2022

# Strategies Using Threat Intelligence to Detect Advanced Persistent Threats: A Qualitative Case Study

Melisa A. Joyner
*Walden University*

# Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Melisa Joyner

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Gary Griffith, Committee Chairperson, Information Technology Faculty
Dr. Cesar Casas, Committee Member, Information Technology Faculty
Dr. Bob Duhainy, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2022

Abstract

# Strategies Using Threat Intelligence to Detect Advanced Persistent Threats: A Qualitative Case Study

by

Melisa A. Joyner

MSIT, Walden University, 2019

M. Ed, Wayland Baptist University, 2013

BSOE, Wayland Baptist University, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

September 2022

# Abstract

Advanced persistent threats (APTs) targeting critical infrastructures can adversely impact human lives. Cyber security analysts are concerned with APT attacks because they make it challenging to defend critical infrastructures. Grounded in routines activity theory (RAT), the purpose of this qualitative exploratory multiple case study was to explore strategies cybersecurity analysts use to defend critical infrastructures from APT attacks. Data were collected through interviews with 8 participants and documents from two organizations. Participants were required to have experience analyzing network traffic on a critical infrastructure network, one year of cyber threat hunting experience, prior or current knowledge of cyber threat intelligence (CTI) and reside in the Southwestern and Northeastern United States.  Through thematic analysis, four themes emerged: (a) CTI and threat hunting are part of the defense-in-depth strategy, (b) the lack of standards on CTI and threat hunting has created numerous challenges, (c) CTI informs threat hunting, and (d) threat hunting consists of looking at behaviors, not IOCs. A key recommendation is for cyber security analysts to enhance their defense strategies by incorporating threat hunting and cyber threat intelligence into their playbooks. The implications for positive social change include the potential to protect critical infrastructures and support the local community welfare.

# Strategies Using Threat Intelligence to Detect Advanced Persistent Threats: A Qualitative Case Study

by

Melisa A. Joyner

MSIT, Walden University, 2019

M. Ed, Wayland Baptist University, 2013

BSOE, Wayland Baptist University, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

September 2022

# Dedication

I would like to dedicate this research to the loving memory of my grandmother. She always encouraged me to pursue my dreams. I also want to dedicate this research study to my colleagues and fellow threat hunters. Thank you for helping me to fly and supporting me when I could not. May you continue to lead the way through innovation.

# Acknowledgments

I want to thank my husband for always supporting me, my mentors always encouraging me, and God always giving me the strength I need. I would also like to thank Dr. Desi. Dr. Desi listens to his patients, shows compassion, and he helped me overcome lots of pain. I also want to thank my chair, Dr. Griffith, for helping me during my journey.

Table of Contents

# List of Tables

## List of Figures

# Section 1: Foundation of the Study

Critical infrastructures have become the focus of advanced persistent threats (APTs). APTs target the infrastructures for their data. Many defense strategies do not focus on the APTs’ behavior to protect the networks. APTs' ability to access networks and the data on the networks create a threat to national security, intellectual property, and finance (Holt et al., 2018). President Biden signed the Executive Order on Improving the Nation’s Cybersecurity in May 2021 (Cybersecurity & Infrastructure Security Agency, 2021b). The three key points from the executive order related to this study include (a) removing barriers to increasing threat information sharing, (b) creating a standard incident response playbook, and (c) improving incident detection, forensic analysis, and incident remediation (see Cybersecurity & Infrastructure Security Agency, 2021b).

My goal for this qualitative exploratory multiple case study was to explore cybersecurity analysts' cyber threat intelligence strategies to defend critical infrastructures from APT attacks. Section 1 includes the foundation of the study, the background of the problem, the nature of the study, the research question, the interview questions, the conceptual framework, the operational definitions, the assumptions, limitations, and delimitations, the significance of the study, a review of professional and academic literature, and a transition to Section 2. I focused on routine activities theory (RAT), APTs, and cyber threat intelligence (CTI) in the literature review. The targeting criteria of the victim was the focus of the RAT overview. The research on APTs included the complexity of cybercriminal groups and notable breaches. Finally, the review of CTI focused on various strategies and types of CTI.

## Background of the Problem

Evolving information technology infrastructures introduce challenges that prevent traditional network security from adequately protecting the environment (Chen et al., 2018). In 2018, cybercrime reached $600 billion, according to McAfee (Amin et al., 2021). Many governments and companies have been targeted and breached by APTs, a type of advanced cybercriminals (Chen et al., 2018). Protection from APT attacks is complicated. Cybercriminals use advanced malware for espionage, destruction, and profit (Alenezi et al., 2020). Cybersecurity analysts face continuous challenges in detecting and countering APT attacks (Han et al., 2021). The average endpoint infection time is 145 days; however, some endpoints were infected for up to 660 days (Chen et al., 2018). The SolarWinds attack impacted 18,000 public and private sector businesses, including multiple United States government agencies (Cybersecurity & Infrastructure Security Agency, 2021c).

Russian APT attacks, such as the SolarWinds compromise, pose a grave risk to critical infrastructure agencies (Cybersecurity & Infrastructure Security Agency, 2021c). Critical infrastructures are targets for cyber-attacks (Pleta et al., 2020). Some of the infrastructures targeted include energy, water dams, financial networks, healthcare, and communication (Pleta et al., 2020). The infrastructures rely on cyber assets to ensure the services are always available (Robinson et al., 2018). Cyber-attacks on organizations can damage their reputation, interrupt services, and have severe economic costs (Vanni, 2019). These attacks can also lead to blackouts, impacts on drinking water, decreased travel security, and loss of economic stability (Robinson et al., 2018). Cyber-attacks can also cause physical damage, harm the environment, and impact the lives of humans, thereby violating human rights (Pleta et al., 2020; Robinson et al., 2018). Most organizations cannot respond to these attacks (Pleta et al., 2020). Additionally, the amount of people with specialized and advanced skills to defend networks against APTs is low (Robinson et al., 2018). Cyber-attacks are viewed as cyber warfare because militaries include cyberspace in their warfighting domains (Robinson et al., 2018).

## Problem Statement

The adversary group, APT10, is responsible for stealing personally identifiable information (PII) of over 100,000 United States Navy (USN) personnel (Federal Bureau of Investigation, 2018). The USN networks are part of the designated 16 critical infrastructure sectors (Cybersecurity & Infrastructure Security Agency, 2021a). Critical infrastructures are targets of cyberattacks (Department of Homeland Security, 2019). In 2020 cyber security incidents increased across all critical infrastructures (Goettl, 2021). Threat actors used the opportunities presented during the COVID-19 pandemic to target vulnerable entities (Goettl, 2021). The defense of critical infrastructures is necessary as people depend highly on them for their livelihood (Safa et al., 2018). The general IT problem is a lack of knowledge to defend critical infrastructures against APTs. The specific IT problem is that some cybersecurity analysts lack cyber threat intelligence strategies to defend critical infrastructures from APT attacks.

## Purpose Statement

The purpose of this qualitative exploratory multiple case study was to explore the cyber threat intelligence strategies that cybersecurity analysts use to defend critical infrastructures from APT attacks. The targeted population group included cybersecurity analysts with at least 1 year of cyber threat hunting experience in the Southwestern and Northeastern United States. The implications for social change include the potential to prevent data breaches, financial loss due to stolen credentials, loss of social security numbers, and reduced phishing attacks.

## Nature of the Study

The method most appropriate for this study was qualitative. Qualitative research shows how events are related or a specific phenomenon occurs (Maxwell, 2019). Peterson (2019) stated that the reason to complete qualitative research is to observe behaviors, examine data, and analyze data narratively. A qualitative research design was appropriate for this study because I explored cyber threat intelligence strategies to defend critical infrastructures from APT attacks. Quantitative research relies on assumptions based on statistics and data analysis (Nimon, 2011). Data analysis for quantitative research uses statistical testing (Nimon, 2011). Quantitative research requires data appropriate for the measurement tool among variables (Nimon, 2011). Quantitative research was not applicable because I did not use statistical tests to validate the findings. Mixed methods include both quantitative and qualitative research ideas, data, and analysis to provide a new understanding of a complex research question (Plano Clark, 2019). Mixed-method research was inappropriate for this study because I did not use a quantitative research method.

The qualitative research design most appropriate for my research was an exploratory multiple case study. I used an exploratory multiple case study to achieve the goal of gaining an in-depth understanding of the phenomenon of cyber threat intelligence. The phenomenological design focuses on the experiences of individuals who lived through a specific phenomenon or event (Kafle, 2013). I did not focus on a particular event; therefore, the phenomenological design was inappropriate. Ethnography researchers use situations and behaviors to describe the research study participants' experiences, attitudes, beliefs, thoughts, and reflections (Marcen et al., 2013). I did not focus on the participants' culture; therefore, ethnography was not the right design. Participants' stories and experiences are collected for study in narrative research (Moen, 2006). The narrative design was inappropriate as the study was not a biography of the participants. Case studies focus on collecting evidence to understand the activity or process (VanWynsberghe & Khan, 2007). I used a case study design to develop an in-depth understanding of cyber threat intelligence strategies used to defend critical infrastructures. My goal was to understand the current strategies used to defend critical infrastructures, not develop a new theory.

## Research Question

What cyber threat intelligence strategies are cybersecurity analysts using to defend critical infrastructures from APT attacks?

### Demographic Questions

1. What is your current title and role?
2. What role do you play in defending critical infrastructures?
3. How many years of experience do you have in cybersecurity?
4. What is your threat hunting experience?

## Interview Questions

1. What is your experience with cyber threat intelligence?
2. What does cyber threat intelligence mean to you?
3. How do you hunt for APTs on the networks that you defend?
4. Which hunting methods were more successful?
5. What are the successful strategies you have employed to defend critical infrastructures from attacks by APTs?
6. How do you use cyber threat intelligence to defend critical infrastructures from attacks by APTs?
7. What impact has cyber threat intelligence had on hunting for APTs on networks?
8. What factors play a role in the decision of how to implement cyber threat intelligence to defend critical infrastructures from attacks by APTs?
9. What are some obstacles or challenges to using cyber threat intelligence to hunt for APTs and defend critical infrastructures from APT attacks?
10. What are your experiences surrounding the challenges of using cyber threat intelligence to defend critical infrastructures from attacks by APTs?
11. How do you improve the success rate of finding APTs on networks?
12. What other factors or tactics would you like to add for using cyber threat intelligence to defend critical infrastructures from attacks by APTs?

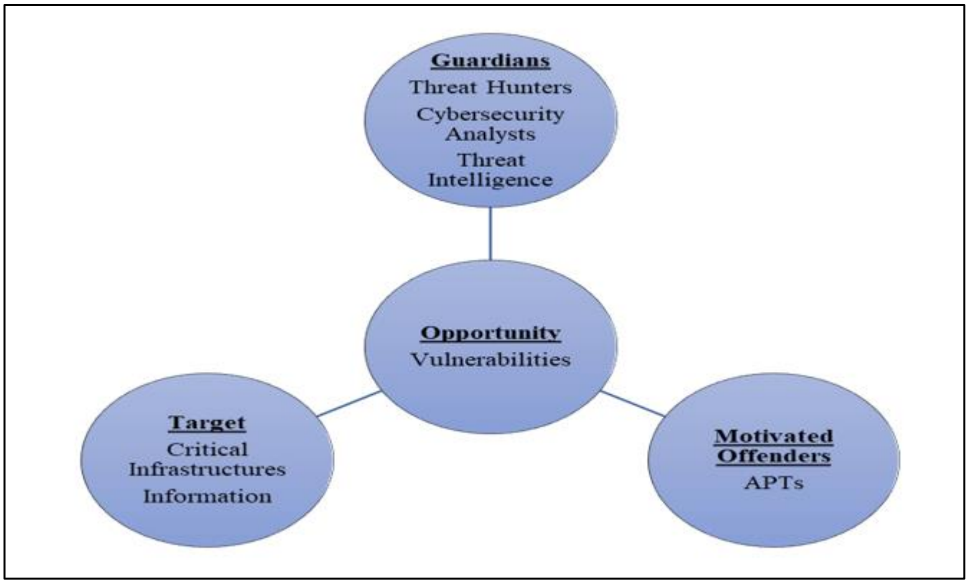
## Theoretical or Conceptual Framework

The theory that I used to support this study was routine activity theory (RAT). RAT was published in 1979 by Cohen and Felson. Cohen and Felson (1979) defined routine activities as activities that an individual or population performs regularly. These routine activities affect the crime rate by influencing criminal opportunity (Cohen & Felson, 1979). In RAT, crime occurs when three conditions overlap, a motivated offender, a suitable target, and the lack of a guardian (Jansen & Leukfeldt, 2016). RAT occurs when guardians are limited, but the adversary is interested in a target (Vakhitova et al., 2016).

As applied to the study, the opportunity (vulnerability) occurs when the motivated offender (APTs) seeks the data on networks (target), and there is a lack of guardians (cybersecurity analysts). I explored the strategies using cyber threat intelligence to reduce the opportunity (vulnerability) by increasing the guardians' knowledge to defend critical infrastructures (target) from APT (offender) attacks.

**Figure 1**

*Routine Activities Theory and APT Attacks*



## Definition of Terms

I discuss cyber threat intelligence strategies used to defend critical infrastructures from APTs. The following definitions are for terms that I used throughout the study.

*Advanced persistent threat (APT).* A threat actor that continually transforms using persistence, metamorphosis, and obfuscation to perform targeted attacks with multiple attack vectors to gain unauthorized and undetected access and control of the target systems for an extended period so that organizations are affected negatively through the exfiltration of confidential information, creating access for future attacks amongst others (Ishaya et al., 2021).

*Critical Infrastructures.* Assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health, or safety, or any combination thereof (Cybersecurity & Infrastructure Security Agency, 2021).

*Cyber threat intelligence (CTI).* Enables proactive response to attacks by correlating trends and analyzing cyberattacks to predict future attack patterns based on current data (Gong & Lee, 2021).

*Tactics, techniques, and procedures (TTPs).* The behavior of threat actors in cybersecurity. The tactics describe the objectives behind the activity, the techniques are how the objectives are achieved, and the procedures are the process of implementing a technique for the objective (Egloff & Smeets, 2021)

*Threat hunting.* The use of proactive threat intelligence-driven defense to reduce the attack scope and impact on the network by identifying previous and ongoing unknown cyber-attacks and threats while gaining a deeper understanding of the environment (Anstee, 2017; Bromiley, 2019).

## Assumptions, Limitations, and Delimitations

### Assumptions

Assumptions are perceptional and cognitive biases based on the individual's beliefs (Walsh, 2015). Assumptions fill the knowledge gaps and are accepted as accurate without proof (Weisman et al., 2020). I made several assumptions for my research. My first assumption was that some cybersecurity analysts use cyber threat intelligence to defend their networks. My second assumption was that the cybersecurity analysts would answer truthfully during interviews. My third assumption was that the participants or the researcher would not introduce bias that would impact the research. My final assumption was that cybersecurity analysts who use cyber threat intelligence made up a smaller percentage of information technology and cybersecurity industries. After validation, assumptions may turn into facts (Weisman et al., 2020). I used semistructured interview questions and member checking to mitigate my assumptions and validate each interviewee's responses.

## Limitations

Limitations are imperfections of the study that have no impact on the validity of the findings (Busse et al., 2016). There were several limitations in this study. The commercial sector discusses threat hunting, however, the academic or peer-reviewed side does not. Second, threat hunters have various names in the industry. Third, each organization in the case study uses multiple forms of threat intelligence at different levels.

## Delimitations

Delimitations are the constraints placed on the study to shape the research contextually and analytically (Svensson & Doumas, 2013). The interview pool, or the population sample, was in the Southwestern and Northeastern United States for this study. The population included participants who currently work in a critical infrastructure security operations center as defined by the Department of Homeland Security. Additionally, I did not consider participants without knowledge of threat intelligence or threat hunting experience.

## Significance of the Study

### Contribution to Information Technology Practice

Security controls are failing, and adversaries can steal and destroy data. Organizational leaders seek to minimize the loss of data. The study is significant to information technology practice because it may offer the community the knowledge to use cyber threat intelligence for defending networks from APT attacks. CTI can help find the adversary and reduce data loss. Cybersecurity teams can use CTI to understand APT behaviors to identify defensive techniques that protect networks against adversaries and prevent future attacks. Raju and Geethakumari (2016) discussed event correlation helping cybersecurity analysts identify the incident's source and scope. Cybersecurity analysts can use the information from the root cause to implement security controls after a breach (Raju & Geethakumari, 2016). Cybersecurity analysts can use CTI to proactively implement security controls and updates to reduce vulnerabilities on the network, preventing an opportunity for APTs to steal data.

### Implications for Social Change

Computers are an essential part of life that stores readily available and valuable information (Alenezi et al., 2020). According to Hsieh and Wang (2018), 89% of people in the United States use the internet daily. Internet use includes communications, information distribution, entertainment, education, business investment, and transaction (Hsieh & Wang, 2018). The loss or destruction of that data affects society. The implications for positive social change could include reducing data breaches and better protection of critical infrastructures, such as military networks, medical systems, financial sectors, and industrial control systems (ICS). The ability to use cyber threat intelligence as a defense strategy to protect networks from APT attacks may (a) reduce power outages, (b) prevent the closure of fuel pipelines and meat factories, (c) reduce personal identifying information from being stolen during data breaches, (d) prevent of death in patients wearing medical devices, (e) reduce money stolen from financial institutions, and (f) the protection of online learning through academic institutions.

## A Review of the Professional and Academic Literature

Cyber threat intelligence is critical to protecting critical infrastructures from APTs (Anstee, 2017). Identifying vulnerabilities and threats before adversaries attack the network can prevent data breaches from occurring. Threat intelligence is useful in detecting and preventing attacks by including detailed information about current or possible threats (Han et al., 2021).

I used a qualitative case study to explore cybersecurity analysts' cyber threat intelligence strategies to defend critical infrastructures from APT attacks. I used the research question and purpose to guide the literature review. I focused the professional literature review on APTs, CTI, and RAT. My focus of the RAT overview was targeting the criteria of the victim. The research on APTs included the complexity of cybercriminal groups and notable breaches. Finally, in my review, I discuss various strategies and types of CTI.

I researched multiple databases for 36 months, reviewing scholarly and peer-reviewed content. Additional publications that I reviewed are from the Federal Bureau of Investigations (FBI), the National Institute of Standards and Technology (NIST), and the

SysAdmin, Audit, Network and Security (SANS) Institute. I looked for specific terms such as threat hunting, APTs, and threat intelligence platforms. My literature review identified a lack of scholarly and peer-reviewed data on CTI strategies to defend critical infrastructures from APT attacks.

I used the Ulrich database to verify the peer-reviewed status. Of the 62 sources I reviewed, 60 were peer-reviewed, five were government sources, and 52 were published within the 5 years of the anticipated approval of my doctoral study. I focused on sources published in 2017 or later to maintain the 5-year requirement. However, some historical sources and supporting references for the theories and frameworks may be over five years. I used Google Scholar, ScienceDirect, and the Walden University Library to find relevant sources.

## Routine Activity Theory (RAT)

Cohen and Felson (1979) published RAT in 1979 to explain why crime occurs. Criminologists use RAT to correlate risk factors with the victimization of a crime (Holt et al., 2018). As Cohen and Felson (1979) defined, routine activities are the reoccurring activities that influence criminal opportunity. The Internet is an essential part of people’s routines worldwide due to its availability (Hsieh & Wang, 2018). According to Cohen and Felson (1979), routines are the activities that provide the population with necessities either at home or away from home. The routines individuals engage with correlate to an offender's risk of being victimized (Hawdon et al., 2020). Three conditions must overlap: a motivated offender, a suitable target, and the lack of a guardian (Jansen & Leukfeldt, 2016; Pratt & Turanovic, 2016). If one condition can be removed from the equation, then victimization will not occur (Pratt & Turanovic, 2016). Cohen and Felson applied the three conditions to physical crime, but RAT has been applied to crime in cyberspace (Holt et al., 2018).

An offender is someone with an inclination for crime and the ability to commit the crime (Cohen & Felson, 1979). Motivation explains the offender's behavior and can be extrinsic or intrinsic (Safa et al., 2019). In this study, I focused on APTs as the motivated offender. Holt et al. (2021) used the Jihadi threat group as their motivated offender. The threat actor's motivation can impact the selection of the target (Holt et al., 2021). Safa et al. (2018) noted that motivation and opportunity are crucial to information security violations.

A suitable target is anything the motivated offender wants or needs and serves as a function of VIVA (Hawdon et al., 2020). VIVA is the target's value, inertia, visibility, and access (Hawdon et al., 2020). Value is the worth of the target to the offender (Hawdon et al., 2020). Critical infrastructures have data that may be valuable to APTs. Inertia can reduce contact with the offender and may influence the value (Hawdon et al., 2020; Holt et al., 2021). Leukfeldt and Yar (2016) pointed out that files and technology are a form of inertia because the offender can determine their target's suitability based on the security controls in place. Visibility is the ability to be seen by the offender (Hawdon et al., 2020). Access is the offender's opportunity for the crime (Hawdon et al., 2020). Holt et al. (2021) pointed out that the target's visibility and accessibility may increase after a successful attack. The vulnerabilities of the online devices provide the offenders the accessibility to perform online attacks (Leukfeldt & Yar, 2016).

The internet diminishes the geographic distance for the attackers and is always available, creating an abundance of targets and opportunities (Holt et al., 2020). The offender must have the desire and ability to commit the crime on the intended target (Holt & Bossler, 2013). Guardians reduce the likelihood of the offender attacking the target (Hawdon et al., 2020). RAT occurs when guardians are limited, but the adversary is interested in a target (Vakhitova et al., 2016). The lack of guardianship does not mean the victim is conducting risky activities (Pratt & Turanovic, 2016). Cohen and Felson proposed that offenders are omnipresent, which also applies to cyberspace (Hawdon et al., 2020). Hawdon et al. (2017) identified that RAT applies to cyberspace. They stated that contact between the victim and the offender can occur asynchronously through network devices (Hawdon et al., 2017). The availability of the internet provides numerous opportunities and targets for motivated offenders (Hsieh & Wang, 2018).

Felson proposed that guardianship is the presence of a person to deter crime (Hawdon et al., 2017). However, Hawdon et al. (2017) stated that guardianship for cyberspace includes hardening the target using firewalls, antivirus programs, filtering, and blocking. Hsieh and Wang (2018) stated that cyber guardianship is formal and informal and includes the users, administrators, firewalls, antivirus, those who monitor the network, and security software. They stated that it is also crucial for those who observe the network to detect the adversary and intervene against offenders (Hsieh & Wang, 2018). Hollis et al. (2013) defined guardians as the people whose proximity and presence create challenges for the criminal acts to occur on specific targets. Security controls can reduce the attack surface but cannot eliminate the likelihood of being targeted (Holt & Bossler, 2013). However, security controls fall into the areas of target hardening and target suitability instead of guardianship, according to Hollis et al. (2013). Additionally, Reynald stated that the action of guardianship is observed through availability, supervision, monitoring, and intervention activities (Hollis et al., 2013). For this study, the cyber analysts or the cyber threat hunters fall into this category.

Cybercriminals can remain invisible and anonymous due to the vast space and lack of adequate guardianship in cyberspace (Hsieh & Wang, 2018). Victims often do not realize when they have been targeted in cyberspace because the adversary can hide in plain sight (Holt & Bossler, 2013). However, the system functions, even with antivirus programs (Holt & Bossler, 2013).

RAT analyzes multiple types of criminal behavior and has been used to help understand cybercrime (Hsieh & Wang, 2018; Leukfeldt & Yar, 2016). Holt et al. (2021) used RAT to examine Jihadi cyberattacks. Multiple empirical tests were validated using RAT with cybercrime (Holt et al., 2021). Cybercrime is a type of crime that relies on technology to perform illegal actions (Leukfeldt & Yar, 2016). It includes various illicit activities such as hacking, malware, piracy, fraud, bullying, and sexual victimization (Leukfeldt & Yar, 2016). Malware enables cybercriminals to target many systems at once to gather sensitive information and gain an economic advantage (Holt et al., 2018). Holt et al. (2020) identified that academic research and criminal justice policy focus on profit-driven hacking. They recognized the need to understand the behavior of cybercriminals to defend against future attacks (Holt et al., 2018). APTs are sophisticated cybercriminals who repeatedly pursue specific objectives and overcome the defense (Joint Task Force, 2020). APTs perform espionage and sabotage specific targets during a planned cyber-attack (Alenezi et al., 2020).

I explored the strategies that use cyber threat intelligence to reduce the opportunity (vulnerability) by increasing the guardians' knowledge to defend critical infrastructures (target) from APT (offender) attacks. I used RAT in this study to focus on the guardianship strategies to protect critical infrastructures. As applied to the study, the opportunity (vulnerability) occurs when the motivated offender (APTs) seeks the data on networks (target), and there is a lack of guardians (cybersecurity analysts).

## Supporting Theories

I reviewed multiple crime prevention theories before I chose RAT. Crime prevention theories focus on reducing criminal activities (Safa et al., 2018). I did not concentrate on motivation theories based on human emotions, which did not apply to APTs. Crime prevention theories focus on reducing the opportunities for a crime to occur (Padayachee, 2016).

### *Rational Choice Theory (RCT)*

Rational choice theory (RCT) focuses on the offender's perspective to understand the reason for a crime (Jeong & Zo, 2021). According to RCT, two conditions must be met for a crime to take place (a) motivation for the crime and (b) low risk of being captured for the crime (Jeong & Zo, 2021). Kranenbarg et al. (2018) used rational choice theory (RCT) to explore whether a researcher will sell vulnerabilities to the underground market or report vulnerabilities to a legal bug bounty program. The RCT implies that a person commits a crime for financial gain (Paternoster et al., 2017). The chances of receiving punishment for the crime are low (Paternoster et al., 2017). Additionally, the person can be motivated by the payout for others (Paternoster et al., 2017). In cybercrime, the rate of capturing the criminals and the severity of punishment is low (Kranenbarg et al., 2018). People choose offensive actions because of the availability, costs, and returns (McCarthy, 2002). McCarthy (2002) argued that rational choice is premeditated; however, Lenine (2020) argued that choice is an impulse, not a process. RCT focuses on the criminal's motivation, not the guardian. Therefore, I did not choose RCT for this study.

### *Crime Pattern Theory*

Crime pattern theory includes multiple theories, including RCT, RAT, and the geometric theory of crime (Hewitt et al., 2020). In crime pattern theory, crime occurs when the known environment merges with an opportunity (Paraskevas & Brookes, 2018). Crime pattern theory proposes that similar crimes present the same patterns while focusing on the offender and victims (Hewitt et al., 2020; Quick et al., 2018). The theory identifies patterns of criminal activities by focusing on the convergence of offenders and victims in a specific environment that lacks guardians (Paraskevas & Brookes, 2018). The offender chooses crime when the benefit outweighs the cost (Hewitt et al., 2020). Motivated offenders are enticed by the locations (Quick et al., 2018). Criminals gather information about the environment through legitimate daily activities (Paraskevas & Brookes, 2018). Each environment generates different opportunities for the criminal (Kim & Hipp, 2018). Opportunities are more significant in the location where the victims and offenders spend the most time (Hewitt et al., 2020). The criminal’s chance of detection depends on the location's boundaries and guardianship (Kim & Hipp, 2018).

Additionally, the offender responds to environmental cues for the area (Quick et al., 2018). Paraskevas and Brookes (2018) discussed that the lack of guardians at each point of contact between the criminal and the victim provides more opportunities for crime to occur. Crime pattern theory focuses on the opportunities that the specific location creates. While critical infrastructures have many opportunities through their vulnerabilities, this study focused on enhancing guardianship to prevent future cyber-attacks.

### ***Situational Crime Prevention Theory (SCPT)***

Ronald Clarke (1980) published situational crime prevention in 1980 as a strategy to prevent crime. Situational crime prevention theory (SCPT) focuses on reducing the opportunities and motivation to commit a crime through practical implementations instead of using policies (Freilich & Newman, 2018; Safa et al., 2018). The goal of SCPT is to develop an environment that organizations can use to reduce crime (Safa et al., 2018). Jeong and Zo (2021) stated that opportunity is the root cause of crime. Clarke stated that crime is controlled by “regulating and controlling crime opportunities” (Freilich & Newman, 2018, p. 11). Reducing opportunity is common in reducing criminal acts (Safa et al., 2019). The environment would make it difficult for criminals to exploit the vulnerabilities (Safa et al., 2018). Jeong and Zo (2021) identified environmental conditions that needed to be eliminated to reduce insider attacks. The environment needs to (a) increase the effort needed for a crime, (b) increase the risks of the criminal act, (c) fewer rewards from the crime, and (d) removal of excuses (Jeong & Zo, 2021). Safa et al. (2018) used SCPT to reduce insider threat to networks by identifying the relationship that reducing the motivation and opportunity has on the attitude of an insider threat. Jeong and Zo (2021) also used SCPT to minimize the chance of insider threat. Safa et al. (2019) used situational crime prevention theory to reduce “misbehavior” in information security. SCPT proposes that the effort to commit a crime and the risk increase while the rewards, provocations, and excuses are reduced or removed (Padayachee, 2016; Safa et al., 2018).

Padayachee (2016) determined that SCP was ineffective for insider threats based on his research on information security and SCPT. Freilich and Newman (2018) identified that international regulations impact the possible controls for an organization to implement to reduce cybercrime. SCPT is most effective when strategies for reducing crime occur at a macro-level at every location (Freilich & Newman, 2018). SCP reduces the opportunities for criminal acts to occur. The current study aimed to provide strategies of guardianship for critical infrastructures. APTs are advanced adversaries that governments hire to exploit existing opportunities (vulnerabilities) or develop new opportunities (Lemay et al., 2018). Therefore, I did not apply SCPT to my study.

### Analysis of Potential Themes and Phenomena

During my research, I used several potential themes to guide the path to a deeper understanding. I centered the themes around the selected theory. The themes included APTs (offenders), opportunities APTs have used, critical infrastructures (target), and threat intelligence used by cybersecurity analysts or threat hunters.

### *APT*

The term "advanced persistent threat" was initially patented in 2007 and published in 2008 (Ahmad et al., 2019). APTs use targeted and malicious attacks with multiple stages and strategies (Cho & Nam, 2019). The multiple attack vectors can be physical, deceptive, or cyber (Joint Task Force, 2020). APTs are sophisticated and can be undetected for an extended period (Tounsi & Rais, 2018). APTs use malware that bypasses security infrastructure by exploiting the network's vulnerabilities (Ishaya et al., 2021). Funding and training are provided for APTs to carry out the organization's objectives (Ahmad et al., 2019). The primary targets of APTs include targeted critical infrastructures, such as military, financial, industrial control systems (ICS), and medical infrastructures (Cho & Nam, 2019). APTs have been reported in financial crime, political espionage, industrial espionage, and influencing elections (Ahmad et al., 2019; Lemay et al., 2018). Organizations exploited include Sony, Citigroup, RSA Security, NASA, FBI, and Fox Broadcasting (Ishaya et al., 2021). Another group that APTs target includes telecommunication organizations, government organizations, and other organizations tied with defense (Ahmad et al., 2019).

Documentation for APT research is maintained mainly through open-source and academic publications (Lemay et al., 2018). APT groups, malware attacks, and campaigns have various naming conventions because open-source research groups do not agree on a standard naming (Lemay et al., 2018). The evolving information technology infrastructures introduce challenges that prevent traditional network security from adequately protecting the environment (Chen et al., 2018). Many governments and companies have been targeted and breached by the APTs (Chen et al., 2018). Protection from APT attacks is complicated. There is not a single technology solution to solve the problem; instead, different technologies must be combined to protect various areas of the network (Chen et al., 2018). APTs can stay on networks for long periods without being detected (Amin et al., 2021). The average endpoint infection time is 145 days; however, some endpoints have been infected for up to 660 days (Chen et al., 2018).

APTs will continually perform actions over an extended period to meet their objectives while adapting to the network defenses to maintain a foothold to achieve them (Chen et al., 2018). They are exceptionally skilled at their tradecraft and motivated (Amin et al., 2021). APTs avoid detection methods by deceiving security software (Cho & Nam, 2019). APTs create customized tools for the targeted environment to attain a foothold (Chen et al., 2018). Objectives for APTs include attaining specific data on specific networks for destruction or exfiltration (Cho & Nam, 2019).

Nation-state espionage groups, a type of APTs, perform large-scale breaches (Lemay et al., 2018). The groups target the networks because the gain or rewards from the target outweighs the punishment for the crimes (Hsieh & Wang, 2018). The ability to profit, influence, exploit, and facilitate military actions motivate APTs (Ahmad et al., 2019). The targeted systems have information that the APTs will sell, sabotage credibility, or disrupt the organization (Cho & Nam, 2019). Attacks on cyber can influence diplomacy and war (Brantly, 2014). Covert cyber-attacks are sometimes conducted because the leader benefits from the attack, but the state does not (Brantly, 2014). Covert actions, such as cyber-attacks, can change international relationships and help various governments (Brantly, 2014). The actions of the cyber-attack range from information operations to swaying opinions to the destruction of critical infrastructure (Brantly, 2014). The use of state-sponsored cyberattacks leads to the achievement of political objectives (Brantly, 2014). The economic impact of the cyberattacks is unknown (Vanni, 2019). Damages can include loss of service, data theft, and loss of reputation (Vanni, 2019).

### *Target*

APTs use their attacks to collect intelligence and exfiltrate data (Amin et al., 2021). Types of organizations breached include health insurance companies, entertainment groups, critical infrastructures, and democratic institutions (Lemay et al., 2018). Critical infrastructures are essential for the daily operations of the nation (Kure & Islam, 2019). Critical infrastructures are a prime target for cybercriminals (Kure & Islam, 2019). Attacks on critical infrastructures can impact the sustainability of a nation socially, environmentally, and economically (Malatji et al., 2021).

In 2008, the Chinese conducted espionage operations through cyber to impact the presidential elections and influence geopolitical agendas (Urie, 2019). Other attacks include Stuxnet, Shamoon 2, Crash Override, Flame, and WannaCry (Ahmad et al., 2019; Alenezi et al., 2020). Stuxnet targeted Iran’s uranium enrichment program (Ahmad et al., 2019). The automated attack destroyed centrifuges in control systems and infected 100,000 hosts (Ahmad et al., 2019; Pleta et al., 2020). Flame recorded audio and video from Skype and copied files on computers in the Middle East (Alenezi et al., 2020). The Stuxnet worm targeted the specific programmable logic controllers (PLCs) of the Iranian facilities (Pleta et al., 2020). In 2012 APTs targeted the largest oil production company in the world with Shamoon malware (Pleta et al., 2020). Shamoon 2 led to the destruction of computer hard drives of Saudi Arabian organizations and the government (Ahmad et al., 2019). The victim of the Crash Override attack was the Ukrainian power grid (Ahmad et al., 2019). Crash Override caused control systems to shut down equipment (Ahmad et al., 2019). The equipment malfunction led to 30 substations disconnecting from the power grid and 200,000 customers losing power (Pleta et al., 2020). WannaCry accessed computers in 150 countries, infecting networks in hospitals, banks, telecommunications, and other critical infrastructures (Alenezi et al., 2020). In the United Kingdom, the WannaCry ransomware prevented hospital medical staff from accessing their patients' medical records (Van Dine, 2020).

In 2016 the United States Intelligence agencies reported that Russian cyber actors influenced the presidential election through cyber effects (Robinson et al., 2018). Then in 2017, it is believed that the French election was also impacted (Robinson et al., 2018). Recently, APTs targeted the SolarWinds Orion platform by compromising the supply chain (Malatji et al., 2021). Each attack threatens human life and national security, which is seen as a form of cyber warfare (Robinson et al., 2018). The current cybersecurity strategies are not working (Van Dine, 2020). Organizations lack the strategy to prevent or detect attacks on these infrastructures (Pleta et al., 2020).

### ***Opportunity***

Network complexity is evolving and creating additional attack surfaces that enable more opportunities for cyber criminals (Rowley, 2019). The tools used by APTs are inexpensive, easy to develop, and abundant (Vanni, 2019). APTs use various sequential tactics to complete a unified goal (Ahmad et al., 2019). Attacks are planned and organized for a specific target (Ahmad et al., 2019). APTs use multivectored attacks through various stages (Tounsi & Rais, 2018). Initial network entry includes social engineering, spear-phishing, and exploitation of vulnerabilities (Amin et al., 2021). The Cyber Kill Chain can represent the stages of attacks (Tounsi & Rais, 2018). The cyber kill chain shows the order of events that APTs take to successfully gain access to the network and send network data to another location (Tounsi & Rais, 2018). Additionally, the cyber kill chain helps identify the attackers' tactics, techniques, and procedures (TTPs) and develop threat intelligence (Dargahi et al., 2019). The cyber kill chain identifies the stages of attack as (a) reconnaissance, (b) weaponization, (c) delivery, (d) exploitation, (e) installation, (f) command and control (C2), and (g) actions towards the objectives (Shin et al., 2019).

Reconnaissance and weaponization techniques help develop the attack plan (Tounsi & Rais, 2018). Through reconnaissance, the adversary identifies targets and gains knowledge of the targets, then uses that knowledge to develop a custom weapon (Tounsi & Rais, 2018). The weapon is then delivered to the target using delivery methods such as an e-mail with malicious URLs (Tounsi & Rais, 2018). The adversary exploits vulnerabilities using the knowledge gained during reconnaissance (Tounsi & Rais, 2018). Social engineering is one of the most popular methods to bypass network security (Chen et al., 2018).

Humans are the most vulnerable aspect to network security (Pleta et al., 2020; Safa et al., 2018). Adversaries use the knowledge of the network and the people to infiltrate networks using various scams. Several prevalent malicious e-mails include money scams, information scams, malware distribution, multiple file extensions, disguised links, spear-phishing, and wire transfer requests (Ross, 2018). The attacker sends the target an e-mail that focuses on social engineering (Ross, 2018). The purpose of the scams is to steal money and information, distribute malware, and establish trust (Ross, 2018). The e-mails also allow the attackers a method for persistence.

The adversaries can then gain persistence by installing malicious executables (Tounsi & Rais, 2018). The malicious executables can contain key-loggers, password crackers, and other backdoors to enable the adversary to maintain their presence if the initial compromise is lost (Tounsi & Rais, 2018). Once the malicious executable is on a system and elevated permissions are attained, C2 is established (Tounsi & Rais, 2018). The C2 is used to exfiltrate data from the infected systems (Tounsi & Rais, 2018). The exfiltration of data can lead to the loss of data integrity and availability (Tounsi & Rais, 2018). To create a stronger foothold on the network, the adversary uses its hold and elevated permissions to spread laterally (Tounsi & Rais, 2018). APTs have a robust tool bag and various techniques, such as zero-day exploits, distributed agents, social engineering techniques, spear phishing data mining, and exfiltration (Ahmad et al., 2019).

### *Guardians*

Organizations rely on defense-in-depth to protect their networks. Defense-in-depth uses multiple layers of security to reduce or mitigate the risks (Alsaqour et al., 2021). The multiple layers of security for defense-in-depth include data, application, session, host, network, physical, perimeter, and event logging and monitoring (Alsaqour et al., 2021). Krause et al. (2021) list defense-in-depth for critical infrastructure as (a) policies, procedures, and awareness, (b) physical security, (c) network security, and (d) device and application security. The Joint Task Force (2020) has identified numerous security controls that can be used to develop an organization's defense-in-depth strategy. The multiple security layers interconnect and have interdependencies (Huang & Zhu, 2020). However, APTs continue to evade the traditional defense-in-depth strategy using tailored actions (Huang & Zhu, 2020). Rapid network changes increase opportunities for attacks (Krause et al., 2021).

The ability to detect and protect networks against APTs has become challenging (Han et al., 2021). Defenders must adopt proactive defense measures to their defense-in-depth strategies (Huang & Zhu, 2020). Patches for the network's vulnerabilities are not always available before an attack (Amin et al., 2021). APTs can be detected using behavior analysis, traffic analysis, security events, and threat intelligence mining (Han et al., 2021). Intrusion detection systems (IDS) can detect APTs using a signature or behavioral analysis (Cho & Nam, 2019). Signature analysis uses data from malicious patterns previously discovered to detect new attacks (Chen et al., 2018). However, APTs have techniques that can bypass the IDS and create false negatives (Amin et al., 2021). APTs use zero-day vulnerabilities to evade signature detection (Chen et al., 2018). Behavioral detection methods evaluate and predict suspicious behavior of the data-driven security records while aggregating, normalizing, analyzing, and reassembling network traffic at multiple layers (Chen et al., 2018). Correlation analysis uses numerous variables to detect APT attacks (Cho & Nam, 2019). Data-driven security records, parses, normalizes, analyzes, and reassembles network traffic at multiple layers (Chen et al., 2018).

APTs bypass firewalls, intrusion prevention systems (IPS), anti-virus (AV), and security gateways (Tounsi & Rais, 2018). Defenses built for static malware, signature-based, and pattern-matching technology leave networks exposed to evolved threats (Tounsi & Rais, 2018). Multiple-stage attacks allow APTs to bypass security controls by staging the attacks from a few minutes to a few months (Shin et al., 2019). The attacks are difficult to detect because administrators must correlate alerts from different machines from various periods (Shin et al., 2019). Defenses are developed to protect networks from cybercriminals; however, they quickly create new attacks to bypass defenses (Ross, 2018).

To protect against APTs, organizations need a deeper understanding and situational awareness of the terrain (Ahmad et al., 2019). Situational awareness allows the organization to see what is occurring during a set time to help make informed decisions (Ahmad et al., 2019). Understanding the threat landscape, the adversary’s strategy, and the attack techniques allow the organization to define the requirements for cyber defense (Amin et al., 2021). Cyber threat intelligence enables the defenders to understand the existing or potential threats on their networks so that APT attacks can be prevented or detected (Han et al., 2021).

### *Cyber Threat Intelligence*

Security teams are moving strategies towards CTI to prevent data breaches (Rowley, 2019). CTI is the collection and analysis of information that help identify potential attacks on the organization (Kure & Islam, 2019). CTI helps organizations change unknown threats into known threats (Kure & Islam, 2019). CTI is the knowledge that can be sent to organizations to defend networks based on specific knowledge of a threat and the industry that it is targeting (Tounsi & Rais, 2018). CTI identifies the cyber threat and helps determine the best response to the situation (Kure & Islam, 2019). Actionable data accelerates decision-making to reduce gaps between current defenses and adversaries (Rowley, 2019; Tounsi & Rais, 2018). Cyber threat intelligence is gathered from multiple locations to categorize threat profiles and assist with actionable responses against the threat (Qamar et al., 2017). However, the sources do not share a standard naming convention (Lemay et al., 2018). Each security group has a different name for the various APTs, malware, and campaigns (Lemay et al., 2018). The threat profiles contain information on campaigns, victims, motivation, tools, and attack methodologies (Qamar et al., 2017). Decisions are made, and risks are identified based on the evidence-based knowledge of threats (Tounsi & Rais, 2018). Threat intelligence aims to reduce the number of days between compromise and detection of APTs (Tounsi & Rais, 2018).

CTI allows organizations to have situational awareness (Wagner et al., 2019). Sharing the latest threats and vulnerabilities can help organizations make tactical decisions to resolve the issues (Wagner et al., 2019). Organizations can improve cybersecurity by applying CTI to strategic, operational, and tactical decisions (Kure & Islam, 2019). CTI aims to improve risk management (Kure & Islam, 2019).

### ***Technical Threat Intelligence***

Technical threat intelligence (TTI) feeds firewalls, gateways, Security Information and Event Management (SIEM), and other appliances with indicators of compromise (IOCs) (Tounsi & Rais, 2018). IOCs enable intelligence to be produced (Tounsi & Rais, 2018). IOCs can be categorized into network, host-based, e-mail indicators, unusual file modifications, and malicious code (Joint Task Force, 2020; Tounsi & Rais, 2018). Network indicators include URLs, domain names, and IP addresses (Tounsi & Rais, 2018). Network IOCs have a short time to live (Tounsi & Rais, 2018). Host-based indicators include the names of malware, documents, file hashes (MD5, SHA-1, SHA-256), dynamic link libraries (DLLs), and registry keys that are found during forensic analysis (Tounsi & Rais, 2018). Email IOCs are the e-mail addresses, IP addresses, e-mail headers, subjects, attachments, links, and objects created during targeted social engineering e-mail attacks (Tounsi & Rais, 2018).

IOCs are attributes that allow CTI to develop into actionable intelligence (Wagner et al., 2019). Other features include threat actor descriptions, campaigns, and motivations (Wagner et al., 2019). CTI must be relevant, timely, accurate, complete, and ingestible (Wagner et al., 2019). Relevant means that the identified threat proposes a risk to the system (Wagner et al., 2019). The sharing of CTI will help critical infrastructures gain a strategic advantage.

### *CTI Sharing*

The sharing of CTI is needed to survive APT attacks (Wagner et al., 2019). Sharing information with others can assist with the development of response options (Egloff & Smeets, 2021). The sharing of technical intelligence allows for identifying previous malicious actions and protecting assets (Egloff & Smeets, 2021). There are multiple methods and formats of information sharing. Manual CTI sharing of CTI can be slow, tedious, and contain errors (Wagner et al., 2019). CTI can be shared through e-mail, phone calls, web-community portals, shared databases, and data feeds (Wagner et al., 2019).

One significant issue with CTI sharing is the non-standard naming convention (Lemay et al., 2018). Each research group may have different names for malware and APT actors (Lemay et al., 2018). Additional challenges to CTI sharing of CTI include overloading threat data, poor quality of data, privacy and legal issues governing the data, interoperability issues among threat intelligence platforms, and multiple standards used by threat intelligence platforms (Kure & Islam, 2019).

The United States Government and the MITRE Corporation created the Structured Threat Information Expression (STIX) and the Trusted Automated eXchange of Indicator Information (TAXII) to provide a standard protocol for analyzing cyber threats, specifying indicator patterns, managing response activities, and sharing CTI (Wagner et al., 2019). TAXII is a tool that automatically sends messages on threat indicators (Jasper, 2017). STIX is a standardized language used to describe threats and is used by the TAXII system (Jasper, 2017). TAXII and STIX are used together to provide situational awareness, real-time network defense, and threat analysis (Jasper, 2017). Both technologies created a standard for sharing data and IOCs and are used on commercial CTI systems (Gong & Lee, 2021). The STIX also identifies how to manage the information and helps determine courses of action against the attacker's tactics, techniques, and procedures (TTPs) (Qamar et al., 2017). The TAXII provides situational awareness of the threats to help mitigate the attack promptly (Qamar et al., 2017). Unfortunately, STIX reports are created manually, not always validated, and can be shared with errors (Qamar et al., 2017). The TAXII helps to share STIX with the community (Qamar et al., 2017). Operational efficiency and quick reaction depend on automated and real-time threat intelligence tailored to the organization (Rowley, 2019). Without the threat intelligence and expert strategies to illuminate and respond to APTs, critical infrastructures will continue to be victims of data breaches (Rowley, 2019).

### ***Threat Intelligence Platform (TIP)***

Threat intelligence is needed to help cybersecurity teams defend networks (Anstee, 2017). Security controls can be implemented if the attack behavior is understood (Khan et al., 2019). A threat intelligence platform (TIP) assists in the understanding of attack behavior (Khan et al., 2019). A TIP has intelligence feeds that give insights into the adversary’s behavior (Khan et al., 2019). A threat intelligence platform can gather data from multiple sources, leading to data overload (Ward, 2017). However, the TIP automatically prioritizes threats based on customer-defined parameters to make the information useful and guide security teams (Ward, 2017). Security teams can use the processed data from the TIP to enhance their networks' security posture (Ward, 2017).

### *Threat Hunting*

Cybersecurity defenders aim to prevent hackers from accessing the organization's assets or data (Van Dine, 2020). One method is using active defense that incorporates intelligence to mitigate the threats and vulnerabilities while enabling them to actively detect, trace, and respond to the threat or attack as it is occurring (Van Dine, 2020). The cybersecurity defenders hunt and expel adversaries from the network while further investigating and collecting additional intelligence on the adversary (Van Dine, 2020). The use of threat hunting enables the security team to locate attacks on the network that evade traditional security controls such as firewalls, intrusion detection systems, and SIEMs (Joint Task Force, 202). Threat hunting changes cyber defenses from reactive to proactive, using cyber threat intelligence to illuminate the adversary on the network (Anstee, 2017). Threat hunting also assumes the network is compromised (Reynolds & Horvath, 2017). The proactive approach combines network traffic analysis and forensics (Reynolds & Horvath, 2017). As previously discussed, APTs use specific TTPs. The TTPs are learned through cyber threat intelligence. Using the intelligence and TTPs of the APT, threat hunters perform specific hunts targeting the APT (Bromiley, 2019). Exploring the environment through threat hunting allows organizations to identify their vulnerabilities before they are attacked by an APT (Bromiley, 2019). The proactive mindset enables organizations to remediate the vulnerability and reduce the threat landscape of the environment (Bromiley, 2019).

Additionally, new intelligence can be gained through threat hunting and shared with peer organizations, Information Sharing and Analysis Organization (ISAO), Information Sharing and Analysis Centers (ISAC), and government agencies (Joint Task Force, 2020). Not all defenders can be threat hunters. Threat hunting is complex (Bromiley, 2019). Threat hunting takes a particular set of knowledge, skills, and abilities (KSAs) of the tools and processes used to find and follow a hidden trail left by the adversary (Anstee, 2017).

## Transition and Summary

APTs select specific networks to gather information or to destroy. Their stealth and advanced techniques make it difficult for defenders or threat hunters to find them on the network. A threat intelligence platform is a tool that security analysts can use to help illuminate the trail of the adversary. CTI sharing is limited and often manual. IOCs are technical and allow defenders to act. APT attacks are growing, and more studies on the use of threat intelligence and the relationship to finding APTs are needed.

# Section 2: The Project

I explored cybersecurity analysts' cyber threat intelligence strategies to defend critical infrastructures from APT attacks. I will discuss the participants, population, sampling, ethics, research methodology, and the justification of each decision in Section 2. Finally, I will discuss the reliability and validity of data collection and data analysis.

## Purpose Statement

My qualitative exploratory multiple case study aimed to explore cybersecurity analysts' cyber threat intelligence strategies to defend critical infrastructures from APT attacks. The targeted population group consisted of cybersecurity analysts with at least 1 year of experience with cyber threat hunting. The sample population has knowledge and experience with cyber threat intelligence strategies that can be used to defend critical infrastructures from APT attacks. The geographical location of the study was the Southwestern and Northeastern United States of America.  The results of my study may assist organizations with critical infrastructures in implementing strategies that may reduce APT attacks. The implications for affecting positive social change may include improved strategies that could better protect data.

## Role of the Researcher

My role as the researcher was to design and conduct the study, collect data, perform data analysis, and present unbiased findings. I was the primary data collection instrument for this study. Researchers must use ethical standards throughout their research (Sanjari et al., 2014). I was engaged in every research stage and utilized ethical standards throughout my research.

A researcher’s subjectivity shapes the methodology, analysis, and data (Karagiozis, 2018). My relationship with the topic includes 15 years of cybersecurity experience: system administration, information assurance, network security analyst, and cyber threat hunting. I do not have any personal or professional relationships with the employees of the identified companies. According to Sanjari et al. (2014), conducting research from which peers may benefit is essential. Karagiozis (2018) stated that the researcher needs to respect the participant’s rights. The *Belmont Report* requires researchers to follow a code of conduct to protect participants' rights.

I reviewed the United States Department of Health and Human Services (1979) *Belmont Report* to meet ethical standards and protocols. According to the *Belmont Report*, the three basic ethical principles are respect for persons, beneficence, and justice. I ensured that my study was conducted within the *Belmont Report's* parameters and followed the identified processes described in the ethical research section. I applied the following requirements to meet the *Belmont Report* standards: (a) acquiring informed consent for each interviewee to ensure respect of persons, (b) assessing the risks and benefits, and (c) establishing unbiased procedures to select participants. I completed the National Institute of Health (NIH) Office of Extramural Research web-based training course (Certification Number: 2922073). The course discusses the protection of human research participants (see Appendix C for certificate). I ensured that all participants remained anonymous and signed the informed consent form. Additionally, I asked that all participants not disclose information relating to the interviews so that the participants' confidentiality and identity are protected.

The ethical challenges of a research project include anonymity, confidentiality, and informed consent (Sanjari et al., 2014). I assigned each interviewee and company with a specific code used throughout the research to protect the interviewees and the companies. Each interviewee filled out an informed consent document before the interview proceeded. The consent provides the type of data to be collected, the purpose of the data, the researcher and interviewees' roles, the objective, and where to find the results (Sanjari et al., 2014). Butler et al. (2016) recommended a systematic qualitative review to enrich the integrity and trustworthiness.

I used semistructured interviews to collect data. A semistructured interview approach contributes to maintaining data quality using an interview protocol (Young et al., 2018). The researcher collects the required data using an interview protocol (Yeong et al., 2018). A researcher uses an interview protocol to standardize the interviews in a set time (Yeong et al., 2018). Additionally, when a researcher uses an interview protocol, the interview remains on track, and the participants provide more in-depth responses (Roberts, 2020). An interview protocol provides structure and increases reliability (Roberts, 2020). I list the interview protocol designed for this research in Appendix A. I used the interview protocol in Appendix A with each participant. I use the interview protocol to reduce personal bias.

I mitigated any personal bias during data collection and analysis. The researcher must reduce bias to increase the quality (Butler et al., 2016). A researcher uses an interview protocol to minimize bias and increase reliability (Roberts, 2020). Roberts (2020) recommends six recommendations to assist researchers in reducing bias in qualitative research data collection. Researchers should develop a qualitative attitude and create open-ended interview questions (Roberts, 2020). The questions should align with the research topic and be assumption-free (Roberts, 2020). Creating an interview guide that is IRB-approved allows the researcher to provide structure and focus during the interview (Roberts, 2020). Another recommendation is to test the interview questions beforehand to rule out bias and strengthen skills (Roberts, 2020). Researchers should also take time to reflect after conducting each interview (Roberts, 2020). Finally, researchers should use their knowledge to strengthen the interview process (Roberts, 2020). Roberts' (2020) recommendations were used to design the interview protocol in Appendix A.

## Participants

The participants' criteria are designed to identify individuals who can answer the research question appropriately based on their experience (Johnson et al., 2020). The interview population consisted of cybersecurity analysts with at least one year of cyber threat hunting experience. The targeted participants provided relevant and current data for cyber threat intelligence strategies used to defend critical infrastructures. The targeted cybersecurity analysts represent the professionals who attain, implement, and utilize cyber threat intelligence for threat hunting on critical infrastructures. Their insights and experiences hunting APTs on critical infrastructures will help identify cybersecurity analysts' cyber threat intelligence strategies. The targeted population of cybersecurity analysts is from the Southwestern and Northeastern United States of America and were volunteers. I used predefined eligibility criteria to identify the participants. The eligibility criteria demonstrates that the interviewees can provide the necessary information for the research topic (Rowley, 2012). The participants were selected from a pool of candidates with experience in attaining, implementing, and utilizing cyber threat intelligence for threat hunting on critical infrastructures.

I used a gatekeeper to gain initial access to the organizations and population pool. Gatekeepers are crucial for gaining organizational access (Hoyland et al., 2015). Furthermore, gatekeepers can assist with managers' approval process, initial contact with participants, and scheduling an initial information meeting with the organization (Hoyland et al., 2015). I found the gatekeepers and obtained their contact information from LinkedIn. The gatekeepers helped vet participants using the pre-determined eligibility criteria. The criteria used to identify potential candidates are (a) cybersecurity professionals with responsibilities associated with critical infrastructures, (b) at least 1 year of threat hunting experience, and (c) knowledge of current cyber threat intelligence strategies used to defend critical infrastructures.

Before interviewing the participants, I received IRB approval from Walden University. An IRB ensures that the three principles of research ethics are applied to the research study (Ritchie, 2021). Once IRB approval was received, I contacted gatekeepers to gain initial access to the potential interview candidates. Each interview participant received an invitation letter via e-mail. A sample e-mail is in Appendix B. The e-mail included the interview's purpose, scope, problem statement, and research question. E-mails provided the initial relationship with the interviewees (Rowley, 2012). Once an individual decided to participate, I discussed logistics via e-mail, including the date and time.

## Research Method and Design

The research method and design for the study are discussed in this section. I also justify using the method and design as it applies to the study. Finally, I discuss the methodologies and designs considered in this section.

### Method

I chose the qualitative method to explore cyber threat intelligence strategies of cybersecurity analysts to defend critical infrastructures from APT attacks. Jones et al. (2019) stated that the problem should guide the research design and that the researcher should use the best research method for the results. Qualitative research aims to develop an understanding in areas where little research has been conducted (Kerr et al., 2010). The researcher can use the qualitative research method to present the identified problem's results

Qualitative research elucidates a particular topic (Tavakol & Sandars, 2014a). The audience sees the evidence through qualitative research and can thoroughly investigate the problem using a verbal style (Jacques, 2014). Qualitative research addresses how events are related or how a specific phenomenon occurs (Maxwell, 2019). Researchers observe behaviors, examine data, and analyze data narratively through qualitative research (Peterson, 2019). Themes and precise narratives of the phenomenon focus on explaining the data (Jones et al., 2019).

I considered the quantitative method for this study. Quantitative research uses a numerical style to communicate with the audience by relying on statistics and data analysis (Jacques, 2014; Nimon, 2011). Data analysis for quantitative methods shows the relationships within the data and then connects the relationships to the research context (Albers, 2017). Quantitative methods focus on questions such as “how many,” “what is happening,” and “what was the outcome” (Albers, 2017; Jones et al., 2019). The purpose of this study was not to answer, “what is happening” but rather to explore “how to.” Quantitative research requires the researcher to collect data appropriate for the variables' measurement tool (Nimon, 2011). Quantitative research is limited based on survey responses and measurements (Jones et al., 2019). Results from quantitative research may identify the requirement to perform an in-depth analysis of the problem (Brannen, 2005). Another limitation is understanding the research problem in detail (Jones et al., 2019). The data from quantitative methods does not allow for understanding complex problems (Jones et al., 2019). The data is often presented in a simplified manner and does not allow for an explanation of a complex issue, nor does it connect the pieces to the big picture (Ahrens & Khalifa, 2013). The purpose of this study was to explore cyber threat intelligence strategies used to defend critical infrastructures. I did not use statistical testing in this study to validate findings or to test a hypothesis; therefore, I ruled out the quantitative research method.

I also considered mixed-method research for this study. Mixed method research provides quantitative and qualitative research ideas, data, and analysis to provide a new understanding of a complex research question (Plano Clark, 2019). Using a mixed method approach, the researcher can validate a qualitative study's findings using large-scale quantitative surveys (Kelle, 2006). The researcher can use mixed methods to identify problems and develop theoretical concepts and additional hypotheses (Kelle, 2006). A researcher can also use mixed methods to find data to assist with the statistics, identify additional variables, and further explain the quantitative data (Kelle, 2006). Mixed method research was inappropriate for this study because I did not use a quantitative research method.

Qualitative research indicates the relationship between cause and effect by identifying the problem and exploring the possible solutions (Dornan & Kelly, 2017). The themes generated from the collected data allowed the exploration of the strategies used by the participants. Using qualitative research methods, I explored cybersecurity analysts' cyber threat intelligence strategies to defend critical infrastructures from APT attacks.

## Research Design

I applied an exploratory multiple case study design to my research. An exploratory multiple case study allowed me to achieve the goal of gaining an in-depth understanding of the phenomenon of cyber threat intelligence. Case studies show an understanding of complex issues by providing in-depth analysis and a detailed description of the data (Jones et al., 2019).

Researchers use case studies to collect evidence and understand the activity or process (VanWynsberghe & Khan, 2007). The researcher uses a case study to understand a complex issue through descriptive analysis and connecting pieces to the whole (Jones et al., 2019). They help to answer “how” and “why” and are often used when events have no control (Yates & Leggett, 2016).

Initially, I identified a few designs as an option, but ultimately chose the case study design. The designs included phenomenological, ethnography, narrative, and grounded theory. The phenomenological design describes the experiences of individuals who lived through a specific phenomenon or event (Kafle, 2013). The results help create policies and best practices (Yates & Leggett, 2016). I did not focus on one specific event; therefore, the phenomenological design was not optimal.

Researchers use ethnography to study an entire cultural group (Yates & Leggett, 2016). Situations and behaviors are used to describe the experiences, attitudes, beliefs, thoughts, and reflections of the research study participants (Marcen et al., 2013). Observations of the culture, art, and cultural artifacts are used for data collection (Yates & Leggett, 2016). Ethnographers try to understand how the cultural group views the word (Tavakol & Sandars, 2014b). The study did not address the participants' culture; therefore, ethnography was not the right design. The participants' stories are collected, and their experiences are studied during narrative research (Moen, 2006). It is often used for biographies or autobiographies to describe life experiences in detail (Yates & Leggett, 2016). The narrative design was inappropriate as the study was not a biography of the participants. A case study contributed to an in-depth understanding of the current cyber threat intelligence strategies to defend critical infrastructures.

Data saturation is essential to the validity of the completed research (Fusch & Ness, 2015). Saturation is grasped when the information becomes redundant, and the researcher cannot identify any new properties of a specific category (Saunders et al., 2018). When conducting interviews, data saturation is reached when the same comments are repeated by multiple interviewees (Saunders et al., 2018). Fusch and Ness (2015) stated that data saturation is not about the quantity but rather the quality or depth of the data. The data collection methodology should lead to data saturation fulfillment (Fusch & Ness, 2015). Fusch and Ness (2015) identified data collection methodology by performing structured interviews in which participants are asked the same questions. Fusch and Ness (2015) also established the relationship between data saturation and triangulation. Triangulation explores the different layers of the event and ensures validity (Fusch & Ness, 2015). Researchers use triangulation to understand the research problem in-depth (Adami & Kiger, 2005). To achieve data saturation, I conducted semistructured interviews with the identified population comprised of cybersecurity analysts from the Southwestern and Northeastern United States’ critical infrastructure networks. I completed data triangulation by comparing the interviews with multiple people from different companies with the organizations’ documents.

## Population and Sampling

The population for this study will comprise cybersecurity analysts from critical infrastructure networks in the Southwestern and Northeastern United States who have experience in cyber threat hunting and using cyber threat intelligence to hunt for APTs. Cybersecurity analysts may include positions such as cyber threat hunters and cyber threat intelligence analysts. Stern et al. (2014) stated that qualitative research populations' characteristics are related to their experience in the subject. I used pre-defined eligibility criteria to select interviewees from each participating organization. The pre-defined eligibility criteria were included in the interview protocol located in Appendix A.

There are two main categories of sampling methods – probability and non-probability (Berndt, 2020). Probability sampling chooses participants at random (Tavakol & Sandars, 2014b). Participants were determined using a non-probability sampling method using a purposive sampling strategy. The targeted population represents a smaller proportion of the general population, thus meeting the criteria for non-probability sampling methods (Berndt, 2020). I used purposive sampling to select the interview candidates. The purposive sampling strategy uses specific criteria to identify the participants (Tavakol & Sandars, 2014b). Purposive sampling will illuminate information on the research topic (Jahja et al., 2021). In purposive sampling, participants are selected based on the likelihood that their responses will generate valuable data for the study (Barratt et al., 2015; Campbell et al., 2020). The purposive sampling method will ensure that the selected participants for this study have specific knowledge and experience on the research topic. In qualitative research, sampling gathers detailed information on a subject (Jahja et al., 2021). I anticipated there would be at least three organizations with at least five eligible cyber analysts with the appropriate experience. The sample size required was less than twenty. Jahja et al. (2021) state that a small number is required to gather detailed information on the topic. Based on these assumptions, I anticipated that data saturation was reached between ten to fifteen interviews have been completed. Kerr et al. (2010) state that the sample size is defined by the point at which data saturation is reached. Vasileiou et al. (2018) identified that data saturation could occur with as few as nine interviews. An in-depth understanding can be achieved through a small purposeful sample size (Campbell et al., 2020). Data saturation is achieved when redundancy is attained (Tavakol & Sandars, 2014b).

Each participant chooses their virtual interview preference. The participants selected either video chat, audio-only, or e-mail. Options were discussed and identified before the interview was scheduled. Interviews conducted via Skype or telephone may reduce interviewer bias (Rowley, 2012). Rowley (2012) stated that some participants might prefer an interview conducted via e-mail because it allows them to answer the questions at their leisure.

## Ethical Research

Belmont’s four main principles for ethical research include autonomy, beneficence, nonmaleficence, and justice. My job as the researcher was to ensure that each principle was followed. The ethical principles are interconnected (Salazar, 2021). Participation was volunteered-based only. Salazar (2021) stated that participants are respected through volunteerism and informed consent. The participants were chosen based on pre-determined selection criteria to allow for a fair and unbiased selection. Participant transparency was achieved by providing each participant with an informed consent form and a study description. Informed consent is the understanding shared between the researcher and the participants (Onen & Balli, 2020). According to Onen and Balli (2020), the elements of informed consent are the purpose, risks, and benefits of the study, confidentiality, voluntariness, the ability to withdraw at any time, and the participant's ability to contact the researcher for questions. The consent form includes how to withdraw from the interview. If a participant decided to withdraw, all associated data was deleted. All participants were provided with the purpose and problem statement for the research study. Informed consent will protect the rights of the participants and provide access to information on the study (Barrett, 2005). The participants did not receive any compensation. The incentive was the knowledge gained from each participant's expert interviews, allowing each participant to contribute to the field.

I served as the data collection instrument. I used a data collection method that does not harm the participant and guarantees the participant's confidentiality and anonymity. Each participant received a unique code that will help maintain their privacy and confidentiality. The study utilized semistructured interviews and organizational documents to collect data. The interview questions were open-ended, targeting the knowledge and experience of the participants. I collected, analyzed, and identified themes from the data collected from the interviews and organizational documents. Each participant was informed about the data storage procedures. Researchers must guarantee confidentiality and anonymity to ensure autonomy or respect for the participant (Tavakol & Sandars, 2014b). Each participant had a unique code assigned to them (P1, P2, P3, and so forth). All collected data was stored on an encrypted external hard drive, thus ensuring the participants' privacy and confidentiality. The hard drive was stored in a local bank's safe deposit box that only I can access. The data may include interview logs, transcripts, organizational documentation, and other digital data. The data was maintained for five years. The interview questions and informed consent are in Appendix D and Appendix E. Before I reached out to candidates or collected data, I obtained approval from Walden's

Institutional Review Board (IRB). The approval number issued by the IRB is 02-01-22-0744878.

## Data Collection

The following section discusses the data collection instrument, technique, and organization.

### Instruments

As the researcher, I was this study's primary data collection instrument (Karagiozis, 2018). In qualitative research, the researcher is the instrument that performs analysis, observation, and interviews (Jahja et al., 2021). An interview is required when interpersonal contact is essential (Yates & Leggett, 2016). Interviews allow the participants to discuss their knowledge or experience with the topic in depth (Tavakol & Sandars, 2014b). Qualitative research uses interviews to help the researcher collect facts and gain insight into and under the topic's experiences and processes (Rowley, 2012). Interviews help identify themes and help identify the best practices from various viewpoints (Sulewski et al., 2019). I used a semistructured interview as the primary data collection method. Semi-structured interviews enable the exploration of themes and their relationships (Kerr et al., 2010). Additional data collection instruments include an interview protocol, an interview guide, research notes, and data analysis to ensure reliability and validity. The interview protocol will allow for the standardization of interviews. Qualitative research uses an interview protocol to obtain quality data (Yeong et al., 2018). Each participant was asked the same questions and followed member checking as described via the interview protocol. Asking participants the same interview questions will help achieve data saturation (Fusch & Ness, 2015).

The interview protocol (Appendix A) was used to conduct each interview; it included the interview script, interview questions, and the participant criteria. Bias was reduced using open-ended questions. The participants' confidentiality was ensured by removing all personal identifiable information (PII) from the data collected. Additionally, each participant was assigned a code, such as P1, P2, and P3. The data was secured on an encrypted hard drive.

Member checking was used to validate my findings and to reduce bias. Member checking is the process of modifying data and sharing analysis with the participants (Caretta & Perez, 2019). Participants will receive the researcher's interpretations to validate the accuracy (Tavakol & Sandars, 2014b). I sent each participant my interpretation of their response to validate. I provided each participant's transcribed data, interview notes, and other findings for member checking.

## Data Collection Technique

Before data collection began, I obtained IRB approval. Data collection involved conducting interviews and document analysis. The data collection process identified and accessed interview candidates, picked the participants, gathered informed consent, coordinated interviews, performed member-checking, and ensured data triangulation. The participants that met the required criteria were chosen from the population pool. Each potential participant received an invitation to participate in the research study from me via e-mail. Once they agreed to participate, a consent form was sent to the potential participant. The consent form contained the research topic, sample interview questions, withdrawal process, disclosure of incentives, and an overview of data confidentiality. Once the consent was received, an interview was scheduled via Zoom. All participants received a copy of the interview questions beforehand (Appendix D).

Interviews were chosen as the primary data collection technique because they gather detailed information from people with experience in the target area (Jones et al., 2019). A data collection guide was used throughout the study. A data collection guide is a pre-built template with open-ended questions designed to solve the research problem (Ranney et al., 2015). The data collection guide for this study was the interview guide in Appendix A. The questions for the interviews were pre-planned and outlined in an interview guide. Each question was designed to be open-ended (Appendix D). Interviewees should answer each question as they were based on their expertise and role (Hamilton & Finley, 2019). Interviews were recorded digitally, and notes were taken during the interview, providing the analysis foundation (Yates & Leggett, 2016). Notes assisted in the initial analysis of the data (Ranney et al., 2015). My laptop was used to record all interviews. The recorded interview was transcribed using a voice-to-text application. Additionally, I performed member checking on the data. Each interview was reviewed, transcribed, and sent to the interviewee for confirmation.

Member checking establishes the study's validity and trustworthiness (Birt et al., 2016). Member checking relies on the researcher following up with the participants (Caretta & Perez, 2019). The participants can confirm the credibility of the data presented (Creswell & Miller, 2000). The interview data was reviewed for themes. The results were then sent to the participants via e-mail to validate the accuracy of the themes. Participants had the opportunity to comment on the results to help validate the themes. Member checking continued until the participant agreed that I accurately interpreted the data they provided. The feedback received from the participants was incorporated into the data analysis to confirm the identified themes. The process continued until data saturation was reached.

**Data Organization Techniques**

I followed a data organization technique during the study's lifecycle to ensure that data was organized and analyzed. The data was coded to identify themes. The data was then categorized based on the identified coding and grouping of the data. Coding allows the data to be sorted and labeled in an organized manner (Sulewski et al., 2019). The themes identified through the coding process enable the researcher to describe the data patterns (Sulewski et al., 2019). Each participant had a log used to document my thoughts and any questions I needed to clarify. Reflective journaling was used to reflect on the data sources and the interviews. Journaling creates an audit trail, develops reflexivity, and provides context during analysis (Vicary et al., 2017).

I stored all data collected in a customized electronic file system. Each participant was assigned a non-identifying label. The labels were used to name each participant's folder, containing the interview recordings, audio transcripts, notes, and analysis of identified themes. Qualitative data analysis software was used to assist in the organization of the data. The software helped link additional data to the identified themes, such as interview notes, journal entries, and organizational data. I stored all data collected on an encrypted external drive. The encrypted external hard drive and any hardcopy material are stored in a locked file cabinet when not in use. As required by Walden University, data will be stored for five years from the publication date of this study.

## Data Analysis Technique

Data analysis is the researcher's process of transforming raw data into meaningful information (Jahja et al., 2021). As the researcher, I was the primary tool to analyze the data (Clark & Veale, 2018). The researcher provides meaning to the data during data analysis and describes that meaning (Tavakol & Sandars, 2014b). Data analysis and coding in qualitative research should be transparent to ensure rigor (Ranney et al., 2015). Data analysis should consist of triangulation and member checking to help validate the data (Yeong et al., 2018). Data triangulation uses multiple data sources to validate the data and enhance the research's validity (Adami & Kiger, 2005). The multiple viewpoints collected provide a complete picture of the topic (Adami & Kiger, 2005).

I used the collected data from the semistructured interviews and organizational documents to identify patterns. Each interview was transcribed for analysis. The transcripts were uploaded to computer-assisted qualitative data analysis software (CAQDAS) to identify codes and themes (Ranney et al., 2015). CAQDAS can handle a large amount of data accurately and quickly (Cypress, 2019). CAQDAS provides data collection and analysis management (Cypress, 2019). I applied a data coding process. Coding helps the researcher organize the data for analysis (Ranney et al., 2015). Data coding ensures transparency and identifies the main ideas from the data (Clark & Veale, 2018; Ranney et al., 2015). Transparency can be achieved by documenting analysis steps and data with field notes (Snelgrove & Vaismoradi, 2019). I documented my decisions for each step in the field notes. Codes were assigned, categorized, and linked logically into themes. After the data was coded, it was then sorted. Sorting is the process that categorizes the codes to generate themes from the identified patterns (Clark & Veale, 2018). Themes were generated from the codes. The CAQDAS that I used is the ATLAS.ti qualitative software. ATLAS.ti assisted in organizing the data, assigning codes, and identifying themes in the study. Data was able to be coded, linked, and visualized using ATLAS.ti (Cypress, 2019). Once ATLAS.ti completed the data coding and organization, I compared the results to my field notes.

The conceptual framework that helped inform this study is RAT. The study's topic informs theme development (Snelgrove & Vaismoradi, 2019). I looked for patterns associated with CTI strategies for defending critical infrastructures from APTs to support the formation of the themes. I kept interviewing participants until data saturation was reached. Data was generated from the semistructured interviews, field notes, and organizational documents. Any new data identified during the analysis phase was added to the study if relevant. Member checking was utilized with each interview to enable the credibility and validity of the data collected.

## Reliability and Validity

Reliability and validity are used to determine the research's trustworthiness (Tavakol & Sandars, 2014b). The research findings are central to measuring reliability and validity (Yeong et al., 2018). Validity is the extent to which the results depict the phenomenon investigated and is credible (Creswell & Miller, 2000; Yates & Leggett, 2016). For the research to be reliable, the collected data must be consistent with the findings (Jahja et al., 2021). Dependability, credibility, transferability, and confirmability establish the reliability and validity of the research.  Researchers may use member checking, triangulation, audits, and reflexivity to validate their findings (Creswell & Miller, 2000). Triangulation helps to validate the findings and comprehend the results (Tavakol & Sandars, 2014b; Yates & Leggett, 2016). Information convergence through multiple triangulation sources helps identify the study's main themes (Creswell & Miller, 2000). Member checking allows researchers to achieve validity (Caretta & Perez, 2019). I used member checking and triangulations so that the findings could be validated. I also identified my assumptions, beliefs, and biases.

## Dependability

I used an interview protocol and kept a research journal to create audit trails for dependability and confirmability. Following a research protocol can reduce bias during data collection (Ivey, 2020). Additional support to dependability includes the recording, transcribing, and review of each interview through member checking. Incorporating multiple data collection methods lead to triangulation (Moon, 2019). Triangulation increases the dependability of the findings (Moon, 2019). The specific criteria for the participants of the study create an audit trail (Campbell et al., 2020). The audit trail created leads to the study's dependability (Campbell et al., 2020). Additionally, member checking and observations during the interview were performed to assist with dependability. Member checking provides dependability through the deep analysis of the data (Birt et al., 2016). I described my study design and methods and documented the processes and procedures for my study. I ensured that the participants were selected based on the eligibility criteria.

### Creditability

Creditability is achieved through member checking. Creswell and Miller (2000) state that "member checking is the most crucial technique for establishing credibility." Member checking explores the credibility of results by allowing for accurate interpretations of the collected data (Birt et al., 2016). Respondent validity will enable participants the ability to review the findings for accuracy (Lietz et al., 2006). Member checking and respondent validity help reduce the bias of the results (Lietz et al., 2006). I performed member checking and triangulation on the collected data throughout the study. Additionally, ATLAS.ti provided an audit trail, making strategies visible, creditable, and valid (Cypress, 2019).

### Transferability

Likewise, trustworthiness results from accurate findings using defined and rigorous procedures (Lietz et al., 2006). Rigor is established through transparency (Ranney et al., 2015). Transferability determines if the study's findings can apply to other fields (Bleiker et al., 2019). Transparency is established in this study using data coding and an audit trail during the analysis phase. I have provided information about my research methods and will provide my findings. The research design and how I collected, organized, and analyzed the data were described. Additionally, I provided the interview protocol and interview questions in Appendix A.

### Confirmability

Confirmability determines the findings' accuracy; therefore, the researcher must identify their bias (Tavakol & Sandars, 2014b).  Rigor increases the confidence that the results are presented by the researcher accurately with minimum bias (Lietz et al., 2006). I stated my bias and assumptions during the research process. I used triangulation, member checking, and audit trails to have rigorous and trustworthy results. Member checking, triangulation, and audit trails are strategies used for rigor and trustworthiness (Lietz et al., 2006). I took notes and created journal entries during the interviews and the analysis phase. A journal yields rigor and transparency by generating an audit trail (Vicary et al., 2017). Triangulation and member checking contributed to the verification of the results. Triangulation helps confirm the findings of the research (Moon, 2019). I performed member checking with each participant to validate my findings.

I used an interview protocol and the same questions to enable the identification of themes. I collected data until data saturation was achieved. Data saturation is achieved when no new data, themes, or codes are found (Vasileiou et al., 2018). I used a comparative method for themes (CoMeTs) to confirm data saturation of themes. CoMeTs compare interviews to the previous findings of the collected data until no new theme has been identified, thus establishing theme saturation (Vasileiou et al., 2018). Additionally, I developed a codebook with the assistance of ATLAS.ti qualitative software. A codebook allows for a systematic approach to mapping the data to themes and creates an audit trail documenting how saturation was achieved (Kerr et al., 2010).

## Transition and Summary

The tools, techniques, and methodologies for completing my study were discussed in Section 2. A qualitative exploratory multiple case study was used to answer the research question. I discussed the participants, population, sampling, ethical considerations, data collection, data organization, the analysis technique, role of the researcher, validity, and reliability. The following sections discuss the findings, the implications for IT professional practice, the impact on social change, recommendations to consider, the need for additional research, and my reflections.

## Section 3: Application to Professional Practice and Implications for Change

I will present an overview and a presentation of the findings in Section 3. The findings will include the themes illuminated through data analysis. This section will also include the applications to professional practice, implications for social change, recommendations for action, recommendations for further study, and my reflections. Finally, I will close with a summary and the study conclusions.

### Overview of Study

I used this qualitative exploratory multiple case study to explore cybersecurity analysts' cyber threat intelligence strategies to defend critical infrastructures from APT attacks. The targeted population consisted of cybersecurity analysts of critical infrastructures with at least 1 year of threat hunting and CTI experience. All cybersecurity analysts who participated had at least 2 years of experience in threat hunting and CTI. I collected 10 publicly available organizational documents and conducted interviews with two organizations located in the Southwestern and Northeastern United States. I collected data from one organization in two different geographical areas. The data for the research included semistructured interviews, publicly available organizational documents, field notes, and a reflective journal. I conducted member checking with each participant and triangulated the data.

I discovered four major themes through this qualitative case study: (a) CTI and threat hunting are part of the defense-in-depth strategy, (b) the lack of standards on CTI and threat hunting has created numerous challenges, (c) CTI informs threat hunting, and (d) threat hunting consists of looking at behaviors, not IOCs. I used RAT as the conceptual framework to understand the CTI strategies used to defend critical infrastructures. The themes are consistent with trends revealed in the literature review and support the use of RAT. The four themes are explored in the next section.

## Presentation of the Findings

The study’s research question was: What cyber threat intelligence strategies are cybersecurity analysts using to defend critical infrastructures from APT attacks? Once I collected the organizational documents and transcribed the semistructured interviews, I triangulated the data. I entered the transcripts and documents into Atlas.ti analysis tool that resulted in four themes. After analyzing the data, four themes were identified that related to this study's conceptual framework and literature review. I explore the four themes discovered in the presentation of findings section.

The participants were skilled threat hunters with experience using cyber threat intelligence. Each participant had at least 2 years of threat hunting and CTI experience. Two organizations participated in the research. One organization had multiple geographic locations, two of which were a part of the study. Both organizations performed threat hunts on multiple critical infrastructure networks.

Data triangulation was achieved using semistructured interviews, organizational documents, and notes collected during the interview. I used member checking to reduce bias. Atlas.ti contributed to the analysis of the collected data. Researchers use qualitative data analysis software (QDAS), like Atlas.ti, to assist throughout their research process (Oswald, 2019). Once I completed the analysis of the collected data, I identified multiple codes and applied them to the data set to reveal the major themes was completed were identified. Documents collected from the organizations include published white I will discuss the identified themes and connect them to the literature and the conceptual framework in the next section.

### Theme 1: CTI and Threat Hunting Are Part of The Defense-In-Depth Strategy

Critical infrastructures need defensive strategies that protect the networks from APT attacks. The first theme presented was the need to integrate CTI and threat hunting into the organizations' defense-in-depth strategy. Krause et al. (2021) discussed defense-in-depth to defend critical infrastructure. However, Krause et al. (2021) did not identify CTI or threat hunting as part of defense-in-depth. Instead, defense-in-depth is listed as (a) policies, procedures, and awareness, (b) physical security, (c) network security, and (d) device and application security. Threat hunting is listed as a security control in NIST SP 800-53 Version 5 but is not exclusively called out as part of defense in depth (Joint Task Force, 2020). Participant 6 mentioned that organizations lack threat hunting teams even though it is mandated by the Cybersecurity and Infrastructure Security Agency (CISA).

Each participant listed a component of defense-in-depth. Participant 4 discussed continuously assessing the security posture and hardening the network. Participant 7 focused on air-gapping and the isolation of networks. Participant 9 highlighted the importance of audits and intelligence-driven threat emulation or purple teams to identify unknown vulnerabilities in the security posture. Participant 2 discussed using multiple security policies so that APTs leave a footprint and make it difficult to move on the network undetected. Participant 5 mentioned that defense starts with the supply chain and that the organization should know where the technology came from and identify the known or unknown vulnerabilities in the software or hardware purchased. Participants 2 and 5 also highlighted the need to educate others on how adversaries move on the network.

Five participants explicitly distinguished defense-in-depth as a strategy used to defend critical infrastructures and expressively professed that threat hunting is an integrated layer to the strategy. Kure and Islam (2019) pointed out that CTI provides organizations with insights on emerging threats to develop defense options for their network. The targeted and actionable information help reduce gaps between the adversary and the current defense capabilities (Rowley, 2019; Tounsi & Rais, 2018). Participant 6 mentioned that they constantly improve the organization's security posture even if they do not find APTs while hunting. Bromiley (2019) discussed using threat hunters to identify network vulnerabilities that the organization may not be aware of. Amin et al. (2021) stated that patches are not always available before an attack occurs. Participant 5 mentioned that CTI helps make informed decisions and risk analysis. Participant 10 stated that the CTI informs the organization where to focus and increase its defense capabilities. Participant 10 also discussed using CTI to identify the threat surface to quantify risk, identify vulnerabilities, security updates, and required segmentation, and inform business policies. Participant 6 also mentioned that CTI could help identify emerging threats, vulnerabilities, and exploits.

Participant 1 described using threat hunting to look for anomalous or weird behavior that is not standard in the environment. Participant 9 highlighted that CTI informs leadership on the threat surface and enables quicker decision-making for updates segmentation, network access, and business practices. Participant 9 continued with CTI helps identify the potential of insider threats, poor hygiene practices, and employee ignorance.

Two documents from an organization were published by an external entity that set requirements for logging, incident response, and incident remediation. The organization used the external entity documentation because it identified the standards and policies set by higher authorities. Additional organizational documents discussed defense in depth and identified threat hunting as a proactive strategy. Organizations must be proactive and mitigate attacks before they occur. Having incident response plans and waiting to be attacked is no longer an effective strategy. The react and defend approach does not protect critical infrastructure from an attack. Polymorphic and obfuscated malware evade traditional defense-in-depth strategies and require a proactive approach. One of the organizational documents states, “threat hunting is essential to any organization that wants to stop and prevent attacks in its networks.” Organizations use threat hunting to be proactive so that they detect, mitigate, or prevent attacks from occurring.

I selected RAT as the conceptual theory for this study. RAT consists of three components: a motivated offender, a suitable target, and a lack of guardians. Critical infrastructures have data that may be valuable to APTs. Over the last few years, APT attacks have targeted critical infrastructure. By applying CTI and threat hunting with defense-in-depth, an organization can reduce the opportunities the APTs have for an attack. Reducing or removing opportunities from the equation reduces the likelihood of victimization (Pratt & Turanovic, 2016). Additionally, adding threat hunters or elite guardians to the defense can reduce the likelihood of an attack (Hawdon et al., 2020).

### Theme 2: The Lack Of Standards On CTI and Threat Hunting Has Created Numerous Challenges

The lack of standards for CTI and threat hunting has created numerous challenges. Each participant had their definition of what CTI is and what it includes. Each one described a different hunting methodology. Participant 6's definition included information that helps identify vulnerabilities and targets consisting of behaviors, TTPs, trends, and the adversary's motivations. Participant 1 thought CTI was a specific data type tailored for the network and organization. Participant 9 stated that CTI is another domain in intelligence that collects data about threats and adversaries. Participant 2 had a similar definition as Participant 9, that it was information for the pursuit of the adversary. Participant 10 thought that CTI is a form of raw data used to write detection analytics broken into categories such as persona, group, and technical. Participant 7 highlighted that CTI is strategic, operational, tactical, and technical. Participant 4 said it was more than IOC, behaviors, and technical information. In contrast, Participant 6 stated that CTI identifies the team's behavior, TTPs, trends, motivations, vulnerabilities, and targets.

Every author had a different definition and description of CTI in the literature review. The Computer Security Resource Center (CSRC), part of the National Institute of Standards and Technology (NIST), has multiple terms, descriptions, and definitions for threat intelligence. Three terms from the NIST include threat information, threat intelligence, and threat reports (Johnson et al., 2016). NIST lists three different definitions for threat information. Threat intelligence is threat information that has been aggregated, whereas a threat report describes threat-related information (Johnson et al., 2016).

Each participant identified at least two different challenges for CTI alone. Lemay et al. (2018) and Kure and Islam (2019) identified numerous challenges with CTI. Participant 9 highlighted that malicious activity does not always get attributed correctly and that multiple names exist for the same group and activity. Lemay et al. (2018) discussed non-standard naming conventions, applying different names for the same malware and APT actors. Participant 4 mentioned that CTI is behind open-source intelligence (OSINT) and not detailed enough. At least two participants identified that intelligence is not timely and that there is too much data, making it challenging to parse in a timely manner. Kire and Islam (2019) highlighted the poor quality of data, interoperability issues, and multiple standards. Participant 7 identified that too much information is passed on as CTI, but not all of it is intelligence. Another challenge identified by Participants 5 and 10 is access to intelligence. Participant 5 discussed classified versus non-classified, whereas Participant 10 discussed military versus commercial intelligence. Their point was that intelligence is not shared in a timely manner and is sometimes only shared with specific government entities, making it difficult to help protect non-government critical infrastructure.

**Table 1**

*Challenges of CTI*

| Challenges | # Of Participants |
|---|---|
| Lack of access | 2 |
| Unverified information | 2 |
| Not timely | 2 |
| Separation of duties | 1 |
| Unwillingness to share | 1 |
| Incorrect Attribution | 1 |
| Quality of information | 1 |
| Non-naming standard | 1 |
| Lack of Detail | 1 |
| Not real-time | 1 |

The lack of standards for sharing CTI and the identification of CTI led to a lack of hunt methodology standardization. The participants described five different methodologies – behavior-based, MITRE ATT&CK Matrix, hypothesis, structured and unstructured, and a combination of 2 or more methods. Six participants used a behavior-based approach, four used the MITRE ATT&CK Matrix, two used a hypothesis method, and one used a structured and unstructured methodology for threat hunting. Interestingly, five participants used a combination of two threat hunting methodologies. Participants 1, 2, 4, 6, 9, and 10 each use behavior. Participants 2 and 7 use a hypothesis for hunting. Participants 5, 6,7, and 10 use the MITRE ATT&CK Matrix. In addition to the MITRE

ATT&CK Matrix, Participant 5 used structured and unstructured hunting. Only Participants 1, 4, and 9 mentioned one hunt methodology, which all use a behavioral-based approach. The behavioral-based approach includes analytics and heuristics. The MITRE ATT&CK Matrix is a database of APT TTPs from real-world observations that can be used to build a threat model (Xiong et al., 2022). Participant 6 discussed using the MITRE ATT&CK Matrix to map TTPs for APTs. Participant 10 built heuristics that incorporated the MITRE ATT&CK Matrix, and Participant 9 also built analytics built on TTPs. While the methodologies differed, the consensus was that threat hunting does not involve looking for IOCs generated from CTI.

**Table 2**

*Hunting Methodologies*

| Methodology | # Of Participants |
|---|---|
| Behavior | 6 |
| MITRE ATT&CK Matrix | 4 |
| Hypothesis Based | 2 |
| Structured and Unstructured | 1 |
| Combination | 5 |

The numerous challenges with CTI and threat hunting allow the adversary to be invisible. As applied to RAT, the lack of standardization and numerous challenges limit the amount of guardianship for the network, creating an increase in target suitability for the APTs. Hollis et al. (2013) noted that guardianship is observed through intervention activities. The many challenges of CTI prevent threat hunting from gathering the data they need to harden the network or develop hunt analytics to detect the adversary. It is crucial for the guardians to detect the adversary (Hsieh & Wang, 2018). Without the data, teams cannot identify the adversary's motivations or a possible target. Safa et al. (2018) previously identified motivation and opportunity's role in the information environment. The lack of standards decreases the guardians' situational awareness of the environment and can potentially increase the opportunities for attack.

Leading policy organizations like CISA and NIST must develop standards and policies for CTI and threat hunting. The standards should include, at minimum, a standardized language for threats, one source to name malicious groups and activities, and CTI sharing standards. Executive Order 14028 mandates proactive detection, cyber or threat hunting, and aims to remove barriers to sharing threat information. The order also identifies and orders CISA to develop playbooks for cybersecurity vulnerability and incident response activities.

### Theme 3: CTI Informs Threat Hunting

Organizations need a deeper understanding and situational awareness of their environment to protect against APTs (Ahmad et al., 2019). APT attacks can be prevented or detected using CTI to identify existing or potential threats (Han et al., 2021). The Joint Task Force (2020) stated, "Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies." Two documents provided by the participants discuss using tailored intelligence to enhance security operations so that analytics can be developed and applied to the network. This, in turn, can identify attacks and help harden the networks before they occur. Additionally, another document focuses on data analytics to accelerate security operations and enable teams to make quick decisions.

All participants identified CTI as critical for threat hunting and defense. CTI enables organizations to identify vulnerabilities and reduce opportunities for APTs to target proactively. CTI informs threat hunters to develop their hunt plan. All participants described how CTI informs their hunting. However, the participants described different components of a hunt plan, but none described all the same components. Participants 1 and 7 focused on the specific activity to look for on the network. TTPs are identified through CTI, enabling targeted hunts based on the TTPs (Bromiley, 2019). Participant 1 also mentioned that CTI informs hunt analytics. Participant 2 stated that CTI helps the analysts understand the adversary by identifying who, what and why. Participant 5 mentioned that CTI helps identify the target. In contrast, Participant 10 stated that CTI helps reduce analyst fatigue by identifying their focus area and reducing their haystack. Intelligence feeds can give insights into the adversary’s behavior (Khan et al., 2019).

**Table 3**

*Hunt Plan Components*

| Components | # Of Participants |
|---|---|
| Behavior | 4 |
| Motivation | 1 |
| Adversary | 1 |
| Target | 2 |
| Threat Model | 1 |
| Analytics Needed | 3 |

The theme suggests that the more the guardians learn about the APTs targeting their networks, the more likely the guardians can reduce the opportunities APTs have for an attack. CTI helps identify who wants to target the specific organization or network, their most likely behaviors, and why they want to target the organization. CTI helps understands the motivation of the APT or offender. Motivation explains the offender's behavior and helps identify the target (Safa et al., 2019; Holt et al., 2021). Behaviors are used for threat hunting. CTI helps guardians know who the motivated offender is, what they target and how the offender attacks. Integrating CTI and threat hunting into the defensive strategy may deter APTs from attacking by increasing the environment's security posture.

### Theme 4: Threat Hunting Consists of Looking at Behaviors, Not IOCs

There was not a single strategy that all participants identified. Each participant had their method or strategy. However, all said to avoid IOCs. Participant 6 mentioned that any CTI published, the adversary will read it too and change their infrastructure. Tounsi and Rais (2018) mentioned that some IOCs have a short time to live. One document stated that threat hunting could find anomalies before IOCs are identified. Another document briefly discusses the organization's CTI strategy – which does not include IOCs. The strategy does include threat actor motivations, tactics, techniques, and procedures, and how to detect and mitigate threat actors.

Participants 5, 6, 7, and 10 identified using the MITRE ATT&CK matrix as part of their methodology. One organization document included a high-level response checklist for security teams referencing the MITRE ATT&CK matrix for technical details. The participants used the MITRE ATT&CK to map APTs' TTPs to build queries and hypotheses and gather more intelligence. The MITRE ATT&CK framework provides the behavior analysis, tactics, techniques, and mitigation procedures on each tracked adversary for information and operational technology environments (Schlette et al., 2021). Participant 5 uses standardized hunts based on standard operating procedures (SOPs) and the MITRE ATT&CK.

Participants 1, 2, 6, and 10 identified analytics, heuristics, or hunt TTPs based on behavior, not IOCs. Participant 2 used behavior to create a hypothesis and identify the logs or data showing the APT's activity. Participant 1 avoids IOCs but used CTI to build hunt analytics. Additionally, Participant 1 identifies the data needed for the analytics. Participant 9 builds hunt analytics from TTPs. Participant 10 uses a combination of methods. Participant 10 uses CTI to identify the possible threat actors that might target the network and identifies what the threat actor would do by incorporating the MITRE ATT&CK matric. The idea is to start hunting in a small area, then grow as needed.

Holt et al. (2018) identified the need to understand the behavior of cyber criminals so that attacks could be mitigated. Focusing on the behavior of APTs, threat hunters develop detection analytics. Behavioral detection evaluates and can predict suspicious behavior at multiple layers (Chen et al., 2018). The results of this study revealed that threat hunting could increase their knowledge of APTs using CTI to proactively identify threats and unknown security vulnerabilities before they are used in an attack. Participant 9 discussed how threat hunting allows defense teams to be proactive.

Threat hunting allows the guardians to reduce the opportunities APTs have for an attack. Limiting opportunities through threat hunting can reduce the likelihood of attack because the target has increased guardianship. In RAT, three conditions must overlap- a motivated offender, a suitable target, and the lack of a guardian (Jansen & Leukfeldt, 2016; Pratt & Turanovic, 2016). If one condition can be removed from the equation, then victimization will not occur (Pratt & Turanovic, 2016). Threat hunting increases the guardianship of the network.

## Applications to Professional Practice

The study’s findings, literature review, and conceptual framework analysis highlight strategies to defend critical infrastructures from APT attacks. The results of this study revealed that threat hunting and CTI are crucial to defensive strategies for critical infrastructures. Combined with defense-in-depth, threat-informed, and behavioral-based hunting methodologies appear to have the most significant implications for reducing attack opportunities.

The outcome of this study illuminates the need for organizations with critical infrastructures to add threat hunting teams and CTI to their defense strategy. The defense strategy should include (a) Threat hunting informed by CTI, (b) targeted CTI for the organization, (c) multiple layers of defense, (d) mitigations based on intelligence, (e) behavior analytics, (f) threat modeling using TTPs, and (g) a deep understanding of the network.

Revisiting defensive strategies and applying new concepts will increase the protection of critical infrastructures. A proactive defense approach will enable organizations to reduce their vulnerabilities and threat landscape. The findings from this study align with RAT because successful defensive strategies reduce the opportunities that APTs have for their target.

## Implications for Social Change

The study's findings indicate there could be positive changes in using cyber threat intelligence strategies to defend critical infrastructures. Critical infrastructures are a constant target for APTs. APT attacks have caused several types of critical infrastructures to shut down. Examples are power outages, non-access to medical records, oil production stoppages, and water treatment plant attacks. These types of attacks on critical infrastructures threaten human life and national security. Improvements in the defense of critical infrastructures may increase the availability of critical networks and the protection of critical data on the networks.

As the study identifies, critical infrastructure organizations should ensure their defensive strategies include CTI and threat hunting. Adopting a proactive defensive posture may lead to the protection of human life and national security. Positive social change implications include sharing critical CTI and hunting strategies with similar critical infrastructures. The benefits to the community include safe drinking water and a reduction of blackouts caused by cyber attacks.

## Recommendations for Action

This qualitative exploratory multiple case study intended to explore cybersecurity analysts' cyber threat intelligence strategies to defend critical infrastructures from APT attacks.

This study analyzes multiple scholarly literature documents, interview responses from threat hunters, and organizational documents. These three types of data supported triangulation and corroboration of the research question. Based on the triangulation of the data, four themes were identified: (a) CTI and threat hunting are part of the defense-in-depth strategy, (b) the lack of standards on CTI and threat hunting has created numerous challenges, (c) CTI informs threat hunting, and (d) threat hunting consists of looking at behaviors, not IOCs.

I recommend the following action for cybersecurity teams of critical infrastructures with or without threat hunters:

1. Assess the current cyber threat environment. Ensure that it is based on tailored CTI for your environment. Perform threat emulation or use purple team tactics to identify additional vulnerabilities.

2. Identify your network baseline, ensure that team members know what activities are normal (processes, ports, protocols, IPs, code execution, behavior, etc.), and document. Continuously update documentation.
3. Refine your defense-in-depth strategy, adding cyber threat intelligence and threat hunters.
4. Develop playbooks for your hunt strategy
5. Integrate automation and aggregation for CTI and hunt analytics.
6. Find opportunities to collaborate and share information with others.

I recommend the following action for national policymakers such as NIST, CISA, and the Executive Branch:

1. Develop standard definitions and descriptions of CTI and threat hunting.
2. Develop standard language to describe threats and to enable interoperability with TIPs
3. Review CTI sharing policies to ensure the right people can access the information they need

I plan to disseminate the study findings and recommendations by providing a short academic paper to each participant. I will also share the findings with the academic community through workshops, conferences, and journal publications.

## Recommendations for Further Study

The study findings, conclusions, and recommendations may contribute to existing and future research about cyber threat intelligence strategies used to defend critical infrastructures from APT attacks. I recommend expanding the geographic area and the types of critical infrastructures. CISA identifies sixteen different types of critical infrastructure sectors. This study only included participants from two sectors. Gathering data from all sixteen sectors will validate if similar challenges with CTI exist in all sectors and if the usage of CTI is similar. The next recommendation is to conduct a study on the challenges with CTI. Reducing the limitations of CTI sharing would increase the analysts' knowledge and defense of the critical infrastructures. Additionally, research is needed to identify how CTI can be streamlined for threat hunters. Since not all organizations have threat hunters, I recommend a study to understand the education needed to be a threat hunter and how to implement a threat hunting program.

## Reflections

Working on a DIT Doctoral Study gave me an opportunity that I never dreamt possible. It opened the realm of possibility to achieving something impossible. It has not come without its obstacles. One of the many challenges to academic research is staying determined to finish. There were occasions when I lost my focus due to life events – COVID, death, new life, and surgeries. In the end, I hope my girls have learned that anything is possible if you work hard, stay focused, and surround yourself with people who love and support you.

This study allowed me to grow personally and professionally. I hope that my research can help others protect their networks. I picked the research topic because I am passionate about defending our critical infrastructures and the advantage that CTI can give organizations when implemented. The research findings may help inform future research on challenges and standards needed for the industry. The interviews were a joy because the participants were passionate about CTI and threat hunting. Everyone had a positive attitude and was eager to share their knowledge. I am glad I used an interview protocol because it helped keep the interview moving and prevented me from geeking out with the interviewee.

## Summary and Study Conclusions

This qualitative exploratory multiple case study intended to explore cybersecurity analysts' cyber threat intelligence strategies to defend critical infrastructures from APT attacks. The research study’s findings revealed CTI strategies used to protect critical infrastructures. Four main themes emerged, coinciding with the literature review and the RAT framework. The themes highlighted about the defense of critical infrastructures: (a) CTI and threat hunting are part of the defense-in-depth strategy, (b) the lack of standards on CTI and threat hunting has created numerous challenges, (c) CTI informs threat hunting, and (d) threat hunting consists of looking at behaviors, not IOCs.

# References

Adami, M. F., & Kiger, A. (2005). The use of triangulation for completeness purposes. *Nurse Researcher*, *12*(4), 19–29. https://doi.org/10.7748/nr2005.04.12.4.19.c5956

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics, and a disinformation model of counterattack. *Computers & Security*. *86*, 402–418. https://doi.org/10.1016/j.cose.2019.07.001

Ahrens, T., & Khalifa, R. (2013). Researching the lived experience of corporate governance. *Qualitative Research in Accounting and Management, 10*(1), 4–30. https://doi.org/10.1108/11766091311316176

Albers, M. J. (2017). Quantitative data analysis - In the graduate curriculum. *Journal of Technical Writing and Communication. 47*(2), 215–233. https://doi.org/10.1177/0047281617692067

Alenezi, M. N., Alabdulrazzaq, H. K., Alshaher, A. A., & Alkharang, M. M. (2020). Evolution of Malware Threats and Techniques: A Review. *International Journal of Communication Networks and Information Security (IJCNIS), 12*(3). 326–337 https://www.ijcnis.org/index.php/ijcnis/article/view/4723

Alsaqour, R., Majrashi, A., Alreedi, M., Alomar, K., & Abdelhaq, M. (2021). Defense in depth: Multilayer of security. *International Journal of Communication Networks and Information Security (IJVNIS), 13*(2). 242–248. https://doi.org/10.17762/ijcnis.v13i2.4951

Amin, M., Shetty, S., Njilla, L., Tosh, D. K., & Kamhoua, C. (2021). Hidden Markov model and cyber deception for the prevention of adversarial lateral movement. *IEEE Access*, *9*, 49662–49682. https://doi.org/10.1109/ACCESS.2021.3069105

Anstee, D. (2017). The great threat intelligence debate. *Computer Fraud & Security*, *2017* (9), 14–16. https://doi.org/10.1016/1361-3723(17)30099-4

Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods*, 27, 1–19. https://doi.org/10.1177/1525822X1452683

Barrett, R. (2005). Quality of informed consent: Measuring understanding among participants in oncology clinical trials. *Oncology Nursing Forum*, *32*(4):751–5. https://doi.org/10.1188/05.ONF.751-755

Berndt, A. (2020). Sampling methods. *Journal of Human Lactation*, *36*(2), 224–226. https://doi.org/10.1177/0890334420906850

Birt, L., Scott, S., Carvers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*(13), 1802–1811. https://doi.org/10.1177/1049732316654870/

Bleiker, J., Morgan-Trimmer, S., Knapp, K., & Hopkins, S. (2019). Navigating the maze: Qualitative research methodologies and their philosophical foundations. *Radiography*, *25*(1), S4–S8. https://doi.org/10.1016/J.RADI.2019.06.008

Brannen, J. (2005). Mixing methods: The entry of qualitative and quantitative approaches into the research process. *The International Journal of Social Research Methodology*, *8*(3), 173–184. https://doi.org/10.1080/13645570500154642

Brantly, A. F. (2014). Cyber actions by state actors: Motivation and utility. *International Journal of Intelligence and CounterIntelligence. 27*(3). 465–484. https://doi.org/10.1080/08850607.2014.900291

Bromiley, M. (2019). *Thinking like a hunter: Implementing a threat hunting program.* [White paper]. https://www.sans.org/reading-room/whitepapers/analyst/thinking-hunter-implementing-threat-hunting-program-38923

Busse, C., Kach, A. P., & Wagner, S. M. (2016). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods*, *20*(4) 574–609. https://doi.org/10.2139/ssrn.2713980

Butler, A., Hall, H., & Copnell, B. (2016). A guide to writing a qualitative systematic review protocol to enhance evidence-based practice in nursing and health care. *Worldviews on Evidenced-Based Nursing*, *13*(3), 241–249. https://doi.org/10.1111/wvn.12134

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: Complex or simple? Research case examples. *Journal of Research in Nursing*, *25*(8), 652–661. https://doi.org/10.1177/1744987120927206

Caretta, M. A., & Perez, M. A. (2019). When participants do not agree: Member checking and challenges to epistemic authority in participatory research. *Field Methods*, *31*(4), 359–374. https://doi.org/10.1177/1525822X19866578

Chen, J., Su, C., Yeh, K., & Yung, M. (2018). Special issue on advanced persistent threat.

*Future Generation Computer Systems, 79*(1), 243-246. https://doi.org/10.1016/j.future.2017.11.005

Cho, D. X., & Nam, H. N. (2019). A method of monitoring and detecting APT attacks based on unknown domains. *Procedia Computer Science, 150*, 316–323. https://doi.org/10.1016/j.procs.2019.02.058

Clark, K. R., & Veale, B. L. (2018). Strategies to enhance data collection analysis in qualitative research, *Radiologic Technology, 89*(5), 482CT–485CT. http://www.radiologictechnology.org/content/89/5/482CT.extract

Clarke, R. V. G. (1980). "Situational" crime prevention: Theory and practice. *The British Journal of Criminology, 20*(2), 136–147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory Into Practice, 39*(3), 124–130. https://doi.org/10.1207/s15430421tip3903_2

Cybersecurity & Infrastructure Security Agency. (2021a). Critical infrastructure sectors. https://www.cisa.gov/critical-infrastructure-sectors

Cybersecurity & Infrastructure Security Agency. (2021b). Executive Order on improving the nation's cybersecurity. https://www.cisa.gov/executive-order-improving-nations-cybersecurity

Cybersecurity & Infrastructure Security Agency. (2021c). Joint statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA). https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

Cypress, B. S. (2019). Data analysis software in qualitative research: Preconceptions, expectations, and adoption. *Dimensions of Critical Care Nursing, 38*(4), 213–220. https://doi.org/10.1097/DCC.0000000000000363

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A cyber-kill-chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques,* 1–29. https://doi.org/10.1007/s11416-019-00338-7

Department of Homeland Security. (2019). Cybersecurity Programs. https://www.dhs.gov/science-and-technology/cybersecurity-programs

Dornan, T., & Kelly, M. (2017). What use is qualitative research? *Medical Education, 51*, 3–10. https://doi.org/10.1111/medu.13229

Egloff, F. J., & Smeets, M. (2021). Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies.* https://doi.org/10.1080/01402390.2021.1895117

Executive Order 14028 NSM-8 Improving the Nation’s Cybersecurity (2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Federal Bureau of Investigation. (2018). APT 10 Group. https://www.fbi.gov/wanted/cyber/apt-10-group

Freilich, J. D., & Newman, G. R. (2018). Regulating crime: The new criminology of crime control. *The ANNALS of the American Academy of Political and Social Science, 679*(1), 8–18. https://doi.org/10.1177/0002716218784853

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*(9), 1408–1416. http://www.nova.edu/ssss/QR/QR20/9/fusch1.pdf

Goettl, C. (2021). Prioritising risk for better efficiency and collaboration. *Computer Fraud &Security, 2021*(4), 13–16. https://doi.org/10.1016/S1361-3723(21)00042-7

Gong, S., & Lee, C. (2021). Threat intelligence framework for incident response in an energy cloud platform. *Electronics, 10,* 1–19. https://doi.org/10.3390/electronics10030239

Hamilton, A. B., & Finley, E. P. (2019). Qualitative methods in implementation research: An introduction. *Psychiatry Research, 280*, 1–8. https://doi.org/10.1016/j.psychres.2019.112516

Han, W., Xue, J., Wang, Y., Zhang, F., & Gao, X. (2021). APTMalInsight: Identify and cognize APT malware based on system call information and ontology knowledge framework. *Information Science, 546*(2021), 633–644. https://doi.org/10.1016/j.ins.2020.08.095

Hawdon, J., Costello, M., Ratliff, T., Hall, L., & Middleton, J. (2017). Conflict management styles and cybervictimization: Extending routine activity theory. *Sociological Spectrum, 37*(4), 250–266. https://doi.org/10.1080/02732173.2017.1334608

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amide COVID-19: the initial results from a natural experiment. *American Journal of Criminal Justice*, *45*, 546–562. https://doi.org/10.1007/s12103-020-09534-4

Hewitt, A. N., Chopin, J., & Beauregard, E. (2020). Offender and victim 'journey-to-crime': Motivational differences among stranger rapists. Journal of Criminal Justice, 69, 1–10. https://doi.org/10.1016/j.jcrimjus.2020.101707

Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety*. *15*, 65–79. https://doi.org/10.1057/cpcs.2012.14

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420–436, https://doi.org/10.1177/1043986213507401

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2018). Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology, 62*(6), 1720–1741. https://doi.org/10.1177/0306624X16679162

Holt, T. J., Leukfeldt, R., & Van De Weiher, S. (2020). An examination of motivation and routine activity theory to account for cyberattacks against Dutch websites. *Criminal Justice and Behavior, 47*(4), 487–505.

https://doi.org/10.1177/0093854819900322

Holt, T. J., Turner, N. D., Freilich, J. D., & Chermak, S. M. (2021). Examining the characteristics that differentiate Jihadi-associated cyberattacks using routine activities theory. *Social Science Computer Review.* 1–17. https://doi.org/10.1177/08944393211023324

Hoyland, S., Hollund, J. G., & Olsen, O. E. (2015). Gaining access to a research site and participants in medical and nursing research: A synthesis of accounts. *Medical Education, 49*(2), 224–232. https://doi.org/10.1111/medu.12622

Hsieh, M., & Wang, S. (2018). Routine activities in a virtual space: A Taiwanese case of an ATM hacking spree. *International Journal of Cyber Criminology, 12*(1), 333–352. https://doi.org/10.5281/zenodo.1467935

Huang, L. & Zhu, Q. (2020). A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems. *Computers & Security, 89*(2), 1–16. https://doi.org/10.1016/j.cose.2019.101660

Ishaya, A. O., Aminat, A., Hashim, B., & Adekunle, A. A. (2021). Improved detection of advanced persistent threats using an anomaly detection ensemble approach. *Advances in Science, Technology and Engineering Systems Journal*, *6*(2), 295–302. https://doi.org/10.25046/aj060234

Ivey, J. (2020). Participation and Recruitment. *Pediatric Nursing*, *46*(3), 152–153. https://link.gale.com/apps/doc/A627278456/EAIM?u=minn4020&sid=ebsco&xid=2be27ea5

Jacques, S. (2014). The quantitative-qualitative divide in criminology: A theory of ideas' importance, attractiveness, and publication. *Theoretical Criminology, 18*(3), 317–334. https://doi.org/10.1177/1362480613519467

Jahja, A. S., Sri Ramalu, S., & Razimi, M. S. A. (2021). Generic qualitative research in management studies. *Jurnal Riset Akuntansi Dan Bisnis, 7*(1), 1–13. https://doi.org/10.38204/jrak.v7i1.523

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79–91. https://doi.org/10.5281/zenodo.58523

Jasper, S. E. (2017). U. S. Cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence, 3*(1), 53–65. https://doi.org/10.1080/08850607.2016.1230701

Jeong, M., & Zo, H. (2021). Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques. *Telematics and Informatics, 63*, 1–17. https://doi.org/10.1016/j.tele.2021.101670

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). National Institute of Standards and Technology Special Publication 800-150, Guide to Cyber Threat Information Sharing. http://dx.doi.org/10.6028/NIST.SP.800-150.

Johnson, J. L., Adkins, D., & Chauvin, S. (2020). A Review of the Quality Indicators of Rigor in Qualitative Research. *American Journal of Pharmaceutical Education, 84*(1), 138–146. https://doi.org/10.5688/ajpe7120

Joint Task Force. (2020). National Institute of Standards and Technology Special

Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5

Jones, K. R., Gwynn, E. P., & Teeter, A. M. (2019).  Quantitative or qualitative: selecting the right methodological approach for credible evidence. *Journal of Human Sciences and Extension, 7*(2), 61– 87. https://www.jhseonline.com/article/view/826

Kafle, N. P. (2013). Hermeneutic phenomenological research method simplified. Bodhi: *An Interdisciplinary Journal, 5*(1), 181–200. https://doi.org/10.3126/bodhi.v5i1.8053

Karagiozis, N. (2018). The complexities of the researcher's role in qualitative research: The power of reflexivity. *The International Journal of Interdisciplinary Educational Studies, 13*(1), 19–31. https://doi.org/10.18848/2327-011X/CGP/v13i01/19-31

Kelle, U. (2006). Combining qualitative and quantitative methods in research practice: Purposes and advantages. *Qualitative Research in Psychology*, *3*(4), 293–311. https://doi.org/10.1177/1478088706070839

Kerr, C., Nixon, A., & Wild, D. (2010). Assessing and demonstrating data saturation in qualitative inquiry supporting patient-reported outcomes research. *Expert Review of Pharmacoeconomics &Outcomes Research, 10*(3), 269–281. https://doi.org/10.1586/erp.10.30

Khan, T., Alam, M., Akhunzada, A., Hur, A., Asif, M., & Khan, M. K. (2019). Towards augmented proactive cyberthreat intelligence. *Journal of Parallel and Distributed Computing*, *124*, 47–59. https://doi.org/10.1016/j.jpdc.2018.10.006

Kim, Y., & Hipp, J. R. (2018). Physical boundaries and city boundaries: Consequences from crime patterns on street segments? *Crime & Delinquency*, *64*(2), 227–254. https://doi.org/10.1177/0011128716687756

Kranenbarg, M. W., Holt, T. J., & Van Der Ham, J. (2018). Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. *Crime Science*, 7(16), 1–9. https://doi.org/10.1186/s40163-018-0090-8

Krause, T.; Ernst, R.; Klaer, B.; Hacker, I.; & Henze, M. (2021) Cybersecurity in power grids: Challenges and opportunities. *Sensors*, *21*(18), 1–20. https://doi.org/10.3390/s21186225

Kure, H., & Islam, S. (2019). Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. *Journal of Universal Computer Science*, *25*(11), 1478–1502. http://www.jucs.org/jucs_25_11/cyber_threat_intelligence_for/jucs_25_11_1478_1502_kure.pdf

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, *72*, 26–59. https://doi.org/10.1016/j.cose.2017.08.005

Lenine, E. (2020). The pulse-like nature of decisions in rational choice theory. *Rationality and Society, 32*(4), 485–508. https://doi.org/10.1177/1043463120961578

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. http://dx.doi.org/10.1080/01639625.2015.1012409

Lietz, C. A., Langer, C. L., & Furman, R. (2006). Establishing trustworthiness in qualitative research in social work. *Qualitative Social Work*, *5*(4), 441–458. https://doi.org/10.1177/1473325006070288

Malatji, M., Marnewick, A. L., & Solms, S. (2021). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability, 13*(1), 1–33. https://doi.org/10.3390/su13010291

Marcen, C., Gimeno, F., Gutierrez, H., Saenz, A., & Sanchez, M. E. (2013). Ethnography as a linking method between psychology and sociology: Research design. *Procedia- Social and Behavioral Sciences*, *82*, 760–763. https://doi.org/10.1016/j.sbspro.2013.06.344

Maxwell, J. A. (2019). Distinguishing between quantitative and qualitative research: A response to Morgan. *Journal of Mixed Methods Research*, 1–6. https://doi.org/10.1177/1558689819828255

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology, 28*, 417–442. https://doi.org/10.1146/annurev.soc.28.110601.140752

Moen, T. (2006). Reflections on the narrative research approach. *International Journal of*

*Qualitative Methods*, *5*(4), 56–69. https://doi.org/10.1177/160940690600500405

Moon, M. D. (2019). Triangulation: A Method to increase validity, reliability, and legitimation in clinical research. J*ournal of Emergency Nursing*, *45*(1), 103–105. https://doi.org/10.1016/j.jen.2018.11.004

Nimon, K. (2011). Improving the quality of quantitative research reports: A call for action. *Human Resource Development Quarterly*, *22*(4), 387–394. https://doi.org/10.1002/hrdq.20091

Onen, O., & Balli, F. E. (2020). Examination of informed consent forms in masters and doctorate theses of educational science. *International Online Journal of Educational Sciences*, *12*(2), 119–131. https://doi.org/10.15345/iojes.2020.02.008

Oswald, A. G. (2019). Improving outcomes with Qualitative Data Analysis Software: A reflective journey. *Qualitative Social Work*, *18*(3), 436–442. https://doi.org/10.1177/1473325017744860

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: An insider threat perspective. *Decision Support Systems*. *92*, 47–56. https://doi.org/10.1016/j.dss.2016.09.012

Paraskevas, A., & Brookes, M. (2018). Nodes, guardians, and signs: Raising barriers to human trafficking in the tourism industry. *Tourism Management*, *67*, 147–156, https://doi.org/10.1016/j.tourman.2018.01.017

Paternoster, R., Jaynes, C. M., & Wilson, T. (2017). Rational choice theory and interest in the "Fortune of Others". *Journal of Research in Crime and Delinquency*, *54*(6), 847–868. https://doi.org/10.1177/0022427817707240

Peterson, J. S. (2019). Presenting a qualitative study: A reviewer's perspective. *Gifted Child Quarterly*. *63*(3), 147–158. https://doi.org/10.1177/0016986219844789

Plano Clark, V. L. (2019). Meaningful integration within mixed methods studies: Identifying why, what, when and how. *Contemporary Educational Psychology*. *57*, 106–111. https://doi.org/10.1016/j.cedpsych.2019.01.007

Pleta, T., Tvaronaviciene, M., Casa, S. D., & Agafonov, K. (2020). Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases. *Insights Into Regional Development, 2*(3), 703–715. http://doi.org/10.9770/IRD.2020.2.3(7)

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders, 11*(3), 335–354. https://doi.org/10.1080/15564886.2015.1057351

Qamar, S., Anwar, Z., Rahman, M. A., Al-Shaer, E., & Chu, B. (2017). Data driven analytics for cyber-threat intelligence and information sharing. *Computers and Security*. *67*(C), 35–58. https://doi.org/10.1016/j.cose.2017.02.005

Quick, M., Li, G., & Brunton-Smith, I. (2018). Crime-general and crime-specific spatial patterns: A multivariate spatial analysis of four crime types at the small-area scale. *Journal of Criminal Justice, 58*, 22–32. https://doi.org/10.1016/j.jcrimjus.2018.06.003

Raju, B. K., & Geethakumari, G. (2016). Event correlation in cloud: A forensic perspective. *Computing*, *98*, 1203–1224. https://doi.org/10.1007/s00607-016-0500-2

Ranney, M., Meisel, Z., Choo, E., Garro, A., Sasson, C., & Morrow Guthrie, K. (2015). Interview-based qualitative research in emergency care part II: Data collection, analysis, and results reporting. *Academic Emergency Medicine, 22*(9), 1103–1112. https://doi.org/10.1111/acem.12735

Reynolds, M., & Horvath, C. (2017). Threat hunting: A proactive technique for finding sophisticated cyber threats. https://www.ignet.gov/sites/default/files/files/9_26%20Reynolds%20Horvath.pdf

Ritchie, K. L. (2021). Using IRB protocols to teach ethical principles for research and everyday life: A high-impact practice. *Journal of the Scholarship of Teaching and Learning*, *21*(1), 120–130. https://doi.org/10.14434/josotl.v21i1.30554

Roberts, R. E. (2020). Qualitative interview questions: Guidance for novice researchers. *The Qualitative Report, 25*(9), 3185–3203. https://nsuworks.nova.edu/tqr/vol25/iss9/1

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). An introduction to cyber peacekeeping. *Journal of Network and Computer Applications*, *114*, 70–87. https://doi.org/10.1016/j.jnca.2018.04.010

Ross, C. (2018). The latest attacks and how to stop them. *Computer Fraud & Security. 2018*(11), 11–14. https://doi.org/10.1016/S1361-3723(18)30109-X

Rowley, J. (2012). Conducting research interviews. *Management Research Review. 35*(3/4), 260–271. https://doi.org/10.1108/01409171211210154

Rowley, L. (2019). The value of threat intelligence. *Computer Fraud &Security, 2019*(10), 20. https://doi.org/10.1016/S1361-3723(19)30109-5

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in orgnisations. *Future Generation Computer Systems. 97*, 587–597. https://doi.org/10.1016/j.future.2019.03.024

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications. 40*, 247–257. https://doi.org/10.1016/j.jisa.2017.11.001

Salazar, C. (2021). Participatory action research with and for undocumented college students: Ethical challenges and methodological opportunities. *Qualitative Research.* 1–18. https://doi.org/10.1177/1468794120985689

Sanjari, M., Bahramnezhad, F., Fomani, F., Shoghi, M., & Cheraghi, M. (2014). Ethical challenges of researchers in qualitative studies: the necessity to develop a specific guideline. *Journal of Medical Ethics & History of Medicine*, *7*(14), 1–6. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4263394/

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality and Quantity, 52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

Schlette, D., Vielberth, M., & Pernul, G. (2021). CTI-SOC2M2 –The quest for mature, intelligence-driven security operations and incident response capabilities. *Computers & Security, 111*, 1–20. https://doi.org/10.1016/j.cose.2021.102482

Shin, J., Choi, S., Liu, P., & Choi, Y. (2019). Unsupervised multi-stage attack detection framework without details on single-stage attacks. *Future Generation Computer Systems. 100*, 811–825. https://doi.org/10.1016/j.future.2019.05.032

Snelgrove, S., & Vaismoradi, M. (2019). Theme in qualitative content analysis and thematic analysis. *Forum: Qualitative Social Research, 20*(3), 1–14. https://doi.org/10.17169/fqs-20.3.3376

Stern, C., Jordan, Z., & McArthur, A. (2014). Developing the review question and inclusion criteria. *American Journal of Nursing*, *114*(4), 53–56. https://doi.org/10.1097/01.NAJ.0000445689.67800.86

Sulewski, J. S., Timmons, J. C., Lyons, O., & Hall, A. C. (2019). Guideposts for high-quality community life engagement supports: Results of expert interviews. *Inclusion, 7*(4), 254–268. https://doi.org/10.1352/2326-6988-7.4.254

Svensson, L., & Doumas, K. (2013). Contextual and analytic qualities of research methods exemplified in research on teaching. *Qualitative Inquiry,* 19, 441–450. https://doi.org/10.1177/1077800413482097

Tavakol, M., & Sandars, J. (2014a). Quantitative and qualitative methods in medical education research: AMEE Guide No 90: Part I. *Medical Teacher, 36*(9), 746–756. https://doi.org/10.3109/0142159X.2014.915298

Tavakol, M., & Sandars, J. (2014b). Quantitative and qualitative methods in medical education research: AMEE Guide No 90: Part II. *Medical Teacher, 36*(10), 838–848. https://doi.org/10.3109/0142159X.2014.915297

Tounsi, W., & Rais, H. (2018). A Survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*. *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Urie, E. E. (2019). Dawn of the code war: America's battle against Russia, China, and the rising global cyber threat. By John P. Carlin, with Garrett M. Graff. New York: Hatchett Book Group, 2018. *Journal of Strategic Security*. *12*(3), 179–181. https://doi.org/10.5038/1944-0472.12.3.1766

U. S. Department of Health & Human Services. (2020). Belmont report 1979. http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adoption of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 169–188. https://doi.org/10.1177/1043986215621379

Van Dine, A. (2020). When is cyber defense a crime? Evaluating active cyber defense measures under the Budapest Convention. *Chicago Journal of International Law*, *20*(2), 530–564. https://chicagounbound.uchicago.edu/cjil/vol20/iss2/18

Vanni, D. (2019). Are we any good at protecting our societies and economies from the threat of economic crime and misconduct? A look at the Italian system. *Journal of Financial Crime*, *26*(4), 1006–1013. https://doi.org/10.1108/JFC-11-2017-0115

VanWynsberghe, R., & Khan, S. (2007). Redefining case study. *International Journal of Qualitative Methods*, *6*(2), 80–94. https://doi.org/10.1177/160940690700600208

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterizing and justifying sample size sufficiency in interview-based studies: Systematic analysis of qualitative health research over a 15-year period, *BMC Medical Research Methodology*. *18*(148), 1–18. https://doi.org/10.1186/s12874-018-0594-7

Vicary, S., Young, A., & Hicks, S. (2017). A reflective journal as learning process and contribution to quality and validity in interpretative phenomenological analysis. *Qualitative Social Work, 16*(4), 550–565. https://doi.org/10.1177/1473325016635244

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*. *87*, https://doi.org/10.1016/j.cose.2019.101589

Walsh, R. (2015). Wise Ways of Seeing: Wisdom and Perspectives. *Integral Review,* 11(2), 278–293. https://doi.org/10.1037/gpr0000045

Ward, L. (2017). Building an effective threat intelligence platform that would make Einstein proud. *Computer Fraud & Security, 2017*(4), 11–12. https://doi.org/10.1016/S1361-3723(17)30031-3

Weisman, A., Quintner, J., Galbraith, M., & Masharawi, Y. (2020). Why are assumptions passed off as established knowledge? *Medical Hypotheses. 140*, 1–5. https://doi.org/10.1016/j.mehy.2020.109693

Xiong, W. Legrand, E., Aberg, O., & Lagerstrom, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling, 21*, 157–177. https://doi.org/10.1007/s10270-021-00898-7

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. *Radiologic Technology*, *88*(2), 225–231. https://www.asrt.org

Yeong, M. L., Ismail, R., Ismail, N. H., & Hamzah, M. I. (2018). Interview protocol refinement: Fine-tuning qualitative research interview questions for multi-racial populations in Malaysia. *The Qualitative Report*, *23*(11), 2700–2713. https://nsuworks.nova.edu/tqr/vol23/iss11/7

Young, J. C., Rose, D. C., Mumby, H. S., Benitez-Capistros, F., Derrick, C. J., Finch, T., Garcia, C., Home, C., Marwaha, E., Morgans, C., Parkinson, S., Shah, J., Wilson, K. A., & Mukherjee, N. (2018). A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution*, *9*(1), 10–19. https://doi.org/10.1111/2041-210x.12828

# Appendix A: Interview Protocol

Interview: Strategies Using Threat Intelligence to Detect Advanced Persistent Threats

## Eligibility Criteria

Eligibility criteria was used to identify potential interview participants. Participants will represent experience in cybersecurity-related to critical infrastructure environments as cybersecurity analysts whose daily activities entail functions of cyber threat hunting and/or cyber threat intelligence. To be selected, the candidate must satisfy at least two of the three eligibility criteria, which include:

a. Cybersecurity analysts who analyze network traffic or data on a critical infrastructure network
b. At least one year of cyber threat hunting experience
c. Prior or current knowledge of cyber threat intelligence strategy/implementation in with cyber threat hunting

## Interview Script

1. Introductions.

   Hello, my name is Melisa Joyner. I was conducting your interview today. Thank you for your time and your participation in this interview.

2. Verify informed consent and answer questions.

   I want to make sure that you understand that this interview is voluntary, you can stop the interview at any time, and that the interview is conducted in a manner to ensure that the participant or the researcher has any harm inflicted on them.

3. Identify to the participant the steps to protect the privacy and confidentiality of the individual, audio recordings, and all collected data.

   The interview was recorded via Zoom, and I will also take written notes. The time was limited to one hour, and any identifying information will not be used. All electronic data containing interview information was encrypted on an external hard drive that was stored in a locked safe that only I, the researcher has access to.

4. Remind the participant of the purpose of the study.

   The purpose of this study is to explore the cyber threat intelligence strategies that cybersecurity analysts use to defend critical infrastructures from APT attacks.

5. Identify the reason for the participation of the interviewee.

   The information provided today via interview responses, documentation, or any additional sources of information, will support my study in partial fulfillment of the degree of Doctor of Information Technology from Walden University.

6. Describe the benefit of the interviewee's participation.

   The information provided can add to the academic and professional bodies of knowledge on the defense of critical infrastructures using cyber threat intelligence strategies. There is not any compensation associated with your participation in this study.

7. Confirm the readiness of the interviewee. Ask if a break is needed.

Do you have any questions for me before we start? Do you need a break before we begin?

8. Begin recording once the participant is ready. The date, time, participant's identification number was stated. Additionally, the interview type (initial or follow up) was stated on the recording.

    My name is Melisa Joyner, and I was interviewing Participant <X>. Today's date is <X>, the time is <X>. This is my initial interview with Participant <X>. Can you confirm that I have provided you with the background information for this study that includes the purpose, the reason for your participation, the benefits of participation and that you approve of my recording and taking notes during this session?

9. Start with the first question, wait for an indication from the participant, and ensure that they are finished answering, then proceed to the next question. If needed, ask additional clarifying questions before moving to the next question.

    This is a semistructured interview. I have a few open-ended questions outlined, for which your answers are appreciated. They will assist in providing insights about defending critical infrastructures using threat intelligence.

    Demographic Questions

    1. What is your current title and role?
    2. What role do you play in defending critical infrastructures?
    3. How many years of experience do you have in cybersecurity?
    4. What is your threat hunting experience?

Interview Questions

1. What is your experience with cyber threat intelligence?

2. What does cyber threat intelligence mean to you?

3. How do you hunt for APTs on the networks that you defend?

4. Which hunting methods were more successful?

5. What are the successful strategies you have employed to defend critical infrastructures from attacks by APTs?

6. How do you use cyber threat intelligence to defend critical infrastructures from attacks by APTs?

7. What impact has cyber threat intelligence had on hunting for APTs on networks?

8. What factors play a role in the decision of how to implement cyber threat intelligence to defend critical infrastructures from attacks by APTs?

9. What are some obstacles or challenges to using cyber threat intelligence to hunt for APTs and to defend critical infrastructures from attacks by APTs?

10. What are your experiences surrounding the challenges of using cyber threat intelligence to defend critical infrastructures from attacks by APTs?

11. How do you improve the success rate of finding APTs on networks?

12. What other factors or tactics would you like to add for using cyber threat intelligence to defend critical infrastructures from attacks by APTs?

10. Ask the participant if they have any other information that they would like to share.
11. Ask the participant if they have any documentation that might be relevant to the topic.
12. Explain member checking to participant and schedule a follow up e-mail/interview to review my interpretations.
13. Stop audio recording.
14. Once all questions have been answered, end the interview.

    Thank you so much for your time. If you have any questions or concerns, you may reach me at melisa.joyner@waldenu.edu.
15. End protocol.

## Appendix B: Invitation to Participate E-mail Template

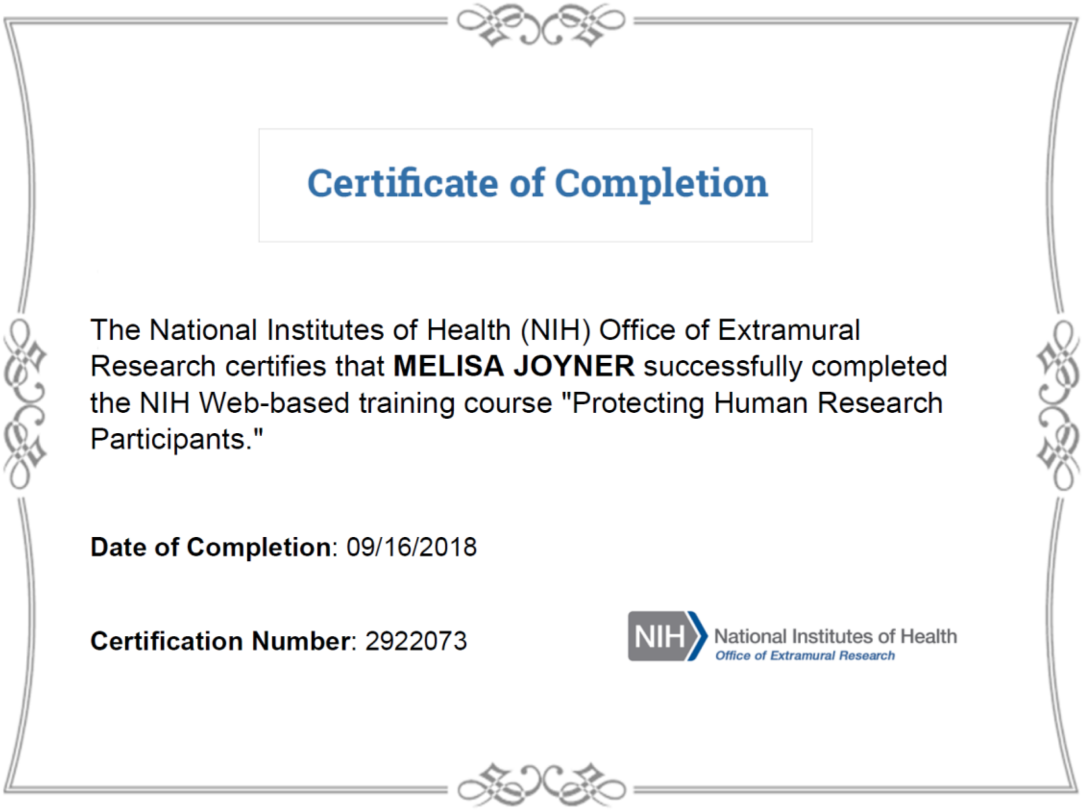
Good morning XXXXX,

I am a current Information Technology doctoral candidate at Walden University. I am researching cyber threat intelligence strategies to defend critical infrastructures from APT attacks.

I am searching for organizations with critical infrastructures that have threat hunting teams consisting of at least 4-10 people to participate in my study. The study would involve a short one on one interview with each person and a review of any documentation involving threat intelligence strategies. All information about the organization and participants was kept confidential and not publicized. A confidentiality agreement can be provided. The results of my study can be provided to the organization.

Sincerely,
Melisa A Joyner

## Appendix C: Training Certificate from the National Institute of Health Office of Extramural Research



**Certificate of Completion**

The National Institutes of Health (NIH) Office of Extramural Research certifies that **MELISA JOYNER** successfully completed the NIH Web-based training course "Protecting Human Research Participants."

**Date of Completion**: 09/16/2018

**Certification Number**: 2922073

NIH National Institutes of Health
*Office of Extramural Research*

# Appendix D: Interview Questions

## Demographic Questions

1. What is your current title and role?
2. What role do you play in defending critical infrastructures?
3. How many years of experience do you have in cybersecurity?
4. What is your threat hunting experience?

## Interview Questions

1. What is your experience with cyber threat intelligence?
2. What does cyber threat intelligence mean to you?
3. How do you hunt for APTs on the networks that you defend?
4. Which hunting methods were more successful?
5. What are the successful strategies you have employed to defend critical infrastructures from attacks by APTs?
6. How do you use cyber threat intelligence to defend critical infrastructures from attacks by APTs?
7. What impact has cyber threat intelligence had on hunting for APTs on networks?
8. What factors play a role in the decision of how to implement cyber threat intelligence to defend critical infrastructures from attacks by APTs?
9. What are some obstacles or challenges to using cyber threat intelligence to hunt for APTs and to defend critical infrastructures from attacks by APTs?

10. What are your experiences surrounding the challenges of using cyber threat intelligence to defend critical infrastructures from attacks by APTs?
11. How do you improve the success rate of finding APTs on networks?
12. What other factors or tactics would you like to add for using cyber threat intelligence to defend critical infrastructures from attacks by APTs?