Purple Team Playbook: Threat Modeling for Security Testing

Felisha Mouchous

Technical Report

RHUL–ISG–2020–7

22 June 2020

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Student Number: 100630252

Felisha Mouchous

Purple Team Playbook:
Threat Modeling for Security Testing

Supervisor: Daniele Sgandurra

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date: 21/08/2019

Page intentionally left blank

ABSTRACT

The reality with information security is that we cannot completely mitigate the threat of an attacker getting into our networks. Organisations can, however, control how they prepare and react to attackers by understanding how they operate. Threat modeling and security testing provide a way to first identify the threats and then simulate how an attack can take hold. In order to fully understand the threats, employees need to have the right information at the right time so that they are fully equipped to match the attacker's capabilities. To do this, the red and the blue team in an organisation must work together to simulate attacks and test their defences.

In this thesis we first explore the available threat models and how they can apply to security testing in an organisation. Based on the research we have conducted and our own knowledge on security testing, we have created a Purple Team Playbook Framework. The purpose of this framework is to allow organisations to leverage existing data on threats, attack techniques, defences and asset data so that they can get the red and the blue team working together. By using this framework, organisations can effectively identify where they have gaps in their defences and how they can simulate threat actor behaviour, in order to assess how they can address these security gaps. To this end, we have formulated proof of concept scenarios to show how this framework can be used in an organisation and how it helps address the challenges with threat modeling and security testing.

Page intentionally left blank

Table of Contents

List of Tables

List of Figures

Acknowledgements

I would like to thank my thesis supervisor Daniele Sgandurra for helping me throughout the process. I would also like to thank my family, friends and work colleagues for their patience and support during my MSc.

List of Abbreviations & Acronyms

API	Application Programming Interface
APT	Advanced Persistent Threat
CIA	Confidentiality Integrity Availability
CVSS	Common Vulnerability Scoring System
IoT	Internet of Things
JSON	JavaScript Object Notation
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
Pen Test	Penetration Test
POC	Proof of Concept
PTES	Penetration test execution standard
PTP	Purple Team Playbook

1. Introduction

As technology evolves, the security threat landscape grows. Just over twenty years ago the internet was not available to everyone, so the landscape was much smaller, and we were less connected. Now the threat landscape is constantly changing - embedded systems, IOT, cloud applications, as well as attackers capabilities - the more ways one tries to defend themselves, an attacker will always find a way to try and circumvent your controls [1]. As a result of the increasing threats born from new technology, we need to be paying attention to what our threats are and how we can protect ourselves from them. In the 2019 Verizon breach report it was reported that 69% of attackers were attributed to outside threat actors, 71% of breaches were financially motivated and 52% of breaches were as a direct result of hacking [2]. It was also reported this year by researchers from Kaspersky that they have found a brand new attack framework, 'Taj Mahal', in one company that had remained undetected for five years [3]. Due to the complexity of this framework they believe that these attackers could have also compromised other organisations, but this is yet to be determined. This reinforces the fact that organisations need to be evolving their testing and defence capabilities in order to try and keep up with these attackers.

This thesis highlights the importance of knowing what your organisations threats are and how one can use security testing to better protect themselves from the evolving threats. Based on our own experience with security testing in a large organisation, we have found that it is not always easy to get all the information one needs on the threats an organisation faces. This puts us at a disadvantage as we may not be simulating the correct attacker behaviour and there will be gaps in our testing. We have also found that it can be difficult to get information on all the security controls that are in place in an organisation. This affects how we test and how we judge the impact of a finding. In order to address these issues, we have created a Purple Team Playbook (PTP) framework which is essentially a big knowledge base that leverages existing data in order to help red and blue teams in an organisation's threat model. This allows an organisation to understand where they are now in terms of what has been tested and what defences they have to enable them to determine where they need to be to strengthen their security posture.

1.1. Threat Modeling

A threat model is characterised by OWASP as "a structured representation of all the information that affects the security of an application. In essence, it is a view of the application and its environment through security glasses" [4]. Another definition of Threat modeling is that it is a way of "using models to find security problems. Using a model means abstracting away a lot of details to provide a look at the bigger picture, rather than the code itself" [5]. By identifying threats to an application, we can be better informed on how to defend against them. By not documenting the threats using a model we run the risk of unknown issues impacting our organisation.

Threat modeling is important during the whole software development lifecycle as it "can lead to proactive architectural decisions that allow for threats to be reduced from the start" [6], this in kind will reduce the cost and time of remediating security issues after development has finished. This however will only work on newer system developments; legacy systems may have been developed without security in mind so there is a need to use threat modeling on

existing systems as well to ensure there are ways to mitigate the risk. Threats are also continuously changing so it may have been designed and created to be secure in the past; however new information in the future could impact a system so threat modeling needs to be conducted throughout the system's life.

Threat modeling can be a very subjective process as different types of applications will have different types of threats and it depends on the experience of the user creating the model. For instance, a government department may be more concerned with attacks from other countries governments. A commercial organisation will be more concerned with competition stealing intellectual property or criminals impacting profits. If the person creating the threat model is misinformed or has a lack of experience, some threats may go undocumented and the use of a model should act as a guide or a tool to help an organisation identify threats. Another issue when looking at threat modeling is that it can be hard to think like an attacker and if we are expected to, it can impact negatively on the way we look at our threats and get them wrong [5].

In order for an organisation to threat model, there are several tools and models both open source and commercially available to use. In Chapter 2 we will explore these models and tools and show how we can use them to elicit threat information for an organisation.

1.2. Security Testing Process

Security testing refers to activities that assess an organisations security posture and try to find their security weaknesses and vulnerabilities [7]. Some of the activities involved are secure code reviews, vulnerability assessments, penetration tests and red team tests. A vulnerability assessment consists of running a scan on the assets that are in scope and reporting on them to determine if there are missing security patches or misconfigurations [8]. A penetration test (Pen Test) is conducted by a tester that will try to simulate threat actor behaviour, "the testers not only discover vulnerabilities that could be used by attackers but also exploit vulnerabilities, where possible, to assess what attackers might gain after a successful exploitation" [9]. Penetration testing is not to be confused with vulnerability assessments as this type of testing only goes as far as identifying a vulnerability and not exploiting them. An organisation conducts security testing for various reasons, mostly they are related to a need to comply with a standard or audit requirement to prove that their systems are secure. Some examples of standards are PCI compliance, ISO 27001, CBEST [10]–[12].

Figure 1: Penetration Testing Execution Standard Phases

There are several methodologies and standards that can be used to provide guidance on how to conduct penetration tests, such as the OSSTMM, ISSAF,PTES and OWASP [13], [14],[15], [16]. As part of a penetration test, each security company or tester will have their own methodology however it is usually aligned to the Penetration Testing Execution Standard (PTES). This standard consists of seven phases [9] (Figure 8). The first phase is a pre-engagement phase [15], where requirements are discussed, and a scope of testing is agreed. The next phase can be an intelligence gathering phase [15]; a customer may provide documentation

for systems in scope or the tester will conduct open source intelligence on the target in order to perform reconnaissance. The next phase is usually a threat modeling phase [15], this phase focuses on what target assets are in scope and what threat actors (2.4.3) are involved. With these two pieces of information a tester can model what potential threats there might be and they will then validate this during the penetration test. No specific model is recommended however attack trees (2.1.2) can be used to map out attacker behaviour and identify the different ways they could reach their goals [17]. An additional activity, once the attackers have been modeled during this phase can be to add scenario-based tests. This is where an organisation can stipulate a specific scenario that they would like the tester to simulate, looking at a specific target or a goal [18].

The phase after threat modeling is Vulnerability Analysis [15]. This phase is the same as a vulnerability assessment where a tester will normally run an automated scanner to find vulnerabilities or misconfigurations. After Vulnerability Analysis is the Exploitation phase [15]. A tester will look to exploit a vulnerability found in the previous phase to provide evidence of the impact of the issue and leverage the vulnerability to get as much access as possible. The tester will need to stay in the scope during this phase and will usually be asked to not exploit an issue if there is a risk of harming the system being tested. This leads into the next phase of Post-Exploitation [15], which involves the tester understanding how valuable the compromised machine is and cleaning up the compromised environment after the test. The goals of the test are dependent on what was defined by the client, for example if they wanted to see if a HR database could be compromised, the tester would rate this issue as high if they were able to achieve this goal. The last phase is reporting [15], where the tester needs to make sure all the findings and evidence are in the report and the recommended remediations are clear enough for the customer to understand. A CVSS score is used to communicate the severity of the issue by using a standard format that everyone can understand (2.1.5).

During a penetration test there are categories that define what type of test it will be and how much knowledge a tester will have beforehand, for instance in a ‘White box’ test a tester will have full access to documentation and credentials [19]. ‘Grey box’ testing involves receiving limited information from the organisation commissioning the test, for instance credentials but limited documentation [19] . ‘Black box’ testing involves the tester having no information on the target, this type of testing best suits a red team testing [19].There are several organisational bodies and qualifications that testers will need to hold in order to have the right training and experience to conduct a good quality penetration test. CREST [20] offer several certifications for companies as well as individuals, there is also the Tiger scheme [21]. Some qualifications are necessary for particular industries for example the NCSC CHECK Scheme is required for organisations with Critical national Infrastructure (CNI) [22].

1.3. Thesis Contributions

The four main goals of this thesis are; to assess a selection of existing threat modeling tools and models, both open source and commercial. The second is to explore the importance of threat modeling during the security testing process. The third is to design the Purple Team Playbook framework that can be used to threat model for the purpose of security testing. The final goal is to create proof of concept scenarios and apply the framework to them and evaluate the effectiveness of the framework. In order to achieve these goals, we will draw upon our own experience as well as pertinent research material. As threat modeling and security testing are both large subjects, we will be selective in the models and tools that we cover in this thesis.

1.4. Thesis Outline

This thesis comprises of seven chapters. In the second chapter we explore what current threat models and tools are currently available and also look at various security testing subjects and tools. In chapter three we looked at the related work for this subject area and how others have attempted to address the problem of threat modeling and security testing. The fourth chapter deals with the main topic of this thesis, which is to design a Purple Team Playbook Framework that can be used for threat modeling and security testing. The fifth chapter applies the proof of concept framework to a set of mock scenarios to establish how effective the framework is when applied to threat modeling and security testing. The sixth chapter includes discussions on how well the playbook works and if it solves the challenges discussed at the beginning of the thesis. The final chapter concludes the thesis and discusses the future work planned for the PTP.

2. Threat Modeling and Security Testing

This chapter provides background information on threat modeling and security testing. In the first section we look at threat modeling tools and techniques in isolation and the second section will look at the subject of security testing.

2.1. Threat Models

In this section we explore a selection of well-known threat models.

2.1.1. STRIDE

STRIDE is a threat classification model and "provides a set of threat categories with definitions so that each identified threat can be categorized in a systematic and repeatable way". The STRIDE approach to threat modeling was invented by Loren Kehfelder and Praerit Garg, it stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege (STRIDE) [5]. This framework and mnemonic was designed to help people developing software identify the types of attacks that software tends to experience [5]. The way the model works is that we will have a system and we will use each word in the STRIDE model to determine if the system is affected by any of these issues. For example, spoofing, if we had a card entry door system and someone were to clone or steal a valid entry card, then this would be a valid threat for a company and would need to be taken into consideration when the product is being designed and created. Table 1 depicts an example of how the model works and the information that can be gathered during the STRIDE process.

Table 1: STRIDE Chart [4]

Threat	Property Violated	Threat Definition	Typical Victims	Examples
Spoofing	Authentication	Pretending to be something or someone other than yourself	Processes, external entities, people	Falsely claiming to be Acme.com, winsock .dll, Barack Obama, a police officer, or the Nigerian Anti-Fraud Group
Tampering	Integrity	Modifying something on disk, on a network, or in memory	Data stores, data flows, processes	Changing a spreadsheet, the binary of an important program, or the contents of a database on disk; modifying, adding, or removing packets over a network, either local or far across the Internet, wired or wireless; changing either the data a program is using or the running program itself
Repudiation	Non- Repudiation	Claiming that you didn't do something, or were not responsible. Repudiation can be honest or false, and the key question for system designers is, what evidence do you have?	Process	Process or system: "I didn't hit the big red button" or "I didn't order that Ferrari." Note that repudiation is somewhat the odd-threat-out here; it transcends the technical nature of the other threats to the business layer.
Information Disclosure	Confidentiality	Providing information to someone not authorized to see it	Processes, data stores, data flows	The most obvious example is allowing access to files, e-mail, or databases, but information disclosure can also involve filenames ("Termination for John Doe.docx"), packets on a network, or the contents of program memory.
Denial of Service	Availability	Absorbing resources needed to provide service	Processes, data stores, data flows	A program that can be tricked into using up all its memory, a file that fills up the disk, or so many network connections that real traffic can't get through
Elevation of Privilege	Authorization	Allowing someone to do something they're not authorized to do	Process	Allowing a normal user to execute code as admin; allowing a remote person without any privileges to run code

The STRIDE model can be very useful during development and Microsoft offers a large suite of security practices and tools as part of their Security Development Lifecycle (SDL) (2.2.1). This means that this is a proven process and there is a lot of support for this model, it can also provide a starting place for developers to address issues before they start coding. On the other hand **"**the drawback of STRIDE is that it is very hard to quantify the cost and effectiveness and also it doesn't generate the list of threats" [23]. STRIDE also does not address any mitigations to the problems we find using this model, so we would need to supplement it with other sources of information.

2.1.2. Attack Trees

Attack Trees were originally developed by Bruce Schneier, who stated that "Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks. Basically, you represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes" [24]. Attack Trees are a logical way of addressing security threats. For instance, if one was worried that someone may break into their house, one could map out the different ways a burglar may succeed, and this will allow us to come up with ways to try and prevent this from happening. In order for the tree to be effective it will need to undergo several iterations until all nodes are found, as a result of this several ways of achieving the same goal may be found [6]. To construct an attack tree, we must start with a root node, this can be the component that prompts the analysis or an adversary's goal [5]. We can then have sub-nodes which will describe how an attacker might achieve the goal, for example how they can break in. The node below can describe how they can achieve the node above, for instance break a window to gain access to a locked door this then achieves the root goal of gaining access. Figure 1 shows an example of the contents of the attack nodes in an attack tree.

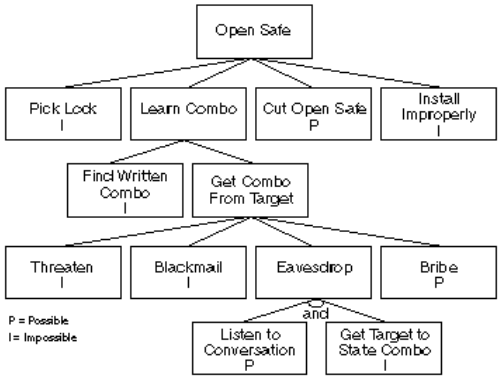


Figure 2: Attack Nodes [8]

Attack trees are cheap to create in terms of costs to a business so they can be good to use to try and understand how to security test a system. They can however be time intensive as they will need to be kept up to date to ensure that they are still relevant in identifying current threats. There is a low barrier to entry as they are similar to mind maps which many people are familiar with and they can be good for brainstorming ideas. There are some things to consider when using attack trees, one of these is the completeness of the model, as threats are continually evolving, how do we know when an attack tree is complete, or can it ever be complete [5]. However, this is true of every threat model as threats can change on a regular basis so there needs to be some scope to evolve in a manageable way. There could be a danger that these

attack trees will become too complicated and therefore lose their effectiveness as a threat modeling tool.

Attack trees can be modified to become attack and defence trees. This is where the trees will consider both attackers and defenders capabilities. These can be helpful to create an understanding of how attacks can be mitigated [25]. This new form of using attack trees still suffers from the same drawbacks as introducing more granularity in the form of defences increases the complexity of the attack trees and depending on the system, they are modelled on they can grow too big to manage properly. When using attack trees or attack defence trees it is important to remember what the purpose of them is, if it is too complicated then maybe another model or tool should be used.

2.1.3. Attack Libraries

Attack Libraries can be useful as they provide a level of granularity that STRIDE does not, as "some practitioners have suggested that STRIDE is too high level and should be replaced with a more detailed list of what can go wrong" [5]. If for instance, an attack tree was growing too complex a library may be useful as it could contain relevant attacks for many systems in an organisation. The way we can create a library is to look at who the audience will be, for instance if it is to be used for the security testing of a system from a specific attacker, then we will need to include a library of known attacks by this type of attacker [26]. We will also need to look at the level of detail we will go into and the scope of the library in order to make it as useful as possible. For a security testing attack library, we will need to know what type of system or network will be in scope and decide how much detail we need on the type of attacks (1.2).

To help with using an attack library we can use MITRE's Common Attack Pattern Enumeration and Classification (CAPEC) to create one. CAPEC provides a large list of known patterns of attacks so that we can understand attackers' behaviours and map each of them to see if they are applicable to your application or network [27]**.** OWASP Top 10 [28] is another popular library and is used heavily in web application security testing as well as for training developers to look out for these issues when they are coding. A paper by Kotenko and Doynikova evaluated the use of CAPEC to generate attack scenarios for network security evaluations and they were successful in doing so. They concluded that the tool they made can be used for penetration testing as the attack scenarios provide useful attack vectors for testers to try and compromise [29].

The use of attack libraries can be extremely beneficial as it can "be useful to those who are not deeply familiar with the ways attackers work" [5]. This goes back to the difficulty with threat modeling and getting people to think like an attacker. Instead of thinking like an attacker there is now a library of known attacks that are publicly understood to help learn and train employees about attacker behaviours. Though attack libraries may have many benefits due to the wealth of information available, it could become overwhelming so it is important that we scope it appropriately or it will be less effective. We also need to maintain the library over time as some attacks may become less relevant and newer ones need to be taken into account. Just like attack trees, this needs to be an iterative approach to stay relevant and mitigate as many new threats as possible.

2.1.4. *Diamond Model*

The Diamond Model of Intrusion Analysis is a paper by Sergio Caltagirone, Andrew Prendergast, and Christopher Betz. In simple terms, the Diamond model shows "that an adversary deploys a capability over some infrastructure against a victim' [30]. The model consists of a diamond which describes an 'event' and 'activity threads' to represent the flow of an adversary. The core features include, who the 'adversary' is, what their 'capability' is in terms of tools and techniques, who their 'victim' is so this would be an asset they are targeting, and what the adversary's 'infrastructure' is [30]. Figure 2 shows an example of how an event would be shown in the diamond; it uses these four corners to show how an attack unfolds.

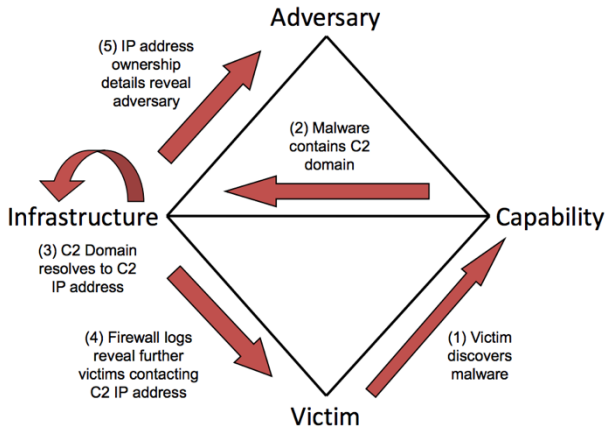


Figure 3: Diamond Model Example [14]

This model is targeted at teams on the defence side of security and they can use this model to map out behaviour of different threat actors and develop defences that will pick up this activity. The diamond model also uses LockheedsMartins Cyber kill chain (2.4.4) to show what events would happen in each phase. The papers authors propose an interesting take on threat modeling and how one can map adversary behaviour in a way that shows the steps of how they gain entry into a system and what their end goal might be. The authors do acknowledge that, as it stands, this is a manual approach to threat modeling and that automating what is modelled with the diamond model is the next step [30]. In comparison to the threat models that we have discussed in the previous sections, the diamond model describes a way of showing how attackers behave in a system. It can be seen as a clearer way to display it than an attack tree and benefits from the use of attack libraries to inform how the model is created. On the other hand, like other threat models, this could become overly complex depending on how many adversaries are being modelled and their capabilities. It is also highly dependent on the capability of the user creating the diamond models.

2.1.5. *Common Vulnerability Scoring System (CVSS)*

The Common Vulnerability Scoring System (CVSS) was developed by NIST and it "provides an open framework for communicating the characteristics and impacts of IT vulnerabilities" [31]. CVSS scores can be used in many different forms, for instance

communicating the impact of a newly published vulnerability in the form of a CVE [32]. It can also be used to show the impact of a vulnerability found during a penetration test (1.2).

CVSS uses three metric groups shown in Figure 3 to calculate the score, these include base, temporal and environmental. The base metrics deal with issues such as the complexity of the vulnerability and the impact on Confidentiality, Integrity and Availability (CIA). The temporal metric includes details on whether there is a valid exploit or remediation for the issue. The environmental metric looks more in depth into the base metrics in order to get some context, for instance the scope of the attack and the importance of the CIA metrics. In order to calculate the CVSS score there is a calculator provided by NIST and it explains what all the metrics mean in order to help the user [33]. Users can use the CVSS calculator to determine the risk of their vulnerability. Like other threat models, the person calculating it needs to have a good understanding of the vulnerability and how it can impact organisations assets.

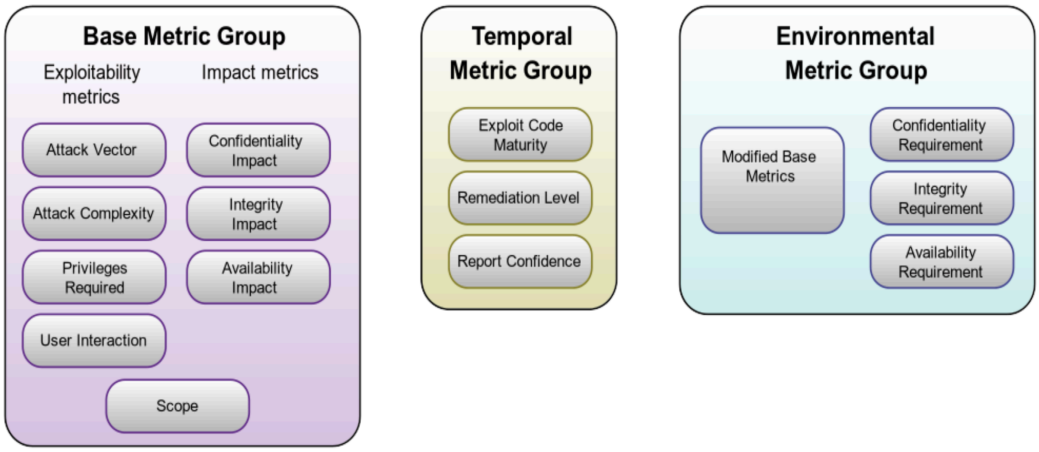


Figure 4: CVSS Metric Groups [18]

Overall, CVSS scores are needed to provide a standard to show how serious the vulnerability is. CVSS is generally not used as a model itself and is usually used with other threat models [6]. For instance, it could be used for assessing the risk of an attack path found in the attack tree threat model. This would let the wider audience know if it needs to be dealt with immediately or if it is low risk. CVSS scores do have the same drawbacks as other threat models, where the score calculated can depend on the level of understanding that the user has on the vulnerability. It also will need to be recalculated for individual organisations as it may be a high overall, but an organisation may have sufficient mitigations in place that lowers the risk which the calculator does not take into consideration.

2.2. Threat Modeling Tools

This section highlights a selection of commercial and open source tools that build upon the models discussed in the section above.

2.2.1. Security Development Lifecycle (SDL)

Microsoft "Security Development Lifecycle (SDL) consists of a set of practices that support security assurance and compliance requirements. The SDL helps developers build more

secure software by reducing the number and severity of vulnerabilities in software, while reducing development cost" [34]. As part of this lifecycle, threat modeling has five major phases 'define, diagram, identify, mitigate, validate' [5]. To facilitate the threat model they have their own threat modeling tool which uses their STRIDE model to assess threats [35] . The result is a visual representation in the form of a data flow diagram (DFD) that can help a project team during development to mitigate risk.

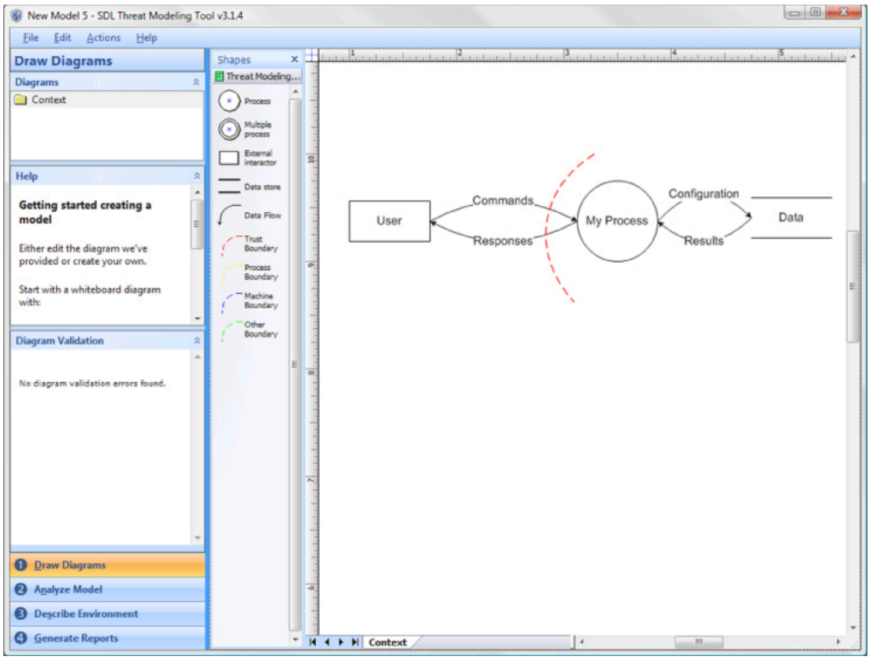


Figure 5: SDL: Draw Diagrams Tool [5]

2.2.2. EOP Card Game

Microsoft have created a card game called 'Elevation of Privilege' (EOP) which uses STRIDE threats as the card 'suits'. We will need a system to model first and then we will use the cards to go around the table and play the game, and the winner gets more points if they achieve 'elevation of privilege'. The cards "provide structure and hints to the beginner, enabling new players to find a threat based on the cards in their hands" [5]. It can be a nice informal way to introduce people to how threat modeling works and gets them thinking in a creative way to solve a problem. Since the game was developed an online version has been created and is available on GitHub [36].

Figure 6: EOP – Threat Modeling Card Game [20]

A paper on the effectiveness of the EOP game by Tondel and Oyetoyan concluded that the game was good for people to learn about security and encouraged good security discussions as a result of playing the game [37]. It was noted that it may not be suitable in all circumstances as it can take time to play and it would only work for some projects [37]. Some organisations may choose this card exercise to help users think about what security threats there could be. However, something more formal will need to be in place in order to threat model effectively so EOP should not be used in isolation.

2.2.3. Tutamantic Tool

Tutamen Threat Model Automator is a solution from the company Tutamantic that is made to be used when an application is being designed to help identify threats automatically [38]. It uses what it calls taxonomies which includes OWASP Top 10, STRIDE, Common Weakness Enumeration (CWE) and Common Attack Patterns (CAPEC). There is limited documentation on the way this threat model automater works but it seems like an interesting tool if it is able to automate the process of using different threat models and attack libraries. This is also proof that not one threat model will fit all business needs so commercial tools need to accommodate to this.

2.2.4. ThreatModeler Tool

The ThreatModeler tool "is an automated threat modeling tool that strengthens an enterprise's SDLC by identifying, predicting and defining threats across all applications and devices in the operational IT stack" [39]. It uses a set of attack libraries, including the MITRE CAPEC [5]. Like the Tutamen Threat Model Automator it is also a threat model automation tool. The use of ThreatModeler may be deemed attractive to large organisations as it is a product that has been adopted by many organisations and there would be experts available to support the threat modeling process. There was however an article based on a report by Gartner they "estimate only 10% of organizations routinely include formal threat modeling as a part of their

development process. We see this trend changing quickly, though, with automated enterprise threat modeling continuing to be the driving force behind greater adoption and implementation of threat modeling in 2018" [40]. Although this tool may be useful it can be very costly, so organisations may opt for something inhouse and create their own tool to suit their needs.

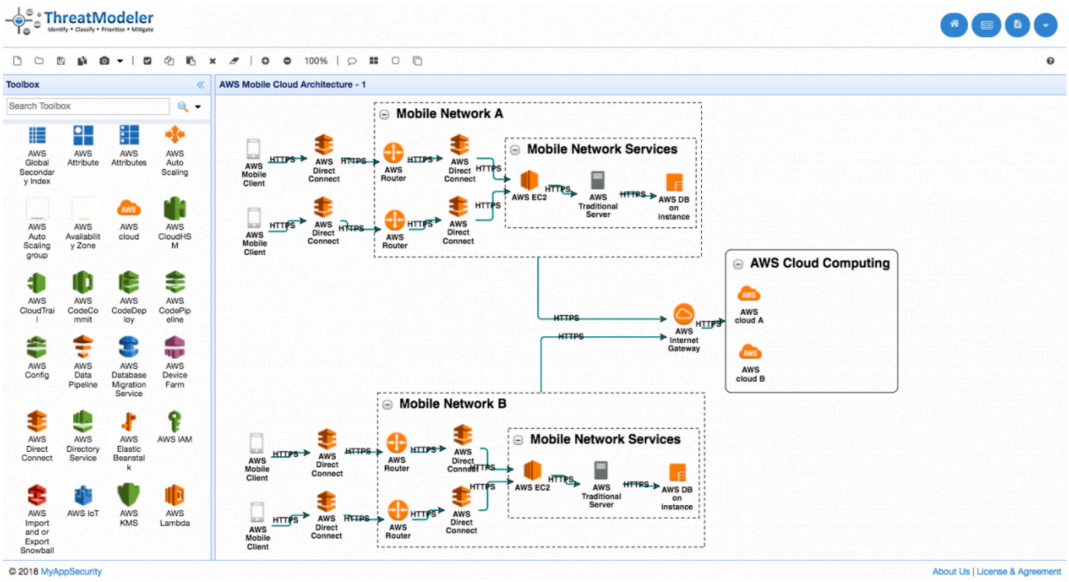


Figure 7: ThreatModeler Model Template [24]

2.2.5. Seasponge Threat Model Tool

Seasponge is a tool created as part of a Mozilla project. It provides a threat modeling tool using the user's browser so nothing will need to be installed. It "allows one to quickly and easily diagram a system and its data flows and begin the important work of focusing on threats" [41]. The ease of use of this tool is attractive as we do not have to install it and we could also customise the modeling menu items, so they suit our purpose for a particular model. This tool could provide a low-cost way to show what threats an organisation may have. The person creating the model will need to have sufficient knowledge on the organisations infrastructure in order to create a valid model. There is the potential that this tool can be easily customised, for instance to include attack library entries, such as CAPEC and the Mitre ATT&CK (2.4.5) framework.

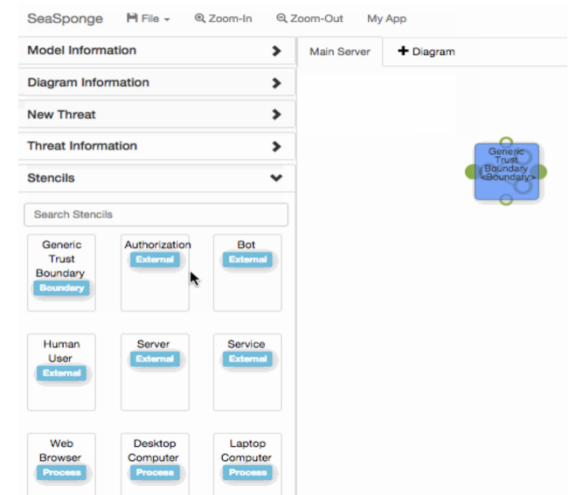


Figure 8: Seasponge Threat Model Tool Example [25]

2.3. An Analysis of Existing Threat Models

In the previous two sections we have discussed a selection of current threat models and the tools that organisations can use to threat model. What we have covered is by no means an exhaustive list of all models and tools. For instance there are other models available, such the Process for Attack Simulation and Threat Analysis (PASTA) model, which is a risk-centric model "that centers on developing countermeasures commensurate to the value of the assets being protected" [17]. There is also the Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance (LINDDUN) model which focuses on modeling privacy concerns in data security [6]. In Table 2 we have summarised the main findings of all the models we discussed in in section 1.1. We talk about the advantages and disadvantages of the models and what conclusions we have made about the models.

Overall, we have found that threat modeling is important during the development process as well as for established systems. It is clear to us that time and expertise needs to be invested in it in order for there to be a valid and useful threat model for an organisation. Threat models also need to be maintained and it is important to pick the correct model for your organisation's needs as there is no recommended threat model that an organisation should use [6]. In regard to the tools an organisation may invest in this will be dependent on the cost and functionality of the tool. They may decide that a tool that offers other functionality such as threat modeling and security testing may be a better investment overall (1.4.8).

Table 2: Threat Models Summary

Models	Advantages	Disadvantages	Conclusions
STRIDE	❖ It is a mature model that is used in Microsoft products. ❖ SDL is part of the security development lifecycle, so security issues are found early in development.	❖ Does not generate a list of threats therefore it does not provide a level of granularity ❖ Need expertise to identify the threats. ❖ No mitigations are provided as part of this model.	Well defined for use in the SDL but might not always be suitable other models may be chosen instead of STRIDE and they take into account mitigations.
Attack Trees	❖ Easy to use. ❖ Logical. ❖ Cheap to construct. ❖ Shows pre-requisites of an attack.	❖ Maintenance of the trees ❖ Can get too complex and lose their effectiveness ❖ We need the knowledge and expertise to construct trees with real value.	Simple and effective sometimes but can become complicated so there needs to be an automated way to do this perhaps. Or a way for it to be easily maintained.
Attack Libraries	❖ Knowledge base of attacks ❖ Good for different types of audiences.	❖ Overwhelming for someone who is less knowledgeable so it may lose its effectiveness. ❖ Maintenance of the library.	Attack Libraries provide a wealth of knowledge on threats, but we need to know how to use it for it to

	❖ Level of granularity on threat actor capabilities and techniques.		be effective. Also, by itself it's not clear how this impacts an organisation, so it needs to be used in conjunction with another model or tool.
Diamond Model	❖ Adversary and goal focused. ❖ Compatible with the Cyber Kill Chain.	❖ Could get overly complicated. ❖ Manual Model at the moment. ❖ Maintenance of the Model.	This model provides a way to map threat actor behaviour and establish what their ultimate goal is. This can be used during red teaming testing to model adversary behaviour.
CVSS	❖ Universal language to understand the risk of a vulnerability. ❖ Has a calculator that can be used easily by anyone.	❖ The person calculating the score must have sufficient knowledge in order to assess it appropriately. ❖ It is not an appropriate model to use in isolation as it only deals with scoring and not identifying threats.	This provides a universal way to communicate and calculate the risk of a vulnerability which is a good way to highlight the risk of an issue. CVSS scores need to be used in conjunction with another model so that threats can be identified before they are rated.

2.4. Security Testing

In the first sections of this chapter we looked at different types of threat models and the tools currently available that facilitate threat modeling, this section follows on from chapter one where we introduced what is involved in a security test. We will focus on a selection of security testing subjects and tools that organisations can use.

2.4.1. Red Teaming

"Deriving from the Cold War, the expression 'red team' among the military is often used to describe a way to think outside the box and to be able to anticipate and model adversarial behaviour" [42]. Standard penetration tests aim to find and exploit vulnerabilities for the targets in scope and follow a methodology like the PTES (1.2), whereas a 'red' team is more goal orientated and looks at the organisation as a whole and how attackers can get in [43]. A report from the NATO Cooperative Cyber Defence Centre of Excellence defines a cyber red team as having four main phases (Figure 9).To conduct a red team test the testers will need to have a signed a rules of engagement contract to protect them if anything goes wrong and this will stipulate the activities that are in scope for the test [44]. As part of this test the internal security operations team also called the 'Blue' team, the defenders of an organisation, will have no prior

knowledge of the red team testing [7]. The goal is to see how the blue team respond to the red teams attack, this is beneficial as it tests an organisations response and identifies areas they need to improve on.

Red Teaming uses a holistic approach as the red teamer can use any means necessary such as exploiting process, people or systems to gain access to an organisation [45]. For example, a red team tester can use social engineering to get an employee to click on a link in order for the tester to gain a foothold on an organisations network. These kinds of activities would not be permitted in a normal penetration test engagement as the scope would be a lot tighter and would restrict these activities. Red team tests can take a long time to conduct and they are costly, due to the fact that one will most likely have to hire a third party with the relevant experience to ensure that the red team is successful [46].

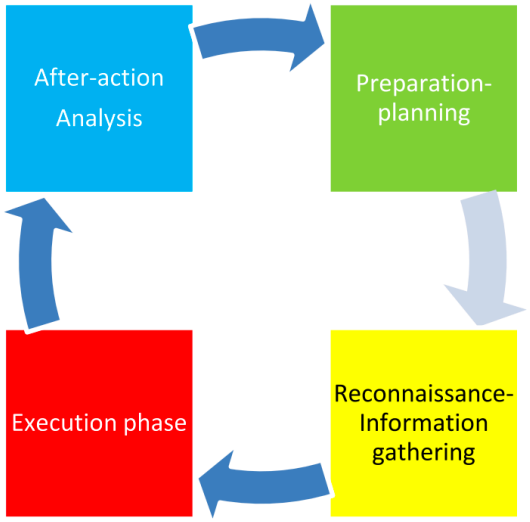


Figure 9: NATO Four Main Phases of a Red Team [42]

2.4.2. Purple Teaming

Purple Teaming "improves the skills and processes of both the red and blue teams by allowing them to work closely together during an exercise to respectively attack and defend a particular target" [47] . This involves the red team conducting a test like they usually would (2.4.1) but instead of the blue team being unaware they will work together to enhance the results of the test. A purple team can be seen as more cost effective as it can identify many avenues into an organisation and allows the blue team to create defences based on the red teams simulated attacks. It also helps enable a collaborative relationship between the two teams so that they push each other to evolve their capabilities for the good of the organisation [48]. In order for a purple team test to be successful an organisation needs to understand what they want out of the test and have a good understanding of their security posture [44]. They will also need to have employees with the relevant red and blue team experience to be able to simulate and detect the attacks.

2.4.3. Threat Actors

During the threat modeling phase of a penetration test, a tester will need to understand what type of threat actors may be targeting an organisation and what their capabilities are. Threat actors are attackers that have an interest in attacking an organisation, their motivations for doing so can vary greatly [49]. Threat actors can be split into groups such as 'Script kiddies', 'Hacktivists', 'Nation State', 'Organised Crime' and 'insiders' and Advanced Persistent Threats (APT).The 'script kiddie' actor is usually a low-level attacker and their motivation for hacking an organisation is for fame and recognition. The company TalkTalk are a good example of a data breach caused by a 'script kiddie', as they were caught out by a SQL injection attack which is a well-known web application attack that has been around for many years [50]. This attack is part of the OWASP Top 10 web application attacks, and this story reinforces the point that organisations should be getting security basics right first or they risk being an easy target for a low skilled attacker. Another threat actor would 'organised crime', their motivation is predominately financial the same as a bank robber would act against a conventional bank [49]. Financial organisations would be particularly interested in protecting themselves against this actor as loss of money could have an impact on their business and reputation.

Nation state actors are probably the most sophisticated of all the actors as they are funded by foreign governments and are politically motivated [51]. The 'insider' threat actor is probably one of the hardest to protect against, as an insider by definition is in a trusted position in an organisation [52]. They are also a difficult actor as their motivations can vary, it could be that they are financially motivated, they are being blackmailed, or they are just careless. An organisation can try to protect themselves by conducting background checks such as looking at their financial history or their conflicts of interest. Advanced Persistent Threat (APT) actors, are deemed to be sophisticated actors that have a lot of resource and expertise. Other characteristics of this actor include having a particular goal that needs them to remain persistent so they will use stealth and evasion techniques in order to achieve this [53]. This actor is usually a nation state actor or an organised crime threat actor as they will usually have the necessary sophistication and funding to have the skills to stay persistent on a system.

2.4.4. Cyber Kill Chain

The Cyber Kill Chain established by the company LockheedMartin, provides a way to model adversary behaviour so that that organisations can detect and prevent threat actor activity, the chain shows the activities the actor must fulfil in order to achieve their objective [54]. The kill chain consists of seven phases shown in Figure 10. The kill chain is a popular way to show the phases of an APT attack, as it provides information on their techniques at each phase and guidance on how to defend against the attack [53].

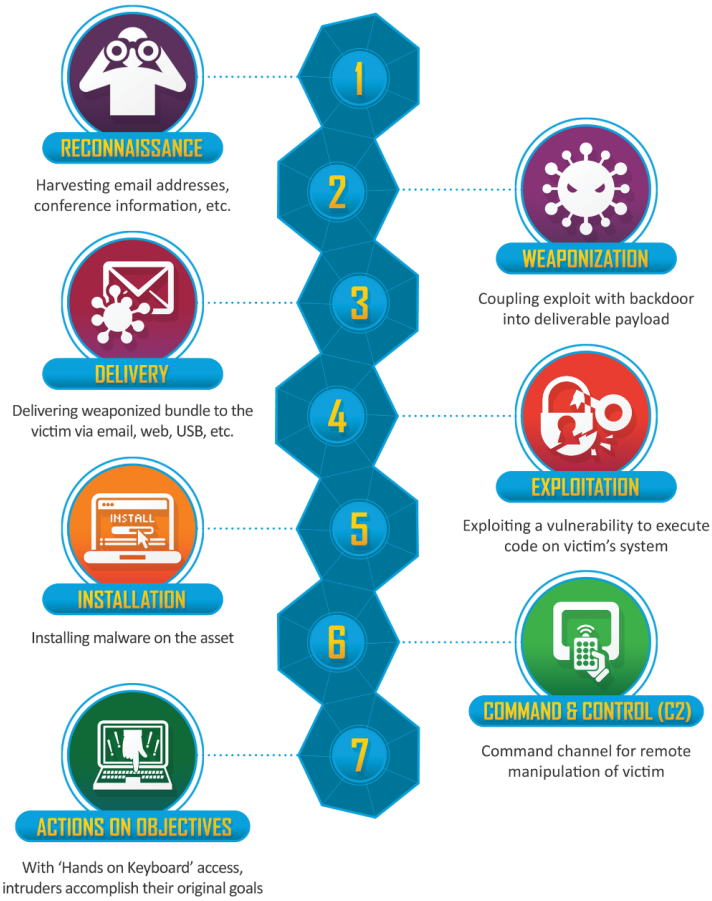


Figure 10: Lockheedmartin Cyber Kill Chain [54]

2.4.5. Mitre ATT&CK Framework

The Mitre ATT&CK framework is a "globally-accessible knowledge base of adversary tactics and techniques based on real-world observations" [55], it can be used for threat modeling in an organisation and can be categorised as an attack library (1.1.3). This framework is widely used in the security industry and organisations can conduct red teams based on the data in this framework [56]. In Figure 11 we show an example of the ATT&CK tactics that are covered in the framework. The framework includes, adversary details, tactics, techniques and mitigations. Mitre have created many tools that complement their framework, for instance they have an attack navigator that allows users to plan a security test by pulling data from their framework (2.4.7).

Tactic	Number	Description
Persistence	51	Any access, action, or configuration change to a system that gives an adversary a persistent presence on that system Examples: Bootkit, Hypervisor
Privilege Escalation	27	The result of actions that allow an adversary to obtain a higher level of permissions on a system or network Examples: DLL injection, Web shell
Defense Evasion	34	Techniques an adversary may use to evade detection or avoid other defenses Examples: Binary padding, File deletion
Credential Access	18	Techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment Examples: Credential dumping, Input capture
Discovery	17	Techniques that allow the adversary to gain knowledge about the system and internal network Examples: Network service scanning, Query registry
Lateral Movement	17	Techniques that enable an adversary to access and control remote systems on a network and could, but do not necessarily, include execution of tools on remote systems Examples: Pass the hash, Windows Remote Management (WinRM)
Execution	25	Techniques that result in execution of adversary-controlled code on a local or remote system Examples: PowerShell, Windows Management Instrumentation (WMI)
Collection	13	Techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration Examples: Audio capture, Clipboard data
Exfiltration	9	Techniques and attributes that result or aid in the adversary removing files and information from a target network Examples: Data encrypted, Scheduled transfer
Command and Control	19	Represents how adversaries communicate with systems under their control within a target network Examples: Data encoding, Uncommonly used port

Figure 11: Mitre ATT&CK Categories of Tactics [57]

2.4.6. Challenges with Security Testing

There are many challenges associated with running a successful security test. One for instance is the view that traditional penetration testing does not factor in the whole organisation's security posture and how they deal with attacks [43]. This has led to the need for red team testing as this type of testing looks at the whole organisation and where it is vulnerable and tests the incident response capabilities. Also, it was found that there can be a disconnect between the defenders (blue team) in an organisation, and the attackers (red team). This is a problem as if the threats are not being properly communicated they cannot be mitigated appropriately [57]. This supports the need for purple team testing where both of the teams work together to protect an organisation.

A paper on whether penetration testing should be standardised raised the issue of the quality of penetration testing [58]. The authors found that testing companies did not always provide enough information on findings, and it would be more beneficial to explain exactly how the issue came about and how it can be a problem. Providing more information would help organisations better understand and fix the issues in future releases. Related to this the authors found in their research that testing companies were reluctant to provide proof on concepts for issues, this could be due to the fact that they want us to pay extra for a retest [58]. This however has a negative impact as it was found that organisations were less likely to fix the issue, they did not understand it fully or could not easily recreate it.

There seems to be balance between how much an organisation is willing to pay as well as how much data a testing company is willing to give. It is also important to pick the right testing

company with testers that have recognised credentials [19], or there is a risk of not getting a good quality test with relevant findings. There is no guarantee that a tester will find all the issues, which is why systems will need to be retested in the future, but a well-known testing company will have a higher success rate. From a threat modeling perspective this could prove damaging to an organisation if they are too reliant on third party testers and do not fully understand their threats.

2.4.7. An Analysis of Existing Security Testing Tools

In the sections above we have spoken about the different types of security testing and looked in depth at penetration testing and red and purple team testing. In Table 3 we have chosen a selection of open source and commercial tools that are used to security test and threat model a system. We have summarised what the tool is and what the potential advantages and disadvantages of the tools are based on our research. There are of course many tools available for security testing purposes, we have selected a few tools that fit with the theme of this thesis; threat modeling and security testing.

Table 3: Related Security Testing Tools Summary.

Tool	Description	Advantages	Disadvantages
Attack-Tools	Attack-Tools is a GitHub open source project that uses the Mitre ATT&CK Framework to create an adversary emulation planning tool. It offers a tool where we can plan as well as a data model that we can query from. Its purpose is to help people integrate their own tools with mitre using the data model they have created [59].	The data model is useful to query the data off of as it uses the mitre attack framework	The planning tool needs to be customised to be used for an organisation. It is also an open source tool so there is limited documentation and no support.
Caldera	Caldera in an automated red team adversary emulation system that has been created by Mitre, they use their ATT&CK framework as their adversary model and have presented a paper of the tool [60]. Mitre have detailed documentation on how to setup and use the tool [61].	This tool is good for blue teams as they can automate attacker behaviour, and this will in turn show them the telemetry they need to test their detection capabilities as well as regression test their capabilities.	There is a steep learning curve associated with setting up and using this tool. It is also an open source tool; therefore, no commercial support is available. This therefore may be an issue for an organisation to deploy it on their network.
Mitre Attack navigator/ Mitre Caret	Mitre have several open source tools that users can use to leverage their ATT&CK framework. One of which is the ATT&CK navigator, this allows users to pick what techniques and tactics they would like to cover and export it as a JSON or excel file [62]. Another tool is Mitre Caret, which leverages data from their analytics repository (CAR) and the ATT&CK	Security testers can use these tools to plan their tests, they are open source tools, so they do not have any cost associated with using them. The tools are created by Mitre which are well-known in the industry so the data can be deemed as trustworthy.	The tools need to be customisation to be used in an organisation, by itself its more of a reference tool.

	framework. “CARET is used to develop an understanding of defensive capabilities and to aid in their development and use“ [63]. It is currently a proof of concept application that is available to everyone.		
Palo Alto playbook	This open source tool has been created by Palo Alto networks, it is a playbook viewer of adversary behaviour that maps to the Mitre ATT&CK framework. It organises the techniques and tactics of each APT using the Cyber Kill Chain and allows the user to select and find out more information on the viewer [64].	Its main purpose is to create an adversary playbook that can be used to help defenders of an organisation understand how the adversaries work. They can then develop capabilities to detect and respond to the APT activities.	It is not tailored to an organisation and is more of a generic reference tool that’s users can use to find out information on certain APT threat actors.
Vectr.io	Vectr is a purple team threat simulation tool that has been created by the company SecurityRisk Advisors, it offers a free open source community edition for everyone to use [65]. The company Digital Shadows reviewed this tool and found that users can create fully customisable test cases and the adversary simulations map to the Mitre ATT&CK Framework [66]. This tool can be used to plan, track and monitor all purple team activities in an organisation.	This tool is opensource and facilitates organisations in conducting purple teaming assessments. It is customisable so we can use any attack library or test cases we want in the tool.	There is a learning curve when a user first uses the product. It is also an open source product so organisations may choose to go with a purple team tool that comes with commercial support and guidance.
Scythe.io	Scythe is a commercial purple team simulation tool, its functionality is very similar to Vectr and uses the Mitre ATT&CK framework to simulate attacker behaviour [67].	This is a commercial tool so will have documentation and support. It also helps a team simulate purple team assessments and keep track of the results.	There is a cost involved with this tool so this will need to be taken into account. Also, extra costs may be incurred to customise the tool to suit an organisation’s needs.
XM Cyber	XM Cyber offer a commercial tool that can be used by organisations to automate their red team activities. It allows users to create and track tests and run them simultaneously [68]	This tool allows organisations to easily automate red team activities so that they can identify gaps in their testing. This also facilitates purple team testing.	There is a cost involved with this tool so this will need to be taken into account. It also

3. Related Work: Threat Modeling and Security Testing

There are many academic papers that address the parallels between security testing and threat modeling, they each provide different ways in which we should address this issue. This section evaluates a selection of current papers on this subject and we critically analyse what the authors have found against what we have discussed about threat modeling and security testing in the previous chapters.

3.1.1. Cyber Kill Chain and the Diamond Model for Security Testing

In the previous chapter we discussed the diamond model (2.1.4) a paper published on this subject uses the diamond model and the cyber kill chain to map out how the Microsoft Advanced Threat Analytics (MS ATA) solution detected threats [69]. The authors conducted experiments using the MS ATA to understand how intruders get in and persist in a system. They concluded that by using the diamond model and the kill chain phases to translate what the MS ATA tool had detected they could convey their message across more effectively as they could show this step by step process [69]. This paper raises an interesting point about how we can use a threat model to raise awareness about issues. It is important that models can be translated and read by different audiences so that it can be dealt with effectively. This problem was raised in the paper on whether pen testing needs to be standardised [58] where they explain that being able to get the point across in a way that people can understand is a difficult thing but is required if we want to make sure an identified threat gets mitigated.

Several other pieces of academic work also use of the diamond model and the kill chain as the model of choice. H. Al-Mohannadi et al. discuss the use of the diamond model, kill chain and attack graphs for use in planning how to respond and understand a cyber-attack [70]. The authors conclude that the use of these three models is useful as the diamond model identifies how and why an attack took place. The kill chain gives more detail on how an attack can happen and the attack graph shows all the ways an attacker might try and attack an organisation. M. Khul et al. discusses the use of an Attacker Behaviour Model (ABM) in order to conduct cyber threat assessments [71]. The authors believe the model they propose is needed to provide a more pro-active, rather than a reactive approach to security assessments. The ABM they have created models an attacker's, intent, opportunity, capability, preference, and uses the Cyber Kill Chain to show the phases of attacks. The framework they have created models attacker behaviour based on real cyber-attacks and theoretical attacks and their paper provides data on how the attacker attacks a network [71]. They conclude that their framework simulates how attackers and defenders interact with each other by using the ABM to simulate attack behaviour and build up attack data for future analysis.

3.1.2. Attack Trees and STRIDE for Security Testing

In the paper 'A threat model-based approach to security testing' [72], the authors try to automate the generation of security testing test cases with the use of attack trees. In order to do this, they also use the STRIDE model. At the end of the study the authors found that their threat-modeling security testing approach can be effective in finding unmitigated threats [72]. It benefits from the advantages of using attack trees where one can map adversary behaviour to try and find vulnerabilities and how it affects other systems. The authors do however acknowledge that the methods they propose suffers from one of the pitfalls that threat modeling has which is it needs the users to have the correct knowledge to create the correct attack tree. It

also suffers from the limitations of using STRIDE where it lacks the granularity of the threats and is confined to the parameters of the STRIDE options.

Another paper entitled 'A threat model driven approach for security testing' explores the use of the Unified Modeling Language (UML) used in software development [26]. The authors discuss that during software development UML diagrams can be used to threat model, for instance a UML sequence diagram describes the system interactions. From a threat perspective we can use this to understand where the weaknesses are and apply the threats that could impact this process. The paper comes to the conclusion that using UML diagrams could become widely accepted as UML is already an accepted software design language, so they believe it would be easy to apply to a real-life scenario [26]. As we have discussed in the threat modeling chapter in this report, a security testing model using UML will still need to have someone with experience modeling and it will need to be continuously maintained. A normal UML diagram used for design purposes is unlikely to change as much as a security UML diagram will need to. The authors recognise that there needs to be a repository of knowledge formulated by security professionals to aid this process so that security engineers can use this security testing threat modeling tool [26].

In the paper 'Security Attack Analysis Using Attack Patterns' the authors discuss looking at the holistic view which includes people as well as technology in security [73] . The paper uses CAPEC patterns (2.1.3) to look at attack strategies and behaviours and model these against the whole organisation. The authors conclude that using CAPEC works with a small number of patterns as it will have less of an impact on employee resources, however it becomes unmanageable with larger number of patterns. This is an issue with many threat models as there is always a risk that they become unmanageable and therefore lose their effectiveness (2.3). The authors propose a semi-automated approach in order to try and compensate for this issue.

3.1.3. Automation for Security Testing

D.Miller et al from the company Mitre discuss in their paper how it is possible to automate red team activity through the use of the tool they have created called Caldera [60]. The authors discuss the benefits of red teaming in organisations which we have discussed in the previous section (2.4.1). However, they also recognise that there are significant overheads involved in conducting a red team, these include cost, time and the having testers with the right experience, so it is not feasible to perform this activity on a regular basis. The paper aims to help solve this issue by bringing about consistency into red teaming and aid the process of setting up an internal red team function where red teams can be run at any time if required. The framework that feeds into Caldera is based on their Mitre ATT&CK (2.4.5) framework which maps APT techniques and tools. Overall this paper covers in detail how an organisation can use Caldera to automate their red teaming activity and it could also be customised to add techniques not covered in the Mitre ATT&CK framework. Pwc published an article on how they used Caldera and their SIEM solution Tanium, they found it was useful for testing their detection capabilities and their response processes [74].

S. Randhawa et al. proposes another automated red-teaming system called 'Trogdor', which uses a model based Automated Cyber Red Team (ACRT) and "critical node analysis to visually present the impact of vulnerable resources to cyber dependent missions" [75]. The AI planner in the tool allows a user to generate attack graphs of an environment and the use of the visualisations it offers allows users to identify mission-critical artefacts. Trogdor supports the use of the cyber kill chain and has a custom-built plan library so that they can map adversary

behaviour [75]. Trogdor, unlike Caldera is currently a research prototype, they do however share similarities in the fact that they were both made to enhance red teaming. Trogdor looks more at the mission critical aspects of an organisation to simulate adversary behaviour.

H. Ray et al. describe an attack model that can be used for automated red teaming through the use of "UML-based use cases, sequence and state-chart diagrams, and XML to depict an attack, attacker, and defense methods" [76]. The attack model the authors propose should be able to get information on the attack's functionality, attackers' profile and the best way to defend from an attack. This is similar to the way Caldera uses the Mitre framework to simulate attacker's behaviour. The authors conclude that their model allows red team to document security attacks and this in turn aids developers in creating automated attacks [76].

3.1.4. Other Security Testing Models

Authors, Y.Kim and W.Park have written a paper on a prediction model for intrusion detection events so that they can detect the threat of APT attacks sooner [77]. They found that there is a correlation of intrusion detection events that can be used to create predictions and they address the issue with the use of time-series predictions. The authors conclude that in order for an intrusion detection prediction engine to work it must satisfy three requirements. These are that they can only base a prediction on an environment where there are no technical issues, the availability of usable data and that the operating system is appropriately equipped [77]. Another paper on the subject of using predictive models, proposes a model for insider threat mitigation instead of APT attack detection. Authors F. Greitzer and D. Frincke propose a conceptual model for predictive modeling, this includes what data is processed, what one can observe from the data, an indicator which is an action or event and the behaviour of the actor [52].

A paper by the Mitre corporation entitled 'Playbook orientated cyber response', discusses how a playbook of activity may be used to help analysts respond to security incidents [78]. This paper is not directly related to the subject of this thesis as it deals with blue team activities, however this paper contains an interesting idea of using a playbook to communicate information. The authors provide a framework on how to create the playbook and conclude that playbooks can help with knowledge management and automation so that security operation teams can act consistently and quickly in the event of an incident. A knowledge repository that is needed for a playbook of this type would provide a good way to solve a threat modeling weakness. In the previous chapter, we concluded that threat models are only as good as the knowledge and experience being used to create it, if there were to be a repository of knowledge this could help bridge the gap between less knowledgeable users to more experienced users.

V. Veksler et al. presented a paper on using cognitive modeling to understand attackers, defenders and users in an organisation [79]. They discuss that a cognitive model is like behavioural modeling and can be used to simulate the network behaviours of users and attackers. They conclude that simulating human cognitive process is a good way to predict "user error and negligence, defender best-practices, most likely attack behaviour, and ultimately, network vulnerabilities" [79]. This way can also be used for training and to aid security research in the future by understanding the relationships between all the users on a network.

3.2. Analysis of the Related Work

In this chapter we looked at a variety of recent academic research papers on the topic of threat modeling and security testing. It was clear from our research that there are many ways threat models can be applied to security testing and there are no single models that suit all organisation's needs, so organisations need to consider what is best for them [80]. We found that a lot of research tends to favour the use of the cyber kill chain (2.4.4) in their models to show how adversaries move though a system or environment. This addresses a challenge with security testing where we found that communicating testing results is important as if we cannot explain the impact of the issue it may go un-remediated (2.4.6). We also noticed that the use of UML is a popular choice for the purpose of modeling for security testing. This may be because UML is a universal design language, so developers know how to read these diagrams.

We also found that automated red team testing (3.1.2) was a popular way to address the challenges with red teaming. As it can be a costly and time-consuming operation, an automated tool would provide many benefits for organisations. In order to successfully automate the planning and running of red team tests the correct information needs be used for it to be effective. Organisations may also be concerned with running automated tools on their production systems as there is a risk it could affect normal operation. From our research we also found that many models favoured the adversary led models, for instance using an Attacker Behaviour model to understand what attackers normally do on a system and what tools they usually use. Some papers also looked to correlate the data they have on APTs to predict what they might do and make sure that they are ready for them.

During our research we discovered that it was difficult to find papers on the subject of threat modeling and purple teaming. We discussed purple teaming in the second chapter (2.4.2), it is where the attackers (red team) and the defenders (blue team) in an organisation work together in order to identify and protect organisations against threats. We believe this is beneficial for the evolution of threat modeling in an organisation as both teams working together can find gaps that may have previously gone undiscovered. This thesis addresses the lack of current research on purple teaming and threat modeling and builds a framework that organisations can use to conduct this activity. We focus on how organisations can use the available data they already hold and put it all in the centralised place so that issues are easier to identify. In our research we have seen how a playbook can help the blue team with their incident response capabilities (3.1.3) and how they benefit from the consistency of using a knowledge base for their playbook. We believe that we can benefit from the use of a playbook for both red and blue teams to help with security testing. In the next chapter we will detail how the framework has been designed and how it can be used for threat modeling and security testing.

4. Designing the Purple Team Playbook Framework

In the previous two chapters we explored how we can threat model and what is involved in a security test. We also looked at current research on how threat modeling and security testing can be conducted together. We found that there are many challenges with threat modeling and security testing, we also found that there was not a lot of academic research on the subject of purple teaming and threat modeling. In this chapter we explain the different elements of the Purple Team Playbook Framework design.

4.1. Purple Team Playbook Framework

Our framework, the Purple Team Playbook (PTP) addresses threat modeling from the perspective of the red and blue teams in an organisation to be used in the security testing process (1.2). The purpose of conducting various types of security assessments is to ensure that we can protect and detect if an attacker has breached an organisation. APTs (2.4.3) rely on stealth and are harder to detect, so security testing needs to evolve in order to match the pace they are working at. By centralising the knowledge in the PTP and getting internal red team testers and blue team testers working together we can better understand where an organisation is currently and identify where the gaps are in testing. This framework also allows an organisation to fully understand what data they need to hold in order to threat model effectively. They could of course purchase commercially supported tool that may do the same thing, however they still need to design and decide what data they want to leverage and what they want out of the tool. This framework shows organisations how they can use their own data to understand what threat actors are targeting them and how they can use this to security test their systems.

In Figure 12 we demonstrate how the framework works and what data is included in it as well as some examples of commercial tools that can be used. In the first section of the diagram the ‘Data Feeds’, we need to make a decision on what data we have and can be used to feed into the framework. We have picked a selection of data that an organisation will most likely hold, this can however vary dependant on the type of organisation. This part of the framework can be automated using a data ingestion engine, for instance pulling data from an API and dropping it into the database using Powershell or an ETL (Extract Transform and Load) application. This data is collected and fed into the databases in the next section. In the ‘Data Models’ section, we split the data that is ingested from the data feeds into four datasets. One of the datasets is for red team data, which includes past details on tests that have been run and are planning to be run. Also, any remediations that have been proposed to fix any security issues found in the security tests and data on what security tools are being used. The organisation dataset stores the data that is needed to describe the status of all the organisations assets. For example, how important the asset is, and the permissions required for the application. This is an important dataset as if the data is incorrect this could have an effect how we model the threats for the whole organisation.

The Blue Team Data provides all the information that has been gathered from their detection tools. They usually use a Security Information and Event Management system (SIEM) this collects “security events from many diverse sources in enterprise networks, normalize the events to a common format, store the normalized events for forensic analysis, and correlate the events to identify malicious activities in real time” [81]. The team can create custom use cases that can they can use to identify attacker behaviour on their network, the SIEM tool Splunk is an example of a tool that offers this capability [82]. All these Datasets feed into the Purple Team Playbook Dataset, this is the main dataset that is used in the framework

to threat model from during the security testing process. By combining the three datasets we can get a good picture of what assets are important and where there are gaps in the testing and security controls of the assets. In the section (4.2.2) we will discuss in more depth with the aid of a database diagram data model to show what data will be stored in the Purple Team Playbook. The applications (4.2.3) part of the diagram shows how the users will interact with the Purple Team Playbook. The user can use data visualisation software and connect it to the Purple Teams Playbook Knowledge base database. This gives the user freedom to search and show the data in any way they would like and create dashboards to model the data. A user can also use the Purple Team Playbook Web Application, to view the data in a pre-defined way and to update the playbook. We will discuss more about how the application will work and look in section 4.2 of the thesis.

4.1.1. Purple Team Playbook Audience

Threat modeling affects the whole organisation and employees will have varying levels of experience and knowledge. This playbook is primarily targeted at Security Analysts wishing to conduct security tests such as penetration tests, red team or purple team tests. It can be used during the threat modeling phase of a penetration test (1.2) to understand what capabilities the threat actors have and how they can simulate them. It can also be used to show the impact of a vulnerability found during a security test to ensure that it is appropriately risk assessed against the whole organisation. For instance, if one analyst knows of a threat it may be difficult to fully understand the impact if there is not a centralised place where all the knowledge is based. It also provides a platform to encourage innovation, as threat actors become more sophisticated it makes sense that organisations will need to try and keep up.

We also believe that this tool could be used by less technical users as an aid to fully understand the results of a security test (2.4.6). As business users are primarily the drivers for providing funding for vulnerability remediation, we need to find a way to communicate the impact of an issue and provide them with statistics on how effective security testing is having on the organisation.

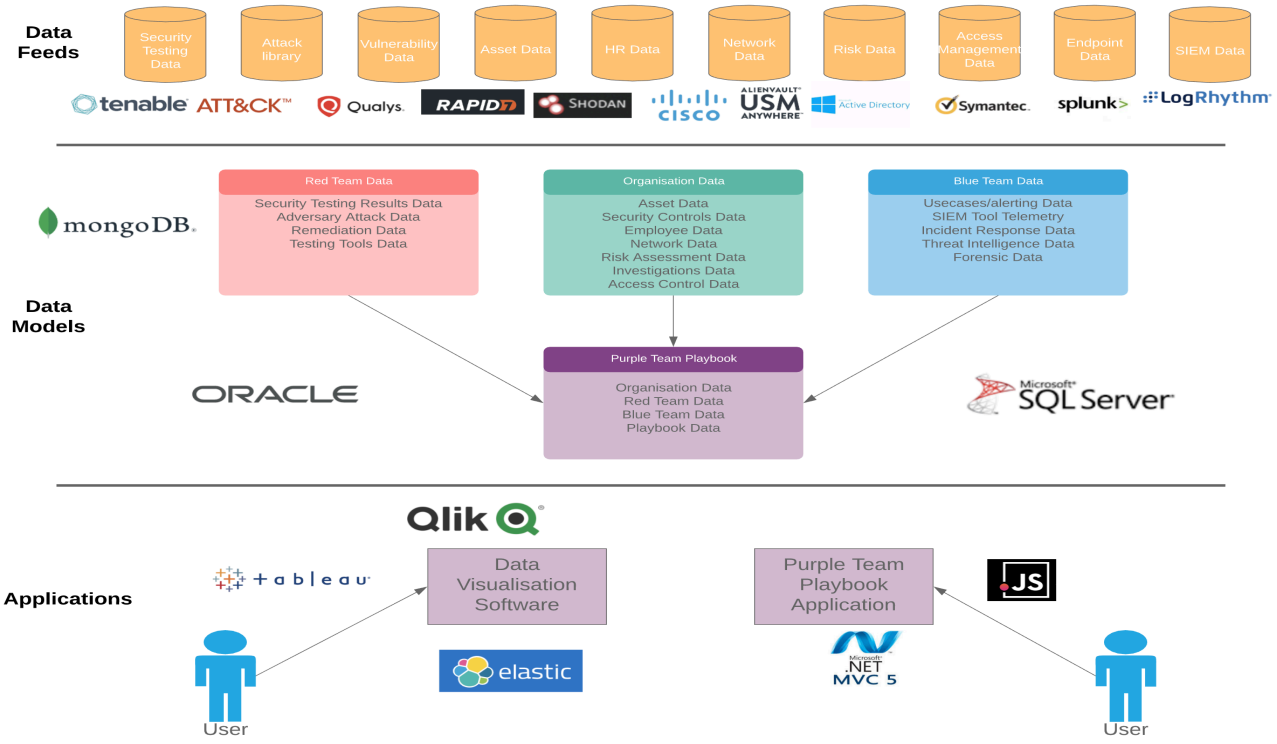


Figure 12: Purple Team Playbook Data Architecture Diagram

4.2. Purple Team Playbook Design Decisions

We understand that the framework we propose might have an overhead at the start in order to create a playbook with all the necessary information. There will also need to be experienced individuals that will oversee what information goes into the tool and a process of Quality Assurance for new entries. They will need to make certain that only relevant employees have access to the data in the PTP as existing vulnerabilities of an organisation will be held in the playbook. Once the PTP framework is in place the data feeds will be automated so there will be less maintenance for an organisation. This framework should complement what organisations already have in place as part of their security testing program and therefore will only benefit them in the long run.

For the purpose of this thesis we are trailing a small Proof of Concept (POC) of this framework and will go through each of the sections of the framework in the sections below. Due to time constraints on this thesis we have manually simulated the data stored in the PTP and explained how one can set up the framework in their own organisation.

4.2.1. Purple Team Playbook Data Feeds

In order to build the PTP special attention needs to be paid to the data that will need to be stored and how it will be used. The framework will not work if the quality of the data or the wrong data is fed into the playbook. In the previous chapter it was established that attack libraries (2.1.3) provide a wealth of knowledge on how attackers act and what tools tactics and procedures (TTP) they use. In the PTP framework, it is valuable to look at using the Mitre ATT&CK framework as this has detailed information on Advanced Persistent Threats (APTS) and is used throughout the industry (2.4.5). Mitre offer ways in which one can access the Mitre ATT&CK library, for instance one can use python or JSON [83].

In the data feeds section of Figure 12, we selected a few examples of security applications that can be used to gather data from. The majority of these applications will have APIs that one can call on to pull down data and load it into a database (4.2.2). For the purpose of this thesis we have not gone into depth into how data is ingested into a database from a data source as we have manually created data for the POC of the PTP. The book the ‘Security Data Lake’ provides information on the ways security data can be ingested and how one can extract data effectively from a SIEM tool [84]. It also goes into how one can automate the process, for instance running a batch jobs overnight to populate the database with the latest data.

4.2.2. Purple Team Playbook Data Model

The data model in Figure 13 shows how the data gathered from the various data sources determined in the data feeds section is modelled for the PTP. This is a POC version that allows us to populate the data visualisation tool (4.2.3). We have included organisation data, such as assets, software and employee data. As well as red and blue team data in the form of SIEM data, security testing data and attack library data. This data can of course vary based on an organisation’s requirements; however, we believe this model serves as a foundation for what data should be held in the PTP. Organisations can choose what database they would like to store

the data in, this is dependent on what platform they already use, we have provided some examples in Figure 12.

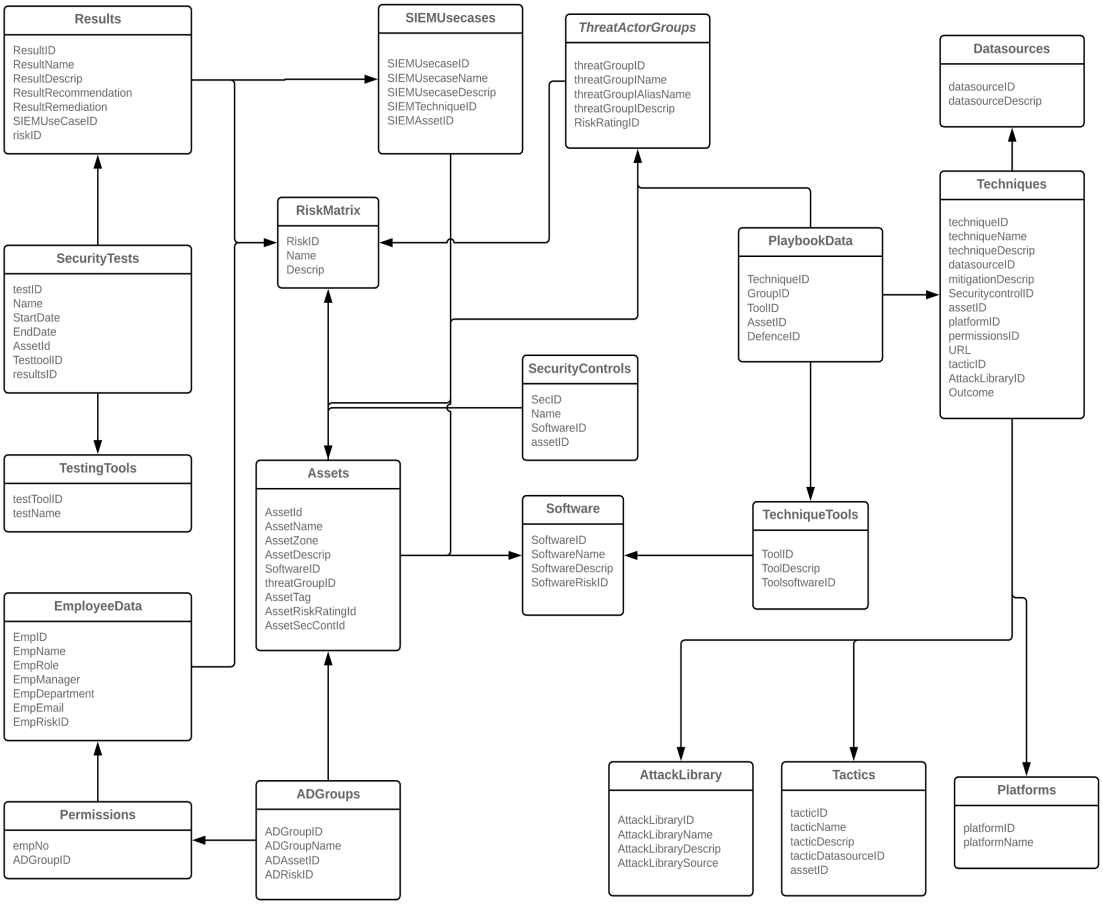


Figure 13: Purple Team Playbook Data Model Diagram

4.2.3. Purple Team Playbook Data Visualisation Application

There are many data visualisation tools that can be used, for the purpose of the POC we have used the software Tableau [85]. Tableau allows us to connect to the database that we have modeled in the above section and populate it for analysis. In order to populate tableau for the POC, we are using mock data and we are adapting data from a GitHub project that uses the Mitre ATT&CK Framework and Tableau [86]. We are also using data from the OWASP Top 10 library to populate the attacker techniques (2.1.3). In Figure 14 we show how the PTP looks and how we can the data in the PTP. We have filtered on a small section of data based on an organisation's assets, when it was last tested and what techniques have monitoring in place by the blue team (Usecase ID). In chapter five (5.2) we discuss in more detail how the data in the PTP can be used to threat model during a security test.

Asset Name	Testcase Name	Technique Name	Usecase ID	Group Name
(Multiple values)	(Multiple values)	(All)	(All)	(All)

Asset Na..	Risk Name	Technique ID	Technique Name	Technique Description	Mitigation	Testcase Name	Tested?	Usecase ID
Application	Critical	T1032	Standard Cryptographic Protocol	Adversaries use command and control over an ..	Network intrusion detection and preventio..	RedTeamTest	Assessed	Blue-Web-3
		T1132	Data Encoding	Command and control (C2) information is encoded using a standard data encoding syste..	Network intrusion detection and prevention systems that use network signatures to ide..	RedTeamTest	Assessed	Blue-Web-5
								Blue-Web-6
		T1172	Domain Fronting	Domain fronting takes advantage of routing schemes in Content Delivery Networks (CDNs) ..	If it is possible to inspect HTTPS traffic, the captures can be analyzed for connections th..	RedTeamTest	Assessed	Blue-Web-7
								Blue-Web-8
Bank WebSite	Critical	OWASPA1	Injection	An application is vulnerable to attack when:..	Preventing injection requires keeping data ..	Website Testing	Assessed	Null
		OWASPA2	Broken Authentication	Confirmation of the user's identity, authentica..	• Where possible, implement multi-factor a..	Website Testing	Assessed	Null
		OWASPA3	Sensitive Data Exposure	The first thing is to determine the protection n..	Do the following, at a minimum, and consul..	Website Testing	Assessed	Null
		OWASPA4	XML External Entities (XXE)	Applications and in particular XML-based web ..	Developer training is essential to identify a..	Website Testing	Assessed	Null
		OWASPA5	Broken Access Control	Access control enforces policy such that users ..	Access control is only effective if enforced i..	Website Testing	Assessed	Null
		T1032	Standard Cryptographic Protocol	Adversaries use command and control over an ..	Network intrusion detection and preventio..	RedTeamTest	Assessed	Blue-Web-3
		T1132	Data Encoding	Command and control (C2) information is encoded using a standard data encoding syste..	Network intrusion detection and prevention systems that use network signatures to ide..	RedTeamTest	Assessed	Blue-Web-5
								Blue-Web-6
		T1172	Domain Fronting	Domain fronting takes advantage of routing schemes in Content Delivery Networks (CDNs) ..	If it is possible to inspect HTTPS traffic, the captures can be analyzed for connections th..	RedTeamTest	Assessed	Blue-Web-7
								Blue-Web-8
DatabaseApp	high	T1032	Standard Cryptographic Protocol	Adversaries use command and control over an ..	Network intrusion detection and preventio..	RedTeamTest	Assessed	Blue-Web-3
		T1132	Data Encoding	Command and control (C2) information is encoded using a standard data encoding syste..	Network intrusion detection and prevention systems that use network signatures to ide..	RedTeamTest	Assessed	Blue-Web-5
								Blue-Web-6
		T1172	Domain Fronting	Domain fronting takes advantage of routing schemes in Content Delivery Networks (CDNs) ..	If it is possible to inspect HTTPS traffic, the captures can be analyzed for connections th..	RedTeamTest	Assessed	Blue-Web-7
								Blue-Web-8
DatabaseAPP2	Critical	T1032	Standard Cryptographic Protocol	Adversaries use command and control over an ..	Network intrusion detection and preventio..	RedTeamTest	Assessed	Blue-Web-3
		T1132	Data Encoding	Command and control (C2) information is encoded using a standard data encoding syste..	Network intrusion detection and prevention systems that use network signatures to ide..	RedTeamTest	Assessed	Blue-Web-5
								Blue-Web-6
		T1172	Domain Fronting	Domain fronting takes advantage of routing schemes in Content Delivery Networks (CDNs) ..	If it is possible to inspect HTTPS traffic, the captures can be analyzed for connections th..	RedTeamTest	Assessed	Blue-Web-7
								Blue-Web-8

Figure 14: Purple Team Playbook Data Visualisation Example

4.2.4. Purple Team Playbook Viewer Application Design

In this section we describe the design of the PTP Application Viewer and what functionality it should have. Due to the limited time for this thesis, we have decided not to make the PTP viewer at this time (7.2). However, organisations may wish to purchase a tool or use an open source tool with similar functionality and the use PTP data to populate it.

4.2.4.1.Purple Team Playbook Main View

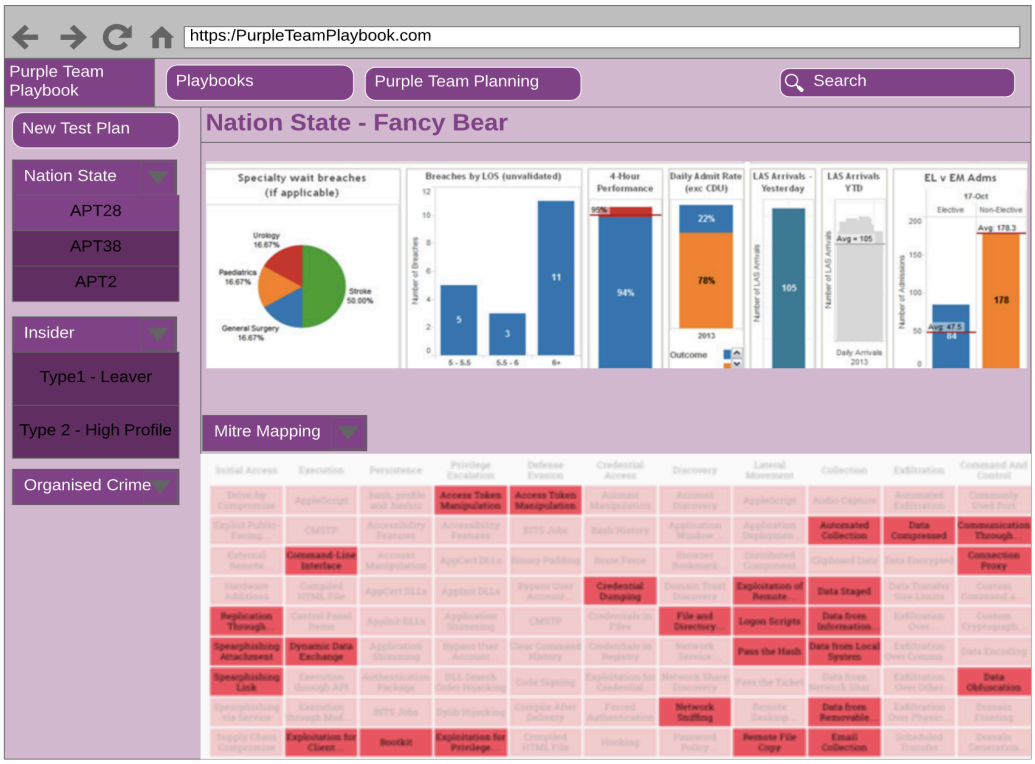


Figure 15: Purple Team Playbook Viewer Application Design

In Figure 15 we have created a design of how the web application view of the PTP should look. The design was inspired by Palo Alto's opensource UNIT-42 Adversary Playbook [64], and we decided that this was a good way to show threat actor data in the playbook view. It offers an easy to use interface that users can use if they do not want to view the PTP data using a data visualisation software (4.2.3). We also used Mitre Caret [87], to show the threat actor Mitre ATT&CK data on the design. The playbook viewer allows the user to search by threat group (2.4.3), for instance the 'insider' threat group. This shows the types of threat actors and view a table of the techniques and tools that have been attributed to them. They can view this data in the mitre kill chain view or view the threat groups data by the cyber kill chain (2.4.4). Based on our research the Cyber Kill Chain is a popular way to view the stage of activities an attacker normally goes through to reach their objective. In this table view a user can click on a technique and get information on whether it has been tested in an organisation.

Users can also search the whole playbook using the search bar, they can for example search for a software like 'powershell', and all attacks involving the use of 'powershell' will be shown in the search results. This is useful if a user wants to check if an organisation has tested a specific software or if more testing is needed. A Tableau dashboard shows analytics on the threat actor group that may be of interest to the user. For example, it can show how many tests an organisation has conducted against them in the past year and how successful they were. Section 4.2.3 provides more information on tableau and what data users can see.

4.2.4.2.Purple Team Playbook Security Test Planning View

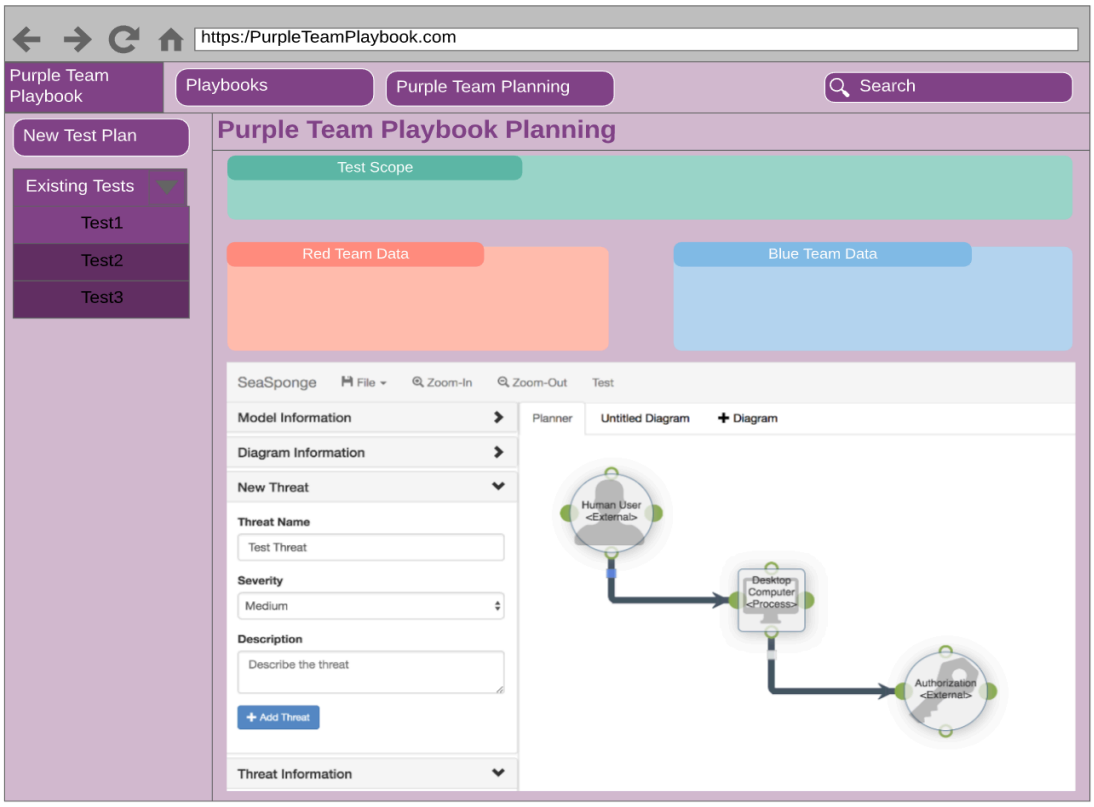


Figure 16: Purple Team Playbook Planner Application Design

In Figure 16 we show how the planner for the PTP works. The planner uses the data that is in the PTP Dataset to allow the user to pick which data they would like to be involved in a test. They can also view past test data in this planner as well. As part of a security test a user will need to choose assets that are in scope and select red team techniques that they would like to use in the test. The blue team section will allow the user to select relevant controls and usecase that are currently in place that they would like to be tested to make sure that they are working. We have decided that the Seasponge threat modeling tool (2.2.5) can be used to model the data in the PTP for a test. Seasponge is a lightweight HTML5 tool that can easily be adapted to use PTP data and provide users with a visual model tool to help them plan a test. The planning functionality in our design is very similar to some of the tools that we have discussed in a previous section (2.4.7), in particular the 'Vectr' tool offers such a planning capability for purple teaming tests. We believe that this tool can potentially be adapted to use the data from the PTP to populate it and then users can track and plan tests.

5. Purple Team Playbook in Practice

In this section we look at how the PTP can apply to the security testing threat modeling process. In order to assess how the PTP works, we look at two security testing scenarios and we pay special attention the threat modeling phase and results phase of a security test.

5.1. Purple Team Playbook Security Testing Process

In Figure 17 we describe the stages involved for a traditional penetration test as well as the purple team testing process. This process is adapted from the PTES (1.2) so it is aligned to how organisations usually conduct penetration tests. The main difference is that we are conducting threat modeling from the red and blue teams' perspective. The purple team TM phase uses the data that the red and blue team have provided in the PTP to determine where the gaps are in testing. As threat actor capabilities are always evolving, it is important to understand what has been tested and what monitoring and mitigations are currently in place and where improvements can be made.

The next phase, 'Purple Team Testing' is the actual testing phase, during this phase it will work like a normal purple team test (2.4.2) where the red team executes a test case. The blue team provides feedback on whether they were successful in detecting the red teams' activities and feeds this back to them. If the red team were unsuccessful, they can try other ways to evade detection and feed this back. The next phase in the process is when the two teams review the data for the test and decide on what mitigations should be put in place if any of the test cases were successful. For instance, if the red team were able to conduct an activity without the blue team knowing, the blue team can look at the telemetry they have and generate a use case alert on this behaviour to catch it in future. The next phase 'Reporting' corresponds the PTES where a report detailing all the activities during the test are provided to the relevant users. The findings in the report will then be added back into the PTP via one of the relevant data feeds (4.2.1).

In the sections below we look at two scenarios to show how the PTP framework can be used during the threat modeling phase of a security test. The data visualisation tool is used below to simulate how the users will use the framework and what data they can use to security test a system.

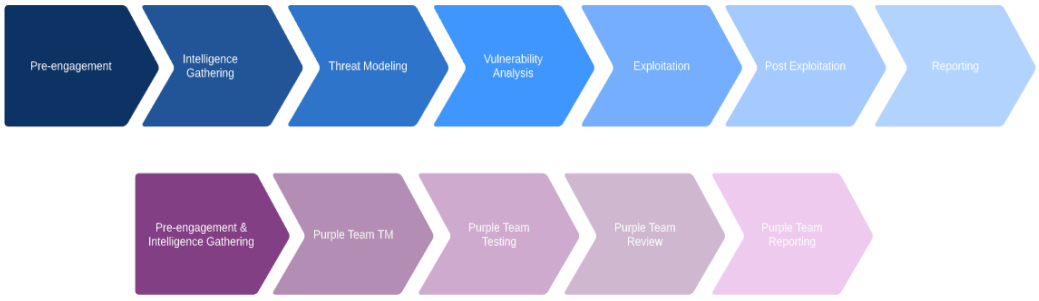


Figure 17: Purple Team Playbook Security Testing Process

5.2. *Security Testing Scenario: Web Application Penetration Test*

In the first scenario, we are acting as internal penetration testers for an organisation. In this scenario we explain how the PTP can be applied to a traditional Pen Test to evaluate whether it adds value to a normal test. For the purpose of this scenario we will be focusing on the threat modeling phase of the penetration testing process in Figure 17. The organisations data and defence data being used for the playbook is mock data so that we can provide an example of what the testers will see when they use the playbook (4.2.3).

5.2.1. *Purple Team Playbook Threat Modeling Scenario Planning*

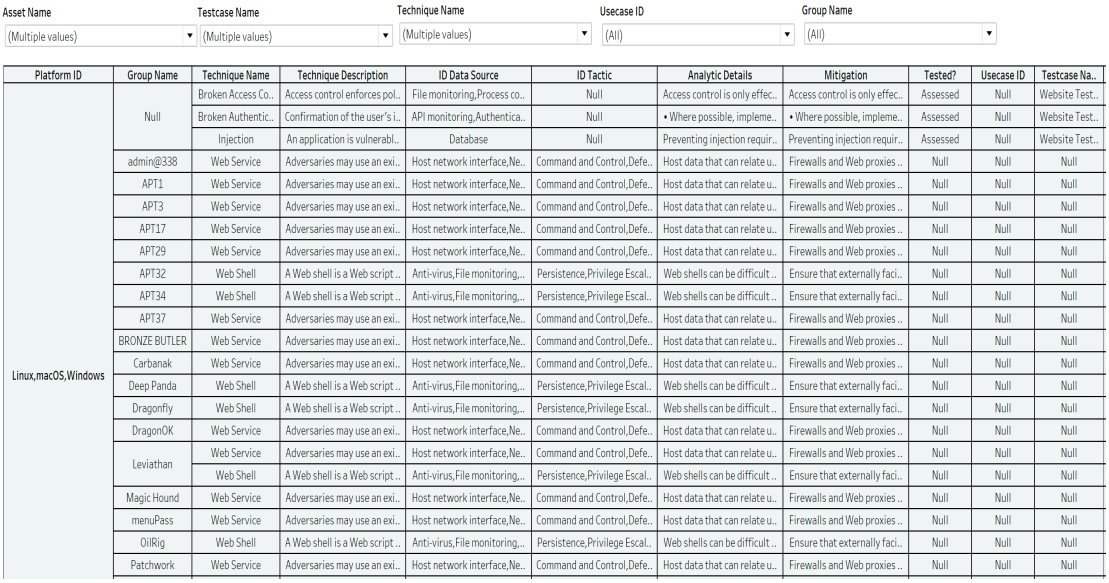
An organisation wishes to conduct a security assessment on its external website. They are adding new functionality to their checkout functionality and want to make sure that it is secure enough before it goes into production. Only the web application and supporting infrastructure is in scope for this test. During the threat modeling phase for this application, we identify the attackers of the application and what the worst-case scenarios are. For instance, if an organised crime actor were to steal customer card details or elevate their privileges to admin. This information is gathered by talking to technical and business areas and the testers own experience.

During the Purple Team Threat Modeling phase of this test we use the PTP to find out what the current status of the web application is. This includes; results of previous tests, risk rating of the asset, threat groups the asset is vulnerable to and the protections in place. From the data visualisation tool (Figure 18.), we can filter the PTP data by the asset in scope, we can see that this asset has been tested before and the vulnerabilities have been remediated. We have however noticed that there are several web-based techniques that have not been tested yet and the blue team (usecaseID) do not have monitoring in place (Figure 19). By allowing the user to filter this information we have identified gaps in testing that would not have usually been known in a traditional penetration test.

Asset Name	Testcase Name	Technique Name	Usecase ID	Group Name
Main WebSite	(Multiple values)	(All)	(All)	(All)

Asset Name	Technique Name	Technique Description	ID Data Source	Mitigation	Tested?	Testcase Na..	Year of Dat..	Results Remediation	Usecase ID
Main WebSite	Broken Access Control	Access control enforces policy such that users cann..	File monitoring,Process co..	Access control is only effec..	Assessed	Website Test..	2018	Remediated	Null
	Broken Authentication	Confirmation of the user's identity, authentication,..	API monitoring,Authentica..	• Where possible, impleme..	Assessed	Website Test..	2018	Remediated	Null
	Data Encoding	Command and control (C2) information is encoded using a standard data encoding system. Use of dat..	Packet capture,Process use of network,Process Monito..	Network intrusion detection and prevention systems th..	Assessed	RedTeamTest	2018	Null	Blue-Web-5
									Blue-Web-6
	Domain Fronting	Domain fronting takes advantage of routing schemes in Content Delivery Networks (CDNs) and ..	SSL/TLS inspection,Packet capture	If it is possible to inspect HTTPS traffic, the captures..	Assessed	RedTeamTest	2018	Null	Blue-Web-7
									Blue-Web-8
	Injection	An application is vulnerable to attack when:..	Database	Preventing injection requir..	Assessed	Website Test..	2018	Remediated	Null
	Sensitive Data Exposure	The first thing is to determine the protection needs..	File monitoring,Process co..	Do the following, at a mini..	Assessed	Website Test..	2018	Remediated	Null
	Standard Cryptographic Prot..	Adversaries use command and control over an encr..	Packet capture,Netflow/En..	Network intrusion detectio..	Assessed	RedTeamTest	2018	Null	Blue-Web-3
	XML External Entities (XXE)	Applications and in particular XML-based web servi..	File monitoring,Process co..	Developer training is essen..	Assessed	Website Test..	2018	Remediated	Null

Figure 18: Purple Team Playbook Asset and Past Test Results Example



Asset Name	Testcase Name	Technique Name	Usecase ID	Group Name
(Multiple values)	(Multiple values)	(Multiple values)	(All)	(All)

Platform ID	Group Name	Technique Name	Technique Description	ID Data Source	ID Tactic	Analytic Details	Mitigation	Tested?	Usecase ID	Testcase Na..
Linux,macOS,Windows	Null	Broken Access Co..	Access control enforces pol..	File monitoring,Process co..	Null	Access control is only effec..	Access control is only effec..	Assessed	Null	Website Test..
		Broken Authentic..	Confirmation of the user's i..	API monitoring,Authentica..	Null	• Where possible, impleme..	• Where possible, impleme..	Assessed	Null	Website Test..
		Injection	An application is vulnerabl..	Database	Null	Preventing injection requir..	Preventing injection requir..	Assessed	Null	Website Test..
	admin@338	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
	APT1	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
	APT3	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
	APT17	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
	APT29	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
	APT32	Web Shell	A Web shell is a Web script ..	Anti-virus,File monitoring,..	Persistence,Privilege Escal..	Web shells can be difficult ..	Ensure that externally faci..	Null	Null	Null
	APT34	Web Shell	A Web shell is a Web script ..	Anti-virus,File monitoring,..	Persistence,Privilege Escal..	Web shells can be difficult ..	Ensure that externally faci..	Null	Null	Null
	APT37	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
	BRONZE BUTLER	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
	Carbanak	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
	Deep Panda	Web Shell	A Web shell is a Web script ..	Anti-virus,File monitoring,..	Persistence,Privilege Escal..	Web shells can be difficult ..	Ensure that externally faci..	Null	Null	Null
	Dragonfly	Web Shell	A Web shell is a Web script ..	Anti-virus,File monitoring,..	Persistence,Privilege Escal..	Web shells can be difficult ..	Ensure that externally faci..	Null	Null	Null
	DragonOK	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
	Leviathan	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
		Web Shell	A Web shell is a Web script ..	Anti-virus,File monitoring,..	Persistence,Privilege Escal..	Web shells can be difficult ..	Ensure that externally faci..	Null	Null	Null
	Magic Hound	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
	menuPass	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null
	OilRig	Web Shell	A Web shell is a Web script ..	Anti-virus,File monitoring,..	Persistence,Privilege Escal..	Web shells can be difficult ..	Ensure that externally faci..	Null	Null	Null
	Patchwork	Web Service	Adversaries may use an exi..	Host network interface,Ne..	Command and Control,Defe..	Host data that can relate u..	Firewalls and Web proxies ..	Null	Null	Null

Figure 19: Purple Team Playbook Web Based Attacker Techniques View Example

In Table 4 we have summarised the information found in the threat modeling phase as well as the gaps identified by the PTP. This forms part of the test plan that is used for the penetration test so that all stakeholders understand what kind of testing will be conducted.

Table 4: Web Application Penetration Test - Threat Modeling Summary

Assets in Scope	External Web application and supporting infrastructure (servers and database)
Threat Actors	• Insider • Organised Crime • Script Kiddie

Goals and objectives	• Identify vulnerabilities in the application configuration
	• Identify any authentication weaknesses in the application;
	  ○ Identify if a lower privilege user can elevate their access.
	  ○ Identify if unauthenticated users can elevate their access.
	• Identify vulnerabilities in the web app using the OWASP top 10
	• Identify any vulnerabilities in the applications error handling
	• Identify any vulnerabilities that will affect the integrity of the application transaction
	• Identify any vulnerabilities that will affect the availability of the application

PTP Gaps	• T1102 - Web Service • T1051 – Shared Webroot • T1100 - Web Shell

5.2.2. Purple Team Playbook Threat Modeling Scenario Analysis

The reasons for conducting a penetration test can vary (1.2), based on our experience it can be difficult to get all the information needed for the threat modeling phase of a test. We are usually dependant on our own experience and by talking to the owners of the system to get the information we need. By using the PTP we have a centralised place to look at all the relevant data, for instance data from previous tests whether the findings have been fixed. We also have visibility on the security controls that the Blue team have in place for each of the techniques. For a traditional pen test, we would not normally look at blue team data as there are time constraints for each test so the applications security should be prioritised. Red and blue team tests are usually conducted independently as they look at the whole organisation (2.4.1).

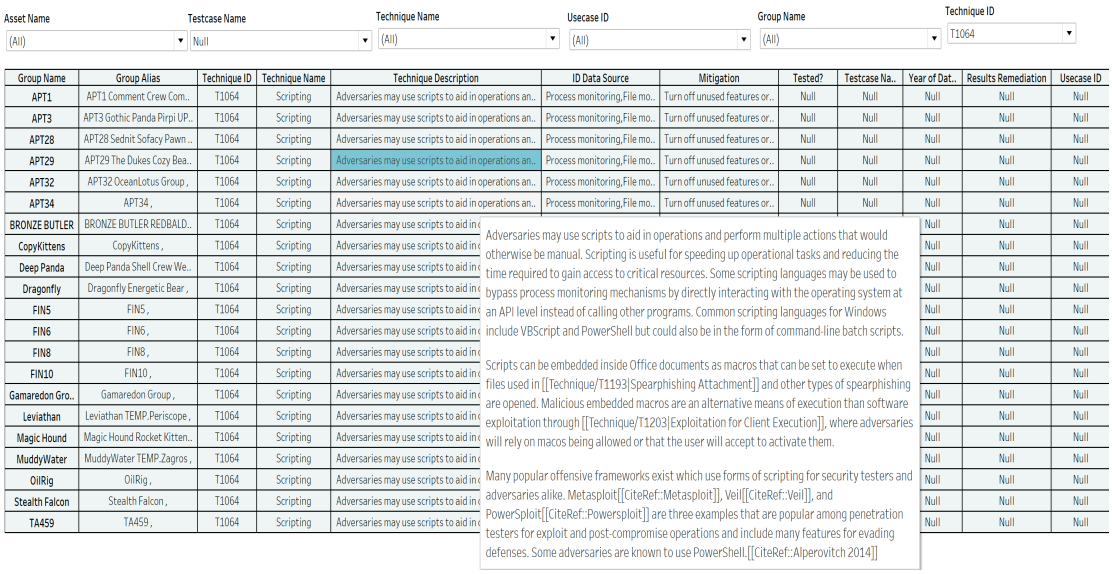
In the scenario above we believe that by using the PTP we can add value to a normal Pen Test by identifying security gaps that might impact the application that is in scope. In doing this we are continuously testing the blue team in each test we do and giving them feedback as well as keeping track of what testing we have conducted. The PTP also provides access to data on other tests that have been conducted on a target asset and the current security controls. This builds a picture for the tester so that they can adjust their testing to try and circumvent these controls.

5.3. Security Testing Scenario: Purple Team Test

In the second scenario we are acting as internal purple team (2.4.2) testers for a financial institution. For the purpose of this scenario we will be focusing on the threat modeling phase of the penetration testing process in Figure 17. The organisations data and defence data being used for the playbook so that we can provide an example of what the testers will see when they use the playbook (4.2.3).

5.3.1. Purple Team Playbook Threat Modeling Scenario Planning

The scope of this test is the entire organisation as is usually the case in a normal purple team test or red team test (2.4.1). In order to understand what we need to test we need to look at what has been covered in the PTP. As this is a financial institution, we will narrow down the PTP and look at techniques that can be used to target financial organisations. During our research we have found a white paper from the company BitDefender on the subject of APTs and financial threats. The paper details how the APT group Carbanak conduct their attacks on financial organisations and details their spearphishing techniques [88]. For this purple team test, we work with the blue and red team to determine if we have tested any spearphishing techniques in our environment. The PTP contains details from the Mitre ATT&CK framework that show the tester how the adversary conducts their attack and mitigations in order to prevent an attacker from exploiting the issue (4.2.3). With the aid of the PTP, in Figure 20 we can see that there are techniques that we have not tested yet and the various threat groups that are attributed to these techniques. In Figure 21 we have shown the tools that the threat groups use in order to use this spearphishing technique, we can then use this data to find out if we have tested any of these tools before. In order to conduct this test, we will also need to make sure our testers have the right tools and experience to simulate this actor behaviour.



Asset Name	Testcase Name	Technique Name	Usecase ID	Group Name	Technique ID
(All)	Null	(All)	(All)	(All)	T1064

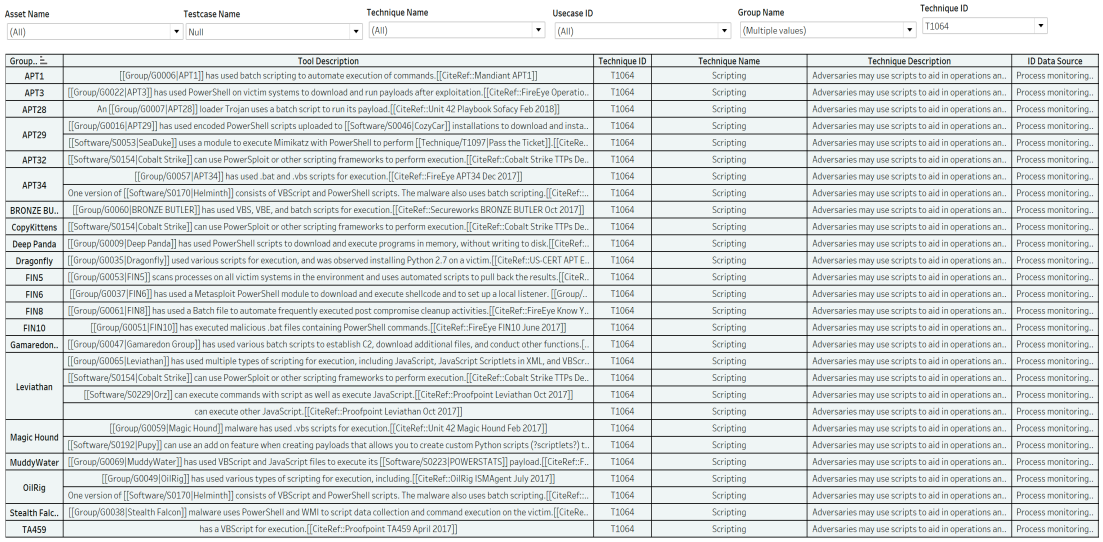
Group Name	Group Alias	Technique ID	Technique Name	Technique Description	ID Data Source	Mitigation	Tested?	Testcase Na..	Year of Dat..	Results Remediation	Usecase ID
APT1	APT1 Comment Crew Com..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring,File mo..	Turn off unused features or..	Null	Null	Null	Null	Null
APT3	APT3 Gothic Panda Pirpi UP..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring,File mo..	Turn off unused features or..	Null	Null	Null	Null	Null
APT28	APT28 Sednit Sofacy Pawn ..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring,File mo..	Turn off unused features or..	Null	Null	Null	Null	Null
APT29	APT29 The Dukes Cozy Bea..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring,File mo..	Turn off unused features or..	Null	Null	Null	Null	Null
APT32	APT32 OceanLotus Group ,	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring,File mo..	Turn off unused features or..	Null	Null	Null	Null	Null
APT34	APT34 ,	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring,File mo..	Turn off unused features or..	Null	Null	Null	Null	Null
BRONZE BUTLER	BRONZE BUTLER REDBALD..	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
CopyKittens	CopyKittens ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
Deep Panda	Deep Panda Shell Crew We..	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
Dragonfly	Dragonfly Energetic Bear ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
FIN5	FIN5 ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
FIN6	FIN6 ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
FIN8	FIN8 ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
FIN10	FIN10 ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
Gamaredon Gro..	Gamaredon Group ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
Leviathan	Leviathan TEMP.Periscope ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
Magic Hound	Magic Hound Rocket Kitten..	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
MuddyWater	MuddyWater TEMP.Zagros ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
OilRig	OilRig ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
Stealth Falcon	Stealth Falcon ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null
TA459	TA459 ,	T1064	Scripting	Adversaries may use scripts to aid in o						Null	Null

Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and PowerShell but could also be in the form of command-line batch scripts.

Scripts can be embedded inside Office documents as macros that can be set to execute when files used in [[Technique/T1193|Spearphishing Attachment]] and other types of spearphishing are opened. Malicious embedded macros are an alternative means of execution than software exploitation through [[Technique/T1203|Exploitation for Client Execution]], where adversaries will rely on macos being allowed or that the user will accept to activate them.

Many popular offensive frameworks exist which use forms of scripting for security testers and adversaries alike. Metasploit[[CiteRef::Metasploit]], Veil[[CiteRef::Veil]], and PowerSploit[[CiteRef::Powersploit]] are three examples that are popular among penetration testers for exploit and post-compromise operations and include many features for evading defenses. Some adversaries are known to use PowerShell.[[CiteRef::Alperovitch 2014]]

Figure 20: Purple Team Playbook Threat Group Spearphishing Techniques Example



Asset Name	Testcase Name	Technique Name	Usecase ID	Group Name	Technique ID
(All)	Null	(All)	(All)	(Multiple values)	T1064

Group..	Tool Description	Technique ID	Technique Name	Technique Description	ID Data Source
APT1	[[Group/G0006|APT1]] has used batch scripting to automate execution of commands.[[CiteRef::Mandiant APT1]]	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
APT3	[[Group/G0022|APT3]] has used PowerShell on victim systems to download and run payloads after exploitation. [[CiteRef::FireEye Operatio..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
APT28	An [[Group/G0007|APT28]] loader Trojan uses a batch script to run its payload.[[CiteRef::Unit 42 Playbook Sofacy Feb 2018]]	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
APT29	[[Group/G0016|APT29]] has used encoded PowerShell scripts uploaded to [[Software/S0046|CozyCar]] installations to download and insta..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
	[[Software/S0053|SeaDuke]] uses a module to execute Mimikatz with PowerShell to perform [[Technique/T1097|Pass the Ticket]]..[[CiteRe..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
APT32	[[Software/S0154|Cobalt Strike]] can use PowerSploit or other scripting frameworks to perform execution.[[CiteRef::Cobalt Strike TTPs De..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
APT34	[[Group/G0057|APT34]] has used .bat and .vbs scripts for execution.[[CiteRef::FireEye APT34 Dec 2017]]	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
	One version of [[Software/S0170|Helminth]] consists of VBScript and PowerShell scripts. The malware also uses batch scripting.[[CiteRef::...	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
BRONZE BU..	[[Group/G0060|BRONZE BUTLER]] has used VBS, VBE, and batch scripts for execution.[[CiteRef::Secureworks BRONZE BUTLER Oct 2017]]	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
CopyKittens	[[Software/S0154|Cobalt Strike]] can use PowerSploit or other scripting frameworks to perform execution.[[CiteRef::Cobalt Strike TTPs De..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
Deep Panda	[[Group/G0009|Deep Panda]] has used PowerShell scripts to download and execute programs in memory, without writing to disk.[[CiteRef:..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
Dragonfly	[[Group/G0035|Dragonfly]] used various scripts for execution, and was observed installing Python 2.7 on a victim.[[CiteRef::US-CERT APT E..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
FIN5	[[Group/G0053|FIN5]] scans processes on all victim systems in the environment and uses automated scripts to pull back the results.[[CiteR..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
FIN6	[[Group/G0037|FIN6]] has used a Metasploit PowerShell module to download and execute shellcode and to set up a local listener. [[Group/..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
FIN8	[[Group/G0061|FIN8]] has used a Batch file to automate frequently executed post compromise cleanup activities.[[CiteRef::FireEye Know Y..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
FIN10	[[Group/G0051|FIN10]] has executed malicious .bat files containing PowerShell commands.[[CiteRef::FireEye FIN10 June 2017]]	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
Gamaredon..	[[Group/G0047|Gamaredon Group]] has used various batch scripts to establish C2, download additional files, and conduct other functions.[..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
Leviathan	[[Group/G0065|Leviathan]] has used multiple types of scripting for execution, including JavaScript, JavaScript Scriptlets in XML, and VBScr..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
	[[Software/S0154|Cobalt Strike]] can use PowerSploit or other scripting frameworks to perform execution.[[CiteRef::Cobalt Strike TTPs De..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
	[[Software/S0229|Orz]] can execute commands with script as well as execute JavaScript.[[CiteRef::Proofpoint Leviathan Oct 2017]]	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
	can execute other JavaScript.[[CiteRef::Proofpoint Leviathan Oct 2017]]	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
Magic Hound	[[Group/G0059|Magic Hound]] malware has used .vbs scripts for execution.[[CiteRef::Unit 42 Magic Hound Feb 2017]]	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
	[[Software/S0192|Pupy]] can use an add on feature when creating payloads that allows you to create custom Python scripts (?scriptlets?) t..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
MuddyWater	[[Group/G0069|MuddyWater]] has used VBScript and JavaScript files to execute its [[Software/S0223|POWERSTATS]] payload.[[CiteRef::F..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
OilRig	[[Group/G0049|OilRig]] has used various types of scripting for execution, including.[[CiteRef::OilRig ISMAgent July 2017]]	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
	One version of [[Software/S0170|Helminth]] consists of VBScript and PowerShell scripts. The malware also uses batch scripting.[[CiteRef::...	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
Stealth Falc..	[[Group/G0038|Stealth Falcon]] malware uses PowerShell and WMI to script data collection and command execution on the victim.[[CiteRe..	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..
TA459	has a VBScript for execution.[[CiteRef::Proofpoint TA459 April 2017]]	T1064	Scripting	Adversaries may use scripts to aid in operations an..	Process monitoring..

Figure 21: Purple Team Playbook Threat Group Tools for Spearphishing Example

5.3.2. Purple Team Playbook Threat Modeling Scenario Analysis

A purple team test will work differently from a normal penetration test, it will follow a similar format to a red team test (2.4.1). In this test the blue team will share any information they have on the controls they have in place for various APT actors. The red team will share details on new techniques they have found that they want to try. The PTP is used to bring all this information together so that they can plan what should be tested. In the above scenario we have to be selective as we cannot test all the techniques in our attack libraries as some may not be relevant and it would take a long time to test at once, this should be tested over a period of time. For the scenario we used specific intelligence in the form of a white paper to inform what should be tested in this test which was centred around spearphishing and how the APT Carbanak

gains access into a network. The PTP enabled us to check if we had tested any of their techniques in the past and if we have not then they would be included in the test. It also allowed us to view the different tools that the APT uses and to find out if we had tested any of these tools in the past as well.

Once testing is complete the PTP can be updated with the results of the test so that there is a record of the test and the new security controls that have been put in place. We can also communicate with other users the effect the results have on the whole system, for instance using the kill chain to describe how an attacker gets in through spearphishing techniques and how far they could get into the organisation. The PTP could also be used to highlight risk areas for instance many organisations conduct phishing simulation tests on their employees to see if they click links on phishing emails. As this purple team is looking at phishing techniques, we could also show which employees have repeatedly been clicking on phishing links as this could mean that more awareness training is needed.

6. Purple Team Playbook Discussion

In this section we discuss how the PTP framework designed in Chapter four aligns with the objectives of this thesis. It includes discussions on how well it deals with the issues in threat modeling when applied to security testing scenarios (Chapter Five). We will also discuss the limitations of the framework and the other applications for the PTP.

6.1. Purple Team Playbook Framework Discussion

Whilst conducting our background research for this thesis, we found that there was a lack of threat modeling frameworks for red and blue teams to use internally in their organisations. The Purple Team Playbook addresses this gap by providing a framework that can be used to provide relevant attack and defence data for an organisation. The PTP is still in the prototype phase and we have created the data visualisation (4.2.3) part of the framework and manually simulated the data feeds and data models required for the framework. The PTP is addressing a complex issue where organisations have many security tools, but they do not have access to all of the data in a centralised knowledge base and therefore may not fully understand what they need to test. As the PTP leverages data from existing systems, this keeps the costs down as an organisation already owns these systems. We do recognise that to use this framework in an organisation it will take some time and internal resource to be able to find the appropriate data feeds and get them to feed into the purple team dataset. Once this is in place there will be less maintenance as the data feeds should be automated (4.2.1). This data is then easily accessible to the relevant teams and they can use a data visualisation tool to view the data in any way they like. The primary purpose of the PTP is to provide a framework that can be used by internal red and blue teams to identify gaps that need to be tested.

One of the main challenges with threat modeling (2.3) is that models can be hard to maintain, and they are only as good as the user modeling them. The PTP framework cannot replace the experience of a professional red or blue team tester; it can however, offer a centralised knowledge base with reliable data that can be used for security testing modeling purposes. We acknowledge that there are tools that will have similar functionality however they can be costly as they are mostly commercial tools. In the related work chapter (2.4.7), we have discussed the different advantages and disadvantages of each of these tools. We believe that the PTP can be used by organisations as a foundation to understand their security data. They can then make more informed decision if they decide to purchase a security testing or automation tool. Smaller organisations may not be able to justify the cost of commercial tools so the PTP gives them a framework that they can use so they are not disadvantaged by not using commercial security testing tools.

One challenge with security testing (2.4.6) was that there was seen to be a disconnect between the red and the blue teams in an organisation. The PTP allows the teams to have access to each other's data so that there is an understanding on what has been covered and what needs to be tested. This encourages innovation as the red team will know what will not work so they will research new ways in which an attacker could try to attack a system. This also helps the blue team to formulate new defences such as SIEM usecases that will pick up behaviours based on the technique's that attackers may try. The PTP also allows users to look at the whole organisation at once so that they can judge the impact of a vulnerability and how it affects their assets. For example, a web vulnerability was found in one test, we can use the PTP to understand what other web applications the organisation has and if they are affected.

The PTP addresses some of the concerns with the STRIDE model (2.3) where it was seen to have a lack of granularity and provided no mitigations for threats. The PTP uses established attack libraries such as the Mitre ATT&CK Framework to offer the level of granularity needed and it also provides mitigations and tracking data to understand whether an organisation has remediated an issue. The PTP application viewer (4.2.4) addresses a challenge that attack trees have which is that the trees may become unmanageable. The viewer organises the playbook data by kill chain or Mitre tactics to give a clear view of what has been tested and where the organisation is still vulnerable. A user can also use the PTP as a data source for a threat modeling tool such as Seasponge (2.2.5) as this tool can easily be changed to suit an organisation's needs. According to the PTES (1.2) threat modeling for penetration testing has no recommended model to use so the data held in PTP can be used interchangeably with other models. For example, it could be used to populate the data for the Diamond Model (2.1.4), by providing a good quality data in the PTP, analysts can be better informed when they are using other models to make sure that they are identifying the correct threats.

6.2. POC Discussion

In chapter five we looked at two security testing scenarios and used the PTP to help in the threat modeling phase of the tests. For the purpose of these scenarios we only looked at the threat modeling phase of the test and used the data visualisation tool 'Tableau' to view the PTP data. In the first scenario (5.2) we looked at a traditional penetration test of a web application, in a normal test like this the tester would use their own knowledge as well as any data they get from the relevant business stakeholders. From our own experience the relevant data needed for the test would be in different places, for instance previous test results, asset data and threat data. Also, in a traditional penetration test the blue team would not normally be involved so we would not know all the security controls in place for the application. The PTP allows a tester to find out all the relevant data they need to know for a test in one place and they can also view the blue team data. This adds value to the test as they could add any relevant gaps in testing that are identified in the playbook. As this is a normal penetration test the goal is more to make sure the application is secure so the scope will just be the application and supporting infrastructure. Overall, we believe that the PTP can aid traditional penetration tests as it provides a centralised data source for all users, this should ensure that each user models in a consistent way as the threats are defined in the PTP.

In the second scenario a purple team test (5.3), we follow the purple team testing process that we defined in chapter five (5.1). As part of this test the red and the blue teams can meet to look through the PTP to find out what has been tested already and what needs to be tested. In this scenario we specifically looked at spearphishing techniques that APTs use to get into financial institutions. The PTP provided data on what had been accessed and what already had blue team controls in place, and this then gave us the testing gap we needed to define what to test. We found that the PTP could also allow us to understand the internal threat from users clicking on a phishing link as we can store data on phishing simulations. This adds value to a test as we can communicate what techniques worked as well as the risk to the organisation if there is a high level of users clicking on phishing emails. We found in the related work section (3.1.3) that being able to correlate insider data can allow us to predict how this actor will behave in the future.

These small test scenarios were built to show how the PTP can add value to a normal penetration test as well as a purple team test. We showed that by having a centralised database of all the relevant organisational, red and blue team data we are able to get a better picture who may be attacking an organisation and where the gaps are. In the threat modeling introduction (1) of this thesis we spoke about the difficulty in getting users to think like attackers while threat modeling. The PTP can help red and blue team testers gain the relevant experience by testing attacker techniques and overtime they will begin to notice patterns of behaviour. This should help encourage innovation in an organisation as the testers may think of other ways to compromise a system. This benefits an organisation as they can help train their testers internally so they are less reliant on third party testers and an organisation should have better detection from attackers.

6.3. Limitations

In order for the PTP to work, there needs to be a way to reliably obtain data from existing systems and make sure that it is in the correct format. This can be an issue as some systems may incompatibilities with their data and it could be hard to translate. Large organisations may have many data sources so it may be impossible to get data from every source or almost all sources we need. In this situation a decision needs to be made to prioritise the importance of certain data sources and how it will help the PTP overall. Also, security issues may arise with some systems as there could be a concern about who will have access to the PTP data, as access will need to be identified and managed appropriately. There also may be an issue with users having access to blue team data, organisations may want to limit knowledge of these controls to the blue team only as they may be worried about 'insider' threat actors. In order for the framework to work a good relationship between the red and the blue team should be fostered so there is trust between them. Also, the organisation needs to be on board with the framework at an executive level to ensure there is funding and time allocated to setting it up. Experienced personnel will also need to oversee how the framework is setup to ensure that the correct data is being obtained and translated into the databases and that there are sufficient access control mechanisms in place.

Given the fact that we have only trialled a proof of concept version of the PTP, this is not a true representation of how this framework would be implemented in a real organisation. We were used a limited amount of data for the POC as we could simulate the data in a real organisation. Therefore, the PTP needs to be trialled as a POC in a real organisation to understand where all the limitations are and if any changes need to be made to the framework. Each organisation of course works differently so the PTP can act as a guide on how one might implement it to achieve the goal of purple team threat modeling. In terms of the effectiveness of the PTP we acknowledge that there may be too much information in the playbook, and this could overload a user. This is also true when using attack libraries (2.1.3), so it is necessary to carefully model what data one would need in the playbook. It is equally relevant to make sure we record what is not relevant so that all users know not to test it. In the related work section (3.1.2) we found that there are many papers addressing threat modeling and security testing with automation. The PTP could benefit from the security testing part of the purple teaming activities being automated. For instance, an organisation can purchase an automation tool to enable them to conduct purple teaming (2.4.7) and use the PTP as a data source to define the tests.

6.4. Other Applications

During the course of this thesis we have found that the PTP can potentially be used for other purposes and not just security testing. It could be used for educational purposes for instance red and blue team training. The open cyber challenge platform offers an open source platform to coordinate cyber simulation challenges [89]. The PTP could provide data for this challenge so that a user simulating the blue team in this challenge can have some information on the current state of the environment. In essence it will be a playbook that they can use and add to as they go through the challenge, so they have something to refer back to re-enforce their learning. It could also be used to train new employees, as they can view the PTP and have a good understanding of what their threats are and information on attacker techniques to learn.

The data in the PTP could also be used for identifying risk areas for example it will show various attributes an employee has. This can be used to identify high risk employees, for instance if they have high privilege access to critical systems special attention needs to be paid to the standard of their passwords or if they are up to date on their security training. It can also be used to facilitate an organisation if they wish to automate some of their security processes. In chapter two (2.4.7) we looked at some security testing tools, the PTP data could for instance be fed into the ‘Vectr’ tool or ‘Caldera’ tool to automate the testing.

7. Conclusion & Future Work

In this section we evaluate the thesis as whole and how we have achieved our objectives set out at the start. We will also look at the future work we plan to do as a direct result of this thesis.

7.1. Conclusion

In this thesis we set out to explore current threat modeling methodologies and tools as well as how threat modeling and security testing are related. We found that there are no recommended models for security testing, and it is completely up to the organisation which model they use to determine their threats. During our research we also found that there was not a lot of academic research in the field of purple teaming and threat modeling. This is where red and blue teams in an organisation work together to test their systems. As a result of this we set out to design a Purple Team Playbook framework which leverages an organisations existing data to be used for the purpose of security testing. As organisations can use any models and tools for threat modeling it was important for us to build a framework that contained all the data they would need to model their threats effectively. Also, by leveraging existing data this can work out more cost effective in the long run as an organisation has already paid for these security products.

During this thesis we also looked at how the PTP can help during a traditional penetration test and a purple team test. We found that by having this centralised knowledge base we were able to identify the gaps in testing easily and understand where our defences are currently. We could also correlate data with other data sources in a more effective way, for instance understanding the impact of our phishing attack risk by using employee phishing training records. We do acknowledge that the PTP needs to be trialled as a POC in a real organisation for us to fully understand the benefits it would have and if any changes need to be made.

We believe that we have achieved what we set out to do at the start of this thesis which was to get the red and blue teams in an organisation working together. As we discussed in our introduction, the threats we face are continuously evolving and it is difficult for organisations to keep up with all the attacker's techniques and tactics. By allowing both teams to share data we believe that this also encourages innovation as employees will be able to find new ways to try and circumvent defences and come up with new defence capabilities. This can only benefit an organisation as they need their staff to be just as motivated as attackers would be so that they can have a chance at protecting themselves against them. We have also presented threat models and tools that organisations can use in order to understand their threats. Our PTP framework complements these tools and models and gives a consistent set of data for users to use in order to threat model.

7.2. Future Work

It is our intention to implement the PTP in a real organisation in order to improve our security testing capabilities. By using the PTP framework design we aim to decide on the appropriate data feeds that we need and use the PTP as part of our normal testing process. This will help us set up an internal purple team capability in our organisation and will help us improve on our attack and defence capability. As discussed in this thesis we can use the PTP as

a foundation to understand our security data so that we can build up a business case to purchase an automated security testing tool.

During this thesis we did not have the time to create the application view of the PTP (4.2.4). We would like to create this viewer to give the users an easy to use application that they can use instead of the data visualisation tool. We can also adapt a threat modeling tool discussed in this thesis for our security testing planning. We believe that the application view of the PTP will help us communicate test findings to less technical users by showing data in the kill chain view. Once the PTP framework and viewer application is in place, we would like to use it for educational purposes such as training new staff. As well as helping existing staff build up their technical knowledge on attackers' techniques.

Bibliography

[1] Y. Diogenes and E. Ozkaya, *Cybersecurity, attack and defense strategies : Infrastructure security with Red Team and Blue Team tactics*. Packt Publishing, 2018.

[2] 'Verizon: 2019 Data Breach Investigations Report', *Computer Fraud & Security*, 2019.

[3] 'Project TajMahal – a new sophisticated APT framework | Securelist'. [Online]. Available: https://securelist.com/project-tajmahal/90240/. [Accessed: 17-Aug-2019].

[4] 'Category:Threat Modeling - OWASP'. [Online]. Available: https://www.owasp.org/index.php/Category:Threat_Modeling. [Accessed: 01-Mar-2019].

[5] A. Shostack, *Threat Modeling: Designing for Security*. John Wiley & Sons Ltd, 2014.

[6] N. Shevchenko, T. A. Chick, P. O'riordan, T. P. Scanlon, and C. Woody, 'Theat Modeling: A Summary of Available Methods', 2018.

[7] J. Wittkop, *Building a comprehensive IT security program : practical guidelines and best practices*. Apress, 2016.

[8] A. Tang, 'A guide to penetration testing', *Network Security*, vol. 2014, no. 8, pp. 8–11, 2014.

[9] G. Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*, vol. 1st Editio, no. 1. 2014.

[10] 'PCI Data Security Standard (PCI DSS) Penetration Testing Guidance', 2015.

[11] G. Disterer, 'ISO/IEC 27000, 27001 and 27002 for Information Security Management', *Journal of Information Security*, vol. 04, no. 02, pp. 92–100, 2013.

[12] 'CBEST Intelligence-Led Testing CBEST Implementation Guide', 2016.

[13] P. Herzog, 'OSSTMM: The Open Source Security Testing Methodology Manual: v3', 2016.

[14] B. Rathore *et al.*, 'Information Systems Security Assessment Framework (ISSAF) d', 2006.

[15] C. Nickerson, D. Kennedy, and C. J. Reil, 'The Penetration Testing Execution Standard', *2014*, 2017.

[16] 'Penetration testing methodologies - OWASP'. [Online]. Available: https://www.owasp.org/index.php/Penetration_testing_methodologies. [Accessed: 13-Jul-2019].

[17] T. Ucedavélez and M. M. Morana, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. Wiley Blackwell, 2015.

[18] F. Baiardi, 'Avoiding the weaknesses of a penetration test', *Computer Fraud and Security*, vol. 2019, no. 4, pp. 11–15, Apr. 2019.

[19] J. Creasey and I. Glover, 'A guide for running an effective Penetration Testing programme', 2013.

[20] 'CREST Exams'. [Online]. Available: https://www.crest-approved.org/professional-qualifications/crest-exams/index.html. [Accessed: 04-Aug-2019].

[21] 'Qualifications | Cyber Security Certificates | CHECK Qualifications'. [Online]. Available: https://www.tigerscheme.org/qualifications.php. [Accessed: 03-Aug-2019].

[22] 'CHECK - penetration testing - NCSC'. [Online]. Available: https://www.ncsc.gov.uk/information/check-penetration-testing. [Accessed: 03-Aug-2019].

[23] V. Maheshwari and M. Prasanna, 'Integrating risk assessment and threat modeling within

SDLC process', in *2016 International Conference on Inventive Computation Technologies (ICICT)*, 2016, pp. 1–5.

[24] B. Schneier, 'Academic: Attack Trees - Schneier on Security'. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html. [Accessed: 25-Feb-2019].

[25] Z. Aslanyan and F. Nielson, 'Pareto Efficient Solutions of Attack-Defence Trees', Springer, Berlin, Heidelberg, 2015, pp. 95–114.

[26] L. Wang, E. Wong, and D. Xu, 'A threat model driven approach for security testing', in *Proceedings - ICSE 2007 Workshops: Third International Workshop on Software Engineering for Secure Systems, SESS'07*, 2007.

[27] 'CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC)'. [Online]. Available: https://capec.mitre.org/index.html. [Accessed: 25-Feb-2019].

[28] 'Category:OWASP Top Ten Project - OWASP'. [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. [Accessed: 25-Feb-2019].

[29] I. Kotenko and E. Doynikova, 'The CAPEC based generator of attack scenarios for network security evaluation', in *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2015, pp. 436–441.

[30] S. Caltagirone, A. Pendergast, and C. Betz, 'The Diamond Model of Intrusion Analysis'.

[31] 'NVD - Vulnerability Metrics'. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss. [Accessed: 25-Jul-2019].

[32] 'NVD - CVE-2016-5235'. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2016-5235. [Accessed: 25-Jul-2019].

[33] 'NVD - CVSS v3 Calculator'. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator. [Accessed: 25-Jul-2019].

[34] 'Microsoft Security Development Lifecycle Practices'. [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl/practices#practice4. [Accessed: 01-Mar-2019].

[35] 'Getting Started - Microsoft Threat Modeling Tool - Azure | Microsoft Docs'. [Online]. Available: https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool-getting-started. [Accessed: 01-Mar-2019].

[36] D. M. Gorski, 'Home | Elevation of Privilege (EoP) - Threat Modelling Card Game'. [Online]. Available: https://eopgame.azurewebsites.net/. [Accessed: 01-Mar-2019].

[37] I. A. Tøndel, T. Daniel, O. Martin, G. Jaatun, and D. Cruzes, 'Understanding challenges to adoption of the Microsoft Elevation of Privilege game', 2018.

[38] 'Home | Tutamantic'. [Online]. Available: http://www.tutamantic.com/. [Accessed: 25-Feb-2019].

[39] 'ThreatModeler Software Inc - Industry's #1 Threat Modeling platform'. [Online]. Available: https://threatmodeler.com/. [Accessed: 25-Feb-2019].

[40] 'ThreatModeler Identified by Gartner in the "Hype Cycle for Application Security, 2017" Report', 2017. [Online]. Available: http://www.prweb.com/releases/2017/12/prweb15027487.htm. [Accessed: 01-Mar-2019].

[41] 'Introducing Project Seasponge: Quick and Easy Threat Modeling | Mozilla Security Blog'.

[Online]. Available: https://blog.mozilla.org/security/2015/04/02/introducing-project-seasponge-quick-and-easy-threat-modeling/. [Accessed: 09-Jul-2019].

[42] P. Brangetto, E. Çalişkan, H. Rõigas Cyber, and R. Teaming, 'Cyber Red Teaming - Organisational, technical and legal implications in a military context', 2015.

[43] M. Dalziel and H. Dalziel, *Next Generation Red Teaming*. Syngress Media Incorporated, 2015.

[44] J. G. Oakley, *Professional Red teaming : conducting successful cybersecurity engagements*. Apress, 2019.

[45] S. Mansfield-Devine, 'The best form of defence – the benefits of red teaming', *Computer Fraud and Security*, vol. 2018, no. 10, pp. 8–12, Oct. 2018.

[46] A. Applebaum, D. Miller, B. Strom, C. Korban, and R. Wolf, 'Intelligent, automated red team emulation', 2016, pp. 363–373.

[47] A. Harper *et al.*, *Gray hat hacking : the ethical hacker's handbook*. McGraw-Hill, 2018.

[48] H. Johnson, 'Red Team v. Blue Team? They Are in Fact One - The Purple Team'. [Online]. Available: https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/red-team-v-blue-team-they-are-in-fact-one-the-purple-team/. [Accessed: 14-Aug-2019].

[49] I. Neil, *CompTIA security+ Certification Guide*. Packt, 2018.

[50] G. Burton, 'TalkTalk's lessons for cyber security | Computing', 2015. [Online]. Available: https://www.computing.co.uk/ctg/analysis/2432169/talktalks-lessons-for-cyber-security. [Accessed: 20-Jul-2019].

[51] I. Winkler and A. T. Gomes, *Advanced persistent security*. Syngress, 2016.

[52] F. L. Greitzer and D. A. Frincke, 'Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation', *Advances in Information Security*, vol. 49, pp. 85–113, 2010.

[53] P. Chen, L. Desmet, and C. Huygens, 'A Study on Advanced Persistent Threats', 2014, pp. 63–72.

[54] 'Cyber Kill Chain® | Lockheed Martin'. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Accessed: 25-Jul-2019].

[55] 'MITRE ATT&CK™'. [Online]. Available: https://attack.mitre.org/. [Accessed: 24-Jul-2019].

[56] D. Strom, 'What is Mitre's ATT&CK framework? What red teams need to know | CSO Online', 2018. [Online]. Available: https://www.csoonline.com/article/3267691/what-is-mitres-attandck-framework-what-red-teams-need-to-know.html. [Accessed: 10-Aug-2019].

[57] H. Al-Mohannadi, I. Awan, J. Al Hamar, Y. Al Hamar, M. Shah, and A. Musa, 'Understanding awareness of cyber security threat among IT employees', in *Proceedings - 2018 IEEE 6th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2018*, 2018, pp. 188–192.

[58] W. Knowles, A. Baron, and T. McGarr, 'The simulated security assessment ecosystem: Does penetration testing need standardisation?', *Computers and Security*, 2016.

[59] 'GitHub - nshalabi/ATTACK-Tools: Utilities for MITRE™ ATT&CK'. [Online]. Available: https://github.com/nshalabi/ATTACK-Tools. [Accessed: 12-Aug-2019].

[60] D. Miller, R. Alford, A. Applebaum, H. Foster, C. Little, and B. Strom, 'Automated Adversary Emulation: A Case for Planning and Acting with Unknowns'.

[61] ‘CALDERA User Documentation — CALDERA 0.3.0 documentation’. [Online]. Available: https://caldera.readthedocs.io/en/latest/. [Accessed: 13-Aug-2019].

[62] ‘ATT&CK™ Navigator’. [Online]. Available: https://mitre-attack.github.io/attack-navigator/enterprise/. [Accessed: 18-Aug-2019].

[63] ‘GitHub - mitre/caret: CARET - A tool for viewing cyber analytic relationships’. [Online]. Available: https://github.com/mitre/caret. [Accessed: 13-Aug-2019].

[64] ‘GitHub - pan-unit42/playbook_viewer’. [Online]. Available: https://github.com/pan-unit42/playbook_viewer. [Accessed: 13-Aug-2019].

[65] ‘Vectr’. [Online]. Available: https://vectr.io/. [Accessed: 30-Jun-2019].

[66] S. Hall and I. Monogioudis, ‘Purple Teaming with Vectr, Cobalt Strike, and MITRE ATT&CK™ | Digital Shadows’, 2019. [Online]. Available: https://www.digitalshadows.com/blog-and-research/purple-teaming-with-vectr-cobalt-strike-and-mitre-attck/. [Accessed: 11-Aug-2019].

[67] ‘Scythe’. [Online]. Available: https://www.scythe.io/platform. [Accessed: 15-Aug-2019].

[68] ‘Red Team APT Attack Scenarios | XM Cyber’. [Online]. Available: https://xmcyber.com/haxm-use-cases-red-team/. [Accessed: 26-Jul-2019].

[69] L. Ertaul and M. Mousa, ‘Applying the Kill Chain and Diamond Models to Microsoft Advanced Threat Analytics’, in *Int’l Conf. Security and Management*.

[70] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, ‘Cyber-attack modeling analysis techniques: An overview’, in *Proceedings - 2016 4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2016*, 2016, pp. 69–76.

[71] S. Moskal, S. J. Yang, and M. E. Kuhl, ‘Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach’, *Journal of Defense Modeling and Simulation*, 2018.

[72] A. Marback, H. Do, K. He, S. Kondamarri, and D. Xu, ‘A threat model-based approach to security testing’, *Software: Practice and Experience*, vol. 43, no. 2, pp. 241–258, Feb. 2013.

[73] T. Li, E. Paja, J. Mylopoulos, J. Horkoff, and K. Beckers, ‘Security attack analysis using attack patterns’, in *Proceedings - International Conference on Research Challenges in Information Science*, 2016.

[74] P. Bottomley and W. Beukema, ‘Signal the ATT&CK: Part 1 - PwC UK’. [Online]. Available: https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/signal-att-and-ck-part-1.html. [Accessed: 24-Jul-2019].

[75] S. Randhawa, B. Turnbull, J. Yuen, and J. Dean, ‘Mission-Centric Automated Cyber Red Teaming’, in *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018*, 2018, pp. 1–11.

[76] H. T. Ray, R. Vemuri, and H. R. Kantubhukta, ‘Toward an Automated Attack Model for Red Teams’, *IEEE Security and Privacy Magazine*, vol. 3, no. 4, pp. 18–25, Jul. 2005.

[77] Y.-H. Kim and W. H. Park, ‘A study on cyber threat prediction based on intrusion detection event for APT attack detection’, *Multimedia Tools and Applications*, vol. 71, no. 2, pp. 685–698, Jul. 2014.

[78] A. Applebaum, S. Johnson, M. Limiero, and M. Smith, ‘Playbook Oriented Cyber Response’, 2018, pp. 8–15.

[79] V. D. Veksler, N. Buchler, B. E. Hoffman, D. N. Cassenti, C. Sample, and S. Sugrim,

‘Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users’, *Frontiers in Psychology*, vol. 9, no. MAY, 2018.

[80] D. J. Bodeau, C. D. Mccollum, and D. B. Fox, ‘Cyber Threat Modeling: Survey, Assessment, and Representative Framework’, 2018.

[81] S. Bhatt, P. K. Manadhata, and L. Zomlot, ‘The operational role of security information and event management systems’, *IEEE Security and Privacy*, vol. 12, no. 5, pp. 35–41, 2014.

[82] G. Bhat, ‘Introducing Splunk Security Use-Cases’. [Online]. Available: https://www.splunk.com/blog/2016/02/03/introducing-splunk-security-use-cases.html. [Accessed: 10-Aug-2019].

[83] ‘Interfaces for Working with ATT&CK’. [Online]. Available: https://attack.mitre.org/resources/working-with-attack/. [Accessed: 16-Aug-2019].

[84] R. Marty, *The Security Data Lake*. O’Reilly Media, Inc., 2015.

[85] ‘Business Intelligence and Analytics Software’. [Online]. Available: https://www.tableau.com/. [Accessed: 13-Aug-2019].

[86] ‘GitHub - Cyb3rPanda/Tableau-ATTCK: Understanding ATT&CK Matrix for Enterprise’. [Online]. Available: https://github.com/Cyb3rPanda/Tableau-ATTCK. [Accessed: 18-Aug-2019].

[87] ‘Mitre Att&ck Caret’. [Online]. Available: https://mitre-attack.github.io/caret/#/. [Accessed: 17-Aug-2019].

[88] Bitdefender, ‘An APT Blueprint: Gaining New Visibility into Financial Threats’, 2019.

[89] ‘Open Cyber Challenge Platform’. [Online]. Available: https://opencyberchallenge.net/. [Accessed: 14-Aug-2019].