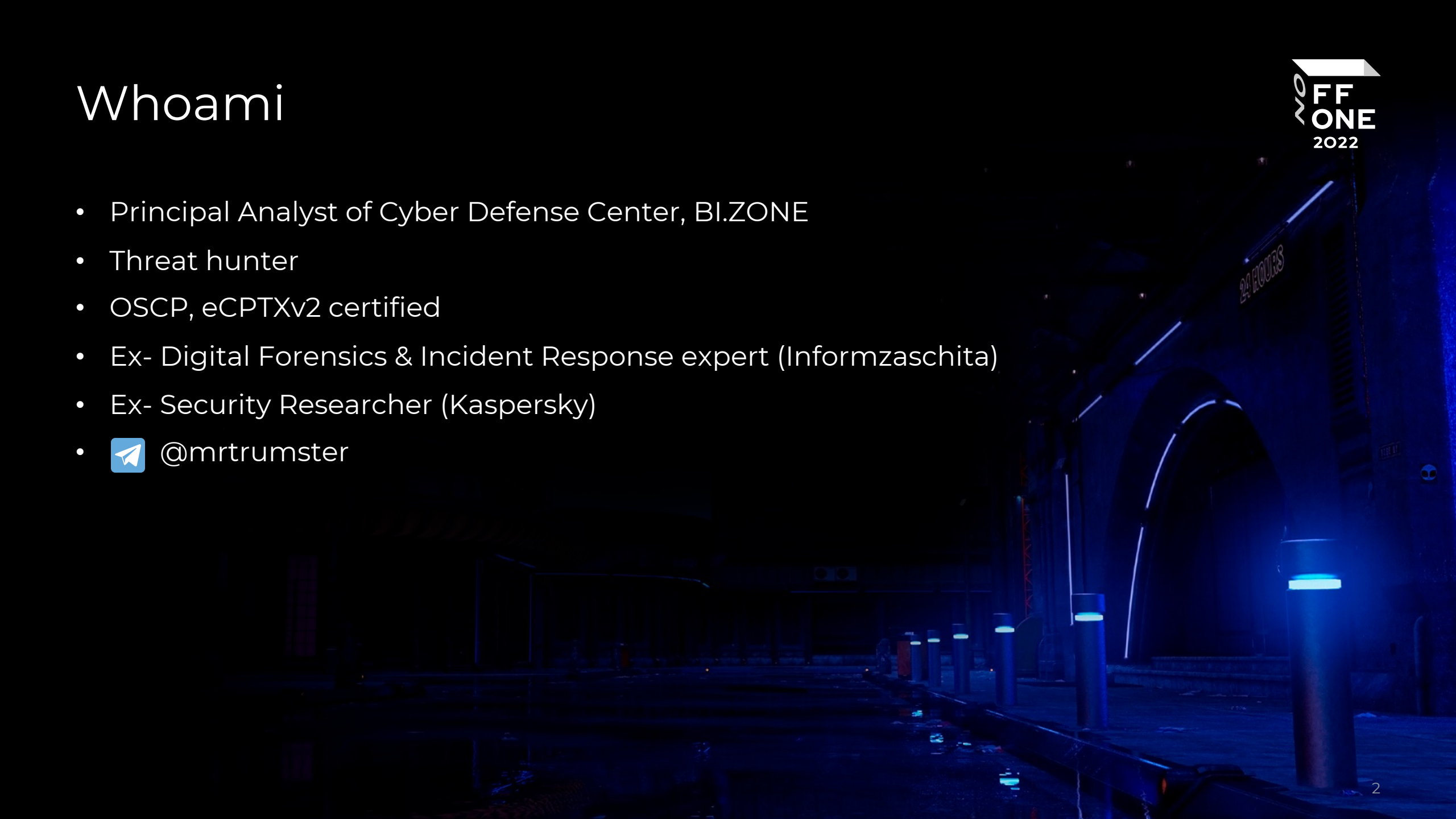
Chasing evil: Modern approaches to anomaly detection in windows infrastructures with LDAP and RPC monitoring

Maxim Tumakov

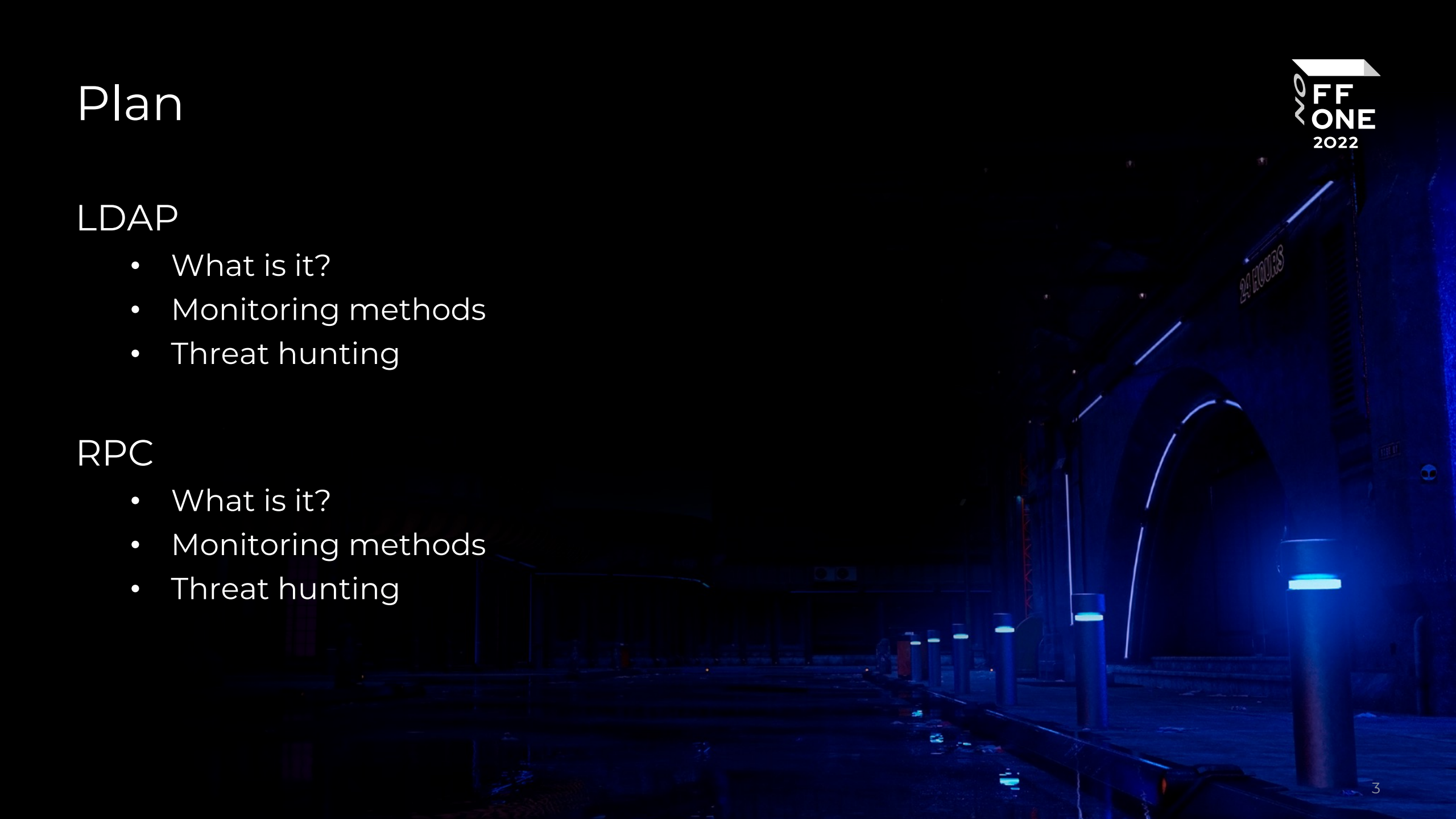
Principal Analyst of Cyber Defense Center, BI.ZONE

Whoami

- Principal Analyst of Cyber Defense Center, BI.ZONE
- Threat hunter
- OSCP, eCPTXv2 certified
- Ex- Digital Forensics & Incident Response expert (Informzaschita)
- Ex- Security Researcher (Kaspersky)
- @mrtrumster



Plan



LDAP

- What is it?
- Monitoring methods
- Threat hunting

RPC

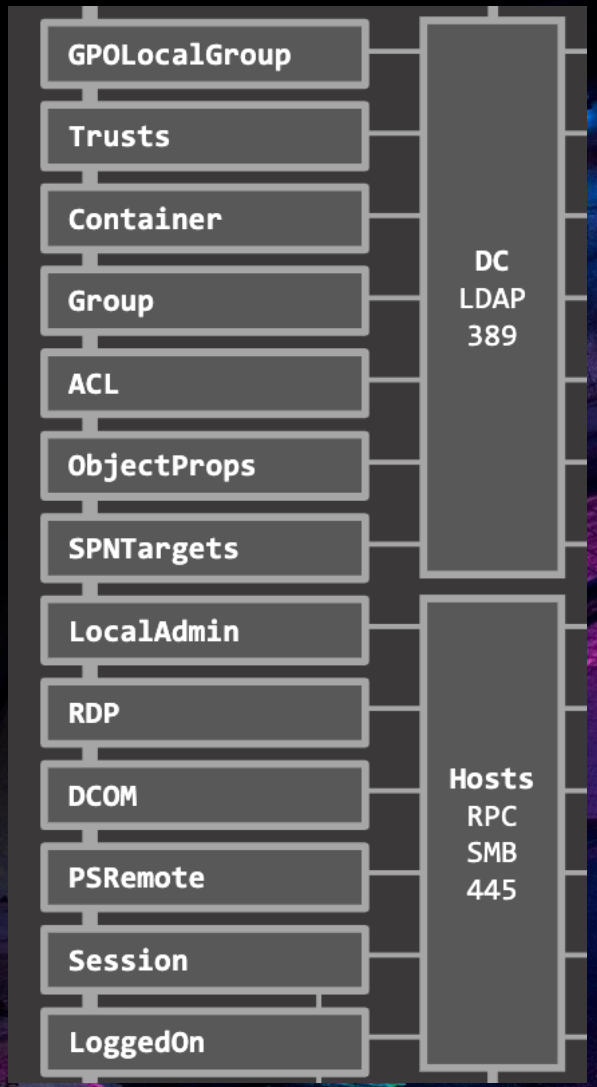
- What is it?
- Monitoring methods
- Threat hunting

Motivation

Detection of suspicious discovery activity in Windows infrastructure before start of active phase of the attack

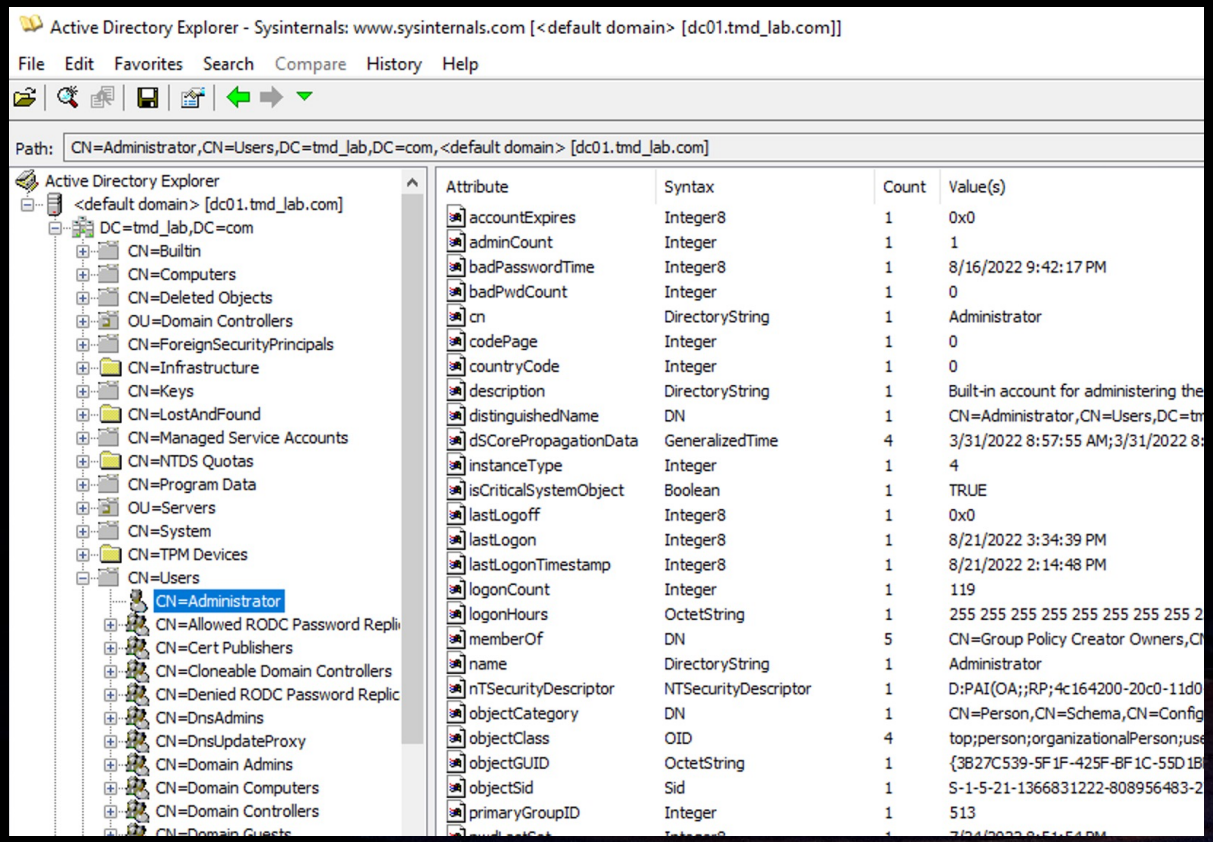
HackTools

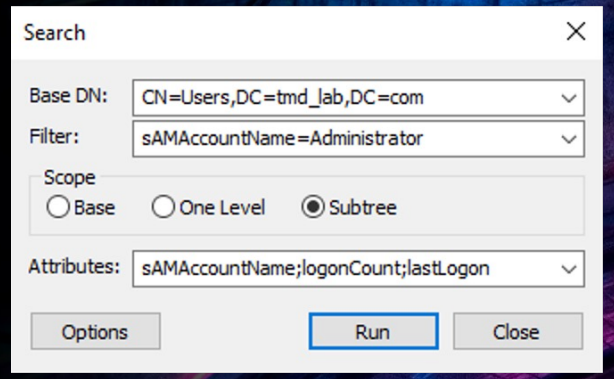
- BloodHound ingestors
- AdFind
- PowerView
- Coercer, SpoolSample, etc
- …

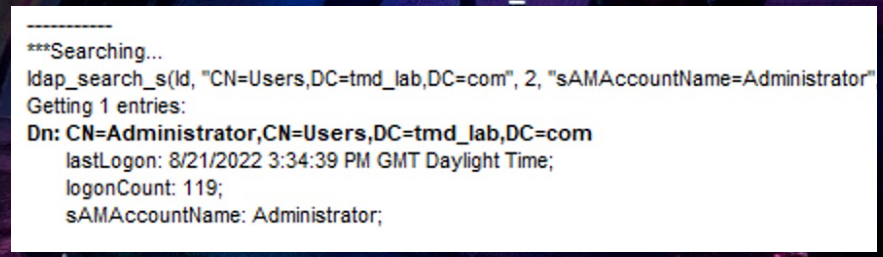


LDAP. What is it?

The Lightweight Directory Access Protocol (LDAP) is a protocol for searching information in the Active Directory database, but not only...



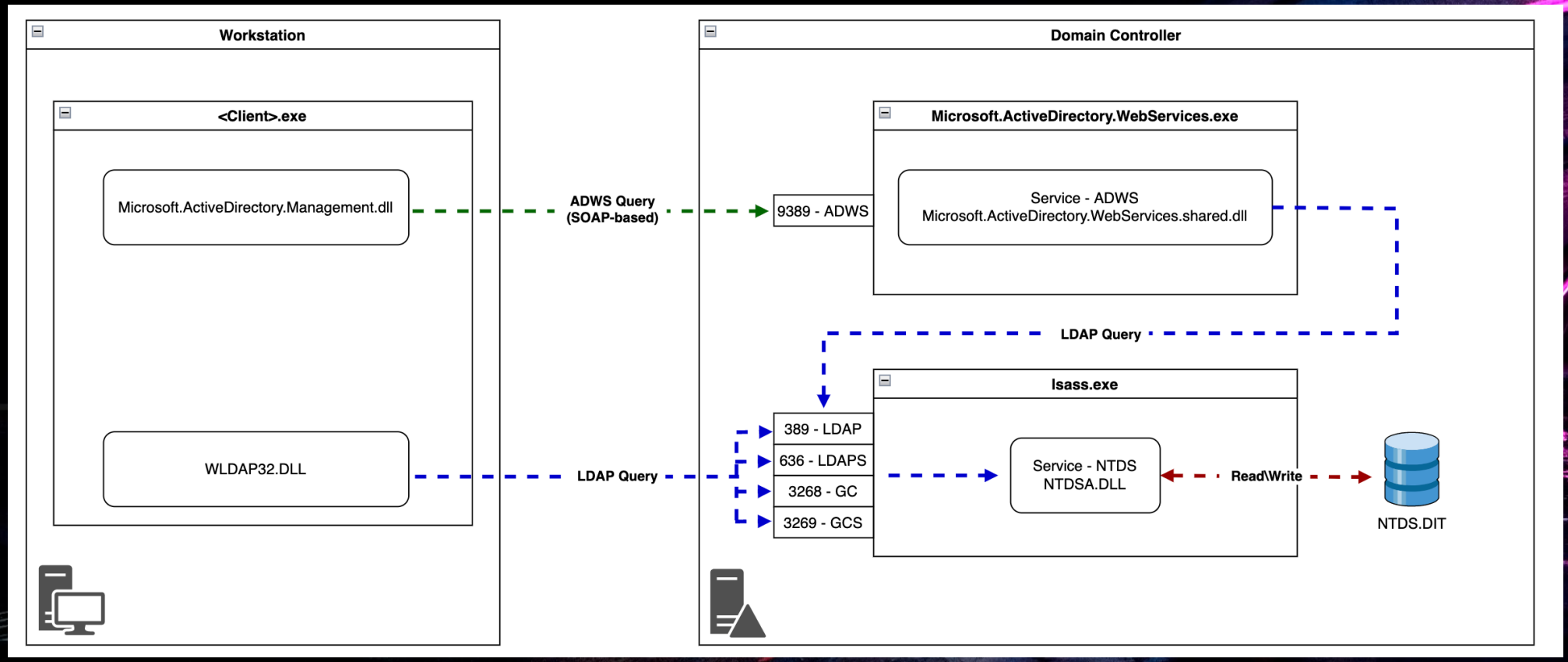




LDAP. What is it?

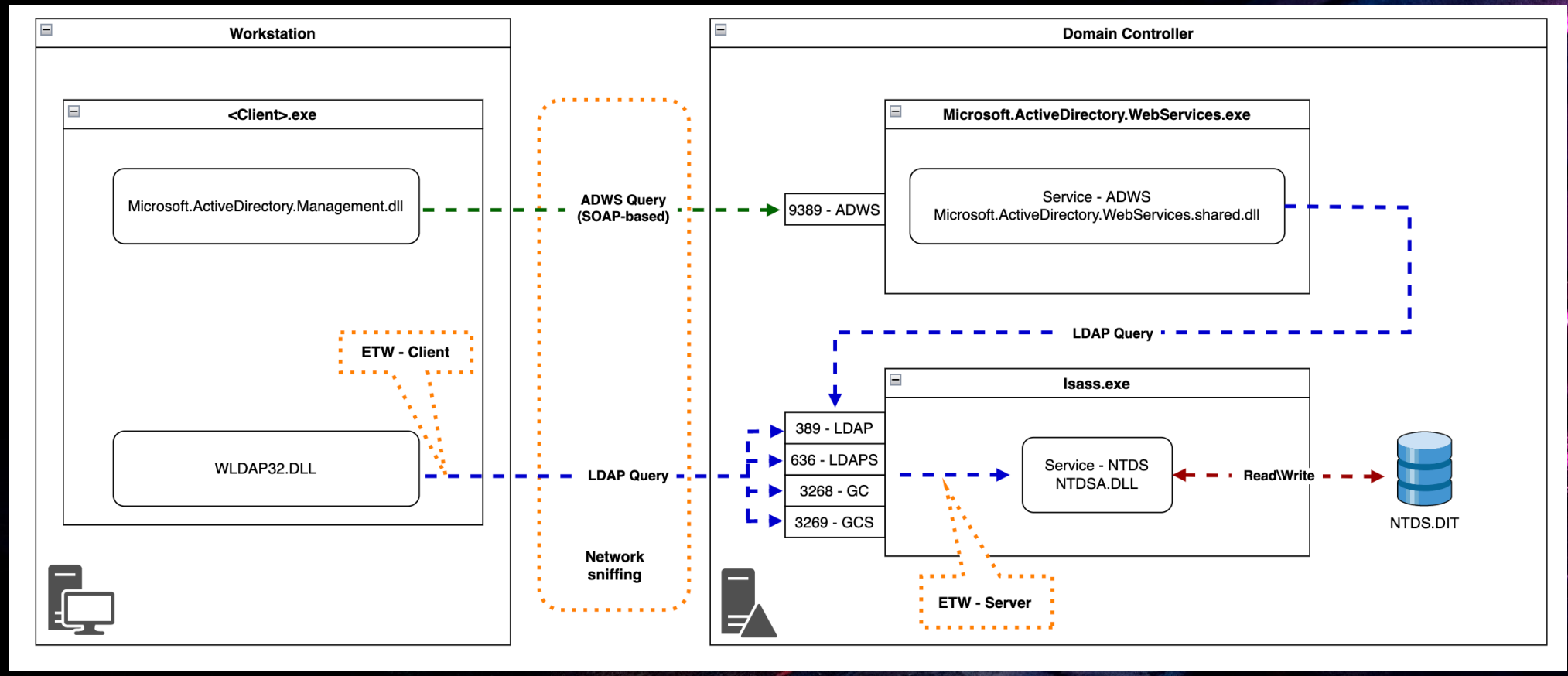
Protocols

- LDAP - 389
- LDAPS (Secure) - 636
- ADWS (AD Web Services) - 9389
- GC (Global Catalog) - 3268
- GCS (Global Catalog Secure) - 3269



LDAP. Monitoring methods

- Client ETW provider
- Network sniffing
- Server ETW provider

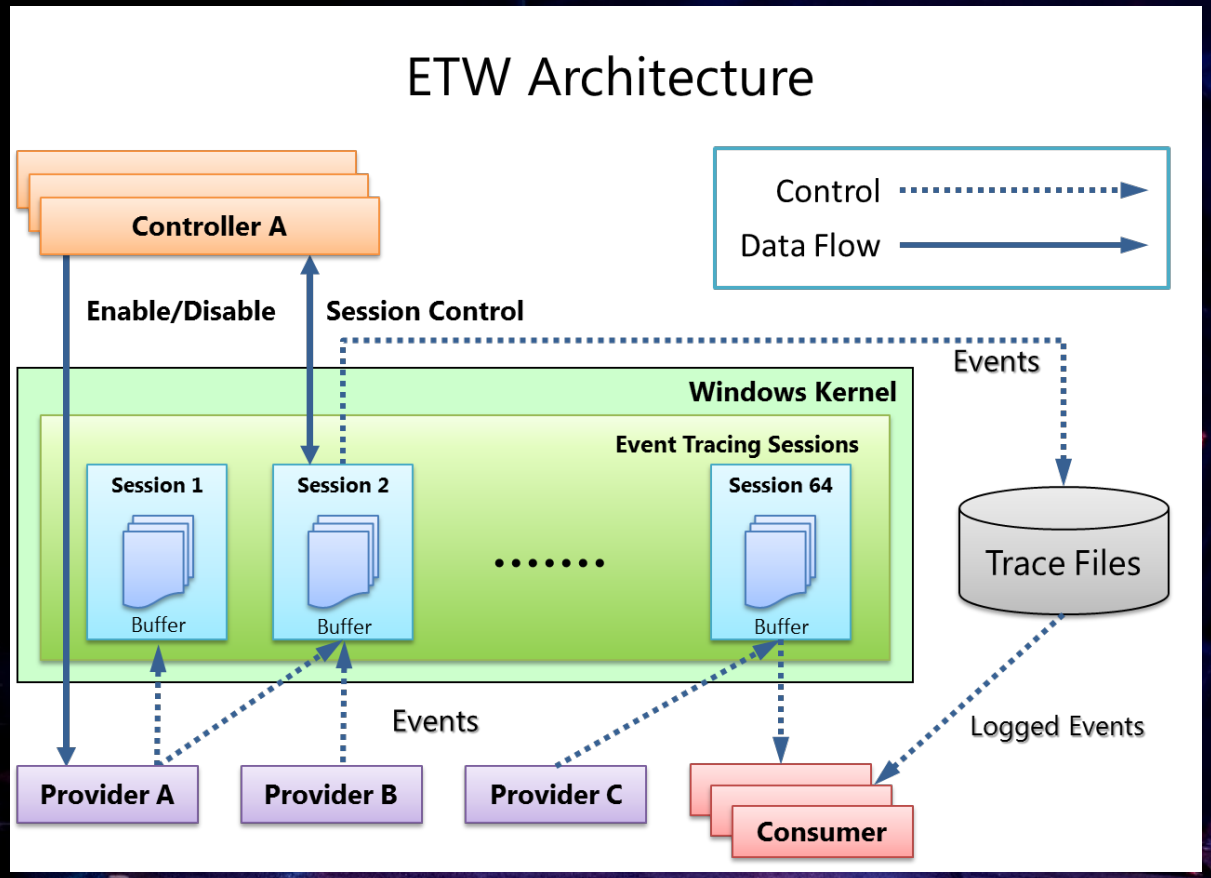


ETW. What is it?

A ***ETW provider*** is an instrumented component that generates events.

The ***ETW session*** infrastructure works as an intermediate broker that relays the events from one or more providers to the consumer.

A ***ETW consumer*** is an app that reads a logged trace file (ETL file) or captures events in an active trace session in real time, and processes events.



https://docs.microsoft.com/en-us/windows-hardware/test/weg/instrumenting-your-code-with-etw

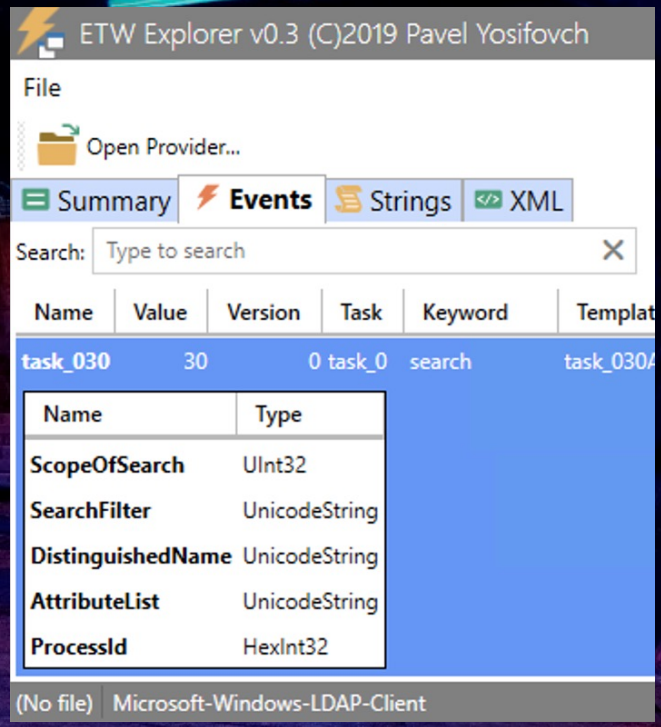
LDAP. Client ETW provider

ETW Name: Microsoft-Windows-LDAP-Client

ETW GUID: {099614A5-5DD7-4788-8BC9-E29F43DB28FC}

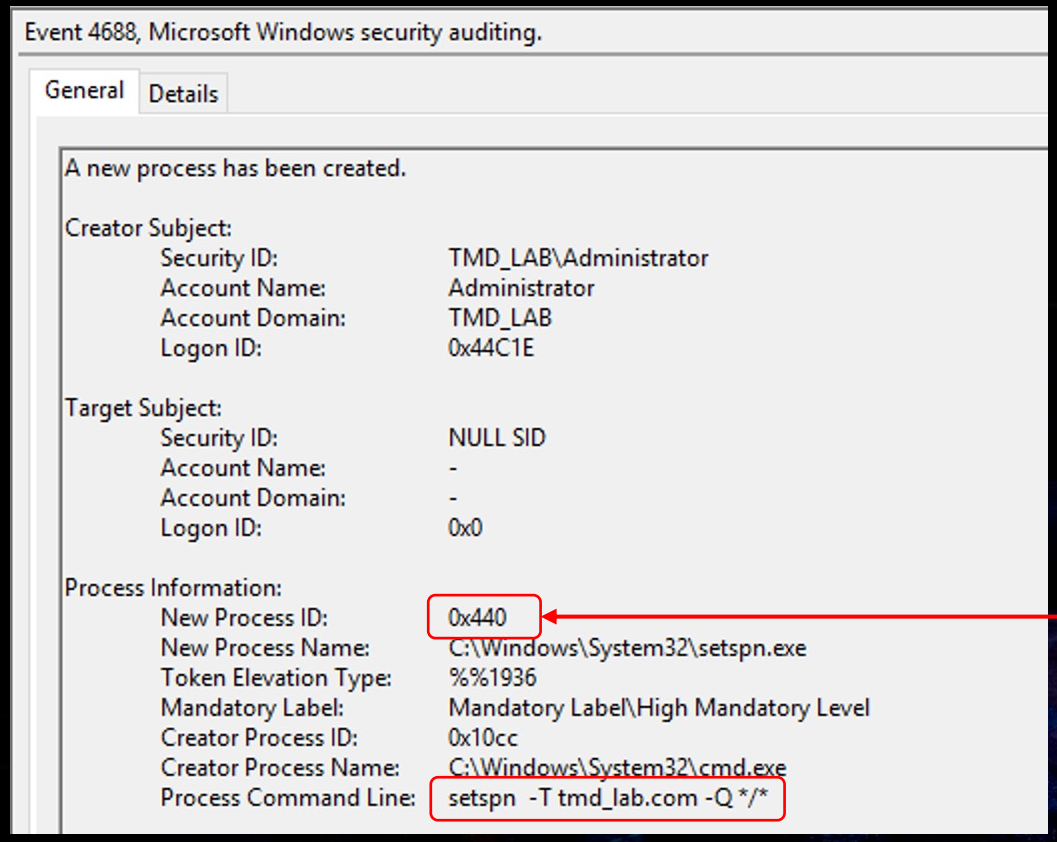
Event ID: 30

Field Name	Type	Example value
ScopeOfSearch	UInt32	2
SearchFilter	UnicodeString	(objectclass=domain)
DistinguishedName	UnicodeString	DC=tmd_lab,DC=com
AttributeList	UnicodeString	objectsid;objectguid
ProcessId	HexInt32	0x1EDC



LDAP. Client ETW provider

Time	ldap_scope	ldap_filter	ldap_dn	ldap_attrib_list	proc_id
Jul 24, 2022 @ 14:42:12.875	wholeSubtree	servicePrincipalName=*/*	DC=tmd_lab,DC=com	servicePrincipalName	1,088



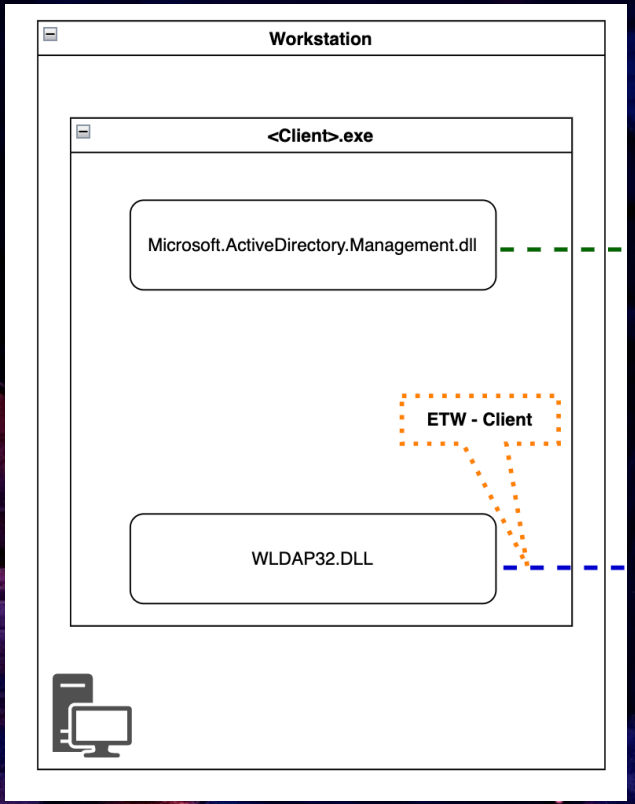
LDAP. Client ETW provider

Advantages:

- There is a PID of the initiating process in the event. It is possible to determine the path to the executable, account, etc.

Disadvantages:

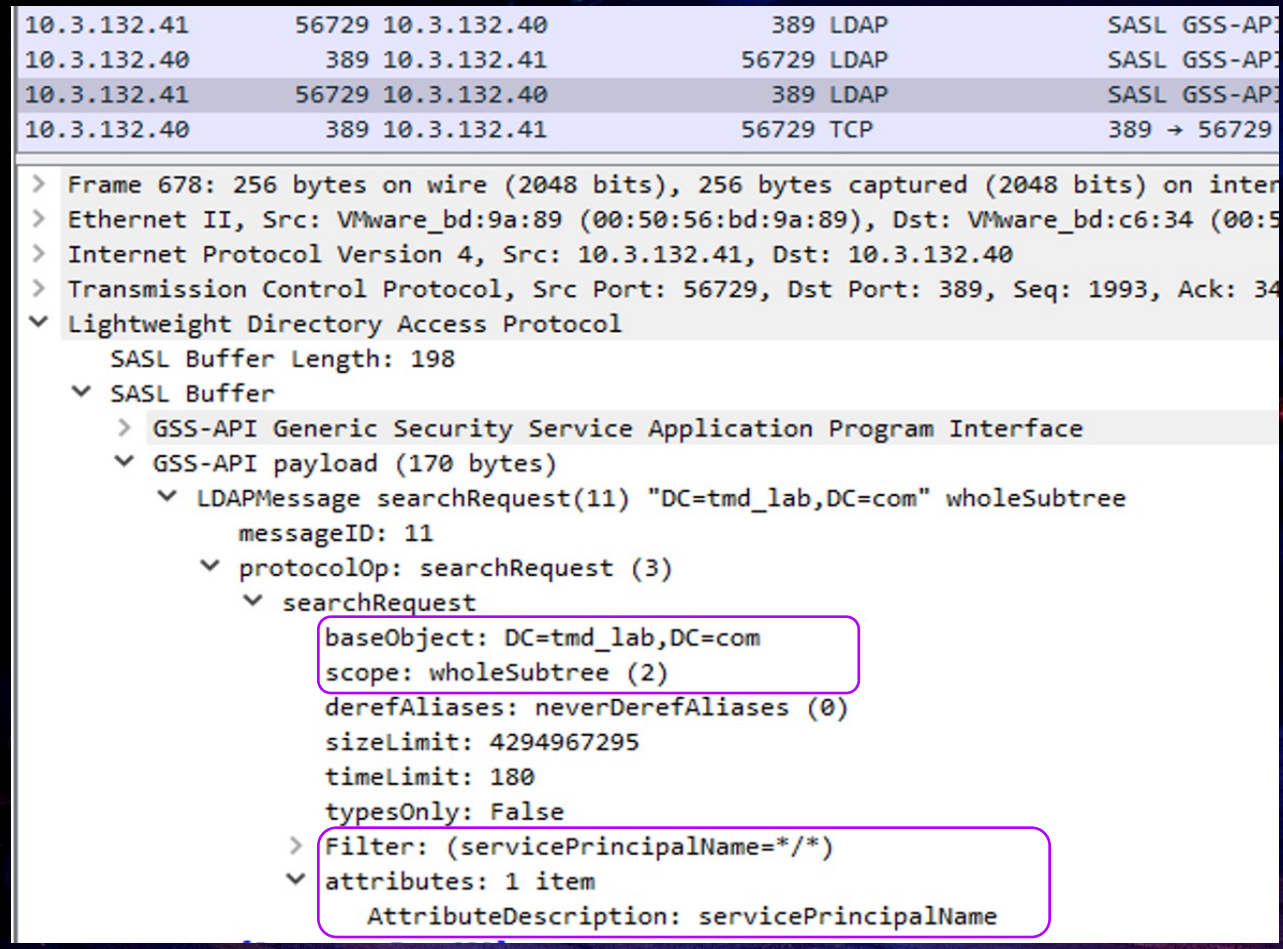
- Need to collect ETW events from all hosts in the domain
- LDAP requests from non-domain computers are not monitored. The attacker can use his "evil" computer
- No ability to inspect ADWS requests
- Possible bypass when using a fully customized LDAP client



LDAP. Network sniffing

Tools

- Zeek
- Suricata, etc.



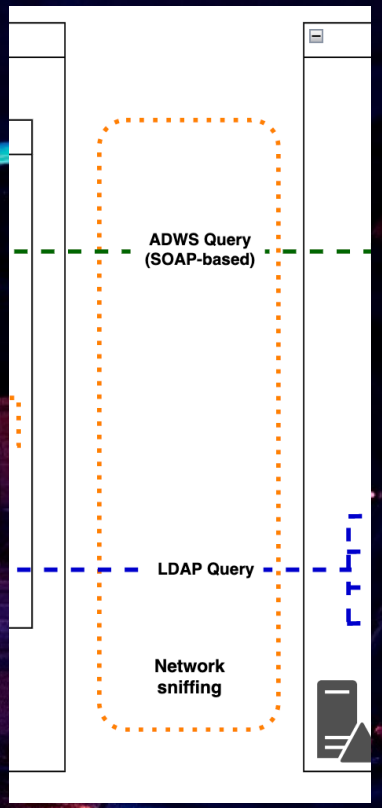
LDAP. Network sniffing

Advantages:

- It is possible to use a small number of network sensors

Disadvantages:

- It is impossible to inspect the encrypted content of secure protocols without importing a certificate (LDAPS, GCS) or developing a custom handler (ADWS)
- May require the deployment of additional equipment for traffic mirroring (SPAN\network TAP)
- The event does not contain the initiator process



LDAP. Server. Method 1

Event Log: Directory Service.evtx

Event ID: 1644

Preparatory steps:

- Allow diagnostic logging
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics
  - 15 Field Engineering == 0x05
- Allow logging "expensive" LDAP queries
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
  - Expensive Search Results Threshold == 0x00

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961809(v=technet.10)?redirectedfrom=MSDN

LDAP. Server. Method 1

Event Log: Directory Service.evtx

Event ID: 1644

Field name	Example value
Client	10.3.132.41 : 50540
Starting node	DC=tmd_lab,DC=com
Filter	servicePrincipalName=*/*
Search scope	subtree
Attribute selection	servicePrincipalName
Visited entries	3710
Returned entries	4
User	TMD_LAB\Administrator

LDAP. Server. Method 2

ETW Name: Active Directory Domain Services: Core

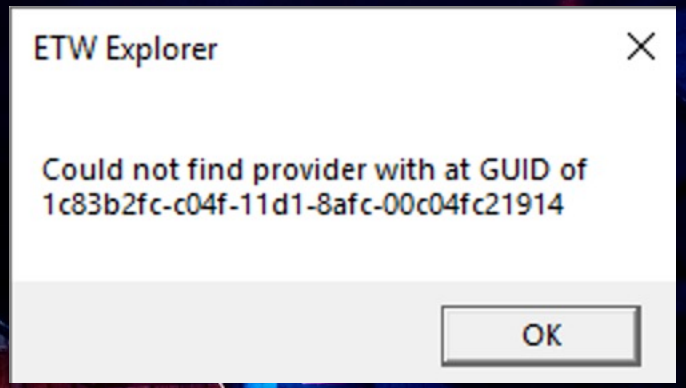
ETW GUID: {1C83B2FC-C04F-11D1-8AFC-00C04FC21914}

Event ID: 0

Event Name: DsDirSearch

Event Type: Start

Field name	Type	Example value
Caller	UnicodeString	10.3.132.41 : 50540
Choice	UnicodeString	subtree
ObjDN	UnicodeString	DC=tmd_lab,DC=com
Filter	UnicodeString	servicePrincipalName=*/*
RequiredAttributes	UnicodeString	servicePrincipalName



C:\Windows\System32\wbem\ntdsa.mof

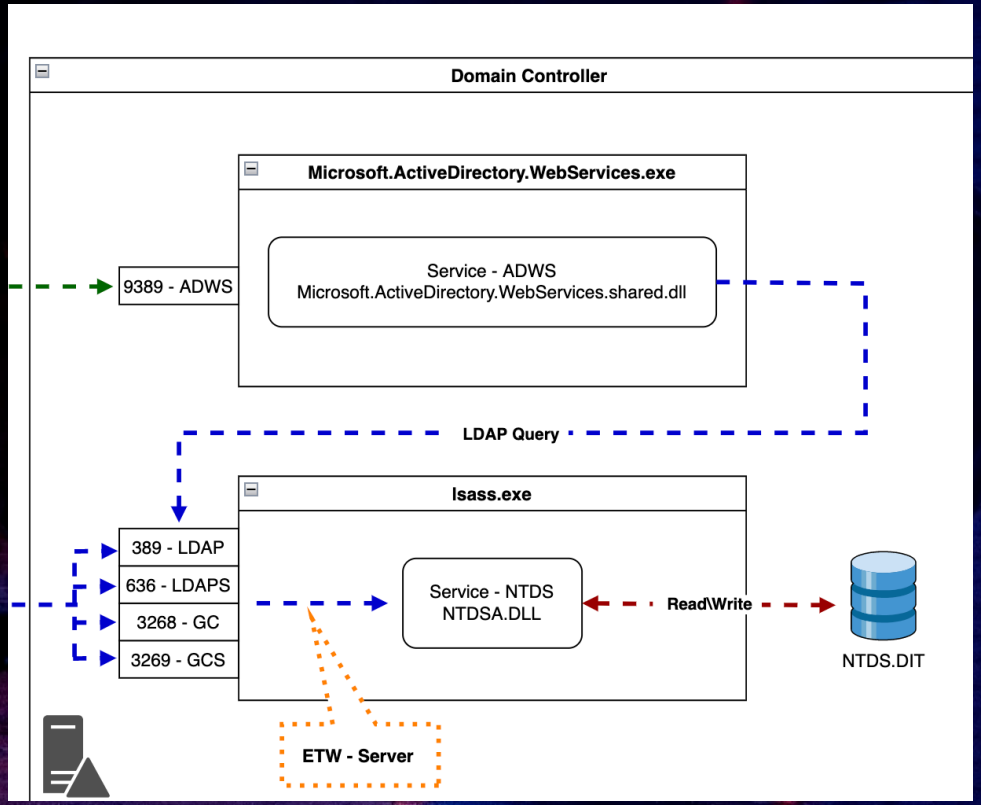
LDAP. Server

Advantages:

- LDAP requests from all endpoints (including non-domain computers and "evil" devices) are logged at a single point
- All requests are captured in decrypted form regardless of the protocol used
- The source address of the request and the initiating account are captured

Disadvantages:

- Huge flow of events
- Additional correlation is required to determine the origin of an ADWS request (with events 4624, 4769, NetworkConnection etc)



LDAP. Threat hunting. BloodHound

Attribute list

objectSid,objectGUID,isDeleted,userAccountControl,sAMAccountType,objectClass,sAMAccountName,msDS-GroupMSAMembership,distinguishedName,pwdLastSet,lastLogon,lastLogonTimestamp,sIDHistory,dNSHostName,operatingSystem,operatingSystemServicePack,servicePrincipalName,displayName,mail,title,homeDirectory,description,adminCount,userPassword,gPCFileSysPath,msDS-Behavior-Version,name,gPOptions,msDS-AllowedToDelegateTo,msDS-AllowedToActOnBehalfOfOtherIdentity,whenCreated,gPLink,member,cn,primaryGroupID,nTSecurityDescriptor,trustAttributes,securityIdentifier,trustDirection,trustType

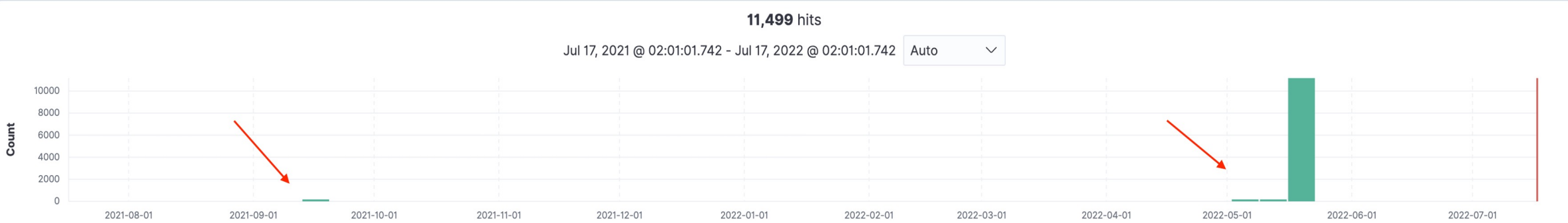
Filter

```
( |
   ( sAMAccountType = 805306369 )
   ( objectClass = container )
   ( sAMAccountType = 805306368 )
   ( |
      ( sAMAccountType = 268435456 )
      ( sAMAccountType = 268435457 )
      ( sAMAccountType = 536870912 )
      ( sAMAccountType = 536870913 )
   )
   ( objectClass = domain )
   ( objectCategory = organizationalUnit )
   ( &
      ( objectCategory = groupPolicyContainer )
      ( flags = * )
   )
   ( primaryGroupID = * )
)
```

LDAP. Threat hunting. BloodHound

```
event_type:LDAPQuery AND
ldap_attrib_list:(
    "trustAttributes;securityIdentifier;trustDirection;trustType;cn" OR
    "objectSid;objectGUID;isDeleted;userAccountControl;sAMAccountType;objectClass;sAMAccountName;msDS-GroupMSAMembership;trustAttributes;securityIdentifier;trustDirection;trustType;cn" OR
    "objectSid;objectGUID;isDeleted;userAccountControl;sAMAccountType;objectClass;sAMAccountName;msDS-GroupMSAMembership;servicePrincipalName" OR
    "objectSid;objectGUID;isDeleted;userAccountControl;sAMAccountType;objectClass;sAMAccountName;msDS-GroupMSAMembership;displayName;name;gPLink;gPOptions" OR
    "objectSid;objectGUID;isDeleted;userAccountControl;sAMAccountType;objectClass;sAMAccountName;msDS-GroupMSAMembership;distinguishedName;member;cn;primaryGroupID;dNSHostName" OR
    "sAMAccountType;objectSid;objectGUID;objectClass;sAMAccountName;msDS-GroupMSAMembership" OR
    "objectSid;objectGUID;isDeleted;userAccountControl;sAMAccountType;objectClass;sAMAccountName;msDS-GroupMSAMembership;gPLink;name"
)
```

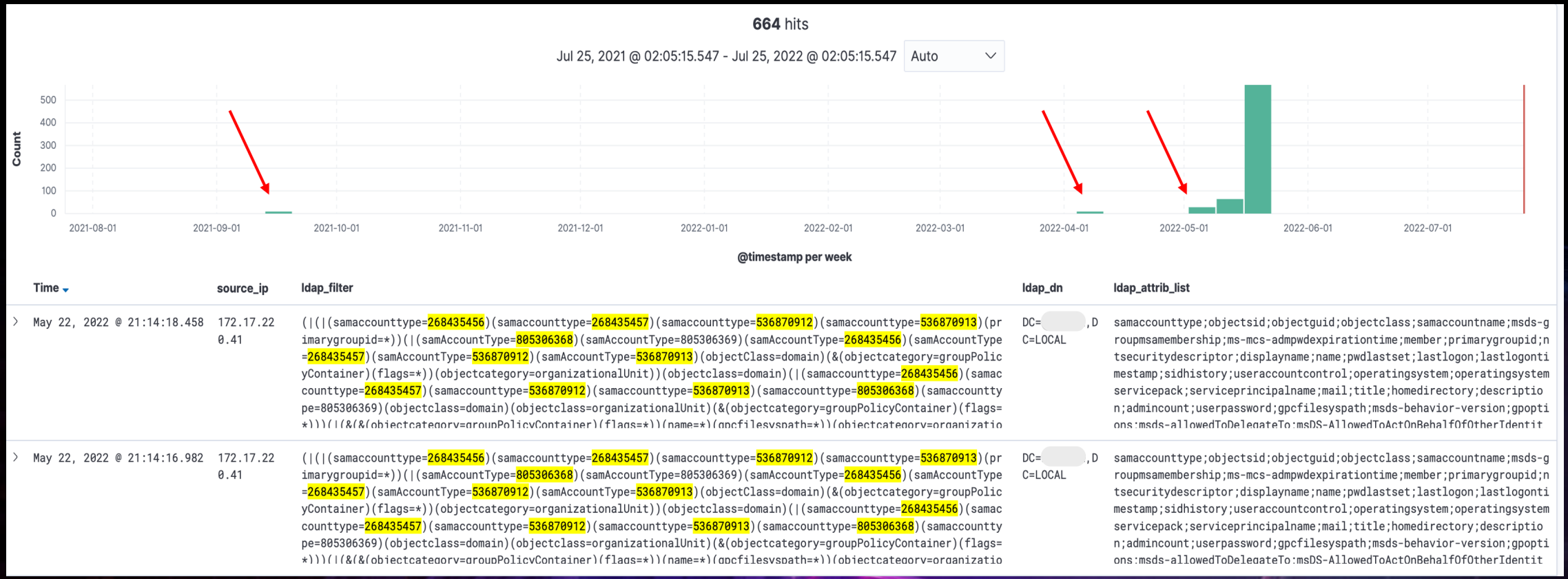
LDAP. Threat hunting. BloodHound



Time	source_ip	ldap_filter	ldap_dn	ldap_attrib_list
May 22, 2022 @ 21:15:53.493	172.17.220.41	(objectclass=trusteddomain)	DC=[redacted],DC=LOCAL	trustattributes;securityidentifier;trustdirection;trusttype;cn
May 22, 2022 @ 21:15:53.492	172.17.220.41	(|(samAccountType=805306368)(samAccountType=805306369))	CN=Users,DC[redacted]DC=local	samaccounttype;objectsid;objectguid;objectclass;samaccountname;msds-groupmsamembership
May 22, 2022 @ 21:15:53.491	172.17.220.41	(|(samAccountType=805306368)(samAccountType=805306369))	CN=System,DC[redacted]DC=local	samaccounttype;objectsid;objectguid;objectclass;samaccountname;msds-groupmsamembership
May 22, 2022 @ 21:15:53.491	172.17.220.41	(|(samAccountType=805306368)(samAccountType=805306369))	CN=Program Data,DC[redacted]DC=local	samaccounttype;objectsid;objectguid;objectclass;samaccountname;msds-groupmsamembership
May 22, 2022 @ 21:14:22.336	172.17.220.41	(|(samAccountType=805306368)(samAccountType=805306369))	CN=ForeignSecurityPrincipals,DC[redacted]DC=local	samaccounttype;objectsid;objectguid;objectclass;samaccountname;msds-groupmsamembership
May 22, 2022 @ 21:14:22.336	172.17.220.41	(|(samAccountType=805306368)(samAccountType=805306369))	CN=Computers,DC[redacted]DC=local	samaccounttype;objectsid;objectguid;objectclass;samaccountname;msds-groupmsamembership

LDAP. Threat hunting. BloodHound

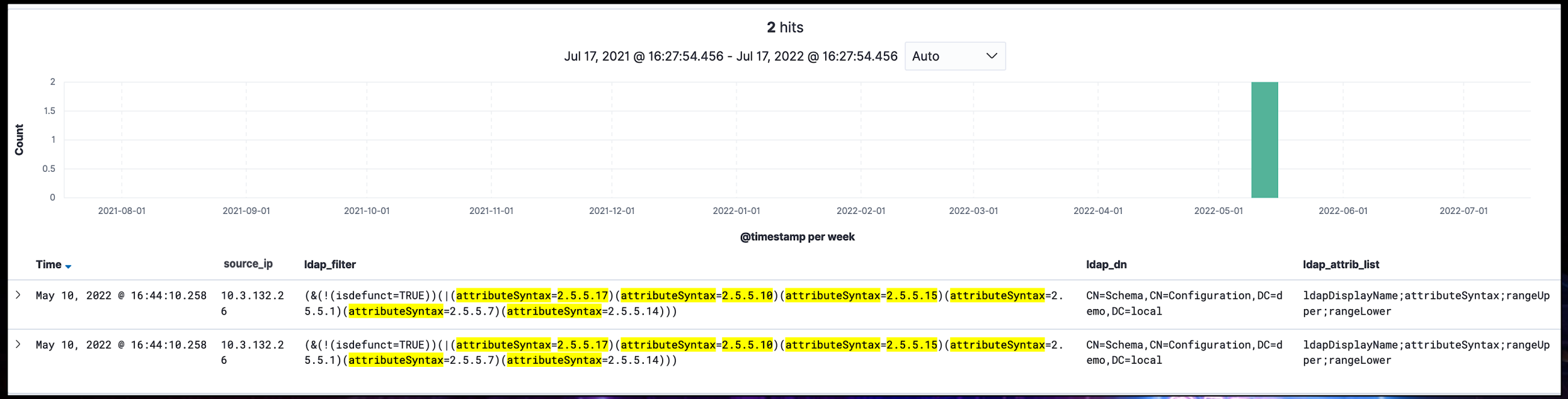
```
event_type:LDAPQuery AND
ldap_filter:(
    ( 268435456 AND 268435457 AND 536870912 AND 536870913 ) OR
    ( 805306368 AND "servicePrincipalName=*" )
)
```



Time	source_ip	ldap_filter	ldap_dn	ldap_attrib_list
May 22, 2022 @ 21:14:18.458	172.17.220.41	(|(|(samaccounttype=268435456)(samaccounttype=268435457)(samaccounttype=536870912)(samaccounttype=536870913)(primarygroupid=*))(|(samAccountType=805306368)(samAccountType=805306369)(samAccountType=268435456)(samAccountType=268435457)(samAccountType=536870912)(samAccountType=536870913)(objectClass=domain)(&(objectcategory=groupPolicyContainer)(flags=*))(objectcategory=organizationalUnit))(objectclass=domain)(|(samaccounttype=268435456)(samaccounttype=268435457)(samaccounttype=536870912)(samaccounttype=536870913)(samaccounttype=805306368)(samaccounttype=805306369)(objectclass=domain)(objectclass=organizationalUnit)(&(objectcategory=groupPolicyContainer)(flags=*))(|(&(&(objectcategory=groupPolicyContainer)(flags=*))(name=*)(gpcfilesyspath=*))(objectcategory=organizatio	DC=[redacted],DC=LOCAL	samaccounttype;objectsid;objectguid;objectclass;samaccountname;msds-groupmsamembership;ms-mcs-admpwdexpirationtime;member;primarygroupid;ntsecuritydescriptor;displayname;name;pwdlastset;lastlogon;lastlogontimestamp;sidhistory;useraccountcontrol;operatingsystem;operatingsystemservicepack;serviceprincipalname;mail;title;homedirectory;description;admincount;userpassword;gpcfilesyspath;msds-behavior-version;gpoptions;msds-allowedToDelegateTo;msDS-AllowedToActOnBehalfOfOtherIdentit
May 22, 2022 @ 21:14:16.982	172.17.220.41	(|(|(samaccounttype=268435456)(samaccounttype=268435457)(samaccounttype=536870912)(samaccounttype=536870913)(primarygroupid=*))(|(samAccountType=805306368)(samAccountType=805306369)(samAccountType=268435456)(samAccountType=268435457)(samAccountType=536870912)(samAccountType=536870913)(objectClass=domain)(&(objectcategory=groupPolicyContainer)(flags=*))(objectcategory=organizationalUnit))(objectclass=domain)(|(samaccounttype=268435456)(samaccounttype=268435457)(samaccounttype=536870912)(samaccounttype=536870913)(samaccounttype=805306368)(samaccounttype=805306369)(objectclass=domain)(objectclass=organizationalUnit)(&(objectcategory=groupPolicyContainer)(flags=*))(|(&(&(objectcategory=groupPolicyContainer)(flags=*))(name=*)(gpcfilesyspath=*))(objectcategory=organizatio	DC=[redacted],DC=LOCAL	samaccounttype;objectsid;objectguid;objectclass;samaccountname;msds-groupmsamembership;ms-mcs-admpwdexpirationtime;member;primarygroupid;ntsecuritydescriptor;displayname;name;pwdlastset;lastlogon;lastlogontimestamp;sidhistory;useraccountcontrol;operatingsystem;operatingsystemservicepack;serviceprincipalname;mail;title;homedirectory;description;admincount;userpassword;gpcfilesyspath;msds-behavior-version;gpoptions;msds-allowedToDelegateTo;msDS-AllowedToActOnBehalfOfOtherIdentit

LDAP. Threat hunting. AdFind

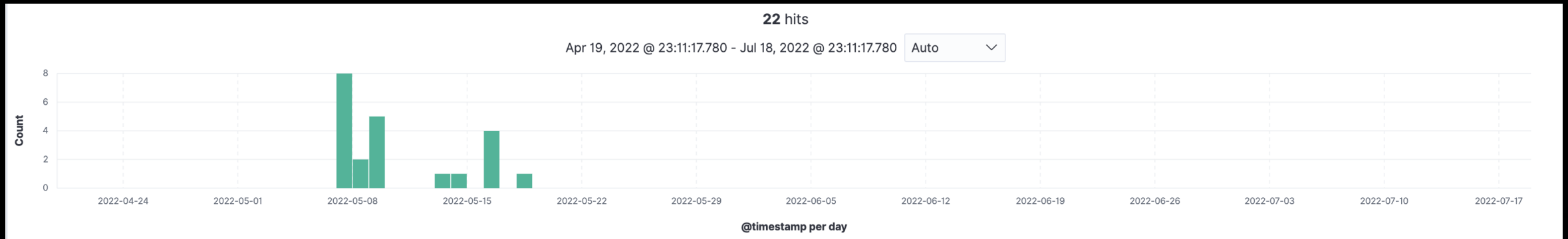
event_type:LDAPQuery AND
ldap_filter:("attributeSyntax" AND "2.5.5.17" AND "2.5.5.10" AND "2.5.5.15")



Time	source_ip	ldap_filter	ldap_dn	ldap_attrib_list
May 10, 2022 @ 16:44:10.258	10.3.132.26	(&(!(isdefunct=TRUE))(|(attributeSyntax=2.5.5.17)(attributeSyntax=2.5.5.10)(attributeSyntax=2.5.5.15)(attributeSyntax=2.5.5.1)(attributeSyntax=2.5.5.7)(attributeSyntax=2.5.5.14)))	CN=Schema,CN=Configuration,DC=demo,DC=local	ldapDisplayName;attributeSyntax;rangeUpper;rangeLower
May 10, 2022 @ 16:44:10.258	10.3.132.26	(&(!(isdefunct=TRUE))(|(attributeSyntax=2.5.5.17)(attributeSyntax=2.5.5.10)(attributeSyntax=2.5.5.15)(attributeSyntax=2.5.5.1)(attributeSyntax=2.5.5.7)(attributeSyntax=2.5.5.14)))	CN=Schema,CN=Configuration,DC=demo,DC=local	ldapDisplayName;attributeSyntax;rangeUpper;rangeLower

LDAP. Threat hunting. Certify

event_type:LDAPQuery AND
ldap_filter: "objectCategory=pKICertificateTemplate" AND
ldap_attrib_list.keyword://

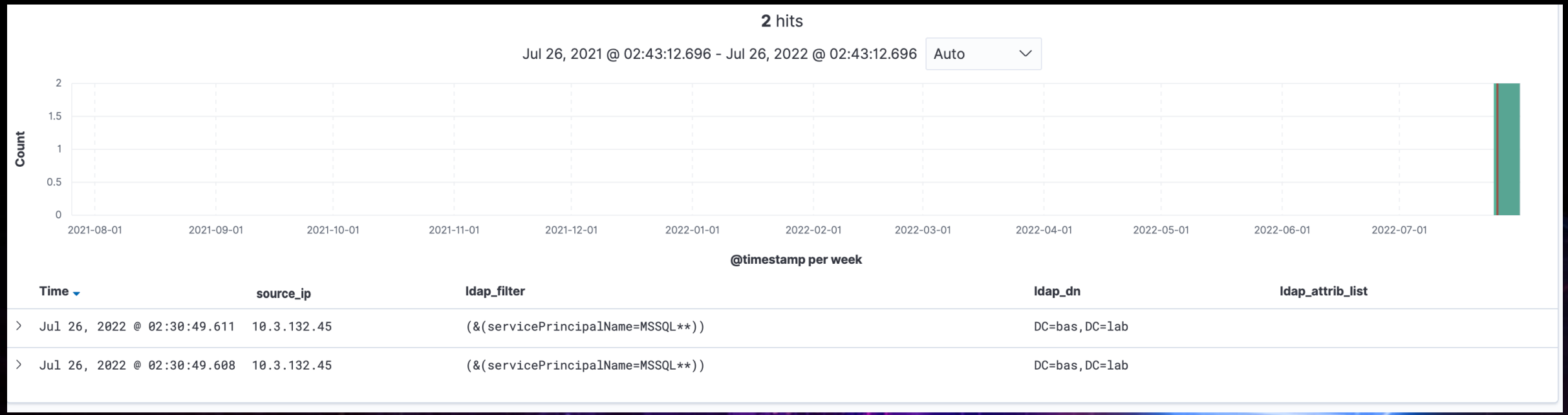


Time	dev_ipv4	proc_cmdline	ldap_filter	ldap_attrib_list
May 18, 2022 @ 21:06:07.142	10.3.132.26	.\Certify.exe find	(objectclass=pKICertificateTemplate)	
May 16, 2022 @ 19:02:02.979	10.5.1.15	"C:\Users\ \Documents\Проекты ИБ\PKI\ \Certify.exe" find /vulnerable	(objectclass=pKICertificateTemplate)	
May 16, 2022 @ 18:57:54.637	10.5.1.15	"C:\Users\ \Documents\Проекты ИБ\PKI\ \Certify.exe" find /vulnerable	(objectclass=pKICertificateTemplate)	
May 16, 2022 @ 18:56:26.929	10.5.1.15	"C:\Users\ \Documents\Проекты ИБ\PKI\ \Certify.exe" find	(objectclass=pKICertificateTemplate)	
May 16, 2022 @ 11:16:24.537	10.5.1.15	Certify.exe find / vulnerable	(objectclass=pKICertificateTemplate)	
May 14, 2022 @ 15:57:41.258	10.3.132.26	"C:\Users\dadmin\Desktop\Certify.exe" find	(objectclass=pKICertificateTemplate)	
May 13, 2022 @ 21:49:46.432	10.3.132.26	Certify.exe find /vulnerable	(objectclass=pKICertificateTemplate)	
May 9, 2022 @ 16:29:48.606	10.3.132.26	Certify.exe find /vulnerable	(objectclass=pKICertificateTemplate)	
May 9, 2022 @ 16:05:38.364	10.3.132.26	Certify.exe find /clientauth	(objectclass=pKICertificateTemplate)	
May 9, 2022 @ 16:04:36.514	10.3.132.26	Certify.exe find /vulnerable	(objectclass=pKICertificateTemplate)	

LDAP. Threat hunting. PowerUpSQL

PowerUpSQL cmdlet: Get-SQLInstanceDomain

event_type:LDAPQuery AND
ldap_filter.keyword:/.*servicePrincipalName=MSSQL**.*/ AND
ldap_attrib_list.keyword://

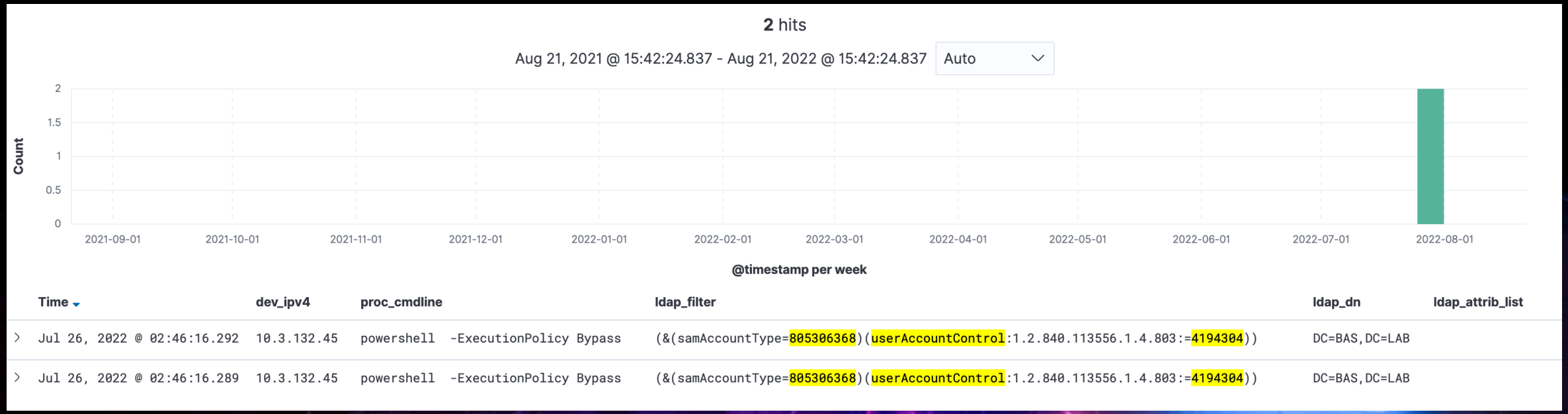


Time	source_ip	ldap_filter	ldap_dn	ldap_attrib_list
Jul 26, 2022 @ 02:30:49.611	10.3.132.45	(&(servicePrincipalName=MSSQL**))	DC=bas,DC=lab	
Jul 26, 2022 @ 02:30:49.608	10.3.132.45	(&(servicePrincipalName=MSSQL**))	DC=bas,DC=lab	

LDAP. Threat hunting. PowerView

PowerView : Get-DomainUser -PreauthNotRequired -Verbose

event_type:LDAPQuery AND
ldap_filter:("805306368" AND "userAccountControl" AND "4194304") AND
ldap_attrib_list.keyword://



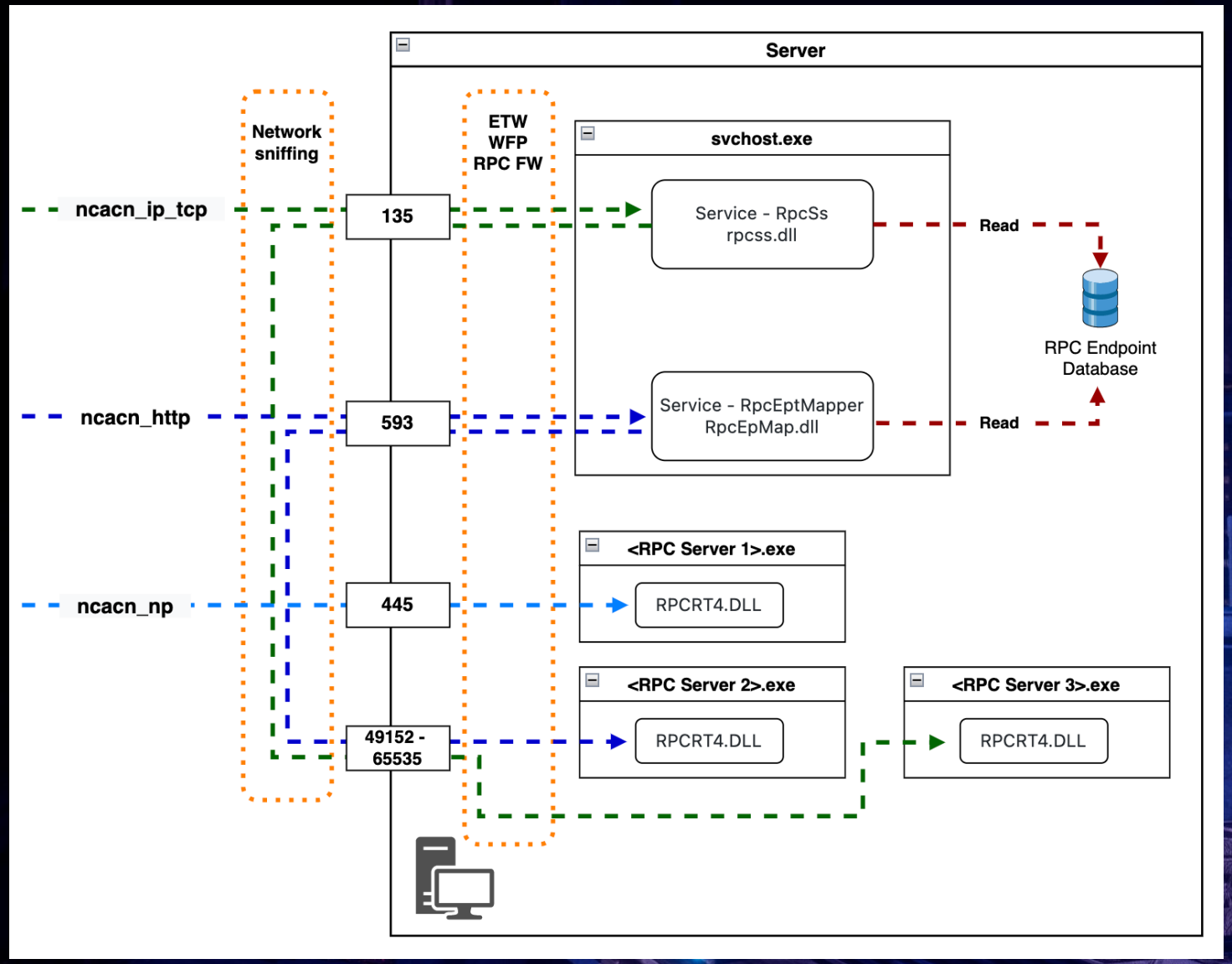
Time	dev_ipv4	proc_cmdline		ldap_filter	ldap_dn	ldap_attrib_list
Jul 26, 2022 @ 02:46:16.292	10.3.132.45	powershell	-ExecutionPolicy Bypass	(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))	DC=BAS,DC=LAB	
Jul 26, 2022 @ 02:46:16.289	10.3.132.45	powershell	-ExecutionPolicy Bypass	(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))	DC=BAS,DC=LAB	

LDAP. Threat hunting

Activity	Hunting query
Accounts for Kerberosting	event_type:LDAPQuery AND ldap_filter.keyword:/.*servicePrincipalName=*.*/
Unconstrained delegation	event_type:LDAPQuery AND ldap_filter:524288
Admin accounts	event_type:LDAPQuery AND ldap_filter:"admincount=1"
LAPS password dump	event_type:LDAPQuery AND ldap_filter.keyword:/.*ms-MCS-AdmPwd=*.*/
gMSA password dump	event_type:LDAPQuery AND ldap_attrib_list:"msDS-ManagedPassword"
KrbRelayUp usage	event_type:LDAPquery AND ldap_filter:*KRBRELAYUP*

RPC. What is it?

RPC (Remote Procedure Call) is a mechanism that allows programs from different machines to communicate between them by calling functions over the network.



https://zer1t0.gitlab.io/posts/attacking_ad/

RPC. ETW + Audit

Preparatory steps:

1. Enable RPC Audit

   auditpol /set /subcategory:"RPC Events" /success:enable /failure:enable

2. Adding RPC Filters for required interfaces

   netsh -f rpcfilter.txt

```
rpc
filter
add rule layer=um actiontype=permit audit=enable
add condition field=if_uuid matchtype=equal data=<RPC_iface_UUID>
add filter
quit
```

rpcfilter.txt

https://www.akamai.com/blog/security/guide-rpc-filter

Docs / Windows / Security / Security auditing /

5712(S): A Remote Procedure Call (RPC) was attempted.

Article • 10/29/2021 • 2 minutes to read • 5 contributors

It appears that this event never occurs.

Subcategory: Audit RPC Events

Event 5712, Microsoft Windows security auditing.

General | Details

A Remote Procedure Call (RPC) was attempted.

Subject:
- SID: TMD_LAB\Administrator
- Name: Administrator
- Account Domain: TMD_LAB
- LogonId: 0x96B759A

Process Information:
- PID: 636
- Name: lsass.exe

Network Information:
- Remote IP Address: 10.3.132.41
- Remote Port: 50154

RPC Attributes:
- Interface UUID: {e3514235-4b06-11d1-ab04-00c04fc2dcd2}
- Protocol Sequence: ncacn_ip_tcp
- Authentication Service: 9
- Authentication Level: 6

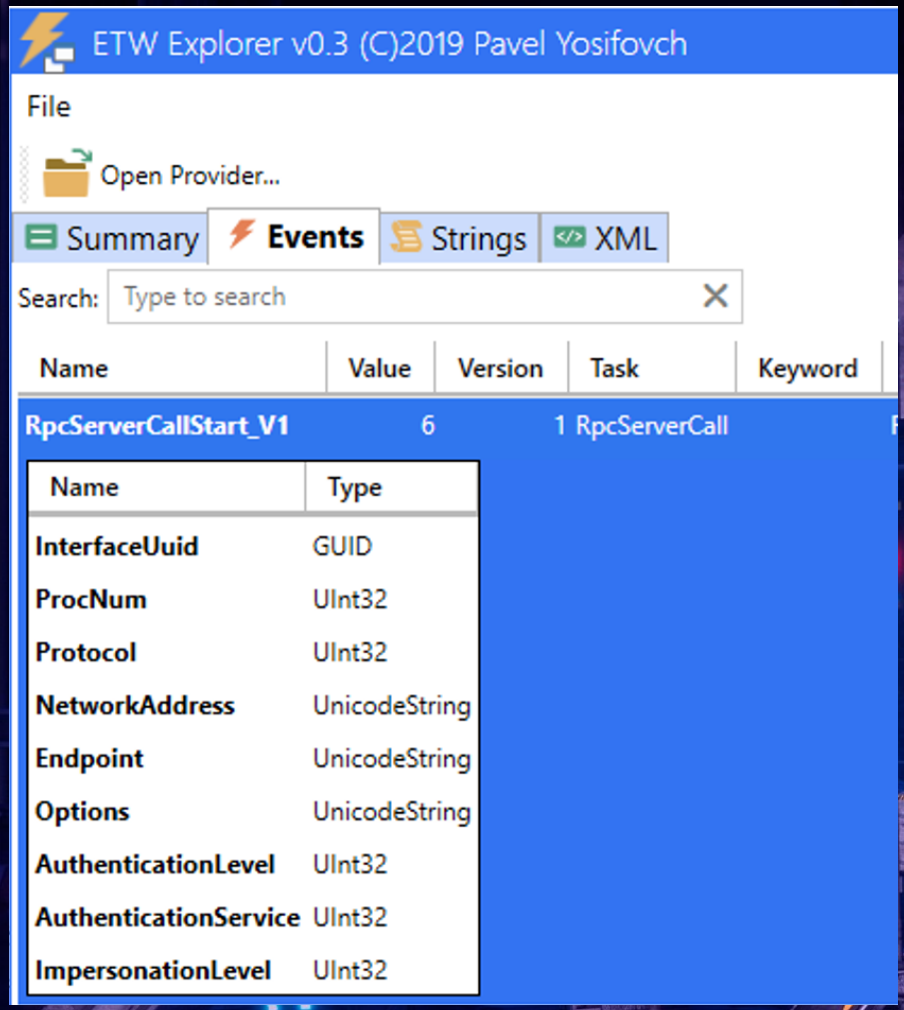
RPC. ETW + Audit

ETW Name: Microsoft-Windows-RPC

ETW GUID: {6AD52B32-D609-4BE9-AE07-CE8DAE937E39}

Event ID: 6

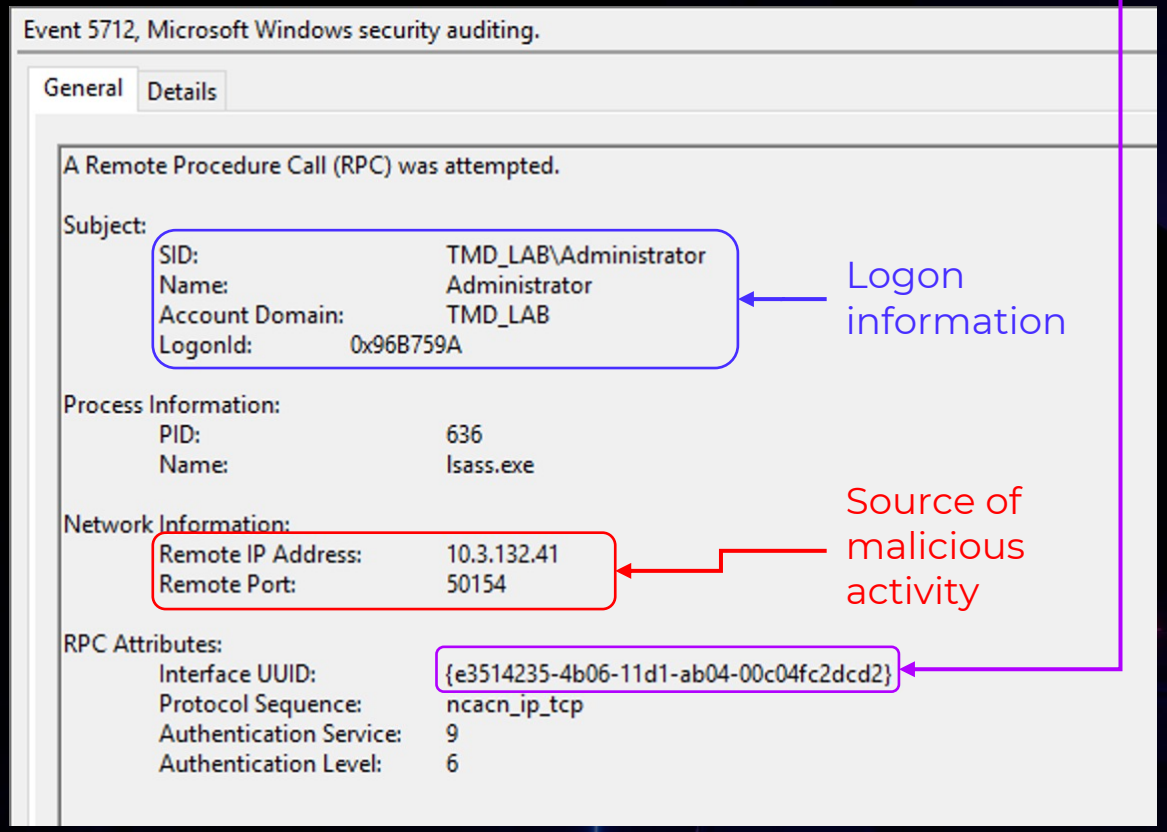
```
{
        e3514235-4b06-11d1-ab04-00c04fc2dcd2},
        0x3,
        "TCP ",
         "NULL",
        "49670",
        "NULL",
        "Packet Privacy ",
         "Kerberos ",
        "Default "
}
```



RPC. ETW + Audit

Time	rpc_iface	rpc_iface_uuid	rpc_opnum	rpc_method	rpc_endpoint
Aug 22, 2022 @ 17:25:57.741	MS-DRSR	E3514235-4B06-11D1-AB04-00C04FC2DCD2	3	DsGetNCChanges	49670

Malicious activity
(DCSync)



Logon information

Source of malicious activity

RPC. ETW + Audit

Malicious activity
(SharpHound)

Time	rpc_iface	rpc_iface_uuid	rpc_opnum	rpc_method	rpc_endpoint
Aug 22, 2022 @ 17:25:57.741	MS-SRVS	4B324FC8-1670-01D3-1278-5A47BF6EE188	12	NetrSessionEnum	\PIPE\srvsvc

Event 5712, Microsoft Windows security auditing.

General Details

A Remote Procedure Call (RPC) was attempted.

Subject:
- SID: TMD_LAB\Administrator
- Name: Administrator
- Account Domain: TMD_LAB
- LogonId: 0xD9C4921

Process Information:
- PID: 3468
- Name: svchost.exe

Network Information:
- Remote IP Address: 0.0.0.0 ?
- Remote Port: 0

RPC Attributes:
- Interface UUID: {4b324fc8-1670-01d3-1278-5a47bf6ee188}
- Protocol Sequence: ncacn_np
- Authentication Service: 0
- Authentication Level: 0

Event 4624, Microsoft Windows security auditing.

General Details

New Logon:
- Security ID: TMD_LAB\Administrator
- Account Name: Administrator
- Account Domain: TMD_LAB.COM
- Logon ID: 0xD9C4921
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {8d504349-350f-c658-e274-d28485e8ad34}

Process Information:
- Process ID: 0x0
- Process Name: -

Network Information:
- Workstation Name: -
- Source Network Address: 10.3.132.41
- Source Port: 50440

Source of malicious activity

RPC. ETW + Audit

Advantages:

- Allows native Windows mechanisms to monitor events

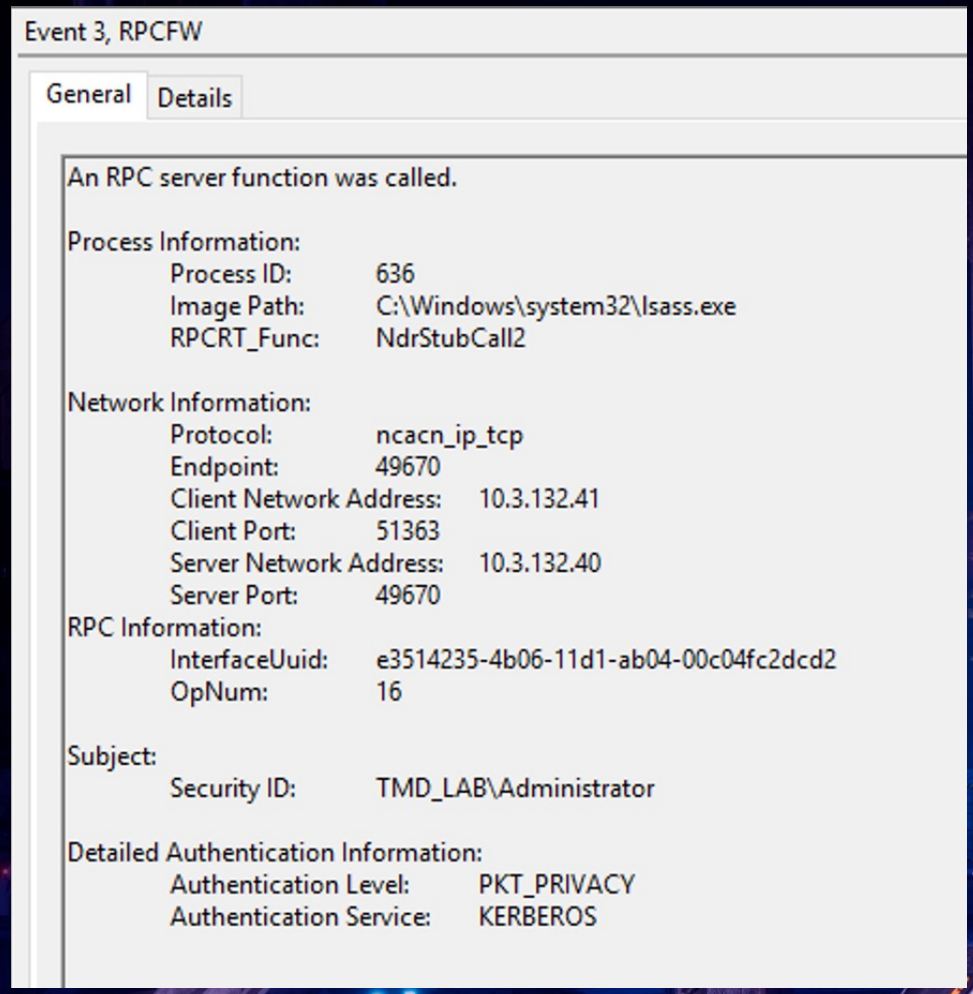
Disadvantages:

- Correlation between 2 or 3 events is required to determine the source of activity
- Huge flow of events

RPC. RPC Firewall

Features

1. RPC Filters - Enables the security audit of RPC events. These could be found under the Security log, with event ID 5712.
2. RPC Firewall - protects any RPC server process which is listening for remote RPC calls.



https://github.com/zeronetworks/rpcfirewall

RPC. RPC Firewall

Advantages:

- Determining the source of activity on a single event

Disadvantages:

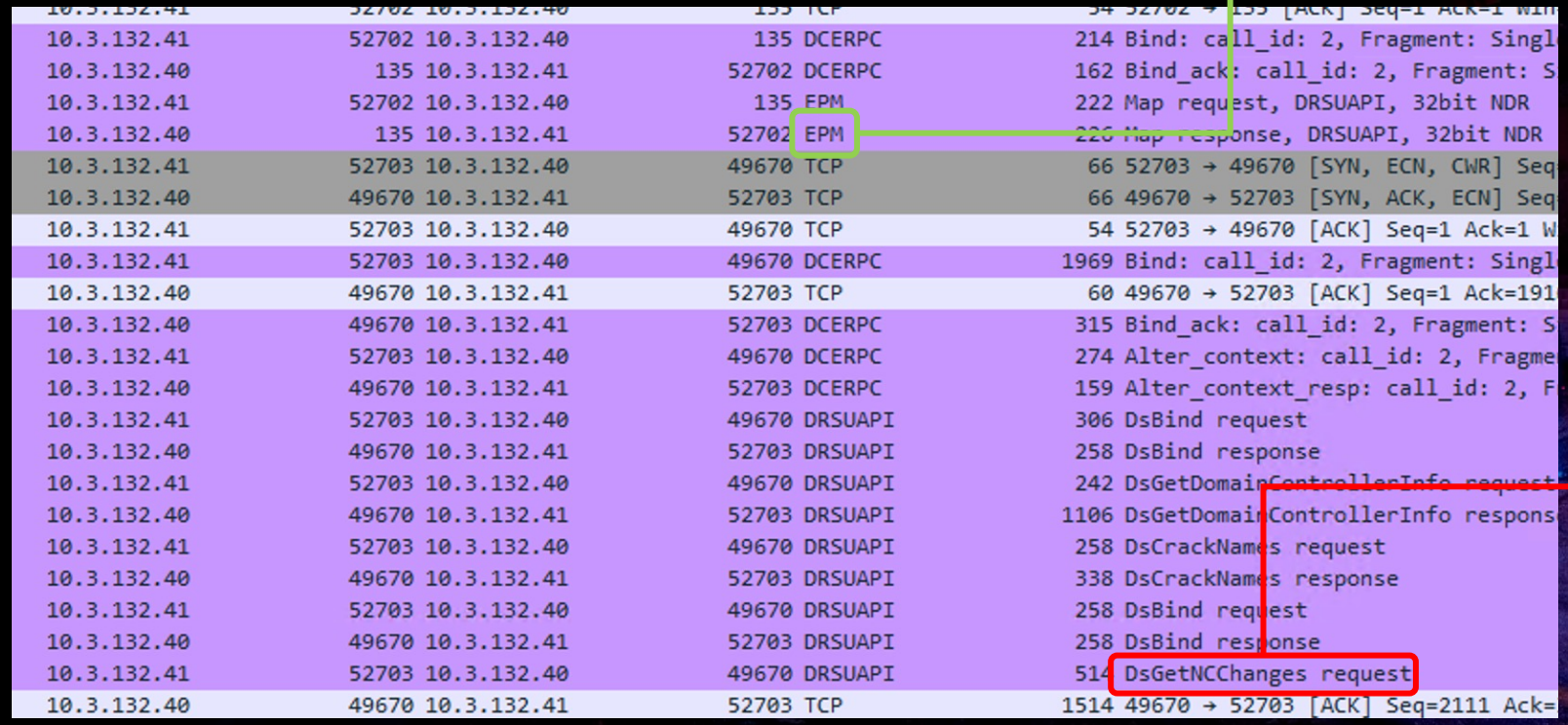
- Requires installation of third-party software
- Code injection into multiple processes (potentially dangerous)

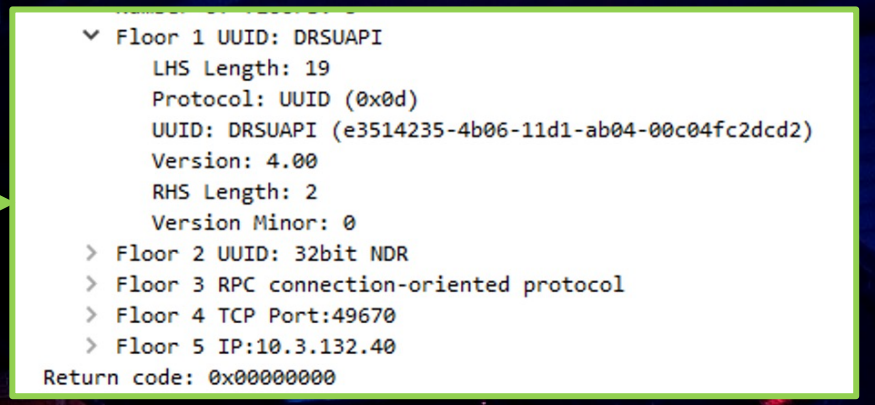
https://github.com/zeronetworks/rpcfirewall

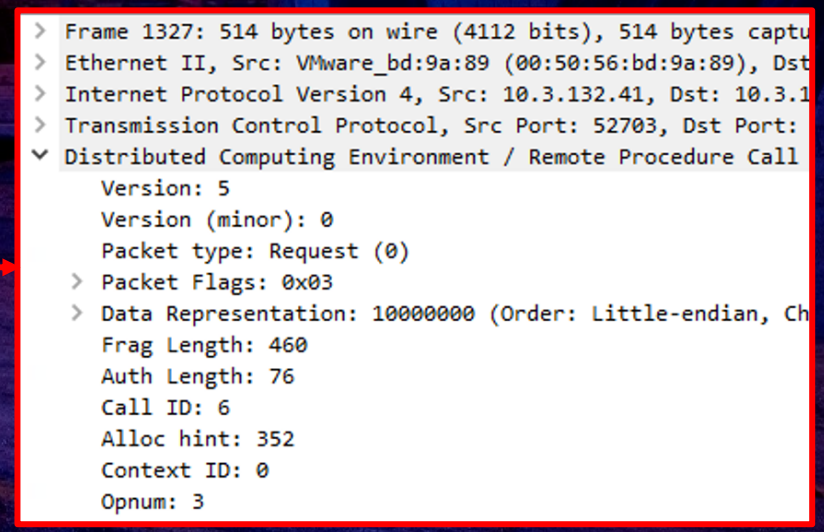
RPC. Network sniffing

Tools

- Zeek
- Suricata, etc.







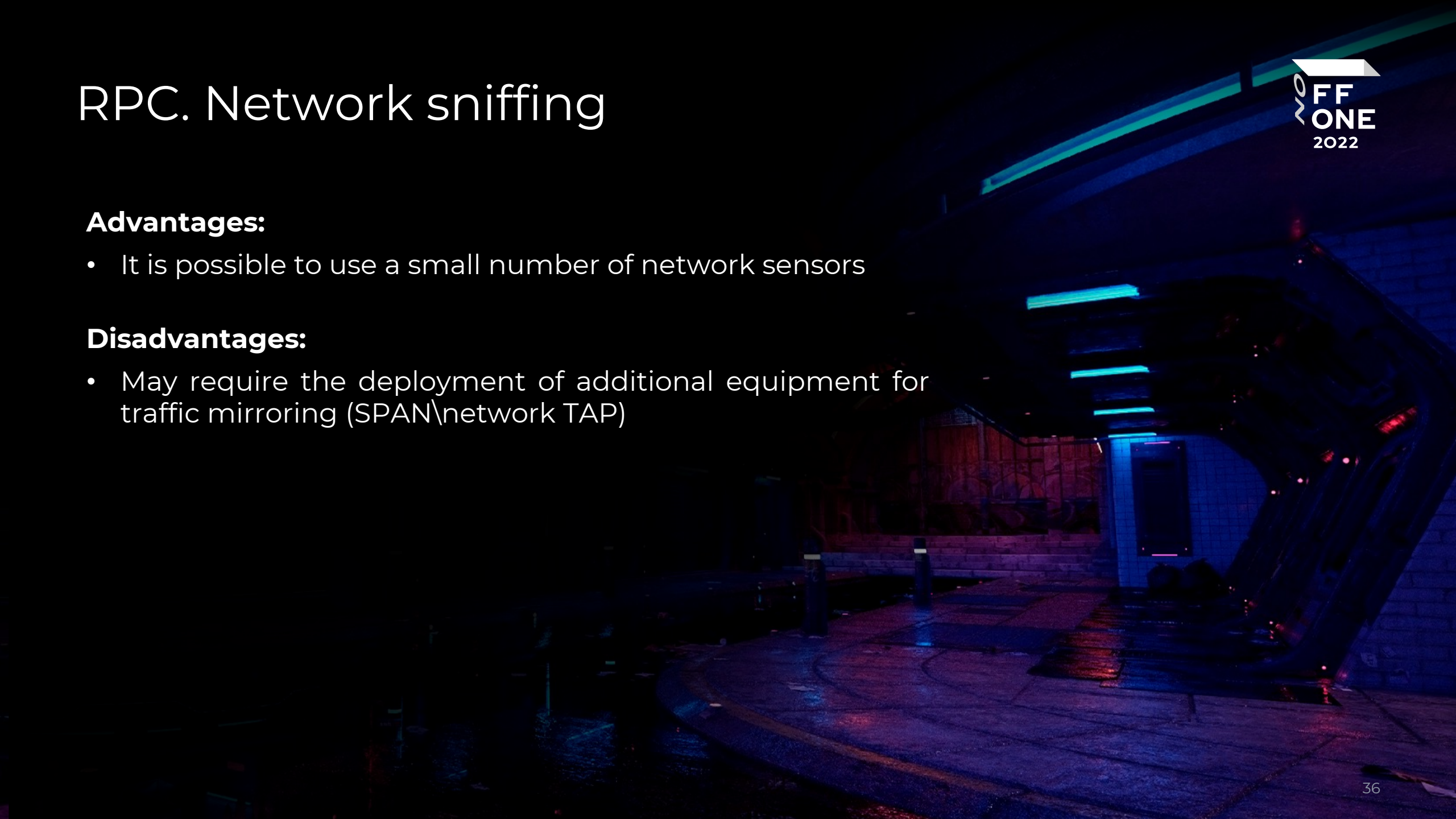
RPC. Network sniffing

Advantages:

- It is possible to use a small number of network sensors

Disadvantages:

- May require the deployment of additional equipment for traffic mirroring (SPAN\network TAP)



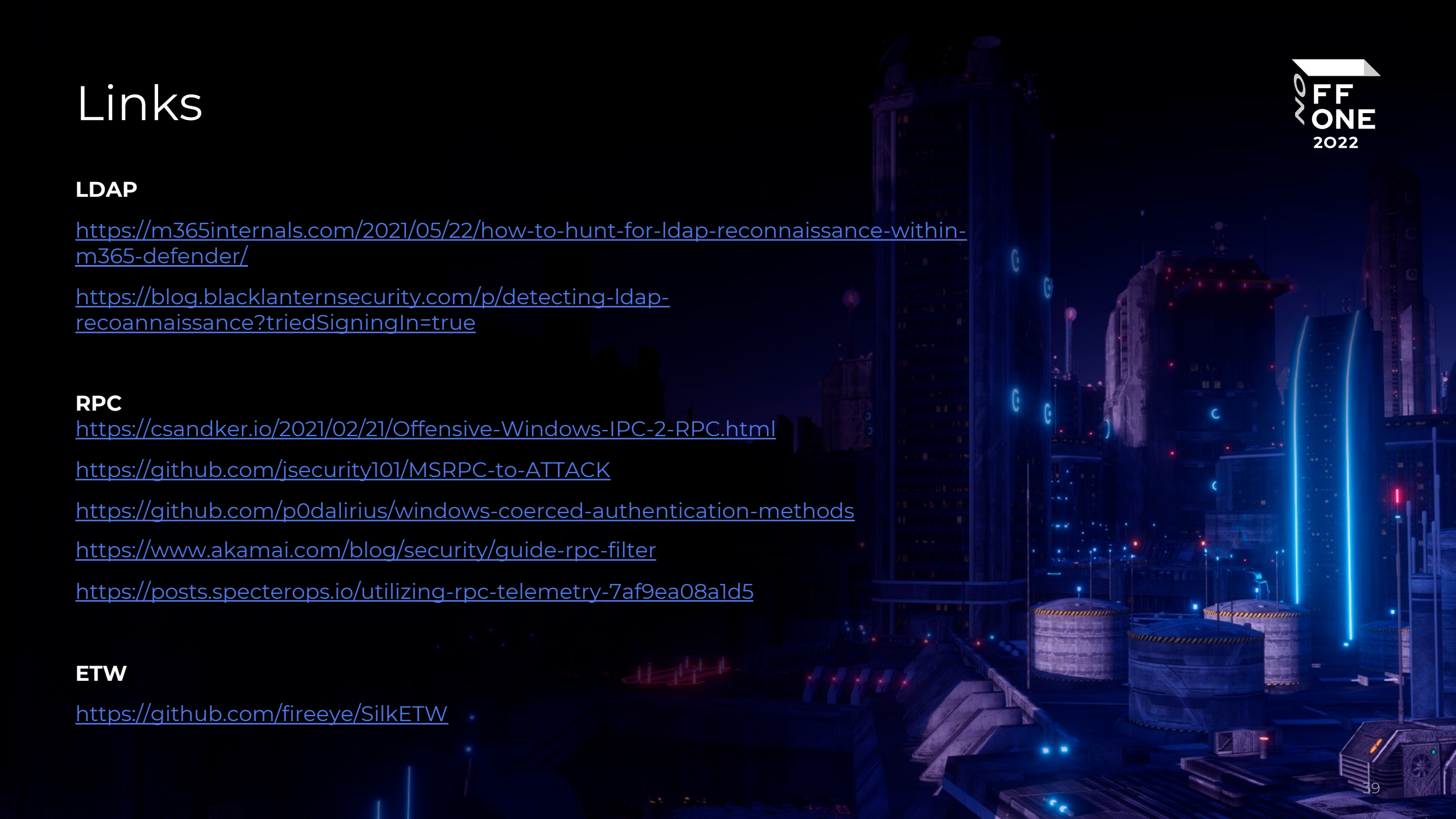
RPC. Threat hunting

Activity	Hunting query
SharpHound.exe --CollectionMethods Session	event_type:RPC AND rpc_iface_uuid:”4b324fc8-1670-01d3-1278-5a47bf6ee188” AND rpc_opnum: 12
SharpHound.exe --CollectionMethods LoggedOn	event_type:RPC AND rpc_iface_uuid:”6bffd098-a112-3610-9833-46c3f87e345a” AND rpc_opnum: 2
SharpHound.exe --CollectionMethods LocalAdmin SharpHound.exe --CollectionMethods RDP SharpHound.exe --CollectionMethods DCOM SharpHound.exe --CollectionMethods PSRemote	event_type:RPC AND rpc_iface_uuid:”12345778-1234-abcd-ef00-0123456789ac” AND rpc_opnum: 33
Mimikatz.exe "lsadump::dcsync /user:krbtgt"	event_type:RPC AND rpc_iface_uuid:”e3514235-4b06-11d1-ab04-00c04fc2dcd2” AND rpc_opnum: 3

RPC. Threat hunting

Activity	Hunting query
PrinterBug	event_type:RPC AND rpc_iface_uuid:"12345678-1234-abcd-ef00-0123456789ab" AND rpc_opnum: (65 OR 62)
ShadowCoerce	event_type:RPC AND rpc_iface_uuid:"a8e0653c-2744-4389-a61d-7373df8b2292" AND rpc_opnum: (8 OR 9)
DFSCoerce	event_type:RPC AND rpc_iface_uuid:"4fc742e0-4a10-11cf-8273-00aa004ae673" AND rpc_opnum: (12 OR 13)
PetitPotam	event_type:RPC AND rpc_iface_uuid:("df1941c5-fe89-4e79-bf10-463657acf44d" OR "c681d488-d850-11d0-8c52-00c04fd90f7e") AND rpc_opnum: (0 OR 4 OR 5 OR 6 OR 7 OR 8 OR 9)

Links



LDAP

https://m365internals.com/2021/05/22/how-to-hunt-for-ldap-reconnaissance-within-m365-defender/

https://blog.blacklanternsecurity.com/p/detecting-ldap-recoannaissance?triedSigningIn=true

RPC

https://csandker.io/2021/02/21/Offensive-Windows-IPC-2-RPC.html

https://github.com/jsecurity101/MSRPC-to-ATTACK

https://github.com/p0dalirius/windows-coerced-authentication-methods

https://www.akamai.com/blog/security/guide-rpc-filter

https://posts.specterops.io/utilizing-rpc-telemetry-7af9ea08a1d5

ETW

https://github.com/fireeye/SilkETW


OFF
ONE
2022