PERCEPTIONS OF PURPLE TEAMS AMONG CYBERSECURITY PROFESSIONALS

by

Siddharth S. Chowdhury

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer and Information Technology

West Lafayette, Indiana

May 2019

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Kathryn C. Seigfried-Spellar, Chair
Department of Computer and Information Technology
Dr. Marcus K. Rogers
Department of Computer and Information Technology
Dr. Baijian Yang
Department of Computer and Information Technology

Approved by:
Dr. Eric T. Matson
Head of the Graduate Program

ACKNOWLEDGEMENTS

To Amanda: Thank you for your constant encouragement in pretty much every aspect of my life. Finishing grad school would not have been possible without your love and support. I appreciate you listening to me complain and proof-reading everything I ever wrote including this.

To my parents: I could not have asked for better parents. Thank you for supporting me through my entire college journey in so many different ways and thinking what I do is cool. I am where I am because of your sacrifices, and I look forward to taking care of you.

To Dr. Kate: Thank you for being my mentor throughout grad school and most of my undergrad. I appreciate all of your guidance, and I look forward to continuing our interesting debates. Also, cheers to finally being friends on social media.

To Dr. Rogers and Dr. Yang: Thank you for all of your advice and time. I appreciate everything I learned from you two and having all the nerdy security and forensics conversations that made me excited to be in the field.

To my brother: You may not realize this, but even though you're the little one, you're such an inspiration to me. I appreciate your passion and your ability to express complex concepts with such immaculate creativity and vision. So proud of you.

To Jason: Thank you for pretty much being my partner in crime throughout college. Your openness to adventures is something I value significantly. Looking forward to many more years of friendship, travel, pop culture, memes, and tea.

To all my close Purdue friends: My journey in education would not have been the same without you. You made time outside school really fun and worth remembering. I will cherish all the ridiculous conversation and fun moments, and I hope we can continue to be friends for a long time.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

Blue teams: Information security professionals who use knowledge of attacks and the infrastructure to defend an organization's critical assets and systems against attacks and threats from adversaries (SANS, n.d.).

Command and control: The infrastructure generally consisting of servers and other devices used to control malware, and host computers infected with malware (Ipfs, n.d.).

Encryption: Encoding some information using a key such that only the intended recipient can access and read the information (Scarfone, Souppaya, Cody, & Orebaugh, 2008).

Exploit: Any attack used by an intruder on systems which leverages specific vulnerabilities on a system in order to gain access to it (Symantec, 2018).

Malware: malicious software programs which can damage digital systems, gain unauthorized access to information or user data, or disrupt the normal functioning of devices (Bossler, Holt, & Seigfried-Spellar, 2017).

Methodology: Teams conducting security assessments perform specific steps during engagements (such as gathering intel or identifying threats), which form the team's methodology (Veerasamy, 2009).

Purple teams: Information security professionals who bring together and use concepts and principles of red and blue teams simultaneously, with a focus on collaboration, for cybersecurity assessments (SANS, n,d,).

Red teams: Information security professionals who use tactics, techniques, and procedures (TTPs) to mimic real-world threats in order to measure the security capabilities of an organization's assets (SANS, n.d.).

Security audit: A comprehensive and thorough evaluation of the cybersecurity of a company's information systems and assets by comparing and evaluating it against a set of established criteria (Diogenes & Ozkaya, 2018).

White teams: Individuals responsible to serve as a referee during Red and Blue team engagements in information security audits; such a team evaluates success, resolves issues, and tries to ensure fairness (NIST Computer Security Resource Center, n.d.).

LIST OF ABBREVIATIONS

DOD	Department of Defense
C2	Command and Control
IoC	Indicators of Compromise
IoT	Internet of Things
IR	Incidence Response
IRB	Institutional Review Board
IP	Internet Protocol
NIST	National Institute of Science and Technology
MTTC	Mean Time to Compromise
MTTD	Mean Time to Detection
MTTP	Mean Time to Privilege Escalation
MTTR	Mean Time to Response
TTP	Tactics, Techniques, and Procedures

ABSTRACT

Author: Chowdhury, Siddharth, S. MS
Institution: Purdue University
Degree Received: May 2019
Title: Perceptions of Purple Teams Among Cybersecurity Professionals.
Committee Chair: Dr. Kathryn Seigfried-Spellar

With constant technological advancements, the attacks against existing infrastructure is constantly increasing and causing more damage. The current Red and Blue team approach to cybersecurity assessments is used to test the effectiveness of security defenses and in identifying vulnerabilities before they are exploited. Due to a lack of collaboration and inherently contradicting natures of these teams, the credibility of audits is impacted. While this has led to the synergistic and collaborative Purple team, it is important to understand how cybersecurity professionals perceive this new concept and its function. Analyzing perceptions of self-reported cybersecurity professionals via an online survey showed most believed Purple teams were beneficial and should be created from and collaborate with Red and Blue teams. However, past Red team experience was negatively linked to perceived benefit. Those who had more years of experience or had been on Red teams were more likely to believe Purple teams may have ownership or learning issues. Furthermore, professionals identified active managerial involvement and project clarity as critical success factors for Purple teams. Alongside these, management could help find the right skillset, provide resources, and offer active direction in order to avoid issues and maximize outcomes. Based on assessment relevance, a collaborative agreed-upon methodology for Red, Blue, and Purple teams was provided.

1. INTRODUCTION

1.1 Background

Cybersecurity is becoming increasingly important due to an increase in the number of threats. For example, implanting malware (i.e., malicious software) into a software package meant to be legitimate went up around 200 percent in 2017, while attacks on mobile devices went up around 54 percent since 2016 (Symantec, 2018). Such upward trends were also seen across attacks aimed at gaining cryptocurrencies such at Bitcoin and Ethereum, which went up 8500% in 2017 (Symantec, 2018). Industry surveys showed around 42% of organizations experienced attempts at some form of distributed denial of service (DDoS) attacks in 2017, which aim to make services unavailable to consumers (Cisco, 2018). For 2018, the global average cost of a single data breach now averages at $3.86 million, while the cost of each individual stolen sensitive record is around a $148. The increased value of targets has caused a surge in the volume of attacks, and cybercrime alone is estimated to cause damages of over $6 trillion worldwide within the next three years. (Morgan, 2017b). Since the rate at which companies and governments are attacked has increased, these organizations need to build and maintain a strong cybersecurity infrastructure and constantly evaluate their security capabilities to reduce risk.

The National Institute of Science and Technology (NIST) claims cybersecurity risks can be minimized or mitigated by conducting security audits and tests which include a documented methodology, well-identified resources, and established processes (Scarfone, Souppaya, Cody, & Orebaugh, 2008). Conducting such standardized testing would help in managing constraints, increase re-usability of methods, standardize organizational testing methods, and optimize time required for evaluations (Veerasamy, 2009). When conducting security audits, both offensive and defensive approaches can be taken. The method of simulation offensive and defensive security for testing the cybersecurity posture of an organization is referred to as Red and Blue team, while it is adapted from its traditional military definition (see Yang, Abbass, & Sarker, 2006). The U.S. Department of Defense (DoD) directive 8570 defines the Red and Blue teams as:

> A Red team conducts assessments via an independent, focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities to improve information systems security posture, [while] a blue team conducts systematic examinations of information system or products to determine adequacy of security measures, to identify security deficiencies, to predict effectiveness of proposed security measures, and to confirm adequacy of such measures after implementation (DoD, 2015, p. 86, 92).

The Red team and Blue team approaches to cybersecurity allow organizations to evaluate the susceptibility of their assets without facing a real threat. The Red team can test various exploits and utilize all possible loopholes to try to bypass security controls, while the Blue team can protect their assets and test both passive and active detection of threats in the system.

A new approach to such security auditing is Purple teaming; while the concept itself is not new, the idea of utilizing such an approach in security is (Salerno, 2017). The traditional Red team – Blue team approach yields results, but there are issues with the current approach. The Red team always wins as there is always a loophole to exploit, while the Blue team tries to play catchup (Salerno, 2017). The opposing nature of the teams could cause misleading results as Blue teams can just build to defend against Red Teams (Johnson, 2016). This disconnect between the approaches is due to lack of communication and setup, and thus the new Purple approach focuses on utilizing collaboration and information sharing to achieve the same goals. A Purple team performs and implements principles of both Red and Blue team-based security testing in order to evaluate the security of a company. The Purple team focuses on both attacking and defending which gives them a different perspective into security (SecureAuth, 2018), and maximizes the effectiveness and potential of the Red and Blue teams (Miessler, 2016). This approach integrates the defensive approach and control with the threat research and vulnerability analysis for optimal security auditing (Veerasamy, 2009; Peters, 2016).

1.2 Problem Statement and Significance

The Red team - Blue team approach to information security assessments mimics real-world threat actors and their techniques (NIST Computer Security Resource Center, n.d.). Information gathering from such an approach provides a versatile method of validating the effectiveness of security defenses and identifying vulnerabilities before they are exploited

(Rajendran et al., 2011). However, because of the way security assessments are designed, the Blue and Red teams aim for different, and often contradictory, outcomes during testing, as the success of one is the failure of the other (Mirkovic et al., 2008). The competition created due to their opposing natures leads to secrecy between the teams, which cause the teams to conduct their testing isolated from each other. It can impact credibility of audits as the current setup does not always provide a complete and true picture of the security infrastructure (Miessler, 2016). The dynamic Purple team approach which prioritizes information sharing and collaboration creates a more synergetic relationship between the offensive and defensive approaches (Miessler, 2016).

The combined Purple teams, and the opposing and independent Red and Blue, each have their own advantages and disadvantages when conducting cybersecurity assessments. The Purple team concept provides a newer security perspective and can provide significant value when used alongside traditional Red and Blue teams (SecureAuth, 2018). This makes it necessary to proof-of-concept a purple team and its methodologies and evaluate the best metrics to be an effective Purple team; in cybersecurity, a proof-of-concept involves assessing a method or an idea to evaluate its feasibility in terms of fulfilling its intended aim (Malwarebytes, n.d.). Research has shown role clarity, commitment to job role, and job satisfaction are all impacted by a person's belief of whether their agency or group servers a purpose and has value (Boardman & Sundquist, 2009). Just if Purple teams were to succeed, it becomes essential to understand how the community of professionals perceive the concept. This would help managers and organizations assess if Purple teams and beneficial and if it worked in their respective organizations.

From a research standpoint, Red-Blue oriented cybersecurity testing used to be rare in the academic community (Leggio, 2017; Mirkovic et al., 2008), but it has gained popularity among students through cybersecurity competitions where such simulations can be practiced (Leggio, 2017). Due to increased recognition of the phenomenon and its importance to securing critical infrastructure, academia has also begun to research these assessments with the goal of evaluating and optimizing them (see Carayon & Kraemer, 2004; Fultz & Grossklags, 2009; Mirkovic et al., 2008; Veerasamy, 2009). This study aims to also add to the scientific body of literature by analyzing how security professionals perceive the current Red-Blue approach to security auditing and be one of the first academic studies to evaluate the steps to create and optimize a combined Purple team.

1.3 Research Question

The study aimed to answer the following research question: "How do cybersecurity professionals perceive Purple teams?" This research question was assessed by perception scales, needs analyses, and methodology ratings.

1.4 Assumptions

The assumptions made in the study include:

- Individuals participating in the current study are cybersecurity professionals who have either previously held or currently have a cybersecurity-related job.
- The definitions and understanding of Red, Blue, and Purple teams are the same across individuals in the security industry.
- Companies and individuals performing these assessments follow a standard set of procedures.
- The opinions of individuals participating in the survey will come from their own experiences and not third-party accounts.
- The participants who complete the survey will follow the survey's intended function and answer questions with integrity.

1.5 Limitations

The limitations of the study include:

- Due to the nature of the survey and company policies, not all cybersecurity professionals who see the survey will be able to take it.
- This study only surveys cybersecurity professionals and will not assess how the management component of a company views these assessments.
- Prior experiences of participants who have done such assessments may influence their results.
- The method of survey distribution will only give the researcher access to a specific subset of the security community
- The small sample size obtained by the study may impact overall generalizability to the population of cybersecurity professionals.

1.6 Delimitations

The delimitations of the study include:

- The study only focuses on individuals residing and working in the United States.
- The study will only collect and analyze quantitative data, so qualitative data from context and experiences will not be assessed.
- Only individuals from red teams, blue teams, and purple teams from industry will be included, as government employees may not be able to participate.
- For the purpose of this study, individuals are considered security professionals only if they have previously worked in industry in a security related role.
- Other iterations of assessments such as White teams will not be considered for the purposes of this study.
- Incomplete data from the data collection phase will not be used during analyses.

1.7 Summary

This chapter provided an overview by describing the history, problem being studied, the significance of the problem, and the research questions. Because of the popularity of cybersecurity auditing, and the potential issues of Red team - Blue team testing, Purple teams have been proposed to improve efficiency, information sharing, and communication. The author aims to evaluate the research questions proposed based on this problem and assess if Purple teams are beneficial according to cybersecurity professionals and if a high-level methodology can be created for it. The assumptions, limitations, and delimitations of the current study are also described in this chapter. The next chapter will review the literature describing cybersecurity testing, Red and Blue teaming, Purple teams, and the need for them in industry.

2. REVIEW OF RELEVANT LITERATURE

2.1 Cybersecurity

The concept of cyberspace forms one of the critical components of life in the 21st century, and includes multifaceted and ever-changing connections of devices, information, and technology on a global scale (Maughan, 2010). The need to protect communication, markets and economies, infrastructure, public safety, and security have led to an increasing demand to secure this 'cyberspace' and a need to provide progressive technical and policy-based developments in the field. Cybersecurity, in academia, industry, and at a nation-state level, has grown exponentially over the last decade. The efforts on dealing with cybersecurity threats have become a focus, which is evident from the worldwide cybersecurity spending being around $86.4 billion in 2017; it is set to be around $93 billion dollars in 2018 (Morgan, 2018). The increase in spending and concern of threats is not without reason, as cybercrime has cost the world $3 trillion dollars in 2015 and is predicted to cause damages of over $6 trillion dollars by 2021 (Morgan, 2017b).

The various cybersecurity-related crimes have significantly impacted the world in terms of "damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm" (Morgan, 2017b, p. 1). Individuals committing these cybercrimes, such as hacking and phishing, can utilize the quick and anonymous nature of the Internet to commit criminal activities across the world without any physical borders (Bossler, Holt, & Seigfried-Spellar, 2017; Interpol, n.d.). For example, in 2014, the dates of birth, email addresses, and passwords for three billion Yahoo users were compromised by international hackers which damaged user security and also dropped Yahoo's net worth by around 300 million dollars (Armerding, 2018). In May 2017, one of the largest cyberattacks in history called WannaCry locked individuals and companies out of their data unless ransom was payed. The self-spreading malware infected more than 200,000 computers in around 150 countries across the world (Sherr, 2017); while it was controlled, variants are still active today.

This issue is not just an industry problem, but also a national security and defense issue. The rise of nation state and nation state sponsored attacks have been proven to impact the U.S. in major ways, such as the Russian tampering of the U.S. election process (Simister, 2018). The national intelligence agencies in the U.S. found Russian actors were able to compromise voting systems in around 39 states, as well as create thousands of fake media campaigns to misinform and manipulate unsuspecting voters (Ward, 2017). One of the most impactful breaches of this century occurred in the summer of 2017 when social security numbers, birth dates, addresses, and some drivers' license numbers of 143 million US consumers were leaked; it quickly became a national security issue due to the reliance on social security numbers for financial and other major transactions (Armerding, 2018).

Through time and advancements in technology, both attack and the defense procedures have gotten more advanced. Technologies such as machine learning and automation have been used in both cybersecurity-based defense and attacks; Simister (2018) claims about 87% of US cybersecurity professionals use machine learning, but also are concerned about the use of the same technology in launching more sophisticated attacks. Adversaries have significantly upgraded their tools such as malware (i.e., malicious software) to high levels of sophistication and damage capability. The Cisco (2018) and Symantec (2018) annual reports state upgrading malware such as ransomware to automatically propagate, remove the need for human control, and include other advanced techniques have made detection and response much harder. Some predictions show organizations will experience ransomware attacks every 14 seconds by 2019, and the current amount of spending due to ransomware payments is around a billion dollars (Morgan, 2017b).

Technologies used to evade detection and the ability to weaponize trusted services have become more popular. Adversaries are becoming more adept at evasion and are weaponizing cloud services and other technology meant to be used for legitimate purposes (Symantec, 2018). While there are methods to detect malicious actors or software, advanced threats have been able to elude detection using machine learning and encryption (Symantec, 2018). This makes it easier to hide all command-control (C2) activity, as they are able to implement practices making malicious traffic harder to identify, or indistinguishable from standard user traffic (Cisco, 2018).

Another growing issue is exploiting gaps in security due to the advent of new technology such as the Internet of Things (IoT) and dependence on the public cloud. Adding countless new

devices to networks has significantly increased the attack surface and created multiple points of entry into a network (Cisco, 2018). For example, in 2016, malware called Mirai took over thousands of routers, DVRs, CCTV cameras, and other 'smart' IoT appliances by exploiting vulnerabilities, and used these devices to launch massive denial of service (DDoS) attacks to shut down websites and other services (Symantec, 2016). Due to the increase in complexity of attacks, an increase in the attack surface, and the reliance on technology, it has been essential to protect and secure organizations and systems using novel methods (Morgan, 2017b; Symantec, 2018). When building and maintaining such a system, various measures can be conducted to test and ensure optimal cybersecurity capabilities (Palmer, 2001).

2.2 Strategies for Cybersecurity Testing

The necessity for cybersecurity testing created from the growing threat landscape has led to various strategies to assess the security capability of organizations. These types of security assessments aim to evaluate how accurately the current capabilities meet security related goals and objectives set by both the organizations and good-practice standards; it would involve testing "hosts, systems, networks, procedures, and persons" (Scarfone, Souppaya, Cody, & Orebaugh, 2008, p. ES1). The aim of such testing is to assess if the environment is protected against possible threats in various contexts and settings and evaluate metrics to measure success; which helps prevent circumvention of security controls by attacks (Mirkovic et al., 2008). When conducting such assessments, organizations are constrained by factors such as time, budget, employee skillsets, hardware, and software (Scarfone et al., 2008).

When a system or organization undergoes a cybersecurity evaluation, each component of the system should be tested against all potential possibilities and issues (Palmer, 2001). Individual tools and techniques can prove inefficient in being able to provide a complete and comprehensive image of the cybersecurity capabilities of systems and networks (Scarfone et al., 2008). Pairing combinations of these methods can increase the reliability and validity of these tests. By creating a combination of such methods, security testing can be broadly categorized into offensive and defensive security.

Offensive security testing is based on the idea of testing the system by pretending to be an adversary. By taking an adversarial approach and attacking the system and networks, analysts can identify security vulnerabilities (Scarfone et al., 2008). This would involve the usage of

scanning and penetration testing techniques and can simulate the likelihood of ill-intentioned threats being able to exploit loopholes to gain access to unauthorized information. On the contrary, defensive security is the conventional form of security which is based on the idea of proactive and reactive measures such as implementing security controls, patching hardware and software, and fixing vulnerabilities to safeguard an organization's assets.

2.3 Red and Blue Teams

Offensive and defensive security audits through simulations and testing are known are Red teaming and Blue teaming respectively (NIST Computer Security Resource Center, n.d.). Started by the German military around the 19th century to train its officers as a rule-based map simulation of real war strategies (Fontenot, 2005), the Red and Blue teaming approach stated as a form of interaction were at least one party simulated being an enemy. This idea has since been adopted into the cybersecurity domain to allow testing from an adversarial mindset via replication on threats, and developing countermeasures based on the results of such tests. All of the top Fortune companies either conduct such security auditing themselves or contract them out to consulting firms (Drinkwater & Zurkus, 2017). Organizations and companies who do not have the budget to acquire, build, and retain such teams rely on external professionals (Embers, 2018). Among the companies which implement such testing in-house, some of them have dedicated Blue and Red teams, while some create them for testing exercises as needed (Miessler, 2016).

2.3.1 Red Teams

The Red team engages in offensive security auditing by conducting attacks on a network or system to break through existing security controls (Diogenes & Ozkaya, 2018); this kind of testing is also called penetration testing. The focus of this approach is based on the idea that modeling an adversary and mimicking their behavior can help analysts locate vulnerabilities which would normally go undetected without a real threat (Carayon & Kraemer, 2004). The drive when penetration testing is attacking the existing cybersecurity defenses of an organization, which can then be exploited to gain control of the assets of the entity being tested (Diogenes & Ozkaya, 2018).

The primary metrics used to evaluate Red team exercises are "Mean Time to Compromise" and "Mean Time to Privilege Escalation" (Diogenes & Ozkaya, 2018). Mean time

to compromise is a measure of the length of time it takes to compromise a specific asset, while mean time to privilege escalation is the length of time is takes for the attacker to gain administrative access on the asset (Diogenes & Ozkaya, 2018). These metrics are evaluated during each assessment and used to measure the effectiveness of the security controls the organization has in place. The values of the metrics vary substantially by the organization being tested, as they are impacted by size, scope, type of tests, and other factors. (Scarfone et al., 2008; Miessler, 2016). The good and acceptable values are decided by all involved parties before the assessment occurs (Scarfone et al., 2008), or by using complex mathematical models and functions which account for various factors (see Abraham, 2016; Leversage & Byres, 2008; McQueen, Boyer, Flynn, & Beitel, 2006).

Individuals who are part of a Red team require high levels of domain knowledge of known threats and should have a basic understanding of the organization's functioning. Being able to develop and customize exploits can increase possibility of success, so individuals on this team tend to practice developing malware and other exploits. They also need to be able to create adaptable methods of penetration and be able to dynamically adapt to changing defenses (Carayon & Kraemer, 2004).

2.3.1.1 Red Team Methodology

Red teaming, or offensive penetration testing can be differentiated based on an analyst's approach. One can perform overt testing, also called white hat testing, where the technology department is aware of and has approved the test. This helps organizations evaluate the security of the organization with a targeted approach (Scarfone et al., 2008). However, since the technology department and the defensive Blue team are aware of the attacks, it will impact the validity of the test. Contrarily, testing can also be done covertly, called black hat testing, which involves the analysts acting as adversaries and performing tests without the knowledge of IT (and only known by management). This approach allows the testing of incidence response (IR) practices within the company and evaluation of real-world security controls (Scarfone et al., 2008). This form of testing allows for exploiting more vulnerabilities but requires more time to discover them and get around existing security controls.

In NIST's 800-115 guidelines for information security testing, the Red team methodology is described in Figure 2.1 below. Each assessment in Red teaming starts with the discovery

phase, which would involve gathering information about the target and its assets. This could be done though gathering open source information available online, scanning networks, discovering assets, and other methods. In case of overt testing, the team could also review logs and records before an attack. As shown in Figure 2.1, it follows with gaining access by exploiting vulnerabilities found in the discovery phase. After basic access is gained, the main goal of a Red team is to gain access to a privileged account – the default accounts targeted are "Domain Administrator" accounts, as it gives them access to all assets, and allows creation of users at will (Scarfone et al., 2008). Getting access to such high-level accounts also allows the Red team to learn more about the organization and discover more points of entry, which can be used in later tests. Other tools can also be installed at different phases, to help gain access to the administrator account.

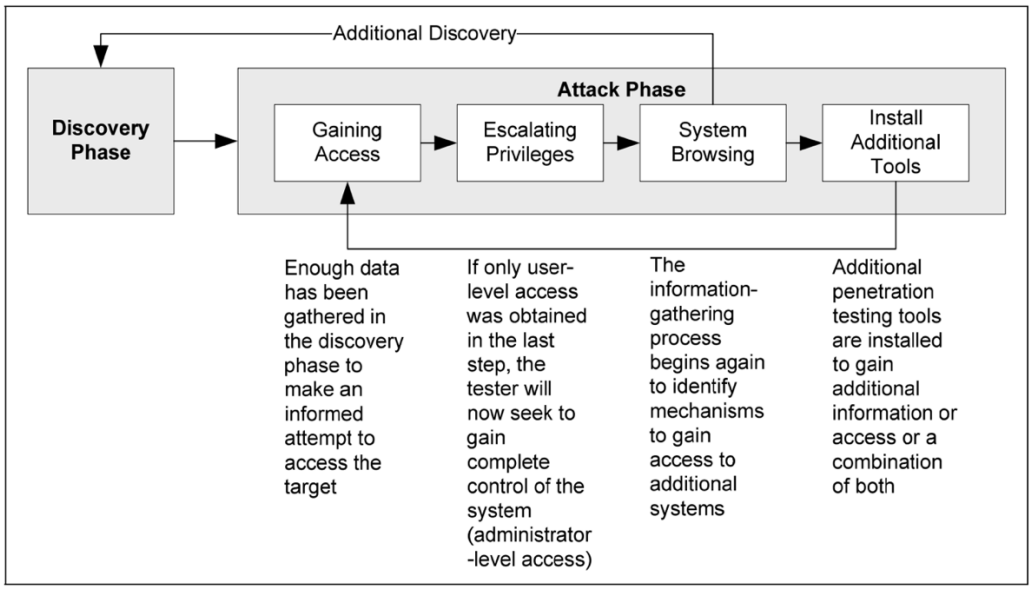


Figure 2.1 NIST Red Team Methodology (Scarfone et al., 2008)

Just as with NIST's guidelines, Veerasamy (2009)'s Red and Blue team methodologies (see Figure 2.2) also cover the same steps to successful Red team assessments. Information gathering and footprinting are always the first step, which is part of the discovery or reconnaissance phase. Footprinting is part of profiling an organization's security by scanning for and discovering domain names, networks and IPs, hosts, operating systems, and other information. The Red team then investigates vulnerabilities and uses them in penetration testing

to simulate attacks on the system; recommendations are made based on the findings. The recommendations are generally expressed in terms of the vulnerabilities located, how they were exploited, and potential steps which could be taken to address each vulnerability (Scarfone et al., 2008); examples of actions suggested could include "policy, process and procedure modifications, security architecture changes, deployment of new security technologies, and deployment of OS and application patches" (Scarfone et al., 2008, p. 8-1).

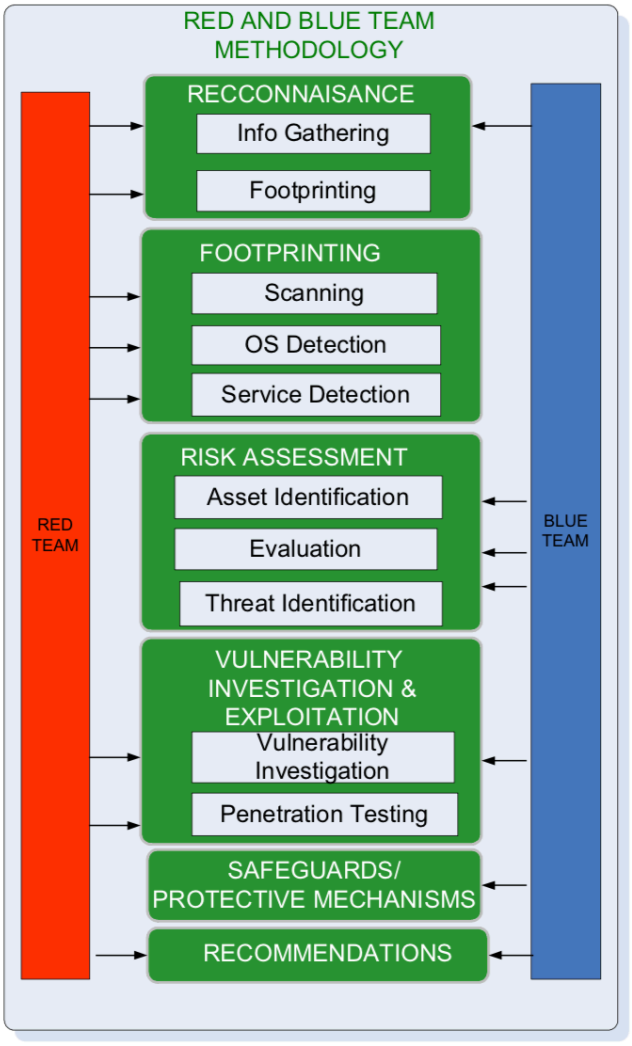


Figure 2.2 Comparison of Red and Blue Team Methodology by Veerasamy (2009)

2.3.2 Blue Teams

The Blue team engages in defensive security auditing which can be performed in two phases: 1) developing security controls before Red team testing, and 2) conducting incidence response and mitigation after Red team testing (Diogenes & Ozkaya, 2018). From the precautionary perspective, Blue teamers are "defense designers" (p. 1098) who build defensive capabilities of an organization such as firewalls, code to detect anomalies, system configurations, etc., and document security design (Mirkovic et al., 2008). If the Red team is able to successfully exploit vulnerabilities, the Blue team analysts save evidence of the "hack" so as to be able to analyze the information to create actionable intelligence (Diogenes & Ozkaya, 2018).

Whatever alerts or information led to knowledge of the breach should also be documented and are called Indicators of Compromise (IoCs). They are critical to proactive Blue teaming as they can be used to automate defenses the next time the same attack types repeat themselves. These IoCs can be used to make changes, be able to patch it if possible, or create detection logic to identify and block such threats in the future (Diogenes & Ozkaya, 2018). From a precautionary standpoint, Blue teams also develop incidence response remediation plans which indicate the steps to be taken in case of a real-world breach using intelligence gathered from Red team testing (Diogenes & Ozkaya, 2018).

For the Blue team, while defenses are evaluated based on how successful the Red team members are, they also need to take precautions and build defenses before testing. The primary metrics used to evaluate Blue team exercises are "Mean Time to Detection" and "Mean Time to Response" (Diogenes & Ozkaya, 2018). Mean time to detection is a measure of the length of time it takes to discover if an organizational asset has been compromised, while mean time to response is the length of time is takes for the defenders to respond to the threat, stop the attackers, and remediate the issues (Diogenes & Ozkaya, 2018). Just like the Red team, these metrics are also evaluated during each assessment. The additional step for Blue teams is after the assessment, the metrics and results are used to strengthen defenses of the organization against real attackers. Just as with a Red team, values are decided by all involved parties before the assessment occurs (Scarfone et al., 2008), or by using complex mathematical models and functions which account for various factors (see Abraham, 2016; Leversage & Byres, 2008; McQueen, Boyer, Flynn, & Beitel, 2006).

Analysts who work as Blue team members need a thorough knowledge of the organization's infrastructure, functioning, and operations (Rajendran et al., 2011). They also need to have some knowledge of threats so as to build defenses and set up security controls against them and be able to think like or put themselves into the mindset of attackers. Blue teamers also should be able to build tools and develop detection logic in order to monitor networks, establish monitoring of servers and client devices, and build firewalls and other security controls (Carayon & Kraemer, 2004).

2.3.2.1 Blue Team Methodology

The process of defending from threats begins with the development of the organization's assets and systems. The Blue team designs and builds security into the hardware and software during development, as well as creates configurations and methods to monitor information (Rajendran, Jyothi, & Karri, 2011). In a real-world setting, even if a single attack bypasses the defenses without being detected at any stage, then the vulnerable defenses are a major liability to the organization. Blue teamers evaluate the effectiveness of defenses by actively and passively monitoring to find threats in the design, as well as find ways to remediate discovered threats (Rajendran et al., 2011).

Veerasamy (2009)'s Red and Blue team Methodologies (see Figure 2.2) describes a high-level methodology to conduct Blue team assessments. It also relates it to the steps the Red team takes so as to highlight where the Blue team activities take place in the larger security evaluation perspective. Just as with the Red team, the information gathering and discovery phase is a critical first component for the Blue team. The team needs to understand the existing infrastructure and security controls, enumerate and document assets, and understand existing and future threats to be able to build defenses. After identifying assets, risk is evaluated for each component, and the relevant threats are identified.

To identify assets and risks, NIST recommends Blue teamers review documentation, logs from software, rulesets and system configurations from hardware, identify vulnerable networks and ports, and review the integrity of files (Scarfone et al., 2008). Using the identified assets, risks, and corresponding vulnerabilities, the Blue team builds and maintains the safeguards and protective mechanisms. Blue teams must also develop Incidence Response plans to deal with breaches and establish remediation strategies in case of a successful attack. This strategy is

developed at the beginning during risk assessment and updated based on reporting provided by the Red team, and well as during any real breaches (Scarfone et al., 2008). After the Red team provides the Blue team with a list of vulnerabilities exploited, Blue teams conduct root cause analyses – tests to determine the actual issue or error causing the vulnerability. Based on the cause, each corresponding security control is then updated so as to mitigate the issue, while balancing security and functionality (Scarfone et al., 2008).

2.4 Purple Teams

Since the use of Red and Blue teams in cybersecurity, various studies have been conducted in the industry as well as some in academia to assess, measure, and improve their performance (see Carayon & Kraemer, 2004; Fultz & Grossklags, 2009; Leggio, 2017; Mirkovic et al., 2008). Simulations of red and blue team exercises using Game Theory by Fultz and Grossklags (2009) shows as long as protections are more than value of loss or self-insurance, Red teams will always attack with maximum force, and the Blue team will suffer that cost. In a real-world setting, such attacks will only occur if the attack is likely to yield profitable results and the deterrence is lower (Fultz & Grossklags, 2009).

While the inherent purpose is to work together to secure a system, this is not always the case as the two traditional teams are competing against one another. The Red teams tends to generally "win" as they just simply need to exploit one loophole or vulnerability that the Blue team may have missed (Johnson, 2016). When validating the security assumptions, they could go out of scope or use information they should not. Similarly, the Blue team may make a system stricter to guard against the Red team specifically, which can provide a false metric of real security capability (Johnson, 2016). Thus, in the growing threat landscape, there is still a constant need to harden one's defenses and actively test its capabilities, which has led to the use of Purple teams in security (SecureAuth, 2018).

2.4.1 Need and Concept

In terms of simulation-based training, when an assessment is planned, it is beneficial to explore the different possible outcomes so as to optimize testing and cybersecurity missions (Yang, Abbass, & Sarker, 2006). From a Red - Blue perspective, the simulation is based on the idea of a Red team trying to gain control of and seize an area or system, while the Blue team

aims to protect this system and deal with the aftermath in case of failure. As long as the attacker is active, the defensive side will try to defend (Fultz & Grossklags, 2009, p. 168). For example, Mirkovic et al. (2008) conducted a simulation of Red and Blue team testing which showed defense systems effectively stopped attacks they were designed to defend against but failed when attacks were more sophisticated. The goal of such testing can be summarized as maximizing damage if one is on the red team, while minimizing damage if one is on the blue team (Yang et al., 2006).

Due to the way security assessments are designed, the Blue and Red teams aim for different, and often contradictory, outcomes during testing, as the success of one is the failure of the other. Those on the defensive side hope the system is resilient to any threats, while those on the offensive side hope to find security loopholes in the system they can exploit (Mirkovic et al., 2008). This has led to hostility and secrecy between the teams, and in turn the level of competition can affect the security capabilities of the organization. This hostility can impact both the credibility of the assessments, as well as increase cybersecurity risk for the organization. Due to the need to better cybersecurity standards, collaboration between the two types of teams is essential, and there is a need to move away from only conducting the traditional kinds of security assessments (Miessler, 2016). Research has shown how dynamic cybersecurity practices are more effective as countermeasures to attacks, and a dynamic technical approach to network defense can negatively impact the adversary's capabilities in information gathering and attacking (Kewley, Fink, Lowry, & Dean, 2001). The need for a more dynamic approach with a more symbiotic relationship between teams led to the concept of a Purple team.

These Purple teams perform and implement principles of both Red and Blue team-based security testing in order to evaluate the security of a company. The Purple team focuses on assessing both attacking and defending which gives them a different perspective into an organization's or system's security (SecureAuth, 2018). When working with Red and Blue teams who work in isolation, Purple teams can take a white-box approach to testing, as they obtain information from both teams. Thus, along with the simulated adversarial model Red teams use as an approach, Purple teams can also conduct penetration tests with an in-depth knowledge of the assets from Blue teams in order to assess security from a different perspective (Peters, 2016). The idea of a team which combines Red and Blue team principles bridges the gap between the offensive and defensive approaches and focuses on a more collaborative testing methodology. It

can also help evaluate and mitigate unique threats such as insiders, which have one of the greatest potentials for negative impact on a business (Symantec, 2018).

In Purple team assessments, the testing is more targeted, as the offensive objective is to evaluate specific security controls while the defensive objective is to test specific preventative measures and skill sets simultaneously (Peters, 2016). Since a variety of tasks conducted by Red teams and Blue teams, such as information gathering and vulnerability research, are similar, combining activities aims to impact and improve efficiency. Purple team assessments are meant to be designed so as to be able to find, document, and explain both exploitable vulnerabilities and defensive strategies (Veerasamy, 2009). Another factor which differentiates this new type of testing from the traditional ones is information sharing. Unlike Red and Blue teams who traditionally do not share information, Purple teams are meant to synthesize all information collected and constantly share experiences about "attacks, alerting and instrumentation, and detection and response procedures" (Peters, 2016, p. 1)

2.4.2 Purple Team Methodology

In simulation testing environments, the testing space is split into one representing distinct adversarial behaviors, which is a function of the Red team, and the other representing distinct defensive and incidence response-based behaviors, which is a function of the Blue team (Yang et al., 2006). In practice, however, these activities often merge and overlap, which highlight the need for merged methodologies (Veerasamy, 2009). Research shows there is a relationship between "the structure of the defender's network, the attack goal and threat mode" (Fultz & Grossklags, 2009, p. 168); assessing them in just an isolated Red team – Blue team manner might not provide us with a complete picture of the cybersecurity capabilities of the entity being tested. By combining certain aspects of testing and collaborating with teams who do the individual secretive testing, it may be possible to make security auditing more efficient and effective. Thus, by assessing steps from existing Red and Blue team methodologies and the optimal balance of secrecy and collaboration, a Purple team methodology could be crafted. The synergetic relationship between the offensive and defensive approaches would be able to provide a more detailed view of an organization's security posture, alongside the traditional assessments, if a well-designed methodology is created and implemented.

2.5 Summary

Due to an increase in the frequency, magnitude, and complexity of cybercrime and cybersecurity threats, there is an increased need for securing individuals and organizations across industry, academia, and government. This can be done by conducting security assessments which simulate the attacker and defender scenario, called Red and Blue teaming, to secure assets before any real threats occur. However, due to their isolated methodologies and contradictory nature, they often compete without sharing information and intel, and can bias an evaluation. A need for a new kind of assessment has led to the idea of a Purple team, which focuses on collaboration and simultaneous offensive and defensive testing. A review of existing literature in the academic community and throughout the industry shows the need for security assessments. It discusses Red and Blue team assessments and their methodologies, their flaws, the concept of a Purple team, and its need in the industry. The next chapter details the research methods related to the current study and how it plans to evaluate Purple teams.

3. FRAMEWORK AND METHODOLOGY

As traditional Red and Blue teams in security auditing have contradictory natures and lack information sharing, the new approach of Purple teams was assessed to provide a complete and true picture of the security infrastructure. The study aimed to answer the following research question: "How do cybersecurity professionals perceive Purple teams?" This research question was assessed by perception scales, needs analyses, and methodology ratings.

3.1 Hypotheses

The current study aimed to investigate the phenomenon of Purple teaming in cybersecurity auditing, and evaluate factors contributing to an optimal Purple team. Due to this study being one of the first academic studies comparing such assessments, it was exploratory in nature (Mirkovic et al., 2008). Based on the research questions proposed by the study, the hypotheses were:

H_1: There is a significant difference in the perceptions of cybersecurity professionals between Purple teams and the traditional Red and Blue team approaches.

H_2: Through needs analyses, there are specific agreed upon factors needed to create an ideal Purple team.

H_3: Cybersecurity professionals can differentiate steps based on relevance to create a high-level methodology for Purple teams based on existing Red and Blue team methodologies.

The study aimed to survey the targeted population in order to test the hypotheses and answer the research questions.

3.2 Operational Definitions

For the purpose of this study, each of the concepts studied were operationalized in order to be able to measure them. They are as follows:

- Cybersecurity professional: Any individual who has worked in a cybersecurity related job at any point in their career (NIST, n.d.; SANS, n.d.).

- Red teams: Information security professionals who use tactics, techniques, and procedures (TTPs) to mimic real-world threats in order to measure the security capabilities of an organization's assets (SANS, n.d.).
- Blue teams: Information security professionals who use knowledge of attacks and the infrastructure to defend an organization's critical assets and systems against attacks and threats from adversaries (SANS, n.d.).
- Purple teams: Information security professionals who bring together and use concepts and principles of red and blue teams simultaneously for security assessments (SANS, n,d,).
- Perception: Measured by responses on usefulness of a purple team, and scales modified from collaboration across teams in national security (Jarvenpaa & Majchrzak, 2008). Aimed to measure the constructs of combinative information sharing, security practices, knowledge dissemination, ownership, and learning across Purple, Red, and Blue teams.
- Needs analysis: Based on the methodology of Rogers and Seigfried (2004), measured by factors Purple teams need to succeed, issues associated with Purple teams, and what management could do to help Purple teams.
- Methodology: Teams conducting security assessments perform specific steps during engagements (such as gathering intel or identifying threats), which form the team's methodology (Veerasamy, 2009).

3.3 Sample

To answer the research questions, cybersecurity professionals who have worked in industry across different security roles were surveyed. Statistics showed, in 2017, the U.S. employed around 780,000 people in cybersecurity positions, with approximately 350,000 unfilled cybersecurity openings (NeSmith, 2018; Morgan, 2017a). However, predictions said there will be around 3.5 million unfilled positions in the industry by 2021 (NeSmith, 2018). The current study was based in the U.S. as it is one of the world's most advanced countries in terms of cybersecurity development and investments (NeSmith, 2018). To qualify for the study, participants had to be current residents in the U.S. and 18 years of age or older. The participants were asked if they had workplace experience in Red and Blue teams, and if they ever worked with Purple teams. Even though the professionals could only be part of one team at a time based

on a job role, they may have moved across different security functions throughout their career. If they had previous experience on both teams, the were included in a different group (both Red and Blue team experience) for part of the analyses.

Since the current study included security professionals working across various industries, it was challenging to locate enough participants for a sample. As the study specifically targeted security professionals, who are a specific and harder to identify and reach population, a snowball sampling strategy was used (Graziano & Raulin, 1993; Kitchenham & Pfleeger, 2002). The information security professionals who saw the survey, as well as those who completed it, were asked to pass it on to other professionals in the field who could complete the survey, and so on until a desired sample size was reached. By the end of data collection, $N = 122$ responses were obtained (before removing any incomplete or missing data).

3.4 Survey Design

For the current study, participants took a quantitative self-report survey (see section 3.5). The participants were first shown a consent form and had to voluntarily accept it to proceed. After which, they answered two questions about their age and current country of residence. These questions were used to validate age and U.S. residency; those who did not qualify were sent to a "thank you" page and were not allowed to proceed. Since the cybersecurity industry and its assessments may change across countries, and minors require parental consent, they were excluded from the survey. Respondents were also asked if they met the definition of a cybersecurity professional, and those who did not were also excluded from the survey. The overall survey flow is shown in Figure 3.1.

For the first major section of the survey after these validations, respondents completed questions about demographics. Information such as education level, experience in industry, employment, age, sex, and others were collected to provide the researcher with descriptive information about the sample. The researcher chose to include demographics as the first section of the survey as collecting them in the beginning increases the accuracy of self-reported subject variables (see Birnbaum, 2000). After answering questions about general demographics, the survey also asked participants for information and experiences about prior security assessments and Red and Blue teaming. By collecting security-related demographic information, the

researcher was able to record and evaluate how various security experiences impacted opinions on security testing and Purple Teaming.

The next three sections intended to answer the primary research question as well as the ancillary questions the study intended to investigate. The second major section of the survey aimed to assess how cybersecurity professionals perceived Purple teams in terms of their function and their relationship with the Red and Blue teams. Participants answered questions to measure their understanding of a Purple team, and their perceptions of the concept. This section also included a modified version of validated subscales developed by Jarvenpaa and Majchrzak (2008) which were initially developed to measure knowledge collaboration among professionals protecting national security. The modified scale was used to measure and compare the constructs of combinative information sharing (six items), security practices (ten items), knowledge dissemination (three items), ownership (three items), and learning (five items) across Purple, Red, and Blue teams. Compared to the original subscales, each item measuring the various constructs were adapted into five-point Likert scales from seven-point Likert scales; it allowed for increased readability on mobile devices and increased the rate of survey completion.

As Jarvenpaa and Majchrzak (2008) did in their study, the Cronbach's alpha scores were calculated to assess and measure internal consistency for the subscales, which helps establish reliability. The subscales of combinative information sharing ($\alpha = .82$), security practices ($\alpha = .86$), ownership ($\alpha = .90$), and learning ($\alpha = .86$) were found to be internally consistent. Kline (1999) stated a reliable scale has an $\alpha > .70$, which shows the knowledge dissemination ($\alpha = .46$) subscale is not reliable. However, analysis showed removing one of the items contributing to knowledge dissemination increased internal reliability ($\alpha = .57$). This item was not included in the aggregated knowledge dissemination score in any further analyses. For the purposes of this study, findings related to dissemination should be interpreted with caution.

The third major section collected responses to perform a textual frequency-based needs analysis to evaluate what is needed to create an ideal Purple team and maximize the effectiveness of a Purple team assessment. This section followed the validated methodology of Rogers and Seigfried (2004). The participants were asked three free-form answer questions, which asked them to list up to three responses on what they considered important factors Purple teams needed to succeed, the main issues associated with Purple teams, as well as things management can do to support Purple teams and help them succeed.

Once responses were collected, they were put into categories for frequency analysis. Just as with Rogers and Seigfried (2004), if multiple answers from the same participant fit into the same category, they were combined and scored as a single item within that group. To evaluate each of the three free-form question (success factors, issues, managerial support), two researchers independently classified each unique response into one of the categories to ensure inter-rater reliability; any differences in classification were compared, if one category could not be agreed upon, the response was classified as "other." To establish reliability between the researchers' categorizations, inter-rater reliability was assessed to determine consistency among the responses rated (Landis & Koch, 1977). Based on the method created by Landis and Koch (1977), the categorization of responses into six categories for success factors (kappa = .98, $p <$ .001), four categories for issues (kappa = .95, $p < .001$), and six categories for managerial support (kappa = .98, $p < .001$), all showed almost perfect agreement between the two raters.

The fourth and last major section intended to create a high-level methodology, based on participants responses, for Purple Teams from existing Red and Blue team methodologies. Participants were asked to rate steps on a scale from least to most relevant based on the methodologies created by NIST (Scarfone et al., 2008) and Veerasamy (2009); the purpose was to assess if the industry agreed upon steps in a potential Purple team methodology (adapted from Red and Blue teams). They were asked to think about collaboration factors and ownership of tasks so as to think about how to best distribute responsibilities. After completing this section, the survey concluded, and respondents were directed to a thank you page.

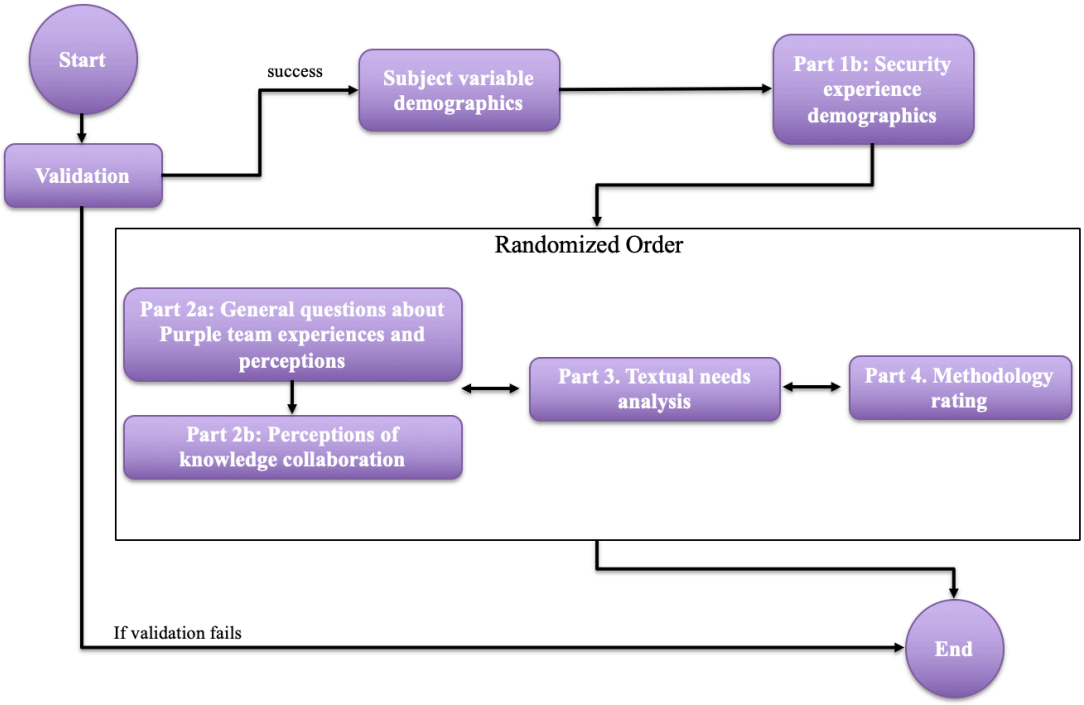


Figure 3.1 Survey flow

3.5 Procedure

When the survey was finalized, it was first piloted by sending it out to some of the intended target population known to the researcher through social media. The results from the pilot test were used to assess the phrasing of the questions, the flow, and the overall survey. After collecting the desired amount of results from the pilot study, the data was analyzed for its construct and content validity. The author conducted statistical analyses to assess if the scale items were measuring their corresponding construct based on the analytical strategies chosen (see section 3.6). Once the survey was adjusted and updated based on the analyses, the updated survey and related documents were sent to the Institutional Review Board (IRB) for approval.

Once approval was received, the anonymous survey was sent out to cybersecurity professionals via Twitter, LinkedIn, and other forms of social media. The self-report survey was conducted via Qualtrics. When collecting data through Qualtrics, all responses were anonymized and assigned random IDs so as to not collect any personally identifying information. Before participants could start the survey, they had to sign a consent form which provided information about confidentiality, anonymity, and detailed information about the survey and its purposes; only those who voluntarily signed the form were shown the survey. Also, only participants who

were both over 18 years of age and currently residing in the US were allowed to proceed with the survey. The data collection phase lasted until an appropriate sample size was reached. After the data was collected, it was cleaned and analyzed using statistical software (see section 3.6).

3.6 Analytical Strategies

All the data collection from the study was analyzed using quantitative methods due to the survey design and the chosen delimitations. Data collected from the survey was downloaded from Qualtrics and put into IBM® SPSS statistics software for analyses. The data was then cleaned by removing missing and incomplete data, as well as tested for outliers. After the data was cleaned, the author began hypothesis testing by conducting quantitative statistical tests (as long as their underlying statistical assumptions were met). Before the hypotheses were tested, descriptive statistics were performed on the sample demographics. Along with general demographics, descriptives were also calculated for security related demographics and prior cybersecurity experience questions.

The second section of the survey was assessed to evaluate the primary hypothesis. After assessing subscale reliability, zero-order bivariate correlational analyses were run between the demographics and the information security knowledge collaboration subscales; the significance level was set at $\alpha = .05$. Based on the correlations, the author evaluated if there was a relationship between demographics and how professionals perceived Purple teams. Between nominal security related demographics and the nominal Purple team perception variables, Chi-Square type analyses were conducted. By comparing frequency distributions based on observed and expected values, the relationship between the variables were investigated to see how demographics impacted the perception of Purple teams. These analyses showed if prior experiences had an impact on how cybersecurity professionals perceived Purple teams in relation to Red teams and Blue teams and how they were compared.

In order to test the first ancillary hypothesis, the textual answers from each of the three questions on section three of the survey were put into categories; two authors independently classified and compared items. In order to conduct the needs analyses, a frequency distribution was conducted so as to determine the most relevant and commonly shared needs agreed upon by cybersecurity professionals (see Rogers & Seigfried, 2004). Data was used from section four of the survey to identify the critical components of the methodologies from Red and Blue teams

essential to Purple assessments, which helped evaluate the second ancillary hypothesis. The most relevant methodological steps were determined based on average score provided to each item across the entire sample calculated through descriptives. These were set in chronological order based on the descriptive aggregates and were used alongside the existing NIST (Scarfone et al., 2008) and Veerasamy (2009) methodologies to build a high-level proof-of-concept for Purple teaming methodologies.

3.7 Summary

This chapter highlighted the hypotheses derived based on the research questions the study aimed to answer and the existing scientific body of literature in academia and industry. In order to collect data, a snowball sampling method was used to send out a Qualtrics survey to cybersecurity professionals via social media such as Twitter and LinkedIn. The survey included demographics, previous work experience with Red, Blue, and Purple teams, and questions about Purple team perceptions, after participants finished the validation questions. It also included a scale modified from Jarvenpaa and Majchrzak (2008) to measure perceptions of collaboration across the different teams. There were three open-answer questions for needs analysis, and rank type questions to measure importance of existing Red and Blue methodology steps. The survey took respondents around 15 minutes to complete. After the survey responses were collected, quantitative analyses were conducted based on the proposed analysis strategies described.

4. ANALYSES AND RESULTS

After the data collection period, the dataset was imported from Qualtrics. For the statistical analysis, the author used IBM® SPSS (Statistical Product and Service Solutions v.25). To assess the collected sample, descriptive analytics were conducted on the demographic variables collected via the self-reported survey. Descriptives were calculated and reported on participant responses regarding general demographics such as education level, experience in industry, employment, age, gender, and others, as well as information and experiences about prior security assessments (Red, Blue, and Purple teaming). Hypothesis testing was then conducted to evaluate the research question of the study regarding perceptions of Purple teams among cybersecurity professionals. Since the research question was assessed based on three hypotheses, each hypothesis was then evaluated based on the data. Prior to analysis, statistical significance was set at the alpha level of .05. Due to the study's exploratory nature, all correlations significant at and below $p = .10$ were also considered.

4.1 Descriptives

Before analyzing the data collected from the survey, responses were examined in SPSS to eliminate invalid responses. Of the 122 responses received, 5 participants did not consent to moving forward with the survey, 36 either declined to respond or were not currently residing in the US, and 5 did not meet the minimum age requirement of 18. These responses were considered invalid since they failed to meet the validation checks and were removed. Since this survey was targeted towards cybersecurity professionals, the 18 participants who self-reported not meeting the definition of cybersecurity professional or declined to answer were removed. After removing invalid responses, 7 more responses were removed for missing data, leaving 53 respondents who had valid responses for analysis.

Of the valid sample ($N = 53$), as shown in Table 4.1, the age of the participants reached from snowball sampling ranged from 21 to 69 ($M = 32.18$, $SD = 10.40$), of which, the majority self-identified as males ($n = 40$, 75.5%), followed by females ($n = 11$, 20.8%). Most participants worked in either the tech industry ($n = 22$, 41.5%) or professional services/consulting ($n = 11$, 20.8%), with majority having full-time jobs ($n = 40$, 75.5%). A majority of the population had

completed at least a bachelor's degree (n = 21, 39.6%); 13 (24.5%) individuals had a master's degree and two (3.8%) had a PhD, among which 14 (93.3%) of those degrees were in a cybersecurity-related field.

Table 4.1 Sample demographics

Variable		Frequency (N = 53)	Percentage
Age (in years)	21-25	18	34.0%
	26-30	10	18.8%
	31-35	7	13.2%
	36-40	11	20.8%
	40+	7	13.2%
Gender	Male	40	75.5%
	Female	11	20.8%
	Non-binary	1	1.9%
	Other	1	1.9%
Education	Some high school, no diploma	1	1.9%
	High school graduate, diploma, or equivalent	4	7.5%
	Some college credit, no degree	10	18.9%
	Associate's degree	2	3.8%
	Bachelor's degree	21	39.6%
	Master's degree	13	24.5%
	PhD or Doctorate	2	2.9%
Employment status	Employed full-time	40	75.5%
	Student	9	17.0%
	Unemployed looking for work	2	3.8%
	Employed part-time	1	1.9%
	Retired	1	1.9%
Work sector	Industry (Tech)	22	41.5%
	Professional Services/ Consulting	11	20.8%
	Industry (Non-Tech)	8	15.1%
	Academia	6	11.3%
	Government	2	3.8%
	Other	2	2.8%
	Prefer not to say	1	1.9%
	Unemployed	1	1.9%

The participants also answered demographic questions related to previous cybersecurity experience. As shown in Table 4.2, participants had between one to 35 years of experience across the sample (M = 7.38, SD = 7.63), with the highest frequency group having 5 years of experience (n = 11, 20.8%). Of the sample, 25 (49.1%) had previously worked on a Red team and/or in an offensive security role, while 45 (84.9%) had previously worked on a Blue team of a

defensive security role; of the total, 21 (39.6%) had worked on both teams, while 21 (39.6%) had managed or been in charge of a cybersecurity team. As for Purple teams, most of the sample had previously heard of the concept (n = 42, 79.2%), but only some (n = 17, 32.1%) had previously been part of a Purple team assessment. Overall, 15 (28.3%) had previously worked at or with an organization that had a Purple team.

Table 4.2 Cybersecurity-related demographics

Variable		Frequency (N = 53)	Percentage
Cybersecurity experience (in years)	1-5	33	62.3%
	6-10	9	16.9%
	11-15	5	9.5%
	15-20	2	3.8%
	21+	4	7.5%
Previous Red team/ offensive security experience	Yes	26	49.1%
	No	25	47.2%
	Unsure	1	1.9%
	Decline to respond	1	1.9%
Previous Blue team/ defensive security experience	Yes	45	84.9%
	No	7	13.2%
	Unsure	1	1.9%
Managed cybersecurity team	No	30	56.6%
	Yes	21	39.6%
	Maybe	2	3.8%
Heard of Purple teams	Yes	42	79.2%
	No	10	18.9%
	Unsure	1	1.9%
Been part of Purple team assessment	No	35	66.0%
	Yes	17	32.1%
	Unsure	1	1.9%
Worked at/ with organization having Purple team	No	35	66.0%
	Yes	15	28.3%
	Unsure	3	5.7%

4.2 Hypothesis Testing

H_1: There is a significant difference in the perceptions of cybersecurity professionals between Purple teams and the traditional Red and Blue team approaches.

Descriptive statistics were calculated for participant responses on if Purple teams were beneficial, how Purple teams should be created, and if they should share information with Red and Blue teams. As shown in table 4.3, of the total number of participants ($N = 53$), the majority claimed Purple teams are beneficial ($n = 17$, 32.1%), or they are beneficial but only when used alongside Red and Blue teams ($n = 17$, 32.1%). Over half of the sample ($n = 31$, 58.5%) agreed if Purple teams are created, they should be made from some existing Red team professionals and some existing Blue team professionals already in the organization. Similarly, over three quarters of the sample ($n = 40$, 75.5%) agreed Purple teams should collaborate with both Red and Blue teams within an organization when conducting security assessments.

Table 4.3 Respondents' Opinions of Purple teams

Question		Frequency ($N = 53$)	Percentage
Do you think Purple teams are beneficial?	Yes, it is beneficial	17	32.1%
	Yes, when working alongside existing Red and Blue teams	17	32.1%
	Yes, but only for specific testing cases	9	17.0%
	No, it is repetitive	7	13.2%
	Unsure	2	3.8%
	I don't know	1	1.9%
If we were going to create a Purple team, how would they be created?	From some existing Red team professionals, and some existing Blue team professionals	31	58.5%
	From some new Red team professionals, and some new Blue team professionals	7	13.2%
	From a random combination of professionals regardless of previous experience	5	9.4%
	From only individuals that have both Red and Blue team skills	4	7.5%
	Unsure	3	5.7%
	I don't know	3	5.7%
Should Purple teams share information with Red and Blue teams	Yes, they should collaborate with both teams	40	75.5%
	Unsure	4	7.5%
	I don't know	3	5.7%
	Yes, but with Red team only	3	5.7%
	Yes, but with Blue team only	2	3.8%
	No, they should work independently	1	1.9%

Cross-tabs were calculated to assess if prior security experiences with Red and Blue teams, as well as Purple teams impacted perceptions of Purple teams. The cross-tabs and analytical statistics such as Chi-Square tests assessed if the categorical variables in Table 4.3 had a significant difference between the levels of categorical variables in Table 4.2 (such as previous Red and Blue team experience as well as awareness and prior experience with Purple teams). Before any hypothesis testing were conducted, all responses for variables which had "Unsure", "Maybe", or "Decline to respond" in Table 4.2, and "Unsure" or "I don't know" in Table 4.3 were set as missing. The primary assumption of a chi-square analysis of independence was met as each person in the data set contributed to only one cell of the contingency table, the levels of the variables were mutually exclusive, and the data in the cells were all frequencies. For standard Chi-Square analyses using the Pearson Chi-Square value, expected frequencies in each cell should be greater than 5; this assumption was not met for any of the comparisons, thus, Fisher's exact test was conducted on the data as it deals with Chi-Square comparisons for datasets with small sample sizes and low cell counts.

Between the variables of "prior Red team experience" and "benefit of Purple teams" (N = 48), 4 cells (50.0%) had expected counts less than 5, and the minimum expected count was 2.29; thus, a Fisher's exact test was conducted. Results showed a significant association between the two variables, Fishers = 11.95 at p = .006. As shown in Table 4.4, among participants who stated, "Purple teams were only beneficial for specific test cases", those without prior Red team experience were counted lower than the expected count, while those with prior experience were counted higher than expected count. Of those who believed "Purple teams were repetitive and not beneficial", those without prior Red team experience were counted lower than expected count, while those with prior experience were counted higher than expected count. Results indicated those with prior Red team experience were more likely to believe Purple teams were either beneficial only for specific test cases or were not beneficial because they were repetitive; those without prior Red team experience were more likely to believe the opposite in those cases. There was no significant difference between prior Red team experience, and both "Purple teams being beneficial" as well as "Purple teams only being beneficial when working with Red and Blue teams". For the overall data, Cramer's V was .50, which indicated a large effect size.

Between the variables of Purple teams sharing information with Red and Blue teams and prior Blue team experience (N = 46), 6 cells (75.0%) had expected counts less than 5, and the

minimum expected count was .13; thus, a Fisher's exact test was conducted. Results showed a marginally significant association between the two variables, Fishers = 6.43 with $p = .110$. While the relationship was not significant at a .05 level, it is possible the relationship may be significant with a larger sample size; it can be considered marginally significant. Of those who believed "Purple teams should work independently," those who did not have prior Blue team experience were counted lower than expected count. The results showed individuals who do not have prior Blue team experience are more likely to think "Purple teams should work independently without sharing information with Red and Blue teams." There was no significant difference between those with previous Blue team experience, and whether individuals believed Purple teams should share information with just Red teams, just Blue teams, or both teams. For the data, Cramer's *V* was .43, which indicated a large effect size.

There were no significant associations (based on Fisher's exact test) between the variables of "Purple teams being beneficial" and all of the following: prior Blue team experience, previous experience on a Purple team, or having worked at/with an organization having a Purple team. There were also no significant associations between the variables of "how should a Purple team be created" and previous Red, Blue, or Purple team experiences. No significant associations were found between "Purple teams sharing information with Red and Blue teams" and previous Red team or Purple team experience.

Table 4.4 Cross-tabulations for prior Red team experience and benefit of Purple teams

			Previous Red team experience		
			No	Yes	Total
Benefit of Purple teams	Yes, it is beneficial	Actual count	11.0	6.0	17.0
		Expected count	7.8	9.2	
	Yes, when working alongside Red and Blue teams	Actual count	10.0	7.0	17.0
		Expected count	7.8	9.2	
	Yes, but only for specific testing cases	Actual count	1.0	8.0	9.0
		Expected count	4.1	4.9	
	No, it is repetitive	Actual count	0.0	5.0	5.0
		Expected count	2.3	2.7	
	Total		22.0	26.0	48.0

A two-tailed zero-order correlation was conducted to assess if a relationship exists between demographic variables such as age, years of experience in cybersecurity, previous Red and Blue team experience, and the subscales of combinative information sharing, security

practices, knowledge dissemination, ownership, and learning (see Table 4.5). Due to the study's exploratory nature, all correlations significant at and below $p = .10$ were considered. There was a medium, statistically significant relationship between number of years of cybersecurity experience and knowledge ownership, $r(53) = .29$, $p = .038$, $r^2 = .08$. The ownership construct was also moderately correlated to age in years at $r(53) = .23$ ($p = .10$, $r^2 = .05$). The pairwise positive correlations indicated individuals who have more years of cybersecurity experience and are older are more likely to score high on ownership. The finding suggests those who have been in the cybersecurity field longer and are older are more likely to think Purple teams will face ownership issues compared to Red and Blue teams (related to owning solutions, discoveries, knowledge, and inventions).

Among the demographics, gender was related to both knowledge dissemination and ownership. There was a medium, significant relationship between gender and knowledge dissemination at $r_{pb}(51) = -.34$ ($p = .01$, $r^2 = .12$), as well as a marginally significant correlation between gender and ownership at $r_{pb}(51) = -.24$ ($p = .10$, $r^2 = .06$). Both of these pairwise negative correlations suggest those who identify as women are more likely to score low on dissemination and ownership. It indicated those identifying as men are more likely to think Purple teams will have issues with the dissemination of information and owning solutions, discoveries, etc. compared to Red and Blue teams.

There was also a statistically significant, medium, negative relationship between number of years of cybersecurity experience and learning, $r(53) = -.38$, $p = .006$, $r^2 = .14$; there was also a significant medium negative relationship between prior Red team experience and learning, $r_{pb}(51) = -.31$, $p = .028$, $r^2 = .10$. The result indicated those who have previously been on Red teams and those who have more years of cybersecurity experience are more likely to score lower on learning. The finding suggests those who have been in the cybersecurity field longer and who have previously worked on Red teams are more likely to think that Purple teams will be less likely to have learning experiences (such as about new technology, threats, and problems) than Red and Blue teams. Overall, the hypothesis was partially supported in that cybersecurity professionals perceived Purple teams differently compared to Red and Blue teams only on certain criteria and only if they belonged to certain demographics.

Table 4.5 Zero-order correlations between demographics and modified perception subscales

		Information security knowledge collaboration scale				
		info_sharing	sec_practices	dissemination	ownership	learning
Demographics	Gender	-.02	.15	-.34**	-.24*	.14
	Age in years	-.01	.03	.13	.23*	-.22
	Years of cybersecurity experience	-.07	-.10	.02	.29**	-.38***
	Prior Red team experience	-.03	-.19	-.17	.04	-.31**
	Prior Blue team experience	.05	-.01	.10	.14	.10

* $p < .10$ (two-tailed); ** $p < .05$ (two-tailed); *** $p < .01$ (two-tailed)

Note. Correlations are pairwise. $N = 51$ for gender; $N = 53$ for age in years and years of cybersecurity experience; $N = 51$ for prior Red team experience; $N = 52$ for prior Blue team experience

info_sharing = collaborative information sharing; sec_practices = security practices; dissemination = knowledge dissemination

H_2: Through needs analyses, there are specific agreed upon factors needed to create an ideal Purple team.

Participants were asked to enter up to three factors for Purple teams to succeed. Of the total sample, 28 individuals entered at least one success factor. The responses were grouped into six high-order categories, namely, collaboration, employee skillsets, innovation, management assistance, project clarity, and other. To evaluate factors needed for Purple teams to succeed, each response from the 28 individuals were separated to get a total of 70 text-based responses for success factors. Table 4.6 shows the frequency distributions of each of the categories; "managerial support" ($n = 18$, 25.7%) was the most reported, while "innovative approaches" ($n = 7$, 10%) was the least reported, when not factoring in the "other" category.

Table 4.6 Frequency analysis of success factor categories

Category	Frequency*	Percentage
Managerial support	18	25.7%
Employee skillsets	16	22.9%
Project clarity	15	21.4%
Cross-team collaboration	13	18.6%
Innovative approaches	7	10.0%
Other	1	1.4%

**Note.* The 70 responses were collected from 28 professionals as each respondent was allowed up to 3 responses

Participants were also asked to enter up to three issues Purple teams might face. Of the total sample, 29 individuals entered at least one issue. The responses were grouped into four high-order categories, namely, assessment design and prioritization, management and resource constraints, workforce and inter-team constraints, and other. Each response from the 29 individuals were separated to get a total of 61 text-based responses for issues. Table 4.7 shows the frequency distributions of each of the categories; "management and resource constraints" (n = 21, 34.4%) was the most reported, while "assessment design and prioritization" (n = 19, 31.1%) as well as "workforce and inter-team constraints" (n = 19, 31.1%) were least reported, when not factoring in the "other" category.

Table 4.7 Frequency analysis of issue categories

Category	Frequency*	Percentage
Management and resource constraints	21	34.4%
Assessment design and prioritization	19	31.1%
Workforce and inter-team constraints	19	31.1%
Other	2	3.3%

**Note.* The 61 responses were collected from 29 professionals as each respondent was allowed up to 3 responses

Lastly, respondents also entered up to three things management can do to help Purple teams succeed. Of the total sample, 30 individuals entered at least one step (up to three) management can take. The responses from this question were grouped into six high-order categories, namely, active personnel management, collect and provide performance metrics, provide clear definitions, provide resources, provide training and development, and other. Each response from the 30 individuals were separated to get a total of 62 text-based responses for managerial support factors. Table 4.8 shows the frequency distributions of each of the categories; "provide clear definitions" (n = 19, 30.6%) was the most reported, while "collect and provide performance metrics" (n = 7, 11.3%) and "provide training and development" (n = 7, 11.3%) were the least reported, when not factoring in the "other" category.

Table 4.8 Frequency analysis of managerial support categories

Category	Frequency*	Percentage
Provide clear definitions	19	30.6%
Active personnel management	16	25.8%
Provide resources	12	19.4%
Collect and provide performance metrics	7	11.3%
Provide training and development	7	11.3%
Other	1	1.6%

**Note.* The 62 responses were collected from 30 professionals as each respondent was allowed up to 3 responses

H_3: Cybersecurity professionals can differentiate steps based on relevance to create a high-level methodology (steps performed during engagements) for Purple teams based on existing Red and Blue team methodologies.

Reponses were collected from participants ($N = 41$) who ranked methodology steps (taken from Red and Blue teaming) from 0 to 10 based on how relevant they believed it was to Purple teaming. Descriptive analyses were performed on the ratings of participants on 12 methodology steps based on NIST (Scarfone et al., 2008) and Veerasamy (2009). As shown in Table 4.9, aggregate statistics show information gathering ($M = 8.10$, $SD = 2.31$) and providing recommendations ($M = 8.56$, $SD = 1.76$) were rated the highest in relevance among the various steps. These were followed by vulnerability investigation ($M = 7.71$, $SD = 2.03$), threat identification ($M = 7.54$, $SD = 2.19$), and evaluation ($M = 7.10$, $SD = 1.97$) in descending order. Among the steps, penetration testing ($M = 6.88$, $SD = 2.36$), asset identification ($M = 6.49$, $SD = 1.80$), safeguarding creations ($M = 6.34$, $SD = 2.69$), and footprinting ($M = 6.00$, $SD = 2.52$) were classified lower; OS detection ($M = 5.66$, $SD = 2.58$) and service detection ($M = 5.46$, $SD = 2.60$) were considered the least relevant steps to Purple teams. In order to create the suggest methodology, all steps over $M = 7.00$ will be included; this is done so as to maximize relevance to Purple teams and simultaneously increase approval (as the professionals are the ones who ranked the steps). Overall, the hypothesis was supported as the sample assigned different relevance values to the each of the steps; these values could be used as a cutoff to create a methodology the professionals may agree with.

Table 4.9 Descriptive statistics on methodology steps

Methodology step	Minimum	Maximum	*M*	*SD*
Provide recommendations	4.00	10.00	8.56	1.76
Information gathering	2.00	10.00	8.10	2.31
Vulnerability investigation	2.00	10.00	7.71	2.03
Threat identification	2.00	10.00	7.54	2.19
Evalution	1.00	10.00	7.10	1.97
Penetration testing	0.00	10.00	6.88	2.36
Asset identification	3.00	10.00	6.49	1.80
Network and port scanning	1.00	10.00	6.34	2.59
Safeguard creations	1.00	10.00	6.34	2.69
Footprinting	1.00	10.00	6.00	2.52
OS detection	1.00	10.00	5.46	2.60
Service detection	0.00	10.00	5.66	2.58

Note. $N = 41$ for all methodology steps

Participants rated all methodology items on a scale of 0 to 10 (based on relevance to Purple team with 0 being least relevant and 10 being most relevant)

5. DISCUSSION

The research objective of the current study was to assess how cybersecurity professionals perceived Purple teams, specifically, in comparison to Red and Blue teams and its functions and role in cybersecurity assessments. The survey conducted assessed self-reported responses of cybersecurity professionals and statistical analyses were used to determine their perceptions. Overall, participants believed Purple teams had benefit (64.2%), but it may vary across professionals in specific organization. The finding shows professionals currently working in industry agree with previously conducted research (SecureAuth, 2018; Miessler, 2016; Yang, Abbass, & Sarker, 2006) in that a new approach is needed to assessments, and Purple teams provide added value to the current assessment designs.

In case an organization does want to create a Purple team, professionals agreed (58.5%) they should be created from existing Red and Blue team professionals already in the organization. This would possibly allow for better budget management, as management may not need to hire additional employees until the team is mature and established. It will also assist in training and development as these employees would already have prior knowledge of the overall organization. Using this strategy to build a Purple team would help collaborative efforts as the members would have previously worked together; professionals agreed (75.5%) Purple teams should collaborate with both Red and Blue teams within an organization when conducting security assessments. However, this may only be possible in companies with a mature cybersecurity program and a high number of cybersecurity professionals; this is because the Red and Blue teams would have to be efficient and impactful with fewer members. Based on these findings, organizations should only attempt to form a Purple team if they already have a large, established, and mature cybersecurity infrastructure.

Previous research in academia and industry has assessed Purple teams (see Carayon & Kraemer, 2004; Fultz & Grossklags, 2009; Leggio, 2017; Mirkovic et al., 2008) but not how the community of professionals perceive the Purple team concept. The relationship found in the current study between having prior Red team experience and the perceived benefits of Purple teams indicated those with prior Red team experience were more likely to believe Purple teams were either beneficial only for specific test cases or were not beneficial because they were

repetitive; those without prior Red team experience were more likely to believe the opposite in those cases. Similar findings were also observed through the correlational analyses conducted on demographics and the constructs of combinative information sharing, security practices, knowledge dissemination, ownership, and learning (see Jarvenpaa & Majchrzak, 2008). Among cybersecurity professionals, those who have previously worked on Red teams are more likely to think Purple teams will be less likely to have learning experiences (such as about new technology, threats, and problems) than Red and Blue teams.

Those on the Red team have more successes than failures as they only need to find one loophole or vulnerability (Johnson, 2016; Miessler, 2016; Mirkovic et al., 2008), which may be a factor in why Red teams are more likely to not see Purple teams are beneficial. As they do not see the benefit in Purple teams, they may also perceive them as unnecessary. If one has not had previous Red team experience, it is likely they may have been on a blue team or had a manager role, so they may have seen the "gap" with traditional assessments or had issues with past experiences. It may explain why they may want change and perceive Purple teams are being more beneficial. If managers and organizations plan to create Purple teams, it would be critical to get those on the Red team on board as job satisfaction and commitment are linked to perceived value (Boardman & Sundquist, 2009).

Just as with Red teams, organizations would have to develop a strategy to get those with more experience on board. While individuals with more experience do not have any significant differences in opinion on the benefit of Purple teams, they do perceive them negatively. This is because those who have been in the cybersecurity field longer are more likely to think Purple teams will have less learning experiences than Red and Blue teams; this may be due to those individuals with experience believing the current methods are sufficient. Those with experience are also more likely to think Purple teams will face ownership issues compared to Red and Blue teams (e.g., owning solutions, discoveries, and inventions). The newer generation of cybersecurity professionals are more open to new experiences and change, and thus, may support the adoption of newer methods across the industry (Miessler, 2016; Tesch & Cameron, 1987). Managers and organizations can, however, use the input of those with experience to mitigate risk of ownership issues. Since those who have been in the cybersecurity industry longer know the trends and patterns of cybersecurity assessments (Diogenes & Ozkaya, 2018), their knowledge may be of value when making Purple teams work successfully.

Individuals who do not have prior Blue team experience are more likely to think Purple teams should work independently without sharing information with Red and Blue teams. The result can also be explained by the previous research based on the Blue team often "losing", considering the success of the Red team means the failure of the Blue team (Johnson, 2016; Mirkovic et al., 2008). Those without Blue team experience may not have experienced the same issues, and even if they think Purple teams are beneficial, may believe Purple teams should work independently. As Purple teams are meant to emphasize collaborations, organizations evaluating Purple teams maybe have to evaluate and optimize the balance between collaboration and secrecy through repeated security assessments. Since Red and Blue team assessments need to have an aspect of secrecy during testing (Scarfone et al., 2008), teams could share all background information with Purple teams, and continue testing individually as per the traditional format (Fultz & Grossklags, 2009). The author believes Purple teams would be able to provide a more comprehensive test using information from both teams as well as test different facets of an organization's security than Red and Blue teams while working together.

In the "needs analysis" conducted by the author, results indicated professionals believed the top factor required for a Purple team to succeed was managerial support (25.7%). It was followed by employee skillsets (22.9%), project clarity (21.4%), cross-team collaboration (18.6%); innovative approaches (10.0%) was the least reported topic. Boynton and Zmud (1984) found managerial support in terms of strategic and operational guidelines increase chance of optimal project completions and contribute to overall success. The finding goes hand-in-hand with the findings of the current study, as professionals appear to agree support from management is the primary factor in the success of Purple teams. Since Purple teams are a newer concept (SecureAuth, 2018), alongside management support, employee skillsets to match the role and project clarity for assessments will both play an important role. Results from the current study have indicated experienced professionals believe Purple teams may have potential ownership issues, and the newer dynamic approach will require well outlined clear guidelines (Kewley et al., 2001). In order to make Purple team assessments have value, the team members would need to have the correct skillset but also have clearly defined "swim lanes" so as to work well alongside Red and Blue teams with the optimal amount of overlap.

A needs analysis was also conducted to assess what professionals identified at the main issues a Purple team might face. Of the different categories, "management and resource

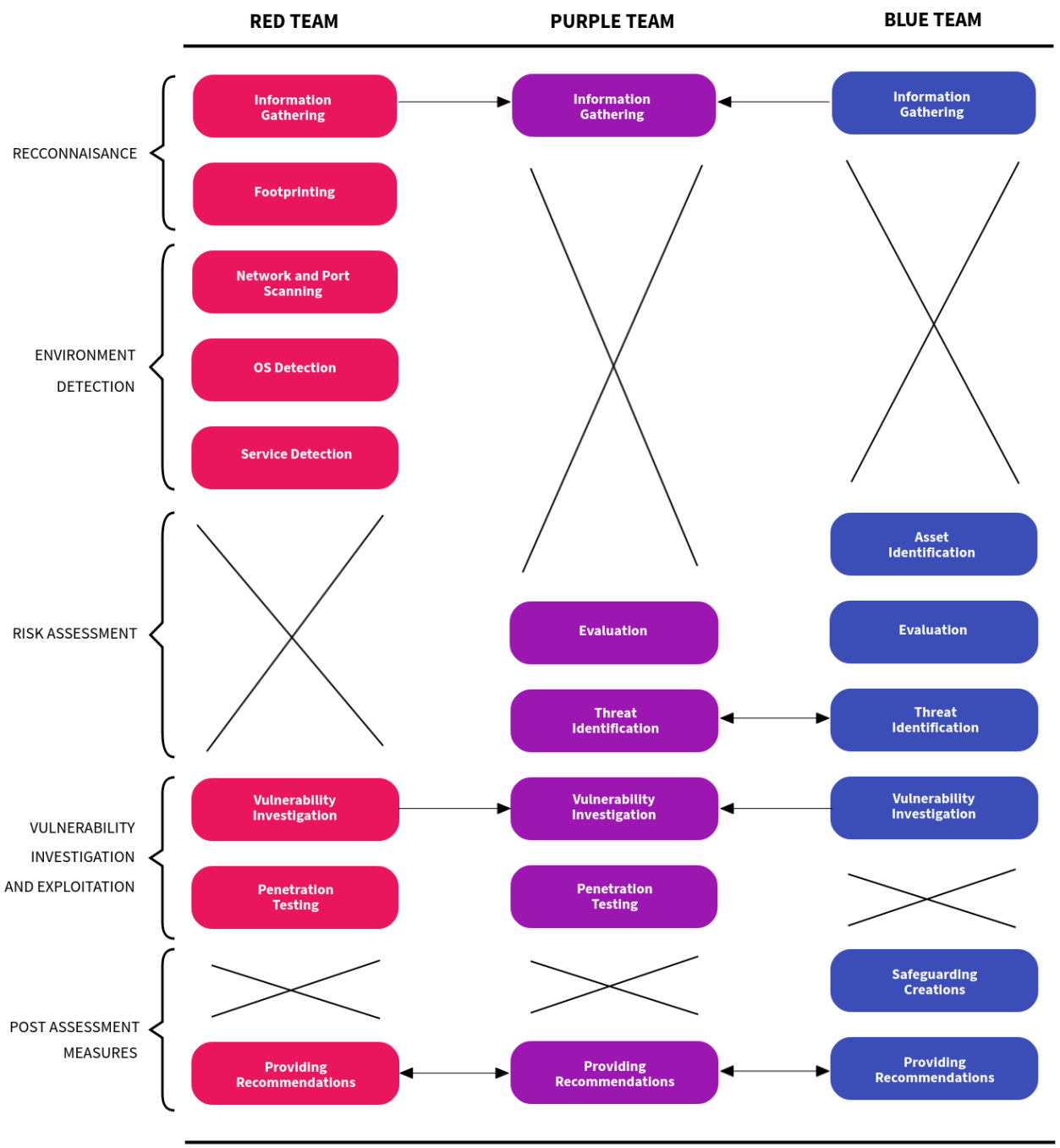
constraints" (34.4%) was the most reported, while assessment design and prioritization (31.1%) as well as workforce and inter-team constraints (31.1%) were ranked after it. These findings are similar to major project issues identified by a MIT study which found project goals, team compositions, management, technical knowledge, and infrastructure were the factors which proved to be the biggest issues if not handled correctly (Ewusi-Mensah, 1997). Without management oversight, resources required to succeed, and control of project scope, Purple teams may not be able to accomplish the goals they are made to fulfill. The author believes organizations will need to address these issues among the cybersecurity teams and existing infrastructure in order to optimize the relationship between the different security assessment teams. Carvalho (2008) suggested along with the factors previously discussed, which tend to be issues in project success, group communication and inter-team collaboration would also be a factor that makes or break a project.

Both success factors and issues indicated cybersecurity professionals agreed management played a tremendous role in making Purple teams work efficiently and provide value in security assessments. For the success of any major project, a strong management presence within projects is essential as it helps manage scope, project expectations, employees, resources, and all major supervisory factors (Munns & Bjeirmi, 1996). The needs analysis conducted on managerial support helps narrow down the role of management into specific identifiable and measurable categories. Results showed providing clear definitions (30.6%) was the most reported, followed by active personnel management (25.8%) and providing resources (19.4%). Among the categories, collecting and providing performance metrics (11.3%), and providing training and development (11.3%) were the least reported.

Organizations would have to ensure Purple teams and the Red and Blue teams working alongside them have access to the managerial support factors identified in the current study. Several variations of these factors have also previously been identified for the success of teams and projects (Sumner, 1999; Ewusi-Mensah, 1997; Porter & Parker, 1993). This shows the managerial support factors are consistent across industries, and they just need to be adapted to fit cybersecurity assessments. If managers are able to actively listen, define scope and ownership, manage and hire the right personnel, and provide resources and metrics needed, Purple teams can be highly effective.

Since the activities conducted during cybersecurity assessments can merge and overlap (Veerasamy, 2009), professionals rated methodology steps based on relevance to Purple teams. By combining these aspects of testing and including aspects of controlled information sharing and collaboration, it may be possible to make security auditing more efficient and effective. Figure 5.1 represents a high-level methodology suggested for Purple teams. The model created by the author represents what professionals in industry consider the most relevant methodology for Purple teams when working alongside Red and Blue teams.

In the proposed model, the steps are not equivalent to either other steps taken by the same team or across other teams. For example, when working for a Blue Team, safeguarding creations and organizational assets is the primary role of an individual, and takes more resources and time than most of their other responsibilities (Scarfone et al., 2008). Similarly, while Red teams spend a majority of the assessment on penetration testing (Scarfone et al., 2008), Purple teams may not spend as many resources (due to having information from Blue teams) and have a different scope than them. The outlined methodology not only creates optimal collaboration conditions between the teams but is also likely to be accepted by professionals already in Red and Blue teams. Having a methodology with relevant steps professionals agree upon, on average, it is likely to increase acceptance, which would impact perceived value and job satisfaction positively (Boardman & Sundquist, 2009).



Note. Arrow keys indicate direction of collaboration (if any). Two-sided arrows show teams working together, while one sided arr
show one team helping the other with a step. Crosses indicate steps in the assessment that team will not be involved in.
The steps in the methodology above are not equally weighted. Each team may perform steps in different capacities and complexities than the other teams. Even among the same team, the different steps are not equivalent.

Figure 5.1 Updated Veerasamy (2009) methodology to include Purple teams and inter-team collaboration

5.1 Limitations

The survey in the current study was distributed to residents of the U.S., and thus cannot be generalized to professionals across the world. The current study surveyed cybersecurity professionals using snowball sampling through social media channels such as LinkedIn and Twitter. Due to the nature of snowball sampling, survey takers were mostly those individuals who accessed the survey through others' shares. Using this method may limit who takes the survey and impact external validity, as is may be possible the sample is not a completely accurate representation of the population. The issue of overall generalizability is also impacted by the limited sample size of the current study. From the data collection phase, the author had results from 53 respondents for analysis after data cleaning (varied between hypothesis testing analyses). It is possible, with an increase sample size, not only will external validity be increased, but it may also impact the strength of relationships found.

The study analyzed perceptions of cybersecurity professionals about Purple team assessments and their usefulness when testing an organizations cybersecurity infrastructure. The study evaluates specific aspects of Purple teams through perception, but does not assess an organization's maturity and size, budget, time, and basic security hygiene as it relates to cybersecurity assessments. These variables may have impacted a professional's perceptions on Purple teams based on prior experiences and may have acted as plausible alternative explanations. Similar, there can be scenarios where organizations want to create a Purple team, and use Purple team methodology, but may not be at a point where one is useful or needed. Purple teams may have benefit as identified by the respondents, but only if certain foundational security basics (e.g., developing security mechanisms for hosts, employee training, quality-controlled coding practices, network monitoring) are met; these basic prerequisites were not evaluated.

5.2 Conclusions

As the need for both modification of current cybersecurity practices and popularity of Purple teams in cybersecurity assessments increase, it is critical to assess how the workforce and community feel about and perceive this new concept. Even though professionals believe Purple teams have benefit and can work alongside Red and Blue teams, it appears if organizations want to implement Purple teams, they need to be able to get existing Red teams and individuals with

more experience on board. Throughout the process of creating and running Purple team assessments, managerial support and project clarity are factors organizations have to be constantly aware of, control, and provide. The security teams conducting the tests need to work together to collectively define roles, assign individuals with the right skillsets to the right teams, and implement a well-defined and agreed-upon methodology for Red, Blue, and Purple teams.

Future research should aim to expand on the current study by assessing perception alongside more contextual information. By assessing factors such as the maturity of an organization's security infrastructure and costs associated with security assessments, the real-world impact of Purple teams can be assessed along with how it impacts perceptions. Organizations who conduct all the different types of audits should also conduct research to assess actual metric-based benefit. While knowing if the workforce and community support the newer concept of Purple teams is beneficial to management and an organization, it would also be important to test real world impact of Purple teams and compare them to the perceived benefits. Future studies can compare and contrast team reality and perception to upper management perspectives and gain a holistic view of how elements interact during cybersecurity testing.

APPENDIX A. IRB NARRATIVE

A. Proposed research rationale

To evaluate the cybersecurity capabilities of a company, professionals often conduct security audits to discover issues and fix them before any real threats occur. This anonymous survey aims to evaluate how cybersecurity professionals perceive the general nature of these information security assessments. The main research question proposed by this study is 'how is the role of a Purple team and its relationship with Red and Blue teams in cybersecurity assessments perceived by professionals in the field?'. The study also has the ancillary research questions of 'how can the effectiveness of a Purple team assessment be impacted in terms of success factors, issues, and managerial support?' and 'can a high-level methodology for Purple teams be created from existing Red and Blue team methodologies?'

B. Specific procedures to be followed

An anonymous survey made on Qualtrics will be distributed to security professionals through social media channels such as Twitter, LinkedIn, and Email. For individuals that click on the distributed survey link, they will be directed to the consent form for the anonymous survey on the secure Qualtrics website. If they have read and accepted the consent form (see Attachment: Consent form), and agree to voluntarily participate, the participants will be shown the online survey. The consent form will state that only individuals 18 years of age and older AND current residents in the United States will be able eligible to complete the study; if a participant is under 18 or is not a current resident of the US, he/she will not be allowed to continue.

As this study aims to survey cybersecurity professionals, participants will be asked if they meet the definition. If they answer 'no' or decline to answer, they will not be allowed to continue the survey. Participants can choose to withdraw from the survey at any time and skip or decline any questions they do not wish to answer. After the consent page, respondents will complete questions about demographics. Information such as education level, experience in industry, employment, age, sex, and others will be collected, to provide the researcher with descriptive information about the sample. After answering questions about general demographics, this

section of the survey will also ask participants for non-identifying information about prior security experiences with security assessments.

This survey will then ask about perceptions of information security assessments and how participants feel about such testing. The perception is evaluated based on three subsections. One section will ask participants to answer questions to measure their understanding of a Purple team, and their perceptions of the concept, as well as used a modified 'knowledge collaboration scale' to assess how Purple teams would work with Red and Blue teams. One of the sections will ask open-ended text responses to three questions about success factors, issues, and managerial support needed related to Purple teams. The third section will have participants rate steps from existing Red and Blue methodologies, as suggested by the National Institute of Standards and Technology, on how relevant they would be to Purple teaming, from a scale of 0-10. These sections will be presented in a randomized order through Qualtrics to control for order effects. No personally identifying data will be collected from the participants and only aggregated data from all the participants will be presented in a paper. After this is completed, they participants will be directed to a thank-you page.

The Knowledge Collaboration Scale by Jarvenpaa and Majchrzak (2008) is a 27-item scale measuring knowledge collaboration among professionals protecting national security. The modified scale will measure and compare the constructs of combinative information sharing (six items), security practices (ten items), knowledge dissemination (three items), ownership (three items), and learning (five items) across Purple, Red, and Blue teams.

C. Subjects to be included

Participants will be 250 cybersecurity professionals who have worked in industry across different security roles will be recruited through social media as mentioned above. Participants will be required to over the age of 18 and to be current residents of the United States. Individuals will be asked if they meet the definition of a cybersecurity professional and those not meeting the definition will be excluded as this research specially aims to study how cybersecurity professionals perceive security assessments. The target sample size for the study is chosen through power analysis.

D. Recruitment of subjects and obtaining informed consent

Respondents ($N = 250$) will be solicited through social media such as Twitter, LinkedIn, and Email. For the current study, a snowball sampling method will be used. This solicitation will include a survey link that respondents can click on if they are interested in participation. This link will direct them to Purdue University's Qualtrics website, where the entirety of study procedures will take place. When the survey link is distributed through social media, participants and those to see the post will be requested to voluntarily share the post with other cybersecurity professionals. The snowball sampling method is chosen as the study targets security professionals working across various industries, and it might be challenging to directly locate enough participants for a sample; the sampling strategy is helpful when trying to study a specific and harder to identify and reach population (Graziano & Raulin, 1993; Kitchenham & Pfleeger, 2002).

The opening page of the Qualtrics survey will include the Informed Consent (see Attachment: Consent form). If respondents choose to proceed with participation, they will click on the survey link and be directed into the survey. There will be no direct or indirect contact between researchers and potential participants. No identifying information will be collected. The consent form will state that only individuals 18 years of age and older AND permanent residents in the United States will be able eligible to complete the study. In addition, the demographics questionnaire will specifically ask the respondents to identify their current age and permanent residence – any individual who is not 18 years of age or older AND a permanent resident of the US will be screened out of the study and not eligible for compensation.

E. Procedures of payment of subject

For the current study, participants will not be *not* given any monetary compensation or payment.

F. Confidentiality

The study is completely anonymous. All data will be collected via an internet-based survey via Qualtrics. No identifying information will be collected, such as IP addresses or names. Each response is assigned a completely random ID by Qualtrics that does not provide any information or connection to the participant. A copy of the raw data will be downloaded from

Qualtrics and stored on the PI's computer. This raw data will already be anonymous since no identifying information will be collected in the survey. The file will be saved in an encrypted format. Only the PI and Co-PI will have access to the encrypted file. The encrypted data will be kept indefinitely and will be used only for research purposes.

G. Potential risks to subjects

The risks to the participants of the study are minimal, i.e. they are not greater than those ordinarily encountered in daily life. The survey is anonymous and conducted securely through Qualtrics. No identifiable information is collected and thus responses cannot be linked to any specific person in any way. The only risk is breach of confidentiality in that the respondent tells someone that they completed the study; however, even then it will not be possible to link the responses back to an individual. The safeguards used to minimize this risk can be found in the confidentiality section. The participants may quit the survey at any time if they do not wish to continue and can also skip questions if they do not feel comfortable answering any of them.

H. Benefits to be gained by the individual and/or society

There are no direct benefits to individuals completing the study. Potential benefits to society are small based on this study alone. There may be broader benefits to society to be had from the larger program of research into cybersecurity testing and its potential impact on society. Understanding how security professionals perceive such assessments in the field may be of value to a cybersecurity professional conducting such assessments or as a manager planning them, which may impact cybersecurity practices.

I. Investigator's evaluation of the risk-benefit ratio

Risks are minimal, no greater than that encountered in daily life. There are, however, potential benefits of this research to the field of cybersecurity.

J. Written informed consent form

See Attachment: Consent form

K. Waiver of informed consent or signed consent

The researchers request a Waiver of Signed Consent since this is an Internet-based study. Although there will be a consent form with all necessary elements (see Attachment: Consent form), the respondents will not be "signing" the online form but instead clicking "Agree" as an indication of their consent. The research study is completely anonymous and does not pose greater than minimal risk to general Internet users. The current study is completely anonymous and does not record any identifiable information. The current study would not require signed consent if it were to be conducted in a non-research context. The respondents will still read a consent form and have to accept it before they can see the survey; it will just be online, and they will indicate their consent by clicking on "agree" rather than signing their name.

L. International Research

N/A

M. Supporting documents

I. Recruitment advertisements, flyers, emails and letters. (see Attachment: Recruitment material)

II. Survey instruments, questionnaires, tests, debriefing information, etc. (see Attachment: Survey)

III. Consent Form, Parental Permission, Assent Form (see Attachment: Consent form)

APPENDIX B. RESEARCH PARTICIPANT CONSENT FORM

Key Information:

Please take time to review this information carefully. This is a research study. Your participation in this study is voluntary which means that you may choose not to participate at any time without penalty or loss of benefits to which you are otherwise entitled. You may ask questions to the researchers about the study whenever you would like. If you decide to take part in the study, you will be asked to sign this form, be sure you understand what you will do and any possible risks or benefits.

To evaluate the cybersecurity capabilities of a company, professionals often conduct security audits to discover issues and fix them before any real threats occur. This anonymous survey aims to evaluate how cybersecurity professionals perceive the general nature of these information security assessments. The current 15-20-minute survey is a part of a 6-month research project at Purdue University.

What is the purpose of this study?

The purpose of this study is to survey how cybersecurity professionals perceive information security assessments, and how Red, Blue and Purple teams conduct these audits. This study shall anonymously ask you to answer questions regardless of your whether you have a positive, negative, neutral, or other perception of such assessments. We would like to enroll 250 cybersecurity professionals to participate in this study.

What will I do if I choose to be in this study?

If you choose to be part of the current survey, it will be conducted anonymously via a secure website. Once you have read this consent form, and agree to voluntarily participate, you will be shown the online survey. You may withdraw from the survey at any time and you may skip or decline any questions that you do not wish to answer. After the consent page, you will first answer some general demographic questions about yourself. You will then answer general non-identifying questions about previous cybersecurity experiences. This survey will then ask about perceptions information security assessments and how you feel about such testing. No personally

identifying data will be collected from the participants and only aggregated data from all the participants will be presented in a paper.

How long will I be in the study?

Most participants take around 15-20 minutes to complete the entire survey for this study.

What are the possible risks or discomforts?

The risks to you are minimal. They are not greater than those ordinarily encountered in daily life. Please know that this is an anonymous survey that uses a secure link. The survey is anonymous because we will not be able to link your responses back to you – we do not ask for any identifiable information (Ex. name). While completing the survey, the only risk to you might be if someone were to see your responses to the survey, so we recommend that you take this survey when you have complete privacy. Since the survey is anonymous, no one will know that you completed this survey unless you personally tell him or her; breach of confidentiality is always a risk with data, but we take precautions to minimize this risk as described in the confidentiality section below.

Are there any potential benefits?

There are no direct benefits to you. Eventually, we hope to publish the research results, and if you want to see them, you should send an email requesting information to the Principal Investigator at kspellar@purdue.edu. We believe you may be interested in reading the publication as a cybersecurity professional conducting such assessments or as a manager planning them.

What alternatives are available?

Since participation in the survey is voluntary, individuals may choose not to participate in the research study.

Will information about me and my participation be kept confidential?

We do not ask for your name or any other information that could be used to identify you at any time before, during, or after the survey. No IP addresses will be recorded. There will be no way

to determine where the survey was taken or by whom. Instead, the survey software will randomly assign an ID number to your responses. This means that the responses to the questionnaires cannot be linked or matched to you, which means your responses will remain completely anonymous. Only researchers associated with this study will have access to the data. In addition to the data being anonymous, it will be stored electronically in an encrypted format. The encrypted data will be kept indefinitely and will be used only for research purposes.

What are my rights if I take part in this study?

Your participation in this study is voluntary. You may choose not to participate or, if you agree to participate, you can withdraw your participation at any time without penalty or loss of benefits to which you are otherwise entitled.

Who can I contact if I have questions about the study?

If you have questions, comments or concerns about this research project, you can talk to one of the researchers. Please contact Dr. Kathryn Seigfried-Spellar at xxx-xxx-xxxx. To report anonymously via Purdue's Hotline see www.purdue.edu/hotline. If you have questions about your rights while taking part in the study or have concerns about the treatment of research participants, please call the Human Research Protection Program at (765) 494-5942, email (irb@purdue.edu) or write to:

Human Research Protection Program - Purdue University
Ernest C. Young Hall, Room 1032
155 S. Grant St.
West Lafayette, IN 47907-2114

Documentation of Informed Consent

I have had the opportunity to read this consent form and have the research study explained. I have had the opportunity to ask questions about the research study, and my questions have been answered. I am prepared to participate in the research study described above. If I wish, I may print this form for my records. If you agree, please click on the "I Agree" button below. Otherwise, we thank you for your time and ask that you click on the "I Do Not Agree" button.

I Agree I Do Not Agree

APPENDIX C. SURVEY

Start of Block: validation

age What is your current age in years?

_____

location Are you currently residing in the United States of America?

- ○ No (1)
- ○ Yes (2)
- ○ Decline to answer (3)

meet_definition A cybersecurity professional is defined as: "Any individual who has worked in a cybersecurity-related role at any point in their career."

Do you meet this definition?

- ○ No (1)
- ○ Yes, I have worked in this capacity for less than 2 years (2)
- ○ Yes, I have worked in this capacity for 2 years or more (3)
- ○ Decline to answer (4)

End of Block: validation

Start of Block: demographics

gender What is your gender?

- ○ Male (1)
- ○ Female (2)
- ○ Transgender (3)
- ○ Non-Binary (4)
- ○ Other (5) _____

education What is your highest completed education level?

- ○ Some high school, no diploma (1)
- ○ High school graduate, diploma or the equivalent (such as GED) (2)
- ○ Some college credit, no degree (3)
- ○ Associate's Degree (4)
- ○ Bachelor's Degree (5)
- ○ Master's Degree (6)
- ○ PhD or Doctorate (7)

advanced_degree Based on your previous answer, was your advanced degree in a field related to cybersecurity?

- ○ No (1)
- ○ Yes (2)
- ○ Unsure (3)

employment_status What is your current employment status?

- ○ Employed full time (1)
- ○ Employed part time (2)
- ○ Unemployed looking for work (3)
- ○ Unemployed not looking for work (4)
- ○ Retired (5)
- ○ Student (6)
- ○ Disabled (7)

---

industry What sector do you currently work in?

- ○ Industry (Tech) (1)
- ○ Industry (Non-Tech) (2)
- ○ Professional Services/ Consulting (3)
- ○ Government (4)
- ○ Academia (5)
- ○ Unemployed, not currently working (8)
- ○ Other (6)
- ○ Prefer not to say (7)

---

red_blue_def For the purpose of this study,

Red team is defined as "Information security professionals who use tactics, techniques, and procedures (TTPs) to mimic real-world threats in order to measure the security capabilities of an organization’s assets."

Blue team is defined as "Information security professionals who use knowledge of attacks and the infrastructure to defend an organization’s critical assets and systems against attacks and threats from adversaries."

experience How many total years have you worked in a cybersecurity-related role?

_____

red Have you ever worked on a Red team and/or in an offensive security role?

- ○ No (1)
- ○ Yes (2)
- ○ Unsure (3)
- ○ Decline to respond (4)

blue Have you ever worked on a Blue team and/or in a defensive security role?

- ○ No (1)
- ○ Yes (2)
- ○ Unsure (3)
- ○ Decline to respond (4)

manager Have you ever managed or been in charge of a cybersecurity team?

- ○ No (1)
- ○ Yes (2)
- ○ Maybe (3)

End of Block: demographics

Start of Block: purple intro

purple_def For the purpose of this study,

Purple team is defined as "Information security professionals who bring together and use concepts and principles of red and blue teams simultaneously, utilizing collaboration and information sharing, for security assessments"

For this study, it is assumed a Purple team is used alongside traditional Red and Blue teams.

purple_know Have you ever heard of Purple teams?

- ○ No (1)
- ○ Yes (2)
- ○ Unsure (3)

purple_part Have you ever been part of a Purple team assessment?

- ○ No (1)
- ○ Yes (2)
- ○ Unsure (3)

purple_work Have you ever worked at/with an organization that has a Purple team?

- ○ No (1)
- ○ Yes (2)
- ○ Unsure (3)

End of Block: purple intro

Start of Block: purple, red, blue perceptions

purple_benefit Please select the statement below that you agree with the most:

Do you think Purple teams are beneficial?

- Yes, it is beneficial (1)
- No, it is not beneficial (2)
- Yes, when working alongside existing Red and Blue teams (3)
- Yes, but only for specific testing cases (4)
- No, it is repetitive (5)
- Unsure (6)
- I don't know (7)

purple_creation If we were going to create a Purple Team, how should they be created?

- From some existing Red professionals, and some existing Blue professionals (1)
- From some new Red professionals, and some new Blue professionals (2)
- From only individuals that have both Red and Blue skills (3)
- From a random combination of professionals regardless of previous experience (4)
- Unsure (5)
- I don't know (6)

purple_share Should Purple teams share information with Red and Blue teams?

- ○ Yes, they should collaborate with both teams (1)
- ○ Yes, but with Red teams only (2)
- ○ Yes, but with Blue teams only (3)
- ○ No, they should work independently (4)
- ○ Unsure (5)
- ○ I don't know (6)

---

text The questions below compare your perception of Purple teams to Red and Blue teams, and examines your perceptions on the role of a Purple team on a variety of factors.

---

info_sharing Compared to Red and Blue teams, how would a Purple team perform in terms of sharing the following information?

	Much worse (1)	Slightly worse (2)	The same (3)	Slightly better (4)	Much better (5)
Knowledge about how a threat was identified (1)	○	○	○	○	○
Knowledge about steps taken to respond to a threat (2)	○	○	○	○	○
Knowledge about preventing future similar threats (3)	○	○	○	○	○
Reason for decisions others made when responding to a threat (4)	○	○	○	○	○
Reasons for involving certain people in the security response (5)	○	○	○	○	○
Reasons behind decisions made for not pursuing certain security responses (6)	○	○	○	○	○

security_practices In day-to-day operations, how likely is a Purple team to engage in the following practices?

	Extremely unlikely (1)	Slightly unlikely (2)	Neither (3)	Slightly likely (4)	Extremely likely (5)
Develop several options for responding to a threat (1)	○	○	○	○	○
Describe problems are both a summary and detailed level (2)	○	○	○	○	○
Describe alternate scenarios for a problem (3)	○	○	○	○	○
Brainstorm about ideas or possible solutions (4)	○	○	○	○	○
Describe detailed context of threat information (5)	○	○	○	○	○
Understand how information changes over time (6)	○	○	○	○	○
Discuss source of ideas for handling threats (7)	○	○	○	○	○
Discuss how time is affecting information (8)	○	○	○	○	○

Revisit decisions about previous security issues (9)	○	○	○	○	○
Discuss source of threat information (10)	○	○	○	○	○

dissemination

Provide your opinion on the following statements:

A Purple team would have managerial and executive directions on:

	Strongly disagree (1)	Slightly disagree (2)	Neither (3)	Slightly agree (4)	Strongly agree (5)
Norms and procedures for information others about security threat information (1)	○	○	○	○	○
Procedures for identifying for information is sensitive (2)	○	○	○	○	○
Safeguard to protect the privacy of the source (3)	○	○	○	○	○

ownership

Provide your opinion on the following statements:

Having a Purple team alongside a Red and Blue team would cause:

	Strongly disagree (1)	Slightly disagree (2)	Neither (3)	Slightly agree (4)	Strongly agree (5)
Confusion about ownership of the knowledge shared between the teams (1)	○	○	○	○	○
Ambiguity about who owns the solutions created between the teams (2)	○	○	○	○	○
Lack of clear policies on who owns what rights to knowledge, discoveries, and inventions (3)	○	○	○	○	○

learning Would working in a Purple team help analysts:

	Extremely unlikely (1)	Slightly unlikely (2)	Neither (3)	Slightly likely (4)	Extremely likely (5)
Learn about new technology (1)	○	○	○	○	○
Learn about new management techniques (2)	○	○	○	○	○
Learn about new ways to prevent security problems (3)	○	○	○	○	○
Learn about new ways to respond to security threats (4)	○	○	○	○	○
Have access to other's skills and knowledge (5)	○	○	○	○	○

End of Block: purple, red, blue perceptions

Start of Block: needs analysis

needs_success If Purple teams were to succeed, what factors would they need most? (Please enter up to three factors):

○ Factor #1: (1) _____

○ Factor #2: (2) _____

○ Factor #3: (3) _____

needs_issues What are the issues you associate with Purple teams? (Please enter up to three factors):

- Factor #1: (1) _____
- Factor #2: (2) _____
- Factor #3: (3) _____

needs_management What are the ways in which management can help Purple teams? (Please enter up to three factors):

- Factor #1: (1) _____
- Factor #2: (2) _____
- Factor #3: (3) _____

End of Block: needs analysis

Start of Block: methodology

methodology Red teams and Blue teams often conduct specific steps during engagements (such as gathering intel or identifying threats), which form the Red team and Blue team methodology. These steps are sometimes common across the teams, while sometimes they are unique.

If you were to create a new methodology for Purple teams, on a scale of 0-10, please rate how relevant you believe each of these phases would be? (0 being not relevant at all and 10 being very relevant)

	0 1 2 3 4 5 6 7 8 9 10
Information gathering ()	
Footprinting ()	
Network and pot scanning ()	
OS detection ()	
Service detection ()	
Asset identification ()	
Evaluation ()	
Threat identification ()	
Vulnerability investigation ()	
Penetration testing ()	
Safeguard creations ()	
Providing recommendations ()	

End of Block: methodology

APPENDIX D. RECRUITMENT MATERIALS

An anonymous survey made on Qualtrics will be distributed to security professionals through social media channels such as Twitter, LinkedIn, and Email. For individuals that click on the distributed survey link, they will be directed to the consent form for the anonymous survey on the secure Qualtrics website.

For the study, an example of a solicitation will be as follows:

Researchers from Purdue are looking for cybersecurity professionals to take an anonymous survey on how they perceive security assessments and the roles of Red, Blue, and Purple teams. Please take the survey at https://purdue.ca1.qualtrics.com/jfe/form/SV_cwMWKckeQUh04iV and if you choose, please share it with other professionals.

If the participants do not agree to the consent form, if they are below the age of 18, or if they are not current residents of the US, they will see the following message:

Sorry, but based on one or more of your responses, you did not qualify for the survey.
Thank you for your interest, please contact the principal investigator Dr. Kathryn Seigfried-Spellar at xxx-xxx-xxxx or kspellar@purdue.edu if you have any questions.

If they complete the survey, they will be presented with the following message:

Thank you so much for your participation!
Your responses are valuable to the researchers. For any questions about the project, the survey, or the data, please contact Dr. Kathryn Seigfried-Spellar at kspellar@purdue.edu or xxx-xxx-xxxx.

APPENDIX E. IRB EXEMPTION

PURDUE UNIVERSITY

HUMAN RESEARCH PROTECTION PROGRAM
INSTITUTIONAL REVIEW BOARDS

To:	SEIGFRIED-SPELLAR, KATHRYN C
From:	DICLEMENTI, JEANNIE D, Chair Social Science IRB
Date:	01/18/2019
Committee Action:(2)	Determined Exempt, Category **(2)**
IRB Action Date:	01 / 18 / 2019
IRB Protocol #:	1901021516
Study Title:	Perceptions of Purple Teams Among Cybersecurity Professionals

The Institutional Review Board (IRB) has reviewed the above-referenced study application and has determined that it meets the criteria for exemption under 45 CFR 46.101(b).

Before making changes to the study procedures, please submit an Amendment to ensure that the regulatory status of the study has not changed. Changes in key research personnel should also be submitted to the IRB through an amendment.

General

- To recruit from Purdue University classrooms, the instructor and all others associated with conduct of the course (e.g., teaching assistants) must not be present during announcement of the research opportunity or any recruitment activity. This may be accomplished by announcing, in advance, that class will either start later than usual or end earlier than usual so this activity may occur. It should be emphasized that attendance at the announcement and recruitment are voluntary and the student's attendance and enrollment decision will not be shared with those administering the course.
- If students earn extra credit towards their course grade through participation in a research project conducted by someone other than the course instructor(s), such as in the example above, the students participation should only be shared with the course instructor(s) at the end of the semester. Additionally, instructors who allow extra credit to be earned through participation in research must also provide an opportunity for students to earn comparable extra credit through a non-research activity requiring an amount of time and effort comparable to the research option.
- When conducting human subjects research at a non-Purdue college/university, investigators are urged to contact that institution's IRB to determine requirements for conducting research at that institution.
- When human subjects research will be conducted in schools or places of business, investigators must obtain written permission from an appropriate authority within the organization. If the written permission was not submitted with the study application at the time of IRB review (e.g., the school would not issue the letter without proof of IRB approval, etc.), the investigator must submit the written permission to the IRB prior to engaging in the research activities (e.g., recruitment, study procedures, etc.). Submit this documentation as an FYI through Coeus. This is an institutional requirement.

REFERENCES

Armerding, T. (2018, Jan). *The 17 biggest data breaches of the 21st century*. Retrieved from https://www.csoonline.com/

Abraham, S. M. (2016, June). Estimating mean time to compromise using non-homogenous continuous-time Markov models. In *Proceedings of 40th Annual Computer Software and Applications Conference* (Vol. 2, pp. 467-472). Georgia, USA: IEEE.

Birnbaum, M. H. (Ed.). (2000). *Psychological experiments on the Internet*. Amsterdam, Netherlands: Elsevier.

Boardman, C., & Sundquist, E. (2009). Toward understanding work motivation: Worker attitudes and the perception of effective public service. *The American Review of Public Administration*, *39*(5), 519-535.

Bossler, A., Holt, T. J., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics: An introduction*. Abingdon, United Kingdom: Routledge.

Boynton, A. C., & Zmud, R. W. (1984). An assessment of critical success factors. *Sloan management review*, *25*(4), 17-27.

Carayon, P., & Kraemer, S. (2004). *Red team performance: Summary of findings at University of Wisconsin-Madison & IDART*. Albuquerque, New Mexico: Sandia National Laboratories.

Carvalho, M. M. (2008, July). Communication issues in projects management. In *Proceedings of the Portland International Conference on Management of Engineering & Technology* (pp. 1280-1284). Portland, Oregon: IEEE.

Cisco. (2018, Feb). *Cisco 2018 annual cybersecurity report*. Retrieved from https://www.cisco.com

Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity - attack and defense strategies: Infrastructure security with red team and blue team tactics*. Birmingham, United Kingdom: Packt Publishing.

DoD (2015). DoD 8570.01-M: Information assurance workforce improvement program. *Department of Defense*. Retrieved from http://www.esd.whs.mil/

Drinkwater, D., & Zurkus, K. (2017, Jul). *Red team versus blue team: How to run an effective simulation*. Retrieved from https://www.csoonline.com/

Embers, R. (2018, May). *Cyber security and the growing role of red teaming*. Retrieved from https://www.itproportal.com/

Ewusi-Mensah, K. (1997). Critical issues in abandoned information systems development projects. *Communications of the ACM*, *40*(9), 74-80.

Fontenot, G. (2005). Seeing red: Creating a red-team capability for the blue force. *Military Review*, *85*(5), 4-8.

Fultz, N., & Grossklags, J. (2009). Blue versus red: Towards a model of distributed security attacks. In *Proceedings of International Conference on Financial Cryptography and Data Security* (pp. 167–183).

Graziano, A. M., & Raulin, M. L. (1993). *Research methods: A process of inquiry*. New York, USA: HarperCollins College Publishers.

IBM. (2018). *Cost of a Data Breach Study by Ponemon*. Retrieved from https://www.ibm.com/

Ifps. (n.d.). *Command and control (malware)*. Retrieved from https://ipfs.io/

Interpol. (n.d.). *Cybercrime*. Retrieved from https://www.interpol.int/

Jarvenpaa, S. L., & Majchrzak, A. (2008). Knowledge collaboration among professionals protecting national security: Role of transactive memories in ego-centered knowledge networks. *Organization Science*, *19*(2), 260-276.

Johnson, H. (2016, Oct). Red team v. blue team? They are in fact one - the purple team. *Tripwire*. Retrieved from https://www.tripwire.com/

Kewley, D., Fink, R., Lowry, J., & Dean, M. (2001). Dynamic approaches to thwart adversary intelligence gathering. In *Proceedings of 2001 DARPA Information Survivability Conference & Exposition II* (Vol. 1, pp. 176–185). California, US: IEEE.

Kitchenham, B., & Pfleeger, S. L. (2002). Principles of survey research: part 5: populations and samples. *ACM SIGSOFT Software Engineering Notes*, *27*(5), 17-20.

Kline, P. (1999). *The handbook of psychological testing* (2nd ed.). London: Routledge

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, *33*, 159-174.

Leggio, J. (2017, May). *How "adversarial engineering" of red teams is strengthening security practitioners*. Retrieved from https://www.zdnet.com/

Leversage, D. J., & Byres, E. J. (2008). Estimating a System. *IEEE Security & Privacy*, *6*(1), 52-60.

McQueen, M. A., Boyer, W. F., Flynn, M. A., & Beitel, G. A. (2006). Time-to-compromise model for cyber risk reduction estimation. In *Proceedings of Quality of Protection* (pp. 49-64). Boston, MA: Springer.

Maughan, D. (2010). The need for a national cybersecurity research and development agenda. *Communications of the ACM*, *53*(2), 29-31.

Malwarebytes. (n.d.). *Glossary*: *Proof of concept.* Retrieved from https://blog.malwarebytes.com/

Miessler, D. (2016, Feb). *The Difference Between Red, Blue, and Purple Teams*. Retrieved from https://www.danielmiessler.com/

Mirkovic, J., Reiher, P., Papadopoulos, C., Hussain, A., Shepard, M., Berg, M., & Jung, R. (2008). Testing a collaborative DDOS defense in a red team/blue team exercise. *IEEE Transactions on Computers*, *57*(8), 1098–1112.

Morgan, S. (2017a, Jun). *Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021*. Retrieved from https://cybersecurityventures.com/

Morgan, S. (2017b, Oct). *Cybercrime damage $ 6 trillion by 2021*. Retrieved from https://cybersecurityventures.com/

Morgan, S. (2018, Jan). *Top 5 cybersecurity facts, figures and statistics for 2018*. Retrieved from https://www.csoonline.com/

Munns, A. K., & Bjeirmi, B. F. (1996). The role of project management in achieving project success. *International journal of project management*, *14*(2), 81-87.

NIST Computer Security Resource Center. (n.d.). *Glossary*. Retrieved from https://csrc.nist.gov/glossary

NeSmith, B. (2018, Aug). *The cybersecurity talent gap is an industry crisis*. Retrieved from https://www.forbes.com/

Palmer, C. C. (2001). Ethical hacking. *IBM Systems Journal*, *40*(3), 769-780.

Peters, S. (2016, Jul). *Purple teaming: Red & blue living together, mass hysteria*. Retrieved from https://www.darkreading.com/

Porter, L. J., & Parker, A. J. (1993). Total quality management—the critical success factors. *Total quality management*, *4*(1), 13-22.

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. In *Proceedings of 2011 IEEE 29th International Conference on Computer Design* (pp. 285–288). Brooklyn, USA: IEEE.

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. *Computers & Security*, *23*(1), 12-16.

Salerno, C. (2017, Jan). *Purple teaming: How to approach it in 2017*. Retrieved from https://www.securityriskadvisors.com/

SANS. (n.d.). SEC564: *Red Team Operations and Threat Emulation*. Retrieved from https://www.sans.org/

SANS. (n.d.). *Blue Team Summit & Training 2019*. Retrieved from https://www.sans.org/

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical guide to information security testing and assessment. *NIST Special Publication*, *800*(115), 2–25.

SecureAuth, (2018, May). *Security in plain English: What are red, blue, and purple teams?* Retrieved from https://www.secureauth.com/

Sherr, I. (2017, May). *WannaCry ransomware: Everything you need to know*. Retrieved from https://www.cnet.com/

Simister, A. (2018, Jan). *7 cybersecurity trends to watch out for in 2018*. Retrieved from https://www.csoonline.com/

Sumner, M. (1999). Critical success factors in enterprise wide information management systems projects. In *Proceedings of Americas Conference on Information Systems* (pp. 297-303). Milwaukee, Wisconsin: AMCIS.

Symantec. (2018, Feb). *2018 internet security threat report* (Vol. 23). Retrieved from https://www.symantec.com/

Symantec. (2016, Oct). *Mirai: what you need to know about the botnet behind recent major DDoS attacks*. Retrieved from https://www.symantec.com/

Tesch, S. A., & Cameron, K. A. (1987). Openness to experience and development of adult identity. *Journal of Personality*, *55*(4), 615-630.

Veerasamy, N. (2009). High-level methodology for carrying out combined red and blue teams. In Proceedings of *2009 Second International Conference on Computer and Electrical Engineering* (Vol. 1, pp. 416–420). Dubai, United Arab Emirates: IEEE.

Ward, A. (2017, Jun). *Russia hacked voting systems in 39 states before the 2016 presidential election*. Retrieved from https://www.vox.com/

Yang, A., Abbass, H. A., & Sarker, R. (2006). Characterizing warfare in red teaming. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *36*(2), 268–285.

Zurkus, K. (2016, Oct). *Best tools for red and blue teams are methodology, experience*. Retrieved from https://www.csoonline.com/