2023

AI Usage in Development, Security, and Operations

Maurice Ayidiya
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Maurice Ayidiya

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. Yoseph Tsehay, Committee Chairperson, Information Technology Faculty
Dr. Donald Carpenter, Committee Member, Information Technology Faculty
Dr. Bob Duhainy, University Reviewer, Information Technology Faculty

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

Walden University
2023

Abstract

AI Usage in Development, Security, and Operations

by

Maurice Ayidiya

MS, Walden University, 2020

BS, University of Missouri St Louis, 2010

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

March 2022

Abstract

Artificial intelligence (AI) has become a growing field in information technology (IT). Cybersecurity managers are concerned that the lack of strategies to incorporate AI technologies in developing secure software for IT operations may inhibit the effectiveness of security risk mitigation. Grounded in the technology acceptance model, the purpose of this qualitative exploratory multiple case study was to explore strategies cybersecurity professionals use to incorporate AI technologies in developing secure software for IT operations. The participants were 10 IT professionals in the United States with at least 5 years of professional experience working in DevSecOps and managing teams of at least three DevSecOps professionals within the United States. Data were collected using semistructured interviews, and three themes were identified through thematic analysis: (a) implementation obstacles, (b) AI cloud implementation strategy, and (c) AI local implementation strategy. A specific recommendation for IT professionals is to identify knowledge gaps and security challenges in the DevSecOps pipeline to facilitate the necessary training. The implications for positive social include the potential to improve organizations' securities postures and, by extension, the societies and individuals they serve.

AI Usage in Development, Security, and Operations

by

Maurice Ayidiya

MS, Walden University, 2020

BS, University of Missouri St Louis, 2010

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

March 2022

Dedication

The subject of my research is my kids. They've motivated me to try to get better every day and to grow in a variety of ways. They were the ones who first gave me the motivation to succeed in life, and they always expressed pride in me whether I succeeded or failed. I am here today, getting a doctorate in part thanks to their inspiration, encouragement, and sacrifice for me.

I'd like to dedicate this to my family as well. Everybody that has stood with me through everything has encouraged me and provided me with support when I've needed it. I dedicate my study to my family, friends, students, and coworkers who supported me, offered advice, and helped me to see my progress along the way.

Acknowledgments

I must first thank my Lord God on whom I leaned on for perseverance, patience, and strength during this trip. I want to thank my doctoral committee, Dr. Tsehay Yoseph, Dr. Donald Carpenter and Dr. Bob Duhainy. They put a lot of effort into helping me become a better writer and researcher, which has helped me both professionally and personally. I thank you. I'm grateful. Dr. Nicholas Harkiolakis deserves a particular thank you as well. I am grateful for his support, which continued through the last day of his tenure as my chair. He spent years guiding me and helping me get to this point. I'll never be able to express how much I value him and my doctoral committee.

I want to thank everyone who took part in my study, including those who couldn't. I am here because you gave up something priceless to make my success possible. Our exchanges not only enabled me to obtain the information I required for my studies, but also enriched me.

I want to thank every professor and student I spoke with while attending Walden University. I gained knowledge from every one of you, and every letter we exchanged enriched my education.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

In an ideal software development environment, developers and security professionals would work collaboratively using typically agile methodology to develop, secure, and move it into operations. Using this collaborative approach can efficiently deliver more secure code and contribute to continuous integrations and development (CICD(Lam & Chaillan, 2019). The next level of innovation would be developing automation and integrating other security capabilities like artificial intelligence (AI) into the process. Advanced automation could reduce the continuous manual involvement of information security professionals, leading to a more efficient system. Since ideal software development environments are often elusive in practice, information security professionals face numerous challenges. One of these challenges includes a lack of knowledge and training on the potential use and integrations of AI (Mohammed et al., 2017). Therefore, in this study I investigated the perceived knowledge gap and whether it prevents information security professionals from integrating AI efficiently into the development, security, and operations (DevSecOps) pipeline.

Background of the Problem

The need for security in software development resulted in the creation of the so-called secure software development life cycle (SSDLC; . Recent research shows that many software development methods do not explicitly include software security measures during software development as they move from demand engineering to their final losses (Khan et al., 2021). In the past, security-related processes were isolated and entrusted to a specific team at the final stage of development (Zaydi & Nassereddine,

2021). For security to become a guide rather than a roadblock, the DevSecOps pipeline was created. Software project practices with DevOps have demonstrated how to streamline the software delivery processes, improve the quality of products with present technologies, and speed up the functions (Ahmed & Francis, 2019).

Furthermore, DevSecOps aims to automate the primary security tasks by adding security controls early in the development process instead of at the end (Karaboga & Kaya, 2019). Modern-day cybersecurity threats require a speed of response far more significant than human decision-making allows. Given the rapid increase in the volume and frequency of malware attacks, AI cyber defense systems are increasingly being implemented to proactively detect and mitigate threats (Babuta et al., 2020). Due to a lack of AI knowledge, many organizations may not readily deploy and develop AI solutions for DevSecOps. In some cases, security experts tasked with building automation into the DevSecOps process may also be responsible for integrating and managing the AI; if they do not have the necessary knowledge, they may fail to understand where to begin.

Rangnau et al. (2020) described integrating three automated testing techniques into a CI/CD pipeline and some of the challenges and pitfalls one may encounter. The use of three security testing types (Web Application Security Test [WAST], Security API Scanning [SAS], and Behaviour Driven Security Testing [BDST]) identified vulnerabilities in the development process for which automation could offer improved detection (Rangnau et al., 2020). Research shows that available testing tools can be integrated into an existing pipeline to capture vulnerabilities in the software process

(Rangnau et al., 2020). When these tools are automated using CI/CD pipelines, they can provide similar results and promote more secure products (Zaydi & Nassereddine, 2021).

Problem Statement

AI and machine learning (ML) can positively impact software security and IT operations. Still, a lack of knowledge among cybersecurity professionals may inhibit the effectiveness of security risk mitigation through AI, particularly within the DevSecOps pipelines (Cognizant, 2019). In 2011, the total investment in AI start-ups across the world was $25.88 million, which increased exponentially to $1,866.6 million throughout the following 5 years, marking a more than 7,200% increase in investments within the United States, seeing the majority of this growth (Soni et al., 2020). In comparison, projections suggest that there will be only a 40% increase in AI in DevSecOps over the next 10 years (Pons, 2020). The general IT problem is that some cybersecurity professionals resist using innovative technologies in the software development process. The specific IT problem is that some cybersecurity professionals lack strategies to incorporate AI technologies in developing secure software for IT operations (DevSecOps).

Purpose Statement

The purpose of this qualitative exploratory multiple case study of cybersecurity professionals was to study the strategies that cybersecurity professionals use to incorporate AI technologies in developing secure software for IT operations (DevSecOps). Furthermore, I explored the challenges of integrating AI solutions in the DevSecOps pipeline by identifying today's strategies to improve organizational security.

Bringing awareness about the security challenges in the DevSecOps pipeline may enable IT security leaders to identify knowledge gaps and facilitate the necessary training.

Therefore, I aimed to identify the strategies that cybersecurity professionals use to incorporate AI technologies within DevSecOps. The implications for positive social change may include a better understanding of how cybersecurity professionals successfully integrate AI into the DevSecOps pipeline to make more secure software products. Understanding AI integration could improve many organizations' security posture and, by extension, the societies and individuals they serve. The target population for this study was comprised of IT professionals in the United States with at least 5 years of professional experience working in DevSecOps, managing teams of at least three DevSecOps professionals within the United States.

Nature of the Study

For this exploratory multiple case study I used a qualitative research method. An exploratory multiple case study denotes an in-depth survey of a specific research problem instead of a comprehensive statistical inquiry (Crowe et al., 2011). It is typically employed to narrow an extensive research field into one narrow and more suitable area for in-depth research (Mocanu et al., 2018). Despite its strengths, some researchers are concerned that in employing the case-study analysis method, the research team may be exposed to the subjects for an extended period, resulting in biases (Hercegovac et al., 2020). It has further been pointed out by Crowe et al. (2011) that essential information can be missing, thereby making it impossible to interpret the collected data. According to Crowe et al. (2011), a case study allows for in-depth, multifaceted explorations of

complex issues in real-life settings. The research method is popular in business, law, and policy (Hercegovac et al., 2020), and its application can aid in answering my research question. Therefore, an exploratory case study can reduce complex issues to well-understood themes while simultaneously allowing research teams to extend their experiences into the survey (Yin, 2018). This research lacks the definite identifiable variables and elements of a quantitative study; thus, using a qualitative design provides an appropriate conceptual framework for analysis (Collins & Stockton, 2018).

This case study's population was comprised of IT professionals with at least 5 years of professional experience working in DevSecOps, managing teams of at least three DevSecOps professionals. They have implemented or are in the process of implementing AI into their DevSecOps pipeline. To identify some of the strategies cybersecurity professionals use to incorporate AI technologies into DevSecOps pipelines, it was necessary to identify the root causes of the data breaches and create an inventory of the tools perpetrators use to compromise and attack the U.S. government and other institutions. The study includes published expert narratives and testimonies= and other remarks. In addition to identifying the root causes for data breaches in the examined cases, other artifacts included checking for instances of avoidance to implement advanced technology. For this study I relied on data extraction techniques and tools to tag, categorize, and consolidate specific interests for thematic analysis (Vaismoradi & Snelgrove, 2019). Comparing and contrasting affirmative arguments and counterarguments with various theoretical assumptions can support comprehension and help explain their relevance (Yin, 2018).

Research Question

What are some strategies cybersecurity professionals use to incorporate AI technologies in developing secure software for IT operations.

Demographic Questions

1. Without including your name or your organization's name, what is your current role, and how long have you been in similar roles?
2. How many years of experience do you have integrating AI as a cybersecurity professional?
3. What is the highest degree and certification earned in IT?
4. How many years of experience do you have working in cybersecurity.
5. How would you describe your knowledge level of security in a DevSecOps pipeline?

Interview Questions

1. To what extent does lack of know-how and competencies in AI affect cybersecurity?
2. How did you improve your knowledge of AI technologies as a cybersecurity professional?
3. If any, what types of solutions do you use to reduce human involvement during security vulnerability testing?
4. How can penetration testing be automated and enhanced by integrating AI into the DevSecOps pipeline?

5. What is the industry of the professional security organization you work for in implementing AI into their DevSecOps pipeline?
6. How can the integration of AI into DevSecOps lead to the mitigation of Zero-day vulnerabilities?
7. How does the integration of AI into your organization's DevSecOps pipeline affect its time to respond to security incidents?
8. What competencies are required to implement AI into your organization's DevSecOps pipeline?
9. What are some of the implications of lacking AI technological competencies to your organization's cybersecurity?
10. What AI solutions may reduce human intervention in conducting security vulnerability testing?

Conceptual Framework

The technological acceptance model (TAM) served as the basis for the conceptual framework for this study. TAM focuses on attitudes toward using a particular IT based on perceived usefulness and ease of use from a user's perspective (Granić & Marangunić, 2019). The DevSecOps pipeline is designed through the agile process to deliver secure software. TAM states that perceived ease of use and usefulness could help users accept and adopt new technologies (Farooq, 2021). Thus, the perceived usefulness of AI in cybersecurity could encourage security professionals to adopt this technology. Therefore, TAM is ideally suited among alternative theoretical models for this research.

TAM is one of the most significant extensions of Ajzen and Fishbein's theory of reasoned action (TRA), developed in 1983 (Sarver, 1983). The most generally used model of user acceptance and use of technology is Davis's technology acceptance model, also developed in 1989 (Davis, 1989). Many of TRA's attitude variables are replaced by two technology acceptance measures: ease of use and utility in TAM. Both TRA and TAM, which have major behavioral components, presume that once someone establishes an intention to act, they will be free to do so without restriction.

TAM has been a useful theoretical model for comprehending and explaining behavior in information system implementation and can be applied here to understand the use of AI by cybersecurity professionals (Sohn & Kwon, 2020). Professionals need to understand the technology before they accept it. This understanding includes knowledge of the implementation; otherwise, it prevents them from accepting it (Ahmed & Francis, 2019). The logical connections between the framework presented and the nature of my study include considering AI in profiling principal agents and automating the negotiations among them. The principal-agent problem is resolved by developing common goals between the different teams.

Definition of Terms

Agile: Relating to or denoting a project management method used primarily for software development. It is characterized by dividing tasks into short phases of work and frequent reassessment and adaptation of plans (Sinha & Das, 2021).

CI/CD Pipeline: CI/CD pipeline is the set of tools and the associated process workflows to achieve continuous integration and continuous delivery with build, test,

security, and release delivery activities, steered by a CI/CD orchestrator and automated as much as the practice allows (Parashar, 2021).

Cybersecurity, Software Cybersecurity: The preventative methods used to protect software from threats, weaknesses, and vulnerabilities (Lotz, 2020).

Delivery: The process by which a released software is placed into an artifact repository that the operational environment can download (Sinha & Das, 2021)

Deployment: The process by which the released software is downloaded and deployed to the production environment (Sinha & Das, 2021)

DevSecOps: DevSecOps is a software engineering culture and practice that aims at unifying software development (Dev), security (Sec), and operations (Ops). The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of software development: plan, develop, build, test, release, deliver, deploy, operate, and monitor (Woody et al., 2020).

DevSecOps Environment: Sets a runtime boundary for the software component to deploy and execute. Typical environments include development, integration, testing, pre-production, and production (Woody et al., 2020).

DevSecOps Phase: The software development, security, and operation activities in the software lifecycle are divided into phases. Each phase completes a part of related activities using tools (Woody et al., 2020).

DevSecOps Pipeline: DevSecOps pipeline is a collection of DevSecOps tools upon which the DevSecOps process workflows can be created and executed (Woody et al., 2020).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are beliefs and opinions accepted as truths by a researcher without measurable proof and introduce bias (Sebele-Mpofu, 2020). Several assumptions were made in conducting this study. First, I assumed cybersecurity professionals understand and answer the semistructured interview questions honestly. The second assumption I made is that cybersecurity professionals are qualified and considered experts in the relevant areas only if they can provide information regarding the integration of AI into the DevSecOps pipeline. My third assumption was that a qualitative research methodology effectively provides the data required for answering the research question. The fourth assumption was that individual interpretations of the data could affect the research direction. In order to address this assumption, I designed the interview questions to minimize bias and prevent my influence on the interviewee. To facilitate this approach, I relied on open-ended questions for the interview part of this study. My final assumption was that my research sample size and the data I collected from the participants I recruited were sufficient to answer my research question.

Limitations

Study limitations, or possible weaknesses, can relate to behavioral, social, or relational factors, the study's design, external validity, and the interview protocol (Schafer Astroth, 2018). As a result of using a multiple case study design, the examination of cases is limited. The interview protocol I relied on for this study was to

only collect the data needed to answer my research question. Considering these limitations, I could interpret my data and findings objectively and without bias.

Furthermore, my chosen research method was also a limitation of this study. Qualitative designs are unsuitable for empirical data analysis (Azungah, 2018). My choice of interview protocol and research method also limits the implications of my findings and their potential transferability (Korstjens & Moser, 2017). I have opted for a qualitative research design to ensure that my study can focus on rich descriptive data and contextual information. However, qualitative research lacks testable measures or statistical analysis.

In contrast, a case study can collect contextual data and explore how constructs are perceived within a particular context (Kumar, 2011). As I relied on a qualitative research method, the study's findings might be limited to a small group of participants and may not apply to the general population (see Rutberg & Bouikidis, 2018). Furthermore, in a qualitative study, validity is largely determined by the interview protocol and the qualifications of the researchers (Junior et al., 2019), which I discussed in the validity section of my study in greater detail. An exploratory case study approach may also introduce research biases due to extended exposure to study participants (Yin, 2018). However, this study mitigated the risk of bias by using narratives and testimony to provide an evidence-based survey, enabling me to understand the developing themes better.

Delimitations

Researchers must establish boundaries for their study to narrow or control its scope (Svensson & Doumas, 2013). In my study, I focused on two primary boundaries. First, I searched for IT professionals with at least 5 years of professional experience working in DevSecOps. Secondly, I only considered professionals managing teams of at least three DevSecOps professionals. The participants in the study must have met one of the following criteria: (a) their organization must have implemented AI into their DevSecOps pipeline and (b) they must be in the process of implementing DevSecOps into their pipeline or, like the DoD, must have the integration of AI in their strategic goals (Rawat et al., 2021). The criteria ensured that participants are relevant to this research and provide usable data.

Significance of the Study

There is a critical shortage of cybersecurity talent, about three million cybersecurity professionals globally and more frequent and impactful large-scale cyberattacks (Beuran et al., 2018). The shortage of cybersecurity talent and threat risk affects many aspects of software development, testing, and information security operations (Smith, 2018), which, in turn, drives a need to address security in all phases of the software development life cycle (Deschene, 2016). Compliance with cybersecurity requirements in business rules, processes, and governmental regulations is also necessary for the software development effort (Dawson, 2019). Therefore, the findings of this study may contribute to improving business practices by guiding software engineers on how to reduce software development risks through the coupling of AI and DevSecOps

The potential social impact of this study is that improvements in techniques to minimize security breaches may help mitigate the impact of those breaches on business performance and the different costs they bring to consumers (Furnell et al., 2020). Another potential impact could come from maximizing the value of vulnerability prevention, detection, and response (see Lu & Koufteros, 2019) through improvements in software engineering development practices (see Williams et al., 2018) and cybersecurity workforce motivation (see Kam, 2020). A further positive social change could be brought about by automation and improvement of penetration testing through the coupling of AI and DevSecOps. This coupling may aid in detecting zero-day vulnerabilities in software, the sort of vulnerabilities that may have escaped a firm's standard bug detection and correction schemes, and reduce the time needed for security reviews (see Kongnso, 2015). In aggregate, society may benefit from improved DevSecOps processes through the integration of AI, which could reduce fraud and better protect consumers' personal identifiable information (PII).

A Review of the Professional and Academic Literature

The literature review focused on a collection of resources about the current understanding of the relationship between AI technologies in developing secure software for IT operations and how the technology acceptance model can explain some of the underlying dynamics between AI and IT security. Zaydi and Nassereddine (2021) conducted a study and found that information technology service management (ITSM) can greatly benefit from automated monitoring, but to adapt best practices, professionals may first require a framework to understand the DevSecOps culture better. Similarly,

(Bhatele et al., 2019) suggested that the potential use of intelligent and automated systems is no longer limited to cybersecurity professionals and that cybercriminals are also increasingly employing AI-based approaches to attack and compromise information systems. Cybersecurity professionals must adapt their approaches accordingly to respond appropriately to the increasing threat of AI-based attacks (Zarina I. Khisamova, 2019).

The literature review incorporates peer-reviewed articles and journals, seminal works, reports, white papers, and regulations published since 2018. Of the resources I used in this study, 86.46% were published between 2017 and 2021, and 88 (91.66%) of the 96 resources I referred to in the literature review were peer-reviewed. The databases I used to collect my references included ScienceDirect, EBSCOhost, Google Scholar, ProQuest, SAGE Journals Online, and Thoreau as an aggregator for various databases. I verified the academic journals I used as part of this review for their peer-review status through Ulrich's Global Serials Directory. While I employed a follow-up search strategy, linking related articles and publications to my initial search results, I focused on keywords related to my conceptual framework, like *AI, DevSecOps, cybersecurity,* and *common practices related to using automated systems across the DevSecOps process*. The keywords I used were *DecSecOps, IT project management, SDLC, software development, AI, automated security practices, AI frameworks, social change, society, technology acceptance, cybersecurity, IT development*, and *software security*. My initial focus on the abstracts of each resource allowed me to screen my search results for relevance so that I could select those most applicable to my research and warranted inclusion. Lastly, the in-depth evaluation of resources enabled me to find related articles

suggested by the search engines or referenced within the resources I examined, allowing me to understand the examined topics thoroughly.

I focused my review of the academic literature on three areas: (a) the technology acceptance model, (b) DevSecOps frameworks, and (c) the use of AI in DevSecOps. Limiting the academic and professional literature to these themes allowed me to focus my research on examining existing AI frameworks and solutions and how they could be applied in the DevSecOps pipeline. Examining current trends through the lens of the technology acceptance model enabled me to evaluate the use of AI in DevSecOps and identify why some professionals are more likely to include automated systems than others.

The Technology Acceptance Model

Researchers frequently use the TAM to examine how individuals adapt to and use technology (Ajibade, 2018). While the acceptance of technology, particularly newly introduced technology, can be influenced by many factors, the TAM asserts that perceived norms, usefulness, and ease of use impact an individual's willingness to adapt to technology (Davis, 1986, 1989). For example, Mushtaq et al. (2018) studied consumers' acceptance of autonomous vehicles. However, they noted that the lack of perceived usefulness and established norms limited the ability of participants to imagine if and how they would adapt to such a technology when it becomes available. In another study with 276 participants on the adaption and use of smartwatches, the researchers found that a willingness to use a smartwatch directly correlated with its perceived hedonic and utilitarian value, suggesting that consumer innovativeness may also be an

important factor related to technology acceptance (Hong et al., 2016). As this study aims to examine the strategies some DevSecOps professionals use to integrate AI into their security pipeline, the TAM offers a useful lens through which perceived usefulness and utility can be studied in the context of willingness to adopt new technologies into existing processes. In particular, the TAM can be applied to understanding users' perceived usefulness and ease of use attitudes toward a particular IT (Ajibade, 2018).

Evolution of the TAM

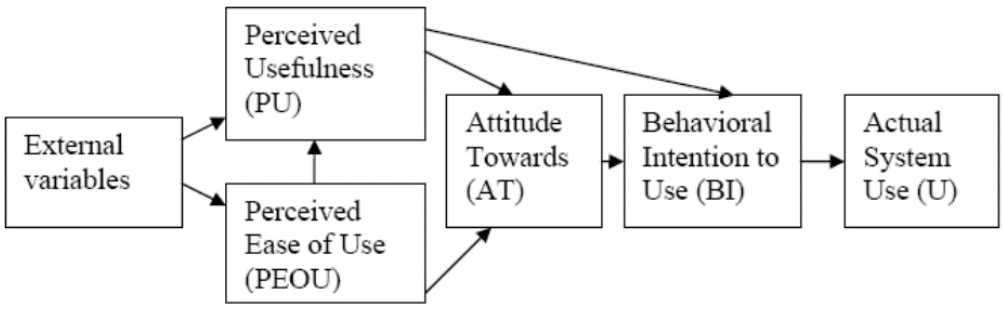
First developed by Davis (1986), TAM assumes that two primary factors influence the willingness to accept technology: (a) perceived usefulness and (b) perceived ease of use. By extending the theory of reasoned action (Fishbein & Ajzen, 1980) and focusing on technology acceptance measures instead of attitudes, TAM is better suited for examining IT-related adoption behavior. Although TAM has frequently been criticized for its limited predictive power and lack of transferability beyond traditional IT, researchers continue to use and expand upon its original concepts (Granić & Marangunić, 2019). These evolutionary expansions include the TAM2 and the unified theory of acceptance and use of technology, or UTAUT, for example (Venkatesh & Davis, 2000; Venkatesh et al., 2003). Even though the UTAUT assesses the acceptance of information technology through (a) performance, (b) effort expectancy, (c) social influence, and (d) facilitating conditions, the focus on assessing intention and behavior may not be a good fit for examining all information systems usage behavior equally (Venkatesh et al., 2003).

For example, Rahman et al. (2017) examined the usefulness of TAM, UTAUT, and the theory of planned behavior for predicting users' perception of the usefulness of

driver assistance systems. The researchers found that all theories offered a significant predictive power for estimating outcomes, even though TAM performed best, apparently due to its focus on only two behavioral factors, creating a more diffuse filter for categorizing intentions (Rahman et al., 2017). In another study, TAM was used together with other theories to assess the behavioral impact of consumer innovativeness on the intended use of a smartwatch (Hong et al., 2016). As with many other studies, the TAM was used to understand behavior and intention better, and its findings formed the basis for informing other theories for further examination of perceived relationships and behavioral patterns. While TAM is often expanded through other theories for a more finely grained explanation of examined phenomena, its universal and somewhat broad approach to intention and behavioral examination in the context of IT made it the preferred choice for this study.

Figure 1

Primary Factors in the Technology Acceptance Model



Note: An overview of TAM primary factors. Reprinted from "Understanding the adoption and usage of mobile payment services by using TAM," by M. I. Jaradat, & A. Al-Mashaqba, 2014, *Int. J. of Business Information Systems, 16*, 271-296. Copyright 2014 by M. I. Jaradat, & A. Al-Mashaqba. Reprinted with permission.

Application of the TAM

TAM has been widely used to examine behavioral aspects of using technology. While it can be argued that TAM is primarily designed to examine the intentions when using information technology, given that consumer electronics heavily rely on microcontrollers, any newly introduced technology, by extension, is an IT-related product, and, thus, TAM has also been used to explain user behavior on a variety of products or innovations other than traditional hardware and software (An-Chi & Tsung-Yu, 2020; Chuttur, 2009; Masrom, 2007; Miko, 2017; Panagiotopoulos & Dimitrakopoulos, 2018; Tavares & Oliveira, 2017). For example, Masrom (2007) used TAM to examine users' intention to participate and embrace online learning, whereas (Al-Emran, 2021) aimed to explain their willingness to adapt to and the usage of smartwatches. Traditionally, TAM can be a predictor for information systems usage when acquiring information systems literacy (Mohammad Ebrahimzadeh Sepasgozar et al., 2020).

Considering the broad application of TAM for acceptance-related research whenever technology is involved (Granić & Marangunić, 2019), TAM presents itself as an ideal fit for this study, as it can examine the perceived usefulness and ease of use in the context of software development. In particular, as far as the introduction of new software capabilities or workflows goes, ease of use and perceived usefulness seem to be the primary factors influencing technology acceptance (Granić & Marangunić, 2019). However, training on new features can also impact behavior (Riemenschneider & Hardgrave, 2001). Considering the lack of current literature on the acceptance of AI in

the DevSecOps pipeline and especially the intentions to use or further such implementations by relevant professionals, TAM offers a broad approach to capturing behavioral patterns related to the issue. While other theories exist that could be used to examine the questions of acceptance and motivations, I chose TAM as it is better equipped to address the central research question.

Supporting Theories

Software development, particularly the acceptance of software and technology, has been examined through various theories and frameworks. While TAM is one approach to assessing and predicting behavior and related acceptance, other theories could be used as an alternative to examining the research question of this study from a different angle. For example, the acceptance of features and processes used in software development has been examined using the unified theory of acceptance and use of technology (Venkatesh et al., 2003; Widianto et al., 2020). In another example, sociotechnical systems theory was used to assess best how to integrate AI into an organization (Makarius et al., 2020).

Unified Theory of Acceptance and Use of Technology

The UTAUT is a logical extension of TAM. It incorporates additional factors into the assessment of technology adoption at the workplace by adding (a) social influence, (b) performance expectancy, (c) facilitating conditions, and (d) effort expectancy (Venkatesh et al., 2003). For example, Widianto et al. (2020) used UTAUT to examine user preferences for mobile software development approaches. While many approaches exist, the researchers found that most developers were reluctant to implement alternatives

and thus preferred a waterfall approach to software development. Although their analysis stopped there, some factors that influence the resistance to adapt to more modern software development approaches could likely be investigated in the context of AI adaption in the DevSecOps pipeline.

To examine user acceptance and intentions to use AI when introduced to a customer relationship management (CRM) system, Sheshadri Chatterjee et al. (2021) studied data from 315 organizational users in India. They used UTAUT to assess factors that might influence this new technology's adaption and perceived usefulness. The researchers found that performance expectancy, effort expectancy, facilitating conditions, compatibility, CRM quality, and CRM satisfaction influence behavioral intentions for using an AI-enhanced CRM. However, the study also revealed that the user's attitude toward an AI-based solution influenced behavioral intention and actual user behavior. While some operations-supporting staff primarily use CRM systems, similar concerns and observations may apply to the adaption and willingness to use AI in the DevSecOps pipeline.

Sociotechnical Systems Theory

Researchers often rely on the sociotechnical systems theory to investigate how technical systems impact social behavior (Tyfield & Zuev, 2018). For example, IT systems are generally subject to various sociological and behavioral forces, and the implementation or effectiveness should also consider sociotechnical forces as part of a holistic approach (Laracy & Marlowe, 2018). While ensuring ongoing system and software security may often require an agile approach to software development and

software lifecycle management, the researchers argue that tensions between the socio-technological viewpoint and the practical requirements for developing and maintaining secure systems may sometimes be incompatible. While looking at the implementation and use of AI in the DevSecOps pipeline can be examined through the lens of socio-technical systems theory, using this framework would arguably limit the scope of this research to social behavior and somewhat neglect the forces exerted by individual preference and motivations as intended by this study.

Theory of Reasoned Action.

The theory of reasoned action informed the development of TAM (Venkatesh et al., 2003). With its initial constructs developed by Fishbein (1976), subsequent refinements asserted that human behavior is primarily driven by attitude, where the actual behavior is determined by the individual's intention to perform this behavior before the action takes place (Fishbein & Ajzen, 1980; Fishbein & Ajzen, 1977). While it could be argued that the willingness to incorporate AI into the DevsSecOps pipeline is based on an intentional behavior, the focus of this study is to examine the strategies that some DevSecOps professionals use to incorporate AI into the DevSecOps pipeline and not whether behavioral intentions exist that would prevent them from doing so. Therefore, the theory of reasoned actions was rejected as a suitable lens for this study as it may be better suited to examine intentions rather than strategies for incorporating technology.

Contrasting Theories

As the previous section illustrates, several supporting theories could be used to examine the research question through alternative lenses. However, I decided to apply

TAM as the conceptual framework for my study. It needs to be noted that several contrasting theories exist. Contrasting theories approach a construct through a different lens or understanding of the matter (Marcelin et al., 2019). I briefly examined and highlight some of them to illustrate why they are inappropriate as a conceptual framework.

Complexity Theory

Researchers often use complexity theory as part of a risk assessment to study the organizational and technical complexity of systems and evaluate associated uncertainties (Mihić et al., 2018). While complexity theory is most commonly used to assess risk in complex systems (Cicmil et al., 2017; Emblemsvåg, 2020), other use-cases are possible. For example, Lemon and Macklin (2021) used complexity theory to understand employee engagement and associated systems better. As this study seeks to identify the strategies some security professionals use to incorporate AI into the DevSecOps pipeline, a conceptual framework that is primarily suitable for evaluating uncertainty or assessing individual risk would be unlikely to answer the research question.

General Systems Theory

General systems theory (GST) is often used to examine the interactions between organizational and technological factors in a system, where changes in one system directly impact another (Sutirtha Chatterjee et al., 2021). While GST is not frequently associated with AI or DevSecOps processes, Mämmelä et al. (2018) used GST and other theories as a multi-faceted lens to examine self-organizing and autonomous technologies used in multiple disciplines for a better understanding of highly intelligent and

autonomous decision-making processes. Here, the GST could examine how the use of AI in DevSecOps influences the perceptions and acceptance of such technologies and, in turn, how a lack thereof would equally impact the willingness to adopt AI into a given workflow. Although this approach could arguably yield some interesting findings, the focus of this study is to identify cybersecurity professionals' strategies to incorporate AI technologies in developing secure software for IT operations and some of the challenges they may face. Because GST is better suited for examining cause and effect relationships between variables, it was not a good fit here as this study aims to identify some of those relationships without assuming they even exist.

Theory of Dynamic Capabilities

First developed by Teece et al. (1997), the theory of dynamic capabilities asserts that organizations need to manage knowledge and competencies, develop resources to innovate, and continuously gain or maintain a competitive advantage. Previously, the theory of dynamic capabilities has been used to evaluate marketing as a way to gain a competitive advantage (Ferreira et al., 2018), examine strategies used for autonomous vehicle development (Munoz, 2020a), and explore the relationships between innovation, dynamic capabilities, and organizational leadership (Schoemaker et al., 2018), for example. While using AI in the DevSecOps pipeline could certainly offer a competitive advantage, I aimed to identify current strategies some security professionals use to implement AI into the DevSecOps pipeline and not whether such implementation offers a competitive advantage and how it could contribute to a firm's dynamic capabilities.

AI and DevSecOps Frameworks

With advancements in computer technologies, software continues to become more complex. The added complexity also increases the associated security risk as more developers work on more elaborate systems, making the probability of human error or undetected vulnerabilities more likely (Williams et al., 2018). Although integrating automated detection systems into the DevSecOps pipeline is ongoing, using AI to fine-tune these approaches beyond merely recognizing patterns presents additional challenges (Bhatele et al., 2019). The following section examines the current literature on frequently used DevSecOps and AI frameworks in connection with these technologies and their common practices.

Frameworks and Practices used in DevSecOps

DevSecOps frameworks emerge around industry best practices and are often integrated as part of an organization's cybersecurity and continuous integration and development efforts (Rangnau et al., 2020; Woody et al., 2020). DevSecOps, then, are often integrated into the software development lifecycle (SDLC), utilize user acceptance testing (UAT), and rely on dynamic and static testing approaches (Ahmed & Francis, 2019; Mohammed et al., 2017; Rangnau et al., 2020; Venkatesh et al., 2003). Furthermore, in a meta-analysis of common DevSecOps practices, Mohammed et al. (2017) identified five main categories, including (a) secure requirements modeling; (b) vulnerability identification, adaption, and mitigation; (c) software security-focused process; (d) extended UML-based secure modeling profiles; (e) non-UML-based secure modeling notations.

Software Development Lifecycle

The SDLC is a process-oriented framework used in the software industry to conceptualize, develop, test, and maintain software throughout its life cycle (Usha Rani, 2017). A major concern developers aim to address by using an SDLC framework is ensuring reliability and quality, providing documentation, and enabling certification (Falcini & Lami, 2017; Mohammed et al., 2017). SDLC is closely associated with DevSecOps, with water fall software development approaches being the preferred approach by engineers for many years (Singh et al., 2020). More recently, agile methodologies have been used increasingly in software development projects and across DevSecOps (Zaydi & Nassereddine, 2021). Agile development approaches, in particular, exhibit elevated software security and vulnerability identification and mitigation concerns, requiring developers and security professionals to work side-by-side and integrate security tools to produce a specific software product (Alnaim, 2019).

The initiation phase of the SDLC is critical to ensuring that a system is correctly planned for and developed. This phase is initiated by the decision to design and implement the system. Generally, the SDLC involves seven development stages, including (a) initiation, (b) planning, (c) feasibility, (d) design and prototyping, (e) software development, (f) implementation and integration, and (g) operations and maintenance (Khan et al., 2021; Sorte et al., 2015). Researchers have argued for DevSecOps to be integrated into several of the stages of development to ensure the quality and security of the software during the development lifecycle (Mohammed et al., 2017; Usha Rani, 2017), thus improving software security and reducing vulnerabilities

throughout the process (Deschene, 2016; Fujdiak et al., 2019). While many DevSecOps professionals have adopted manual and automated processes within the SDLC to secure software products, general requirements or universal best practices are missing (Fujdiak et al., 2019; Lam & Chaillan, 2019; Maro et al., 2018; Rice, 2019; Tomas et al., 2019; Zaydi & Nassereddine, 2021). Furthermore, following best practices becomes increasingly difficult when software developers rely on agile frameworks within the SDLC, where changes often happen rapidly and may have wide-ranging implications for the project's functionality, codebase, and overall security (Ahmed & Francis, 2019; Williams et al., 2018).

Continuous Integration and Delivery

Continuous integration (CI) and continuous delivery (CD) approaches serve as a framework for quality assurance in rapidly evolving software development environments, such as could often be found when an agile software development approach is used (Shajadi, 2018; Zaydi & Nassereddine, 2021). Rapid changes across the entire software development life cycle require refined and automated testing and quality assurance approaches, where traditional manual testing procedures fall short. The automated approach to CI and CD is especially useful in DevSecOps. It can reduce the security professional's constant review and testing burden and reduce vulnerabilities and quality issues to those that fail to be detected automatically (Kumar & Goyal, 2020; Rangnau et al., 2020).

While CI and CD greatly improve the ability to test and improve software automatically, they are not without shortcomings. In particular, most literature on CI and

CD only covers static approaches to automated software testing, whereas a dynamic approach may often lead to better results (Rangnau et al., 2020). For example, many tools used to test web applications before delivery for vulnerabilities automatically rely on pattern matching and predefined testing processes, thus reducing their efficiency to how well the security professional identifies potential vulnerabilities and selects the appropriate tests (Shajadi, 2018). Using rule-based systems for testing throughout the CI and CD cycles is only as good as the rules they are based on, resulting in potentially many untested and insecure scenarios not covered by this approach (Alnaim, 2019; Rangnau et al., 2020; Smith, 2018). While CI and CD aim to simplify and automate the processes required to deliver and integrate software updates into production environments, the shortcomings of commonly used rule-based automation tools for testing limit the security professional's ability to adequately reduce the risk of unknown and future vulnerabilities (Alnaim, 2019; Shajadi, 2018).

User Acceptance Testing

The final stage within the SDLC is user acceptance testing (UAT). UAT aims to validate whether a given software meets its design and functionality goals (Lobkov, 2019). Generally, UAT is a manual process where security professionals, engineers, and customers validate whether the software is meeting requirements (Sanders et al., 2021). However, some rule-based automation exists to streamline the testing processes (Camilleri et al., 2020; Sualim et al., 2017). Considering the manual approach to UAT, regressions after making changes or introducing vulnerabilities during the process are common issues security professionals must be aware of (Mitev, 2020).

In particular, UAT only aims to test for compliance with requirements but not particular vulnerabilities or security overall, as is generally of interest to the DevSecOps professional (Sanders et al., 2021). While testing for user acceptance is as much a usability test as it is to confirm intended outcomes, the lack of automation processes beyond usability and functionality can cause significant issues for DevSecOps professionals (Mitev, 2020; Sanders et al., 2021; Sualim et al., 2017). For example, web-based semiautomated user acceptance testing often fails to include vulnerability testing, which then requires the security professional to conduct additional tests, further disconnecting them from the software development and delivery process (Camilleri et al., 2020; Rangnau et al., 2020; Sualim et al., 2017). While UAT is an important aspect of the SDLC, it does not integrate well with the objectives DevSecOps professionals pursue and instead may create redundancies and result in inefficient and insecure software development cycles (Fujdiak et al., 2019; Lobkov, 2019; Mitev, 2020; Queiroz et al., 2018; Shajadi, 2018).

The Use of AI in DevSecOps

Currently, AI solutions can be divided into two categories: (a) static and (b) dynamic solutions (Haenlein & Kaplan, 2019). Most AI applications today rely on a static solution where a ML model is trained on existing data to extrapolate how well new data would relate to the model, giving an approximation of how close something unknown is to something that is known (Hatcher & Yu, 2018; Munoz, 2020a). In contrast, dynamic AI approaches assume that the computer system can learn new relationships and derive strategies without the presence of particularly annotated training

data, approaching a learning behavior similar to that of the human brain (Mocanu et al., 2018). Unsupervised or dynamic approaches have the potential to dramatically influence an AI's ability to learn and derive solutions for unknown problems (Maurer et al., 2021) but may also offer new ways for criminals to exploit existing computer systems and software in a way that has not yet been anticipated (Bhatele et al., 2019; Caravelli & Jones, 2019; Sullivan, 2018; Zarina I. Khisamova, 2019).

General Application of AI

AI sees wide application in today's technology. From translation to text and speech processing (Hatcher & Yu, 2018), self-driving vehicles (Gallardo et al., 2017; Hatcher & Yu, 2018; Stilgoe, 2018), cybersecurity (Bhatele et al., 2019; Dawson, 2020; Department of Defense, 2018; Mori, 2018; Veiga, 2018; Zarina I. Khisamova, 2019), and shopping solutions (Paul et al., 2021), to name a few. Most of these systems are static AI solutions and heavily rely on pre-trained models, making high-quality training data imperative (Ming Deng & Yuying Cao, 2018; Rao & Frtunikj, 2018). In that regard, these commonly found AI applications make decisions based on previously learned information where the output is limited to predefined categories or binary options.

For example, an AI focused on detecting traffic lights will only detect those it has learned to interpret. A stop sign, although indicating to a driver to come to a standstill similar to a red light, would not elicit the same response from an AI trained only to recognize traffic lights (Munoz, 2020b; Rao & Frtunikj, 2018; Sadighi et al., 2018; Van Brummelen et al., 2018). Likewise, an AI trained to anticipate irregular network traffic is likely only able to identify unusual traffic, whether it is legitimate or not, but not those

data packets that are disguised as expected or normal interactions (Korzeniowski & Goczyla, 2019; Sullivan, 2018; Zarina I. Khisamova, 2019). While virtual assistance systems, such as Siri or Alexa, suggest a dynamic approach to AI, they are essentially only dynamic in learning how to interpret spoken words but less so when asked to do something new (George et al., 2021). It is conceivable that static AI solutions are sufficient for many applications, whereas successful use in cybersecurity and DevSecOps may require more sophisticated approaches (Chatterjee, 2019; Sullivan, 2018).

Application of AI in DevSecOps

As an integral part of the SDLC, DevSecOps aims to understand the software lifecycle and identify vulnerabilities or other security concerns to strengthen the resilience and reliability of software while also reducing cyberattacks and preventing damage (Ahmed & Francis, 2019; Lam & Chaillan, 2019; Rice, 2019). The use of AI in DevSecOps primarily aligns with how AI is used in other AI environments, including the creation of AI-based filters and rules which can detect abnormal behavior or carry out attacks on software and infrastructure to simulate a potential intrusion attempt (Caravelli & Jones, 2019; Dawson, 2020; Khan et al., 2021; Kumar & Goyal, 2020). One advantage of automating some testing in DevSecOps operations is that AI-based systems can scan software and systems much faster than a human could achieve manually, thus allowing the security professional to focus on particular concerns rather than general security (Dallas, 2020). While AI-based filters and rules have dramatically improved the odds of finding vulnerabilities or identifying attacks, cybercriminals use similar tools to probe for

existing and new vulnerabilities, somewhat negating the advances security professionals have made since starting to incorporate AI into their strategies (Sullivan, 2018).

Most commonly, DevSecOps professionals use AI-based testing to scan for vulnerabilities (Mohammed et al., 2017; Williams et al., 2018), test for user acceptance (Camilleri et al., 2020; Rangnau et al., 2020; Shajadi, 2018), test for compliance (Alnaim, 2019; Dawson, 2019; Kumar & Goyal, 2020), and identify ongoing or attempted attacks (Alnaim, 2019; Sullivan, 2018; Williams et al., 2018; Woody et al., 2020). Therefore, the use of AI in DevSecOps is mostly limited to rule and filter automation, but a few novel approaches aim to redefine and expand on the current ones. For example, Bahaa et al. (2021) explained that unsupervised or dynamic ML models offer better AI performance than static rule and filter-based approaches when detecting intrusion attempts. Unsupervised advantages seem to hold, particularly where novel attack vectors were used to circumvent the static rules and filters where traditional AI approaches performed poorly in comparison (Bahaa et al., 2021). While dynamic, unsupervised approaches to AI show promising results, these technologies have yet to be adopted widely, and it remains to be seen how effective they will be once hackers employ similar approaches (Sullivan, 2018).

Common Challenges in DevSecOps

DevSecOps best practices should be maintained to enable continuous IT services delivery with a considerable security risk, and, thus, security should be integrated into all points of software development (Zaydi & Nassereddine, 2021). While DevOps supports a culture that enables teambuilding by promoting cooperation and communication, SecOps,

on the other hand, is a variant of DevOps centered on security. Its culture is essential in development, enabling the team to focus intensely on possible vulnerabilities and address them accordingly. However, while efficient communication is imperative within software security workflows, AI-assisted automation may overcome these requirements by reducing the need for interaction (Ahmed & Francis, 2019; Alnaim, 2019; Khan et al., 2021).

One of the challenges multilevel security analysts face is reviewing many warnings, logs, and other reports to assess security risks and identify vulnerabilities (Ahmed & Francis, 2019; Rice, 2019). In contrast, when automated detecting systems are deployed, large datasets can be reviewed and analyzed in a fraction of the time it takes an analyst to do the same (Chatterjee, 2019). Furthermore, when ML is integrated into the development cycle, AI can help transform diagnostics across many systems, subsequently helping the developers be vigilant of faults which can often lead to the faster resolution of errors (Dallas, 2020). The challenge DevSecOps professionals face, however, is that these AI-based systems are not universal, are not used everywhere, often require additional training to be set up effectively, and are often not equally embraced by all developers or security professionals within the DevSecOps teams (Dawson, 2020; Tomas et al., 2019; Woody et al., 2020).

In a study conducted among developers on their DevSecOps practices, a lack of early integration of security practices rooted in the four pillars of DevOps, namely culture, automation, sharing, and measurement, stood out (Tomas et al., 2019). The findings counter the goal of DevSecOps, where collaboration within the security teams

and developing an integrative security culture is considered essential (Lam & Chaillan, 2019; Woody et al., 2020; Zaydi & Nassereddine, 2021). Kumar and Goyal (2020) suggested that if an organization wants to get to true DevSecOps, it must foster a culture of collaboration, communication, and sharing among developers and security professionals. While a continuous security framework may provide a standard minimum set of processes (Kumar & Goyal, 2020, p. 6) to achieve these goals, the reality of most DevSecOps suggests a lack of uniformity and unity among security professionals and software developers (Ahmed & Francis, 2019; Lee, 2018; Rice, 2019; Tomas et al., 2019).

Gap in the Literature

The early integration of security is essential to delivering a secure software application. Although research has resulted in many models and recommendations for best practices, no universal standard exists for including AI in existing workflows (Sharma et al., 2020; Sorte et al., 2015). While security solutions have been integrated into software engineering and security methodologies for more than two decades, the use of AI, as illustrated in Table 1, and in particular the use of dynamic AI based on unsupervised learning, has only been explored recently and has yet to see universal adoption (Bahaa et al., 2021; Dallas, 2020; Dawson, 2020; Rangnau et al., 2020; Rice, 2019; Soni et al., 2020). Similarly, research efforts on unsupervised AI to gain a competitive advantage over cybercriminals or improve the DevSecOps workflow and its overall effectiveness and efficiency are minimal. The literature currently fails to address why unsupervised learning is not actively encouraged among security professionals.

Supervised ML continues to be the dominant approach for creating AI solutions, regardless of industry. DevSecOps and most cybersecurity operations mostly rely on supervised learning, where a computer program is taught to recognize malware through a set of training data. The resulting model is used to evaluate new inputs for their likelihood of matching a recognizable pattern: the output will determine whether something is more likely to be of one kind than the other, assisting in detecting malware (Yang et al., 2015). However, this approach is not without fault, as it can only detect a pattern that aligns with the trained data but not those that deviate from the learned approach. In particular, supervised learning may only lead to temporary success with securing software and systems, and the lack of literature in this regard illustrates how researchers often oversimplify AI in the context of DevSecOps and fail to address the current shortcomings (Bahaa et al., 2021; Chatterjee, 2019; Dawson, 2020; Kumar & Goyal, 2020; Sanders et al., 2021; Zaydi & Nassereddine, 2021).

Table 1

Selected Studies on Common DevSecOps Practices and Use of AI

Author/date	Research Focus	Findings
Zarina I., K., Ildar R., B., & Elina L., S. (2019)	AI and problems of ensuring cybersecurity.	The authors analyzed in detail the main problems in the field of cybersecurity in connection with the active use of AI
(Dawson, 2019)	Is AI the future of DevSecOps?	The role AI and ML have in the future of DevSecOps.
(Yang et al., 2015)	Application of hybrid ML to detect and remove malware	Transactions on ML and AI 2015
(Zaydi & Nassereddine, 2021)	DevSecOps practices for an agile and secure IT service management	This paper investigates how DevSecOps culture can be applied in IT service management.
(Dilek et al., 2015)	Applications of AI techniques to combating cybercrimes: A review	This study presents advances made so far in applying AI techniques for combating cybercrimes, demonstrating how these techniques can be an effective tool for detection and prevention of cyber-attacks, and giving the scope for future work.
(Sorte et al., 2015)	Use of AI in software development life cycle: a state of the art review	This paper presents a state-of-the-art literature review that reveals the past and present work done for automating Software Development Life Cycle (SDLC) using AI.
(Lee, 2018)	The DevSecOps and Agency Theory	Development of a framework based on Agency Theory that sheds light on the role of goal incongruency and information asymmetry in the DevSecOps context.
Mori (2018)	Us defense innovation and AI	The article makes two caveats regarding the actual introduction of AI into the US battle network and briefly points to implications for US allies.

Transistion and Summary

I reviewed several challenges in Section 1 that DevSecOps professionals face during daily operations and integrating AI into their workflows. I followed up with a discussion on the background of the problem and an overview of the literature on DevSecOps practices, the use of AI in IT, and how a lack of acceptance and knowledge among professionals may limit the integration of the former. I also reviewed the technology acceptance model as the underlying conceptual framework I used as a lens through which I examined the findings of my study. Furthermore, I added a discussion on the evolution of the technology acceptance model and its origins and an overview of a selection of supporting and contrasting theories.

Furthermore, I will continue this discussion in Section 2, where I describe the methodology, the role of the researcher, the participants, and how I intend to collect and analyze the data for this study. I also include a review of my approach to population and sampling, study validity, ethical research, and instrumentation related to the study. I close out Section 2 by detailing my preference for the chosen methodology and discussing my interview protocol.

Section 2: The Project

Section 2 expands on the methodology I used and defines the researcher's role and my participant selection process. I outline how I collected and analyzed the research data for my study. This section also includes a review of my approach to the population sample, study validity, ethical research, and instrumentation related to the study. I close

the section by justifying my preference for the chosen methodology and discussing my interview protocol.

Purpose Statement

The purpose of this qualitative exploratory multiple case study of cybersecurity professionals was to study the strategies that cybersecurity professionals use to incorporate AI technologies in developing secure software for IT operations (DevSecOps). Furthermore, I explored the challenges of integrating AI solutions in the DevSecOps pipeline by identifying today's strategies to improve organizational security. Bringing awareness about the security challenges in the DevSecOps pipeline may enable IT security leaders to identify knowledge gaps and facilitate the necessary training of their employees.

Therefore, I aimed to address the development of frameworks and algorithms to ensure that AI as a tool is employed efficiently. The implications for positive social change include a better understanding of how cybersecurity specialists successfully integrate AI into the DevSecOps pipeline to make more secure software products. Understanding AI integration could improve many organizations' security posture and, by extension, the societies and individuals they serve. This study's sample group was comprised of IT professionals with at least 5 years of professional experience working in DevSecOps, managing teams of at least three DevSecOps professionals.

Role of the Researcher

The qualitative exploratory multiple case study method is prevalent in many areas but is highly appealing in applied disciplines (Abdalla et al., 2018). Applied disciplines

study processes, problems, and programs to improve understanding of phenomena (Abdalla et al., 2018). As the researcher, I was the primary instrument in collecting the data, meaning I collect, sort, and organize the data for analysis and interpretation.

In this multiple case study, my role was to develop interview questions aligned with the overarching research question. The questions are designed to capture the needed data to complete an unbiased analysis of the data. As a cybersecurity engineer, I have 8 years of professional experience and a great interest in the research topic. Even though the researcher's positionality can lead to research bias, approaching the research from a different lens can limit the impact (Holmes, 2020).

A researcher should standardize the questions asked, allowing them to minimize research and observed bias (Hoyer et al., 2018). Other methods, such as participant observation and organizational reports, can further reduce research bias (Korstjens & Moser, 2017). Furthermore, I also include published expert narratives, testimonies, and other remarks as part of this study. In addition to identifying the root causes for data breaches in the examined cases, other artifacts include checking for instances of avoidance to implement advanced technology. Data extraction techniques and tools to tag, categorize, and consolidate specific interests for thematic analysis are common in qualitative studies (Vaismoradi & Snelgrove, 2019), so I relied on them here. Comparing and contrasting affirmative arguments and counterarguments with various theoretical assumptions supported comprehension and help explain their relevance (Yin, 2018). Furthermore, by following established research procedures and using structured questions during data gathering, I ensured that I asked each participant the same questions. Asking

all participants the same structured questions can lead to more objective data (Stenfors et al., 2020).

Even though I selected organizations where I have a previous connection, I ensured that I have not previously worked with the study participants or am related to them. Another critical role of the researcher is to ensure the ethical treatment of all research participants. I followed the guidelines provided by the Belmont Report released by the National Commission for the Protection of Human Subjects for participants' ethical treatment and any additional requirements specified by Walden University. Each participant was required to review the consent forms I shared, informing them of their right to opt-out of the study at any time. I obtained all participant consent through email.

An interview protocol ensures that all interviews are conducted similarly, thus reducing the potential impact of bias (Williams et al., 2020). Using an interview protocol, a researcher can maintain neutrality and operate merely as a facilitator (McGrath et al., 2019). Then, an interview protocol serves as a checklist to guarantee that all participants are asked questions in the same way and that questions do not lead the participant or fail to probe an answer thoroughly (McGrath et al., 2019).

Participants

Ten IT professionals with at least 5 years of professional experience working in DevSecOps and who have managed teams of at least three DevSecOps professionals participated in my study. Participants had to be cybersecurity professionals who have implemented or are implementing AI into their DevSecOps pipeline. The selection of participants is a critical milestone in the research process; thus, ensuring that participants

have experience in the research topic is critical to their selection (Humble & Radina, 2018). For my study, I used LinkedIn and emails to recruit participants. LinkedIn allowed me to read the participant's background experiences and determine their fit for the research. I then contacted the security professionals requesting their participation in the research. I explained to them the study's purpose and their participation level.

I established a working relationship with participants for face-to-face interviewing by clarifying the scope of the study and how individuals would fit into the research, as stated in the interview protocol (Lunt et al., 2019). The consent form lists the criteria or qualifications for participant selection and outlines the study, including questions to qualify participants and explain the roles of the participants and the research team. Participants must be informed about the study during a consent process, and their participation should be volunteered (Lunt et al., 2019). Furthermore, I informed all participants that their identities in the study will remain anonymous. Anonymizing participants is integral to sound ethical research, and researchers can protect participants by ensuring anonymity and confidentiality (Hesse et al., 2019).

Research Method

I used a qualitative research method for this study. The qualitative technique is a research approach that considers human characteristics, feelings, and experiences as input into study conclusions (Popescul & Jitaru, 2017). A qualitative researcher investigates participants' perspectives of a phenomenon to provide in-depth descriptions and personal understanding, giving significance to their experiences (Popescul & Jitaru, 2017).

Researchers use the qualitative technique to investigate participants' perspectives (Abdalla et al., 2018).

The qualitative method is efficient in research involving human participants in their circumstances and contexts (Popescul & Jitaru, 2017). It focuses on the inquiry's nature, which leads to the generation of questions (Holmes, 2020). Qualitative research often relies on open-ended interview questions. Open-ended questions allow participants to offer information beyond yes-or-no responses (Popescul & Jitaru, 2017). Open-ended questions provide a wide range of responses, including a participant's experience, perception, or understanding (Popescul & Jitaru, 2017). Results may contain a participant's thoughts, opinions, suggestions, or ideas, depending on the nature of the questions.

Popescul and Jitaru (2017) found that overarching research questions can lead to subquestions that help to inform the research investigation. Qualitative researchers use questioning data to identify important themes in the study (Bansal et al., 2018). The researcher should be consistent with their understanding of the data provided by participants and how the data affects the research study based on the participant's perception of a phenomenon (Abdalla et al., 2018). The researcher understands the phenomena the same way each participant understood it (Abdalla et al., 2018). The participants' reflections, feelings, comments, and surroundings provide valuable data by adding context to the research study (Holmes, 2020).

For this investigation, a qualitative technique was the best option. The participants in the study responded to a phenomenon that occurred in their natural environment. It is

crucial to understand the perceptions of issues IT managers identify as factors for IT staff turnover, including IT professional burnout, and gain a deeper understanding of their usage of retention methods. I expected participants to contribute information from personal experiences and points of view by answering open-ended questions, which provided insight into how various techniques influenced IT employees and what made those strategies effective in their surroundings.

This study did not use the quantitative method. Researchers use measurable and statistical data to confirm or reject hypotheses (Hoyer et al., 2018). Although quantitative data allows for statistical analyses, it ignores parts of social life and contextual information (Popescul & Jitaru, 2017). Researchers use quantitative techniques to identify statistical relevance, whereas qualitative approaches are better suited to answer *what*, *how*, and *why* questions (McCusker & Gunaydin, 2015).

Research Design

This study relied on a qualitative exploratory multiple case study research design. Ethnographic, narrative, phenomenological, and case study are the four research designs for qualitative researchers. While choosing an appropriate design for the investigation, the researcher must consider the issue, the study's strategy, and the research questions. The chosen research design informs participant selection and how data is collected (Rutberg & Bouikidis, 2018).

An ethnographic design allows researchers to examine a culture-sharing community by immersing themselves in the daily lives of participants (Mannay & Morgan, 2015). The researcher becomes a member of the participant community (Kassan

et al., 2020), watching the participants' daily activities (Fusch & Ness, 2015). In contrast, a phenomenological design focuses on the participants' lived experiences, and much of the research reflects those experiences. Phenomenological researchers look into how people interpret a phenomenon.

Researchers can approach the topic of study in its natural setting using a case study design, which allows them to consider these elements in relation to natural events (Arseven, 2018). Using this method, the researcher can observe the subject in the environment where the event occurs. This research lacks the definite identifiable variables and elements of a quantitative study; thus, a qualitative design provides an appropriate conceptual framework for analysis (Collins & Stockton, 2018). I used probing questions to understand answers better and help me achieve data saturation. Data saturation occurs when the collected data is similar and provides no new or better understanding of the investigated phenomenon (Weller et al., 2018).

Population and Sampling

IT professionals with at least 5 years of experience working in DevSecOps who manage teams of at least three DevSecOps experts made up the population of this case study. Participants have integrated AI into their DevSecOps workflow as architects or users or plan to do so. One important aspect for qualitative researchers is how the study's samples should be chosen (Shaheen et al., 2019). A random sample would be ideal for analyzing the variation among programs to generalize the findings (Shaheen et al., 2019). However, the participants for this study were selected using purposeful sampling. When there is much data but insufficient resources, purposeful sampling can be the most

suitable approach in qualitative research (Palinkas et al., 2015). Therefore, a purposeful sampling approach is most appropriate for this study.

The more information a participant can provide for relevant research, the fewer participants a researcher may have to recruit for their study (Campbell et al., 2020). As a result, there is no clear requirement for a given sampling size in qualitative research (Shaheen et al., 2019). The sampling size depends on the research's goal, the quality of the participants, the scope of the investigation, and other limiting factors, such as available resources, access to participants, and time (Shaheen et al., 2019). Considering the professional experience requirements for the participants, I assumed that I would not need more than 10 individuals to reach data saturation. Data saturation occurs when the collected data is similar and provides no new or better understanding of the investigated (Fusch & Ness, 2015; Weller et al., 2018).

Ethical Research

Respect for persons, beneficence, and justice are the three main ethical principles and standards for protecting human research subjects outlined in the Belmont Report (Ryan et al., 2014). To address the study's ethical concerns, I requested participants' consent to use the collected data as part of my study. It is an ethical research practice to obtain informed consent and voluntary involvement (Maher et al., 2018). Furthermore, I asked participants to confirm their participation by replying to the informed consent email. The informed consent email also stated the study's objective, benefits, risks, and nature.

All participants were required to acknowledge the study's methodology and their desire to participate voluntarily by responding through email. Following this approach ensures that all participants enter the study voluntarily and are provided with sufficient information to make an educated decision on whether to participate (see Silva et al., 2018). However, I obtained Walden's Institutional Review Board (IRB) permission before collecting data or reaching out to potential participants. Following the IRB approval process ensured that I met all university standards for involving human participants and data collection and identity security procedures by following established practices. Furthermore, Walden University requires that researchers obtain an IRB approval confirmation number, which must then be shared with participants so they can anonymously validate the study's legitimacy.

I adhered to the Belmont Report's ethics and participant protection directions. The 1974 National Research Act created the National Commission for the Protection of Human Subjects in Biomedical and Behavioral Research (Centre of Medical Law and Ethics, 2003). This panel outlined fundamental ethical principles and ethical standards to be followed when researching human subjects to ensure ethical research. There was no incentive for this research, and if a participant chose to participate in the study, they could change their mind and withdraw at any point by sending an e-mail stating their intention to withdraw. They were not required to provide a reason. All personally identifiable information, such as name, business, and precise job title, was omitted from the study. I applied a numerical value to all participant-related references, encrypted all

gathered data, and will store them in a secure and protected cloud storage account for the next 5 years. After 5 years, I will securely delete all data.

Data Collection

The data collecting process is a set of processes that generates considerable data from numerous sources (Clark & Vealé, 2018). To ensure that the data acquired during the research was collected ethically and without prejudice, I detailed the instruments I use to collect the data, the strategies I use to collect the data, and finally, the techniques I use to organize the data properly. Data collection, like other parts of the research process, must be conducted with the protection of the participants in mind (Hesse et al., 2019).

Data Collection Instruments

As the sole data collection instrument, I primarily relied on semistructured interviews (see Appendix C). Through my interviews, I attempted to gather the experiences and perceptions of ten cybersecurity professionals regarding their level of knowledge on integrating AI into their agency's DevSecOps pipeline by asking open-ended questions. Participants responded freely to the open-ended interview questions by my allowing them to elaborate on their responses (Weller et al., 2018). Furthermore, I used probing questions to understand answers better and help me achieve data saturation. Data saturation occurs when the collected data is similar and provides no new or better understanding of the investigated phenomenon (Weller et al., 2018).

I used Skype to record the interviews, and additionally, NVivo to identify themes and codes during postprocessing. Post-processing includes converting the audio recordings to text for verification or analysis using additional software. For this, I used

NVivo software Version 12. By returning accurate transcripts to study participants, I ensured the study's accuracy and allowed participants to make changes should they feel that the meaning of their answers is misrepresented throughout the recordings through member checking. Allowing participants to validate their statements for accuracy ensures that the collected data represents what the participant wanted to convey.

A researcher can establish a study's credibility by various methods, including member checks, extended observations, and data triangulation (Korstjens & Moser, 2017). A researcher can influence the study's credibility through data collection (Korstjens & Moser, 2018). The researcher's data collection approach can suggest whether the researcher's interpretation of the data is consistent with the participant's perspective. Verification of members is a vital stage in establishing the legitimacy of a study (Korstjens & Moser, 2017).

Triangulation, in this study's context, referred to collecting data from multiple sources to obtain the most accurate version of the truth (Abdalla et al., 2018). Researchers can acquire a complete understanding of the phenomenon by conducting interviews, monitoring, and following up with members (Abdalla et al., 2018). Triangulation was used to saturate the data (Weller et al., 2018). After identifying and documenting themes and material, I continued to collect data until the themes and content recurred and I discovered no new information.

Each participant was scheduled for a follow-up interview to discuss how their interview transcripts were interpreted, assuring 100%-member participation aided in the discussion and accuracy of transcription processes. The participant could evaluate and

verify my interpretations as part of the member-checking process (Candela, 2019). Confirming evaluations is important for eliminating researcher bias in the transcript interpretation. Furthermore, this also ensured that any details lost during interpretation can be recaptured.

Data Collection Technique

Initially, I sent an invitation email to each participant following Walden IRB approval. The email included a brief background on the study's purpose and a request to confirm consent if they choose to participate (see Appendix B). By confirming their consent, participants acknowledge their understanding of the study topic and meet participation requirements. After gathering ten qualified, consenting participants, I scheduled a 30-minute interview session with each. I have allowed the participants to decline or revoke their consent for participation at any time during the study. I then shared an introductory interview guide with the participant and informed them before recording.

Due to my participants' geographical locations, interviews might have to be conducted via Skype to observe the participants' facial expressions and body language. While in-person interviews often remain the primary data collection method in qualitative studies, researchers found that collection methods such as Skype communications did not affect the quality of the interviews and that online participants were more open and expressive (Gray et al., 2020). The recorded interviews were transcribed into word documents. I informed the research participant that I will send them a copy of the transcribed interview for review and requested a follow-up interview if they want to add

to or correct previously transcribed information. Transcribing the audio enables me to re-examine the data, familiarizing myself with the information shared by the participant and how it relates to the study. Interviewers have flexibility when they use the qualitative research approach. The interview receives a higher response rate than sent questions, and persons who cannot read or write can also participate (Van de Wiel, 2017). The interviewer can assess the respondent's nonverbal conduct. Qualitative research is iterative, iterating between data collection and analysis while revising and improving the approach as necessary (Busetto et al., 2020; Zyphur & Pierides, 2017). After reviewing the transcript, I requested verification by the participant and their approval by email.

Data Organization Techniques

By utilizing data organization techniques, I can ensure data integrity, increase accessibility, and streamline the analysis process while improving my ability to interpret and comprehend the data. I created folders for each participant and label them with Roman numerals. Each subfolder of the number-labeled folder contained participant-related data, such as audio and transcribed interviews, member checking data, organizational documents, emails, and the consent form. The files and folders are securely stored on a cloud storage service that is also encrypted.

All paper documents collected during the data collection processes were converted to electronic data and uploaded to One Drive storage to align with the data requirements. After that, paper hard copies were shredded and destroyed to ensure participant data confidentiality. All electronic data will be retained in secure and

encrypted cloud storage and maintained under lock for 5 years. According to (Korstjens & Moser, 2017), it is critical to ensure the transparency and quality of data.

Data Analysis Techniques

To support the conclusions of this study, I used methodological triangulation. Methodological triangulation relies on various data sources such as interviews, organizational records, and previous and current research literature to compare and contrast findings and identify similarities (Flick, 2018). Methodological triangulation can be divided into two categories: 'across method' and 'inside method' (Bekhet & Zauszniewski, 2012). Quantitative and qualitative data collection techniques are combined in cross-method studies (Bekhet & Zauszniewski, 2012). Explanatory and textual data gathering is used across all methods, including passive observation, participant observation, open-ended interviews, and patient diary analysis (Bekhet & Zauszniewski, 2012).

Within-method studies employ two or more data-gathering techniques, either quantitative or qualitative, but not both (Bekhet & Zauszniewski, 2012). Quantitative data, for example, can be acquired using two methods: survey questionnaires and a pre-existing database, whereas qualitative data can be collected through participant observation and interviews (Bekhet & Zauszniewski, 2012).

Furthermore, I used the software NVivo. Researchers often use NVivo to assist with identifying themes and emerging patterns (Dalkin et al., 2021). A data management tool, such as NVivo, can augment the research process and help identify themes, organize the data, and establish data patterns (Maher et al., 2018). Establishing patterns assists in

finding emergent themes by converting codes to categories and identifying commonalities or patterns, requiring the researcher to become immersed in the data during analysis (Hoyer et al., 2018). Identifying patterns in research entails combining primary and secondary data.

Reliability and Validity

So far, I have outlined my role as a researcher and my participant selection process. I have reviewed how to conduct this research ethically through proper data collection. I further outline how I can ensure the reliability and validity of my research with appropriate considerations and techniques. Reliability and validity are two of the most critical domains to consider when evaluating any method for collecting data in sound research. As a researcher, I aimed to ensure the quality of the research I conducted through mutual trustworthiness and legitimacy of inquiry. This goal is achieved by ensuring the data obtained are accurate and valid.

The validity of a study is also influenced by how others judge it, both within and beyond the research community. If participants know the study's goal, they are more inclined to participate (Korstjens & Moser, 2017). Because validity and credibility are crucial in the research community, a researcher's attitude toward both could affect his or her reputation (Korstjens & Moser, 2017). Finally, society places a high value on well-rounded, well-founded research. They are more likely to believe the researcher's statements or support them because of their confidence in the findings (Korstjens & Moser, 2017). When designing a qualitative study, the researcher should look at factors

such as credibility, dependability, confirmability, and transferability (Korstjens & Moser, 2017).

Credibility

By being honest about the research, I maintained respect for all volunteers throughout the study. I also provided data for the study consistent with the participants' viewpoints. Respecting these obligations by addressing credibility results in a research method that is ethical and dependable (Korstjens & Moser, 2017). Based on the meaning and goal of the response, I double-checked that I understood a participant's response. As a result, I conveyed the participant's reality and provide the study with credible data.

Some methods a researcher can use to establish the credibility of a study include member checking, prolonged observations, and data triangulation (Korstjens & Moser, 2017). A researcher can impact the study's trustworthiness by how the data is gathered (Korstjens & Moser, 2017). The researcher's approach to data collection can determine whether the researcher's depiction of the data corresponds to the participant's opinions. Member checking is one of the most important elements in establishing credibility in the context of a study (Korstjens & Moser, 2017).

Triangulation is the process of achieving the best version of the truth by merging several data-gathering methods in the context of this investigation (Abdalla et al., 2018). Researchers can better understand the phenomenon through interviews, observations, and member checking (Abdalla et al., 2018). I used triangulation to achieve data saturation. After finding and documenting themes and material, I continued to collect data until the themes and content recurred and no new information arises. Furthermore, I reviewed

pertinent archival documents and conducted semistructured interviews to increase the credibility of the qualitative exploratory multiple case study. Lastly, I conducted all interviews according to the interview protocol, implemented member checking, and verified raw data, field notes, and data products.

Dependability

Dependability determines the repeatability and consistency of research (Forero et al., 2018). In qualitative research, a study is reliable if it can be duplicated with the same or similar procedures and processes to get the same results (Forero et al., 2018). Some processes and procedures employed to improve the study's dependability include member verification, transcript review, and pilot testing. The researcher must leave an audit trail that contains complete, detailed notes of the research's thought process and decision-making (Korstjens & Moser, 2017). This method of explaining the research provides enough information for another researcher to duplicate the previous study's findings so that when repeated, they would come to similar conclusions (Forero et al., 2018). Dependability increases the study's reliability and validity (Forero et al., 2018).

I conducted member checks to strengthen the study's trustworthiness. I also supplied a full audit trail that outlines the methodology and processes used in the investigation that led to my results. Member checking can improve research reliability and dependability by allowing participants to examine and validate the researcher's data collection accuracy (Stahl & King, 2020). It also allows the researcher to ask follow-up questions to ensure comprehension and prevent or correct any misunderstandings or misconstrued claims. I employed member checking to ensure that my understanding and

interpretation of the data correspond to the participants. I returned accurate transcripts to study participants, this ensured the study's accuracy and allowed participants to make changes should they feel that the meaning of their answers is misrepresented throughout the recordings.

When a researcher provides precise instructions on techniques, methodologies, and participant interactions, another can undertake a study with similar results by following in their footsteps (Korstjens & Moser, 2017). I present the research in detail, with notes, comments, and personal thoughts. Each decision taken during the research process has a rationale. This encompasses population and sampling, data gathering, organization, and data analysis procedures. Because of the study's transparency, another researcher can track its progress and determine how the method ended up with the results published (Forero et al., 2018; Korstjens & Moser, 2017). I kept notes of the steps I followed to finish the study, and the results align with the data I have collected. I also tracked how I obtained my population sampling, the interview question creation, the interview conduct, and the data organization and analysis.

Transferability

The transferability of research relates to how well it may be generalized or used in fields other than those for which it was designed (Forero et al., 2018). It is transferable if research can be applied in several situations or environments (Forero et al., 2018). It is unlikely for a researcher to predict if a study will be applicable in other settings (Forero et al., 2018). However, by providing detailed explanations of the research approach and methodologies, the researcher can help other researchers assess whether the study would

work in their context, improving transferability (Korstjens & Moser, 2017). Transferability improves the validity and reliability of a study and broadens the influence of an important study by allowing it to be applied to different locations and contexts (Forero et al., 2018; Korstjens & Moser, 2017).

I provide detailed descriptions of the processes, methods, and actions used for this research in the context of this study. To provide insight into my thought process and decision-making, I explain the data collection method and research strategy in detail. In addition, I go over the study's history, demographic and sampling, and data analysis phases in detail. Finally, I go over the study's findings in depth. The detailed information I supplied brings transparency and accessibility to the study. I share extensive details about the study's specifics, allowing other researchers to replicate it. Reproduction is possible if the researchers determine that the research applies to their field of study (Forero et al., 2018; Korstjens & Moser, 2017).

Confirmability

The concept of confirmability refers to the possibility of the findings being confirmed, corroborated, or backed by others in the scientific community (Forero et al., 2018). A study with confirmability is one in which the findings are generated directly from the data by a researcher. The data informs the researcher's interpretations, viewpoints, and conclusions. Before the findings can be confirmed, the researcher must establish dependability, credibility, and transferability (Forero et al., 2018). Meticulously keeping track of all artifacts and records while also taking extensive notes boosts the research's credibility (Forero et al., 2018)

I explain the reasoning behind each option I have taken for the study's purposes. This was accomplished by recording and delivering extensive detail through descriptions, notes, opinions, options, and decisions. To every investigation component, I impart the understanding that led to the choices and decisions made on the research approach. Methodological triangulation is another way to achieve confirmability (Abdalla et al., 2018). Because the study's findings are based on the data collected, I can ensure the data is accurate and complete.

Confirmability considers triangulation, member checking, repeatability, alignment, and generalizability. Confirmability necessitates each component of dependability, credibility, and transferability. To establish the study's credibility and integrity, the researcher must address the validity and reliability of the research. The research is credible, dependable, and trustworthy if other researchers could follow and repeat the study with similar conclusions (Forero et al., 2018). Therefore, other researchers can benefit from a valid and trustworthy study (Forero et al., 2018).

Transition and Summary

I summarized the research objective and problem, explained the methodology and design chosen for the study, and included data collection instruments and participant and sample procedures in Section 2. Additionally, I discussed the analysis strategy, tools, and techniques I relied on for conducting an ethical, reliable, and valid research study. I elaborated on why a case study approach is most beneficial for my qualitative research since it elucidates the *how and why* of phenomena by interpreting open-ended, narrative results. I have employed semistructured interviewing using open-ended questions,

allowing participants to comment and elaborate on effective SME cybersecurity practices in DevSecOps environments.

I also explained how the NVivo qualitative software aided the classification and analysis of nonnumerical study data. Furthermore, this part emphasized the value of data triangulation in generating themes and patterns while ensuring data saturation. I conclude Section 2 with a review of the validity and reliability of a qualitative research study, emphasizing honesty, transparency, and repetition throughout the study process. Section 3 covers the research findings and its impact on social change.

Section 3: Application to Professional Practice and Implications for Change

Application to Professional Practice and Implications of Change

The purpose of this qualitative multiple case study was to help organizations and government corporations understand why incorporating AI into a company's or institution's cyber-security, development of software systems, and operational systems is significant. In this section, I present the findings from in-depth interviews with professionals in cyber-security, software development, and operational fields in IT or cyber-security. Furthermore, I will elaborate on the progress government and private institutions are making in implementing AI into their DevSecOps pipeline, the nature of AI in DevSecOps, and the current organizational concerns about the existence of AI in software development, cyber-security, and operations.

I will also discuss the professional practice of AI in various fields, its implications for social change, recommendations for action, point out areas of interest for further research, and offer study conclusions. Furthermore, this section illustrates some benefits of AI incorporation into the DevSecOps pipeline, obstacles encountered during the study, possible solutions, and ways to improve AI implementation. While not all findings may represent all industries, they offer insights into how some organizations implement AI into the DevSecOps process. Thus, these findings may serve as a general guideline for similar and other industries.

Presentation of Findings

I used the following research question to inform my understanding and guide my interviews: What are some strategies cybersecurity professionals use to incorporate AI

technologies in developing secure software for IT operations? The answer to the central research question can be used to address the specific IT problem that some cybersecurity professionals resist using innovative technologies in the software development process. Despite the different approaches from the 10 participants, most ended up saying that the incorporation of AI into their DevSecOps is new and requires a slow approach because quick implementation is risky financially and sometimes leads to complications as a result of a lack of knowledge and experience among individuals. DevSecOps frameworks emerge around industry best practices and are often integrated as part of an organization's cybersecurity and continuous integration and development efforts (Rangnau et al., 2020; Woody et al., 2020). According to P4, their organization has different processes for different fields, stressing the complex nature of incorporating AI into the DevSecOps pipeline, encouraging staff to learn respective processes, the cost involved in incorporating AI, as well as managing, securing, and budgeting the operational costs of AI in their DevSecOps pipeline, all of which require time and resources. P5 further stated, “For me, I have only seen two strategies of implementing AI into DevSecOps pipeline,” the first being “a slow and steady win approach,” and the second less cautions by “jumping in with full AI.” However, P 5 clarified that he believes organizations prefer the first approach, stating that “my experience is most organizations choose one because it is safer.” Rapid changes across the entire software development life cycle require refined and automated testing and quality assurance approaches, where traditional manual testing procedures fall short. The automated approach to CI and CD is especially useful in DevSecOps. It can reduce the security professional's constant review and testing

burden and reduce vulnerabilities and quality issues to those that fail to be detected automatically (Kumar & Goyal, 2020; Rangnau et al., 2020). These findings suggest two approaches to incorporating AI into the DevSecOps pipeline, with organizations preferring the slow and steady approach to incorporating AI into the DevSecOps pipelines. This then gives way to the UAT. UAT aims to validate whether a given software meets its design and functionality goals (Lobkov, 2019). Generally, UAT is a manual process where security professionals, engineers, and customers validate whether the software is meeting requirements (Sanders et al., 2021). IT managers can use each theme to form a foundation for implementing AI into the DevSecOps pipeline and enabling me to refine potential areas of interest for future research.

Theme 1: Focus on Implementation

A crucial theme of this study was the examining the implementation of AI into the DevSecOps pipeline, a process that many private and government organizations are starting to implement, have implemented, or are buying a product from vendors that offer an off-the-shelf AI implementation into the DevSecOps pipeline. Under the focus on implementation of AI into the DevSecOps pipeline, I identified three subthemes: (a) implementation obstacles, (b) AI cloud implementation strategy, and (c) AI local implementation strategy.

Most participants and documents mentioned implementation obstacles, AI cloud implementation strategies, or AI local implementation strategies. Nine out of 10 participants mentioned various obstacles when implementing AI, five out of 10 mentioned an AI cloud implementation strategy, and six out of 10 suggested using an AI

local implementation strategy (see Table 2). Furthermore, several artifacts also suggest the existence of implementation obstacles and various AI implementation strategies through a cloud or local deployment (Dawson, 2020; Kumar & Goyal, 2020). Most AI implementation strategies of organizations are similar, especially for entities still in the implementation process. Furthermore, the participants agreed that knowledge of AI is crucial, and organizations should integrate AI into their systems while educating staff on AI's advantages and challenges. For example, P8 mentioned that a "lack of Knowledge and skills will contribute to mistakes and not catching [indicators of compromise] IOCs that you should be catching."

Table 2

Subthemes of Focus on Implementation

Subtheme	Number of references	Participants referred to theme
Implementation obstacles	37	9
AI cloud implementation strategy	13	6
AI local implementation strategy	8	5

The knowledge gap about AI use and implementation strategy may adversely affect an organization's ability to prevent and detect security issues throughout software development cycles. P8 added that "these knowledge gaps are increasingly exposing enterprises to security attacks in endpoint areas and patch management." In line with this understanding of the urgency and lack of knowledge, Umurerwa and Lesjak (2021) suggested that although there is no universal approach to implementing AI throughout an

organization or business, it is even riskier to operate without AI. At the same time, Fountaine et al. (2019) call on organizations to embrace and use AI because this new technology is taking over many business sectors. Using AI is crucial for organizations as it can boost productivity and efficiency while reducing human errors and automating repetitive tasks (NiBusiness.Info, 2022).

Furthermore, The PwC (2022) business report suggested that AI-enabled companies increasingly realize competitive advantages. However, the choice of AI implementation strategy seems to matter more than choosing to implement only some AI. Although the number of organizations with some level of AI use is growing steadily, companies with a holistic strategy benefit more than those who only selectively deploy AI (PwC, 2022). While the holistic approach offers many benefits, Al-Walai and Liang (2021) suggested its biggest disadvantage is cost. The added cost may explain why some organizations are reluctant to invest in a holistic AI strategy, which includes local or cloud deployments, creating infrastructure and systems, and educating employees.

As the basis for the conceptual framework for this study, TAM's focus on attitudes toward using a particular IT based on perceived usefulness and ease of use from a user's perspective (see Granić & Marangunić, 2019). This aligns with the theme found in this study. The study found that the attitudes of the IT professional towards the integration of AI into their DevSecOps pipeline played a significant role in the end results. Nine of the participants mentioned obstacles which affected their ease of implementation Even though all 10 participants identify the usefulness and importance of

AI in improving their security posture within their DevSecOps pipeline (Rangnau et al., 2020).

Subtheme 1: Implementation Obstacles

Under this subtheme, I inspected the obstacles hindering most organizations from implementing AI technologies and solutions into the DevSecOps pipeline inside a cloud computing environment. The lack of cybersecurity engineers and software developers with expertise in AI poses significant challenges. For instance, most participants called for proper training of senior managers, new hires, aspiring developers, cyber-security experts, and AI specialists. P1 suggested that cybersecurity, software development, and AI falls behind because of senior management's lack of knowledge of AI technology. P1 added, "if you just do the legacy way of doing it, then yeah you're already behind the power curve." P1 further stated, "you need to find those people that are willing to accept the leading-edge front of making change and accepting that that's the better way to go." The lack of understanding of AI's benefits may result from the lack of proper training and education in the respected fields, and it seems crucial for developing expertise. In line with what some participants noted, Morrell (2018) suggested that the reluctance to implement AI often stems from a lack of trust, a perceived risk of bias, and other AI errors, creating the belief that AI may be too risky to be useful. P9 noted, "AI is a tool, and like every other tool, they have to learn it." P9 suggested that other industries and data science, in particular, extensively rely on AI and have developed knowledge on how to use it best. P9 added that the "same data science background needs to get folded more into the cybersecurity space than it currently is."

Another obstacle is the lack of sufficient budgets in most organizations which results in partial use of AI for DevSecOps and cloud computing and sometimes increased cost for outsourcing these operations and technologies. Thus, most participants suggested that their organizations were in the process of creating a cloud computing solution, deploying a system locally, or already owning hard and software they use with existing AI-enabled products. For example, P4 suggested that an AI implementation is already underway, and automation may offer the biggest benefits to their organization. In contrast, P7 noted that the "lack of knowledge about the utility and effectiveness of AI is perhaps the biggest threat to its application," but that implementation "will depend on funding." P7 added that a major obstacle for AI implementation "is a lack of understanding that for AI to be effective, it needs a body of good training data to work off of, as well as have that data be updated and maintained to evolve as threats evolve." P7 noted that having adequate funding seems a major obstacle, as it directly affects the strategies an organization can use to deploy AI and its ability to hire specialists to maintain and use AI effectively.

Another obstacle in implementing AI into an organization's cloud computing environment in the cloud or private infrastructure is time, making the process expensive. According to Antunes (2021), implementing AI through a cloud computing environment and integrating it with a DevSecOps pipeline involves several processes, including the manual preparation of data and removing bias within the system, for example. While a local implementation may take even longer and face similar challenges, both approaches require trained professionals, which may be difficult to find or retain. P9 noted, "you got

to get to a point of where people understand it well enough to want to implement it, understand the benefits of it, and the risks, in a way that they can implement it effectively."

Finding people who understand AI and can implement it effectively seems to be a major obstacle when integrating AI into the DevSecOps pipeline. While it is arguably difficult to reduce the cost significantly when looking for an AI solution, outsourcing can offer advantages, such as working with a knowledgeable team, reducing the time to implement AI at an organization, and mitigating the risk of having to find qualified engineers to build out a system from scratch. P8 suggested that buying an off-the-shelf solution would be ideal for their organization to reduce the risk of project failure and control costs because "I think it saves the company of having to train all these people to be AI experts." In this context, physical or rented hardware costs seem to pale compared to the expenses of training employees on how to use AI or finding qualified engineers to develop and integrate AI into an existing DevSecOps pipeline.

This subtheme also outlined the participants attitude towards the integration of AI which is one of the focuses of TAM. P1 suggested that cybersecurity, software development, and AI falls behind because of senior management's lack of knowledge of AI technology. P1 added, "if you just do the legacy way of doing it, then yeah you're already behind the power curve." P1 further stated, "you need to find those people that are willing to accept the leading-edge front of making change and accepting that that's the better way to go." It appears the participants attitude toward the implementation if

new technology is that of lack of trust in the abilities of senior management. (Morrell. 2018).

Subtheme 2: AI Cloud Implementation Strategy

Notably, there were different views among the ten participants concerning this sub-theme. Several participants stated that their organizations did not own a cloud environment but rented cloud services, such as Amazon Web Service (AWS), to build out their DevSecOps environment. For instance, P1 noted that "AI is still an ongoing thing in my organization" but added, "we are migrating on to Amazon Cloud services and building our DevSecOps pipeline environment from there." However, P3 explained a different approach where the cloud functions as a Software as a Service (SaaS), so it can more easily integrate with various environments locally or in the cloud. P3 added that the software "sends the data back up to the central software as a service platform, and then that platform does the running and the understanding of what is normal and abnormal behavior, and then sends it alerts on things we might wanna care about."

Furthermore, how an organization intends to pursue its AI-implementation approach may significantly impact cost and outcomes. For example, P5 suggested that there are generally two approaches, one throwing "caution to the wind" and another with a focus on "slow and steady" instead. Although P5 suggested that picking one over the other may result from the organization's risk appetite, choosing the slow and steady approach has taken "years to get to that point." However, choosing one over the other may not always be an option because of the tradeoffs between time to deploy and cost. P7

noted that the direction they can choose to implement AI into their DevSecOps pipeline "will depend on funding."

Generally, participants noted that their knowledge of cloud strategies includes using a third-party vendor, SaaS, or services, such as AWS, to deploy an online solution and integrate it with local or cloud-based applications within the DevSecOps pipeline. However, participants seemed to have limited experience using cloud-based AI within their DevSecOps pipeline. While two participants noted that they are already using cloud-based AI tools to augment their DevSecOps pipeline, others noted that they work on local solutions or use a third party to provide AI features. Furthermore, participants mentioned cost and skills as the biggest challenges associated with AI implementation regardless of cloud or local approaches. P6 noted that "there's not a lot of skill out there around AI, and where it is, it's enormously expensive."

Subtheme 3: AI local Implementation Strategy

The participants in this study agreed that a local implementation strategy adds additional cost and risk compared to a cloud or third-party approach, which is why most of them prefer a cloud-based approach. However, P2 noted that picking the wrong vendor can also introduce significant risk, "as we saw with solar winds and things like that. "As previously mentioned, many participants believe that local implementation strategies may offer some advantages but also introduce additional uncertainties. For example, P6 noted that "it is taking is far longer" than they had hoped and that "it is slow going. "

While some participants may have investigated and started with a local implementation approach, many seem to realize that a sustainable AI implementation

solution requires scalability and dynamic capabilities only a cloud-based solution may offer. It is, therefore, understandable that some participants prefer a hybrid approach where a local implementation supplements a cloud-based solution. For example, P10 noted that some of their requirements expect "more integrating with elastic and where we can kind of do some more," suggesting that "responding to a cyber event in traditional firms with the traditional analyst process is probably not going to cut it anymore in the future." Most participants seem to have realized that a cloud-based approach offers several advantages over a local implementation strategy.

Theme 2: Focus on AI in DevSecOps.

The use of AI in DevSecOps is arguably in its infancy without a clear set of requirements, proven technologies, or established strategies for successful implementation. Most participants struggled with giving specific strategy or implementation examples, including detailed functionality or feature sets unique to AI and designed to better the DevSecOps process and pipeline. These struggles may result from the novelty of AI use in DevSecOps or general misconceptions about the technology's potential benefits. P6 noted that "what they haven't necessarily always been able to do is put in place use cases that align to practical business use," further suggesting that there may be a disconnect between practical applications of AI in DevSecOps, or a lack of knowledge about what new functionalities this technology could enable.

Under the focus on AI in DevSecOps, several subthemes emerged, including (a) AI versus traditional DevSecOps, (b) reduced reaction time, (c) AI use cases, (d) use of AI justification, and (e) AI education. Table 3 illustrates that almost all participants had

thoughts on AI-enhanced versus traditional DevSecOps, discussed some AI use cases, and mentioned AI education as one of the biggest challenges organizations face when they try to adapt AI-use and integrate it with existing DevSecOps pipelines and practices. Only six out of 10 participants discussed some justifications for AI use which illustrates that only a very small majority of cyber security professionals may believe that AI has a place DevSecOps. Half of all participants were similarly skeptical about whether the reduced reaction time an AI-supported DevSecOps pipeline may offer is enough to pursue AI integration in their organization more actively.

Table 3

Subthemes of Focus on AI in DevSecOps

Subtheme	Number of references	Participants referred to theme
AI versus traditional DevSecOps	25	9
Reduced reaction time	8	5
AI use cases	34	9
Use of AI justification	14	6
AI education	22	9

Subtheme 1: AI versus Traditional DevSecOps

Most participants agreed that introducing AI into the DevSecOps pipeline offers benefits, identifying threats before they become a major breach or spotting malicious activities that would otherwise not trigger more traditional security systems. P6 explained that traditional DevSecOps involves analyzing logs and setting up triggers and filters, all

of which involve humans verifying and acting upon any detected threats. P6 added that "when you think about managing events, and potentially remediation so much is reliant on getting through false positives and doing that with some of sorting and filtering, what we need more is not only the inspection but in an immediate response that is not relying on that human intervention." Other participants agree that the biggest differentiator between AI and traditional DevSecOps is the need, or lack thereof, for human intervention and decision-making.

P10 noted, "one of the big issues we have is being able to handle a cyber security attack in the speed that they come." P10 also suggested that they are "looking at finding ways to be able to find evidence indicators of an attack, and then correlate all that evidence together automatically in an automated way, using things like AI to come up with the best possible solution." While participants agreed that AI could improve an organization's ability to detect and respond to an attack more efficiently, some also suggested that a lack of competencies limits its integration and may result in delays or overly cautious approaches. Most participants were also aware of at least some potential benefits of deploying AI within their DevSecOps pipeline, with reducing reaction time mentioned most often.

Sub-theme 2: Reduced Reaction Time

Participants described reduced reaction time in two contexts: (1) the time it takes to act after identifying a threat and (2) the time it takes to identify new threats. P9 noted, "you could use AI to make better, faster, quicker decisions on huge data sets that are out there and then go apply solutions." While P9 assumes that AI-based decision-making is

faster than humans can accomplish, this advantage becomes more important because of the “constantly evolving nature of threats, and it's always changing, that becomes more and more critical all the time.” P8 shared a similar understanding of the benefits of AI and its effect on reaction time and noted, “AI solutions deliver rapid insights that cut through the clutter of daily alerts and significantly shorten response times.”

Including AI technologies and solutions in a computing system reduces the time it takes to react to cyber-attacks and threats (Biswas, 2020). Similarly, participants suggested that they also expect AI to reduce reaction time by reducing the need for human intervention. However, participants could not agree on whether the reduced reaction time should only apply to processes related to identifying threats rather than identification and automatic action. P10 an AI should be “able to maybe triage something, put it in a safe place,” adding that there “it can't get any worse until a human being can make a, maybe a judgment call onto, you know, what's happened and how it should be dealt with further.” In contrast, P9 would go further and suggests that “if you've got a smart enough system, or if you've got an information-dense enough system, they can even make choices and changes if you've allowed it to do so.”

Sub-theme 3: AI Use Cases

This sub-theme focuses on participant replies about where they used AI, the results of using AI, and their overall thoughts on the need to implement more AI in crucial areas. For example, P5 suggested that their organization currently uses AI in the DevSecOps pipeline to reduce security incidents. However, P5 also suggested that while there is a path for using more AI across their systems, a lack of competencies and

resources limits the current use cases. In contrast, P9 sees automated vulnerability testing as an ideal use case for AI, although their organization currently relies on automation only.

In general, most participants see use cases where AI automates the detection process and, in some cases, isolates and takes further action. P10 noted. “we're really looking at finding ways to be able to find evidence indicators of an attack, and then correlate all that evidence together automatically in an automated way, using things like AI to come up with the best possible solution.” P10 added that “one of the biggest problems is it's trying to get human beings to be able to keep up with the things that you have to keep up with on a network.” In contrast, P6 sees another use case where AI can go “well beyond the typical inspection of correlation,” leading to “more of a proactive of evaluation versus waiting for response to, to[sic] play.”

Sub-theme 4: Use of AI Justifications

Participants have shown two distinct approaches to using AI in DevSecOps, with one group leaning more heavily toward justification for why they are falling behind and another suggesting only limited utility for DevSecOps. For example, P1 suggested that The problem is there's not as many experts in that field and also having to have the deep understanding of how it works, because a lot of that goes back into data science and people aren't as experts in data science as they are in other forms of, or components of cybersecurity.

While P1 acknowledged the perceived difficulties of finding the right talent to implement AI, they are also aware that “if you just do the legacy way of doing it, then

yeah you're already behind the power curve." P7 also remains skeptical about AI's ability to offer anything they cannot already do without it, potentially suggesting that what participants might think AI can do might negatively affect their approach to having AI and the justifications they make in turn. P7 clarified that "we would have to have a clear need for something above and beyond what we currently have, and that doesn't exist at this time."

In contrast, P5 suggested that many solutions may not offer the benefits their creators claim, and many analysts may not trust an AI-based system. Several other participants displayed a similar distrust toward AI capabilities, using it as part of their justification for why they are falling behind on AI use or are otherwise not fully supporting a transition. For example, P5 noted the "Lack of maturity in many AI capabilities – there is a lot of "snake oil" salespeople trying to sell unproven and immature AI technology for everything." P2 echoed similar distrust among their colleagues who "weren't ready for that idea of like, oh, this happens every day," suggesting that the use of AI was limited to once-a-month applications when, in fact, daily use would provide the biggest benefit.

Sub-theme 5: AI Education

Participants agreed that AI education presents multiple challenges when trying to implement AI. For example, a lack of AI knowledge may cause some employees to resist change and embrace the new technology, while similarly, a lack of knowledge may also suggest difficulties in finding appropriate talent and experts. P6 noted that "part of the challenge there is there's not a lot of skill out there around AI and where it is it's

enormously expensive." Although P6 acknowledged that adequate talent for implementing or developing AI solutions is difficult to find, they noted that those experts exist but are expensive. P1, on the other hand, blamed the lack of progress on their AI implementation on the lack of skilled workers and overall limited education on the topic, adding that "finding those experts that have those specific types of skills to be able to actually do that type of coding or skills, to do that type of development" is challenging.

Some participants aim to sidestep the education and qualified employee problem by outsourcing AI. P2 noted that while they have some AI knowledge, they went with a vendor instead who is "building a series of tools that allows you to deploy a node inside your environment that you can run at whatever frequency you choose that uses knowledge about your system and AI to then go after it and, and try and find vulnerabilities that you may not realize are there, or, you know, even down to like simple stuff." However, going with a vendor does not necessarily mean that the organization is aware of the product they buy into because, often, a lack of basic understanding of how AI works limits the ability of these vendors to provide products that could make client systems more secure. For example, P3 uses and sells its AI tools aimed at improving the security of the DevSecOps pipeline, and often "people don't understand how ML and AI helps the problem," so the vendor ends "up with a lot of confusion as to what we need to really look at." Participants seem to agree that the lack of education affects their ability to maximize the benefits of AI in DevSecOps while also making it difficult to find talent who could take over, introduce necessary knowledge, or develop new systems.

Theme 3: Focus on Organizational Concerns

Several participants mentioned organizational concerns, often referring to outsourcing instead of finding talent, solutions and solution-providers, and budgeting. While all participants mentioned the high cost of AI when looking at hardware, software, or qualified engineers, these concerns often aligned with a discussion about the willingness of senior employees to embrace this technology. Participants whose organizations embraced AI and started the transition were generally less concerned about organizational limitations than those who have yet to decide on a strategy or allocate funds. However, several notable sub-themes emerged throughout the interviews when looking at organizational concerns, including budgeting AI, outsourcing AI, and using AWS (See Table 4).

The theme of organizational concerns again aligns with the focus of TAM conceptual framework. the attitudes of all the participants towards the acceptance of new technologies were dependent on factors like cost of AI, hardware and software, qualifications of engineers and acceptance by senior leaderships. the participants who had begun the integration of AI into their organization had less concerns about organizational limitations verses those who were yet to begin the integration process. There was no correlation between the ease of use of the technology and how it was obtained. The few participants who discussed off the shelf and home-built technologies did not seem to see one to have an advantage over the other in perceived usefulness and ease of use.

Table 4

Subthemes of Focus on Organization Concerns

Sub Theme	Number of references	Participants referred to theme
Budgeting AI	1	1
Outsourcing AI	5	4
Use of AWS	3	2

As illustrated above, four participants discussed organizational concerns related to outsourcing AI, and two participants specifically mentioned AWS in this context. While only one participant mentioned budgeting AI as an organizational concern, other participants also noted cost as a prohibiting factor for implementing AI faster. Furthermore, several participants mentioned other concerns related to organizational dynamics. However, I did not include those concerns here because they seemed limited to their particular organization and failed to echo concerns shared by other participants.

Sub-theme 1: Budgeting AI

All participants agreed that cost is a major factor when determining which AI strategy, they decide to follow. However, P5 specifically noted that "adoption varies widely, and that is usually linked to lack of budget." P5 also expressed a structured view of the processes and people involved when integrating AI into the DevSecOps pipeline. Unlike other participants who often made anecdotal references, P5 had very distinct and detailed knowledge of the requirements for an AI integration, suggesting that they may have been or currently are involved in managed projects to achieve the same.

Coincidentally, while none of the other participants went into as much detail on the various cost factors involved in deploying AI within the DevSecOps pipeline, all of them shared similar concerns regarding cost and organizational limitations dictating the speed at which they can implement and innovate.

Sub-theme 2: Outsourcing AI

When participants described outsourcing AI in the context of DevSecOps, they most often mentioned three major organizational concerns, including moving infrastructure to the cloud, using a third-party vendor to provide AI as a software service, or using off-the-shelf solutions instead of developing their own. Most participants suggested that their organization lacks the culture, knowledge, and resources to implement an AI solution without third-party help or the cloud. For example, P8 noted that "if I had to say how we are doing it [AI], I would say we are going to buy the service from a company and have them manage it," and then added that "I think it saves the company of having to train all these people to be AI experts." P9 similarly noted that "we plan to take advantage of the cloud-native solutions" and added, "we are in the process of moving services to the cloud."

Some participants also discussed hybrid solutions where an AI system resides in the cloud as a service, and an API enables the organization to send data and receive assessments in return. P3 noted, "what the software does is it sends the data back up to the central software as a service platform, and then that platform does the running and the understanding of what is normal and abnormal behavior, and then sends it alerts on things we might want to care about." Other participants noted that organizational dynamics,

such as senior leadership concerns or data sensitivity, would not allow them to take a similar approach. However, P1 noted that while deploying an AI solution in the cloud allows them to control their data without the need to share with a third-party vendor, like a local deployment, "finding those experts that have those specific types of skills to be able to actually do that type of coding or skills, to do that type of development" continues to be a challenge.

Sub-theme 3: Use of AWS

Most notably, participants who mentioned their organization has started to transition to the cloud for implementing AI into the DevSecOps pipeline also favored using Amazon Web Services (AWS). P1 noted that their organization realized that apart from offering compute resources in the cloud, they "will be able to take advantage of Amazon's services to automate." P9 favored a similar approach and "just look at what AWS has," adding that they did pan on "reinventing the wheel." While P9 plans to "build the environment in AWS" and "automate it using amazon services," the biggest organizational challenge seems to be "a lot of red tapes[sic] that we have to deal with."

Application to Professional Practice

The specific IT problem serving as the basis of this study was that some cybersecurity professionals lack strategies to incorporate AI technologies in developing secure software for IT operations (DevSecOps). The focus of this study was to identify strategies participants use when integrating AI into the DevSecOps pipeline. While some participants provided details on their implementation strategies, many have yet to begin

integrating AI or decide which strategy they may use to refine their DevSecOps pipeline through AI technologies. Three distinct strategies emerged throughout the interviews.

The first strategy was to rely on a cloud-based approach where participants would either rent infrastructure in the cloud and develop their own AI solutions or rely on a third party and their software as a service. The second strategy involved building an AI solution locally instead of in the cloud. Similarly, some participants noted that an original approach or relying on a third party are both options for implementing AI in the DevSecOps pipeline. Lastly, some participants had no strategy. While this group had some ideas about how AI could help them create secure products, participants with no apparent strategy had little or no in-depth knowledge, in-house expertise across teams, funding, and overall seemed to lack a project plan.

Even though some participants used cloud-based and third-party solutions, no clear strategy emerged. While establishing causality was not the goal of this study, the interviews aligned with the extant literature, suggesting that many cybersecurity professionals may lack strategies for implementing AI into the DevSecOps pipeline. Those participants with some experience implementing AI into their security approach primarily suggested that the biggest benefit they saw and expected to see was a reduction in reaction time. While automating threat and anomaly detection may be a task well-suited for AI, it is likely only one of many areas where AI could change how cybersecurity professionals operate.

Other industries show how the creative use of AI can unlock new technologies, refine products, or make existing workflows dramatically more competitive. There is an

increased risk for DevSecOps professionals who refuse to embrace AI because criminals are much more eager to use this technology to find vulnerabilities and execute complex and more difficult-to-detect attacks (Sullivan, 2018). Some participants suggested that more traditionally educated decision-makers at their organizations are at fault for the slow, or lack of, AI adoption in DevSecOps. Therefore, it is no surprise that all participants saw a lack of education and available talent as one of the main factors limiting their ability to successfully promote and implement an AI strategy within the DevSecOps pipeline at their organizations.

While some participants blamed the lack of AI implementation strategies on cost, lack of education, and resistance to change within their organizational leadership, many answers regarding AI opportunities and benefits suggest that their knowledge about AI and its potential was also limited. The knowledge gaps most participants perceived extends beyond those working on AI implementation to include decision-makers and cybersecurity professionals on all levels. As the participants' limited understanding of the benefits of AI in DevSecOps illustrated, some professionals may have a slightly better understanding of AI capabilities but still fail to grasp and realize its full potential. Limiting AI use cases to mere intrusion, or threat detection may only offer short-lived benefits as it serves as an extension of rule-based filters and detection and is not an entirely new approach to identifying, blocking, and mitigating threats autonomously.

Implications for Social Change

Supported by the extant literature, one of my assumptions at the onset of this study was that AI adoption in DevSecOps is slow and generally falls behind other

industries. As criminals continue to embrace AI for their exploits, the benefit of promoting a similar approach in DevSecOps would at least negate any advantage hackers may have and, in the best-case scenario, offer an upper hand in this increasingly difficult fight. My understanding of the benefits has not changed after conducting the study, and participants seem to agree that the impact of autonomous vehicles on society, in general, will be transformative. The participants in this study seem to agree that reaction time is essential when protecting systems but also acknowledge that many of them currently lack an AI implementation strategy.

Most participants also agreed that preventing damage and intrusions will become increasingly difficult because criminals use AI to attack systems. However, participants also suggested that the lack of experts and knowledge in their organizations and the high cost of deploying AI solutions within the DevSecOps pipeline continue to delay adoption and potentially put them at a disadvantage. With society expected to shoulder most of the substantial damages caused by cybercriminals (Furnell et al., 2020; Korzeniowski & Goczyla, 2019), delaying the adoption of AI across the DevSecOps pipeline and within critical systems seems almost negligent. Without society demanding a shift of liability and better protection against cyber criminals, participants suggested that internal forces, such as corporate culture and lack of funding, will dictate the level of AI adoption and, thus, the organization's ability to defend itself.

If the number of increasingly damaging data breaches indicates (Bhatele et al., 2019; Furnell et al., 2020), DevSecOps can dramatically benefit from AI if it enables early detection and breach prevention other systems or human professionals are unable to

achieve. Cybercriminals are often after valuable user data, such as usernames, passwords, credit card details, and other personally identifiable information (Öğütçü et al., 2016). Society may continue to suffer unless organizations are required to take more responsibility. In some jurisdictions, this trend has started, but until the liability shifts toward an organization, AI strategies may be more dictated by doing the minimum and doing what is most affordable than what might keep DevSecOps and user data safe, regardless of cost or other obstacles.

Therefore, the findings of this study suggest that a more proactive approach to implementing AI into the DevSecOps pipeline is required if organizations want to keep up with criminals and effectively mitigate existing and emerging threats. The sooner these changes take place, the more society will likely benefit. While criminals will undoubtedly adopt their approaches to exploiting vulnerabilities, it seems imperative that cybersecurity professionals adopt a culture of addressing security concerns through AI beforehand. If cybersecurity professionals want to protect society from cyber criminals, achieving superiority and gaining an advantage in defending computer systems and software may require a more proactive approach to AI implementation into DevSecOps.

Recommendations for Action

Even though the participants in this study comprised cybersecurity professionals with different backgrounds, most acknowledged a need for AI in DevSecOps to counter the increasingly sophisticated techniques some criminal's use. However, almost all participants also lacked a sense of urgency. Awareness of the potential threats these professionals face and how AI could better protect them against cyber criminals while

taking a step back to assess available options without taking action seems counterintuitive and counterproductive. The participants in this study consistently lacked the willingness to embrace and accept technology, blaming numerous extant factors, such as perceived usefulness, cost, or organizational culture.

Offering recommendations for actions is challenging because most participants did not show any signs of resentment and instead accepted or wanted to accept the status quo and the lack of AI implementation at their organization. Some of this reluctance to accept technology and change may be a fear of loss of employment. Some participants referred to this vaguely when they mentioned that AI needs experts and that they have only a limited understanding of AI. Some participants noted that they see education on AI as paramount for their organization to develop an AI implementation strategy and gather the necessary support from employees and leadership.

Therefore, my recommendation for action includes the facilitation of education, employee training, and a path to specializations that would allow regular cybersecurity professionals to remain in their positions or advance into more complex parts of the AI software development process. Publishing the findings of this study in related articles, journals, and books, as well as designing training programs and speaking at industry events, could raise awareness. Allowing stakeholders to understand implementation challenges better, they may notice the benefits a quick integration of AI into the DevSecOps pipeline can offer. Furthermore, advancing education on the benefits and challenges of AI in DevSecOps may lead to industry-wide recommendations for actions,

streamlined implementation strategies, and legislation that could force organizations to protect their data better.

Recommendations for Future Research

My experience with interviewing the participants in this study and the literature I reviewed inform my recommendations for future research. Due to the limitations of a qualitative study approach and the limited sample size, the answers provided by the participants may lack transferability across the entire cybersecurity industry as identified in my limitations. However, they still offer a window into common perceptions and issues related to AI implementation strategies throughout the DevSecOps pipeline. While the primary research goal of this study was to identify successful AI implementation strategies, the general lack of using AI in the DevSecOps industry suggested a lack of implementation strategies or AI solutions as its cause.

The interviews with the participants revealed several themes but no clear implementation strategies. It may well be that the participants in this study present an outlier and that several successful AI implementations exist. However, given the diversity of the participants and the extant literature, it is more likely that the DevSecOps industry lacks successful AI implementation strategies or that these strategies, should they exist, are not adopted. As discussed earlier under limitations, a case study can collect contextual data and explore how constructs are perceived within a particular context (Kumar, 2011). As I rely on a qualitative research method, the study's findings might be limited to a small group of participants and may not apply to the general population (Rutberg & Bouikidis, 2018). This study did not aim to quantify the factors contributing

to the lack of strategies or adoption, although several factors emerged throughout the discussions that would warrant further research.

In particular, the reluctance to embrace new technology, the perceived cost of implementation, and the failure to understand the technology and its benefits may all contribute to a lack of strategies or adopting successful strategies that may exist in other industries. Future research may want to focus on more in-depth studies of the dynamics between the above factors and whether one or many are responsible for decisions related to AI implementation strategies. Furthermore, additional research may illustrate whether tighter regulations would force organizations to adopt AI within their DevSecOps pipeline quicker. Similarly, other studies could help to understand the factors better that would reduce the reluctance to accept this new technology, such as education or changes in corporate culture.

Reflections

As a cybersecurity professional, I noticed a general lack of or reluctance to use AI in DevSecOps. Knowing that AI might be a challenging topic for many cybersecurity professionals, I soon realized that finding qualified participants would be difficult. While many showed an interest in AI and were ready to talk about their thoughts on the topic, very few had hands-on experience with AI or were somewhat involved in early discussions about implementation strategies at their organizations. Even those professionals with some AI experience made me realize that using AI in DevSecOps is significantly falling behind other industries.

Overall, I was hoping to identify several strategies cybersecurity professionals use to integrate AI into the DevSecOps pipeline but discovering and finding them applied across multiple organizations was more difficult than I initially imagined. After the initial selection process and subsequent vetting, I was finally able to find suitable participants, and I am grateful for their willingness to participate in this study. The challenges I faced in finding qualified cybersecurity professionals with experience in implementing AI in DevSecOps made me appreciate and anticipate similar experiences other researchers may have had. Finally, my study allowed me to identify some strategies cybersecurity professionals used when implementing AI into the DevSecOps pipeline and enabled me to refine potential areas of interest for future research.

Summary and Study Conclusions

While the findings of this study suggested that some AI implementation strategies exist in the DevSecOps community, most cybersecurity professionals eagerly pointed out the limitations of AI, its cost, and difficulties associated with finding and retaining experts. The lack of knowledge and perceived limitations of AI are problems other researchers also found in the DevSecOps community and noted that a culture of security awareness and technical education alone would be insufficient for changing perceptions among cybersecurity. It seems that issues related to technology acceptance within DevSecOps are deeply rooted, and without a cultural change, cybersecurity professionals may continue to delay the use of AI in DevSecOps, thus putting organizations and users at risk. It may be necessary for legislators to step in and further shift liabilities to organizations, increase potential penalties and enforce AI strategies for best practices.

While rapid cultural changes within the DevSecOps community are unlikely, changing legislation could force any such transition and hopefully provide cybersecurity professionals the incentive to embrace technology further and invest in securing their systems.

References

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulation as a methodological alternative. *Administração: ensino e pesquisa*, *19*(1). https://doi.org/10.13058/raep.2018.v19n1.578

Ahmed, Z., & Francis, S. C. (2019). *Integrating Security with DevSecOps: Techniques and Challenges* International Conference on Digitization (ICD), Sharjah, United Arab Emirates. https://doi.org/10.1109/ICD47981.2019.9105789

Ajibade, P. (2018). Technology Acceptance Model Limitations and Criticisms: Exploring the Practical Applications and Use in Technology-related Studies, Mixed-method, and Qualitative Researches. *Library Philosophy and Practice*, *9*.

Al-Emran, M. (2021). Evaluating the use of smartwatches for learning purposes through the integration of the technology acceptance model and task-technology fit. *International Journal of Human–Computer Interaction*, *37*(19), 1874-1882. https://doi.org/10.1080/10447318.2021.1921481

Alnaim, A. A. (2019). Using Rules Engine in the Automation of System Security Review. 2019 IEEE Cybersecurity Development (SecDev), Tysons Corner, VA, USA

An-Chi, L., & Tsung-Yu, C. (2020). An integrated technology acceptance model to approach the behavioral intention of smart home appliance [Article]. *International Journal of Organizational Innovation*, *13*(2), 95-118.

Arseven, I. (2018). The Use of Qualitative Case Studies as an Experiential Teaching

Method in the Training of Pre-Service Teachers. *International Journal of Higher Education*, *7*(1), 111-125. https://doi.org/10.5430/ijhe.v7n1p111

Azungah, T. (2018). Qualitative research: deductive and inductive approaches to data analysis. *Qualitative Research Journal*, *18*(4), 383-400. https://doi.org/10.1108/QRJ-D-18-00035

Babuta, A., Oswald, M., & Janjeva, A. (2020). Artificial Intelligence and UK National Security. *Royal United Services Institute for Defence and Security Studies*.

Bahaa, A., Abdelaziz, A., Sayed, A., Elfangary, L., & Fahmy, H. (2021). Monitoring real time security attacks for IoT systems using DevSecOps: a systematic literature review. *Information*, *12*(4), 154. https://doi.org/10.3390/info12040154

Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The Role of Artificial Intelligence in Cyber Security. In S. Geetha & A. V. Phamila (Eds.), *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems* (pp. 170-192). IGI Global. https://doi.org/10.4018/978-1-5225-8241-0.ch009

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and practice*, *2*(1), 1-10. https://doi.org/10.1186/s42466-020-00059-z

Camilleri, G., Antonelli, L., Zaraté, P., Gardey, J., Martin, J., Sakka, A., Torres, D., & Fernandez, A. (2020). Tool support for Generating User Acceptance Tests. ICDSST 2020, Zaragoza, Spain.

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

Candela, A. G. (2019). Exploring the function of member checking. *The Qualitative Report*, *24*(3), 619-628. https://doi.org/10.46743/2160-3715/2019.3726

Caravelli, J., & Jones, N. (2019). Cyber Security: Threats and Responses for Government and Business. ABC-CLIO, LLC.

Chatterjee, R. (2019). AI to aid DevSecOps. *dynamic CISO*. https://www.dynamicciso.com/ai-to-aid-devsecops/

Chatterjee, S., Rana, N. P., Khorana, S., Mikalef, P., & Sharma, A. (2021). Assessing organizational users' intentions and behavior to AI integrated CRM systems: a meta-UTAUT approach. *Information Systems Frontiers*, 1-15. https://doi.org/10.1007/s10796-021-10181-1

Chatterjee, S., Sarker, S., Lee, M. J., Xiao, X., & Elbanna, A. (2021). A possible conceptualization of the information systems (IS) artifact: A general systems theory perspective1. *Information Systems Journal*, *31*(4), 550-578. https://doi.org/10.1111/isj.12320

Chuttur, M. Y. (2009). Overview of the Technology Acceptance Model: Origins, Developments and Future Directions.

Cicmil, S., Cooke-Davies, T., Crawford, L., & Richardson, K. (2017). Exploring the complexity of projects: Implications of complexity theory for project management practice. Project Management Institute.

Clark, K. R., & Vealé, B. L. (2018). Strategies to enhance data collection and analysis in

qualitative research. *Radiologic technology*, *89*(5), 482-485.

Cognizant. (2019). *The security challenge whats next?* https://www.cognizant.com/us/en/whitepapers/documents/the-security-challenge-whats-next-codex4830.pdf

Collins, C. S., & Stockton, C. M. (2018). The Central Role of Theory in Qualitative Research. *International Journal of Qualitative Methods*, *17*(1), 10. https://doi.org/10.1177/1609406918797475

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, *11*(1), 100. https://doi.org/10.1186/1471-2288-11-100

Dalkin, S., Forster, N., Hodgson, P., Lhussier, M., & Carr, S. M. (2021). Using computer assisted qualitative data analysis software (CAQDAS; NVivo) to assist in the complex process of realist theory generation, refinement and testing. *International Journal of Social Research Methodology*, *24*(1), 123-134. https://doi.org/10.1080/13645579.2020.1803528

Dallas, K. (2020). How DevOps Powered by AI and Machine Learning Is Delivering Business Transformation. *devops.com*, 1.

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems : Theory and results* [Doctoral Dissertation, Massachusetts Institute of Technology]. http://hdl.handle.net/1721.1/15192

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319-340.

https://doi.org/10.2307/249008

Dawson, A. R. (2019). Exploring Strategies for Implementing Information Security Training and Employee Compliance Practices ScholarWorks.

Dawson, B. (2020). Is Artificial Intelligence the Future of DevSecOps? *CloudBees*, 1.

Department of Defense. (2018). Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense.

Deschene, M. (2016). *Embracing security in all phases of the software development life cycle: A Delphi study* (Publication Number 10156658) [Ph.D., Capella University]. ProQuest One Academic. Ann Arbor.

Dilek, S., Çakir, H., & Aydin, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *International Journal of Artificial Intelligence & Applications*, *6*(1), 21-39. https://doi.org/10.5121/ijaia.2015.6102

Emblemsvåg, J. (2020). Risk and complexity–on complex risk management. *The Journal of Risk Finance*, *21*(1), 37-54. https://doi.org/10.1108/jrf-09-2019-0165

Falcini, F., & Lami, G. (2017). Challenges in certification of autonomous driving systems. 2017 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW),

Ferreira, J., Cardim, S., & Branco, F. (2018). *Dynamic capabilities, marketing and innovation capabilities and their impact on competitive advantage and firm performance* 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, Spain.

Fishbein, M. (1976). A behavior theory approach to the relations between beliefs about an object and the attitude toward the object. In *Mathematical models in marketing* (pp. 87-88). Springer.

Fishbein, M., & Ajzen, A. (1980). Understanding Attitudes and Predicting Social Behaviour. *Englewood Cliffs*.

Fishbein, M., & Ajzen, I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research. *Philosophy and Rhetoric*, *6*(2), 244. https://doi.org/10.2307/2065853

Flick, U. (2018). The SAGE Handbook of Qualitative Data Collection. In. SAGE Publications Ltd. https://doi.org/10.4135/9781526416070

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., McCarthy, S., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research*, *18*(1), 120. https://doi.org/10.1186/s12913-018-2915-2

Fujdiak, R., Mlynek, P., Mrnustik, P., Barabas, M., Blazek, P., Borcik, F., & Misurec, J. (2019). *Managing the Secure Software Development* [Conference]. Canary Islands, Spain

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, *2020*(12), 6-12. https://doi.org/10.1016/s1361-3723(20)30127-5

Fusch, P., & Ness, L. (2015). Are We There Yet? Data Saturation in Qualitative Research. *Qualitative Report*, *20*, 1408-1416. https://doi.org/10.46743/2160-

3715/2015.2281

Gallardo, N., Gamez, N., Rad, P., & Jamshidi, M. (2017). *Autonomous decision making for a driver-less car* 2017 12th System of Systems Engineering Conference (SoSE), Waikoloa, HI, USA.

George, N., Khan, M., Velu, A., & Whig, P. (2021). Framework of Perceptive Artificial Intelligence using Natural Language Processing (PAIN). *Artificial Computational Research Society*.

Granić, A., & Marangunić, N. (2019). Technology acceptance model in educational context: A systematic literature review. *British Journal of Educational Technology*, *50*(5), 2572-2593. https://doi.org/10.1111/bjet.12864

Gray, L. M., Wong-Wylie, G., Rempel, G. R., & Cook, K. (2020). Expanding qualitative research interviewing strategies: Zoom video communications. *The Qualitative Report*, *25*(5), 1292-1301. https://doi.org/10.46743/2160-3715/2020.4212

Haenlein, M., & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review*, *61*(4), 5-14. https://doi.org/10.1177/0008125619864925

Hatcher, W. G., & Yu, W. (2018). A Survey of Deep Learning: Platforms, Applications and Emerging Research Trends. *IEEE Access*, *6*, 24411-24432. https://doi.org/10.1109/ACCESS.2018.2830661

Hercegovac, S., Kernot, J., & Stanley, M. (2020). How Qualitative Case Study Methodology Informs Occupational Therapy Practice: A Scoping Review. *OTJR: Occupation, Participation and Health*, *40*(1), 6-16.

https://doi.org/10.1177/1539449219850123

Hesse, A., Glenna, L., Hinrichs, C., Chiles, R., & Sachs, C. (2019). Qualitative Research Ethics in the Big Data Era. *American Behavioral Scientist*, *63*(5), 560-583. https://doi.org/10.1177/0002764218805806

Hong, J.-C., Lin, P.-H., & Hsieh, P.-C. (2016). The effect of consumer innovativeness on perceived value and continuance intention to use smartwatch. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2016.11.001

Hoyer, J., Holt, K., & Pelaez, J. (2018). Crafting a research question: Differentiated teaching for instruction with primary sources across diverse learning levels. *Society Of American Archive*, 28.

Humble, Á. M., & Radina, E. M. (2018). *How Qualitative Data Analysis Happens: Moving Beyond "Themes Emerged"*. Routledge. https://doi.org/https://doi.org/10.4324/978131517164

Jaradat, M.-I., & Al-Mashaqba, A. (2014). Understanding the adoption and usage of mobile payment services by using TAM3. *Int. J. of Business Information Systems*, *16*, 271-296. https://doi.org/10.1504/IJBIS.2014.063768

Junior, P., Abib, G., & Hoppen, N. (2019). The Qualitative Report Validity in Qualitative Research: A Processual Approach. *Qualitative Report*, *24*, 98-112. https://doi.org/10.46743/2160-3715/2019.3443

Karaboga, D., & Kaya, E. (2019). Adaptive network based fuzzy inference system (ANFIS) training approaches: a comprehensive survey. *Artificial Intelligence Review*, *52*(4), 2263-2293. https://doi.org/10.1007/s10462-017-9610-2

Kassan, A., Goopy, S., Green, A., Arthur, N., Nutter, S., Russell-Mayhew, S., Vazquez, M. S., & Silversides, H. (2020). Becoming new together: making meaning with newcomers through an arts-based ethnographic research design. *Qualitative Research in Psychology*, *17*(2), 294-311. https://doi.org/10.1080/14780887.2018.1442769

Khan, R. A., Khan, S. U., Khan, H. U., & Ilyas, M. (2021). Systematic Mapping Study on Security Approaches in Secure Software Engineering. *IEEE Access*, *9*, 19139-19160. https://doi.org/10.1109/ACCESS.2021.3052311

Korstjens, I., & Moser, A. (2017). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120-124. https://doi.org/10.1080/13814788.2017.1375092

Korzeniowski, Ł., & Goczyla, K. (2019). Artificial intelligence for software development — the present and the challenges for the future. *Bulletin of the Military University of Technology*, *68*, 15-32. https://doi.org/10.5604/01.3001.0013.1464

Kumar, R., & Goyal, R. (2020). Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC). *Computers & Security*, *97*, 101967. https://doi.org/10.1016/j.cose.2020.101967

Lam, T., & Chaillan, N. (2019). *DoD Enterprise DevSecOps Reference Design*. Department of Defence Office of prepublication and secureity review.

Laracy, J. R., & Marlowe, T. (2018). Systems Theory and Information Security: Foundations for a New Educational Approach. *Information Security Education Journal*, *5*(2). https://doi.org/10.6025/isej/2018/5/2/35-48

Lee, J. S. (2018). The DevSecOps and Agency Theory. 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW),

Lemon, L. L., & Macklin, C. (2021). Enriching employee engagement using complexity theory. *Public Relations Inquiry*, *10*(2), 221-236. https://doi.org/10.1177/2046147x20982524

Lobkov, K. (2019). *Methodologies of acceptance testing in SaaS environments* [Bachelor's Thesis, Metropolia University of Applied Sciences]. https://www.theseus.fi/bitstream/handle/10024/264539/Thesis_Lobkov_pdf.pdf?sequence=2

Lotz, V. (2020). Cybersecurity Certification for Agile and Dynamic Software Systems – a Process-Based Approach. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),

Lunt, H., Connor, S., Skinner, H., & Brogden, G. (2019). Electronic informed consent: the need to redesign the consent process for the digital age. *Internal medicine journal*, *49*(7), 923-929. https://doi.org/10.1111/imj.14339

Maher, C., Hadfield, M., Hutchings, M., & de Eyto, A. (2018). Ensuring rigor in qualitative data analysis: A design research approach to coding combining NVivo with traditional material methods. *International Journal of Qualitative Methods*, *17*(1), 1609-4069. https://doi.org/10.1177/1609406918786362

Makarius, E. E., Mukherjee, D., Fox, J. D., & Fox, A. K. (2020). Rising with the machines: A sociotechnical framework for bringing artificial intelligence into the organization. *Journal of Business Research*, *120*, 262-273.

https://doi.org/10.1016/j.jbusres.2020.07.045

Mämmelä, A., Riekki, J., Kotelba, A., & Anttonen, A. (2018). Multidisciplinary and Historical Perspectives for Developing Intelligent and Resource-Efficient Systems. *IEEE Access*, *6*, 17464-17499. https://doi.org/10.1109/ACCESS.2018.2816605

Mannay, D., & Morgan, M. (2015). Doing ethnography or applying a qualitative technique? Reflections from the 'waiting field'. *Qualitative research*, *15*(2), 166-182. https://doi.org/10.1177/1468794113517391

Marcelin, J. R., Siraj, D. S., Victor, R., Kotadia, S., & Maldonado, Y. A. (2019). The Impact of Unconscious Bias in Healthcare: How to Recognize and Mitigate It. *The Journal of Infectious Diseases*, *220*, S62-S73. https://doi.org/10.1093/infdis/jiz214

Maro, S., Steghöfer, J.-P., & Staron, M. (2018). Software traceability in the automotive domain: Challenges and solutions. *Journal of Systems and Software*, *141*, 85-110. https://doi.org/10.1016/j.jss.2018.03.060

Masrom, M. (2007). *Technology acceptance model and E-learning* 12th International Conference on Education, Universiti Brunei Darussalam.

Maurer, A., Parletta, D. A., Paudice, A., & Pontil, M. (2021). Robust unsupervised learning via L-statistic minimization. 38th International Conference on Machine Learning,

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2019). Twelve tips for conducting qualitative research interviews. *Medical Teacher*, *41*(9), 1002-1006.

https://doi.org/10.1080/0142159X.2018.1497149

Mihić, M. M., Dodevska, A. Z., Todorović, L. M., Obradović, L. V., & Petrović, Č. D. (2018). Reducing Risks in Energy Innovation Projects: Complexity Theory Perspective. *Sustainability*, *10*(9), 1-24. https://doi.org/10.3390/su10092968

Miko, J. A. (2017). *Collaboration Strategies to Reduce Technical Debt* (Publication Number 10635282) [Doctoral dissertation, Walden University]. ProQuest Dissertations and Theses Database.

Ming Deng, d. y. e. c., & Yuying Cao, y. p. e. (2018). Innovation and Effect Evaluation Model of Education and Training Outsourcing of State-owned Enterprises under Big Data [Article]. *Educational Sciences: Theory & Practice*, *18*, 3017-3027. https://doi.org/10.12738/estp.2018.6.201

Mitev, M. (2020). Measure Twice, Cut Once: Acceptance Testing. In *The Future of Software Quality Assurance* (pp. 93-104). Springer, Cham.

Mocanu, D. C., Mocanu, E., Stone, P., Nguyen, P. H., Gibescu, M., & Liotta, A. (2018). Scalable training of artificial neural networks with adaptive sparse connectivity inspired by network science. *Nature Communications*, *9*(1), 12. https://doi.org/10.1038/s41467-018-04316-3

Mohammad Ebrahimzadeh Sepasgozar, F., Ramzani, U., Ebrahimzadeh, S., Sargolzae, S., & Sepasgozar, S. (2020). Technology acceptance in e-governance: A case of a finance organization. *Journal of Risk and Financial Management*, *13*(7), 138. https://doi.org/10.3390/jrfm13070138

Mohammed, N. M., Niazi, M., Alshayeb, M., & Mahmood, S. (2017). Exploring software

security approaches in software development lifecycle: A systematic mapping study. *Computer Standards & Interfaces*, *50*, 107-115. https://doi.org/10.1016/j.csi.2016.10.001

Mori, S. (2018). US Defense Innovation and Artificial Intelligence. *Asia-Pacific Review*, *25*(2), 16-44. https://doi.org/10.1080/13439006.2018.1545488

Munoz, A. (2020a). *Exploring Strategies for Adapting Traditional Vehicle Design Frameworks to Autonomous Vehicle Design* [Doctoral dissertation, Walden University]. ProQuest Dissertations and Theses Database. https://scholarworks.waldenu.edu/dissertations/7944/

Munoz, A. (2020b). Traditional vehicle design frameworks in autonomous vehicle development. *International Journal of Teaching and Case Studies*, *11*(3), 238-257. https://doi.org/10.1504/IJTCS.2020.111142

Mushtaq, A., Riaz, S., Mohd, H., & Saleh, A. (2018). *Perception and technology adoption trends for autonomous vehicles: Educational case study* 2018 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, Sharjah, Abu Dhabi, United Arab Emirates https://doi.org/10.1109/ICASET.2018.8376923

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83-93. https://doi.org/10.1016/j.cose.2015.10.002

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in

Mixed Method Implementation Research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*(5), 533-544. https://doi.org/10.1007/s10488-013-0528-y

Panagiotopoulos, I., & Dimitrakopoulos, G. (2018). An empirical investigation on consumers' intentions towards autonomous driving. *Transportation Research Part C: Emerging Technologies*, *95*, 773-784. https://doi.org/10.1016/j.trc.2018.08.013

Parashar, R. (2021). Path to Success with CICD Pipeline Delivery. *International Journal of Research in Engineering, Science and Management*, *4*(6), 271-273.

Paul, S., Mahapatra, P., Banerjee, M., & Nandi, T. K. (2021). *AI shopping solution - the smartest all-in-one shopping solution* IOP Conference Series: Materials Science and Engineering,

Queiroz, M., Tallon, P. P., Sharma, R., & Coltman, T. (2018). The role of IT application orchestration capability in improving agility and performance. *The Journal of Strategic Information Systems*, *27*, 4-21. https://doi.org/10.1016/j.jsis.2017.10.002

Rahman, M. M., Lesch, M. F., Horrey, W. J., & Strawderman, L. (2017). Assessing the utility of TAM, TPB, and UTAUT for advanced driver assistance systems. *Accident Analysis & Prevention*, *108*, 361-373. https://doi.org/10.1016/j.aap.2017.09.011

Rangnau, T., Buijtenen, R. v., Fransen, F., & Turkmen, F. (2020). *Continuous Security Testing: A Case Study on Integrating Dynamic Security Testing Tools in CI/CD Pipelines* 2020 IEEE 24th International Enterprise Distributed Object Computing

Conference (EDOC), Eindhoven, Netherlands

Rao, Q., & Frtunikj, J. (2018). *Deep Learning for Self-Driving Cars: Chances and Challenges* 2018 IEEE/ACM 1st International Workshop on Software Engineering for AI in Autonomous Systems (SEFAIAS),

Rawat, G., Kumar, D., & Agarwal, K. N. (2021). Use of Artificial Intelligence in Modern Warfare and National Security. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),

Rice, T. (2019). Secure DevOps before DevSecOps. *Information System Security Association Journal*, *17*(11), 16-19.

Riemenschneider, C. K., & Hardgrave, B. C. (2001). Explaining software development tool use with the technology acceptance model. *Journal of Computer Information Systems*, *41*(4), 1-8.

Rutberg, S., & Bouikidis, C. D. (2018). Focusing on the Fundamentals: A Simplistic Differentiation Between Qualitative and Quantitative Research. *Nephrology Nursing Journal*, *45*(2), 209-213.

Sadighi, A., Donyanavard, B., Kadeed, T., Moazzemi, K., Mück, T., Nassar, A., Rahmani, A. M., Wild, T., Dutt, N., Ernst, R., Herkersdorf, A., & Kurdahi, F. (2018). *Design methodologies for enabling self-awareness in autonomous systems* 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany https://doi.org/10.23919/DATE.2018.8342259

Sanders, G., Morrow, T., Richmond, N., & Woody, C. (2021). *Integrating Zero Trust and*

DevSecOps.

Sarver, V. T. (1983). Ajzen and Fishbein's "theory of reasoned action": A critical assessment. *Journal for the Theory of Social Behaviour*, *13*(2), 155-163. https://doi.org/10.1111/j.1468-5914.1983.tb00469.x

Schafer Astroth, K. (2018). Exploring the Evidence. Focusing on the Fundamentals: Reading Quantitative Research with a Critical Eye [Article]. *Nephrology Nursing Journal*, *45*, 283-286.

Schoemaker, P. J. H., Heaton, S., & Teece, D. (2018). Innovation, Dynamic Capabilities, and Leadership [Article]. *California Management Review*, *61*, 15-42. https://doi.org/10.1177/0008125618790246

Sebele-Mpofu, F. Y. (2020). Saturation controversy in qualitative research: Complexities and underlying assumptions. A literature review. *Cogent Social Sciences*, *6*(1), 17. https://doi.org/10.1080/23311886.2020.1838706

Shaheen, M., Pradhan, S., & Ranajee. (2019). Sampling in Qualitative Research. In M. Gupta, M. Shaheen, & K. P. Reddy (Eds.), *Qualitative Techniques for Workplace Data Analysis* (pp. 25-51). IGI Global. https://doi.org/10.4018/978-1-5225-5366-3.ch002

Shajadi, A. (2018). Automating security tests for web applications in continuous integration and deployment environment Oulu University of Applied Sciences].

Sharma, G. D., Yadav, A., & Chopra, R. (2020). Artificial intelligence and effective governance: A review, critique and research agenda. *Sustainable Futures*, *2*, 6. https://doi.org/10.1016/j.sftr.2019.100004

Singh, R., Kumar, D., & Sagar, B. B. (2020). Selection of Best Software Methodology Using Entropy and TOPSIS. 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India

Sinha, A., & Das, P. (2021). Agile Methodology Vs. Traditional Waterfall SDLC: A case study on Quality Assurance process in Software Industry. 2021 5th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech),

Smith, G. (2018). The intelligent solution: automation, the skills shortage and cyber-security. *Computer Fraud & Security*, *2018*(8), 6-9. https://doi.org/10.1016/S1361-3723(18)30073-3

Sohn, K., & Kwon, O. (2020). Technology acceptance theories and factors influencing artificial Intelligence-based intelligent products. *Telematics and Informatics*, *47*, 101324. https://doi.org/10.1016/j.tele.2019.101324

Soni, N., Sharma, E. K., Singh, N., & Kapoor, A. (2020). Artificial Intelligence in Business: From Research and Innovation to Market Deployment. *Procedia Computer Science*, *167*, 2200-2210. https://doi.org/10.1016/j.procs.2020.03.272

Sorte, B., Joshi, P., & Jagtap, V. (2015). Use of Artificial Intelligence in Software Development Life Cycle: A state of the Art Review. *International Journal of Technology Management*, *03*, 2309-4893.

Stahl, N. A., & King, J. R. (2020). Expanding Approaches for Research:Understanding and Using Trustworthiness in Qualitative Research. *Journal of Developmental*

Education, *44*(1), 26-29.

Stenfors, T., Kajamaa, A., & Bennett, D. (2020). How to … assess the quality of qualitative research. *The Clinical Teacher*, *17*(6), 596-599. https://doi.org/10.1111/tct.13242

Stilgoe, J. (2018). We Need New Rules for Self-Driving Cars [Essay]. *Issues in Science and Technology*, *34*(3), 52-57.

Sualim, S. A., Yassin, N. M., & Mohamad, R. (2017). Comparative evaluation of automated user acceptance testing tool for web based application. *International Journal of Software Engineering and Technology*, *2*(2).

Sullivan, T. (2018). *The bad news about AI for cybersecurity: Hackers have access to the same tools as hospitals*. https://www.healthcareitnews.com/news/bad-news-about-ai-cybersecurity-hackers-have-access-same-tools-hospitals

Svensson, L., & Doumas, K. (2013). Contextual and analytic qualities of research methods exemplified in research on teaching. *Qualitative inquiry*, *19*(6), 441-450. https://doi.org/10.1177/1077800413482097

Tavares, J., & Oliveira, T. (2017). Electronic Health Record Portal Adoption: a cross country analysis. *BMC Medical Informatics And Decision Making*, *17*, 97-97. https://doi.org/10.1186/s12911-017-0482-9

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*, 509-533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

Tomas, N., Li, J., & Huang, H. (2019). *An Empirical Study on Culture, Automation, Measurement, and Sharing of DevSecOps* 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK.

Tyfield, D., & Zuev, D. (2018). Stasis, dynamism and emergence of the e-mobility system in China: A power relational perspective. *Technological Forecasting and Social Change*, *126*, 259-270. https://doi.org/10.1016/j.techfore.2017.09.006

Usha Rani, S. B. A. S. (2017). A detailed study of Software Development Life Cycle (SDLC) Models. *International Journal of Engineering and Computer Science*, *6*(7).

Vaismoradi, M., & Snelgrove, S. (2019). Theme in Qualitative Content Analysis and Thematic Analysis. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *20*(3), 23. https://doi.org/10.17169/fqs-20.3.3376

Van Brummelen, J., O'Brien, M., Gruyer, D., & Najjaran, H. (2018). Autonomous vehicle perception: The technology of today and tomorrow. *Transportation Research Part C: Emerging Technologies*, *89*, 384-406. https://doi.org/10.1016/j.trc.2018.02.012

Van de Wiel, M. W. (2017). Examining Expertise Using Interviews and Verbal Protocols. *Frontline Learning Research*, *5*(3), 112-140. https://doi.org/10.14786/flr.v5i3.257

Veiga, A. P. (2018). Applications of Artificial Intelligence (AI) to Network Security. University of Maryland.

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology

Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46*, 186-204. https://doi.org/10.1287/mnsc.46.2.186.11926

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*, 425-478. https://doi.org/10.2307/30036540

Weller, S. C., Vickers, B., Bernard, H. R., Blackburn, A. M., Borgatti, S., Gravlee, C. C., & Johnson, J. C. (2018). Open-ended interview questions and saturation. *PloS one*, *13*(6), 18. https://doi.org/10.1371/journal.pone.0198606

Widianto, S. R., SBK, F. A., & Purwanto, A. (2020). Analysis of Mobile Based Software Development Model: Systematic Review. *Jurnal Mantik*, *4*(3), 1703-1711.

Williams, L., McGraw, G., & Migues, S. (2018). Engineering Security Vulnerability Prevention, Detection, and Response. *IEEE Software*, *35*(5), 76-80. https://doi.org/10.1109/MS.2018.290110854

Williams, V., Boylan, A.-M., & Nunan, D. (2020). Critical appraisal of qualitative research: necessity, partialities and the issue of bias. *BMJ Evidence-Based Medicine*, *25*(1), 9-11. https://doi.org/10.1136/bmjebm-2018-111132

Woody, C., Chick, T., Reffett, A., Pavetti, S., Laughlin, R., Frye, B., & BANDOR, M. (2020). Devsecops pipeline for complex software intensive systems: Addressing the cybersecurity challenges.

Yang, R., Kang, V., Albouq, S., & Zohdy, M. (2015). Application of Hybrid Machine Learning to Detect and Remove Malware. *Transactions on Machine Learning and Artificial Intelligence*, *3*. https://doi.org/10.14738/tmlai.34.1436

Yin, R. K. (2018). Case study research and applications: design and methods (6th. ed.). SAGE.

Zarina I. Khisamova, I. R. B., Elina L. Sidorenko. (2019). Artificial Intelligence and Problems of Ensuring Cyber Security. *International Journal of Cyber Criminology*, *13*(2), 15. https://doi.org/10.5281/zenodo.3709267

Zaydi, M., & Nassereddine, B. (2021). DevSecOps Practices for an Agile and Secure IT Service Management. *Defense AR Journal*, *28*(2), 239.

Zyphur, M., & Pierides, D. (2017). Is Quantitative Research Ethical? Tools for Ethically Practicing, Evaluating, and Using Quantitative Research. *Journal of Business Ethics*, *143*, 1-16. https://doi.org/10.1007/s10551-017-3549-8

Appendix A: Permissions to Reprint

Maurice Ayidiya

From: Dr.Mohammed-Issa Riad Mousa Jaradat <mi_jaradat@aabu.edu.jo>
Sent: Wednesday, December 8, 2021 8:32 AM
To: Maurice Ayidiya
Subject: Re: Permission to use figures in dissertation.

Dear sir
You have a permission to use our modified model.

Sincerely,

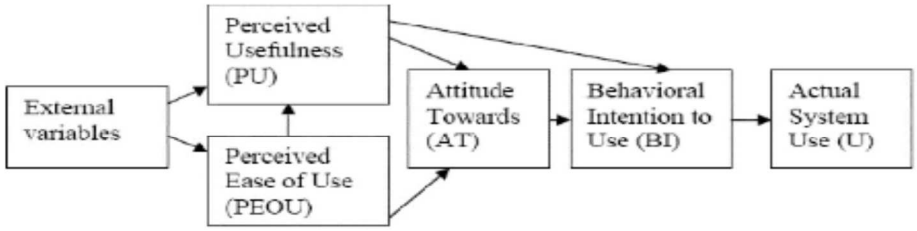
Mohammed-Issa Riad Mousa Jaradat, PhD
Professor

Department of Information Systems
Prince Hussein Bin Abdullah College for Information Technology
Al al-Bayt University

From: Maurice Ayidiya <maurice.ayidiya@waldenu.edu>
Sent: Wednesday, December 8, 2021 2:41 PM
To: abedalellah@yahoo.com <abedalellah@yahoo.com>; Dr.Mohammed-Issa Riad Mousa Jaradat <mi_jaradat@aabu.edu.jo>; mi_jaradat@yahoo.com <mi_jaradat@yahoo.com>
Subject: Permission to use figures in dissertation.

Hello Gentlemen,

I hope this e-Mail finds you in good Health. My name is Maurice Ayidiya. I am an information technology student at Walden University. I am currently working on my proposal for my Doctorate research, and I would like to kindly ask for permission to use



The above image from your paper titled "Understanding the adoption and usage of mobile payment services by using TAM," by M. I. Jaradat, & A. Al-Mashaqba, 2014, *Int. J. of Business Information Systems, 16*, 271-296. Copyright 2014 by M. I. Jaradat, & A. Al-Mashaqba.

1

Appendix B: Email Invitation

Subject: Invitation for Research Study Participation

Dear [Recipient],

My name is Maurice Ayidiya, and I am conducting a doctoral study to pursue a Doctor of Information Technology degree from Walden University. I am conducting a research study on the strategies that cybersecurity professionals use to incorporate AI technologies in developing secure software for IT operations (DevSecOps). Furthermore, this study explores the challenges of integrating AI solutions in the DevSecOps pipeline by identifying today's strategies to improve organizational security. Therefore, the study aims to address the development of frameworks and algorithms to ensure that AI as a tool is employed efficiently.

I would like to request your participation in the study. Participation is voluntary, and you may cease participation at any time. Please see the attached consent form for a detailed description of the research study and the opportunity to consent to participate.

Thank you for your consideration,

Maurice Ayidiya, MS, CE|H, CASP, Net+, Sec+

DIT Student

College of Management & Technology

Walden University

Appendix C: Interview Protocol

Interviews: Strategies that cybersecurity professionals use to incorporate AI technologies in developing secure software for IT operations (DevSecOps).

1. Before we begin, I introduce myself, thank the person for participating, and inquire if the participant has any questions.

2. Confirm consent and inform the participant that the interview will be audio recorded.

3. Begin the recording process. Then, provide the date and time, the participant number, and the study's title.

4. Conduct the interview and ask all pertinent questions. Allow the participant to respond to each question with as much information as they choose. If required, ask follow-up questions.

Demographic Questions

a) Without including your name or your organization's name, what is your current role, and how long have you been in similar roles?

b) How many years of experience do you have integrating AI as a cybersecurity professional?

c) What is the highest degree and certification earned in IT?

d) How many years of experience do you have working in cybersecurity?

e) How would you describe your knowledge level of security in a DevSecOps pipeline?

Interview Questions

a) To what extent does lack of know-how and competencies in AI affect cybersecurity?

b) As a cybersecurity professional, how did you improve your knowledge of AI technologies?

c) If any, what types of solutions do you use to reduce human involvement during security vulnerability testing?

d) How can penetration testing be automated and enhanced by integrating AI into the DevSecOps pipeline?

e) What is the industry of the professional security organization you work for in implementing AI into their DevSecOps pipeline?

f) How can the integration of AI into DevSecOps lead to the mitigation of Zero-day vulnerabilities?

g) How does the integration of AI into your organization's DevSecOps pipeline affect its time to respond to security incidents?

h) What competencies are required to implement AI into your organization's DevSecOps pipeline?

i) What are some of the implications of lacking AI technological competencies to your organization's cybersecurity?

j) What AI solutions may reduce human intervention in conducting security vulnerability testing?

5. Ask the participant if they would like to share more relevant information.

6. Explain how member checking informs the study and schedule a follow-up phone call.

7. End recording.

8. Thank the participant for participating. Offer to be contacted after the interview for any questions, concerns, or additional information.

Appendix D: NIH Certificate of Compliance

Conclusion

Go to Section: Completion Certificate >

Congratulations!

You have completed OHRP's learning module:

Lesson 1: When HHS Regulations Apply

OHRP does not collect information about who completes this training. Please fill out the information below and print this page for your records.

Name: Maurice Ayidiya

Date: 01/20/2022

Conclusion

Go to Section: Wrap Up > Completion Certificate

Congratulations!

You have completed OHRP's learning module:

Lesson 2: What is Human Subjects Research?

OHRP does not collect information about who completes this training. Please fill out the information below and print this page for your records.

Name: Maurice Ayidiya

Date: 01/30/2022

Conclusion

Go to Section: Completion Certificate (#) >

Congratulations!

You have completed OHRP's learning module:

Lesson 3: What are IRBs?

OHRP does not collect information about who completes this training. Please fill out the information below and print this page for your records.

Name: Maurice Ayidiya

Date: 01/30/2022

Conclusion

Go to Section: Completion Certificate >

Congratulations!

You have completed OHRP's learning module:

Lesson 4: Independent Review of Research

OHRP does not collect information about who completes this training. Please fill out the information below and print this page for your records.

Name: Maurice Ayidiya

Date: 01/30/2022