FalconForce

Detection mapping, how does your coverage compare to ATT&CK?

ATT&CK WORKSHOP
BRUSSELS, JUNE 2, 2022

Olaf Hartong

Defensive Specialist @ FalconForce

Detection Engineer and Security Researcher

- Built and/or led Security Operations Centers
- Threat hunting, IR and Compromise assessments

Former documentary photographer
Father of 2 boys
“I like warm hugs”

@olafhartong
github.com/olafhartong
olaf@falconforce.nl
olafhartong.nl / falconforce.nl

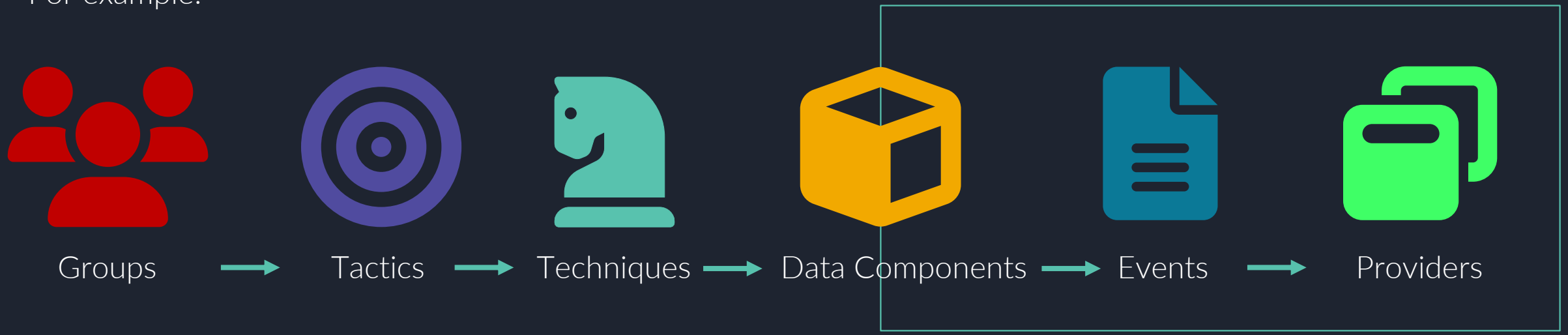
Why did we do this ?

- Measure coverage, also on a data component and event level
- Provide insights that allows us to advise clients what data to ingest
- Focus new development efforts
- Determine most utilized / required data
- Contribute back to ATT&CK

Linking data sources > data components > events

Since ATT&CK contains all kinds relations we can start combining sets of relationships with other sets.

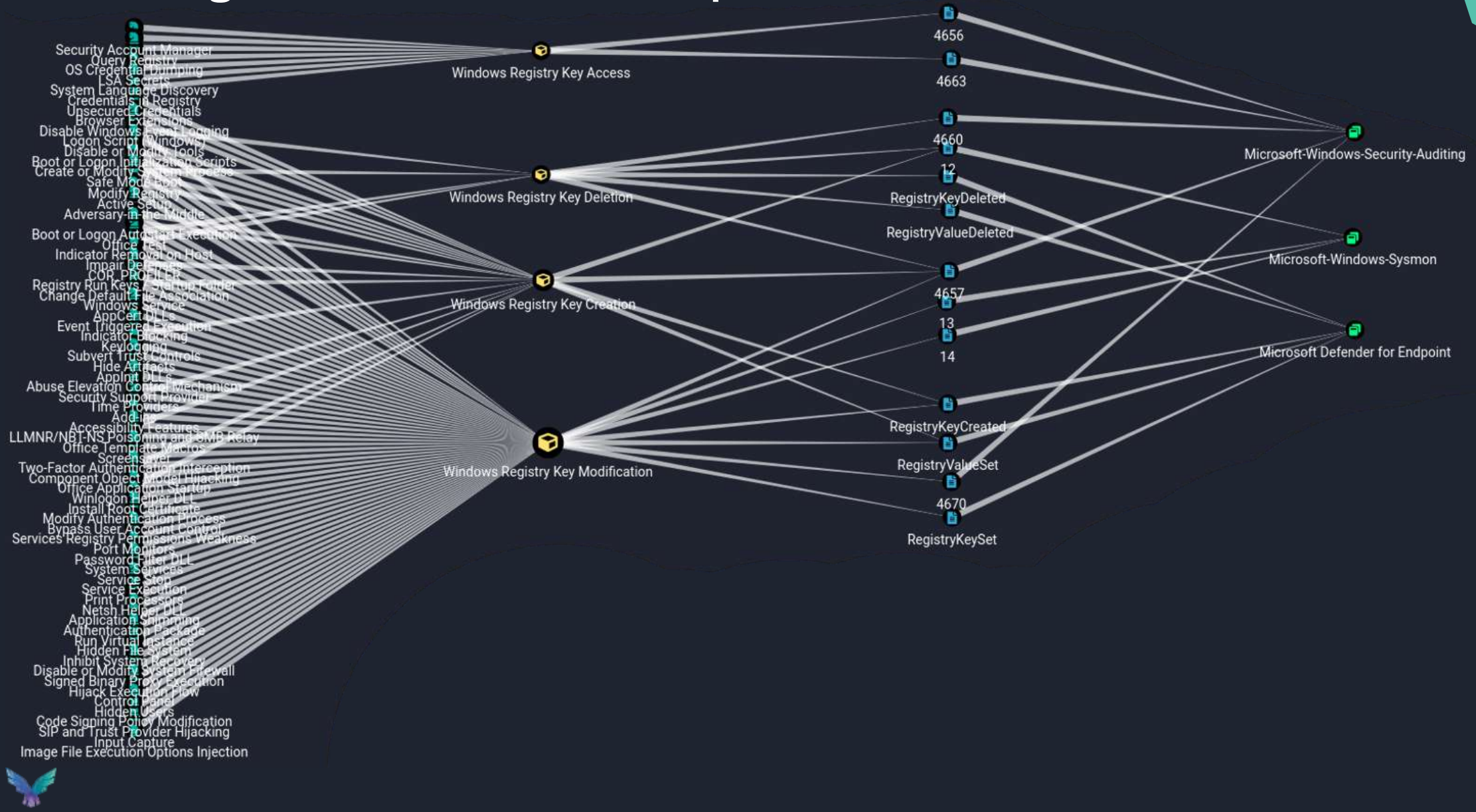
For example:



The same can be done for;
detection rules, attack/validation scripts, event fields and much, much more!

https://github.com/OTRF/OSSEM-DM

Visualizing theoretical relationships



Applying ATT&CK is based on interpretation

TRUTH

TRUTH

TRUTH

How we map our detections

```yaml
name: Possible Defender tampering commands
id: 0xFF-0035-Possible-Defender-tampering-commands-Win
tags:
  - BoosterPack
  - FalconFriday
  - DisableSecurity
os_family:
  - WindowsEndpoint
  - WindowsServer
fp_rate: Low
severity: Medium
attack:
  - {tactic: 'TA0005', technique: T1562, sub_technique: '001'}
data_sources:
  - provider: MDE
    event_id: ProcessCreated
    event_name: DeviceProcessEvents
    attack_data_source: Command
    attack_data_component: Command Execution
  - provider: MDE
    event_id: PowerShellCommand
    event_name: DeviceEvents
    attack_data_source: Script
    attack_data_component: Script Execution
permission_required: User
technical_description: |-
  This query combines known process commandlines with DeviceEvents with a specific PowerShell command
```

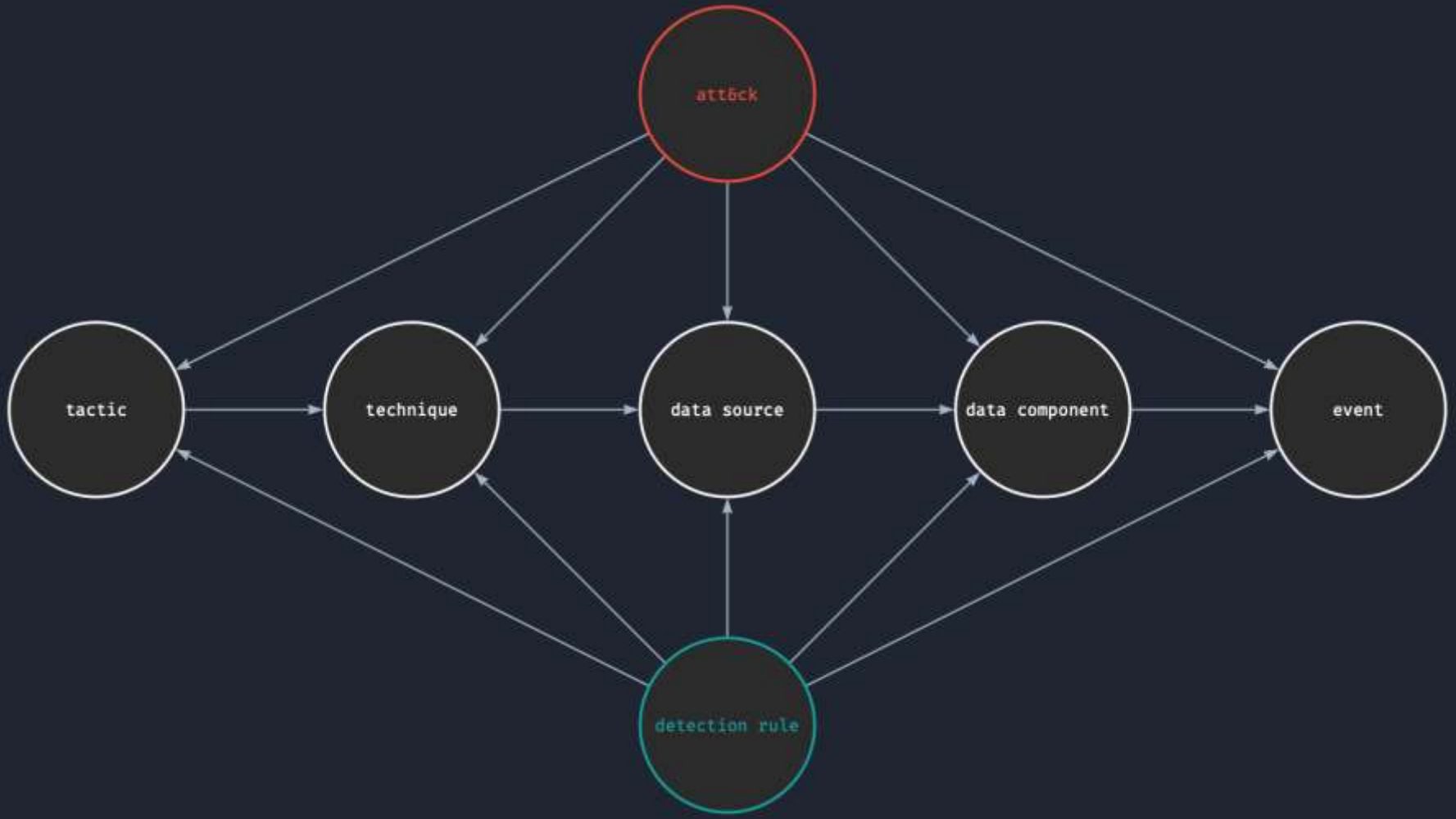
< Similar to ATT&CK, with server/client distinction

< ATT&CK

< ATT&CK data source and components *we use in the detection*

< ATT&CK, but specific to this detection

Some of the relationships we add to our detections



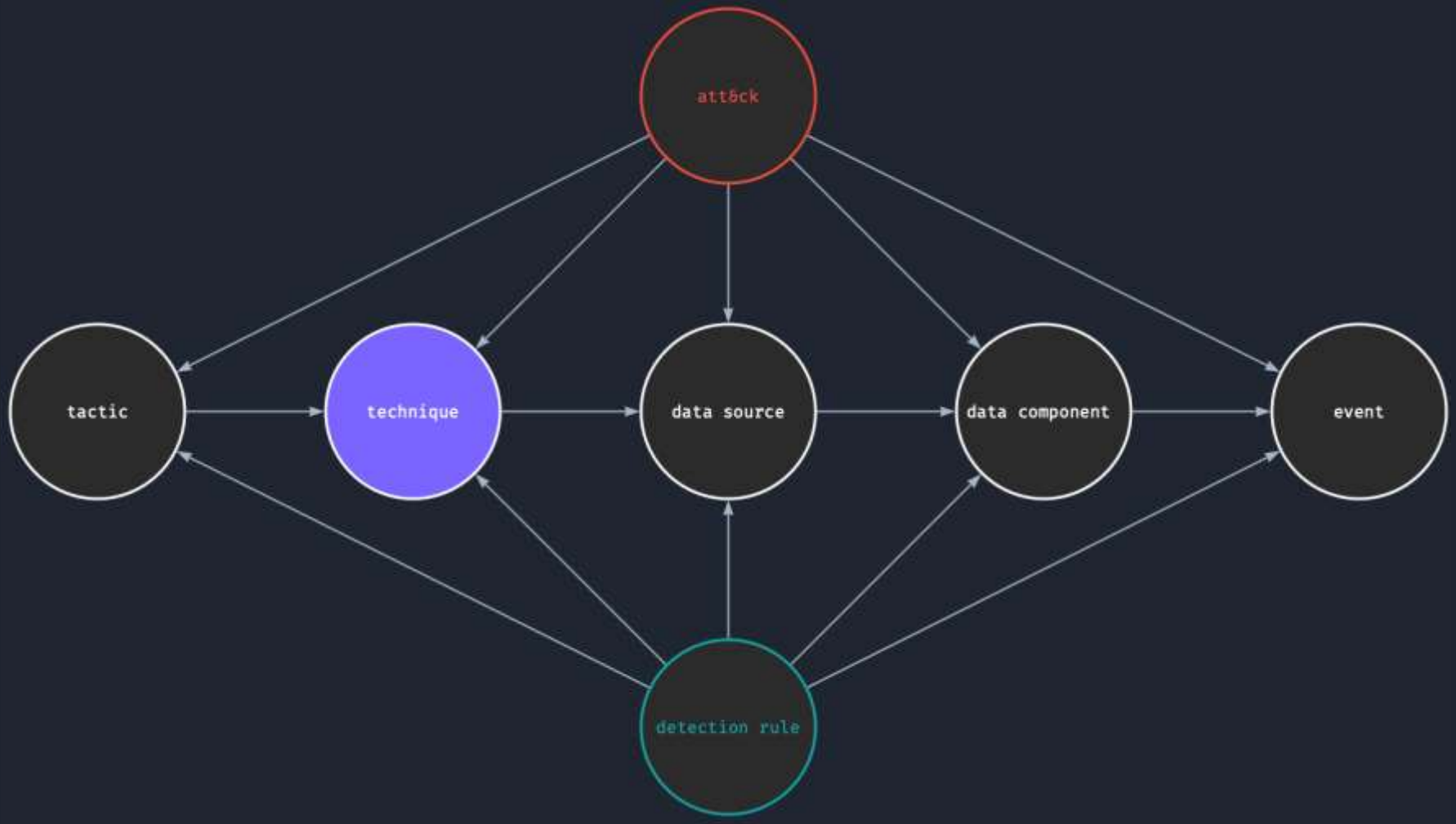
Validating alignment with ATT&CK

Since we have all these identical fields, we were curious how that would line up with ATT&CK.

Our expected outcomes were:

- We have a match
- We didn't tag our rule with the correct technique
- We didn't tag our rule with the expected data source and component
- The data source + data component is not tagged in ATT&CK yet

Checking alignment on Technique and data components



ATT&CK vs our rules, data component use top 15

Command Execution	257
Process Creation	216
Network Traffic Content	101
File Modification	100
File Creation	88
OS API Execution	87
Network Traffic Flow	85
Application Log Content	65
Windows Registry Key Modification	62
Network Connection Creation	58
Module Load	51
File Access	47
File Metadata	40
	35
Logon Session Creation	33

# of techniques

Command Execution	87
Process Creation	80
Process Access	72
Application Log Content	69
File Creation	62
Network Connection Creation	60
Windows Registry Key Modification	56
Module Load	55
User Account Authentication	47
Logon Session Creation	43
Cloud Service Modification	31
Active Directory Object Access	25
User Account Modification	24
Process Metadata	23
Network Traffic Content	21
OS API Execution	21

# of detections

Checking alignment on Technique and data components

Now that we have al these attributes, we can match list contents. When one of the rule components is not present in the ATT&CK technique's component list, its alignment is flagged as false.

Table 1 | Stats | Search | UTC | Done (0.091 s) | 344 records

Rule	RuleComponents	R_EventID	ID	Technique	TechniqueComponents	Aligned
0xFF-0030-Impacket_Secretsdump_Against_System-Win	Windows Registry Key Modification	["RegistryValueSet","LogonSuccess"]	T1003	OS Credential Dumping	["Active Directory Object ...	false
0xFF-0030-Impacket_Secretsdump_Against_System-Win	User Account Authentication	["RegistryValueSet","LogonSuccess"]	T1003	OS Credential Dumping	["Active Directory Object ...	false
0xFF-0205-Creation_Of_Files_Commonly_Used_By_Exploit_Tools-Win	File Creation	FileCreated	T1003	OS Credential Dumping	["Active Directory Object ...	false
0xFF-0282-Kerberos_Key_List_Attack-Win	Active Directory Credential Request	4769	T1003	OS Credential Dumping	["Active Directory Object ...	false
0xFF-0030-Impacket_Secretsdump_Against_System-Win	Windows Registry Key Modification	["RegistryValueSet","LogonSuccess"]	T1003.001	LSASS Memory	["Command Execution","P...	false
0xFF-0030-Impacket_Secretsdump_Against_System-Win	User Account Authentication	["RegistryValueSet","LogonSuccess"]	T1003.001	LSASS Memory	["Command Execution","P...	false
0xFF-0205-Creation_Of_Files_Commonly_Used_By_Exploit_Tools-Win	File Creation	FileCreated	T1003.001	LSASS Memory	["Command Execution","P...	false
0xFF-0205-Creation_Of_Files_Commonly_Used_By_Exploit_Tools-Win	File Creation	FileCreated	T1003.002	Security Account Manager	["Command Execution","...	false
0xFF-0031-Impacket_Secretsdump_drsuapi_Against_DC-Win	Active Directory Object Access	4662	T1003.003	NTDS	["File Access","Command...	false
0xFF-0030-Impacket_Secretsdump_Against_System-Win	Windows Registry Key Modification	["RegistryValueSet","LogonSuccess"]	T1003.004	LSA Secrets	["Command Execution","...	false
0xFF-0030-Impacket_Secretsdump_Against_System-Win	User Account Authentication	["RegistryValueSet","LogonSuccess"]	T1003.004	LSA Secrets	["Command Execution","...	false
0xFF-0031-Impacket_Secretsdump_drsuapi_Against_DC-Win	Active Directory Object Access	4662	T1003.004	LSA Secrets	["Command Execution","...	false

Component Confusion

User Account: User Account Authentication
*An attempt by a user to gain access to a network or computing resource, often by providing credentials (ex: Windows EID **4625** or /var/log/auth.log)*

Logon Session: Logon Session Creation
*Initial construction of a new user logon session (ex: Windows EID **4624**, /var/log/utmp, or /var/log/wmtp)*

Rule	RuleComponents	R_EventID	ID	Technique	TechniqueComponents	Aligned
0xFF-0014-Login_to_server_with_non_admin_account-Win	User Account Authentication	["LogonSuccess",null,"4624"]	T1021	Remote Services	Logon Session Creation	false
0xFF-0163-SSH_Password_Bruteforcing-Linux	User Account Authentication	LogonFailed	T1021	Remote Services	Logon Session Creation	false
0xFF-0202-Pentest_Logins-Win	User Account Authentication	LogonSuccess	T1021	Remote Services	Logon Session Creation	false
0xFF-0203-Metasploit_Logins-Win	User Account Authentication	LogonSuccess	T1021	Remote Services	Logon Session Creation	false
0xFF-0014-Login_to_server_with_non_admin_account-Win	User Account Authentication	["LogonSuccess",null,"4624"]	T1021.001	Remote Desktop Protocol	Logon Session Creation	false
0xFF-0202-Pentest_Logins-Win	User Account Authentication	LogonSuccess	T1021.001	Remote Desktop Protocol	Logon Session Creation	false
0xFF-0203-Metasploit_Logins-Win	User Account Authentication	LogonSuccess	T1021.001	Remote Desktop Protocol	Logon Session Creation	false
0xFF-0163-SSH_Password_Bruteforcing-Linux	User Account Authentication	LogonFailed	T1021.004	SSH	Logon Session Creation	false
0xFF-0202-Pentest_Logins-Win	User Account Authentication	LogonSuccess	T1021.006	Windows Remote Management	Logon Session Creation	false
0xFF-0203-Metasploit_Logins-Win	User Account Authentication	LogonSuccess	T1021.006	Windows Remote Management	Logon Session Creation	false
0xFF-0163-SSH_Password_Bruteforcing-Linux	User Account Authentication	LogonFailed	T1133	External Remote Services	Logon Session Metadata	false
0xFF-0156-ADCS_Abuse_Recently_Issued_Certificate_Exchanged_for_Kerberos_Ticket-Win	User Account Authentication	["4887","4768"]	T1558	Steal or Forge Kerberos Tickets	Logon Session Metadata	false

Indirect / contextual component use

It turns out that next to the expected outcomes there is another possibility;

Components used in a specific correlated detection.

For instance, where we detect possible EDR tampering by correlating machine activity with
the lack of EDR telemetry via several sources, one of which is the logon session / user authentication log.

0xFF-0008-Device_Active_On_Network_No_Defender_Logs-Win	User Account Authentication	["DeviceInfo","4624","4673","5140","463...	T1562	Impair Defenses
0xFF-0008-Device_Active_On_Network_No_Defender_Logs-Win	User Account Authentication	["DeviceInfo","4624","4673","5140","463...	T1562.001	Disable or Modify Tools
0xFF-0221-Kerberos_PAC_confusion_and_impersonation_of_DCs-Win	User Account Authentication	["4741","4742","4781","4769"]	T1574	Hijack Execution Flow
0xFF-0221-Kerberos_PAC_confusion_and_impersonation_of_DCs-Win	User Account Authentication	["4741","4742","4781","4769"]	T1574.001	DLL Search Order Hijacking

Removed components

Some components we tagged were very solution specific and therefore were removed from being considered for ATT&CK contributions to avoid implementation confusion.

One of the examples of this is the File Metadata component, which we use in 74 rules.

In these specific cases the rules utilize the proprietary FileProfile feature within the Microsoft Threat protection portal.

SHA1	FileSize	GlobalPrevalence	GlobalFirstSeen	GlobalLastSeen	SignatureState	IsExecutable
49a0b5bdf000947...	97280	2	May 20, 2022 12:22:44 PM	May 25, 2022 9:39:59 AM	Unknown	0

Since this feature is not available in a lot of other products it did not feel appropriate to submit it to ATT&CK

Going through results, a question

Should ATT&CK contain a listing of data components for the execution of the technique or the (behavioral) effect of the technique as well?

Sometimes this is clear but there are a lot of edge cases, I can imagine the ATT&CK team had a similar internal debate.

Analyzing the mappings in ATT&CK I could not come up with a definitive answer.

Some examples;

Rule name	Rule Component	ID	Technique
Potential privilege escalation by overwriting high privilege executable file	File Creation	T1543.003	Windows Service
SMB Requests by Unexpected Process	Network Connection Creation	T1550.002	Pass the Hash

Inproperly tagged or new perspective

With the cloud attack surface ever growing, a lot of techniques can be interpreted to be applicable to certain techniques.

It's also a matter of perspective as shown on ATT&CKCon 3.0 by the social engineering study.

For example;

Rule name	Rule Component	ID	Technique Name	Technique Components
AzureAD UserAgent OS Mismatch	Logon Session Metadata	T1036	Masquerading	File Modification Service Creation Service Metadata Scheduled Job Metadata File Metadata Command Execution Image Metadata Scheduled Job Modification Process Metadata

Our preliminary results

Based on this we identified 164 data components which can be added to existing techniques. This is based on the components that we use in detection rules for those techniques.

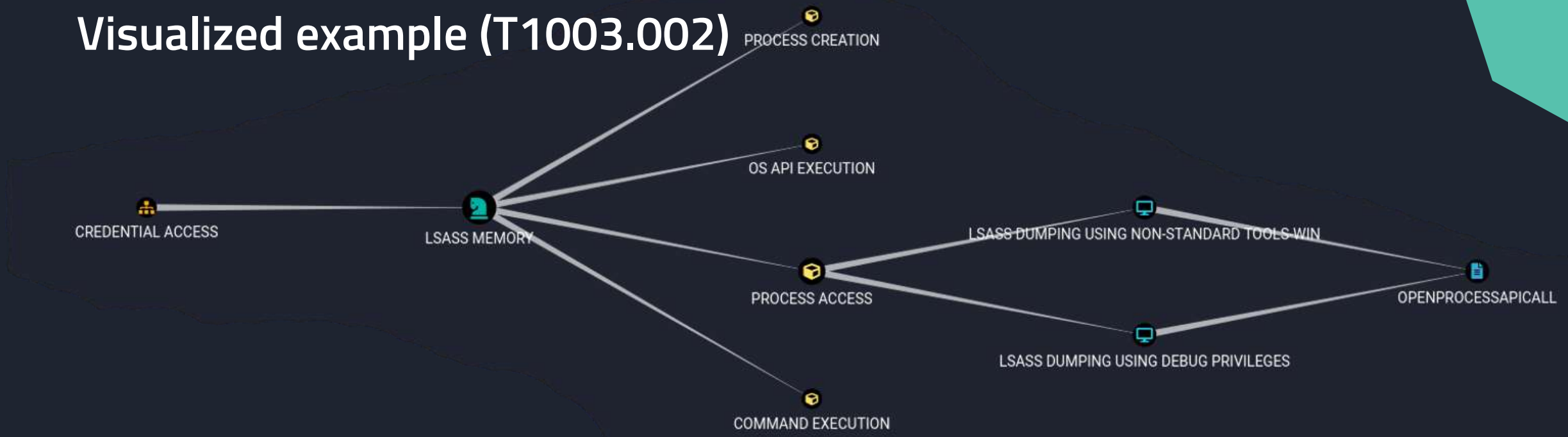
There were even some techniques that did not have *any* data source added to them yet.

These results will need to be shared with the ATT&CK team with some additional context and reasoning to understand our mapping.

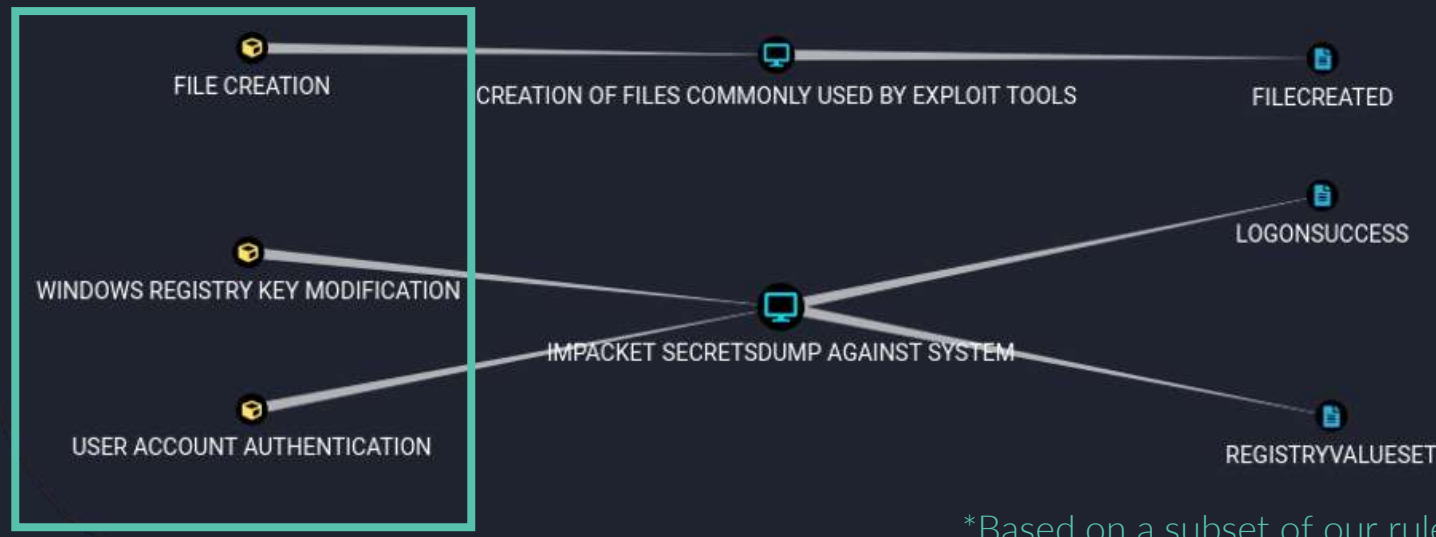
The top 15 added components out of 30 to multiple techniques is;

RuleComponents	count_ID
Application Log Content	25
Network Connection Creation	24
Cloud Service Modification	21
Active Directory Object Access	21
File Creation	17
Logon Session Creation	17
User Account Modification	15
Module Load	15
Process Creation	14
Process Access	13
User Account Authentication	9
Command Execution	8
Process Metadata	6
Network Share Access	6
Network Traffic Content	5

Visualized example (T1003.002)

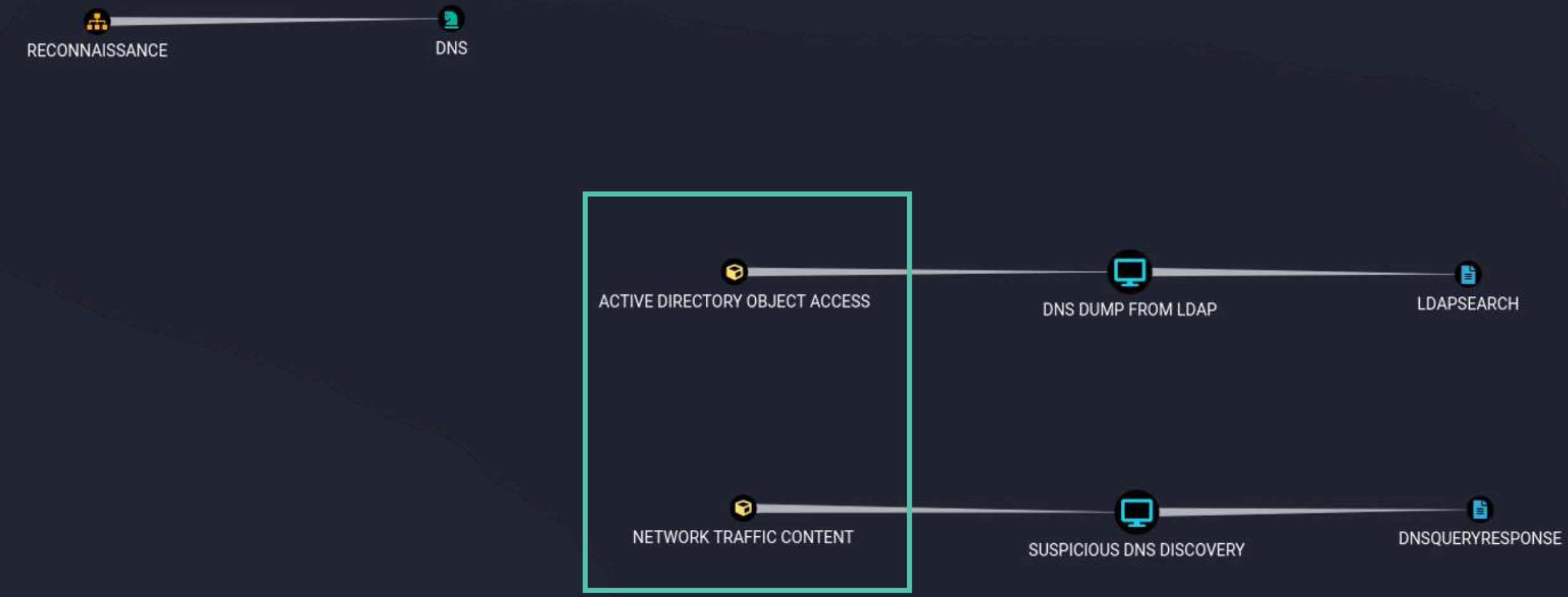


Additional components



*Based on a subset of our rules

Visualized example (T1590.002)



First components

Thought, said, heard, retained.

What we have learnt

- Applying this well, takes time and is not always as simple as expected
- Detections can apply to several techniques, this adds some mapping noise.
- Technique mapping can be done incorrectly, but it is also a matter of perspective
- Cause and effect can influence detection mappings
- We have something to submit to ATT&CK

Thank you! Questions ?

olaf@falconforce.nl

https://falconforce.nl

@olafhartong
@falconforceteam

https://linkedin.com/in/olafhartong