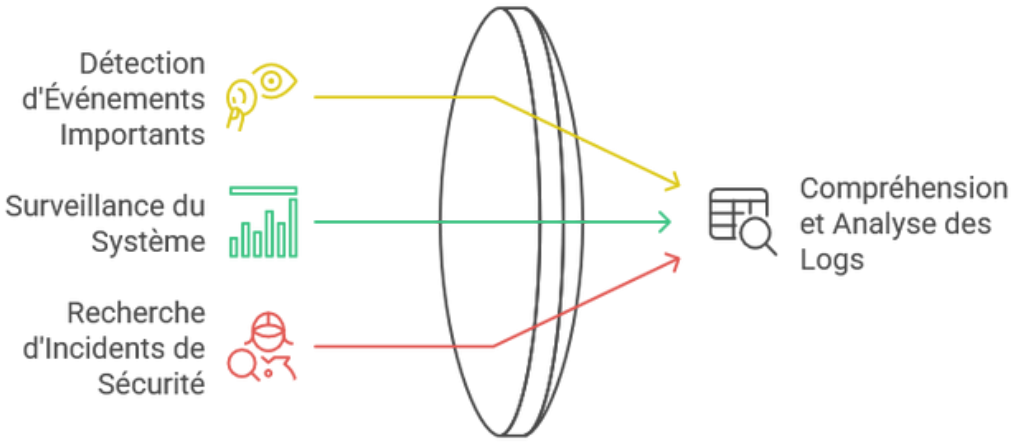
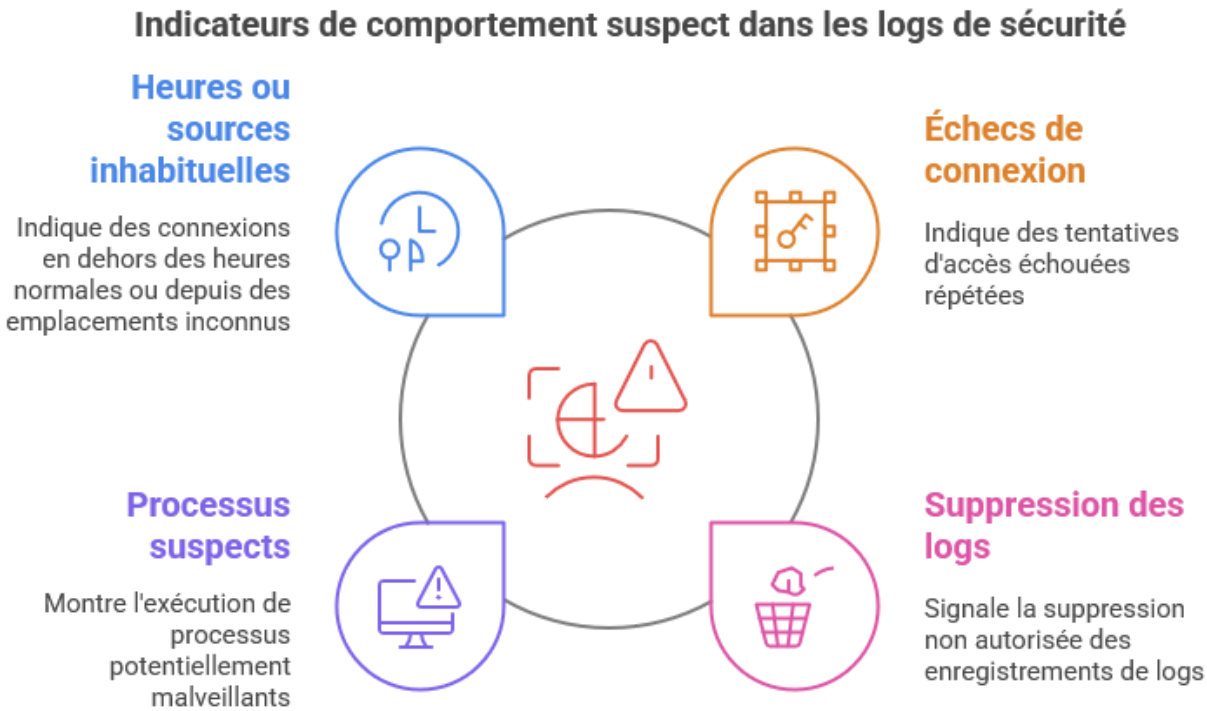
Inteprétation des logs avec GRAYLOG

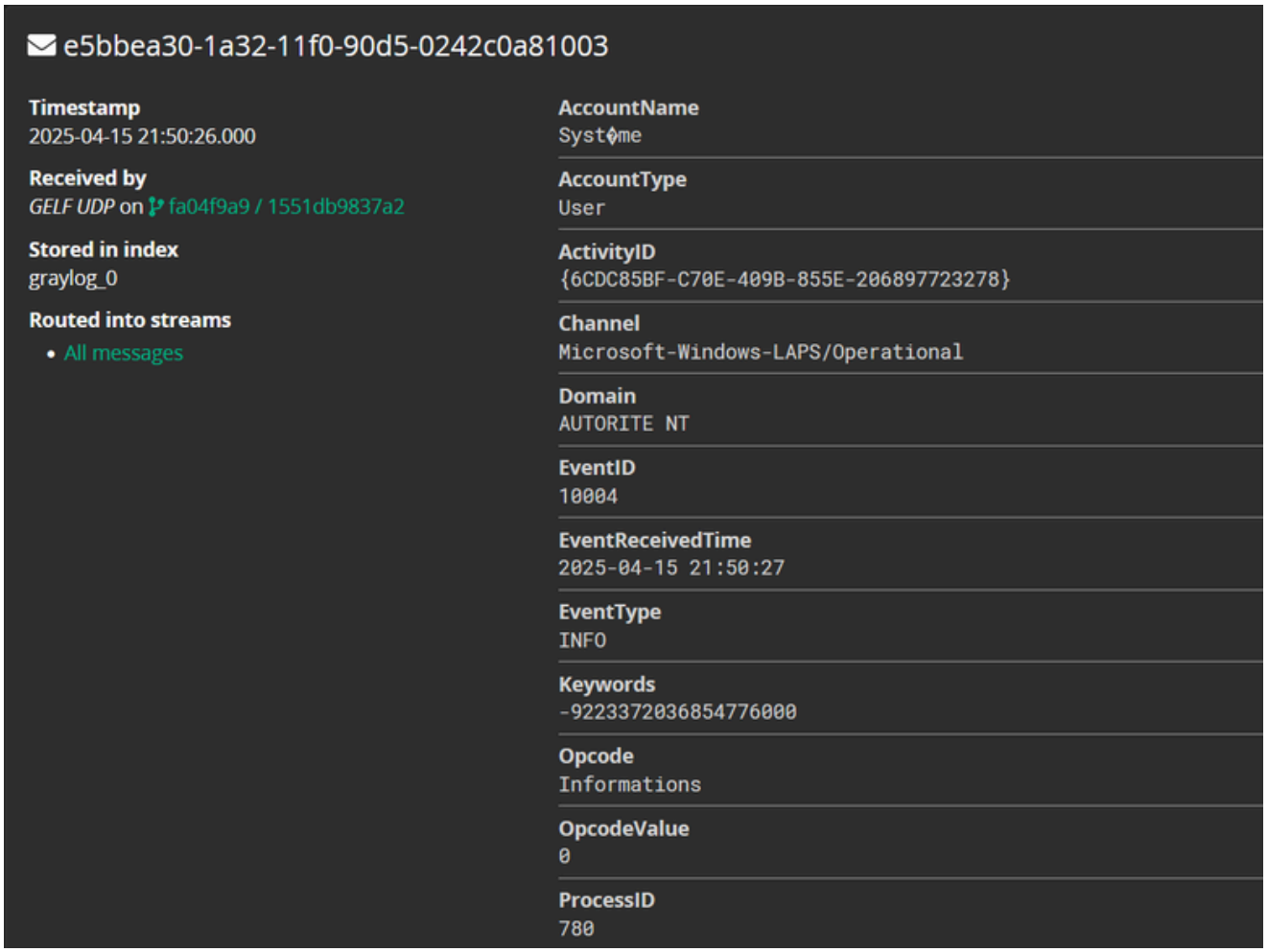
Ce document a pour but de comprendre les informations essentielles contenues dans un log Windows centralisé dans Graylog via NXLog. Cela permet d'analyser l'activité du système et de détecter d'éventuels **comportements suspects ou anormaux**.





Corps d’un journal d’évènement

Pour cet exemple, voici un log provenant d’une machine Windows, donc remontant avec nxlog et utilisant le protocole GELF UDP.



Ce log indique que le compte système a généré un événement informatif provenant du service LAPS. Rien n’indique ici une erreur ou une alerte de sécurité, ce type d’événement est généralement lié à une rotation de mot de passe locale ou à une opération de diagnostic.

Champ	Signification
timestamp	Date et heure exacte où l'événement s'est produit sur la machine source (≠ date de réception)
source	Nom de la machine d'origine (ex : PC-CLIENT, SRV-AD01). Très utile pour filtrer les logs par poste
EventID	Code numérique propre à chaque type d'événement Windows (ex : 4624 = connexion réussie, 1001 = erreur application, etc.)
AccountName	Nom du compte utilisateur ou système à l'origine de l'action
Channel	Journal Windows d'où vient l'événement
EventType	Type général de l'événement : INFO, WARNING, ERROR, AUDIT_SUCCESS, etc.
Severity / SeverityValue	Niveau de criticité (ex : 2 = INFO, 4 = WARNING, 1 = ERROR, 0 = EMERGENCY)
Message / full_message	Description en langage naturel de l'événement (souvent en français dans un environnement Windows FR). Permet une première lecture humaine du log.
ProcessName / ProcessID	Processus concerné par l'événement (souvent svchost.exe, explorer.exe, etc.). Utile pour identifier une action automatique ou manuelle.
Domain / SubjectDomainName	Domaine de l'utilisateur (souvent AUTORITE NT ou un nom de domaine Active Directory)
UserID / SubjectUserSid	SID (identifiant unique) du compte ayant généré l'événement. Utile pour les analyses sécurité fines
Opcode / OpcodeValue	Type d'opération effectuée (ex : "Connexion réussie", "Ouverture de session échouée")
LogonType / LogonGuid	(dans les logs de sécurité) précise le type de session (interactif, à distance, etc.)
SourceModuleName	Module NXLog qui a collecté le log (in_eventlog)
Stored in index	Index Elasticsearch où le log est stocké (utile si plusieurs index tournent)