

# **"Les outils de détection, de supervision et de traitement des évènements de sécurité des systèmes Windows".**

# Les journaux windows (source ANSSI)

- Les évènements des systèmes d'exploitation Windows sont enregistrés dans les fichiers de journaux.
- Ceux-ci sont répartis dans deux rubriques, « **joumaux Windows** » et « **joumaux des applications et des services** ».
- Tous ces journaux sont visualisables à l'aide de la console Microsoft Management Console (MMC) « observateur d'évènements » (eventvwr.msc) et sont stockés par défaut à l'emplacement *%WINDIR%\System32\winevt\Logs*.
- Le format de stockage des journaux est **EVTX** (XML).

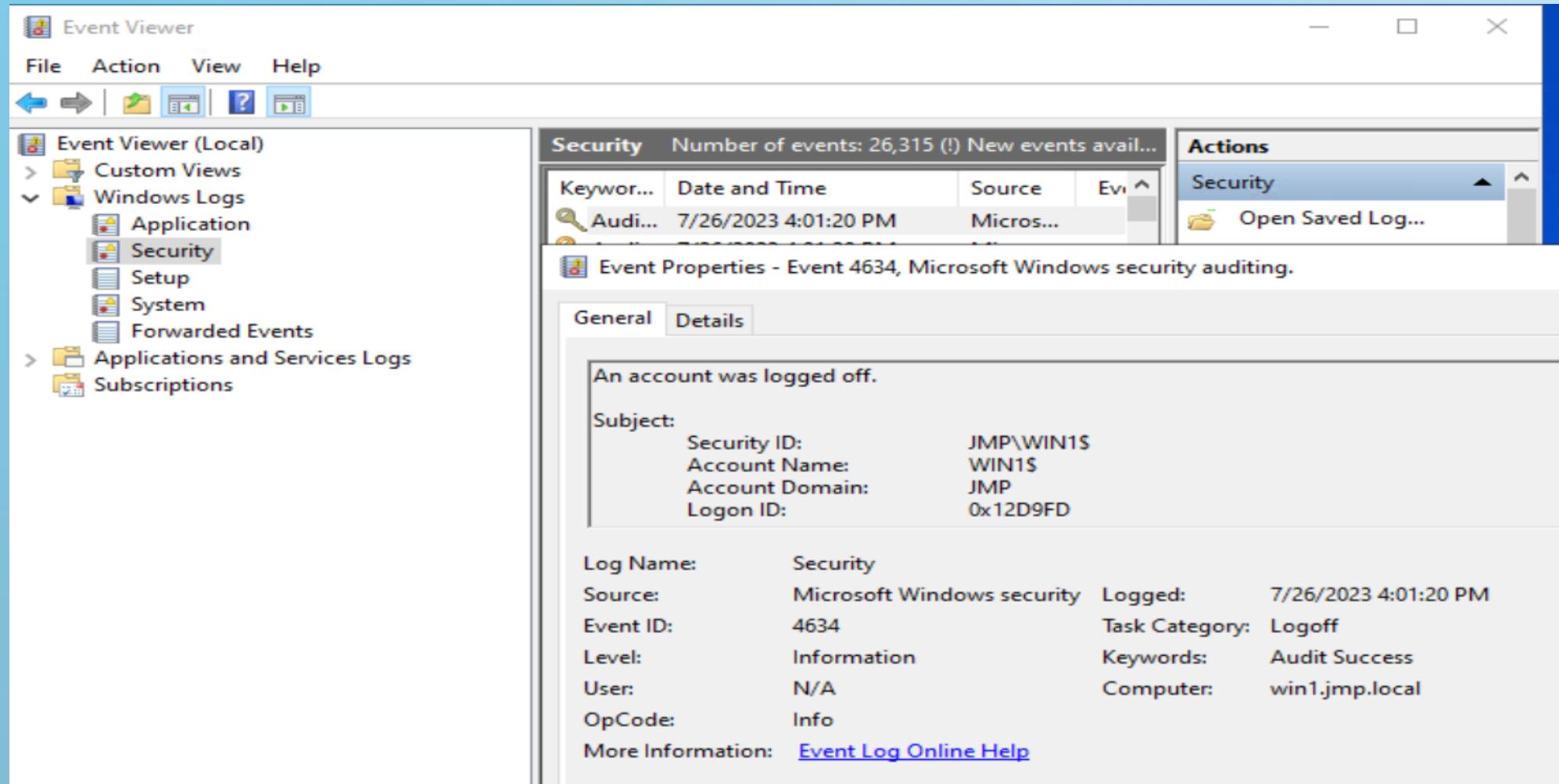
## Les journaux windows (source ANSSI)

- Les journaux Windows sont répartis en quatre canaux: « **Application** », « **Installation** », « **Sécurité** » et « **Système** », chacun servant à l'écriture des évènements liés à ces quatre types d'évènements. "Forwarded Events" est un journal qui contient les évènements transférés par un serveur de collecte (W.E.C.) depuis des ordinateurs sources (WEF).

## Les journaux windows (source ANSSI)

- Les « **joumaux des applications et des services** » sont des journaux secondaires qui peuvent être créés par divers fournisseurs d'évènements et stockent des évènements spécifiques à certains "providers" (Windows Defender, Windows PowerShell...). Certains de ces journaux sont utiles pour la détection d'intrusion.

# "Event viewer": journaux système d'exploitation Windows



# "Event viewer": journaux applicatifs Windows

The screenshot shows the Windows Event Viewer interface. The left pane displays navigation options like Custom Views, Windows Logs (Application, Security, Setup, System, Forwarded Events), Applications and Services Logs, and Subscriptions. The right pane shows the Application log with 247 events. A specific event (Event 16384) is selected, showing details about a scheduled restart for the Software Protection service.

Level	Date and Time	Source	Event ID	Type
Warning	7/25/2023 7:19:11 PM	Perflib	1008	Nc
Information	7/25/2023 7:19:11 PM	edgeupdate	0	Nc
Information	7/25/2023 7:19:11 PM	WMI	5617	Nc
Information	7/25/2023 7:19:10 PM	WMI	5615	Nc
Information	7/25/2023 7:19:10 PM	User Profile Service	1531	Nc
Information	7/25/2023 7:19:10 PM	Security-SPP	1040	Nc
Information	7/25/2023 7:19:10 PM	EventSystem	4625	Nc
Information	7/13/2023 1:43:24 PM	User Profile Service	1532	Nc
Warning	7/13/2023 1:43:24 PM	Winlogon	6001	Nc
Information	7/13/2023 1:43:24 PM	Winlogon	6000	Nc
Information	7/13/2023 1:43:21 PM	Security-SPP	12307	Nc
Information	7/13/2023 1:43:21 PM	Security-SPP	16394	Nc
Information	7/13/2023 1:43:03 PM	MSDTC	4111	SV

Event 16384, Security-SPP

General Details

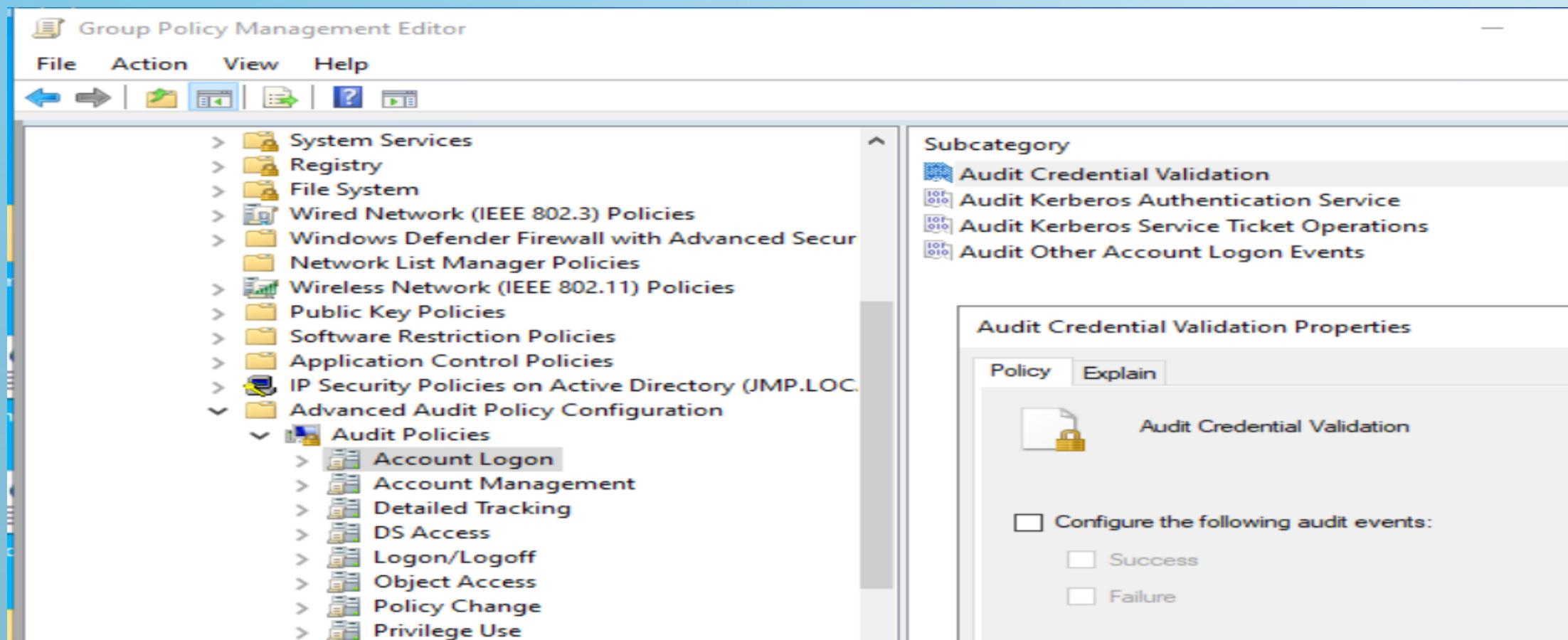
Successfully scheduled Software Protection service for re-start at 2023-12-22T17:19:56Z RulesEngine.

Log Name: Application  
Source: Security-SPP  
Logged: 7/26/2023 4:01:56 PM

## Stratégies d'audit (source ANSSI)

- Les systèmes Windows intègrent nativement plus d'une cinquantaine de stratégies d'audit dont l'activation va avoir pour effet de générer des évènements de sécurité de différentes catégories. Ces évènements sont écrits dans le journal « Sécurité » de Windows.
- C'est un complément **indispensable** à la journalisation des évènements de sécurité pour la détection d'intrusion.

# La mise en oeuvre des stratégies d'audit se fait par GPO.



# Event Tracing for Windows (E.T.W.)

- Event Tracing for Windows (**E.T.W.**) est un **mécanisme de suivi** (tracing) des événements conçu par Microsoft pour le système d'exploitation Windows. Il permet aux développeurs, aux administrateurs système et aux outils de diagnostic de collecter, visualiser et analyser les événements qui se produisent sur un système Windows en temps réel.
- C'est l'équivalent de *Rsyslog* sous Linux mais il génère des événements dans un format XML.

# Collecte des évènements de sécurité avec un service natif de Windows

- **Windows Event Forwarding (W.E.F.)** permet la transmission (forwarding) des **événements** de journalisation depuis un ordinateur source (provider) vers un ordinateur de collecte centralisé appelé **Windows Event Collector (W.E.C.)**.
- C'est un **tampon de données indispensable** avant la transmission des informations vers un S.I.E.M. (cf les 10 commandements du S.I.E.M.) afin d'éviter de perdre des évènements.

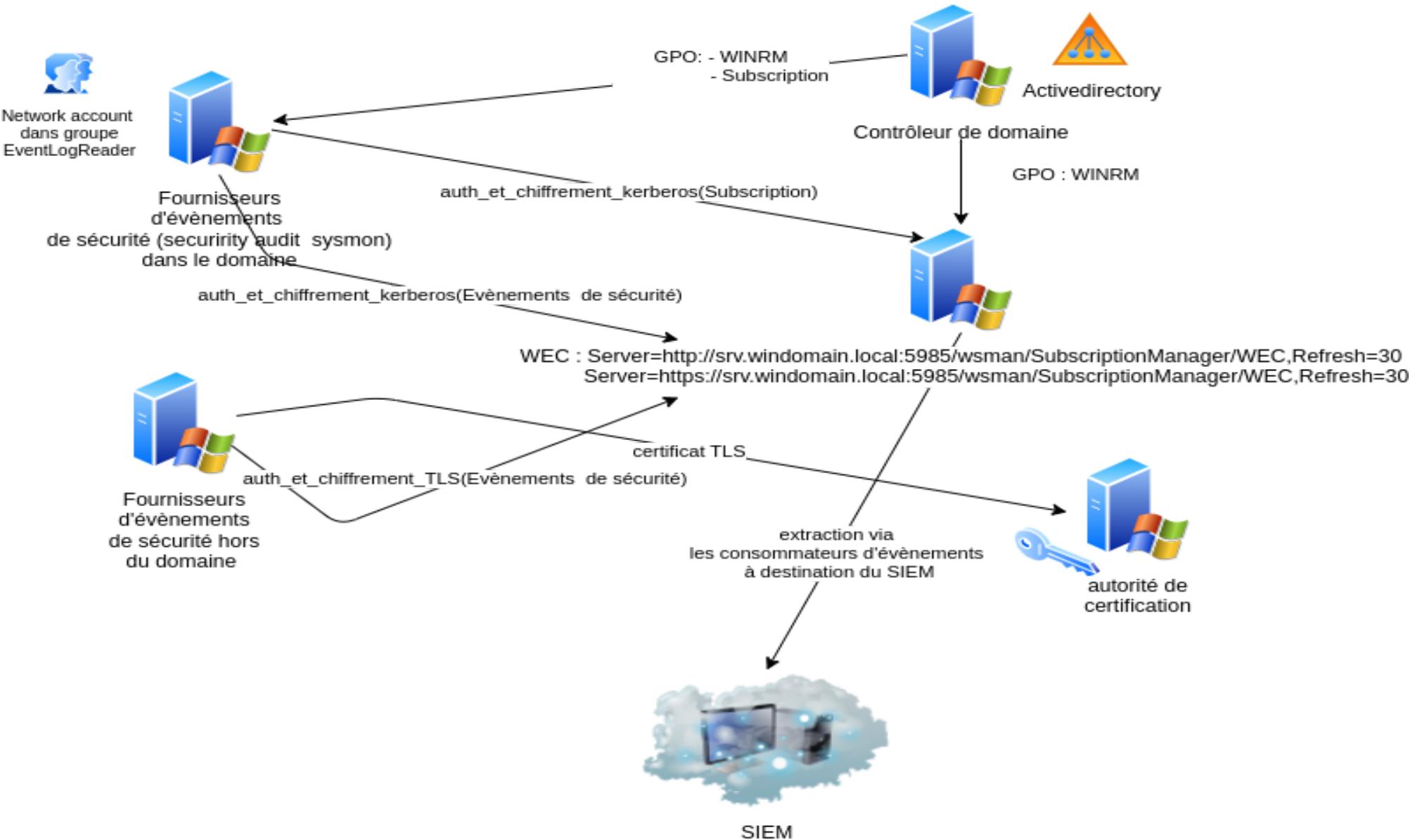
# Vocabulaire E.T.W.

- Une application peut être un *fournisseur(provider)* d'évènements. Elle peut être un service, un pilote, une application, un composant ou un module écrit des évènements dans une session E.T.W.. Le provider est activé par une "*tracing session*".
- Un "*channel*", dont la matérialisation est un fichier de "logs", stocke les évènements qui lui sont envoyés. Il y a des channels par défaut dans Windows et on peut en créer de nouveaux en récupérant les flux de nouveaux providers.
- Ces informations sont utilisées par les consommateurs d'évènements ("*event consumers*") qui peuvent les agréger pour les stocker ou les envoyer vers un S.I.E.M..

## Event Tracing for Windows (E.T.W.) (source Misc HS 23)

- Les *sessions* sont chargées de configurer les providers en spécifiant leurs canaux et leurs niveaux de verbosité. Une session peut agréger les événements provenant de plusieurs providers.
- Les *consumers* sont chargés de collecter les événements depuis les sessions pour les afficher, les stocker ou bien les transférer (par exemple vers un S.I.E.M.).

## R5.cyber.11 Supervision de la sécurité: gestion des évènements de sécurité des systèmes Windows



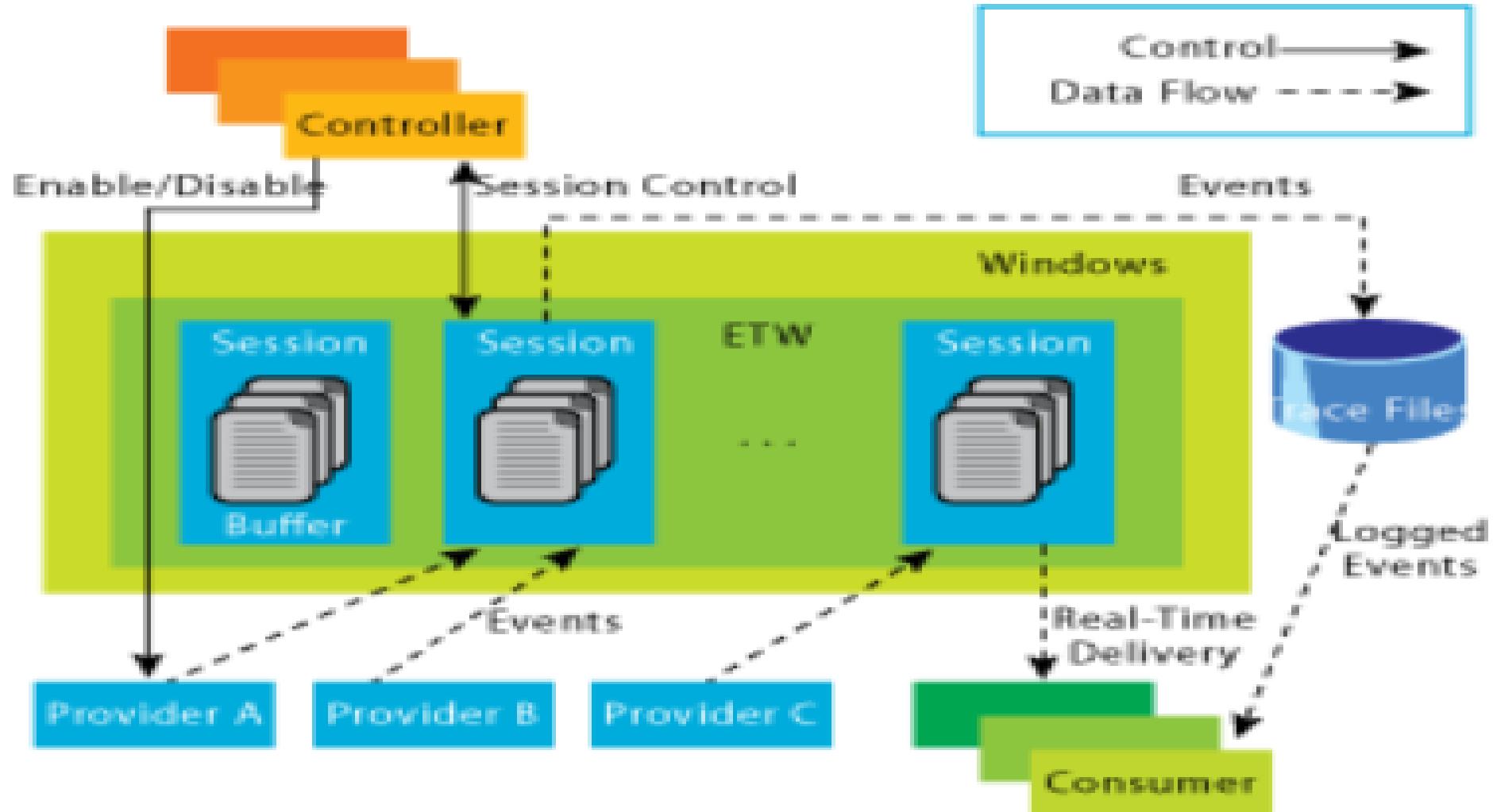
# Logman: interroger les providers

Provider	GUID
<hr/>	
ACPI Driver Trace Provider	{DAB01D4D-2D48-477D-B1C3-DAAD0CE6F06B}
Active Directory Domain Services: Core	{1C83B2FC-C04F-11D1-8AFC-00C04FC21914}
Active Directory Domain Services: SAM	{8E598056-8993-11D2-819E-0000F875A064}
Active Directory: Kerberos Client	{BBA3ADD2-C229-4CDB-AE2B-57EB6966B0C4}
Active Directory: Kerberos KDC	{24DB8964-E6BC-11D1-916A-0000F8045B04}
Active Directory: NetLogon	{F33959B4-DBEC-11D2-895B-00C04F79AB69}
ADODB.1	{04C8A86F-3369-12F8-4769-24E484A9E725}
ADOMD.1	{7EA56435-3F2F-3F63-A829-F0B35B5CAD41}
Application Popup	{47BFA2B7-BD54-4FAC-B70B-29021084CA8F}
Application-Addon-Event-Provider	{A83FA99F-C356-4DED-9FD6-5A5EB8546D68}
ATA Port Driver Tracing Provider	{D08BD88E-F01E-480A-BAC6-B7D24BEFF6BF}

# Logman: interroger les sessions

Data Collector Set	Type	Status
Eventlog-Security	Trace	Running
DiagLog	Trace	Running
Diagtrack-Listener	Trace	Running
EventLog-Application	Trace	Running
EventLog-ForwardedEvents	Trace	Running
EventLog-Microsoft-Windows-Sysmon-Operational	Trace	Running
EventLog-System	Trace	Running
Microsoft-Windows-Rdp-Graphics-RdpIdd-Trace	Trace	Running
NtfsLog	Trace	Running
JAL_Usermode_Provider	Trace	Running
JBPM	Trace	Running
WdiContextLog	Trace	Running
MpWppTracing-20230727-105401-00000003-ffffffffff	Trace	Running
SYSMON TRACE	Trace	Running

## Event Tracing for Windows (source Microsoft SDN)



## Event Tracing for Windows (source ANSSI)

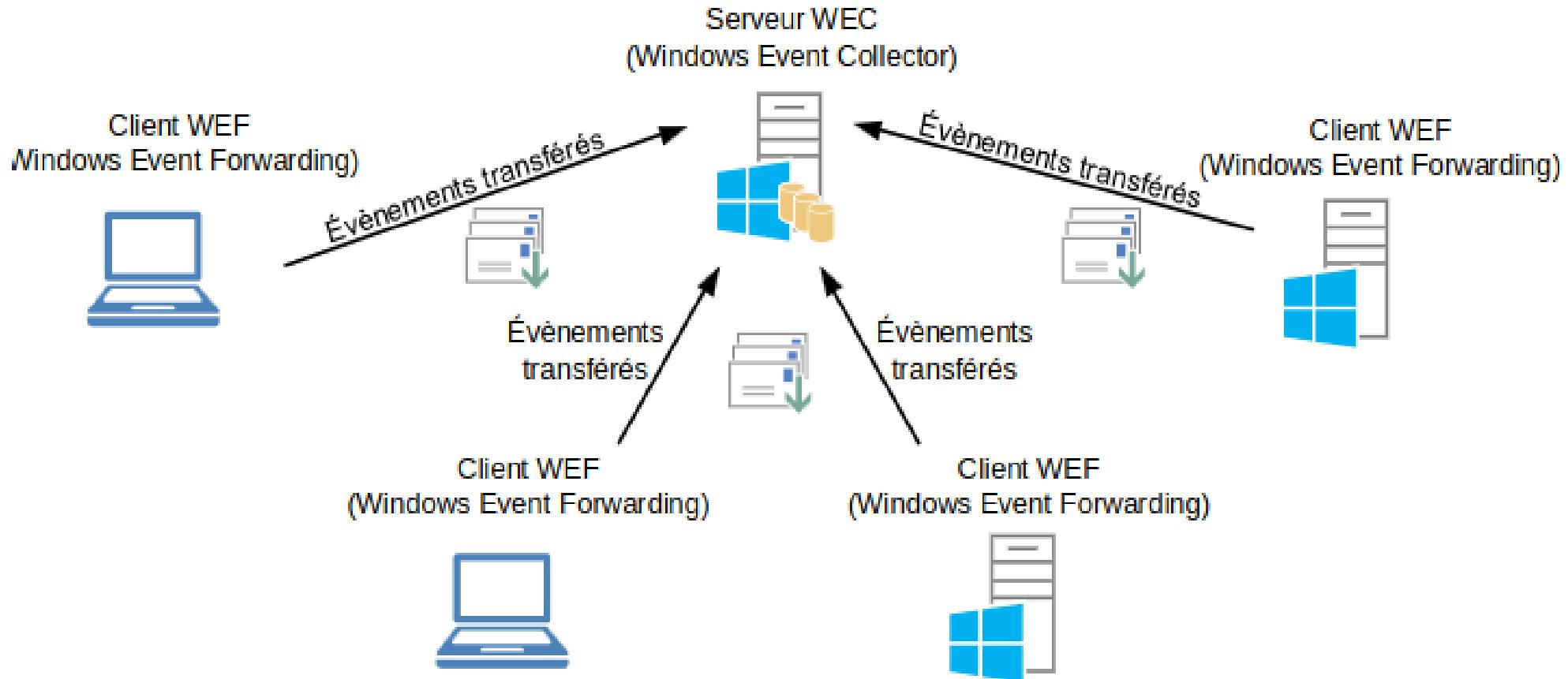


FIGURE 2 – Représentation de l'articulation entre WEC et WEF

**"Services et protocoles Windows utiles pour la gestion des évènements de sécurité".**

# Windows Remote Management (WS-Management)

- **WinRM** est basé sur "Windows Remote Management" qui est l'implémentation de Microsoft de "Web Services for Management (WS-Management)".
- **WS-Management** utilise le protocole *HTTP/SOAP* et échange des informations au format XML.

## Etapes du processus de configuration de E.T.W.

- *Configuration du serveur de collecte (collector)* : Le serveur de collecte est l'ordinateur centralisé qui recevra les événements de plusieurs sources.
- *Configuration des abonnements* : Sur chaque ordinateur source, vous configurez un abonnement qui spécifie les événements que vous souhaitez transférer vers le serveur de collecte.
- *Configuration des canaux de transfert* : Les canaux de transfert définissent comment les événements seront envoyés au serveur de collecte, tels que le mode de connexion (push ou pull) et les protocoles utilisés (par exemple, HTTP(S)).

# Fonctionnement de la solution E.T.W.

- L'**exécution** se fait avec les privilèges **NETWORK SERVICES**. Il faudra modifier les descripteurs de sécurité ([SDDL](#)) pour que l'agent puisse accéder aux journaux de sécurité.
- La remontée des logs peut se faire en mode **push** initié par la source (*méthode recommandée*), ou en mode **pull** initié par le collecteur.

# Fonctionnement de la solution E.T.W.

- L'authentication et le chiffrement sont réalisés par Kerberos ou TLS. La compression des évènements de sécurité est faite via l'algorithme SLDC.
- Le transport se fait par **WinRM** (Windows Remote Management). Le port utilisé est le **5985** (HTTP) ou **5986** (HTTPS) et l'U.R.L. de la forme :

<http://srv.windomain.local:5985/wsman/SubscriptionManager/W.E.C.,Refresh=30>

## Conclusion E.T.W.

- "Au final la solution E.T.W. fournie nativement **assez peu d'évènements** susceptibles d'être exploités pour la détection des T.T.P ("*Tactics, Techniques and Procedures MITRE*") d'un attaquant."
- La configuration avancée de l'*audit* et surtout **Sysmon** permettent de combler ce manque.

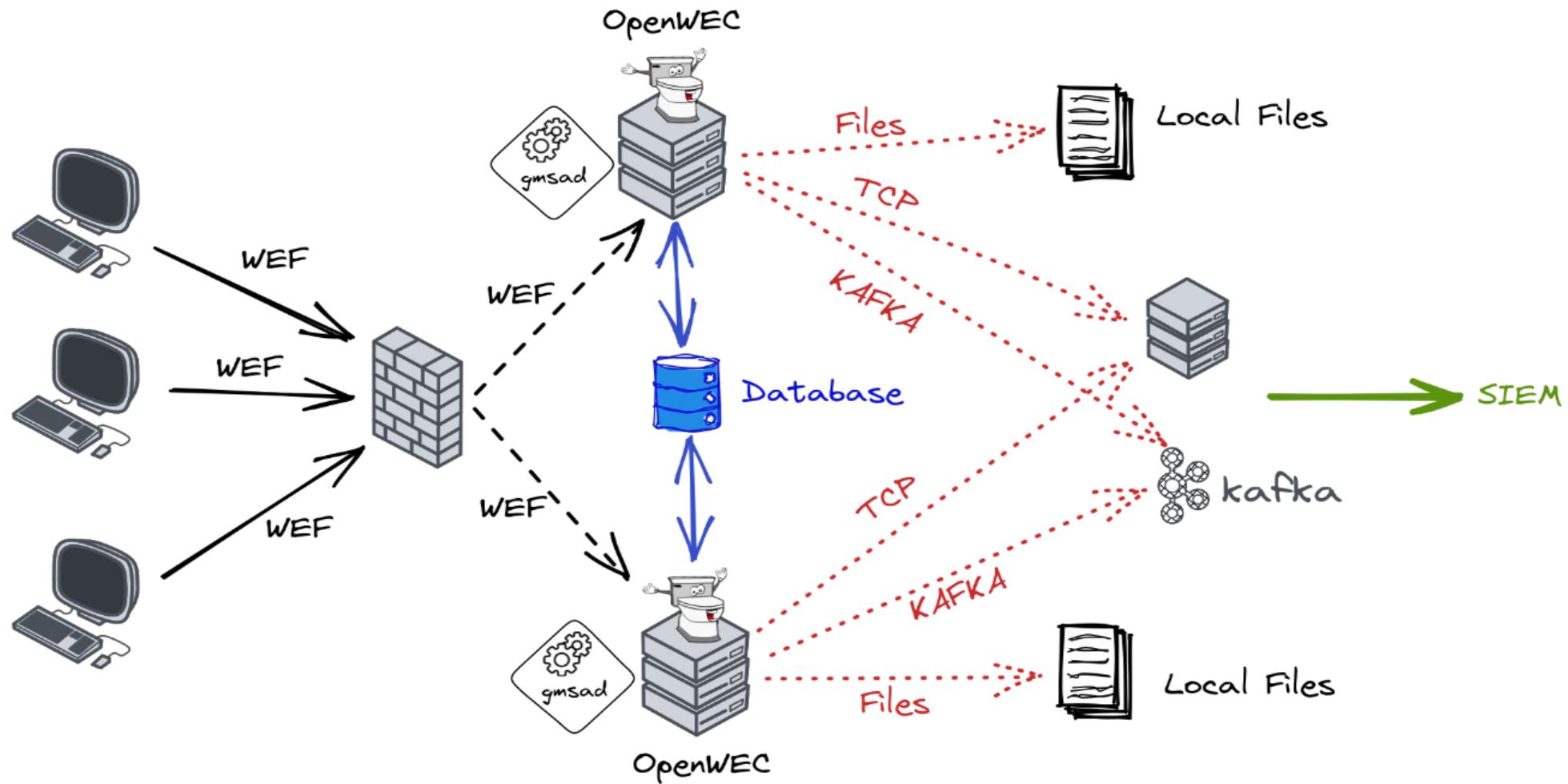
## Autre solution: la collecte des évènements de sécurité sous Windows via un agent externe

- On peut installer un agent externe sous windows pour collecter les évènements de sécurité et les envoyer vers un serveur de collecte.
- On peut citer **NXlogs** et **winlogbeat**(beat Suite d'Elastic) comme solutions ou des **Universal Forwarder** de "Splunk".  
=> La présence d'une solution tierce-partie **augmente la surface d'attaque!** n'est pas recommandé par l'A.N.S.S.I. (voir guide de sécurisation des journaux systèmes source ANSSI)

# "OpenWEC" est un serveur W.E.C. open-source Français !

- C'est un serveur de collecte de journaux Windows open-source écrit en Rust et développé par le C.E.A. (Commissariat à l'énergie atomique et aux énergies alternatives).
- Il permet de rediriger les journaux Windows vers *KAFKA*, des fichiers ou une socket TCP.
- Le service OpenWec nécessite d'avoir un S.P.N. (Service Principal Name) configuré pour le compte de service utilisé par le service OpenWec et donc un "Domaine" Active Directory.

# Architecture OpenWEC (source présentation SSTIC 2023)



# Sysmon (source Microsoft)

- **System Monitor** (Sysmon) est un service système Windows et un pilote de périphérique qui, une fois installé sur un système, reste résident entre les redémarrages du système pour surveiller et consigner l'activité système dans le journal des événements Windows. Il fournit des informations détaillées sur les créations de processus, les connexions réseau et les modifications apportées à l'heure de création de fichier.

# Sysmon

- Il fait partie de la célèbre suite "**SysInternal**" dont le concepteur est *Mark Russinovich* qui travaille maintenant pour Microsoft. Ce n'est pas un produit officiellement supporté bien que largement utilisé par les professionnels de la cyber-sécurité.
- Les logs issues de Sysmon sont stockées dans "*Applications and Services Logs/Microsoft/Windows/Sysmon/Operational*".

# Capacités de détection de Sysmon ()

- Processus
- Network
- Registry
- File
- Windows Management Instrumentation (WMI)

# Capacités de Sysmon ()

- Sysmon peut générer automatiquement des HASHS des binaires qui tournent sur un système et les comparer avec une liste blanche de HASHS (via *VirusTotal* par exemple).

# Exemple: "attaque" via mimikatz

```
mimikatz # sekurlsa::pth /user:vagrant /domain:jmp /ntlm:e02bc503339d51f71d913c245d35b50b
user      : vagrant
domain    : jmp
program   : cmd.exe
impers.   : no
NTLM      : e02bc503339d51f71d913c245d35b50b
| PID  3888
| TID  3188
| LSA Process is now R/W
| LUID 0 ; 8448037 (00000000:0080e825)
\_\_ msv1_0 - data copy @ 000001F1A4FA3D20 : OK !
\_\_ kerberos - data copy @ 000001F1B1333388
  \_\_ des_cbc_md4      -> null
  \_\_ des_cbc_md4      OK
  \_\_ *Password replace @ 000001F1B136F168 (32) -> null
```

# L'attaque est bien détectée par Sysmon

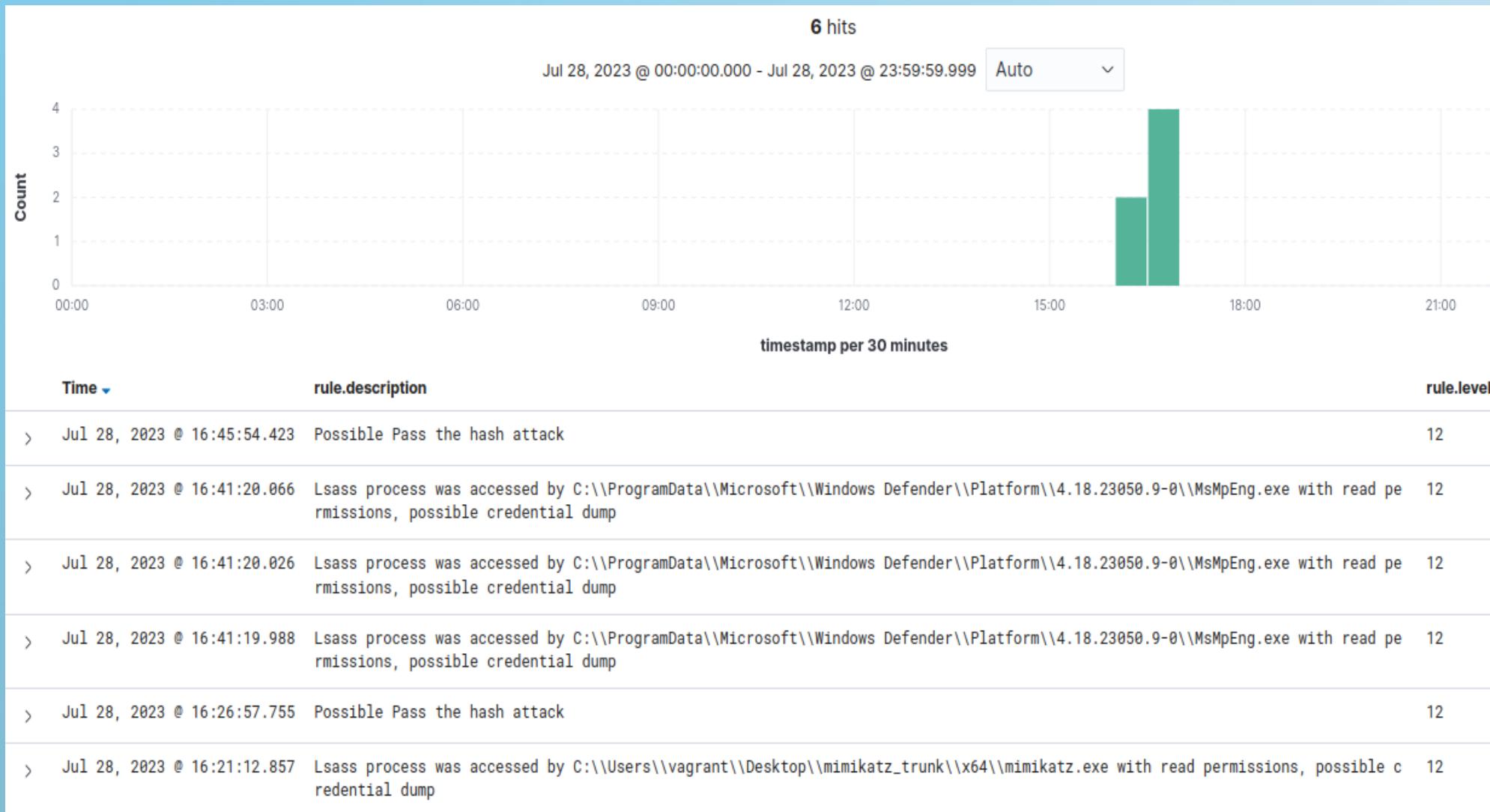
Event Properties - Event 1, Sysmon

General Details

Process Create:  
RuleName: -  
UtcTime: 2023-07-28 16:45:52.978  
ProcessGuid: {f914c434-f0c0-64c3-1003-0000000000f00}  
ProcessId: 5236  
Image: C:\Windows\System32\cmd.exe  
FileVersion: 10.0.20348.1 (WinBuild.160101.0800)  
Description: Windows Command Processor  
Product: Microsoft® Windows® Operating System  
Company: Microsoft Corporation  
OriginalFileName: Cmd.Exe  
CommandLine: cmd.exe  
CurrentDirectory: C:\Windows\system32\  
User: JMP\vagrant  
LogonGuid: {f914c434-f0c0-64c3-a1c7-890000000000}  
LogonId: 0x89C7A1  
TerminalSessionId: 2  
IntegrityLevel: High  
Hashes: MD5=E7A6B1F51EFB405287A8048CFA4690F4, SHA256  
=EB71EA69DD19F728AB9240565E8C7EFB59821E19E3788E289301E1E74940C208, IMPHASH=D60B77062898  
DC6BFAE7FE11A0F8806C  
ParentProcessGuid: {f914c434-eacb-64c3-0403-0000000000f00}  
ParentProcessId: 5524  
ParentImage: C:\Users\vagrant\Desktop\mimikatz\_trunk\x64\mimikatz.exe  
ParentCommandLine: mimikatz.exe  
ParentUser: JMP\vagrant

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon  
Event ID: 1  
Level: Information  
User: SYSTEM  
OpCode: Info  
Logged: 7/28/2023 4:45:52 PM  
Task Category: Process Create (rule: ProcessCreate)  
Keywords:  
Computer: win1.jmp.local

# L'attaque est "logguée" par le S.I.E.M. Wazuh



# bibliographie

- [OpenW.E.C. slides SSTIC2023](#)
- Collecte-de-logs-d-installations-industrielles-isolees (MISC 100 2018)
- [ETW simplifié Microsoft](#)
- [Sécurisation des journaux systèmes source ANSSI](#)
- ("sysmon") [<https://learn.microsoft.com/fr-fr/sysinternals/downloads/sysmon>]

# bibliographie

- [Policy Auditing\\_\(source Palantir\)](#)
- [SDDL language de définition des descripteurs de sécurité](#)
- "Doper votre S.I.E.M." MISC HS 23 (abonnement nécessaire)