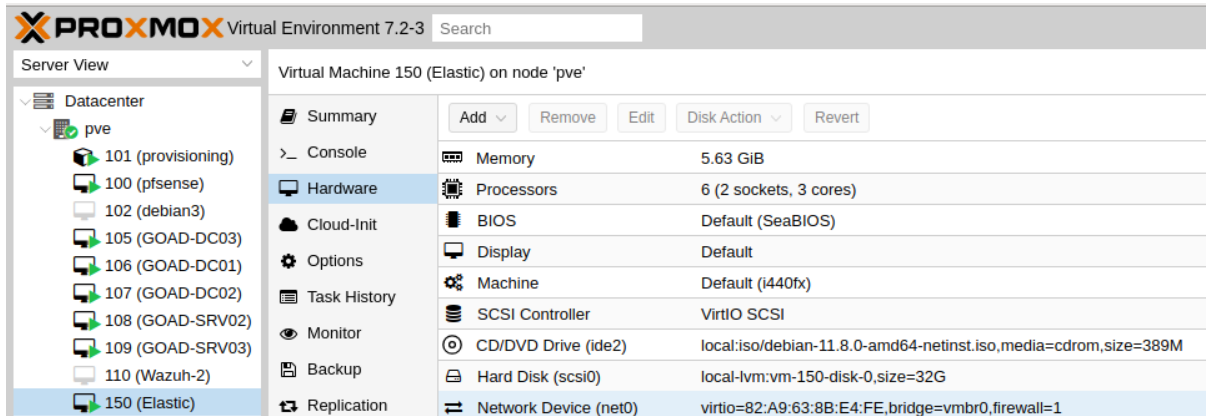


Installation de Elastic

- Créer une VM linux pour le serveur Elastic sur Proxmox



- On configure le serveur Elastic sur la VM
- On fait un : "git clone https://github.com/pushou/siem.git"
-> Afin d'installer "elastic SIEM" , l'IDS "Suricata", Evebox, et Zeek.
- On modifie le fichier suivant pour y ajouter une configuration : /etc/sysctl.conf
vm.max_map_count=262144
- On lance les commande :
make es
make siem
make fleet

Pour vérifier que tous ces bien déployer on peut faire un “docker ps” :

```
root@debian:/home/debian/siem# docker ps
```

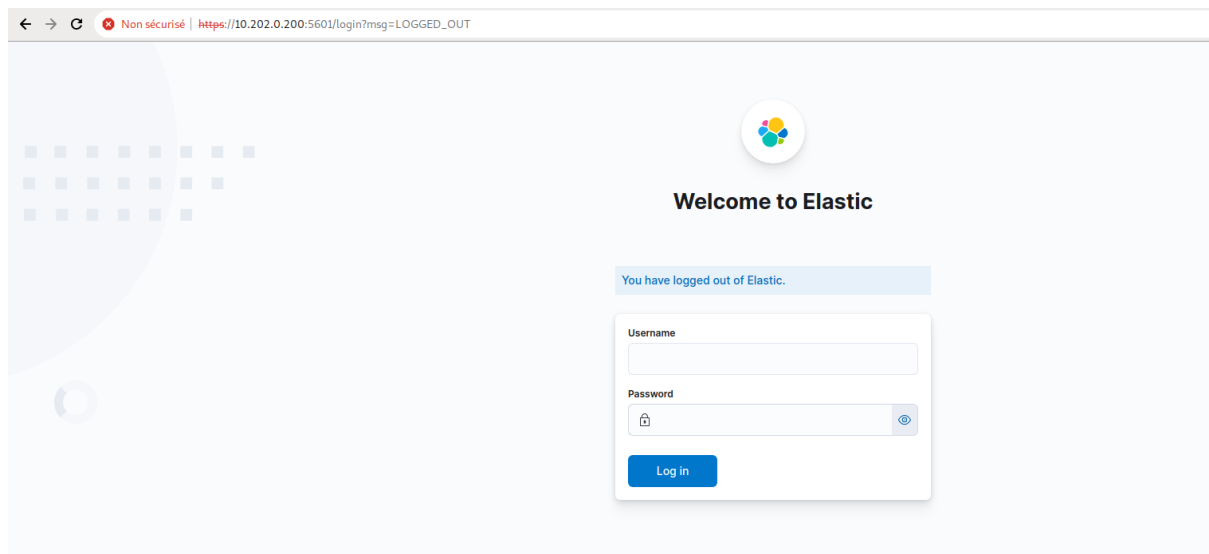
CONTAINER ID	IMAGE	NAMES	COMMAND	CREATED	STATUS	PORTS
c2e6bc6b2fb3	docker.elastic.co/beats/elastic-agent:8.9.0	fleet	"/usr/bin/tini -- /u..."	21 minutes ago	Up 21 minutes	10.202.0.200:8220->8220/tcp
bdaded7b3f2c	registry.iutbeziers.fr/bro:4.2.0	zeek	"/bin/bash -c 'while..."	23 minutes ago	Up 23 minutes	
4c8a7e1dc570	docker.elastic.co/beats/filebeat:8.9.0	filebeat	"/usr/bin/tini -- /u..."	23 minutes ago	Up 23 minutes	
18f3cae86bb8	docker.elastic.co/kibana/kibana:8.9.0	kibana	"/bin/tini -- /usr/l..."	24 minutes ago	Up 24 minutes	10.202.0.200:5601->5601/tcp
317ae857c875	docker.elastic.co/elasticsearch/elasticsearch:8.9.0	es01	"/bin/tini -- /usr/l..."	25 minutes ago	Up 25 minutes	127.0.0.1:9200->9200/tcp, 10.202.0.200:9200->9200/tcp, 127.0.0.1:9300->9300/tcp

```
root@debian:/home/debian/siem#
```

On voit bien que tous nos services sont bien déployés.

Etape 3 : Connexion à l'interface graphique

- On tape l'IP : https://10.202.0.200:5601/



- Pour s'y connecter on a le username = elastic
- Et pour savoir le mot de passe on fait la commande "make pass"

```
debian@debian:~/siem$ make pass
/home/debian/siem/scripts/print_password.sh
password elastic= 0*om2n82l4l-Q3I5wm9J
password kibana= dgRwou45hEZb9L29tVBM
password beats_system= xEqQCdedwvc=nqbPA7cX
password apm_system= xEqQCdedwvc=nqbPA7cX
password remote_monitoring_user= _WNxwuBANP+uw7_akJV7
debian@debian:~/siem$
```

Etape 4 : Configuration du fleet serveur

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Data streams](#) [Settings](#)

Fleet server hosts

Specify the URLs that your agents will use to connect to a Fleet Server. If multiple URLs exist, Fleet will show the first provided URL for enrollment purposes. For more information, see the [Fleet and Elastic Agent Guide](#).

Name	Host URLs	Default	Actions
fleet1	https://10.202.0.200:8220	✓	

[+](#) Add Fleet Server

Outputs

Specify where agents will send data.

Name	Type	Hosts	Default	Actions
default	Elasticsearch	https://10.202.0.200:9200	Agent integrations Agent monitoring	

[+](#) Add output

- Ajouter le CA et le SSL :

Edit output

TypeElasticsearch⌵

This output type currently does not support connectivity to a remote Elasticsearch cluster.

Hostshttps://10.202.0.200:9200+ Add another URL

Elasticsearch CA trusted fingerprint (optional)0801880D6C34D2A1F2303BD77A50669458986FBCA7B4DB93047FF2B7B0477ADA

ProxySelect proxy⌵

Advanced YAML configuration

```
ssl:  
  certificate_authorities:  
    - |  
      -----BEGIN CERTIFICATE-----  
      MIIDSTCCAjGgAwIBAgIUQTaSKJSYUND46oTYrY8rXN5AMWYWdQVJKoZIhvcNAQEL  
      BDAwMDEyMDAxMTUeAAwwBgkqhkiG9w0BBQSwIAQABRzAdBgNVHQ4EFgg=
```

☒

Make this output the default for agent integrations.

☒

Make this output the default for agent monitoring.

- Préparation des agents Windows avec le serveur fleet pour les ajouter. On crée une policy avec des intégrations.

Fleet

Centralized management for Elastic Agents.

[Agents](#)
[Agent policies](#)
[Enrollment tokens](#)
[Data streams](#)
[Settings](#)

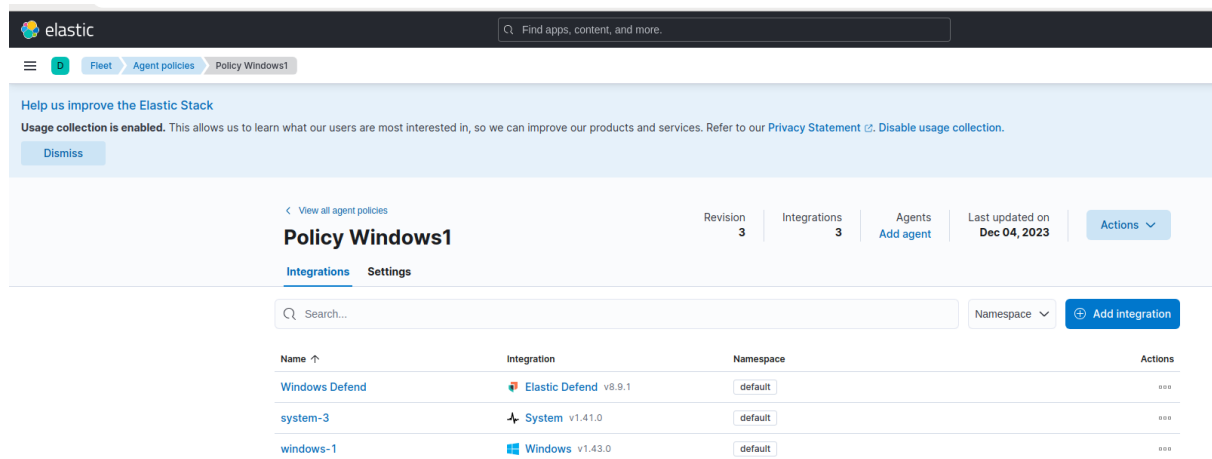
Reload
Create agent policy

Name	Description	Last update...	Agents	Integrations	Actions
Policy Windows <small>rev. 4</small>		Dec 07, 2023	5	3	...
Fleet Server Policy <small>rev. 1</small>	Fleet Server policy generated by Kibana	Dec 07, 2023	0	2	...
Fleet Server policy jmp <small>rev. 3</small>		Dec 07, 2023	1	2	...

Rows per page: 20

1

- On va ajouter des integrations : Windows et Elastic Defend



elastic Find apps, content, and more.

Fleet Agent policies Policy Windows1

Help us improve the Elastic Stack
Usage collection is enabled. This allows us to learn what our users are most interested in, so we can improve our products and services. Refer to our [Privacy Statement](#). [Disable usage collection](#).

Dismiss

< View all agent policies

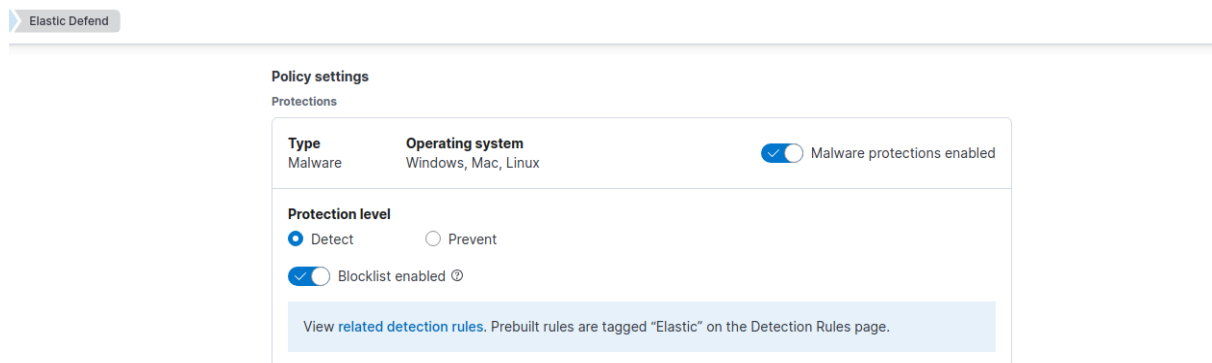
Policy Windows1 Revision 3 Integrations 3 Agents Add agent Last updated on Dec 04, 2023 Actions

Integrations Settings

Search... Namespace Add integration

Name	Integration	Namespace	Actions
Windows Defend	Elastic Defend v8.9.1	default	...
system-3	System v1.41.0	default	...
windows-1	Windows v1.43.0	default	...

- A savoir que pour l'intégration de Elastic Defend il y a quelques modifications a faire. On doit mettre Elastic Defend en mode "Detect"



Elastic Defend

Policy settings

Protections

Type	Operating system	
Malware	Windows, Mac, Linux	<input checked="" type="checkbox"/> Malware protections enabled

Protection level

☒ Detect ☐ Prevent

☒ Blocklist enabled ⓘ

View [related detection rules](#). Prebuilt rules are tagged "Elastic" on the Detection Rules page.

- On ajoute aussi "False" dans la vérification des hostnames :



windows.advanced.elasticsearch.tls.verify_hostname ⓘ 7.9+

false

windows.advanced.elasticsearch.tls.ca_cert ⓘ 7.9+

- On ajoute un premier agent à l'aide des commandes de elastic, avec le packets et le token :

Add agent

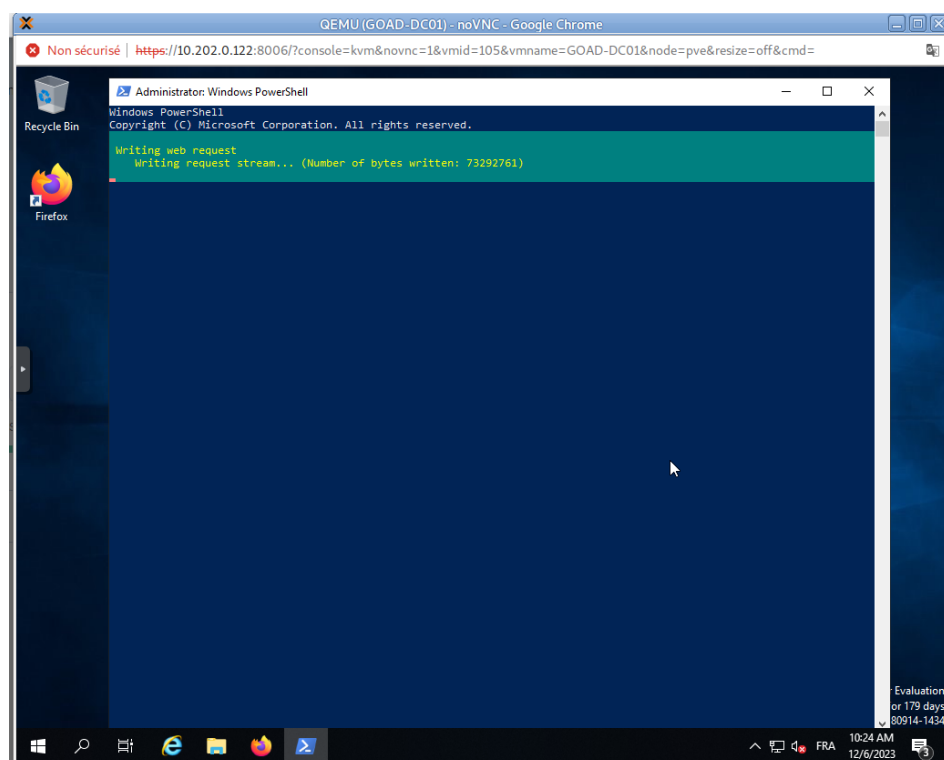
Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

our [installation docs](#).

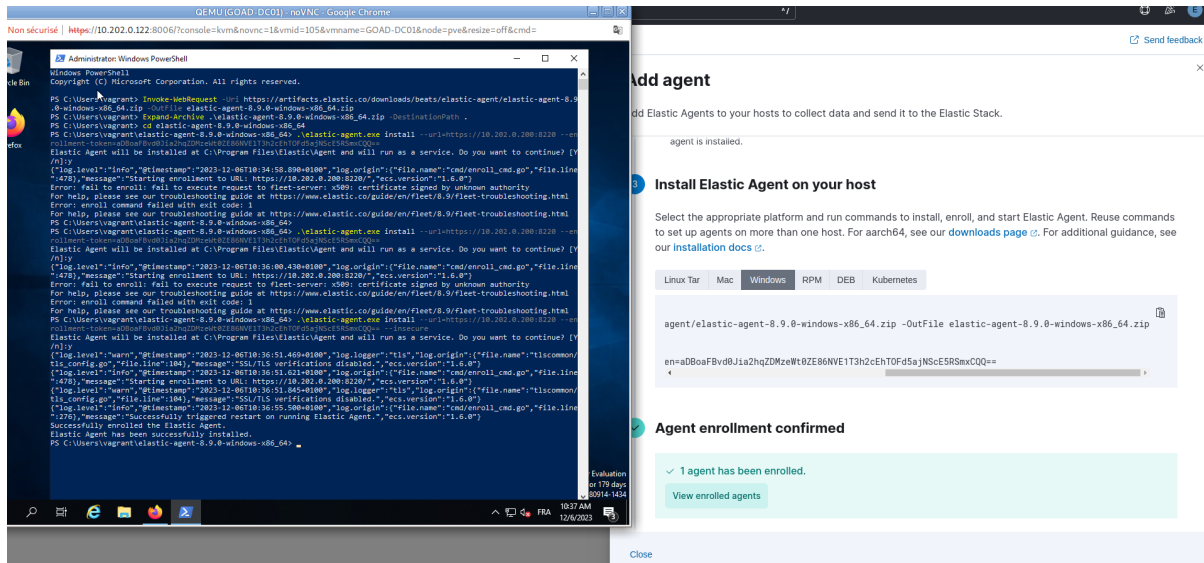
Linux Tar Mac **Windows** RPM DEB Kubernetes

```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-ag  
Expand-Archive .\elastic-agent-8.9.0-windows-x86_64.zip -DestinationPath .  
cd elastic-agent-8.9.0-windows-x86_64  
.\elastic-agent.exe install --url=https://10.202.0.200:8220 --enrollment-token=0DB5eFNZd0JqT
```

- Un fois que l'on accède à la VM, on exécute les commandes :



- Résultat l'agent et bien ajouté



- On obtient cela et on refait le même chose pour les autres agents

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Data streams](#) [Settings](#)

Ingest Overview Metrics Agent Info Metrics

Agent activity Add Fleet Server Add agent

Filter your data using KQL syntax

Status 4 Tags 0 Agent policy 3 Upgrade available

Showing 2 agents Clear filters

Healthy 2 Unhealthy 0 Updating 0 Offline 0

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	kingslanding	Policy Windows1 rev. 7	N/A	N/A	10 seconds ago	8.9.0	...
Healthy	9adc75565abc	Fleet Server policy jmp rev. 3	N/A	N/A	10 seconds ago	8.9.0	...

Rows per page: 20

- Après l'ajout de tous les agents :

elastic

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Data streams](#) [Settings](#)

Ingest Overview Metrics Agent Info Metrics

Agent activity Add Fleet Server Add agent

Filter your data using KQL syntax

Status 4 Tags 0 Agent policy 3 Upgrade available

Showing 6 agents Clear filters

Healthy 6 Unhealthy 0 Updating 0 Offline 0

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	kingslanding	Policy Windows rev. 4	N/A	118 MB	27 seconds ago	8.9.0	...
Healthy	braavos	Policy Windows rev. 4	0.97 %	321 MB	28 seconds ago	8.9.0	...
Healthy	castelblack	Policy Windows rev. 4	369.36 %	208 MB	28 seconds ago	8.9.0	...
Healthy	meereen	Policy Windows rev. 4	0.88 %	243 MB	29 seconds ago	8.9.0	...
Healthy	winterfell	Policy Windows rev. 4	1.40 %	245 MB	33 seconds ago	8.9.0	...
Healthy	fb0767c524ba	Fleet Server policy jmp rev. 3	0.43 %	172 MB	19 seconds ago	8.9.0	...

Rows per page: 20

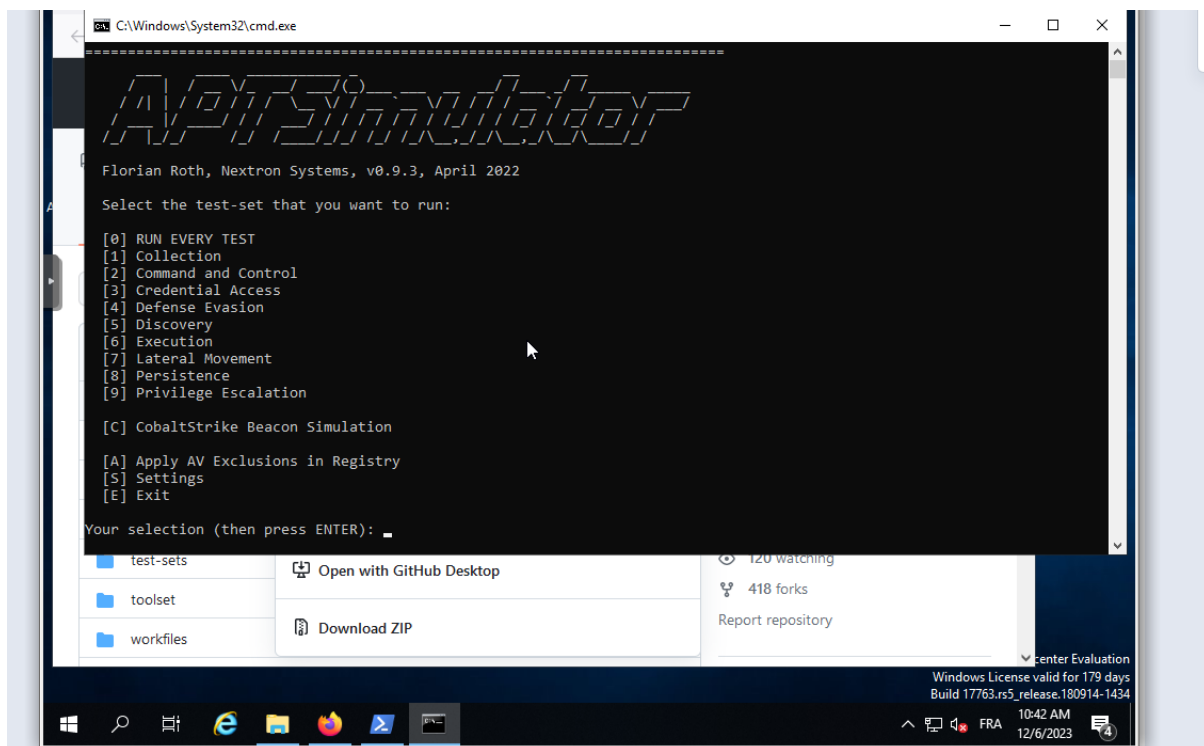
- Pour lancer des alertes on utilise APT Simulator. Avant cela on doit désactiver le Windows Defend avec cette commande pour pouvoir exécuter APT Simulator:

```
get-AppxPackage Microsoft.SecHealthUI -AllUsers | Reset-AppxPackage
```

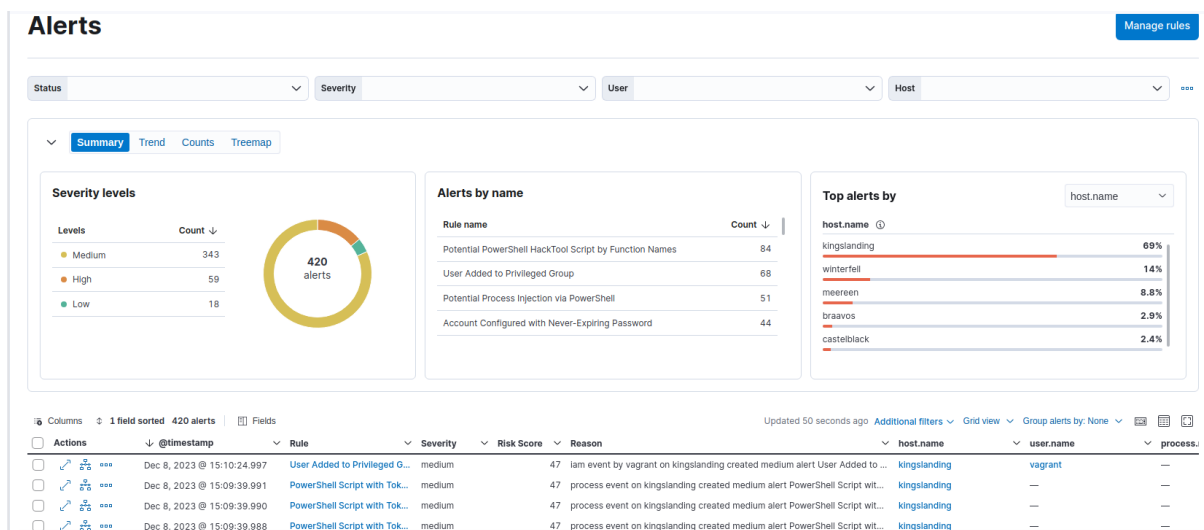
```
Add-AppxPackage -Register -DisableDevelopmentMode
```

```
"C:\Windows\SystemApps\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy\AppData\Local\Microsoft\Windows\SecHealthUI\cw5n1h2txyewy\AppXManifest.xml"
```

- Comme le Pare-feu est déjà désactiver avec le script Ansible, maintenant le Windows Defend est désactivé on peut exécuter les alertes :



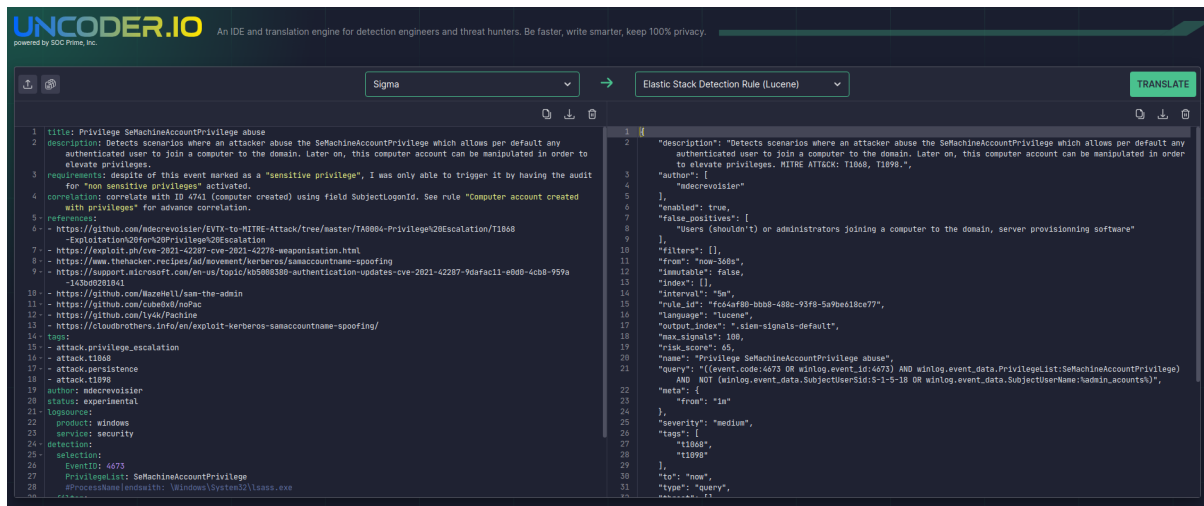
- On peut observer les alertes dans Elastic :



- On va ajouter des Sigma, pour cela j'utilise plusieurs règles Sigma du dépôt github suivant :

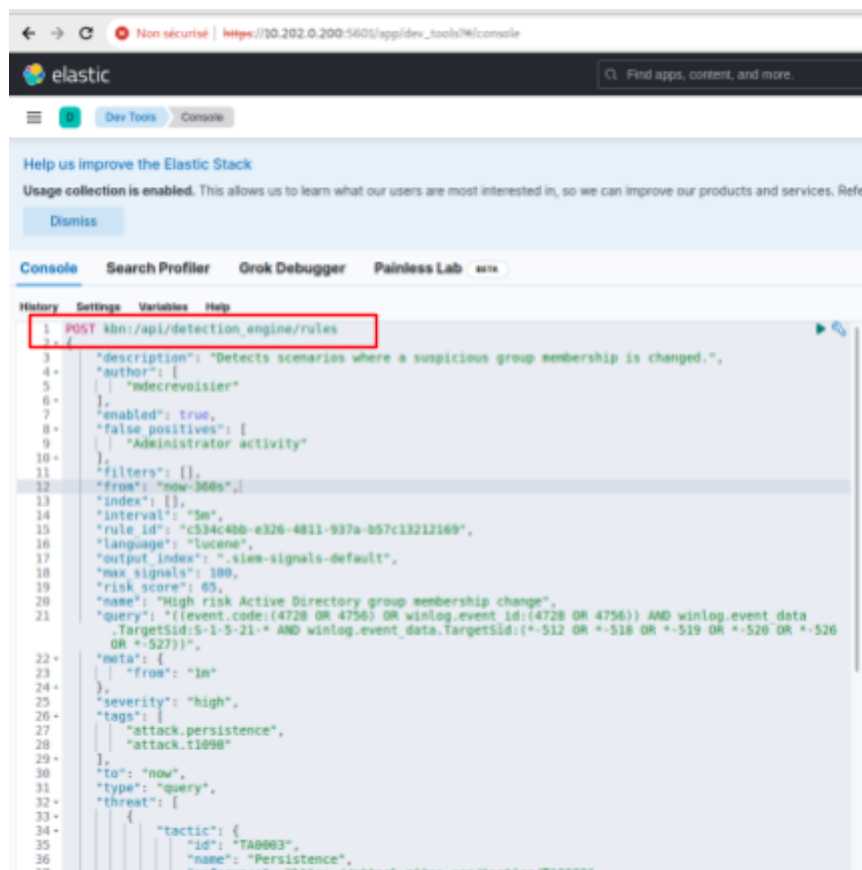
https://github.com/mdecrevoisier/SIGMA-detection-rules/tree/main/windows-active_directory

On choisit une règle et on la traduit de SIGMA vers Elastic Rules avec ce site :



- Ensuite on va dans Elastic dans DevTool et on applique les règle sigma comme ici par exemple :

On ajoute le ligne de "POST", et on retire la ligne "immutable": false," :



Le résultat, cette règles Sigma ci dessous par exemple détecte quand un changement de groupe d'un membre est suspect :

```

1 POST kbn:/api/detection_engine/rules
2 {
3   "description": "Detects scenarios where a suspicious group membership is changed.",
4   "author": [
5     "mdcrevoisier"
6   ],
7   "enabled": true,
8   "false_positives": [
9     "Administrator activity"
10  ],
11  "filters": {},
12  "from": "now-360s",
13  "index": [],
14  "interval": "5m",
15  "rule_id": "c534c4bb-e326-4811-937a-b57c13212169",
16  "language": "lucene",
17  "output_index": ".siem-signals-default",
18  "max_signals": 100,
19  "risk_score": 65,
20  "name": "High risk Active Directory group membership change",
21  "query": "((event.code:(4728 OR 4756) OR winlog.event.id:(4728 OR 4756)) AND winlog.event.data.TargetSid:S-1-5-21-* AND winlog.event.data.TargetSid:(*512 OR *518 OR *519 OR *520 OR *526 OR *527))",
22  "meta": {
23    "from": "1m"
24  },
25  "severity": "high",
26  "tags": [
27    "attack.persistence",
28    "attack.t1098"
29  ],
30  "to": "now",
31  "type": "query",
32  "threat": [
33    {
34      "tactic": {
35        "id": "TA0003",
36        "name": "Persistence",
37      },
38      "framework": "MITRE ATT&CK",
39      "technique": [
40        {
41          "id": "T1098",
42          "name": "Account Manipulation",
43        }
44      ]
45    }
46  ],
47  "tactic": {
48    "id": "TA0003",
49    "name": "Persistence",
50    "reference": "https://attack.mitre.org/tactics/TA0003"
51  },
52  "framework": "MITRE ATT&CK",
53  "technique": [
54    {
55      "id": "T1098",
56      "name": "Account Manipulation",
57    }
58  ],
59  "threat": [
60    {
61      "tactic": {
62        "id": "TA0003",
63        "name": "Persistence",
64      },
65      "framework": "MITRE ATT&CK",
66      "technique": [
67        {
68          "id": "T1098",
69          "name": "Account Manipulation",
70        }
71      ]
72    }
73  ],
74  "tags": [
75    "attack.persistence",
76    "attack.t1098"
77  ],
78  "to": "now",
79  "type": "query",
80  "threat": [
81    {
82      "tactic": {
83        "id": "TA0003",
84        "name": "Persistence",
85      },
86      "framework": "MITRE ATT&CK",
87      "technique": [
88        {
89          "id": "T1098",
90          "name": "Account Manipulation",
91        }
92      ]
93    }
94  ],
95  "tactic": {
96    "id": "TA0003",
97    "name": "Persistence",
98    "reference": "https://attack.mitre.org/tactics/TA0003"
99  },
100 "framework": "MITRE ATT&CK",
101 "technique": [
102   {
103     "id": "T1098",
104     "name": "Account Manipulation",
105   }
106 ],
107 "threat": [
108   {
109     "tactic": {
110       "id": "TA0003",
111       "name": "Persistence",
112     },
113     "framework": "MITRE ATT&CK",
114     "technique": [
115       {
116         "id": "T1098",
117         "name": "Account Manipulation",
118       }
119     ]
120   }
121 ],
122 "tags": [
123   "attack.persistence",
124   "attack.t1098"
125 ],
126 "to": "now",
127 "type": "query",
128 "threat": [
129   {
130     "tactic": {
131       "id": "TA0003",
132       "name": "Persistence",
133     },
134     "framework": "MITRE ATT&CK",
135     "technique": [
136       {
137         "id": "T1098",
138         "name": "Account Manipulation",
139       }
140     ]
141   }
142 ],
143 "tactic": {
144   "id": "TA0003",
145   "name": "Persistence",
146   "reference": "https://attack.mitre.org/tactics/TA0003"
147 },
148 "framework": "MITRE ATT&CK",
149 "technique": [
150   {
151     "id": "T1098",
152     "name": "Account Manipulation",
153   }
154 ],
155 "threat": [
156   {
157     "tactic": {
158       "id": "TA0003",
159       "name": "Persistence",
160     },
161     "framework": "MITRE ATT&CK",
162     "technique": [
163       {
164         "id": "T1098",
165         "name": "Account Manipulation",
166       }
167     ]
168   }
169 ],
170 "tags": [
171   "attack.persistence",
172   "attack.t1098"
173 ],
174 "to": "now",
175 "type": "query",
176 "threat": [
177   {
178     "tactic": {
179       "id": "TA0003",
180       "name": "Persistence",
181     },
182     "framework": "MITRE ATT&CK",
183     "technique": [
184       {
185         "id": "T1098",
186         "name": "Account Manipulation",
187       }
188     ]
189   }
190 ],
191 "tactic": {
192   "id": "TA0003",
193   "name": "Persistence",
194   "reference": "https://attack.mitre.org/tactics/TA0003"
195 },
196 "framework": "MITRE ATT&CK",
197 "technique": [
198   {
199     "id": "T1098",
200     "name": "Account Manipulation",
201   }
202 ],
203 "threat": [
204   {
205     "tactic": {
206       "id": "TA0003",
207       "name": "Persistence",
208     },
209     "framework": "MITRE ATT&CK",
210     "technique": [
211       {
212         "id": "T1098",
213         "name": "Account Manipulation",
214       }
215     ]
216   }
217 ],
218 "tags": [
219   "attack.persistence",
220   "attack.t1098"
221 ],
222 "to": "now",
223 "type": "query",
224 "threat": [
225   {
226     "tactic": {
227       "id": "TA0003",
228       "name": "Persistence",
229     },
230     "framework": "MITRE ATT&CK",
231     "technique": [
232       {
233         "id": "T1098",
234         "name": "Account Manipulation",
235       }
236     ]
237   }
238 ],
239 "tactic": {
240   "id": "TA0003",
241   "name": "Persistence",
242   "reference": "https://attack.mitre.org/tactics/TA0003"
243 },
244 "framework": "MITRE ATT&CK",
245 "technique": [
246   {
247     "id": "T1098",
248     "name": "Account Manipulation",
249   }
250 ],
251 "threat": [
252   {
253     "tactic": {
254       "id": "TA0003",
255       "name": "Persistence",
256     },
257     "framework": "MITRE ATT&CK",
258     "technique": [
259       {
260         "id": "T1098",
261         "name": "Account Manipulation",
262       }
263     ]
264   }
265 ],
266 "tags": [
267   "attack.persistence",
268   "attack.t1098"
269 ],
270 "to": "now",
271 "type": "query",
272 "threat": [
273   {
274     "tactic": {
275       "id": "TA0003",
276       "name": "Persistence",
277     },
278     "framework": "MITRE ATT&CK",
279     "technique": [
280       {
281         "id": "T1098",
282         "name": "Account Manipulation",
283       }
284     ]
285   }
286 ],
287 "tactic": {
288   "id": "TA0003",
289   "name": "Persistence",
290   "reference": "https://attack.mitre.org/tactics/TA0003"
291 },
292 "framework": "MITRE ATT&CK",
293 "technique": [
294   {
295     "id": "T1098",
296     "name": "Account Manipulation",
297   }
298 ],
299 "threat": [
300   {
301     "tactic": {
302       "id": "TA0003",
303       "name": "Persistence",
304     },
305     "framework": "MITRE ATT&CK",
306     "technique": [
307       {
308         "id": "T1098",
309         "name": "Account Manipulation",
310       }
311     ]
312   }
313 ],
314 "tags": [
315   "attack.persistence",
316   "attack.t1098"
317 ],
318 "to": "now",
319 "type": "query",
320 "threat": [
321   {
322     "tactic": {
323       "id": "TA0003",
324       "name": "Persistence",
325     },
326     "framework": "MITRE ATT&CK",
327     "technique": [
328       {
329         "id": "T1098",
330         "name": "Account Manipulation",
331       }
332     ]
333   }
334 ],
335 "tactic": {
336   "id": "TA0003",
337   "name": "Persistence",
338   "reference": "https://attack.mitre.org/tactics/TA0003"
339 },
340 "framework": "MITRE ATT&CK",
341 "technique": [
342   {
343     "id": "T1098",
344     "name": "Account Manipulation",
345   }
346 ],
347 "threat": [
348   {
349     "tactic": {
350       "id": "TA0003",
351       "name": "Persistence",
352     },
353     "framework": "MITRE ATT&CK",
354     "technique": [
355       {
356         "id": "T1098",
357         "name": "Account Manipulation",
358       }
359     ]
360   }
361 ],
362 "tags": [
363   "attack.persistence",
364   "attack.t1098"
365 ],
366 "to": "now",
367 "type": "query",
368 "threat": [
369   {
370     "tactic": {
371       "id": "TA0003",
372       "name": "Persistence",
373     },
374     "framework": "MITRE ATT&CK",
375     "technique": [
376       {
377         "id": "T1098",
378         "name": "Account Manipulation",
379       }
380     ]
381   }
382 ],
383 "tactic": {
384   "id": "TA0003",
385   "name": "Persistence",
386   "reference": "https://attack.mitre.org/tactics/TA0003"
387 },
388 "framework": "MITRE ATT&CK",
389 "technique": [
390   {
391     "id": "T1098",
392     "name": "Account Manipulation",
393   }
394 ],
395 "threat": [
396   {
397     "tactic": {
398       "id": "TA0003",
399       "name": "Persistence",
400     },
401     "framework": "MITRE ATT&CK",
402     "technique": [
403       {
404         "id": "T1098",
405         "name": "Account Manipulation",
406       }
407     ]
408   }
409 ],
410 "tags": [
411   "attack.persistence",
412   "attack.t1098"
413 ],
414 "to": "now",
415 "type": "query",
416 "threat": [
417   {
418     "tactic": {
419       "id": "TA0003",
420       "name": "Persistence",
421     },
422     "framework": "MITRE ATT&CK",
423     "technique": [
424       {
425         "id": "T1098",
426         "name": "Account Manipulation",
427       }
428     ]
429   }
430 ],
431 "tactic": {
432   "id": "TA0003",
433   "name": "Persistence",
434   "reference": "https://attack.mitre.org/tactics/TA0003"
435 },
436 "framework": "MITRE ATT&CK",
437 "technique": [
438   {
439     "id": "T1098",
440     "name": "Account Manipulation",
441   }
442 ],
443 "threat": [
444   {
445     "tactic": {
446       "id": "TA0003",
447       "name": "Persistence",
448     },
449     "framework": "MITRE ATT&CK",
450     "technique": [
451       {
452         "id": "T1098",
453         "name": "Account Manipulation",
454       }
455     ]
456   }
457 ],
458 "tags": [
459   "attack.persistence",
460   "attack.t1098"
461 ],
462 "to": "now",
463 "type": "query",
464 "threat": [
465   {
466     "tactic": {
467       "id": "TA0003",
468       "name": "Persistence",
469     },
470     "framework": "MITRE ATT&CK",
471     "technique": [
472       {
473         "id": "T1098",
474         "name": "Account Manipulation",
475       }
476     ]
477   }
478 ],
479 "tactic": {
480   "id": "TA0003",
481   "name": "Persistence",
482   "reference": "https://attack.mitre.org/tactics/TA0003"
483 },
484 "framework": "MITRE ATT&CK",
485 "technique": [
486   {
487     "id": "T1098",
488     "name": "Account Manipulation",
489   }
490 ],
491 "threat": [
492   {
493     "tactic": {
494       "id": "TA0003",
495       "name": "Persistence",
496     },
497     "framework": "MITRE ATT&CK",
498     "technique": [
499       {
500         "id": "T1098",
501         "name": "Account Manipulation",
502       }
503     ]
504   }
505 ],
506 "tags": [
507   "attack.persistence",
508   "attack.t1098"
509 ],
510 "to": "now",
511 "type": "query",
512 "threat": [
513   {
514     "tactic": {
515       "id": "TA0003",
516       "name": "Persistence",
517     },
518     "framework": "MITRE ATT&CK",
519     "technique": [
520       {
521         "id": "T1098",
522         "name": "Account Manipulation",
523       }
524     ]
525   }
526 ],
527 "tactic": {
528   "id": "TA0003",
529   "name": "Persistence",
530   "reference": "https://attack.mitre.org/tactics/TA0003"
531 },
532 "framework": "MITRE ATT&CK",
533 "technique": [
534   {
535     "id": "T1098",
536     "name": "Account Manipulation",
537   }
538 ],
539 "threat": [
540   {
541     "tactic": {
542       "id": "TA0003",
543       "name": "Persistence",
544     },
545     "framework": "MITRE ATT&CK",
546     "technique": [
547       {
548         "id": "T1098",
549         "name": "Account Manipulation",
550       }
551     ]
552   }
553 ],
554 "tags": [
555   "attack.persistence",
556   "attack.t1098"
557 ],
558 "to": "now",
559 "type": "query",
560 "threat": [
561   {
562     "tactic": {
563       "id": "TA0003",
564       "name": "Persistence",
565     },
566     "framework": "MITRE ATT&CK",
567     "technique": [
568       {
569         "id": "T1098",
570         "name": "Account Manipulation",
571       }
572     ]
573   }
574 ],
575 "tactic": {
576   "id": "TA0003",
577   "name": "Persistence",
578   "reference": "https://attack.mitre.org/tactics/TA0003"
579 },
580 "framework": "MITRE ATT&CK",
581 "technique": [
582   {
583     "id": "T1098",
584     "name": "Account Manipulation",
585   }
586 ],
587 "threat": [
588   {
589     "tactic": {
590       "id": "TA0003",
591       "name": "Persistence",
592     },
593     "framework": "MITRE ATT&CK",
594     "technique": [
595       {
596         "id": "T1098",
597         "name": "Account Manipulation",
598       }
599     ]
600   }
601 ],
602 "tags": [
603   "attack.persistence",
604   "attack.t1098"
605 ],
606 "to": "now",
607 "type": "query",
608 "threat": [
609   {
610     "tactic": {
611       "id": "TA0003",
612       "name": "Persistence",
613     },
614     "framework": "MITRE ATT&CK",
615     "technique": [
616       {
617         "id": "T1098",
618         "name": "Account Manipulation",
619       }
620     ]
621   }
622 ],
623 "tactic": {
624   "id": "TA0003",
625   "name": "Persistence",
626   "reference": "https://attack.mitre.org/tactics/TA0003"
627 },
628 "framework": "MITRE ATT&CK",
629 "technique": [
630   {
631     "id": "T1098",
632     "name": "Account Manipulation",
633   }
634 ],
635 "threat": [
636   {
637     "tactic": {
638       "id": "TA0003",
639       "name": "Persistence",
640     },
641     "framework": "MITRE ATT&CK",
642     "technique": [
643       {
644         "id": "T1098",
645         "name": "Account Manipulation",
646       }
647     ]
648   }
649 ],
650 "tags": [
651   "attack.persistence",
652   "attack.t1098"
653 ],
654 "to": "now",
655 "type": "query",
656 "threat": [
657   {
658     "tactic": {
659       "id": "TA0003",
660       "name": "Persistence",
661     },
662     "framework": "MITRE ATT&CK",
663     "technique": [
664       {
665         "id": "T1098",
666         "name": "Account Manipulation",
667       }
668     ]
669   }
670 ],
671 "tactic": {
672   "id": "TA0003",
673   "name": "Persistence",
674   "reference": "https://attack.mitre.org/tactics/TA0003"
675 },
676 "framework": "MITRE ATT&CK",
677 "technique": [
678   {
679     "id": "T1098",
680     "name": "Account Manipulation",
681   }
682 ],
683 "threat": [
684   {
685     "tactic": {
686       "id": "TA0003",
687       "name": "Persistence",
688     },
689     "framework": "MITRE ATT&CK",
690     "technique": [
691       {
692         "id": "T1098",
693         "name": "Account Manipulation",
694       }
695     ]
696   }
697 ],
698 "tags": [
699   "attack.persistence",
700   "attack.t1098"
701 ],
702 "to": "now",
703 "type": "query",
704 "threat": [
705   {
706     "tactic": {
707       "id": "TA0003",
708       "name": "Persistence",
709     },
710     "framework": "MITRE ATT&CK",
711     "technique": [
712       {
713         "id": "T1098",
714         "name": "Account Manipulation",
715       }
716     ]
717   }
718 ],
719 "tactic": {
720   "id": "TA0003",
721   "name": "Persistence",
722   "reference": "https://attack.mitre.org/tactics/TA0003"
723 },
724 "framework": "MITRE ATT&CK",
725 "technique": [
726   {
727     "id": "T1098",
728     "name": "Account Manipulation",
729   }
730 ],
731 "threat": [
732   {
733     "tactic": {
734       "id": "TA0003",
735       "name": "Persistence",
736     },
737     "framework": "MITRE ATT&CK",
738     "technique": [
739       {
740         "id": "T1098",
741         "name": "Account Manipulation",
742       }
743     ]
744   }
745 ],
746 "tags": [
747   "attack.persistence",
748   "attack.t1098"
749 ],
750 "to": "now",
751 "type": "query",
752 "threat": [
753   {
754     "tactic": {
755       "id": "TA0003",
756       "name": "Persistence",
757     },
758     "framework": "MITRE ATT&CK",
759     "technique": [
760       {
761         "id": "T1098",
762         "name": "Account Manipulation",
763       }
764     ]
765   }
766 ],
767 "tactic": {
768   "id": "TA0003",
769   "name": "Persistence",
770   "reference": "https://attack.mitre.org/tactics/TA0003"
771 },
772 "framework": "MITRE ATT&CK",
773 "technique": [
774   {
775     "id": "T1098",
776     "name": "Account Manipulation",
777   }
778 ],
779 "threat": [
780   {
781     "tactic": {
782       "id": "TA0003",
783       "name": "Persistence",
784     },
785     "framework": "MITRE ATT&CK",
786     "technique": [
787       {
788         "id": "T1098",
789         "name": "Account Manipulation",
790       }
791     ]
792   }
793 ],
794 "tags": [
795   "attack.persistence",
796   "attack.t1098"
797 ],
798 "to": "now",
799 "type": "query",
800 "threat": [
801   {
802     "tactic": {
803       "id": "TA0003",
804       "name": "Persistence",
805     },
806     "framework": "MITRE ATT&CK",
807     "technique": [
808       {
809         "id": "T1098",
810         "name": "Account Manipulation",
811       }
812     ]
813   }
814 ],
815 "tactic": {
816   "id": "TA0003",
817   "name": "Persistence",
818   "reference": "https://attack.mitre.org/tactics/TA0003"
819 },
820 "framework": "MITRE ATT&CK",
821 "technique": [
822   {
823     "id": "T1098",
824     "name": "Account Manipulation",
825   }
826 ],
827 "threat": [
828   {
829     "tactic": {
830       "id": "TA0003",
831       "name": "Persistence",
832     },
833     "framework": "MITRE ATT&CK",
834     "technique": [
835       {
836         "id": "T1098",
837         "name": "Account Manipulation",
838       }
839     ]
840   }
841 ],
842 "tags": [
843   "attack.persistence",
844   "attack.t1098"
845 ],
846 "to": "now",
847 "type": "query",
848 "threat": [
849   {
850     "tactic": {
851       "id": "TA0003",
852       "name": "Persistence",
853     },
854     "framework": "MITRE ATT&CK",
855     "technique": [
856       {
857         "id": "T1098",
858         "name": "Account Manipulation",
859       }
860     ]
861   }
862 ],
863 "tactic": {
864   "id": "TA0003",
865   "name": "Persistence",
866   "reference": "https://attack.mitre.org/tactics/TA0003"
867 },
868 "framework": "MITRE ATT&CK",
869 "technique": [
870   {
871     "id": "T1098",
872     "name": "Account Manipulation",
873   }
874 ],
875 "threat": [
876   {
877     "tactic": {
878       "id": "TA0003",
879       "name": "Persistence",
880     },
881     "framework": "MITRE ATT&CK",
882     "technique": [
883       {
884         "id": "T1098",
885         "name": "Account Manipulation",
886       }
887     ]
888   }
889 ],
890 "tags": [
891   "attack.persistence",
892   "attack.t1098"
893 ],
894 "to": "now",
895 "type": "query",
896 "threat": [
897   {
898     "tactic": {
899       "id": "TA0003",
900       "name": "Persistence",
901     },
902     "framework": "MITRE ATT&CK",
903     "technique": [
904       {
905         "id": "T1098",
906         "name": "Account Manipulation",
907       }
908     ]
909   }
910 ],
911 "tactic": {
912   "id": "TA0003",
913   "name": "Persistence",
914   "reference": "https://attack.mitre.org/tactics/TA0003"
915 },
916 "framework": "MITRE ATT&CK",
917 "technique": [
918   {
919     "id": "T1098",
920     "name": "Account Manipulation",
921   }
922 ],
923 "threat": [
924   {
925     "tactic": {
926       "id": "TA0003",
927       "name": "Persistence",
928     },
929     "framework": "MITRE ATT&CK",
930     "technique": [
931       {
932         "id": "T1098",
933         "name": "Account Manipulation",
934       }
935     ]
936   }
937 ],
938 "tags": [
939   "attack.persistence",
940   "attack.t1098"
941 ],
942 "to": "now",
943 "type": "query",
944 "threat": [
945   {
946     "tactic": {
947       "id": "TA0003",
948       "name": "Persistence",
949     },
950     "framework": "MITRE ATT&CK",
951     "technique": [
952       {
953         "id": "T1098",
954         "name": "Account Manipulation",
955       }
956     ]
957   }
958 ],
959 "tactic": {
960   "id": "TA0003",
961   "name": "Persistence",
962   "reference": "https://attack.mitre.org/tactics/TA0003"
963 },
964 "framework": "MITRE ATT&CK",
965 "technique": [
966   {
967     "id": "T1098",
968     "name": "Account Manipulation",
969   }
970 ],
971 "threat": [
972   {
973     "tactic": {
974       "id": "TA0003",
975       "name": "Persistence",
976     },
977     "framework": "MITRE ATT&CK",
978     "technique": [
979       {
980         "id": "T1098",
981         "name": "Account Manipulation",
982       }
983     ]
984   }
985 ],
986 "tags": [
987   "attack.persistence",
988   "attack.t1098"
989 ],
990 "to": "now",
991 "type": "query",
992 "threat": [
993   {
994     "tactic": {
995       "id": "TA0003",
996       "name": "Persistence",
997     },
998     "framework": "MITRE ATT&CK",
999     "technique": [
1000       {
1001         "id": "T1098",
1002         "name": "Account Manipulation",
1003       }
1004     ]
1005   }
1006 ],
1007 "tactic": {
1008   "id": "TA0003",
1009   "name": "Persistence",
1010   "reference": "https://attack.mitre.org/tactics/TA0003"
1011 },
1012 "framework": "MITRE ATT&CK",
1013 "technique": [
1014   {
1015     "id": "T1098",
1016     "name": "Account Manipulation",
1017   }
1018 ],
1019 "threat": [
1020   {
1021     "tactic": {
1022       "id": "TA0003",
1023       "name": "Persistence",
1024     },
1025     "framework": "MITRE ATT&CK",
1026     "technique": [
1027       {
1028         "id": "T1098",
1029         "name": "Account Manipulation",
1030       }
1031     ]
1032   }
1033 ],
1034 "tags": [
1035   "attack.persistence",
1036   "attack.t1098"
1037 ],
1038 "to": "now",
1039 "type": "query",
1040 "threat": [
1041   {
1042     "tactic": {
1043       "id": "TA0003",
1044       "name": "Persistence",
1045     },
1046     "framework": "MITRE ATT&CK",
1047     "technique": [
1048       {
1049         "id": "T1098",
1050         "name": "Account Manipulation",
1051       }
1052     ]
1053   }
1054 ],
1055 "tactic": {
1056   "id": "TA0003",
1057   "name": "Persistence",
1058   "reference": "https://attack.mitre.org/tactics/TA0003"
1059 },
1060 "framework": "MITRE ATT&CK",
1061 "technique": [
1062   {
1063     "id": "T1098",
1064     "name": "Account Manipulation",
1065   }
1066 ],
1067 "threat": [
1068   {
1069     "tactic": {
1070       "id": "TA0003",
1071       "name": "Persistence",
1072     },
1073     "framework": "MITRE ATT&CK",
1074     "technique": [
1075       {
1076         "id": "T1098",
1077         "name": "Account Manipulation",
1078       }
1079     ]
1080   }
1081 ],
1082 "tags": [
1083   "attack.persistence",
1084   "attack.t1098"
1085 ],
1086 "to": "now",
1087 "type": "query",
1088 "threat": [
1089   {
1090     "tactic": {
1091       "id": "TA0003",
1092       "name": "Persistence",
1093     },
1094     "framework": "MITRE ATT&CK",
1095     "technique": [
1096       {
1097         "id": "T1098",
1098         "name": "Account Manipulation",
1099       }
1100     ]
1101   }
1102 ],
1103 "tactic": {
1104   "id": "TA0003",
1105   "name": "Persistence",
1106   "reference": "https://attack.mitre.org/tactics/TA0003"
1107 },
1108 "framework": "MITRE ATT&CK",
1109 "technique": [
1110   {
1111     "id": "T1098",
1112     "name": "Account Manipulation",
1113   }
1114 ],
1115 "threat": [
1116   {
1117     "tactic": {
1118       "id": "TA0003",
1119       "name": "Persistence",
1120     },
1121     "framework": "MITRE ATT&CK",
1122     "technique": [
1123       {
1124         "id": "T1098",
1125         "name": "Account Manipulation",
1126       }
1127     ]
1128   }
1129 ],
1130 "tags": [
1131   "attack.persistence",
1132   "attack.t1098"
1133 ],
1134 "to": "now",
1135 "type": "query",
1136 "threat": [
1137   {
1138     "tactic": {
1139       "id": "TA0003",
1140       "name": "Persistence",
1141     },
1142     "framework": "MITRE ATT&CK",
1143     "technique": [
1144       {
1145         "id": "T1098",
1146         "name": "Account Manipulation",
1147       }
1148     ]
1149   }
1150 ],
1151 "tactic": {
1152   "id": "TA0003",
1153   "name": "Persistence",
1154   "reference": "https://attack.mitre.org/tactics/TA0003"
1155 },
1156 "framework": "MITRE ATT&CK",
1157 "technique": [
1158   {
1159     "id": "T1098",
1160     "name": "Account Manipulation",
1161   }
1162 ],
1163 "threat": [
1164   {
1165     "tactic": {
1166       "id": "TA0003",
1167       "name": "Persistence",
1168     },
1169     "framework": "MITRE ATT&CK",
1170     "technique": [
1171       {
1172         "id": "T1098",
1173         "name": "Account Manipulation",
1174       }
1175     ]
1176   }
1177 ],
1178 "tags": [
1179   "attack.persistence",
1180   "attack.t1098"
1181 ],
1182 "to": "now",
1183 "type": "query",
1184 "threat": [
1185   {
1186     "tactic": {
1187       "id": "TA0003",
1188       "name": "Persistence",
1189     },
1190     "framework": "MITRE ATT&CK",
1191     "technique": [
1192       {
1193         "id": "T1098",
1194         "name": "Account Manipulation",
1195       }
1196     ]
1197   }
1198 ],
1199 "tactic": {
1200   "id": "TA0003",
1201   "name": "Persistence",
1202   "reference": "https://attack.mitre.org/tactics/TA0003"
1203 },
1204 "framework": "MITRE ATT&CK",
1205 "technique": [
1206   {
1207     "id": "T1098",
1208     "name": "Account Manipulation",
1209   }
1210 ],
1211 "threat": [
1212   {
1213     "tactic": {
1214       "id": "TA0003",
1215       "name": "Persistence",
1216     },
1217     "framework": "MITRE ATT&CK",
1218     "technique": [
1219       {
1220         "id": "T1098",
1221         "name": "Account Manipulation",
1222       }
1223     ]
1224   }
1225 ],
122
```

- On a des alertes par exemple :
 - Injection potentielle de processus via PowerShell
 - Script PowerShell avec capacités d'usurpation d'identité par jeton
- On peut en savoir plus sur des alertes :

The screenshot shows the Elastic Security interface for a specific rule. The rule is titled "Multiple Alerts in Different ATT&CK Tactics on a Single Host". It is created by elastic on Dec 7, 2023, and updated by elastic on Dec 7, 2023. The last response was successful at Dec 8, 2023, at 15:31:30.812. The rule is enabled and has a risk score of 73. The severity is High. The author is Elastic. The license is Elastic License v2. The timestamp override is event.ingested. The tags are Use Case: Threat Detection. The rule is defined by the index pattern .alerts-security.* and the custom query signal.rule.name:* and kibana.alert.rule.threat.tactic.id:*. The rule type is Threshold. The required fields are kibana.alert.rule.threat.tactic.id and signal.rule.name. The timeline template is None. The threshold is Results aggregated by host.id >= 1.

- Ici on peut voir les attaques par règles :

The screenshot shows the Elastic Security interface with the Alerts and Cases sections. The Alerts section shows a donut chart with 1k+ Open alerts. The Cases section shows a table of open alerts by rule. The table has columns for Rule name, Last alert, Alert count, and Severity. The rules listed are Potential Credential Access via DCSync, Multiple Alerts in Different ATT&CK Tactics on a Single..., Potential Invoke-Mimikatz PowerShell Script, and Multiple Alerts Involving a User. The alert counts are 40, 7, 4, and 2 respectively. The severity is High for all rules.

Rule name	Last alert	Alert count	Severity
Potential Credential Access via DCSync	9 hours ago	40	High
Multiple Alerts in Different ATT&CK Tactics on a Single...	8 hours ago	7	High
Potential Invoke-Mimikatz PowerShell Script	9 hours ago	4	High
Multiple Alerts Involving a User	8 hours ago	2	High

Réalisé par Mathéo Balazuc.