LOGS SOUS WINDOWS

Bensoula Khaoula

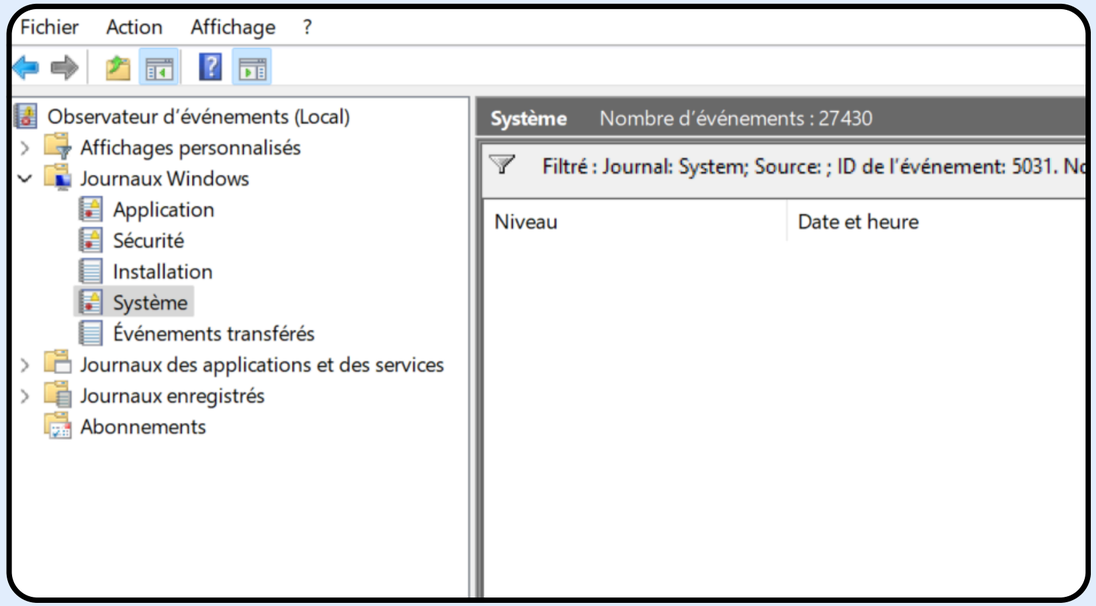
Bensekhar Maria Golsaf

Définition des logs:

Log (journal d’événements)

Un fichier généré automatiquement permet de conserver un historique des événements survenus au sein des systèmes informatiques (réseaux, serveurs, systèmes d’exploitation, applications, etc.).

Emplacement et accès




```
Get-EventLog -LogName Application
```

EMPLACEMENT

C:\Windows\System32\winevt\Logs\

1.

INTERFACE GRAPHIQUE :

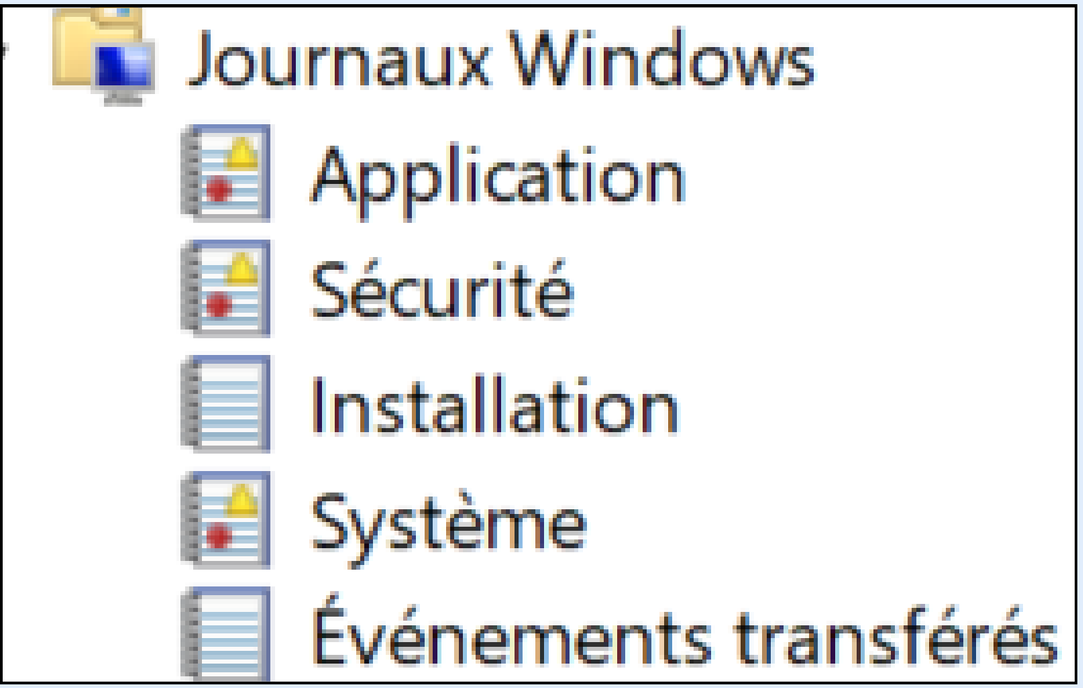
Observateur d'événements (Event Viewer)

2

POWERSHELL

Avec Get-EventLog cmdlet

Principaux types de journaux Windows



APPLICATION

Événements générés par les applications installées

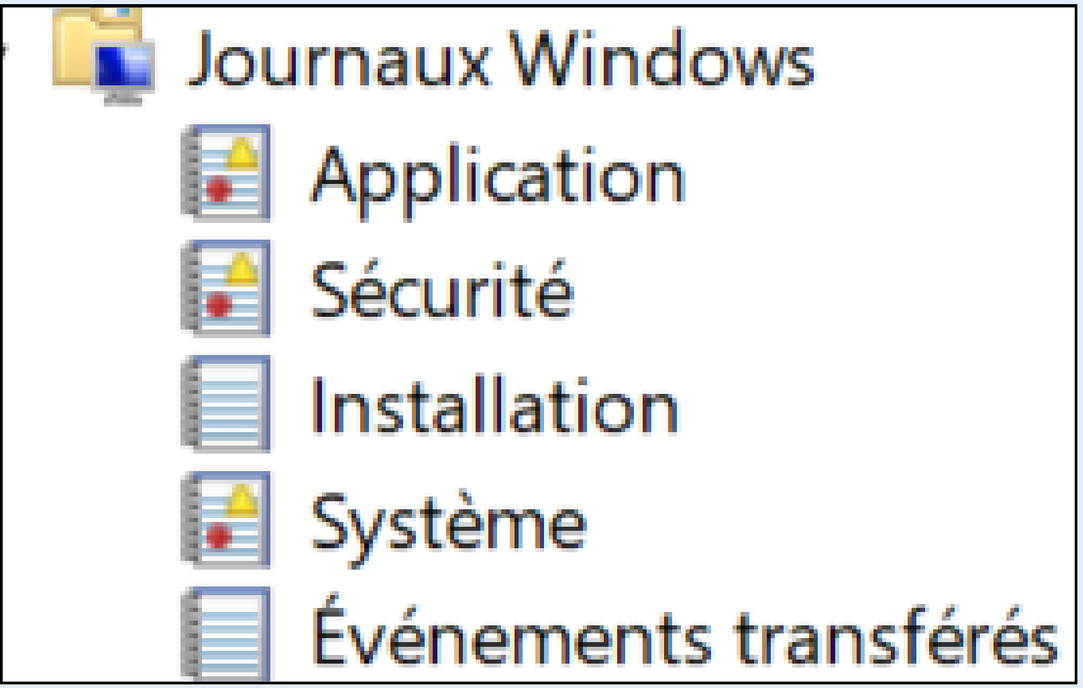
SYSTEM

Événements liés au système d’exploitation et à ses composants

SECURITY

Tentatives de connexion, changements de compte, accès non autorisé

Principaux types de journaux Windows



- **APPLICATION**
- **SYSTEM**
- **SECURITY**
- **SETUP**

Événements liés à l’installation du système ou des logiciels

- **FORWARDED EVENTS**

Journaux d’événements collectés depuis d’autres machines

Composants clés d’un événement log

```
Time          EntryType   Source                 InstanceID Message
----          ---------   ------                 ---------- -------
May 06 23:20  Information brave                           0 La description de l'ID d'événement '0' dans la
May 06 23:19  Information Software Protecti...   1073758208 La planification du redémarrage du service de
May 06 23:18  Information Software Protecti...   3221241866 La migration de bas niveau hors connexion a ré
May 06 23:15  Information Software Protecti...   1073758208 La planification du redémarrage du service de
May 06 23:14  Information Software Protecti...   3221241866 La migration de bas niveau hors connexion a ré
```

- **Horodatage (Timestamp)**
- **Message ou description**
- **Source**
- **Identifiant (Event ID)**
- **Type d’événement**

Type d'entrée (Niveau de l'événement) : Indique la gravité ou la nature de l'événement :

🟢 **Information :** Indique qu'une action ou un événement s'est terminé avec succès.
🟡 **Warning :** Signale un problème non critique qui pourrait entraîner des problèmes s'il n'est pas pris en compte.
🔴 **Error :** Indique qu'un problème est survenu, généralement dû à une opération échouée.
❗ **Critical :** Représente une défaillance grave au niveau du système ou de l'application, nécessitant une attention immédiate.

Audit de succès/échec :

✅ **Audit de succès :** Une action liée à la sécurité s'est déroulée comme prévu (par exemple, une connexion réussie).
❌ **Audit d'échec :** Une action liée à la sécurité a échoué (par exemple, une tentative de connexion non autorisée).

Exemples d'Event ID connus

ID	EVENTS	ID	EVENTS
4720	User Created	4104	execution of a remote PowerShell command
4726	User Account Deleted	4688	new process has been created
4741	User account was changed	2003	USB device connection to the computer
4624	User succefully loggedOn	1102	Security log cleared
4625	Unsuccefull log attempt		

L'IMPORTANCE DES LOGS

01 Détecter des violations de sécurité potentielles

02 Tracer les activités sur le système

03 Analyser les malwares et l'impact d'une attaque

04 Collecter des preuves en cas d'incident (forensic)

La collecte et la centralisation des logs

Collecte locale

Chaque machine Windows conserve ses journaux d'événements localement, accessibles via l'outil Event Viewer. Cela suffit pour un diagnostic ponctuel, mais devient inefficace à grande échelle.

Centralisation des logs

Les logs de plusieurs machines sont automatiquement transférés vers un serveur central, généralement connecté à une solution SIEM

solutions SIEM connues

SPLUNK

Elastic

Wazuh

INVESTIGATION FORENSIC

Collection » Preservation » Examination » Analysis » Reporting

INVESTIGATION FORENSIC

Collection » Preservation » Examination » Analysis » Reporting

↓

Créer des empreintes cryptographiques

Documenter également la chaîne de possession (Chain of Custody), indiquant qui a manipulé les logs à chaque étape

INVESTIGATION FORENSIC

Collection » Preservation » Examination » Analysis » Reporting

↓

Filtrer les logs à la recherche de comportements suspects,

INVESTIGATION FORENSIC

Collection » Preservation » Examination » Analysis » Reporting

la recherche d’élévations de privilèges, d’accès non autorisés, de suppression de log

INVESTIGATION FORENSIC

Collection » Preservation » Examination » Analysis » Reporting

Rédiger un rapport forensique qui inclut les événements clés retrouvés dans les logs, les actions menées par l'attaquant

Conclusion

Les fichiers logs constituent une source critique de preuve en forensic : ils peuvent contenir les empreintes laissées par les attaquants, permettre de reconstruire la chronologie d’une attaque, et identifier des menaces ou comportements suspects en temps réel.

Bien exploités, ils deviennent un levier essentiel pour renforcer la cybersécurité et appuyer juridiquement les investigations post-incident.

Ressources

- nohackme Academygestion-logs-audit-donnees
- graylog critical-windows-event-ids-to-monitor/
- Sufficiency of Windows Event Log as Evidence in Digital Forensics “Article”
- centralisation-des-logs it.connect
- windows-event-log-analyst-reference.pdf