EC-Council

A Complete Guide to Cyberthreat Data Analysis

EC-Council's Cyber Research team would like to thank **Charlene Coon, Director of Cybersecurity, Confidential** for authoring this white paper.

EC-Council Cyber Research

Index

Abstract

There has been a huge advancement in the field of technology. Organizations have increasingly adopted technologies like blockchain, IoT, etc., invariably leading to an increase in cybercrime such as security breaches and data theft. To avoid security threats and safeguard network parameters, it is essential that organizations opt for strong cyberthreat data analysis. This is a process which analyses the security and infrastructure to check vulnerabilities against cyberattacks.

This paper gives a brief introduction to the cyberthreat data analysis process, and what is meant by threat intelligence and its relation to cyberthreat data analysis. The focus is on the components of the cyberthreat data analysis process and methodology, as well as the threat modeling process. Two examples provide an overview. This paper also talks about the generic threat matrix developed by analysts, who can benefit from cyberthreat analysis, the top cyberthreat intelligence tools that help in analyzing and combating threats to reduce risks, and how to become a threat analyst.

Keywords: *Cyberthreat data analysis, threat intelligence, threat modeling process, threat analyst, threat intelligence tools, risks*

What Is Cyberthreat Data Analysis?

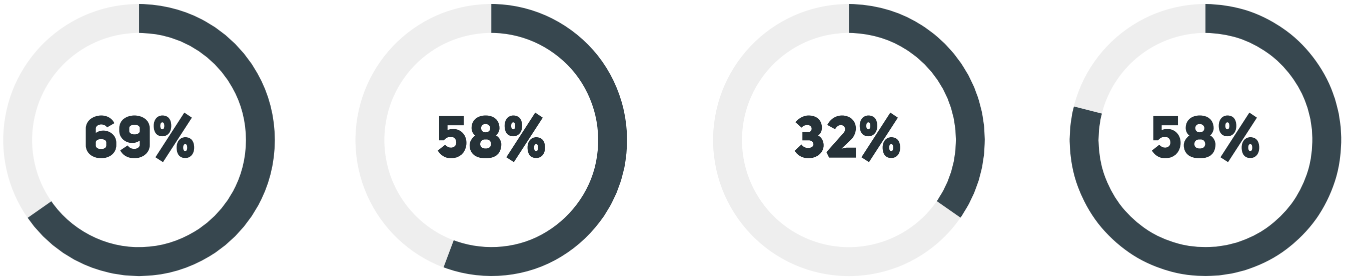
Cyberthreat analysis is the process by which every element of a system or infrastructure (system of systems) is analyzed to determine how vulnerable it is to cybersecurity threats (AKA being hacked). Cyberthreat analysis focuses on a businesses' existing systems and systems being developed. The analyst identifies, tests, and recommends the best practices for maximizing protective measures to keep sensitive information and systems safe and reduce company risks. The work of a cyberthreat analyst is a combination of risk assessment and vulnerability testing to understand the cyberthreats and risks to businesses. For example, the threat of a hacker infiltrating the Command and Control (C&C) system of a power plant energy system has the risk of causing devastating blackouts to communities and businesses.

This threat-oriented approach to the battle against cyberattacks demonstrates a seamless process from a passive security state to a responsive one concerning cybersecurity. Moreover, a threat assessment's intended outcome is to include best practices in the key elements of cybersecurity — enhancing confidentiality, integrity, and availability (CIA). This strategy of using defensive strategies and tools preserves an organization's usability, functions, sensitive information, reputation, and profitability.

Cyberthreat data analysis aims to bolster security and improve existing IT infrastructure systems or new systems being deployed by system administrators or developed by engineers, so that the systems are not prone to attacks by bad actors (inside or outside of the organization). A cyberthreat analyst generates results critical to businesses to help in the initiation and implementation of cybersecurity plans, policies, procedures, configurations, and continuous monitoring (CM) activities to safeguard the organization's assets. Businesses can choose to a) avoid, b) accept, c) countermeasure, d) mitigate, or e) transfer risks for organizational systems. This process involves tailoring industry best practices to meet the needs of each system and company.

Cybersecurity Report

Bricata (2019) employers reported:



are understaffed

have open cybersecurity positions

finding good candidates takes six months or longer

cited employers having to increase pay

There is a huge demand for cybersecurity analyst professionals [1]. Making a career in threat intelligence is easier than people think, since there is a huge demand but very few skilled professionals to fill those roles. According to market statistics, the industry is forecast to grow from $5.3 billion USD to $12.9 billion USD from 2018 to 2023.

It is safe to say that cyberthreat data analysis is a lucrative field and there are tons of opportunities lying in wait for those who want to step into the industry. Comparing the average earning of those with non-cyber degrees with those with cyber degrees shows how lucrative the pay is. The pay rates vary from area to area and country to country, but typically are reflective of a study by the U.S. Census Bureau (2015) [2].

NON-cyber degree average earnings:

- Non-cyber associates
- **$41,498** annual
- Non-cyber bachelors **$51,124** annual
- Non-cyber master degree **$69,732** annual

U.S. Census Bureau (2015)

...Does that look like less than half of cybersecurity salaries???

What Is Threat Intelligence and How Is It Related to Cyberthreat Data Analysis?

Threat intelligence is the information an organization uses to assess and analyze threats. The insights gained from studying this critical information are used to implement new and updated security measures. These measures are utilized to protect organizations from threats and foresee unexpected attacks. In a world where a simple data leak can bring down companies, threat intelligence becomes a core element around which IT infrastructures are designed.

Threat intelligence involves taking data from multiple sources and creating threat intelligence feeds along with management reports. Organizations use these findings to keep themselves informed of various threats, vulnerabilities, and exploits in their systems to identify risks. Threat data becomes threat intelligence when insights can be used to design security strategies with different goals. Analysts can think of the data becoming intelligent when any actionable use becomes applicable to a business. In essence, cyberthreat data analysis is the step before data turns into threat intelligence.

How It Started: A Brief History of Cybersecurity

It was back in 1988 when a Cornell University student, Robert Tappan, transmitted a "Morris Worm" to the web. He claimed the malware was released to analyze the extent and vastness of cyberspace, but this incident no doubt sparked the inspiration for DDoS attacks later on. Fast forward a few years, many high-profile cyberattacks were launched on the likes of giants such as Amazon, eBay, Sony, Google, etc. Small businesses and start-ups were not prone to cyberattacks back then. They stayed outside the radar.

Times have changed. Today, it is not uncommon for entrepreneurs to employ the latest cybersecurity systems to protect their data. Data is the new oil — an invaluable resource in the digital world. Anyone who has unrestricted access to it can cause staggering losses to businesses, besides leaking privacy and confidential information. What motivates hackers? Money, fame, vengeance, politics, social, challenges, and curiosity.

There are business risks involved when these threats are not taken care of. For example, because of the ease of hacking passwords, business managers are moving beyond password-based logins and moving to two-factor authentication for accounts. Businesses now know that having skilled IT and cybersecurity data analyst experts on staff can help screen and ward off these threats and reduce business risks. New emerging technologies that are hot in the industry are behavioral and data analytics utilizing artificial intelligence (AI) and machine learning (ML). Most people know that data analysts are using AI and ML algorithms to find out things like how people use their devices, what are their preferences, what are their dislikes, what motivates them. What most people do not know is that cybersecurity data analysts also look at patterns in data that spot threats and vulnerabilities to ultimately help reduce risks.

Activities that might trigger alerts and warnings could stem from clues like suddenly making a large financial transaction, downloading from archived folders, and shipping to unknown destinations, thus notifying business owners of any suspicious internet users.

Importance of Cyberthreat Data Analysts

Being a cyberthreat data analyst offers many benefits, such as:

1. With a cyberthreat data analyst's efforts, an organization can figure out the weak spots in its security measures, identify the sectors of the system that can easily be attacked by cybercriminals, and develop plans to reduce risks from all the security threats that can destroy an organization. Threat vulnerabilities and misconfigurations of systems can be resolved, resulting in an enhanced cybersecurity posture.

2. With a cyberthreat data analyst's efforts, they can provide the organization with information to check whether it is in compliance with the industry standards required by governments and international bodies. The analysts help determine whether the company fulfills compliance requirements. If it doesn't, undesirable outcomes and frequently huge fines may transpire.

3. The cyberthreat data analyst's threat assessment involves reviewing cybersecurity controls, their efficiency, and whether controls need upgradation. Analysts also assist the organization in taking preventive measures to increase the effectiveness of security.

Watch this detailed video on cyberthreat analysis and its importance in today's world by Matt Russell: https://www.youtube.com/watch?v=jelvfj-fGI4&feature=emb_logo [3]

Threat Actors

Cyber attackers have distinct motivations and capabilities, impacting the assets they will attempt to compromise and the techniques they will use to breach their target. Cybercriminals, nation-states, hacktivists, and insiders are the critical classes of risk involving bad actors (hackers). These classes may be expanded into sub-categories, and there may be slightly different motives and abilities for each separate person in these groups. Threats to businesses are multiple and diverse.

There are threat actors who specifically target a particular organization or sector, and these can be identified and analyzed while analyzing threats and risks. These threat actors are then categorized in order of their motivation, capability, and likelihood of targeting the organization, assigning each a value to determine their overall threat to the organization.

They majorly benefit from and are highly capable of deploying custom-made malware to penetrate a network. The assets they target are valuable data that can even be decrypted, especially if they can decrypt backups, which are often on less protected systems. The threat actors often use one of their phenomenally successful social engineering methods, phishing. Phishing can lead employees to believe an email is an original invoice that needs a link to be clicked or an attachment file that needs to be opened, but in reality, later encrypts the network with malware and demands payment to decrypt the business's data.

Components of Cyberthreat Data Analysis

Cyberthreat data protection systems are automated systems an organization uses to help protect their data. When modeling cyberthreat data protection systems, analysts must walk through a series of steps that define the scope, goals, and features of those systems. The key components involved in the design and development of automated cyberthreat data analysis systems are:

1. Scope

Scope defines the elements of a business that are to be protected. It states the objective of cyberthreat data analysis assessments and accounts for sensitivity of the data. In short, the scope of an analysis describes what to protect and the level of protection needed [4].

2. Data Collection

Most organizations fail to meet security standards when it comes to their defensive capabilities. Companies keep a log of previous threats and incidents and carefully analyze them through data collection. This process involves taking into account not just future verifiable threats but potential threats as well. Potential threats can quickly escalate and turn into real threats, even if they are not serious at first glance.

The focus of data collection is also to differentiate between targeted threats and threats that seem real but are not (false positives). This involves events such as collecting incidences of phishing, uncovering the Command and Control infrastructures of IP addresses and domains, and then looking at the settings of the scope to filter out false positives. Learning how to identify these false positives help organizations not to be distracted and not to waste time and money on them. Automating some of this with ML and AI tools helps improve the security posture of a business.

Cybersecurity analysts often require unrestricted access to data. Activities he/she can participate in are analyzing firewalls, incidents, intrusion measures, open-source internet searches, organizational data history, digital forensic analysis, etc., to get the big picture of a business's cybersecurity maturity and needs. All data about existing policies and legal compliance measures are studied, written, and/or collected depending on one's role. Such documents are examined to check if an organization's corporate policies match the compliance requirements of data security. The analyst has to make use of critical thinking skills and carefully go through the data, both of which are qualities needed for professional cyberthreat data analysis [4].

3. Vulnerability Analysis of Acceptable Risks

Analysts test systems in this stage and assess the degree of vulnerability they have against certain threats. This involves using information to examine the defense mechanisms and see if security systems can protect themselves against said threats and neutralize them, including their capability to safeguard the integrity and confidentiality of data. Penetration testing, a popular role in cybersecurity, is a part of the vulnerability analysis of data [4].

4. Mitigation and Anticipation

Mitigation and Anticipation are the final stages in cybersecurity data analysis where the analyst implements security measures against future threats after making an assessment based on the previous steps. The analyst categorizes different threats and classifies each accordingly (e.g., low, medium, and high), making sure to note any patterns. He/she then uses the results of the findings to implement new security measures to prevent future incidences of cybersecurity attacks. The analyst also future proofs the systems against any upcoming threats and considers any unforeseeable circumstances with implementations [4].

Methodology

This section aims to define what threat models and threat matrixes are. The goal is to characterize different threats and explain the purpose of elementary cyberthreat data analysis and their role in the characterization of risks.

Threat Metrics

Threat metrics define the parameters used for making accurate threat measurements. Understanding how threats work along with the formation of anomalies in systems can fuel the threat analysis process. The missing dots between common threats and potential consequences are connected through threat metrics.

In other words, a metric is a unit of measurement that is used to measure something, often called a baseline, in cybersecurity. Threat metrics measure the potential of a threat. There are benchmarks in the industry set against which the systems utilized to perform baseline analysis are tested. Not that all cybersecurity systems are equal. Nor are the cybersecurity technicians that build the security profiles on these systems for a business. An excellent example of a threat metric would be analyzing how many attacks happen per month, and then using the numbers for the consequent months to reveal the capabilities and limitations of current security systems. The analyst can calculate risks and possible loopholes in the system after reviewing these threat metrics [5][6][7][8]. Choosing a quality system, a capable technician, and a skilled cybersecurity data analyst are vital to success.

Threat metrics also help the analyst know how to act, control, and deal with persistent threats. It improves the analyst's ability to perceive different threat scenarios and extrapolate enough information to design new measures. There would be no cyberthreat data analytics or threat data modeling without threat metrics because these metrics have raw data and collect from sources.

Threat Models

Threat models are generated using various threat metrics. They give a big picture view of current security systems by gathering, organizing, and analyzing the raw data. Analysts make a threat model essentially when they convert the raw data into a representable and usable form. Several metrics together make up the "threat measurement framework."

Threat measurement frameworks encapsulate the threat metrics' behavioral characteristics, which would not usually make sense if they were taken apart and analyzed individually. But together, when seen under a lens, the patterns come into play, and organizations make sense of the data.

These models get updated over time as the data grows, thus creating an index of previous threats. The reason threat models are so useful is because they eliminate personal bias and prejudice from the equation when analyzing various threats. A model simplifies the problems being faced and also gives insight into the little details. The data used for generating threat models should be well-documented by organizations for future reference since other cybersecurity analysts can use it when they start looking at the business' IT systems [5][7].

Threat Modeling Process

The threat modeling process is not taken lightly and delivers key insights to organizations. There are two samples used, with each providing a precise breakdown of how threat attributes are used in the modeling process [7].

Example No 1

There are three significant steps involved in risk assessment and threat modeling:

- **Assessing risks:** This involves looking at the flaws in the organization's security systems. The analyst finds out how much data can be lost if it were under attack.

- **Finding out potential threats:** The analyst discovers the different ways the data can be attacked. Figuring out how frameworks and libraries respond under these risks are also part of this.

- **Mitigating threats:** Making sure the code protects the system and gets updated, along with implementing fixes to become less susceptible.

Example No 2

Here is an overview of the threat modeling process:

- **Identify all assets:** Find out what business assets are at risk and list them.

- **Make an overview of each system architecture:** This involves creating simple diagrams to document different security architecture elements. The diagrams should be easy to understand and give a visual breakdown of each system and how they connect. Other components to be included in them are data flows, trust boundaries, and subsystems.

- **Breakdown the system applications:** Breaking down the system application includes revealing its exposure to various threats and risks. The analyst makes a detailed security profile of the network architecture and goes about uncovering every single vulnerability. All angles and types of software and communication threats are explored in this stage. Identifying ports, protocols, and services is an important step in this stage.

- **Identify risks:** Find out the attackers' motives and see what the company is up against. Distinctively identifying different vulnerabilities, their features, characteristics, and how they impact the system are considered.

- **Documenting threats:** This collects all the threats and records, and places them in a logical sequence. A threat template is used to capture the different attributes and assign every threat to the identified attributes.

- **Threat rating:** Once the attributes have been assigned to specific threats, threat rating comes into action. This is a process where the analyst rates each threat's severity and shows how risky they are to the organization. The scale of the potential damage caused by each is also highlighted by rating these threats.

The Generic Threat Matrix

The Generic Threat Matrix is a structure created by the analyst to explain various threats to organizations. It adds layers to these threats and uses multiple attributes to describe the situations fully. Building the matrix ends up minimizing biases and preconceived notions affecting the analysis, thus giving structure and accuracy to interpretations. Different levels of magnitude are then assigned to the matrix, with each level corresponding to its unique threat, thus providing a better study [7].

a. Threat Attributes

Threat attributes are individual features of a threat. They are classified into two dominant groups:

Commitment Attribute Group

The commitment attribute group classifies the level of commitment an attribute has to achieve its goal. The commitment attribute group is further sub-classified into three groups:

- **Stealth** (Question: How well does the attribute go unnoticed, and does the organization have any existing record of the threat?)
- **Time** (Question: What amount of time is the attribute staying invested in when it comes to seeing through its course of action?)
- **Intensity** (Question: How far is the attribute willing to go to see to the completion of its goal?)

Resource Attribute Group

The resource attribute group defines the amount of resources threats can deploy to attack the system and reach their goal. If the magnitude level is higher than usual, it indicates that the threat can grow sophisticated in its attacks, meaning it can reach its goal more efficiently.
The resource attribute group is also divided into three additional attributes:

- **Access** (Question: How efficiently can the threat attack the system, and what is its level of efficiency?)
- **Technical Personnel** (Question: What resources is the threat using?)
- **Knowledge** (Question: How much skill does the threat actor have?)

b. Attack Vectors

Attack vectors define the routes threats take to hijack a system or data. It outlines the exact steps and creates a pathway out of it, detailing how the threat gets access to the system, facility, environment, or person. No matter how it gathers data or implants malware, attack vectors reveal how hackers act and achieve their goal.

Attack vectors can be categorized as follows:

- Unlocked system screens
- Mobile devices
- Phishing attacks
- Malicious web apps
- Malware
- Viruses
- Unsecured wireless networks
- Insider threats
- Outsider threats
- Insecure buildings and vehicles

c. Target Characteristics

Target characteristics take a look at the targets of the threats.

Questions like:

What makes the target vulnerable?
How likely is it to be attacked?
How frequently is it attacked?

These are answered by exploring the target characteristics. Essentially, analysts get an idea of how vulnerable each target is and what makes them so attractive to the said threats. Thinking like and understanding a bad actor's potential motives helps in this process.

d. Attack Trees

Attack trees break down each threat and its respective agents. It decomposes threats and conceptualizes them in a structured and logical way. An attack tree also documents the data collected about threats that are to be anticipated by the system. If a threat has sub-categories, then an attack tree will cover them. It is an excellent way to categorize different threats and classify them.

Advantages of attack trees:

- Analyzes different target agents and gives complete transparency.
- Uses deductions and observations to give quality outputs.
- With their flexible nature, attack trees encompass the whole spectrum of threat agents.
- It can be used with other threat data models.

e. Attack Frequency

Attack frequency reveals how frequently a threat agent attacks its target. If a target is being attacked multiple times by the same threat or by various threats, there could be something wrong with it. Features such as why it is more vulnerable than the other elements in the system, along with the steps taken to resolve its various issues, are examined.

Getting Feedback

The final step of the cyberthreat data analysis is getting feedback. After receiving the finished reports and threat data visualizations, the analyst can discuss the tactics and security measures to employ. He/she will get to work after the organization's budget, expectations, etc., are set. Plans are developed and steps forward are discussed. The security measures implemented will comply with legal and corporate policies, making sure not to break any laws to protect the data. This process is in a loop called continuous monitoring (CM).

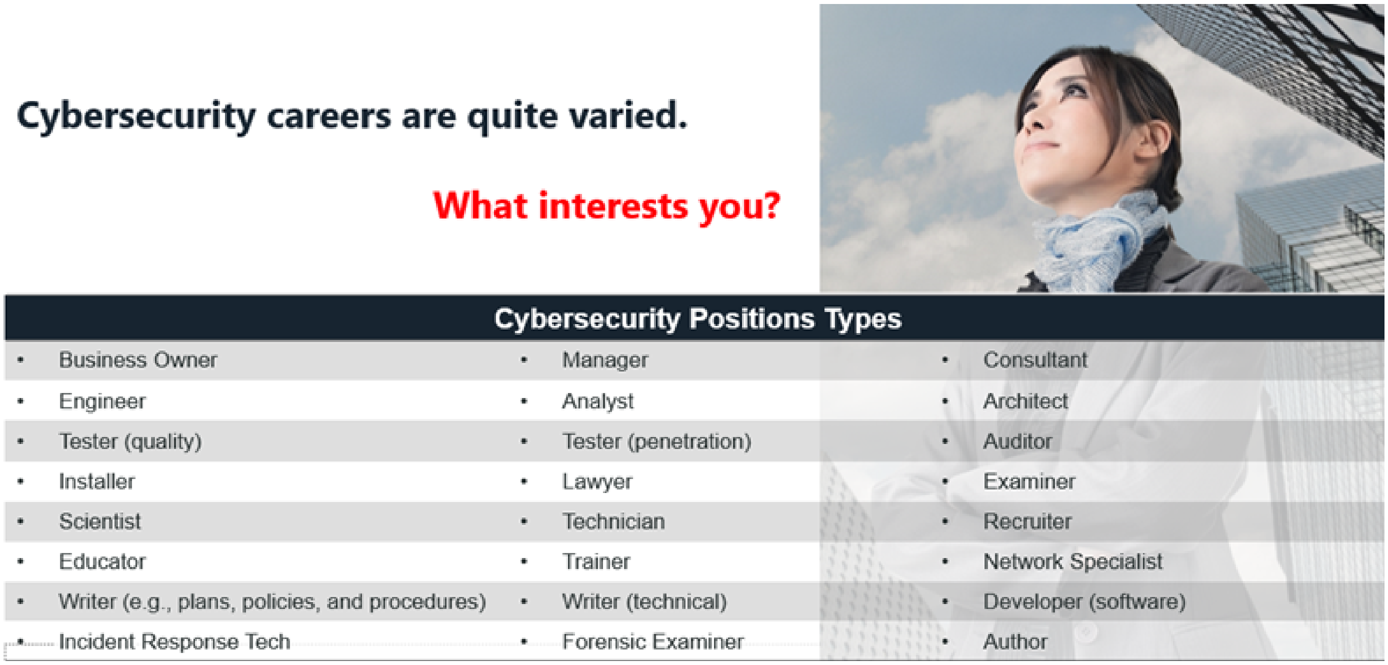
Who Can Benefit from Cyberthreat Data Analysis?

Almost all organizations can benefit from cyberthreat data analysis or threat intelligence. These days the volumes of data and the lack of structure makes it time-consuming and challenging to sort through for untrained individuals. The cybersecurity industry can face many challenges with unconnected systems, the disparity in data, and a lack of skilled professionals. This is why skilled cybersecurity data analysts are very important.

Cyberthreat data analytics that use AI and ML algorithms to create, analyze, and update models can be a strategic solution for businesses. Businesses sometimes use threat data feeds, but they do not know what to do with the extra data. The cyberthreat data analyst is trained to help the organization identify and deal with the threats. New analysts can quickly learn to start helping businesses through study, certifications, and hands-on exposure.

By implementing AI & ML technologies and automating data collection & management solutions, businesses can seal the loopholes in their systems and act immediately. They can also connect the dots by understanding the context of Indicators of Compromise (IoCs) and the tactics, techniques, and procedures (TTP) of cyberthreat agents.

Security agents benefit from cyberthreat data analysis since they can prioritize and filter the threats. Under normal circumstances, they cannot process the alerts and notifications promptly. But with the work of cyberthreat data analysis, security management teams can decide what threats to give priority to the most and act swiftly. They also get access to high-level insights and an overall understanding of the entire threat landscape. It improves other security management aspects, such as fraud prevention, risk analysis, and various security processes, which are all high-level endeavors.



Cybersecurity careers are quite varied.

What interests you?

Cybersecurity Positions Types		
• Business Owner	• Manager	• Consultant
• Engineer	• Analyst	• Architect
• Tester (quality)	• Tester (penetration)	• Auditor
• Installer	• Lawyer	• Examiner
• Scientist	• Technician	• Recruiter
• Educator	• Trainer	• Network Specialist
• Writer (e.g., plans, policies, and procedures)	• Writer (technical)	• Developer (software)
• Incident Response Tech	• Forensic Examiner	• Author

Top Cybersecurity Threats Faced by Organizations in 2020

1. Cloud Vulnerability

A mutual responsibility exists between the cloud service provider (CSP) and the customer company to protect the cloud. Threats include cloud or network intrusion to access confidential data by hacking, insider threat breaches, security breaches, or malware. The risks of using cloud facilities include insecure APIs, IT workers not up to date with the latest security needs and technologies, non-compliance with legislation, locking into a single provider, and losing data due to an event such as a CSP data wipe. Service attack denial, distributed denial-of-service (DDoS) attacks, and crypto-jacking via hacking are other vulnerabilities [10].

2. Machine Learning Poisoning

Machine Learning Poisoning is an attack in which the attacker intentionally "poisons" the algorithm's training information. The purpose of this act is to corrupt the data and weaken the algorithm. The malicious attackers add or generate corrupted data in the machine learning training data to perform poisoning attacks. It changes the perspective of the learned boundaries of an ML program. The algorithm is misinterpreted, which results in incorrect classifications and calculations [10].

3. AI-Enhanced Cyberthreats

Cybercriminals may use AI to assist with the scope and impact of their attacks on social engineering, as an example. Artificial intelligence may learn to spot conduct patterns and figure out how to persuade people that a video, phone call, or email is from a legitimate source. It can then convince them to corrupt networks and provide sensitive data. All the social tactics that cybercriminals are currently using could be developed using AI immeasurably [10].

4. **Deepfakes**

Deepfakes are used to produce fake digital content. Deepfakes refer to manipulated videos created by sophisticated artificial intelligence or other digital representations that generate fake pictures and audio files that appear authentic. The word deep fake is a type of artificial intelligence, combining the words deep learning and fake. Deep learning is a part of AI and refers to an algorithm capable of learning independently and making intelligent decisions. A deep-learning system may create a convincing counterfeit by analyzing photos and videos of a target individual from various perspectives and then mimicking their actions and speech patterns [10].

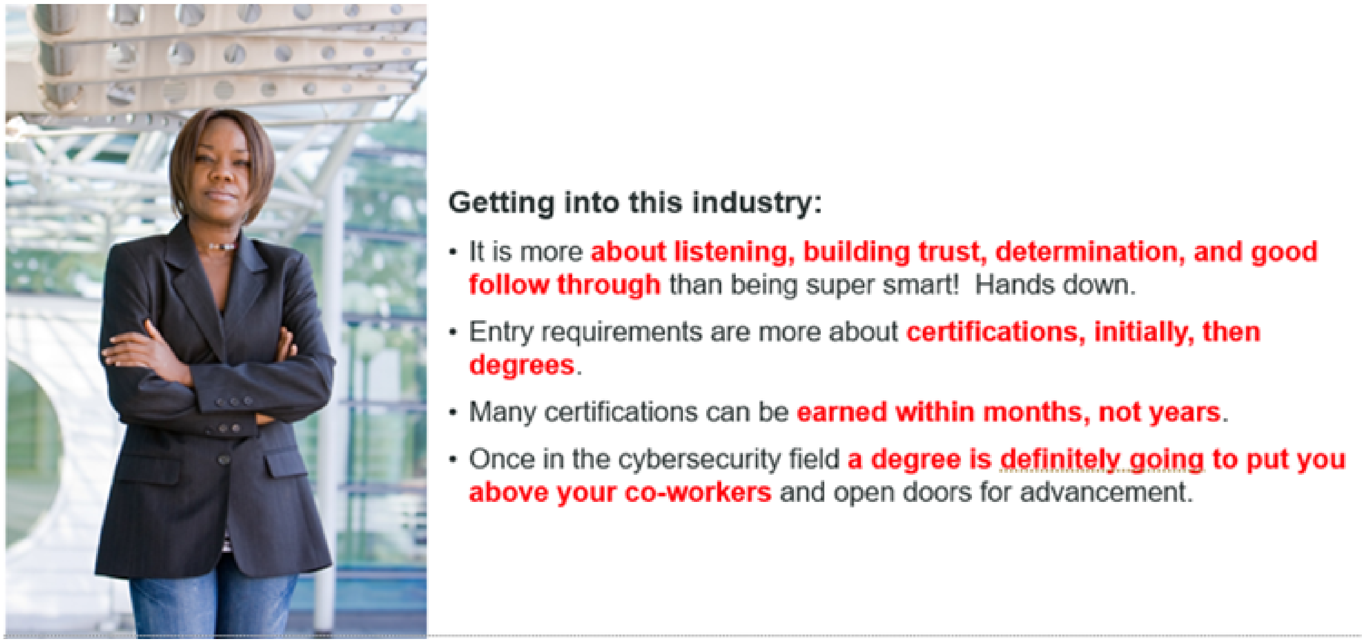
The Australian Department of Foreign Affairs (2017) celebrates women around the world in cybersecurity. Their passion is wonderful. Here is a short clip of the tribute to women: https://youtu.be/C9py3aL_ot8 [11]

Top Cyberthreat Intelligence Tools

Cyberthreat data analysts are using their expertise and these threat intelligence tools to work faster and smarter. In an age where time is of the essence, these cyberthreat intelligence tools make a massive difference in analyzing and combating various threats [12].

- **Authentic8:** It is a cost-effective and lightweight threat intelligent tool for businesses. A visual dashboard is provided where business owners can analyze perceived threats and get detailed reports about the state of their cybersecurity systems. Authentic8 lets its users browse the web in a secure, isolated, cloud-based environment by leveraging Silo for research.
- **Recorded Future:** Recorded Future blends cyberthreat data analysis with human expertise. CISION PR Newswire praised its features and explained how useful it is to collect, detect, and analyze various threats.
- **Threat Connect:** It is a platform that connects threat intelligence, automation, analytics, and templatized workflows to create solutions for handling and managing threats faster. Businesses call it a "productivity hack" because of its features.
- **FireEye:** FireEye improves a business' understanding of risk management and their responses to attacks. Analysts get a comprehensive insight into threat data and intelligence along with detailed reports about past, present, and possible future threats.
- **Forcepoint:** Forcepoint analyzes billions of emails on web traffic intelligence every day and uncovers new trends and threads. It helps businesses stay up-to-date about emerging threats in the cybersecurity landscape and is a growing threat detection database [13].
- **IBM X-Force Exchange:** It is a cloud-based intelligence platform that brings the latest insights and findings from cyberthreat intelligence experts worldwide. It gives organizations the option to collaborate with peers and consult cybersecurity experts, thus helping businesses stay ahead in the game.

How to Become a Cyberthreat Data Analyst?



Getting into this industry:

- It is more **about listening, building trust, determination, and good follow through** than being super smart! Hands down.
- Entry requirements are more about **certifications, initially, then degrees**.
- Many certifications can be **earned within months, not years**.
- Once in the cybersecurity field **a degree is definitely going to put you above your co-workers** and open doors for advancement.

Cyberthreat analysts use reverse engineering techniques to analyze security risks and data threats and capture data to plan and execute different cybersecurity methods.

To become a Cyberthreat Data Analyst for large-scale organizations, enterprises, and start-ups, an individual will require a minimum of a Bachelor's Degree in Computer Science. Taking the Certified Threat Intelligence Analyst (CTIA) course offered by EC-Council is an excellent way to gain the skills needed to step into the industry. Cybrary also has many track programs online with specializations in Cybersecurity and Network Systems, which are valuable to beginners.

First, whatever your fears and hurdles are…

FIGHT TO GET OVER THEM!

Mondo (2019) reports:

- CISOs
  = $175,000 – $275,000
- Information security managers
  = $120,000 – $185,000
- Application security engineers
  = $120,000 – $182,500
- Network security engineers
  = $115,000 – $172,500
- Cybersecurity engineers
  = $110,000 – $165,000

Conclusion

Cyberthreat data analysis is a continuous process where analysts review threats and identify changes in environments. It is imperative to involve different representatives from an organization to participate in the analysis process due to a threat's subjective nature. As the organization grows, the nature of threats will change, and the process of analysis will go through another cycle again. Periodic threat analytics is recommended to make sure new threats and their detection mechanisms are included in existing systems. A review of the securities, policies, and compliance measures should be accounted for, making sure it aligns with the practices of threat intelligence tools and solutions.

Examining cyberthreats is a continuous process that should be conducted regularly to ensure that security measures operate efficiently. Technology and other factors that influence cyberspace are rapidly evolving, such as political factors, social factors, etc. Organizations that do not conduct risk and risk analysis are left exposed to cyber pest attacks that will forever harm the company. Threat intelligence can provide insight into the third-party threat environments the organization works with, provide real-time updates on threats and risk shifts, and provide the information needed to make necessary changes in the security practices.

Technology alone cannot solve all cyberthreat data analysis problems. The human element will be involved and used in tandem with AI and ML technologies. Using sound judgment, having a keen eye for detail, critical thinking skills, and technical expertise are qualities expert cyberthreat data analysts should possess. In essence, analysts should put themselves in the attacker's shoes and figure out how to design solutions for these threats. Because that is what organizations are paying good money for. Next-gen cyberthreat data analytics will leverage scalable Big Data analytics solutions with AI technology and anomaly detection to deal with emerging threats.

Time to upgrade your "Apps."

Getting into cybersecurity is not hard.

"app" 1: Earn a certificate

"app" 2: Network with others

"app" 3: Get some experience

"app" 4: Advance with a degree

"app" 5: Stay knowledgeable

"app" 6: Encourage others

References

1. https://bricata.com/blog/cybersecurity-salary-surveys/

2. https://www.census.gov/programssurveys/acs/guidance/comparing-acs-data/2015.html

3. https://www.youtube.com/watch?v=jelvfj-fGI4&feature=emb_logo

4. https://blog.eccouncil.org/what-is-cyber-threat-analysis-and-its-components/

5. https://resources.infosecinstitute.com/topic/cyber-threat-analysis/

6. https://safetymanagement.eku.edu/blog/the-5-steps-of-threat-analysis/

7. https://www.sciencedirect.com/topics/computer-science/threat-analysis

8. https://cyberexperts.com/cyber-threat-analysis-a-complete-overview/

9. https://www.eccu.edu/women-wanted-benefits-of-cybersecurity-careers/

10. https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020

11. https://youtu.be/C9py3aL_ot8

12. https://www.youtube.com/watch?v=8Q7pkNHhfHc

13. https://www.forcepoint.com/cyber-edu/threat-intelligence

14. https://mondo.com/pre-order-2019-dm-it-salary-guide/

EC-Council