

Détection de processus anormaux

A partir du logs des processus récoltés par *Sysmon*

Hackathon Sujet 3

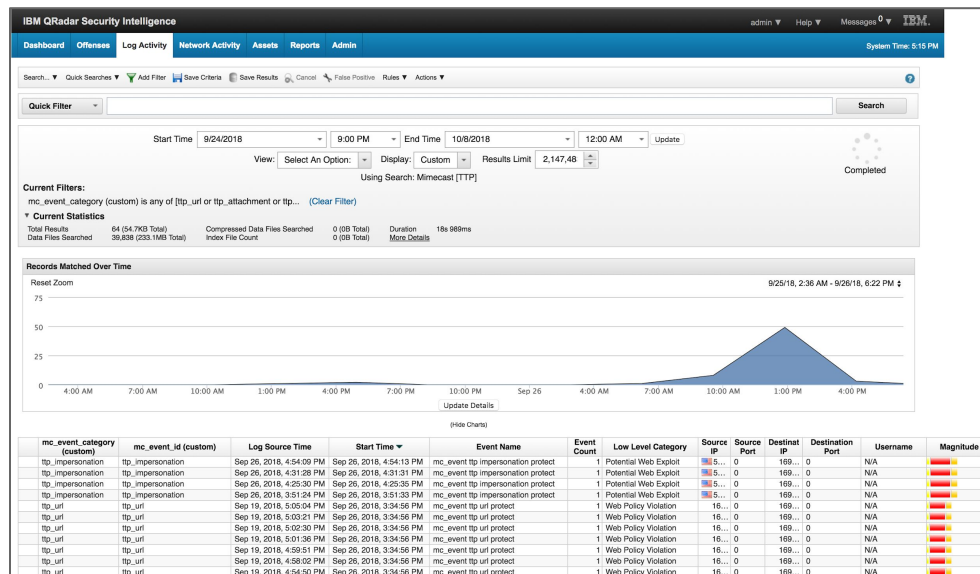
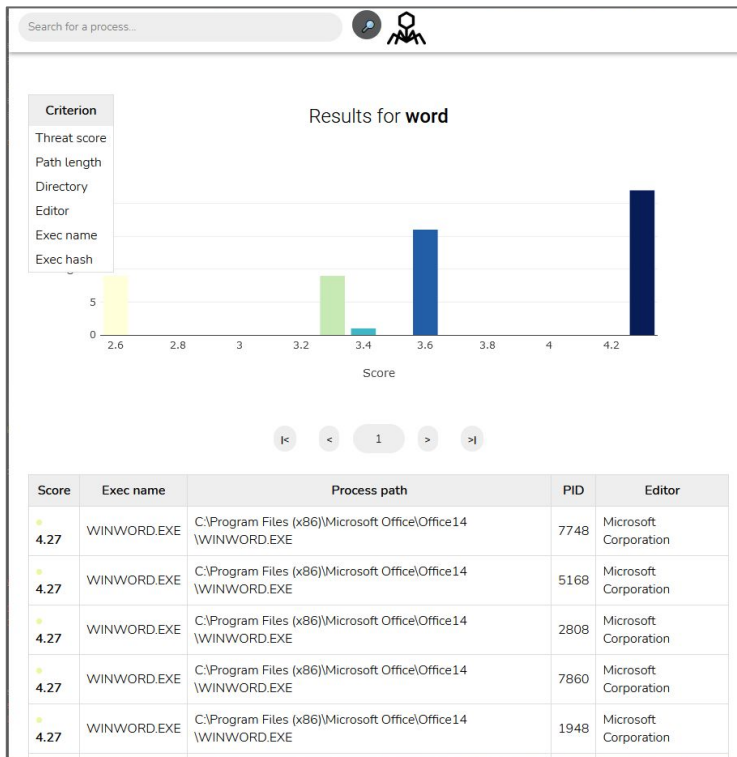
Fabien Bernier

Maxime Botreau

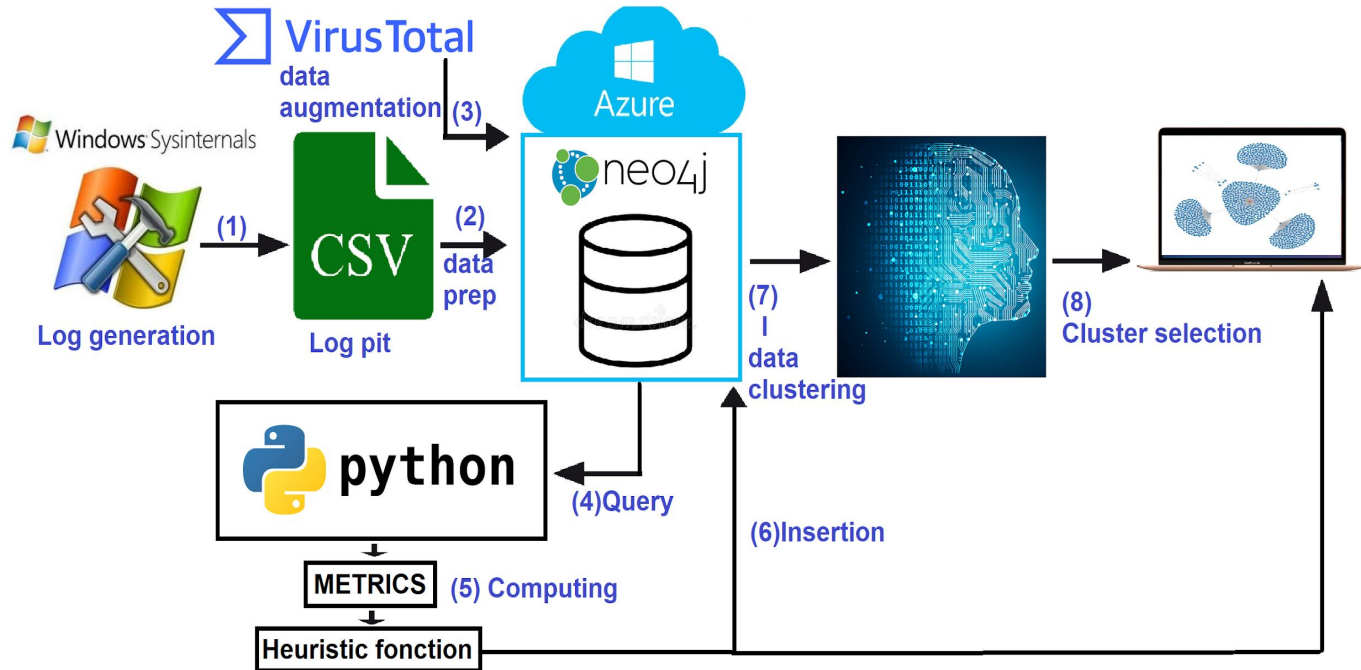
Alexander Lodolo

3A IAMD

Why?



What ?



Sommaire de la présentation

- I. Les données d'entrées
- II. La construction du graphe
- III. Les métriques et le score d'anomalie
- IV. Interface graphique et démonstration

Données d'entrées

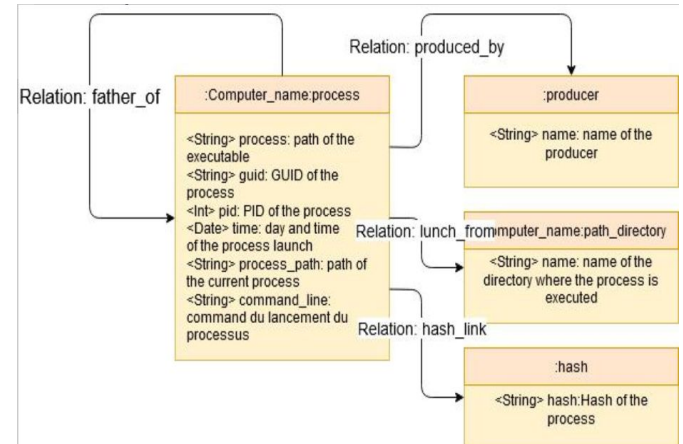
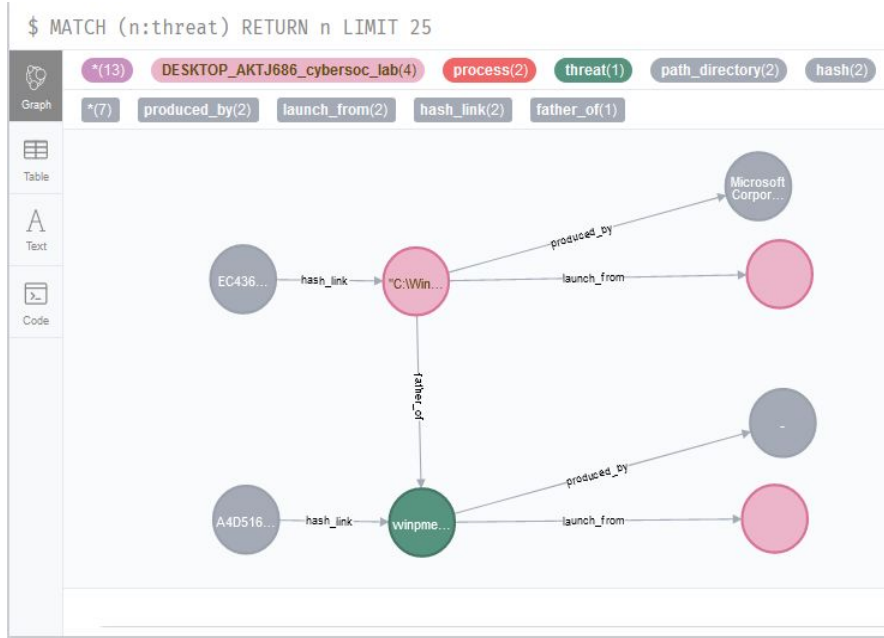
	process	process_company	process_current_directory	process_exec	process_guid	process_hash		process_id			
0	C:\Windows\system32\svchost.exe -k netsvc -p ...	Microsoft Corporation	C:\Windows\system32\	svchost.exe	{5350CD6C-B478-6017-3A62-030000002800}	B868487F8EDBD0571D30D89573F087BFEAC3DA19065234...		1812	xe" 0	DESKTOP-AKTJ686.cybersoc.lab	2021-02-01 08:51:48.000 CET
1	"C:\Windows\system32\SearchFilterHost.exe" 0 7...	Microsoft Corporation	C:\Windows\system32\	SearchFilterHost.exe	{5350CD6C-B314-6017-0F62-030000002800}	086E202398A409CB872C4D17424F81477A4CB37BCD2BBE...		7200	ost.exe"	DESKTOP-AKTJ686.cybersoc.lab	2021-02-01 08:51:48.000 CET
2	"C:\Windows\system32\SearchProtocolHost.exe" G...	Microsoft Corporation	C:\Windows\system32\	SearchProtocolHost.exe	{5350CD6C-B314-6017-0E62-030000002800}	4F8CF68ACDBE04F851763358C3A57A9634CD4F4966619D...		956	stsvcs -p	DESKTOP-AKTJ686.cybersoc.lab	2021-02-01 08:47:13.000 CET
3	C:\Windows\system32\svchost.exe -k netsvc -p ...	Microsoft Corporation	C:\Windows\system32\	svchost.exe	{5350CD6C-B201-6017-EA61-030000002800}	B868487F8EDBD0571D30D89573F087BFEAC3DA19065234...		5048	load	DESKTOP-AKTJ686.cybersoc.lab	2021-02-01 08:47:13.000 CET
4	C:\Windows\system32\wormgr.exe -upload				{5350CD6C-...	B868487F8EDBD0571D30D89573F087BFEAC3DA19065234...		3612			

process_path	parent_process	parent_process_exec	parent_process_guid	parent_process_id	parent_process_path
C:\Windows\System32\svchost.exe	C:\Windows\system32\services.exe	services.exe	{5350CD6C-C21D-5FFD-0A00-000000002800}	600	C:\Windows\System32\services.exe
C:\Windows\System32\SearchFilterHost.exe	C:\Windows\system32\SearchIndexer.exe /Embedding	SearchIndexer.exe	{5350CD6C-C2B7-5FFD-C600-000000002800}	6076	C:\Windows\System32\SearchIndexer.exe
C:\Windows\System32\SearchProtocolHost.exe	C:\Windows\system32\SearchIndexer.exe /Embedding	SearchIndexer.exe	{5350CD6C-C2B7-5FFD-C600-000000002800}	6076	C:\Windows\System32\SearchIndexer.exe
C:\Windows\System32\svchost.exe	C:\Windows\system32\services.exe	services.exe	{5350CD6C-C21D-5FFD-0A00-000000002800}	600	C:\Windows\System32\services.exe
C:\Windows\System32\wormgr.exe	C:\Windows\system32\svchost.exe	svchost.exe	{5350CD6C-...		



Pour le Whaou effect de la slide..

Construction du graphe



Description des métriques

Normalisée : division par la valeur maximale

- ***Path_length*** : Profondeur du dossier dans lequel s'exécute le processus dans l'arborescence des fichiers.
- ***Common_Directory*** : Nombre de processus s'exécutant dans le dossier en question
- ***Different_Directory*** : Nombre de dossiers différent dans lequel un exécutable est appelé
- ***Frequency*** : Nombre de fois où un exécutable est lancé dans la base de log
- ***Producer*** : Nombre de processus déclarant cet éditeur comme le leur
- ***Hash*** : Le score de ce hash trouvé sur VirusTotal : <https://www.virustotal.com/>

Non normalisée : prise en l'état

- ***Childs*** : Nombre de processus fils.

Métriques et score d'anomalie

```
score = 2 * hash_heuristic  
+ 2 * trust_factor  
+ directory_heuristic  
+ path_heuristic  
+ exec_heuristic  
+ child_heuristic  
+ common_dir_heuristic
```

Score
2.32

● 0.0

Hash frequency

● 1.0

Directory frequency

● 0.0

Path length

● 1.0

Name frequency

● 0.14

Number of children

● 0.0

Company trust

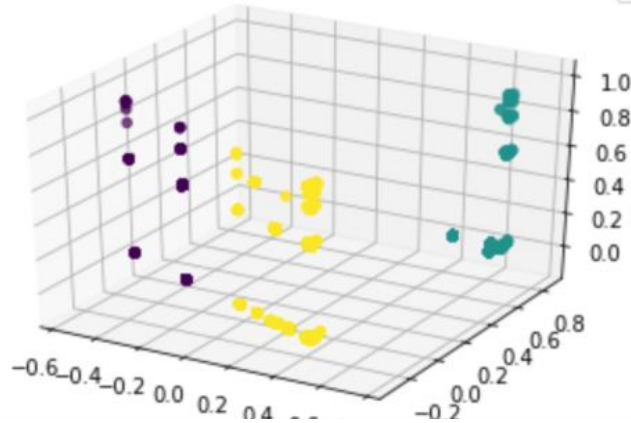
● 0.18

Number of directories
for this program

Mark as a threat

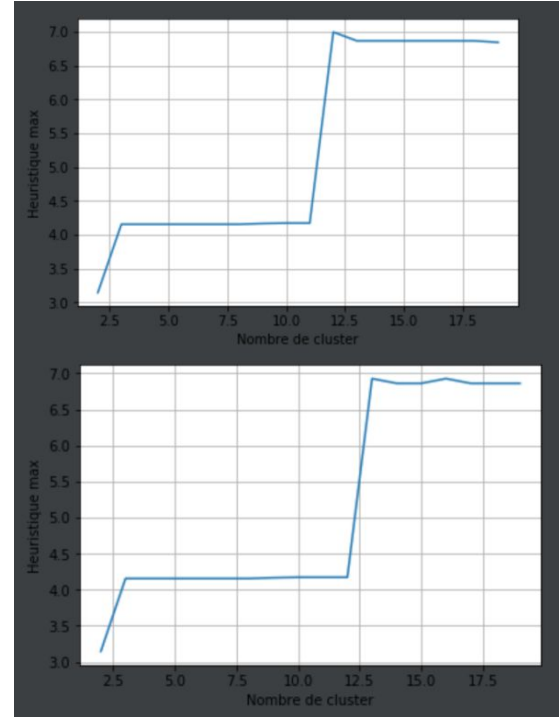
About

Clusterisation




Répartition des clusters des processus
(après une **ACP**)

Score moyen des clusters max



Nombre de clusters **Kmeans**

Interface graphique

Search for a process...			
<hr/>			
Process exec	svchost.exe		
Process	c:\windows\system32\svchost.exe -k netsvcs -p -s Schedule		
Process path	C:\Windows\System32\svchost.exe		
Command line	c:\windows\system32\svchost.exe -k netsvcs -p -s Schedule		
Host	DESKTOP_AKTJ686_cybersoc_lab		
Editor	Microsoft Corporation		
Hash	B868487F8EDBD0571D30D89573F087BFEAC3DA190652344AFD351B1868EA0F8B		
PID	1492		
GUID	{5350CD6C-4EE2-5FBD-2500-000000002700}		
Timestamp	2020-11-24 19:20:51.000 CET Tue. 24 November 2020 - 19:20 51s		
Score 1.18	<div><div>● 0.0 Hash frequency</div><div>● 0.0 Directory frequency</div><div>● 0.0 Name frequency</div><div>● 0.18 Number of directories for this program</div><div>● 1.0 Path length</div><div>● 0.0 Number of children</div><div>● 0.0 Company trust</div><div>Mark as a threat</div><div>About</div></div>		

