

SAE 5.Cyber.03 - R5.Cyber.11

Supervision d'une Machine Windows

Flavien Marchand

Sommaire

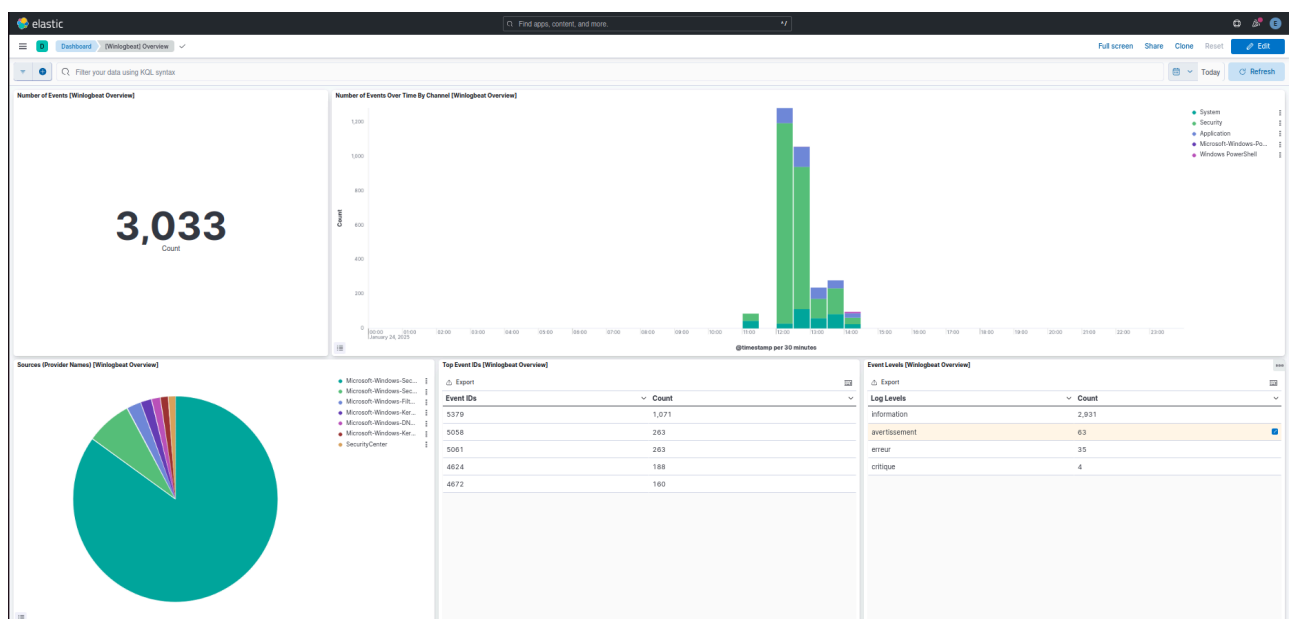
Sommaire	1
Winlogbeat	1
Les informations sur les connexions utilisateurs	1
Les erreurs de connexions et les comptes bloqués	1
Les événements de gestion des utilisateurs	1
Les événements de gestion des groupes	1

Winlogbeat

Grâce à Winlogbeat nous avons dans le Dashboard Elastic les différents dashboards.

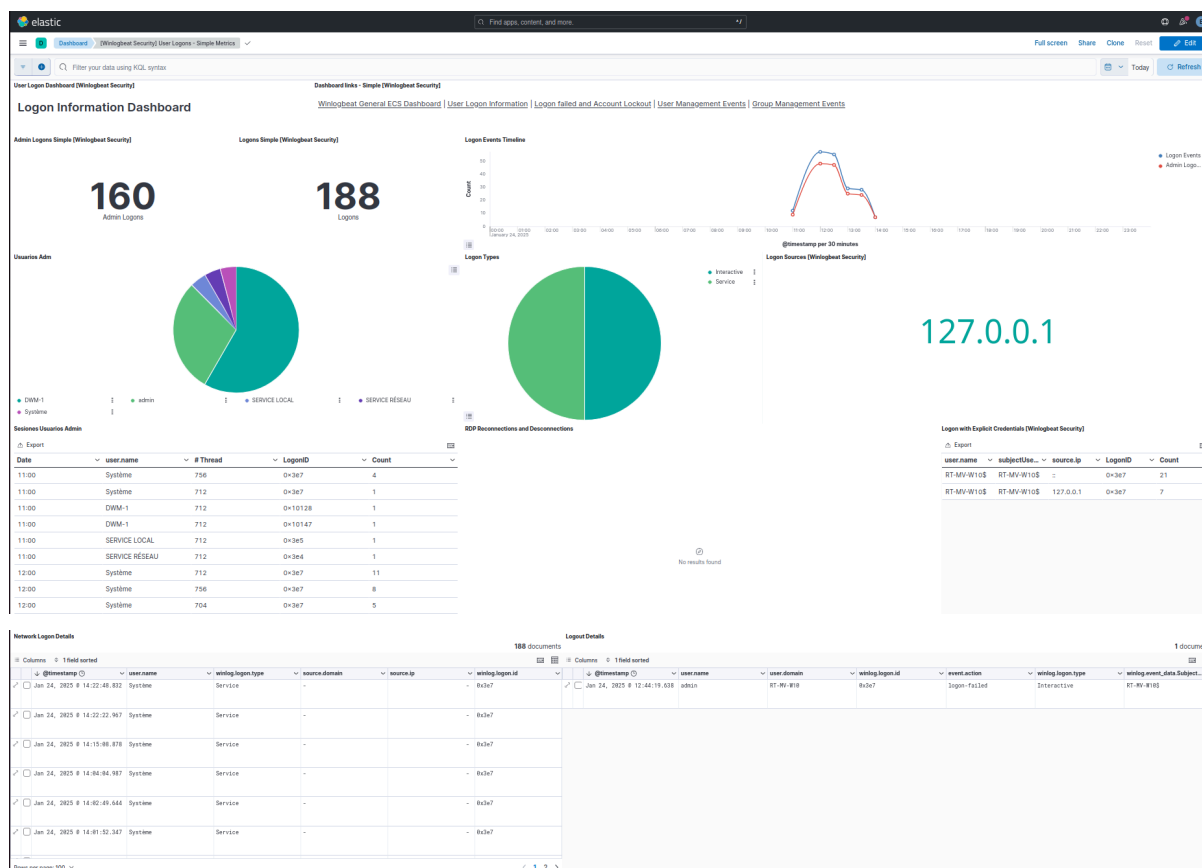
<input type="checkbox"/> [Winlogbeat Security] Failed and Blocked Accounts - Simple Metrics Failed and blocked accounts.	2 hours ago		
<input type="checkbox"/> [Winlogbeat Security] Failed and Blocked Accounts Failed and blocked accounts with TSVB metrics.	2 hours ago		
<input type="checkbox"/> [Winlogbeat powershell] Overview Overview dashboard por powershell module.	2 hours ago		
<input type="checkbox"/> [Winlogbeat Security] Group Management Events Group management activity.	2 hours ago		
<input type="checkbox"/> [Winlogbeat Security] User Logons User logon activity dashboard.	2 hours ago		
<input type="checkbox"/> [Winlogbeat] Overview Overview of all Windows Event Logs.	2 hours ago		
<input type="checkbox"/> [Winlogbeat Security] User Management Events - Simple Metric User management activity with TSVB metrics.	2 hours ago		
<input type="checkbox"/> [Winlogbeat Security] User Management Events User management activity.	2 hours ago		
<input type="checkbox"/> [Winlogbeat Security] User Logons - Simple Metrics User logon activity dashboard with TSVB metrics.	2 hours ago		
<input type="checkbox"/> [Winlogbeat Security] Group Management Events - Simple Metrics Group management activity with TSVB metrics.	2 hours ago		

Dans le dashboard Winlogbeat Overview, on y retrouve toutes les informations sur les évènements de la machine windows :



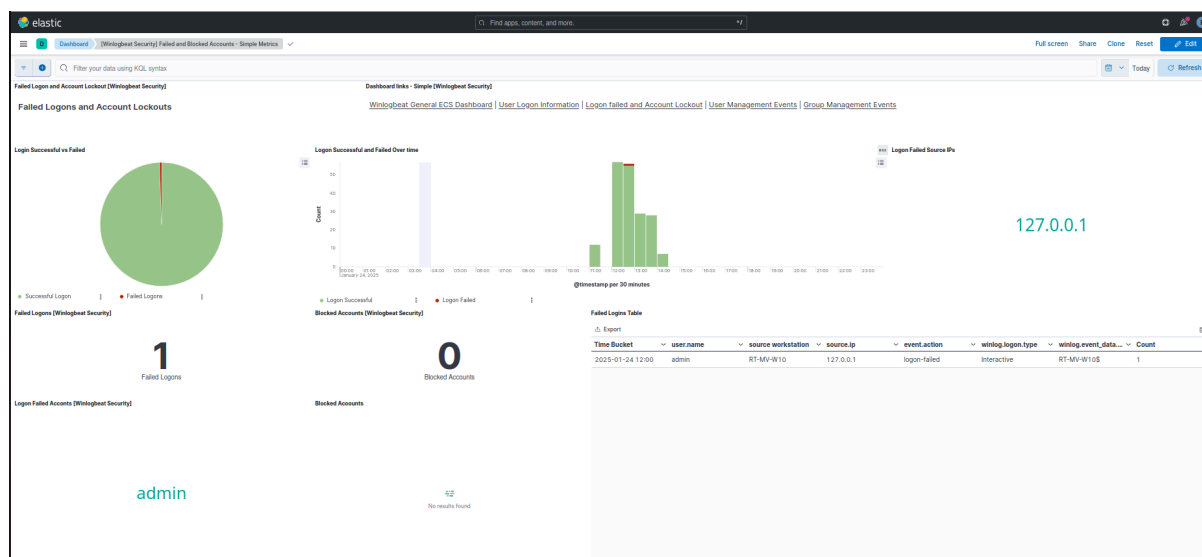
On y voit le nombre total d'événements sur une période donnée, le nombre d'événements par heures, la part des "Sources", des processus qui ont exécuté des événements, l'ID des événements et leur nombre d'occurrences, les niveaux des événements et leur nombre d'occurrences.

Les informations sur les connexions utilisateurs



Sur le User Logon Dashboard, on retrouve le nombre de connexions admins et utilisateurs, quels types de connexions ont été effectuées, l'ip source des connexions et des tableaux reportant chaque connexions et déconnexions.

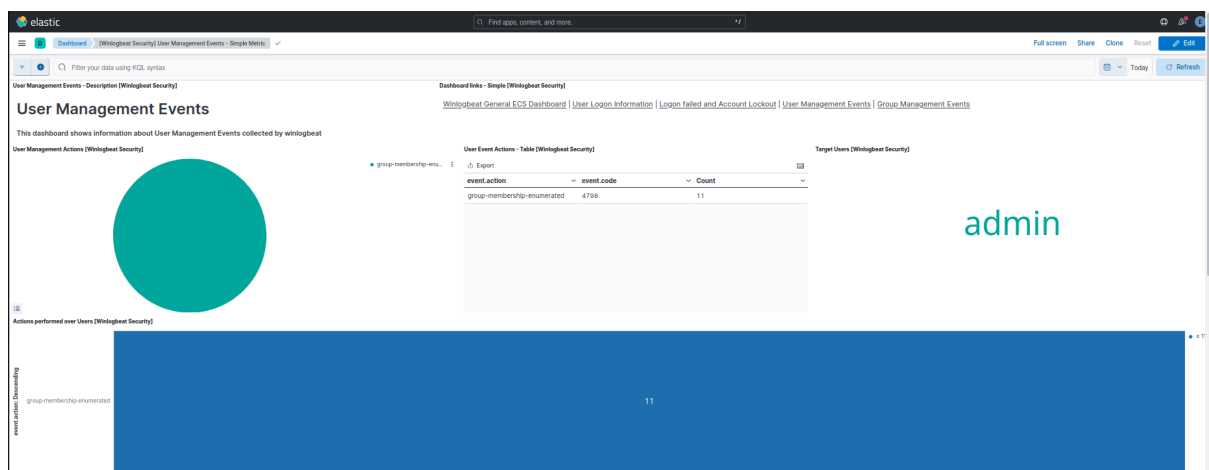
Les erreurs de connexions et les comptes bloqués





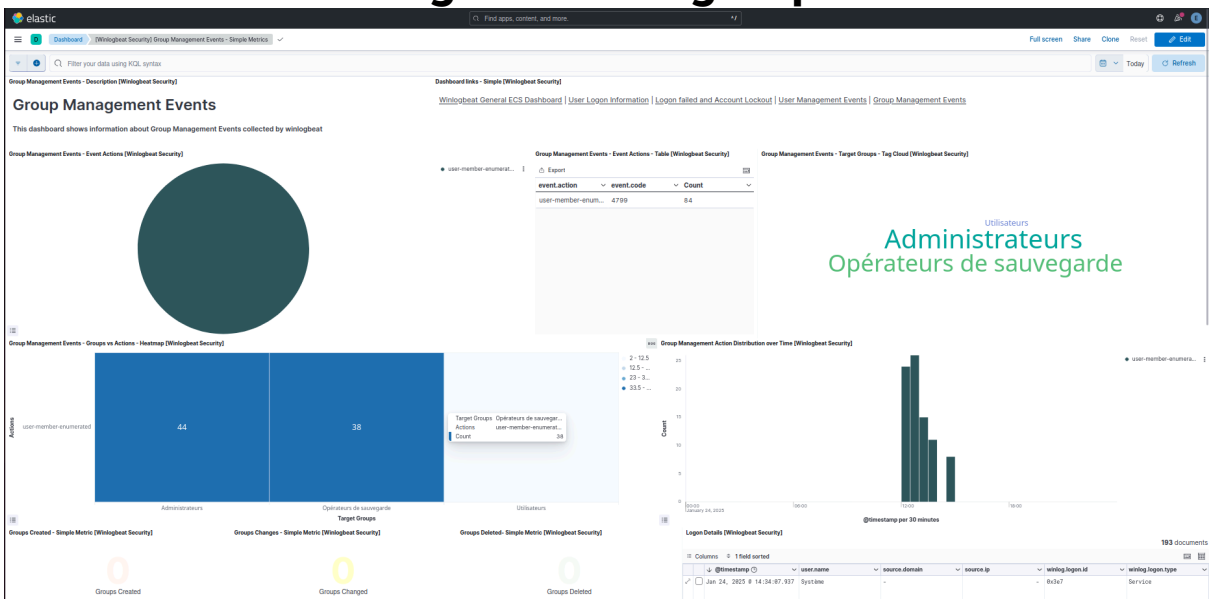
Le Logon failed and Account Lockout dashboard permet de voir les connexions réussies et échouées. Ainsi que les comptes bloqués.

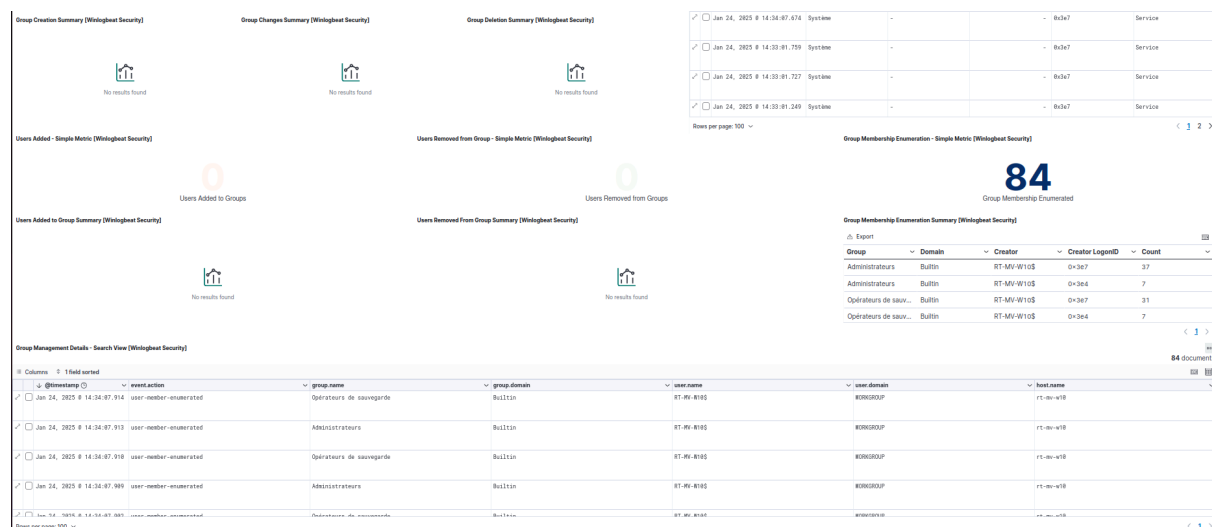
Les événements de gestion des utilisateurs



Sur le User Management Event dashboard on voit les types d'actions et les pseudos des utilisateurs ayant effectué des actions sur la machine Windows.

Les événements de gestion des groupes





Sur le Group Management Events dashboard on voit, les groupes et types d’actions qui ont été effectué par ces groupes sur la machine Windows.