ThreatMAP: Mapping Attack Plans from the Techniques, Tactics and Procedures of the MITRE ATT&CK Enterprise Framework for Plan Recognition

Emilie Coote[1], Taylor Perkins[2]

School of Computing, Queen's University, Kingston, Canada

Abstract

In this research the application of plan recognition is applied in the cybersecurity domain for the detection of anomalous behaviours indicative of cyber kill chains occurring on enterprise Information Technology (IT) networks. Cyberattacks are becoming much more frequent on enterprise networks. As the kill chains developed for cyberattacks become increasingly sophisticated, they become more and more difficult to detect and are only alerted upon after a cyberattack has occurred. The cyber threat landscape is ever evolving and there exists a multitude of combinations of techniques and tactics that can be used to develop a cyberattack, increasing the need for automating the detection of the kill chains outlined by the Mitre Attack Enterprise Matrix. The tactics and techniques of the MITRE ATT&CK Enterprise Framework allow for the unification of network and host-based alerting, providing greater visibility on the network. By modelling the cyber kill chain, it is possible to match the actions of an attacker before the network is compromised.

1. Introduction

With cyberattacks becoming more sophisticated with the implementation of adversaries' defense evasion techniques, there is an increased need for methods to detect these malicious activities before a network becomes compromised. This combined with the increasing usage of the internet as more systems become connected, and more reliant on IT networks, the volume of data that must be analyzed also increases. As adversarial behaviour becomes increasingly similar to normal network behaviour, cyberattacks become easier to masquerade in the flood of collected data, making traditional intrusion detection methods less effective. [1, 2, 3].

Lockheed Martin published the cyber kill chain framework that describes the stages that an adversary must take in order for a cyberattack to be successful [4]. Developed for the purpose of the identification and prevention of anomalous cyber activity, it is meant to break down the stages of a cyberattack into sections where mitigation can be put in place to stop the chain of attack. Lockheed Martin describes the seven stages of the cyber kill chain as follows, reconnaissance, weaponization, delivery, exploitation, installation, command and control, and the actions on objectives stages.

Another framework, the MITRE ATT&CK Enterprise Framework was also developed to provide an understanding of cyber threats, mapping out the common tactics and techniques utilized by adversaries during an attack [5]. This framework allows analysts to categorize adversarial behaviours based on observed techniques. The MITRE ATT&CK Enterprise Framework describes fourteen tactics, reconnaissance, resource development, initial access execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration and impact.

Combining the knowledge of the cyber kill chain and the tactics and techniques of the MITRE ATT&CK matrix attack plans provides a description of the possible avenues of cyberattack that an adversary may take. Modelling this domain would provide a framework to compare enterprise IT network events for the detection of anomalous behaviours.

Plan recognition, a research area in automated planning, is a field of artificial intelligence (AI) that infers the goals of a given set of actions through the observation of behaviours. These observations can be compared to the developed plans and policies generated by the domain and problem definitions. The plan recognition model will be able to describe the set of tactics and techniques of the MITRE ATT&CK Enterprise Framework for the purpose of detecting anomalous network behaviours. Collected observations from network and host logs found on an enterprise IT network can then be compared against the modelled anomalous behaviours to determine if cyber kill chains are occurring.

Using plan recognition does not require any data for training, removing the need for training datasets. This approach addresses the need to identify all malicious events. For anomaly detection techniques the models either require labeled datasets or use machine and deep learning algorithms to identify anomalous behaviours. This can be problematic when the malicious events aren't always known and therefore are not labelled. Modelling adversary behaviours addresses this concern by viewing determined behaviours in the context of deploying a cy-

CISC-813: Automated Planning – Final Project

ber kill chain rather than individual events. Determining this behaviour using the MITRE ATT&CK Enterprise Matrix provides a framework that the cyber kill chain can be compared against, and allows for different attack variations to be included for detection. Modelling adversarial behaviours also gives the model the flexibility to adapt to the changing threat landscape and does not need to be updated for each discovered attack, only when new tactics and techniques are discovered. This removes the requirement for retraining of anomaly detection models using machine and deep learning algorithms.

In this paper, we introduce ThreatMAP, the application of planning recognition for the detection of malicious activities as described by the MITRE ATT&CK Enterprise Matrix. The representation of the matrix is programmed in Planning Domain Definition Language (PDDL) and the observation file is generated from enterprise network data.

1.1. Cyber Kill Chains

A cyber kill chain is a framework that is used to define the seven stages that a cyberattack must achieve in order to be considered successful.

1. The first stage, **Reconnaissance** is where the attacker will gather information on the target network, this includes identifying available systems, possible vulnerabilities, and potential points of entry. Methods to achieve this phase would include active scanning and gathering host information, including active accounts, operating system information, and services available on the network.
2. The next stage is **Weaponization**, where the attacker will develop attacks using strategies including building custom malware or leveraging prebuilt frameworks. These attacks are based on the information gained in the reconnaissance stage, and may include techniques such as building phishing emails.
3. The next stage is the **Delivery** of the weaponized payload, with the goal of getting the developed attack onto a targeted computer. This can be done through phishing emails, infected USB keys, and exploiting publicly facing applications.
4. After the delivery of the payload, **Exploitation** can occur in the target system. This includes actions such as the installation of backdoors, exploiting available services, and user initiated execution.
5. After the target has been exploited, it is important to establish Persistence on the system, this is where **Installation** takes place. This includes the installation of additional malware to maintain control of the system, the addition of user accounts, the creation of scheduled tasks, as well as privilege escalation.
6. Once persistence is gained through installation, **Command and Control** of the system can occur. This is when the attacker has a connection to the system and can continue to execute actions on the system, including lateral movement. This leads into the final stage, actions on Objective.
7. With **Actions on Objective**s the attacker has full control of the system, or even the network at large, and can carry out any malicious activities including exfiltration, manipulation, ransomware, and even system or network wide disruptions.

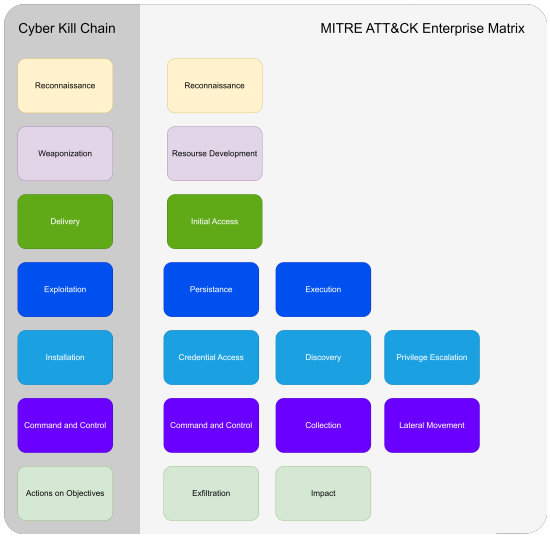

Figure 1: Mapping of the Cyber Kill Chain to The MITRE ATT&CK Enterprise Matrix

The MITRE ATT&CK Enterprise Matrix further breaks the cyber kill chain into fourteen tactics, each having a number of associated techniques. In 1 the fourteen tactics have been mapped out to the seven stages of the cyber kill chain, nothing that defence evasion does not fall under any one category as it is a technique that can be used at any time after the exploitation state has been reached.

1.2. Intrusion Detection

There are generally two methods used for intrusion detection for enterprise networks, signature based and anomaly detection. Signature based detection is used when an exploit or cyberattack has distinguishable features and rules can be created. Alerts for the enterprise

network would be generated when a given signature is detected in the data. One major drawback of signature detection is the delay of the signatures being written and databases being updated. With signature detection, the exploit must first be known and a signature written, unlike with anomaly detection. Anomaly detection methods including AI are used to distinguish benign enterprise network events from malicious ones. Anomaly detection does not require that the parameters of a cyberattack are known, however, it must be considered where there are enterprise network events that individually would be considered normal operations, however, combined with other events, it would indicate the occurrence of a cyber kill chain. This can sometimes be a difficult differentiation to make, even when using machine and deep learning techniques.

Using plan recognition would combine the two methods. The resultant model of this research provides the possible plans and policies that can be built from the Mitre ATT&CK Enterprise Matrix, thereby providing a signature. It is also not limited by the need to update signatures as new attacks become available. Defining the possible actions that are available would build plans that adapt to the evolving threat landscape. The MITRE ATT&CK Enterprise Framework also incorporates both network and host-based events. The correlation of these events gives better insight into what is occurring on the network.

1.3. Automated Planning and Goal Recognition

Automated planning leverages algorithms that aim to develop strategies that result in solutions to specified problems. It is commonly used in areas such as event scheduling and path optimization. Automated planning requires a domain to be modelled and a problem to be described in order to produce plans. The domain is comprised of a set of actions made up of predicates. These predicates can be applied to a number of variables to enable the modelling of a given domain.

Rameriz et al. defines planning recognition as the determination of a goal given a set of observed actions [6]. Plan recognition is a field of automated planning where possible goals are given based on a provided set of observables. An observation is a predicate corresponding to achieved actions. The observables in this research are a list of observed events occurring on a given network. The application of plan recognition is to determine whether given observations allow plans to be generated by the plan recognition model, if so the plan would be a valid plan in the given domain.

2. A Planning Model for Detecting Cyber Kill Chains

This paper proposes the implementation of ThreatMAP, an automated planning to model cyber kill chains as described by the MITRE ATT&CK Enterprise Matrix for plan recognition. This solution addresses the delay found using cyberattack signatures, and gives context to independently occurring events that may be part of a cyber kill chain. ThreatMAP is also flexible and can easily be updated when new techniques and tactics are discovered. The goal of this research is to develop a model that can be used to detect occurring cyber kill chains in enterprise network data and would alert analysts to cyberattacks before any data is compromised. This is achieved by using the model to determine if a sequence of observed actions is part of the possible plans contained within the model.

2.1. States

Each state in the ThreatMAP model is represented as one of the tactics from the MITRE ATT&CK Enterprise Matrix. There are fourteen tactics described by this Matrix. These states are divided into categories based on the stages of the cyber kill chain.

The tactics first had to be mapped to the cyber kill chain. This allows the definition of allowed movements between the tactics as described in the cyber kill chain. This mapping is described in 1. The adversary will only need to reach one tactic for each of the stages of the cyber kill chain.

Defence evasion is not covered by the cyber kill chain, however, this tactic describes techniques that are used to evade detection once the adversary has gained access to the system. This tactic does not aid in the advancement of the cyber kill chain and therefore is not represented as a state in this domain.

2.2. Actions

The actions in this planning domain are the techniques found under the tactics of the MITRE ATT&CK Enterprise Matrix. They describe the transitions between each state. To scope this research a limit was implemented on the number of techniques to model for each tactic. A number of Advanced Persistent Threat (APT) groups. APT29, Axiom, Ferocious Kitten, and Metador were chosen, and their associated techniques have been translated into actions.

For each stage in the cyber kill chain, there are a number of actions that could occur in order to transition to the next stage. Each action is described by the associated technique or sub technique from the MITRE ATT&CK Enterprise Matrix. The action that is chosen by the plan-

ner is dependent on the state of the cyber kill chain on the computer network.

In Listing technique 1566.001 Spearphishing Attachment, a subtechnique of phishing, is described [7]. This action takes 5 parameters, the attacker, user account, computer, delivery state, and exploitation state. The precondition predicate, `(at ?s1)`, restricts this action to only occurring at the initial access stage of the cyber kill chain, while the `(unsecured_credentials ?a ?u ?c)` predicate ensures that previous actions, or techniques, in the cyber kill chain have uncovered that for a given user account on the targeted computer that the advisory has uncovered unsecured credentials. The effect of this action is that it can be determined that the user account has been spearfished.

Listing 1: Technique 1566.001

```
; Phishing: Spearphishing Attachment
(:action t1566_001
    :parameters (
        ?a - attacker
        ?u - user
        ?c - computer
        ?s1 - delivery
        ?s2 - exploitation
    )
    :precondition (and
        (at ?s1)
        (unsecured_credentials ?a ?u ?c)
    )
    :effect (and
        (not (at ?s1))
        (at ?s2)
        (been_spearfished ?u)
    )
)
```

The actions listed, along with 37 others are used to describe the state transitions as the adversary proceeds through the stages of the cyber kill chain. In each action predicates are added to describe the changes on the network that are the result of the cyber kill chain occurring. These changes include the discovery of vulnerabilities, escalation of privileges, and systems becoming exploited, among others described further in this paper. These actions help enable state transitions. The state transitions are determined through valid transitions determined by the cyber kill chain framework. An example of a valid attack graph is featured in 2 where the techniques associated with APT29 describe the transitions between the states of the MITRE ATT&CK Enterprise Matrix. Each of the described techniques shown in 2 in the ThreatMAP implementation are labelled and the lighter grey lines denote other possible transitions. These other state transitions are actions not described by the techniques associated with APT29 but may be part of other cyber kill chains.

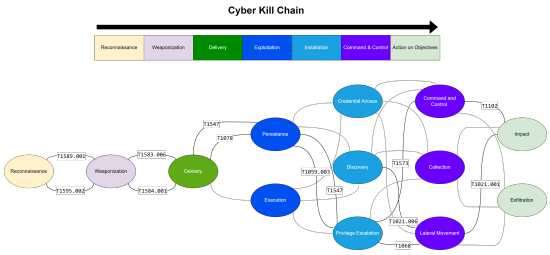

Figure 2: APT29 Techniques State Transitions

2.3. Types

An enterprise network has a number of users and systems on their network, all of which may be vulnerable to cyberattacks and need to be included in the modelling as parameters. Many different parameters can be utilized within the actions not limited to the users and the systems, the status of the network, account access, and the position of the adversary also need to be included. These are all modelled as objects and have corresponding predicates. There are 15 types defined in this domain, 8 entities and 7 stages of the cyber kill chain.

Entities

- attacker
- user
- network
- network_domain
- computer
- software
- token
- exploit

Stages

- reconnaissance
- weaponization
- discovery
- exploitation
- installation
- command_and_control
- act_on_objective

2.4. Implementation

ThreatMAP is a Fully Observable Deterministic (FOD) representation programmed in PDDL. The techniques from the MITRE ATT&CK Enterprise Matrix are known

actions and are modelled to have deterministic outcomes, making the domain fully observable. A deterministic classical planning modelling approach has been taken for the MITRE ATT&CK Enterprise Matrix.

The way in which this model is implemented is by describing the variables found on an enterprise network, including the systems, user accounts, and any associated vulnerabilities that may be present. The status of the cyberattack must also be tracked, this includes any obtained information that an adversary discovers on the network and any exploits that the adversary deploys. The state of the enterprise network as the adversary traverses the cyber kill chain is tracked by the addition of predicates to the environment as the actions occur. The actions act as transitions between the stages of the cyber kill chain.

The 13 states of the MITRE ATT&CK Enterprise Matrix, not including defence evasion, are broken down into the 7 stages of the cyber kill chain. The actions on objective stage has been condensed into a goal stage as both the exfiltration and impact tactics are the final stage of a given cyber kill chain. This mapping of stage types to state objects is described in Listing 2. This allows for a simple `(at ?s)` predicate to be used in each action to control the transition between each stage of the cyber kill chain in order. The described model is then used for

Listing 2: MITRE ATT&CK Domain Objects

```
(define (problem mitreattack)
    (:domain mitreattack)
    (:objects
        ; 7 states
        recon - reconnaissance
        wpze - weaponization
        delv - delivery
        exe - exploitation
        pers - exploitation
        priv_esc - installation
        cred_access - installation
        disc - installation
        lat_mov - command_and_control
        col - command_and_control
        cc - command_and_control
        goal - act_on_objective

        ...
    )
```

plan recognition. The entities on the network can be described along with the associated predicates through processing network and host logs. Observations can be derived from host and network event monitoring solutions. In this work, the cyber kill chains are developed manually, but it is an area for future work to develop a tool to allow for the automatic generation of observed fluents.

For this research 5 separate cyber kill chains are implemented to demonstrate the applicability of the ThreatMAP planning model. The fluents associated with each of the 5 cyber kill chains are described in the goal and the LAMA planner is then used to determine if the given fluents indicate the unfolding of a cyber kill chain. The planner output produced a possible plan based on the observations in the network and host logs, while this is useful for an analyst to know what to investigate, more important is that the given fluents allow for policies to be determined from the model, indicating possible malicious behaviour on the computer network.

2.4.1. Domain

The domain describes the predicates and actions for this problem space. We include a number of predicates that describe the state of the environment, including determining the stage of the cyber kill chain, the user access, and whether the users or computers on the network are exploitable. Listing 3 provides a sample of the possible predicates included in ThreatMAP.

Listing 3: MITRE ATT&CK Domain Predicates

```
(has_credential ?a - attacker ?u - user)
(is_exploitable ?c - computer)
(been_spearfished ?u - user)
(has_vulnerability ?c - computer)
(has_c2_channel ?c - computer)
(in_botnet ?c - computer)
(network_scanned ?n - network)
(malware_running ?c - computer)
```

Techniques selected from the MITRE ATT&CK Enterprise Matrix modelled as actions in ThreatMAP. 4 APT groups are used to select 38 different actions from across all the stages of the cyber kill chain. These actions describe a number of different scenarios including botnets, credential dumping, RDP hijacking, and spearphishing among others. Each one of these actions model the techniques found under the tactics of the MITRE ATT&CK Enterprise Matrix and demonstrates the transition between the stages of the cyber kill chain.

2.4.2. Problem

The problem is described using the variables on the enterprise network as objects, this includes the states of the MITRE ATT&CK Enterprise Matrix, users, computers, and the adversary. In the problem file, all of the objects for the scenarios are included. Two types of objects are described in the domain: the states divided by stages of the cyber kill chain, and the entities found on the computer network. In the implementation of ThreatMAP

one attacker, on one computer network, with one computer, and one user account is included. Other aspects of a typical enterprise network including the network domains, and possible exploits have also been introduced. This problem file can be further expanded to include additional entities of each type in order to model a more realistic enterprise network environment. This allows the ThreatMAP model to be adaptable to any given network.

The initial state of ThreatMAP is a constant, Every cyber kill chain that is to be detected begins at the reconnaissance stage. Therefore the initial state is that the given adversary is at `recon`, the reconnaissance state. Next, the observed fluents are described. Finally, the goal is described, this is that the adversary has reached one of the two goal states, infiltration or impact

2.4.3. Observations

The observations for plan recognition are predicates that are derived from observed events or alerts obtained from network and host monitoring. Host and network monitoring events can be translated into fluents describing the state of a given computer network. The model does not require a fluent derived from each stage of the cyber kill chain.

The observed predicates from the network and host monitoring would be included in the problem file goal, enabling ThreatMAP to detect if these observations from the enterprise network allow a valid policy. Not all activities occurring on the network can be collected and described as a fluent as there are some techniques of the cyber kill chain that are employed outside of a given computer network. An example of this would be the acquisition of a given domain. After gaining knowledge of the services and accounts through a detectable scan of a network the adversary could then use that information to acquire domains in which they could launch attacks from. This acquired domain could then be used in spearphishing campaigns to obtain credentials and further the cyber kill chain. While this action is not described, the predicates that are required for the cyber kill chain to be a valid policy would require the fluent describing a user being spearfished to be included as an observation. The fluents found in the goal are meant to be observable events from the computer network.

If the planning model does not return a solution for a given set of observations it would then be determined that the observed events are likely not part of a defined cyber kill chain. In the implementation of ThreatMAP 5 cyber kill chains are described through observations. These kill chains have been included to demonstrate the applicability of the ThreatMAP model in the detection of cyber kill chains occurring on a computer network. In Listing 4 one of the observations pertaining to a possible kill chain using the techniques associated with APT29

Listing 4: Network Observation Predicates

```
; Observations Kill Chain 1 (Ferocious Kitten)
(unsecured_credentials attacker user computer)
(been_spearfished user)
(is_exploitable computer)
(gained_persistence attacker computer)
```

are described.

.

3. Evaluation

The aim of this research is to build a model that represents the valid transitions of the tactics of the MITRE ATT&CK Enterprise Matrix. In order to achieve this aim the following must be achieved

- Each MITRE Tactic is described as a State
- Each MITRE Technique is described as a valid Action
- Correctly translating movement between stages with fluents
- Accurately modelling a cyber kill chain as a resultant policy
- A FOD model that can be used for the detection of occurring cyber kill chains

The validity of the model can be evaluated through observations derived from network data during the completion of a cyber kill chain. These observation sequences representing known cyber kill chains can be developed and used to determine the ability of the defined model to detect possible cyber kill chains.

3.1. Results

The aim of this work was to develop a planning model that is capable of detecting occurring cyber kill chains from observed actions within enterprise network data. This is achieved through defining actions, predicates, and types that are the foundation of the MITRE ATT&CK Enterprise matrix that builds out this domain. The problem space is then defined by the entities found on a given network. This problem space also includes the fluents that would be observed through enterprise network monitoring as 5 cyber kill chains, presented in Listing 5. The implementation of ThreatMAP successfully translates the MITRE ATT&CK Enterprise Matrix tactics and techniques into states and actions that describe the progression of a cyber kill chain. ThreatMAP is also capable of transitioning between states using derived fluents following the stages of the cyber kill chain. This is demonstrated through the policies resulting from the cyber kill chain

Listing 5: Cyber Kill Chain Observations

```
; Observations Kill Chain 1 (Ferocious Kitten)
(unsecured_credentials attacker_01 user_acct_01 computer_01)
(been_spearfished user_acct_01)
(is_exploitable computer_01)
(gained_persistence attacker_01 computer_01)

; Obervatations Kill Chain 2 (APT29)
(installed_tools attacker_01 computer_01)
(gained_persistence attacker_01 computer_01)

; Obervatations Kill Chain 3 (APT29)
(gained_persistence attacker_01 computer_01)
(exploit_installed exploit_01 computer_01)

; Obervatations Kill Chain 4 (Axiom)
(network_scanned network_01)
(in_botnet computer_01)
(malware_running computer_01)
(has_data computer_01)

;Obervatations Kill Chain 5 (Metador)
(installed_tools attacker_01 computer_01)
(has_system_access attacker_01 computer_01)
(installed_tools attacker_01 computer_01)
```

observations. These observations, found in the goal state, along with the associate domain and problem files were used with the LAMA planner to produce valid policies. These policies are presented in Listing 6.

ThreatMAP has been shown to detect through observed fluents possible ongoing cyber kill chains. This is demonstrated by the 5 cyber kill chains derived from the 4 described APTs that result in policies. The results show

Listing 6: Cyber Kill Chain Resultant Policies

```
; Policy Kill Chain 1 (Ferocious Kitten)
(t1598 attacker_01 user_acct_01 recon res_dev)
(t1586 user_acct_01 attacker_01 computer_01 res_dev init_access)
(t1566_001 attacker_01 user_acct_01 computer_01 init_access exe)
(t1204.002 attacker_01 user_acct_01 computer_01 exe cred_access)
(t1068 attacker_01 computer_01 cred_access cc)
(t1105 attacker_01 user_acct_01 computer_01 exploit cc goal)

; Policy Kill Chain 2 (APT29)
(t1589_001 user_acct_01 attacker_01 recon res_dev)
(t1583_001 domain_01 attacker_01 user_acct_01 res_dev init_access)
(t1078 user_acct_01 attacker_01 computer_01 domain_01 init_access exe)
(t1059_003 attacker_01 computer_01 exe cred_access)
(t1068 attacker_01 computer_01 cred_access cc)
(t1105 attacker_01 user_acct_01 computer_01 exploit cc goal)

; Policy Kill Chain 3 (APT29)
(t1598 attacker_01 user_acct_01 recon res_dev)
(t1586 user_acct_01 attacker_01 computer_01 res_dev init_access)
(t1547_001_pers attacker_01 user_acct_01 computer_01 init_access exe)
(t1547_001_pe attacker_01 computer_01 exploit_01 exe cred_access)
(t1573 computer_01 exploit_01 cred_access lat_mov)
(t1105 attacker_01 user_acct_01 computer_01 exploit lat_mov goal)

; Policy Kill Chain 4 (Axiom)
(t1595 recon res_dev computer_01 network_01)
(t1584_005 res_dev init_access computer_01 network_01)
(t1189 init_access cred_access computer_01)
(t1203 attacker_01 user_acct_01 cred_access cc computer_01)
(t1005 attacker_01 user_acct_01 cc cc computer_01)
(t1001_002 attacker_01 user_acct_01 cc goal computer_01)

; Policy Kill Chain 5 (Metador)
(t1589_001 user_acct_01 attacker_01 recon res_dev)
(t1583_001 domain_01 attacker_01 user_acct_01 res_dev init_access)
(t1078 user_acct_01 attacker_01 computer_01 domain_01 init_access exe)
(t1059_003 attacker_01 computer_01 exe cred_access)
(t1068 attacker_01 computer_01 cred_access cc)
(t1105 attacker_01 user_acct_01 computer_01 exploit cc goal)
```

that ThreatMAP can model the techniques and tactics of the MITRE ATT&CK Enterprise Framework and produce cyber kill chains as resultant policies. ThreatMAP can then be used to determine if observations from an enterprise network fit into the policies that it generates. This allows for the detection of activities on the enterprise network that may be part of a cyber kill chain. The proposed ThreatMAP model can be used for adaptive signature detection, and introduces context to independently occurring events.

4. Related Work

Plan recognition as planning is used in a number of domains. The work of Ramirez et al. outlines the possible application of plan recognition as planning [6]. In this work, the determination of plans for a given problem is explored. Ramirez et al. do not aim to find the optimal solution for a given problem, but a valid plan.

The application of plan recognition to the cybersecurity field has been approached previously. The work of Amos-Binks et al. outlines the application of plan recognition to attack graphs [1]. In this work, a network attack is modeled and plan based security metrics are explored, including the percentage that the plan is complete, the minimum remaining path length (MRPL) that is the shortest possible path to the described goal, and the identification of a choke point, which identifies areas where intervention could prevent the continuation of the cyberattack.

An early work by Geib et Al. explores the utilization of probabilistic planning in plan recognition to replace IDS [8]. In this work a probability model is proposed, modeling the actions that an adversary takes to achieve a goal, however, there are limitations including the inability to model evasion techniques, and that the model is capable of representing a single adversary on the network.

Planning recognition has also been applied to Wireless Local Area Network (WLAN) data in a similar way in the work of Chen et al [3]. WLAN data encompasses 802.11 radio packets and wireless device information. Their aim is to detect one of four types of attacks, Denial of Service (DoS), Media Access Control (MAC) spoofing, Main in the Middle (MITM), or Wi-Fi Protected Access (WPA) attack. Plan recognition techniques are used to predict the type of occurring attacks based on the behaviour of the devices on the network.

The research by Amos-Binks et al, Chen et al. and Wang et al. is focused on using the alerts from network data in order to build a planning model. However, these methods are limited to a subset of the possible cyberattacks and do not leverage the host data on the network. The application of the MITRE ATT&CK Enterprise Framework allows for the unification of network and host based alerting.

Another proposed model. Plan2Defend, leverages plan recognition models in order to monitor and respond to cyber threats on a smart grid [9]. Plan2Defend models a smart grid, and the status of the various operations occurring. The aim is to alert when anomalous behaviours are

occurring on the network. A number of attacks are run against a digital twin similar to the smart grid under attack and these observations are used against Plan2Defend. The goal is to recognize the attack and respond by alerting.

Penetration testing is another popular cybersecurity application. Shmaryahu et al and Bozic et al. [10] [11] present methods to automate penetration testing. The research focuses on leveraging PDDL to discover attack plans by performing penetration testing guided by PDDL. When the generated penetration plans are deemed successful in achieving a malicious objective part or a full kill chain is created. Based on the work by Bozic et al. further research could demonstrate that the attack plans could be used in reverse to detect the same malicious behaviour.

5. Summary

This research presents a plan recognition model that is capable of generalizing the method of attack based on the adversary behaviours outlined by the MITRE ATT&CK Enterprise Matrix. In this paper, cyber kill chains and the MITRE ATT&CK Enterprise Framework were summarized and a brief background on planning recognition was presented. Other works utilizing planning recognition in the field of cyber security were also explored. The details surrounding the implementation of ThreatMAP were also presented. The results show that ThreatMAP can be used as an improvement on signature detection in identifying potentially occurring cyber kill chains through enterprise network event observations. ThreatMAP is adaptable and can be used to contextualize distinct events as a form of intrusion detection.

5.1. Future Work

There are a number of areas where this research can be furthered:

- Running ThreatMAP against an enterprise network to determine performance and scalability
- Applying a probabilistic approach for each action
- Build in an alerting mechanism
- Automatic generation of observation files from enterprise networks
- Automation of actions to prevent the continuation of the cyberattack

References

[1] A. Amos-Binks, J. Clark, K. Weston, M. Winters, K. Harfoush, Efficient attack plan recognition using automated planning, in: 2017 IEEE Symposium on Computers and Communications (ISCC), IEEE, Heraklion, Greece, 2017, pp. 1001–1006. URL: http://ieeexplore.ieee.org/document/8024656/. doi:10.1109/ISCC.2017.8024656.

[2] L. Wang, Z.-T. Li, J. Ma, Y.-M. Ma, A.-F. Zhang, Automatic attack plan recognition from intrusion alerts, in: Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007), IEEE, Qingdao, 2007, pp. 1170–1175. URL: https://ieeexplore.ieee.org/document/4288026/. doi:10.1109/SNPD.2007.396.

[3] G. Chen, H. Yao, Z. Wang, An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition, in: 2010 Second International Conference on Future Networks, IEEE, Sanya, Hainan, China, 2010, pp. 168–172. URL: http://ieeexplore.ieee.org/document/5431861/. doi:10.1109/ICFN.2010.77.

[4] Cyber Kill Chain® | Lockheed Martin, ???? URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[5] T. M. Corporation, Matrix - Enterprise | MITRE ATT&CK®, ???? URL: https://attack.mitre.org/versions/v13/matrices/enterprise/.

[6] M. Ramírez, H. Geffner, Plan recognition as planning, in: Proceedings of the 21st International Joint Conference on Artificial Intelligence, IJCAI'09, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2009, p. 1778–1783.

[7] Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®, ???? URL: https://attack.mitre.org/versions/v13/techniques/T1566/.

[8] C. Geib, R. Goldman, Plan recognition in intrusion detection systems, in: Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01, volume 1, 2001, pp. 46–55 vol.1. doi:10.1109/DISCEX.2001.932191.

[9] T. Choi, R. K. L. Ko, T. Saha, J. Scarsbrook, A. M. Koay, S. Wang, W. Zhang, C. S. Clair, Plan2Defend: AI Planning for Cybersecurity in Smart Grids, in: 2021 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia), IEEE, Brisbane, Australia, 2021, pp. 1–5. URL: https://ieeexplore.ieee.org/document/9715679/. doi:10.1109/ISGTAsia49270.2021.9715679.

[10] D. Shmaryahu, G. Shani, J. Hoffmann, M. Steinmetz, Simulated penetration testing as contingent planning, Delft, The Netherlands, 2018, pp. 241–249. URL: https://ojs.aaai.org/index.php/ICAPS/article/view/13902.

[11] J. Bozic, F. Wotawa, Planning-based security testing of web applications with attack grammars, volume 28, Online, 2020, pp. 307–334. URL: http://link.springer.com/10.1007/s11219-019-09469-y. doi:10.1007/s11219-019-09469-y.