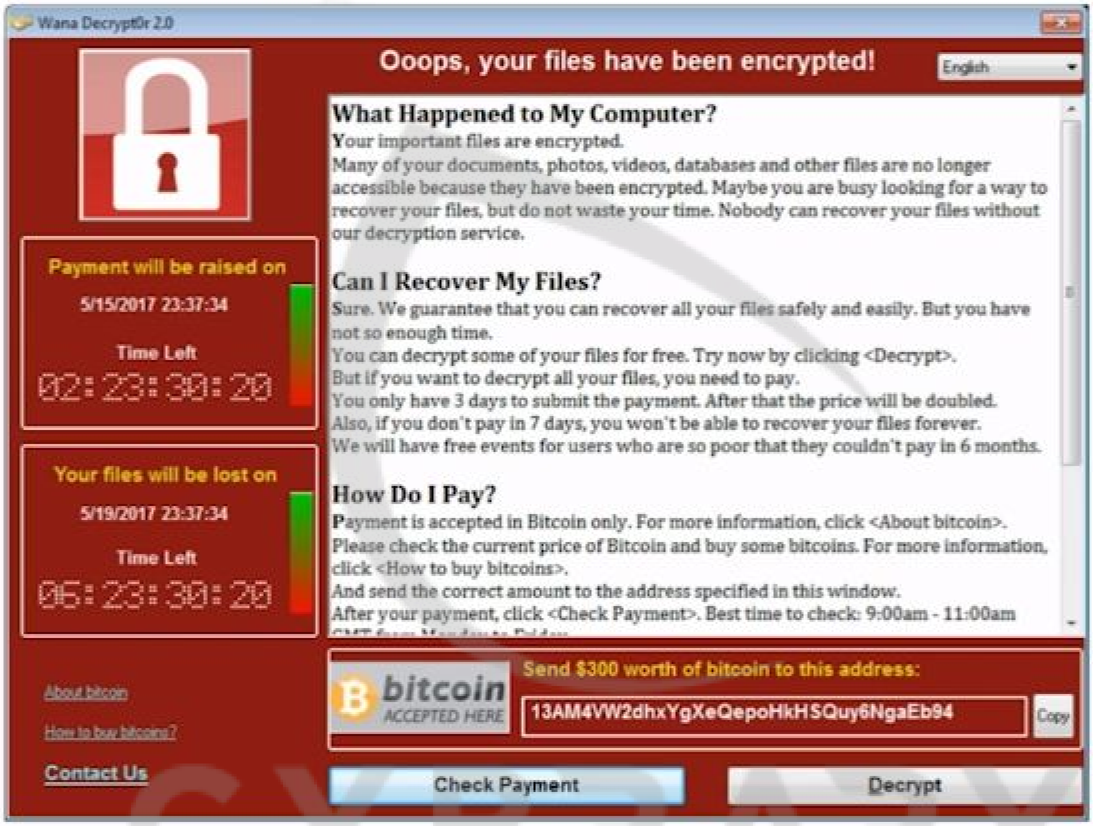
Analysis of Competing Hypothesis (ACH)

- ACH was borrowed from parallel domains to aid analysts
- Producers and consumers of cyber threat intelligence have largely relied ACH to evaluate data and analyze it on the basis of identifying attribution, patterns and more.

ACH steps

1. Enumerate hypothesis
2. Support hypothesis
3. Compare the evidence
4. Refine the matrix
5. Prioritize the hypothesis
6. Determine Evidentiary Dependence
7. Report conclusions
8. Qualify/ evaluation

Use case: Wannacry



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 23:37:34
Time Left
02:23:30:20

Your files will be lost on
5/19/2017 23:37:34
Time Left
06:23:30:20

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

- H1 — A sophisticated financially-motivated cybercriminal actor
- H2 — An unsophisticated financially-motivated cybercriminal actor
- H3 — A nation state or state-affiliated actor conducting a disruptive operation
- H4 — A nation state or state-affiliated actor aiming to discredit the National Security Agency (NSA)

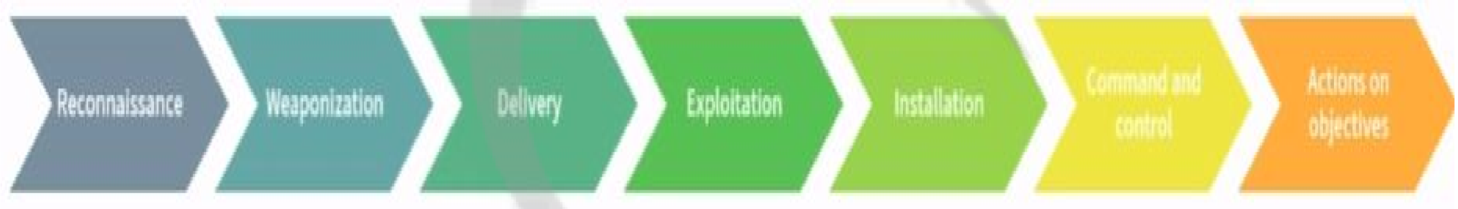
Lesson 4.3: Cyber Kill Chain and Diamond Model

Skills Learned From This Lesson: Cyber Kill Chain, Diamond Model.

Cyber Kill Chain

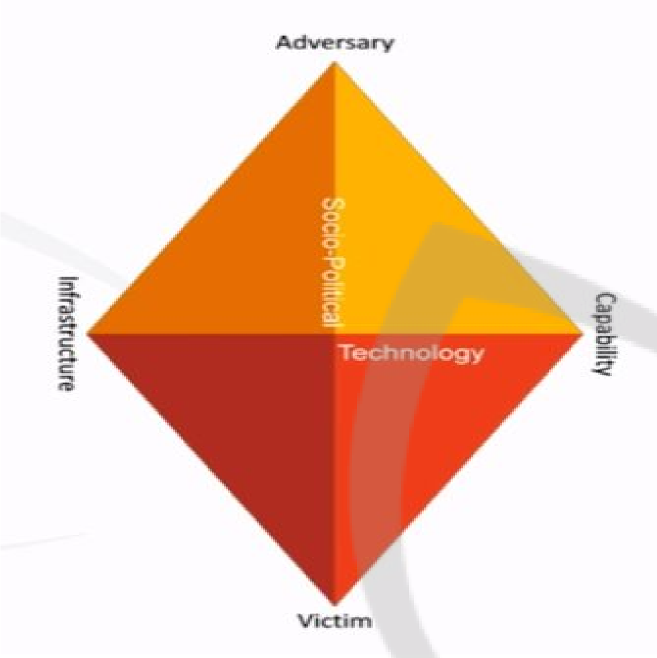
- The concept of the cyber kill chain is attributed to Lockhead Martin and their paper entitled ‘Intelligence-Driven Computer network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains’

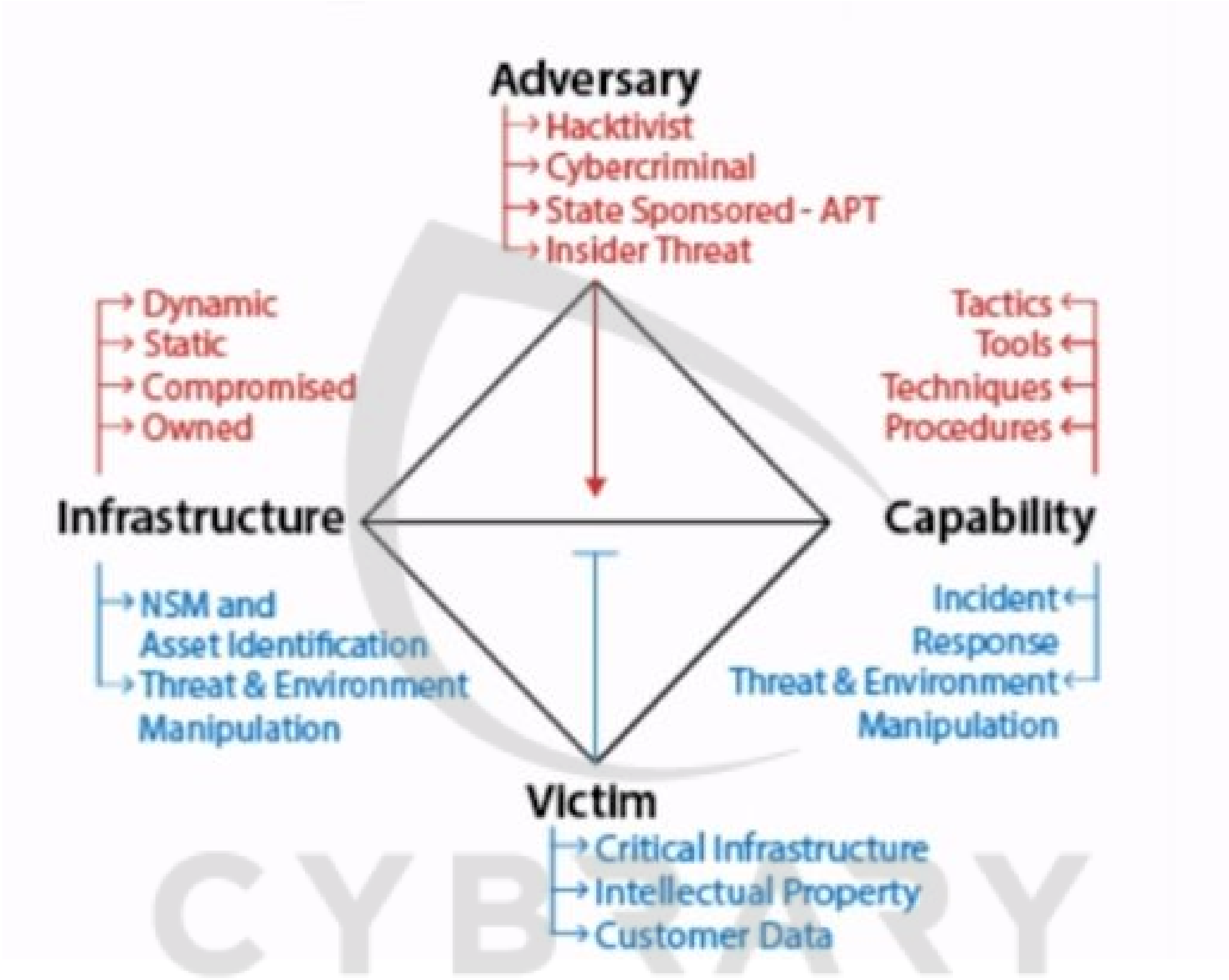
Cyber Kill Chain Steps



Diamond model

- The Diamond Model was published by the Centre for Cyber Threat Intelligence and Threat Research in 2013
- It is one of the novel models for cyber intrusion analysis where an adversary attacks a victim depending on two key motivations rather than using a series of steps like the kill chain.


Adversary
Socio-Political
Infrastructure
Technology
Capability
Victim



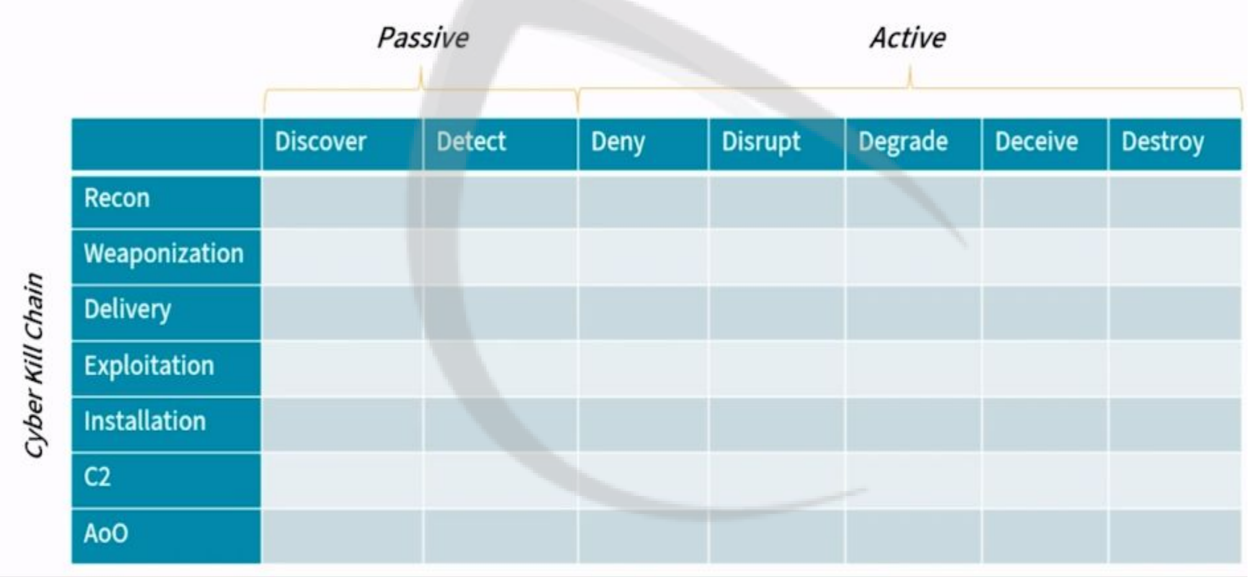
<u>Lesson 4.4</u>: Cyber Kill Chain and Courses of Action Matrix

Skills Learned From This Lesson: Cyber Kill Chain, Passive CoA, Active CoA

Types of Actions

- Passive
- Active

Courses of Action Matrix



		Passive		Active				
		Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Cyber Kill Chain	Recon							
	Weaponization							
	Delivery							
	Exploitation							
	Installation							
	C2							
	AoO							

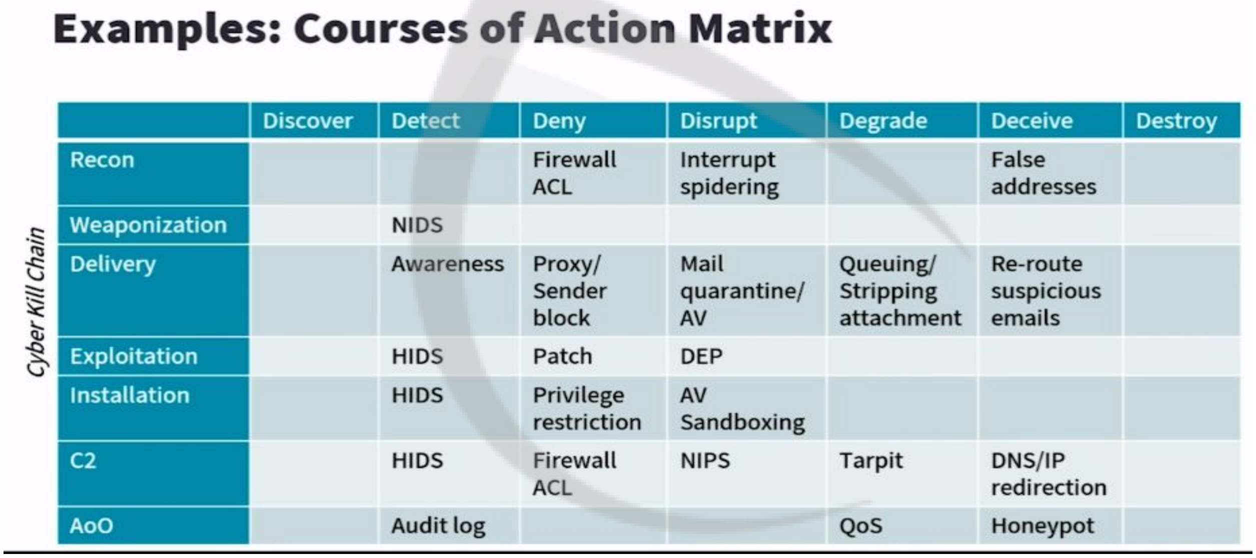
Passive CoA

- Discover
  - The discover action is a “historical look at the data”
- Detect
  - Detecting rules of an indicator for future traffic

Active CoA

- Deny: preventing an event from happening in the first place
- Disrupt: interfere with an event as it is in process to cause it to fail

- Degrade: an action that will interfere with an event as it is in process to reduce its efficiency
- Deceive: lead the adversary to believe the intended event was successful.
- Destroy: This is an offensive action against the attacker and considered illegal for most entities.



Examples: Courses of Action Matrix

Cyber Kill Chain

	Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Recon			Firewall ACL	Interrupt spidering		False addresses	
Weaponization		NIDS					
Delivery		Awareness	Proxy/ Sender block	Mail quarantine/ AV	Queuing/ Stripping attachment	Re-route suspicious emails	
Exploitation		HIDS	Patch	DEP			
Installation		HIDS	Privilege restriction	AV Sandboxing			
C2		HIDS	Firewall ACL	NIPS	Tarpit	DNS/IP redirection	
AoO		Audit log			QoS	Honeypot	

Module 5: Campaign Analysis

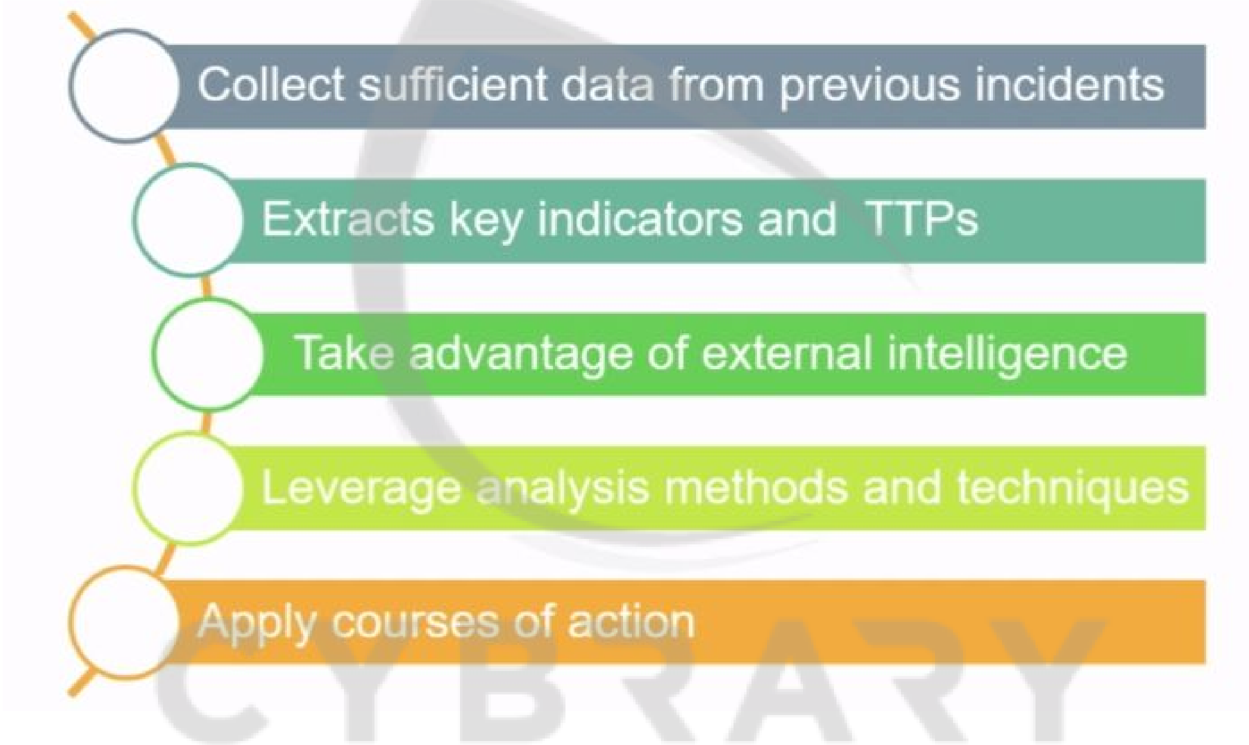
Lesson 5.1: Introduction to Campaigns

Skills Learned From This Lesson: Analysis, Attribution, Techniques.

Definition

A campaign is a set of incidents that occur over a specific time period that relate to each other by shared indicators, tools, infrastructure or TTPs which indicate that they were performed by the same Intrusion Set/Threat Actor/or have a shared objective

Campaign Attribution: where to start?



Collect sufficient data from previous incidents

Extracts key indicators and TTPs

Take advantage of external intelligence

Leverage analysis methods and techniques

Apply courses of action

Campaign analysis techniques

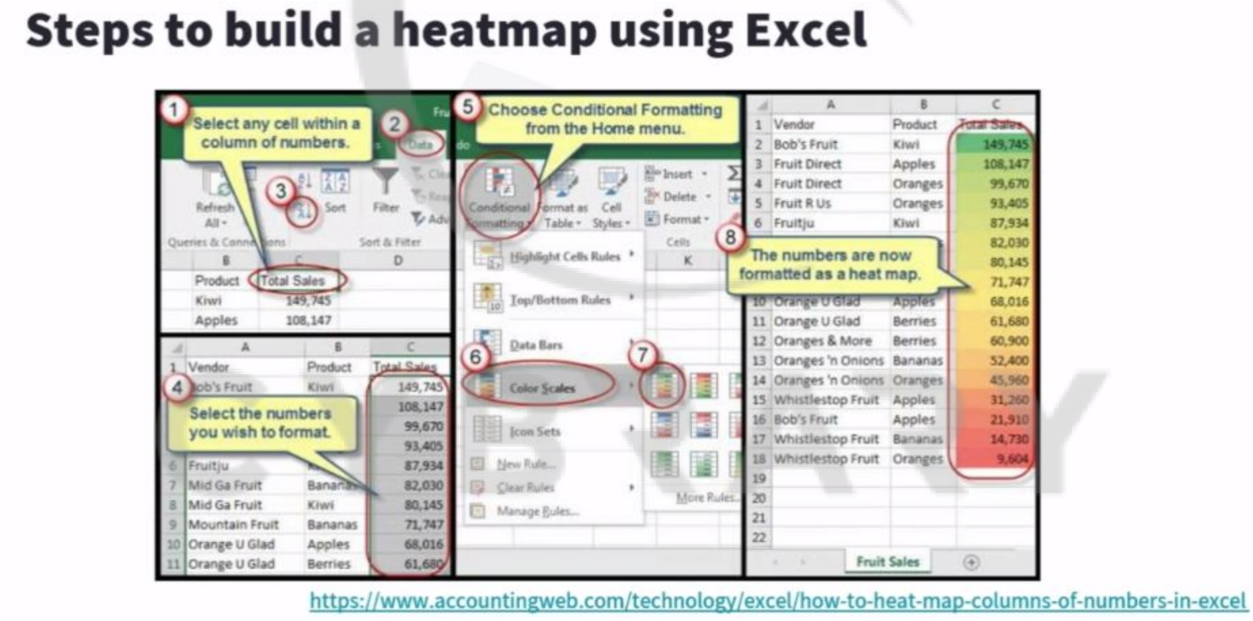
- Data analysis
- Temporal analysis
- Visual analysis
- Heatmap analysis

Lesson 5.2: Heatmap Analysis,

Skills Learned From This Lesson: heatmap, How it works, Examples.

Heatmap

- Graphical representation of data
- A great way to see through data to trends
- They can make complex data sets comprehensible and actionable
- A heatmap shows you in a visual way that is easy to assimilate and make decisions from.



Steps to build a heatmap using Excel

1 Select any cell within a column of numbers.

2 Data

3

4 Select the numbers you wish to format.

5 Choose Conditional Formatting from the Home menu.

6 Color Scales

7

8 The numbers are now formatted as a heat map.

	A	B	C
1	Vendor	Product	Total Sales
2	Bob's Fruit	Kiwi	149,745
3	Fruit Direct	Apples	108,147
4	Fruit Direct	Oranges	99,670
5	Fruit R Us	Oranges	93,405
6	Fruitju	Kiwi	87,934
7	Mid Ga Fruit	Bananas	82,030
8	Mid Ga Fruit	Kiwi	80,145
9	Mountain Fruit	Bananas	71,747
10	Orange U Glad	Apples	68,016
11	Orange U Glad	Berries	61,680
12	Oranges & More	Berries	60,900
13	Oranges 'n Onions	Bananas	52,400
14	Oranges 'n Onions	Oranges	45,960
15	Whistlestop Fruit	Apples	31,260
16	Bob's Fruit	Apples	21,910
17	Whistlestop Fruit	Bananas	14,730
18	Whistlestop Fruit	Oranges	9,604

https://www.accountingweb.com/technology/excel/how-to-heat-map-columns-of-numbers-in-excel

Lesson 5.3: Visual Analysis,

Skills Learned From This Lesson: Graph Analysis, Benefits, Tools.

Graph Analysis

- Also called Visual analysis or Link analysis
- The graph analysis approach relies on a model in which you deal with data as a network
- Information is stored as nodes, connected to each other by edges representing their relationships.

Benefits of Visual Analysis

- Less time is spent assimilating the information because the human brain processes visual information much faster than written one.
- There is a higher chance to discover insights by interacting with the data
- You can achieve a better understanding of a problem by visualizing patterns and context
- Everybody can work with graph visualization, not only technical users

Visual analysis for campaign

- With graph technology, you can combine multi-dimensional data
- Suspicious activities are more easily detected when you analyze the dynamics between entities and not just the characteristics of single entities.
- With this approach, analysts easily gather and analyze data about people, events and locations for example, into one view

Common tools for Visual Analysis

- Maltego
- KeyLines
- Linkurious

Lesson 5.4: MITRE ATT&CK and the MITRE Threat Groups Track

Skills Learned From This Lesson: Mitre ATT&CK framework, Mitre Threat Group Tracker, Benefits of Mitre ATT&CK

Mitre ATT&CK Framework

- ATT&CK is the Adversarial Tactics Techniques and Common Knowledge framework available from MITRE
- Composed of:
    - 11 tactics
    - Hundreds of techniques that attackers can leverage when compromising enterprises.

Benefits of Mitre ATT&CK

- ATT&CK gives us a structured way to describe adversary TTPs and behavior
- Analysts and defenders can both structure their information using ATT&CK
- Organizations can leverage the framework to create a map of their defense systems.
- Creating entries in the MITRE ATT&CK Navigator for specific actors is a good way of visualizing the strengths and weaknesses of one's environment relating to these actors or groups.

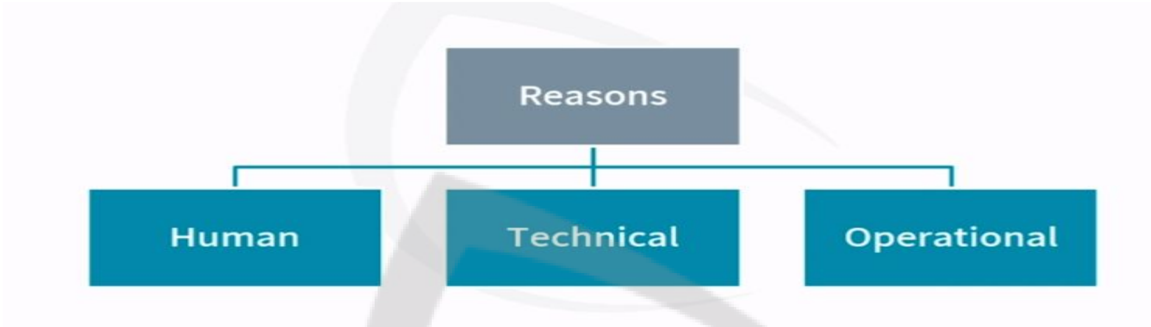
Mitre Threat Group Tracker

- Groups are sets of related intrusion activity that are tracked by a common name in the security community.
- The MITRE ATT&CK team uses the term Group to refer to any of the above designations for a cluster of adversary activity.

Lesson 5.5: Threat Intelligence Naming Conventions

Skills Learned From This Lesson: Naming conventions, Examples.

What leads to different naming conventions



Campaign naming: common recommendations

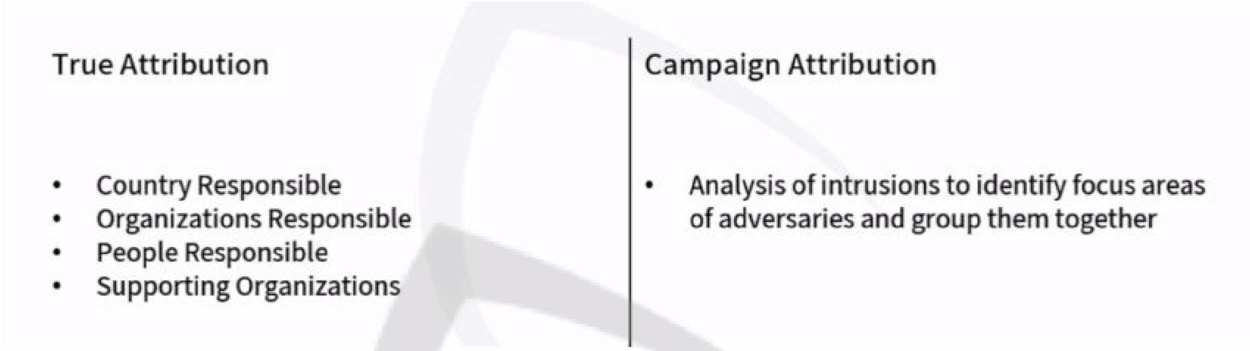
- Things to avoid
  - Numbers, because you may lose track of them
  - Name your campaign after a tool or malware
  - Name based on a country
  - Why not funny names
  - Get inspired by the incidents linked to the campaign (you own incidents)

Module 6: Introduction to attribution

Lesson 6.1: Introduction to Attribution

Skills Learned From This Lesson: Attribution, Types, Requirements.

Types of attribution



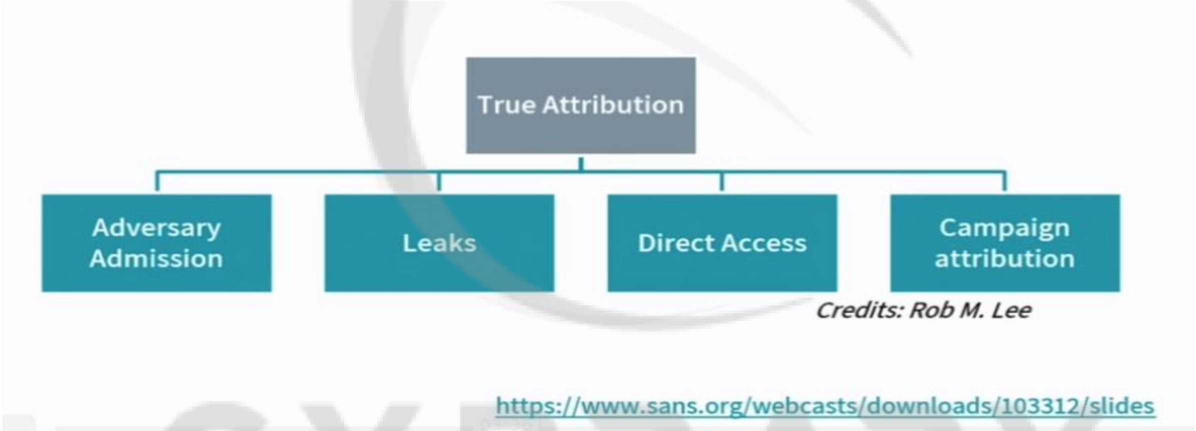
True Attribution

- Country Responsible
- Organizations Responsible
- People Responsible
- Supporting Organizations

Campaign Attribution

- Analysis of intrusions to identify focus areas of adversaries and group them together

Roads to attribution



True Attribution

Adversary Admission

Leaks

Direct Access

Campaign attribution

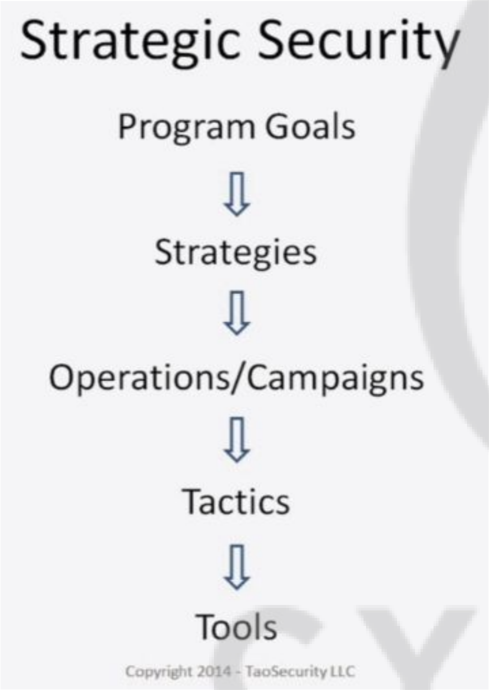
Credits: Rob M. Lee

https://www.sans.org/webcasts/downloads/103312/slides

Why attribution matters

- At the tools level, attribution matters because identifying an adversary may tell defenders what software they can expect to encounter during an intrusion campaign
- The benefits of attribution are similar at the tactics level
- The level of Operations or Campaigns describes activities over long periods of time, over a wider theater of operations from a department or network segment to an entire organization's environment.

- At the level of Strategy, attribution matters to an organization’s management and leadership, as well as policymakers.
- Finally, at the level of policy or “program goals” policymakers can apply many government tools to problems, such as law enforcement, legislation, diplomacy, sanctions, etc. All of these require attribution.


Strategic Security

Program Goals

⇩

Strategies

⇩

Operations/Campaigns

⇩

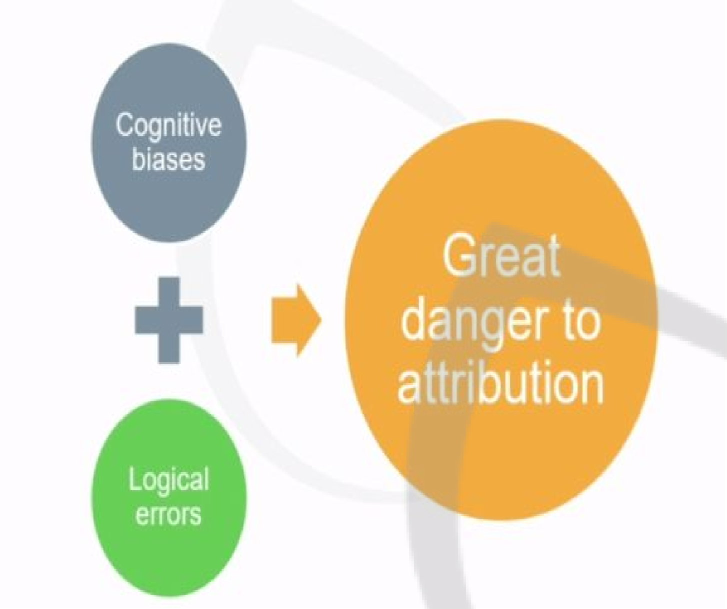
Tactics

⇩

Tools

Copyright 2014 - TaoSecurity LLC

Requirements of attribution



Lesson 6.2: Cognitive Biases

Skills Learned From This Lesson: Biases, Types

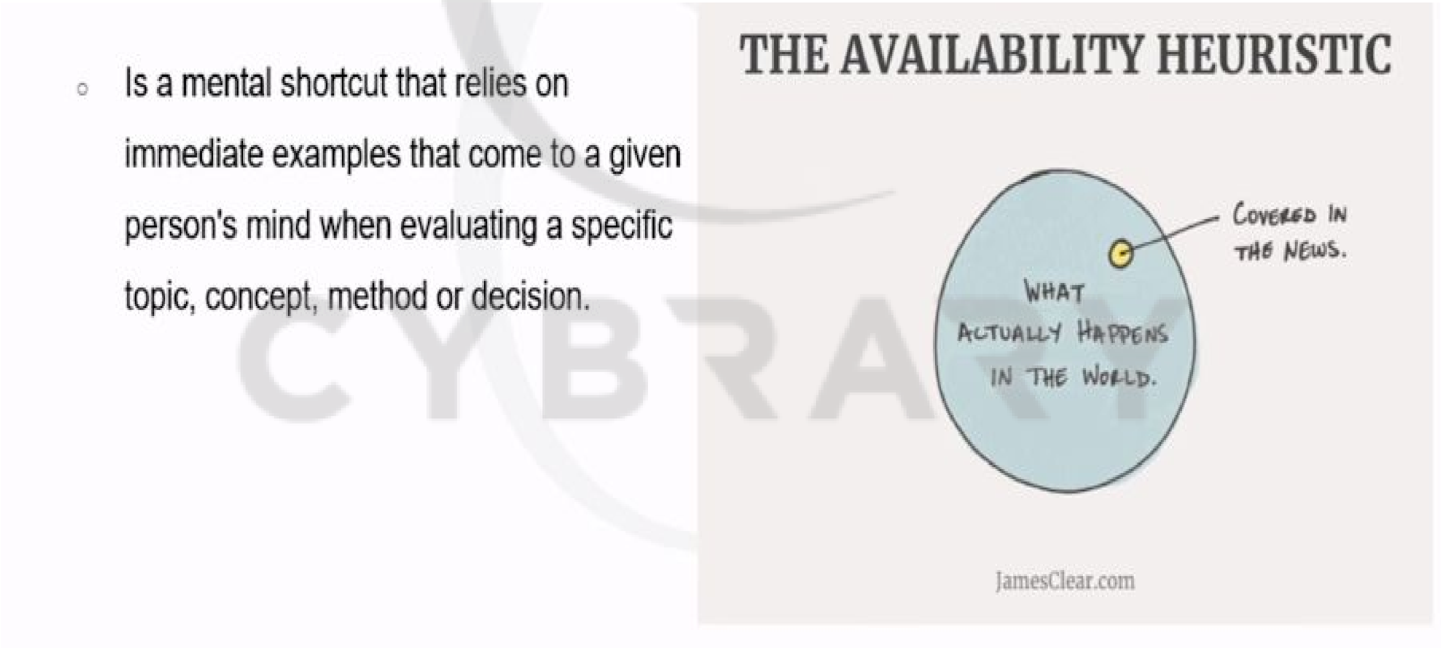
What are Biases

Dr. Margaret Cunningham, principal research scientist at Forcepoint defined biases as: **"***Bias is the tendency for people to favor one group, person, or thing over another, while unfairly discriminating against the remainder of the choices. For better or worse, biase is an inescapable feature of the human experience. We are shaped by a combination of our environment, our genetics, and our cognitive ability to process and make sense of our world. This means that our decisions, behaviors, and experiences are influenced by the experiences of the past and the present"*

Common types of Biases

- ❖ Anchoring bias
- ❖ Availability bias
- ❖ Confirmation bias
- ❖ Correlation is not causation
- ❖ Illusory correlation
- ❖ The framing effect

★ **The availability bias**

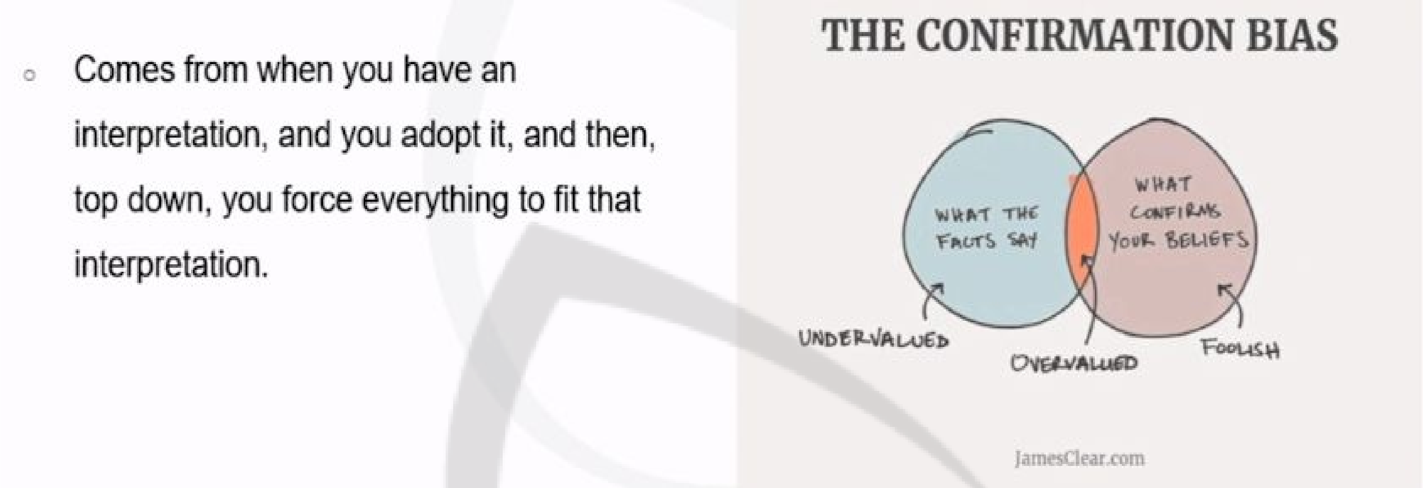


○ Is a mental shortcut that relies on immediate examples that come to a given person's mind when evaluating a specific topic, concept, method or decision.

THE AVAILABILITY HEURISTIC

JamesClear.com

★ **Confirmation bias**

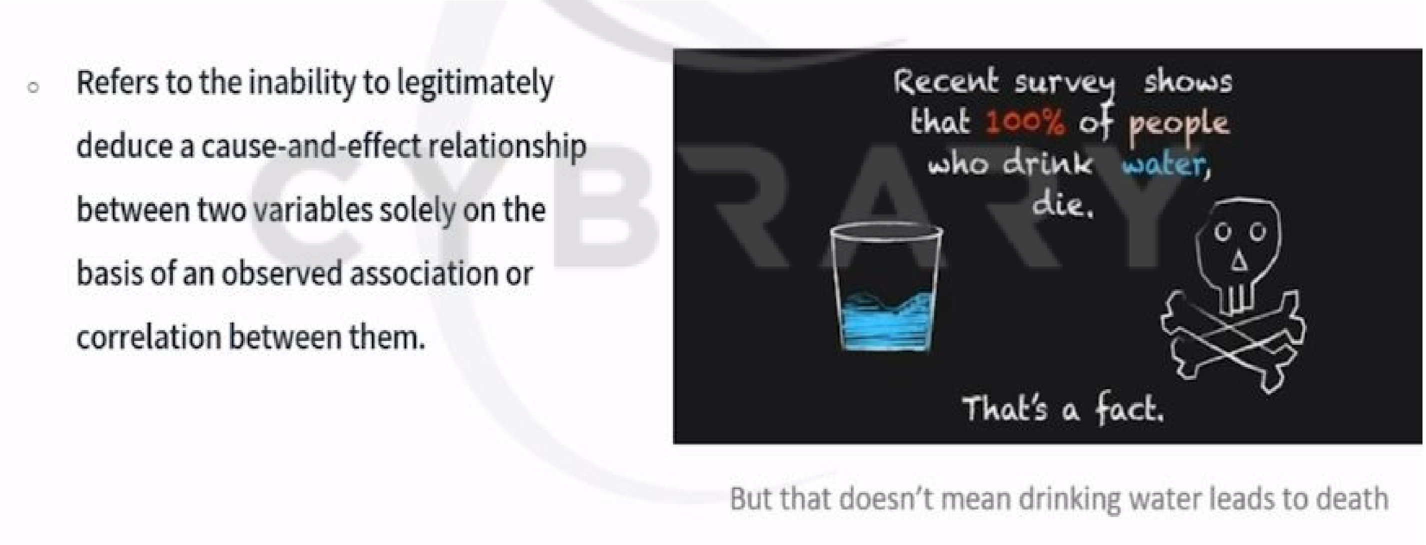


- Comes from when you have an interpretation, and you adopt it, and then, top down, you force everything to fit that interpretation.

THE CONFIRMATION BIAS

JamesClear.com

★ **Correlation is not causation**



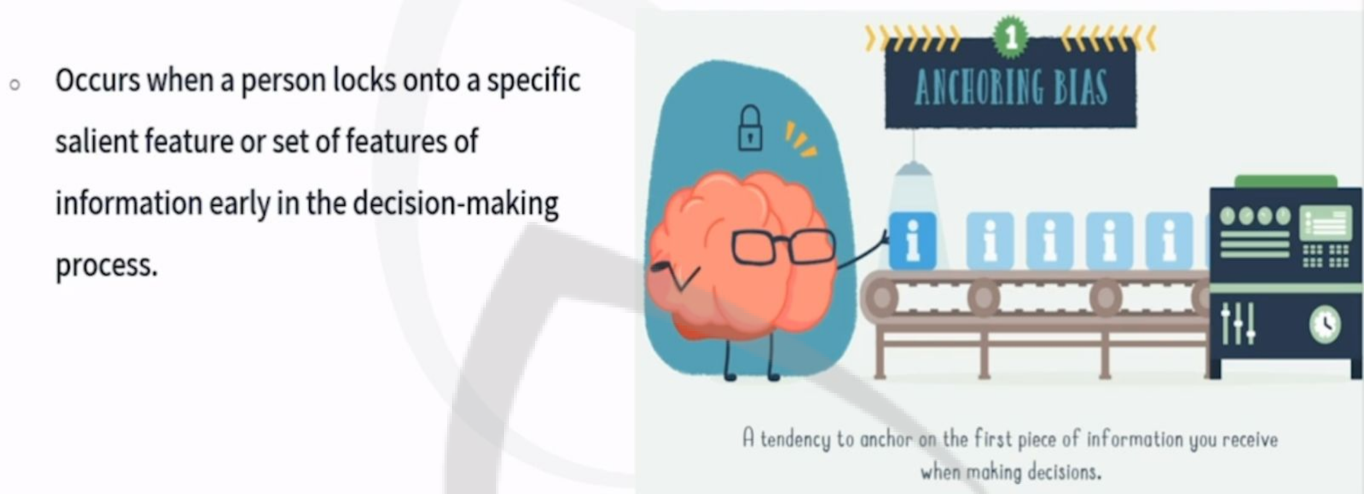
- Refers to the inability to legitimately deduce a cause-and-effect relationship between two variables solely on the basis of an observed association or correlation between them.

Recent survey shows that 100% of people who drink water, die.

That's a fact.

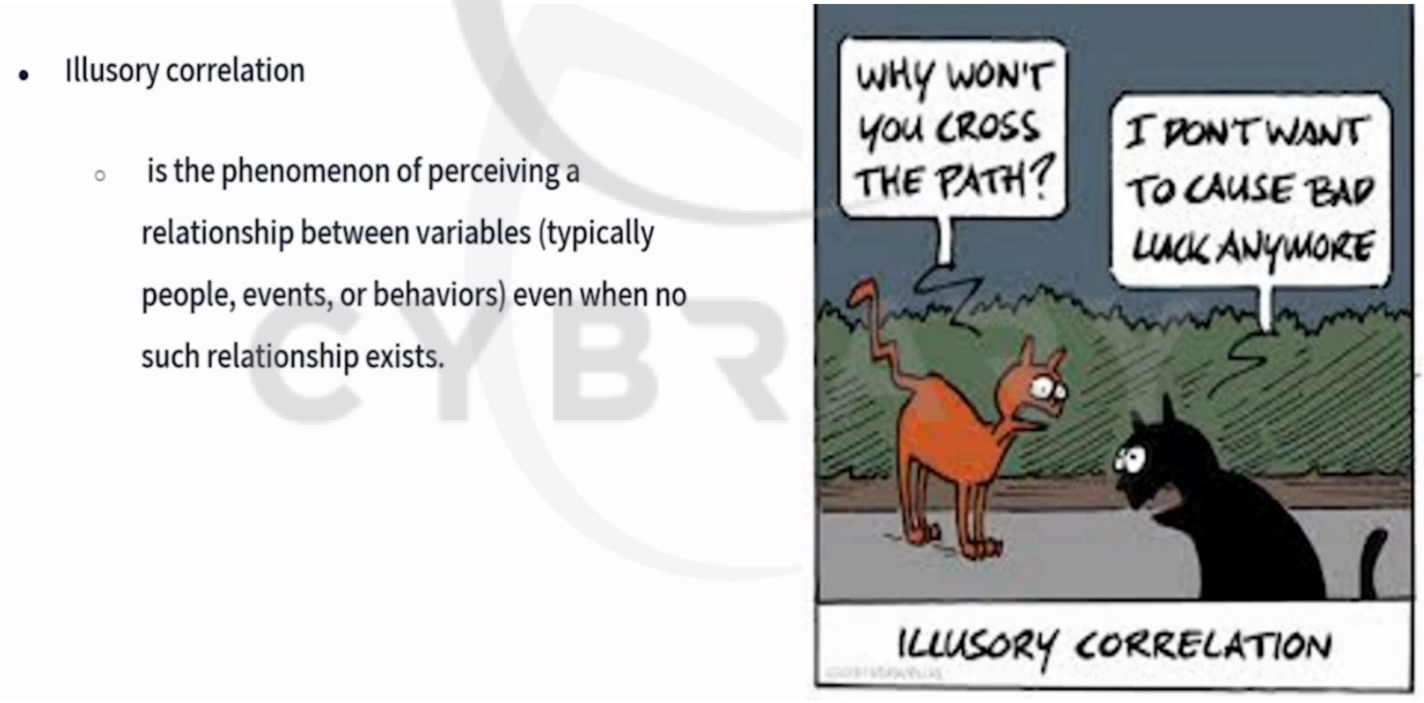
But that doesn't mean drinking water leads to death

★ **Anchoring effect**



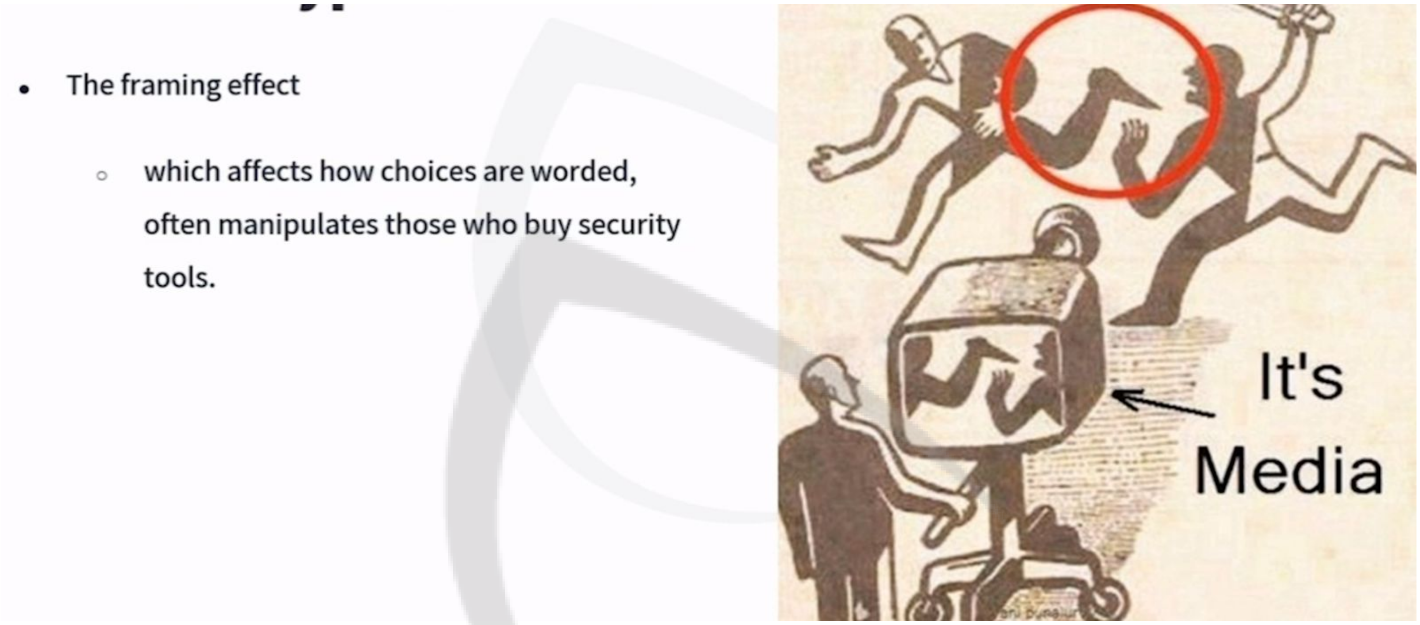
- Occurs when a person locks onto a specific salient feature or set of features of information early in the decision-making process.

A tendency to anchor on the first piece of information you receive when making decisions.



- Illusory correlation
  - is the phenomenon of perceiving a relationship between variables (typically people, events, or behaviors) even when no such relationship exists.

WHY WON'T YOU CROSS THE PATH?
I DON'T WANT TO CAUSE BAD LUCK ANYMORE
ILLUSORY CORRELATION



- The framing effect
  - which affects how choices are worded, often manipulates those who buy security tools.

Lesson 6.3: Logical Fallacies

Skills Learned From This Lesson: Fallacies, Classifications, Common types.

Definition

- A fallacy is the use of invalid or otherwise faulty reasoning, or “wrong moves” in the construction of an argument or analysis. *Wikipedia*
  It is a kind of error in reasoning.

Classification of fallacies

- Formal
- Informal

Common Formal Fallacies

- Appeal to probability
  - X is possible
  - Therefore, X is true

- The Anecdotal Evidence Fallacy
  - One of our clients doubled their conversions after changing all their landing page text to bright red. Therefore, changing all text to red is a proven way to double conversions.

Common Informal Fallacies

- Burden of Proof
  - It is invalid to claim that X is true until someone else can prove that X is not true.

- Argument by Repetition
  - X is true, X is true, X is true, X is true, X is true, X is true...etc.

Lesson 6.4: How to Manage Biases

Skills Learned From This Lesson: Biases, Examples, Recommendations

How to manage biases

- Avoid making decisions under time pressure
- Avoid making decisions when you are cognitively involved in a different task
- Train yourself to think statistically

- Have participants review your results

In this step, it is important to remember the analysis techniques and methods:

- Structured Analytic techniques such as:
    - Analysis of competing hypothesis
    - Devil's advocacy
    - Brainstorming
    - High impact/low probability analysis
- Cyber Kill Chain
- Diamond Model
- Courses of Action

Example

Anchoring - one of the most difficult biases to mitigate.

Recommendation

- ACH or Analysis of competing Hypothesis is a good start point
- Re-think your hypothesis whenever there is new information
- Tweaking your hypothesis when new set of information is available leads to error

Lesson 6.5: Nation-State Attribution Part 1

Skills Learned From This Lesson: Nation-state actors, Modus operandi, Motivations, targets.

Definition

"The nation State Actor has a 'licence to Hack'. They work for a government to disrupt or compromise target governments, organizations or individuals to gain access to valuable data or intelligence, and can create incidents that have international significance." [*https://www.baesystems.com*](https://www.baesystems.com)

Targets of Nation-State actors

- Government institutions
- Industrial facilities
- Other businesses

They use sophisticated tools and techniques to cause massive data and revenue loss.

Motivation of nation-state actors

- Political interests
- Commercial interests
- Military interests

Modus Operandi

- Stealing industrial secrets
- Disrupting critical national infrastructure
- Listening to policy discussions
- Taking down companies that offend its leaders in some way
- Conducting propaganda or disinformation campaigns within and outside of their countries

Methodologies employed in state-sponsored attacks

- Wherever possible, state-sponsored actors will use standard attack methodologies
- They usually involve targeted phishing emails followed by use of recent, known exploits the victim may not have gotten around to patching.
- When they have a foothold, actors often move laterally into shared servers and other systems where they can steal privileged credentials
- Only when a company is highly matured in its security posture, is a high value target, and generic attacks fail, will they resort to using costly 0-day malware developed internally.

The challenge of detection

- State-sponsored actors will rarely make a lot of noise and cause sufficient disruption to warrant suspicion or trigger detection
- Their objectives are to remain persistent to retain oversight of communications, or access to sensitive data.
- They can remain practically invisible until the victim attempts to extract the actors and, just as the victim thinks it was successful, the actors will utilize these to walk straight back in and continue operations.

Lesson 6.6: Nation-State Attribution Part 2

Skills Learned From This Lesson: Nation-state, Fighting sophistications.

Fighting sophistication

- Every enterprise must also educate their teams and enforce best practices.

- Constant vigilance and monitoring of all security processes in place is absolutely essential to defense - for nation state threats
- Be proactive in reducing your ‘attack surface’
- Patch
- ‘Keep your friends close, but your enemies closer’

Module 7: Dissemination and sharing

Lesson 7.1: Introduction to Dissemination

Skills Learned From This Lesson: Dissemination, Sharing, Feedback

Definition

- Dissemination involves getting the finished intelligence output to the places it needs to go.

Forms of Intelligence

- Strategic
- Operational
- Tactical

Sharing

Companies need to be sharing more security intelligence with industry peers to better defend against and more rapidly adapt to ever-changing threats.

A key factor for realizing cooperative approaches are the underlying threat intelligence data formats.

Feedback

- The effectiveness of one cycle of threat intelligence will determine the essential elements of information needed for the next cycle, including what spaces to focus on when collecting data and how fast action needs to be taken.
- After receiving the CTI’s finished intelligence, stakeholders should provide feedback to help fine-tune future iterations of the intelligence distribution and inform future intelligence operations.

Lesson 7.2: Tactical Intelligence

Skills Learned From This Lesson: Benefits, Shortcomings, Audience

- Tactical/ Technical cyber intelligence is information from direct adversary action inside your systems or from other sources that have the potential to immediately influence your tactical decision
- This data is typically derived from real-time monitoring of systems
- Examples include feeds from intelligence providers.

Tactical decisions

Tactical intelligence can lead to conclusions about what adversaries want, which can help you make rapid decisions on what to block, what to allow and, at times, what to shut down.

Benefits of tactical cyber threat intelligence

- Provides context and relevance to a tremendous amount of data
- Empowers organizations to develop a proactive cybersecurity posture.
- Informs better decision making during and following the detection of a cyber intrusion
- Drives momentum toward a cybersecurity posture that is predictive, not just reactive.

Shortcomings

- It is relatively short term in nature
- The ever-evolving threat landscape dictates that sources must be timely and of high quality

Audience

Tactical threat intelligence is intended for a technical audience, and usually includes some technical context. It is particularly consumed by personnel directly involved in the defense of an organization.

<u>Lesson 7.3</u>: Operational Intelligence

Skills Learned From This Lesson: Operational decisions, Benefits, Audience.

Definition

- Operational intelligence is a real-time or near real-time intelligence, often derived from technical means, and delivered to ground troops engaged in activities against the adversary.
- Examples of operational cyber intelligence include information feeds from an information sharing and analysis center (ISAC) and alerts from the Department of Homeland Security (DHS)about a new threat trend.

Operational decisions

Operational decisions made by security professionals, IT teams and even executives are better informed with a knowledge of which tools adversaries are using, which vulnerabilities they are exploiting and what techniques other defenders are using to successfully mitigate the threat.

Other operational decisions include the policies you put into your IT systems to automatically respond to tactical threats.

Benefits

- Enrich security events and alerts for known-bad atomic IOCs
- Enhance incident response plans and mitigation techniques for future attacks and incidents
- Implement and bolster a proactive hunting program
- Extract useful red teaming techniques based on attacker methods in the wild.
- Perform actor-based and malwae family-based analytics for high risk threats to your company, industry, geography or nation.
- Develop detection methodologies that are not dependent on IOCs, ensuring broader coverage of threats in a more timely fashion.

Audience

Operational threat intelligence is intended for an almost exclusively technical audience (eg. security operations personnel and managers).

Lesson 7.4: Strategic Intelligence

Skills Learned From This Lesson: Strategic intelligence, Benefits, Audience

Definition

- ❖ In simple terms, strategic threat intelligence ia a bird's eye view of an organization's threat landscape.
- ❖ Not concerned with specific actors, indicators, or attacks, it instead aims to help high level strategists understand the broader impact of business decisions.
- ❖ It is the most complex form of intelligence to generate and is human resource-intensive. It demands a nuanced understanding of the cyberthreat landscape.

Strategic Intelligence

Unlike other intelligence categories, the majority of strategic threat intelligence sources are open source, making it accessible to anyone. Common examples include:

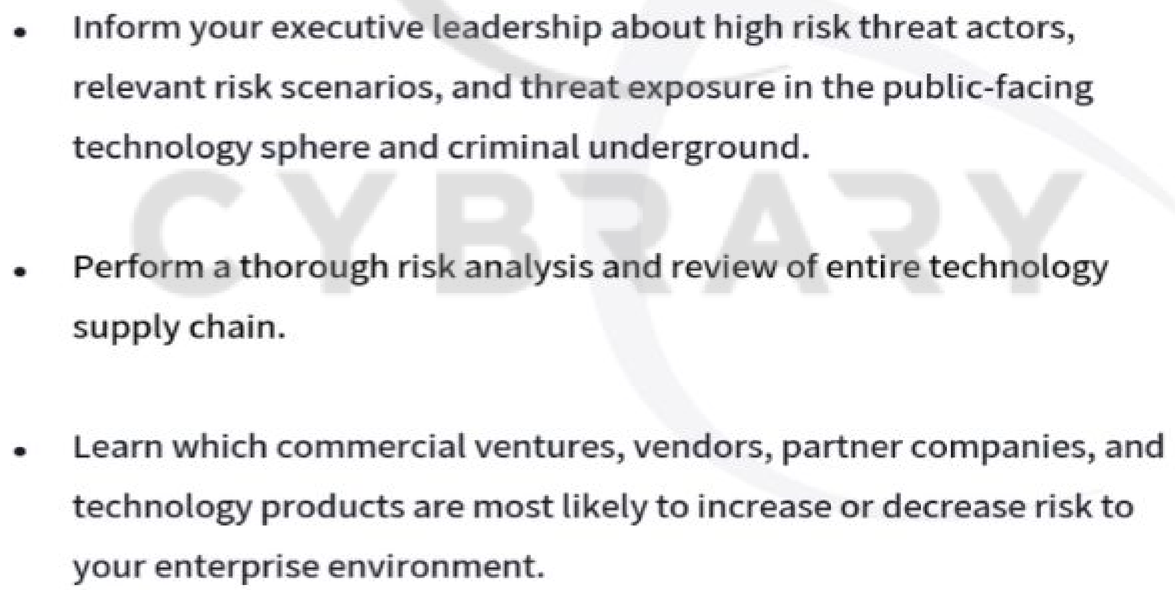
- ❖ Policy documents from nation-states
- ❖ Local and national media
- ❖ Industry and subject specific publications
- ❖ Comments, online activity, and articles from individuals of interest

- Free content produced by security organizations (eg. white papers, research reports etc.)

Strategic decisions

- Strategic intelligence often comes in the form of threat briefings tailored to your industry or organization
- Can be used to advocate for stronger coordination and collaboration with other organizations
- Good strategic intelligence will motivate enterprises to rethink processes - including both nontechnical such as audit, and technical processes such as configuration management- to reduce IT errors.

Benefits of strategic Intelligence



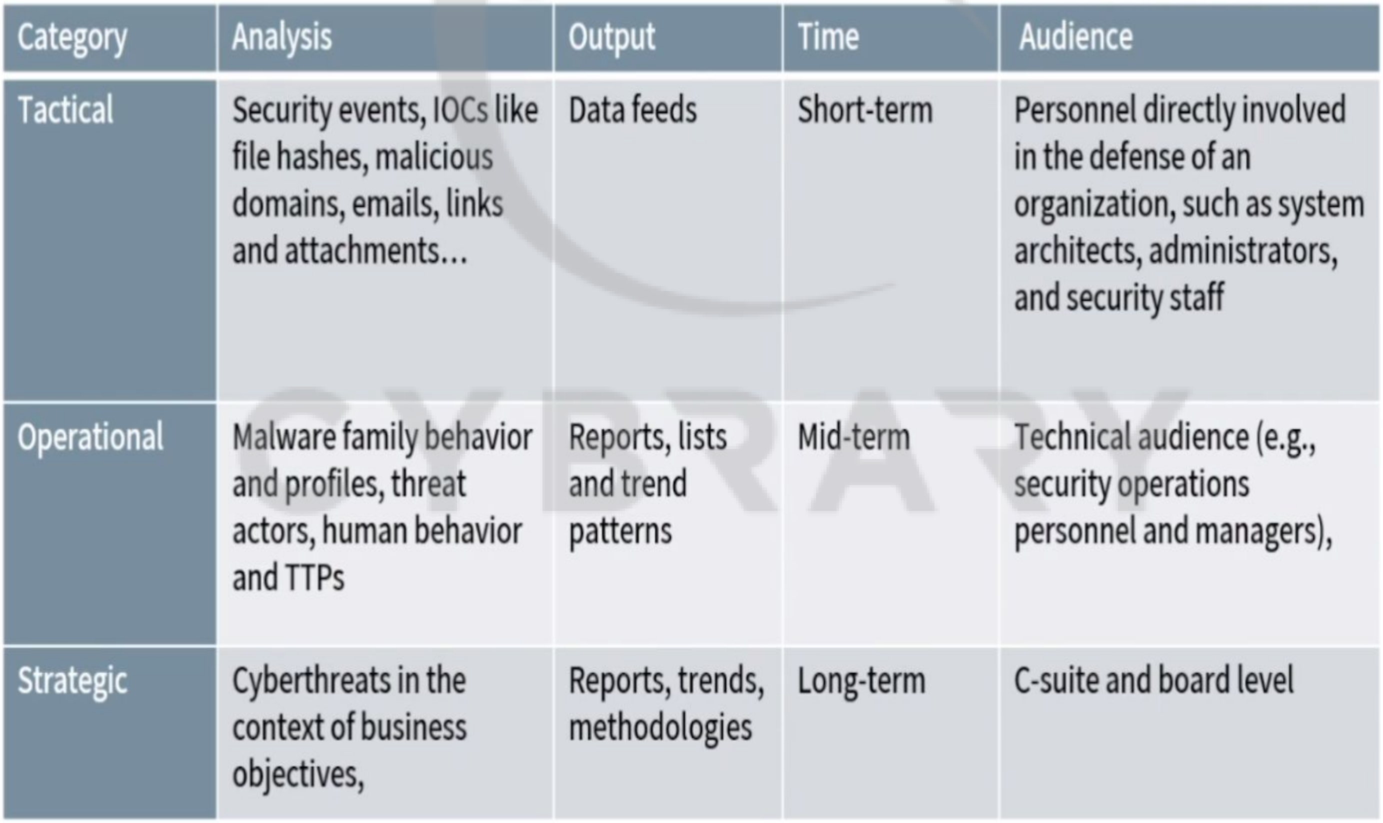
- Inform your executive leadership about high risk threat actors, relevant risk scenarios, and threat exposure in the public-facing technology sphere and criminal underground.
- Perform a thorough risk analysis and review of entire technology supply chain.
- Learn which commercial ventures, vendors, partner companies, and technology products are most likely to increase or decrease risk to your enterprise environment.

Audience

Since it’s used to inform specific, high level decisions, strategic threat intelligence is usually gathered on demand rather than as an ongoing initiative, and is most often presented as a report or briefing.

Given that the audience primarily C-suite and board level, strategic threat intelligence is almost exclusively non-technical.

Quick recap



Category	Analysis	Output	Time	Audience
Tactical	Security events, IOCs like file hashes, malicious domains, emails, links and attachments…	Data feeds	Short-term	Personnel directly involved in the defense of an organization, such as system architects, administrators, and security staff
Operational	Malware family behavior and profiles, threat actors, human behavior and TTPs	Reports, lists and trend patterns	Mid-term	Technical audience (e.g., security operations personnel and managers),
Strategic	Cyberthreats in the context of business objectives,	Reports, trends, methodologies	Long-term	C-suite and board level

Module 8: Summary

Lesson 8.1: Summary

Skills Learned From This Lesson: A recap of all topics in this course.