Rapport de surveillance

A l’attention de IRON4SOFTWARE

Introduction

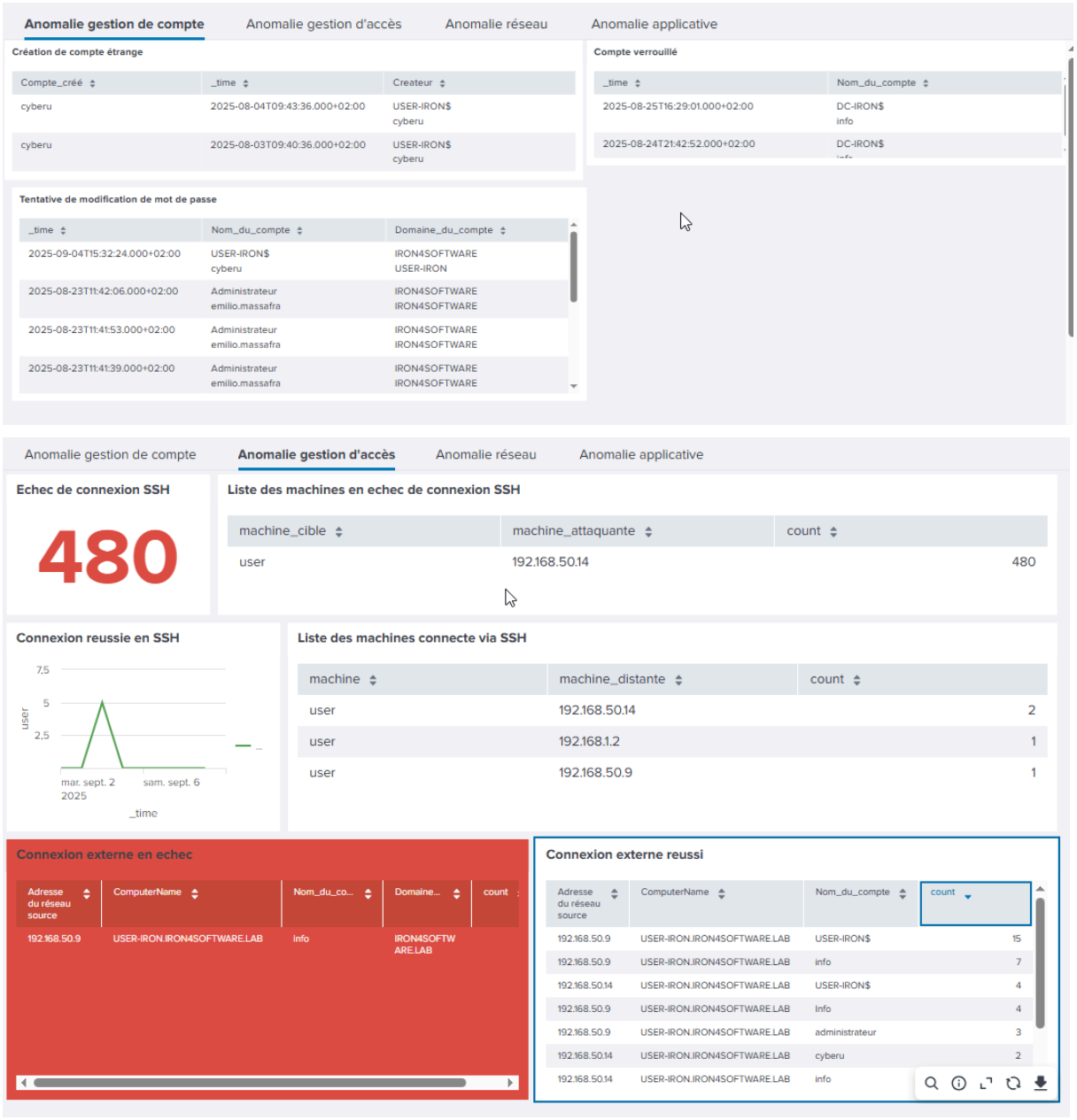
Dans le cadre d'une démarche proactive et continue de renforcement de la posture de cybersécurité de notre organisation, le présent rapport a pour vocation de détailler de manière exhaustive le déploiement, les configurations et les résultats obtenus par le système de surveillance en temps réel. Ce système repose sur l'implémentation d'un ensemble de règles de détection et de mécanismes d'alertes, paramétrés au sein de la plateforme Splunk Enterprise Security.

L'objectif stratégique est d’ identifier rapidement les comportements anormaux et détecter toute tentative d'intrusion ou indice de compromission. Une détection précoce est vitale pour minimiser l'impact et assurer la résilience des infrastructures.

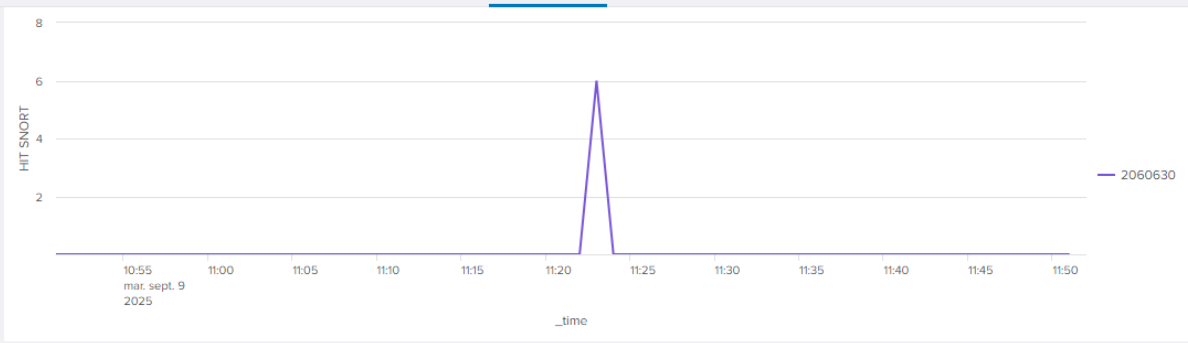
Ce document s'articulera autour de plusieurs axes majeurs. Nous commencerons par une présentation détaillée des différents tableaux de bord analytiques configurés dans Splunk, qui offrent une vue d'ensemble et des perspectives approfondies sur l'état de notre sécurité. Chaque tableau de bord sera décrit en termes de données agrégées, de métriques clés et de capacités de visualisation. Ensuite, le rapport listera et décrira en détail toutes les alertes critiques qui ont été implémentées. Pour chaque alerte, nous spécifierons son déclencheur, les conditions de son activation, sa sévérité.

1. Tableau de bord

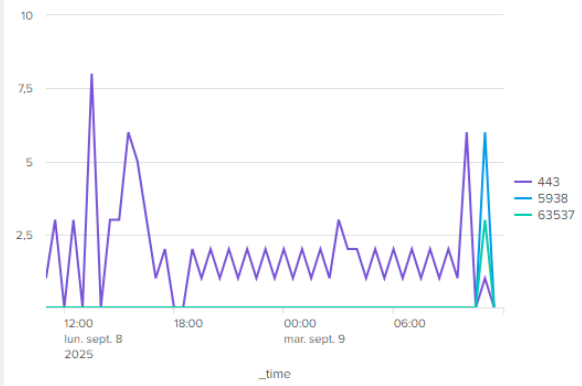
Les tableaux de bord de surveillance jouent un rôle crucial dans la détection précoce des menaces et l'analyse de la posture de sécurité d'une organisation. Cette section présente les tableaux de bord configurés dans Splunk, chacun étant conçu pour offrir une visibilité approfondie sur des aspects spécifiques de la sécurité des systèmes d'information d'Iron4Software.



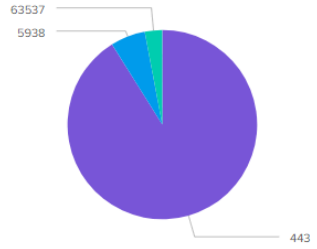
Anomalie gestion de compte | Anomalie gestion d'accès | **Anomalie réseau** | Anomalie applicative



Ports utilisés par les postes windows au fils du temps



Ports utilisés par les postes windows



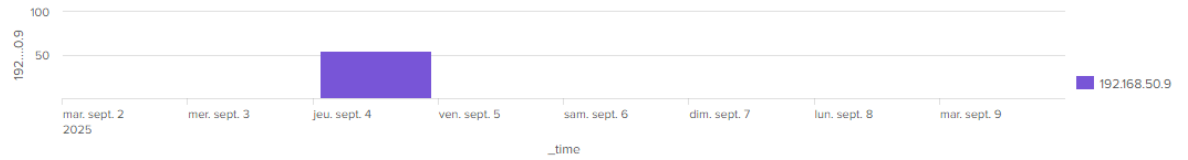
Anomalie gestion de compte | Anomalie gestion d'accès | Anomalie réseau | **Anomalie applicative**

Injection SQL

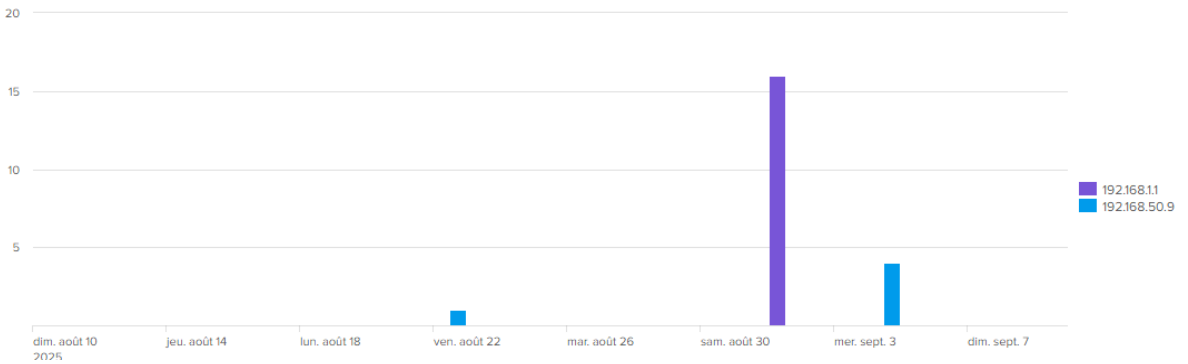
Injection SQL

uri_file	injectionSql
secure/admin.php	70
secure/reports.php	2

Brute force actif (auth en erreur: 401,403,429)

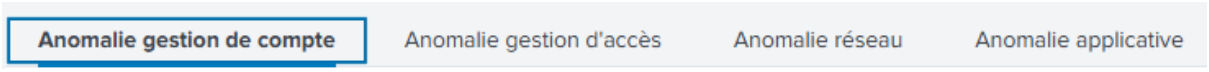


Anomalie LFI détecté



1.1 Anomalie gestion de compte

Onglet du tableau de bord :

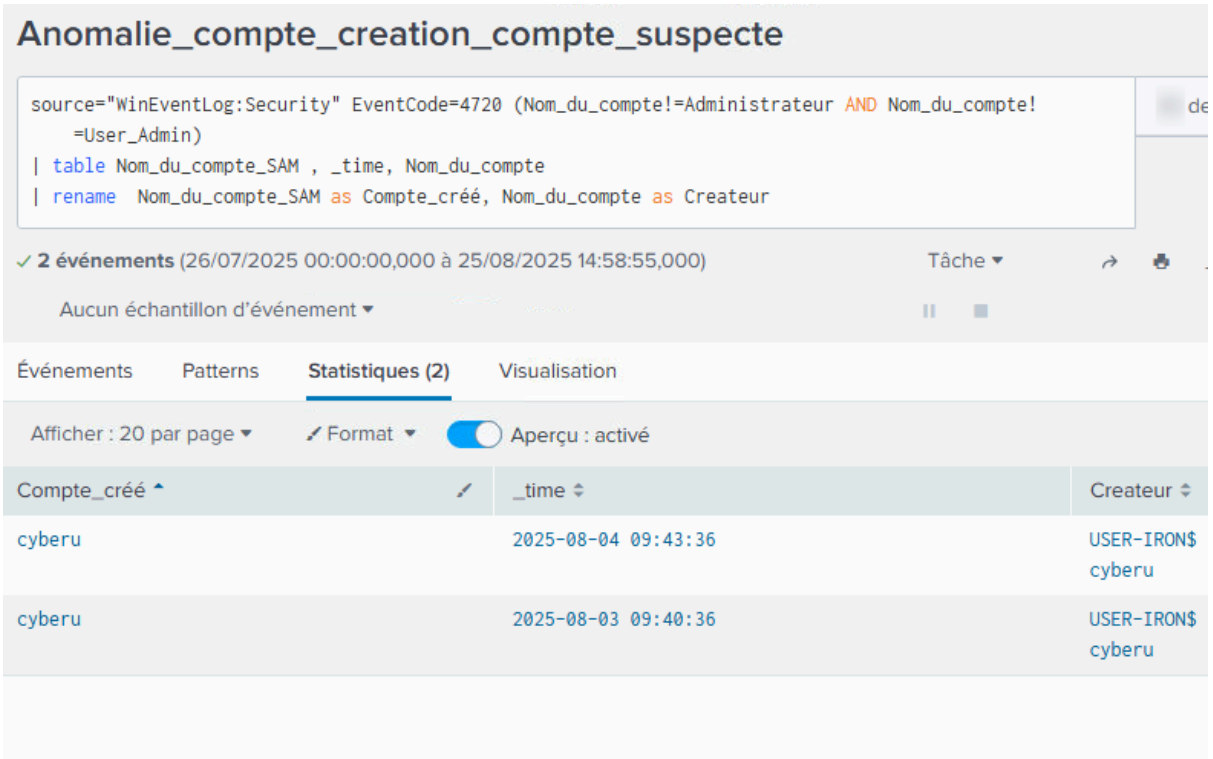


1.1.1 Anomalie création compte

Normalement, un administrateur est le seul à avoir le rôle dans l'entreprise pour créer un compte.

La recherche Splunk a pour objectif de surveiller la création de comptes utilisateurs qui n'auraient pas été créés par les administrateurs légitimes (Administrateur ou User_Admin). L'EventCode 4720 correspond à la création d'un compte utilisateur. Pour éviter les **faux positifs** , on exclut les comptes Administrateur et User_Admin dans la recherche et on identifie les créations de comptes potentiellement non autorisées.

Recherche Splunk :



La recherche retourne trois champs : Nom_du_compte_SAM (le nom du compte tel qu'il est stocké dans la base de données SAM de Windows), _time (l'horodatage de l'événement) et Nom_du_compte (le nom de l'utilisateur qui a créé le compte). Ce dernier champ est ensuite renommé en Createur pour plus de clarté.

Cela correspond à la technique d'attaque **MITRE ATT&CK T1136 : Create Account**

1.1.2 Anomalie tentative de modification de mot de passe

L'objectif de cette recherche est de surveiller les modifications de mot de passe et les réinitialisations de mot de passe.

Recherche Splunk :

```
index=* EventCode=4724 OR EventCode=4723
| table _time, Nom_du_compte, Domaine_du_compte
```

Tentative de modification de mot de passe

_time	Nom_du_compte	Domaine_du_compte
2025-08-23T11:41:53.000+02:00	Administrateur emilio.massafra	IRON4SOFTWARE IRON4SOFTWARE
2025-08-23T11:41:39.000+02:00	Administrateur emilio.massafra	IRON4SOFTWARE IRON4SOFTWARE
2025-08-23T11:14:43.000+02:00	Administrateur emilio.massafra	IRON4SOFTWARE IRON4SOFTWARE
2025-08-23T11:42:06.000+02:00	Administrateur emilio.massafra	IRON4SOFTWARE IRON4SOFTWARE

La recherche affiche un tableau avec les informations suivantes pour chaque événement de modification ou de réinitialisation de mot de passe :

- **_time** : L'heure à laquelle l'événement s'est produit.
- **Nom_du_compte** : Le nom du compte utilisateur dont le mot de passe a été modifié ou réinitialisé.
- **Domaine_du_compte** : Le domaine auquel appartient le compte utilisateur.

Cela correspond à la technique d'attaque **MITRE ATT&CK T1078 : Valid Accounts**

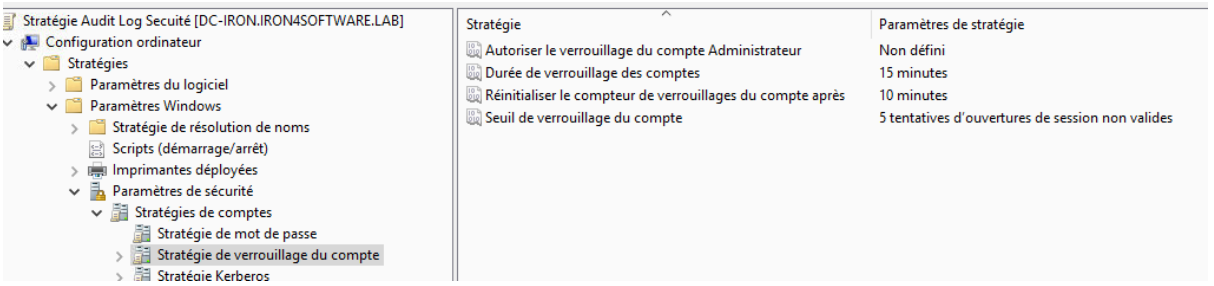
1.1.3 Anomalie compte verrouillé

L'objectif de la recherche est d'identifier les cas de verrouillage de compte d'utilisateur et de détecter les événements de réinitialisation de mot de passe (si l'EventCode 4740 est également lié à la réinitialisation de mot de passe).

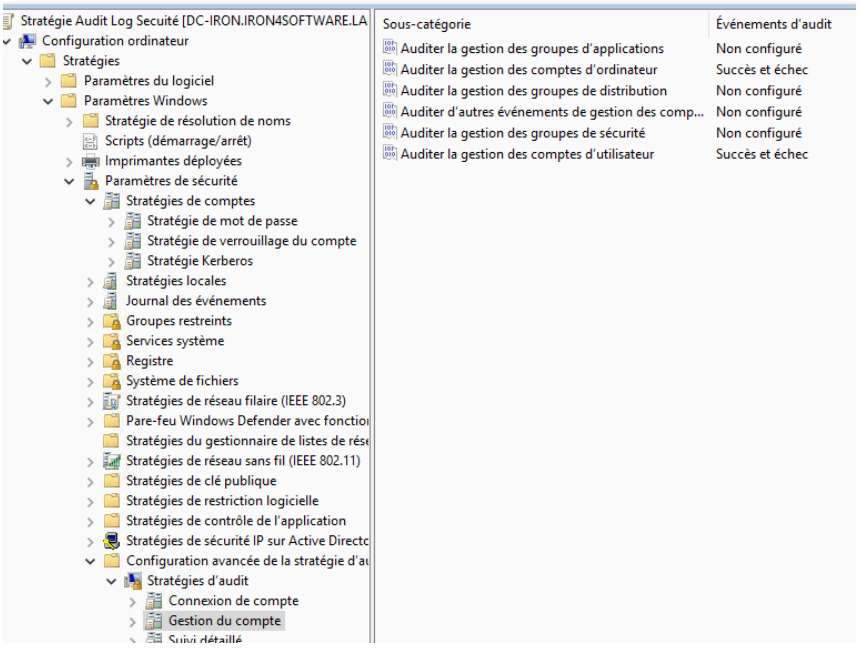
Pour rappel, une stratégie a été mise en place pour bloquer les tentatives d'ouverture de session non valides. Cette stratégie est détaillée ci-dessous.

Via la GPO Audit Log Sécurité appliqué sur l'ensemble des postes de l'entreprise

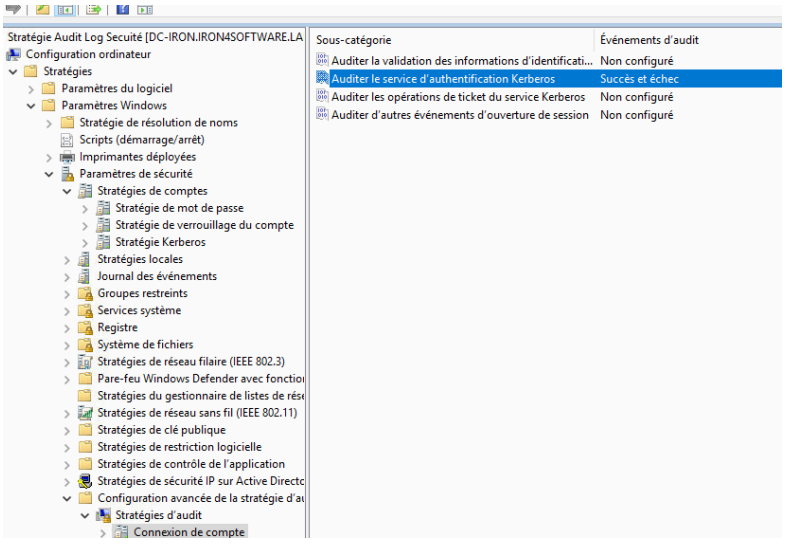
➢ Activation du verrouillage de compte :



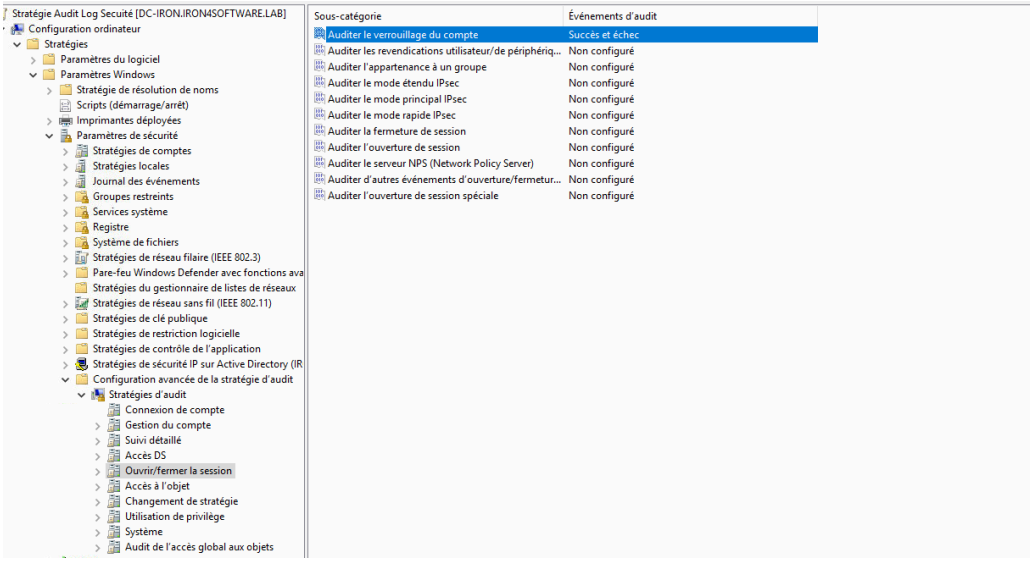
➢ Activation Advanced Audit Policy au préalable >> Gestion des comptes



➢ Activation Advanced Audit Policy au préalable >> Connexion de compte



➢ Activation Advanced Audit Policy au préalable >> Ouverture de compte



Recherche Splunk :

```
index=* (EventCode=4625 AND Sous-état=0xC0000234) OR EventCode=4740
| table _time, Nom_du_compte
```

_time	Nom_du_compte
2025-08-24 21:42:52	DC-IRON$
	info

La recherche remontera tous les événements où :

- EventCode=4625 (Échec de la connexion/ouverture de session) ET Sous-état=0xC0000234 (Indique que le compte est actuellement verrouillé).
- OU EventCode=4740 (Indique un événement de verrouillage de compte).

En résumé, cette recherche permet de surveiller et d'auditer les verrouillage de compte, ce qui est crucial pour la sécurité et la détection d'activités suspectes (par exemple, tentatives répétées de connexion avec de mauvais mots de passe). On affiche les résultats sous forme de tableau.

Cela correspond à la technique d'attaque **MITRE ATT&CK T1078 : Valid Accounts**

1.2. Anomalie gestion d'accès

Onglet du tableau de bord :

1.2.1. Accès RDP non autorisé : Echec de connexion RDP de machine distante (externe)

L'objectif de la recherche est de détecter les tentatives de connexion RDP échouées provenant de machines distantes (externes) qui ne font pas partie du réseau interne (192.168.1.*). Les tentatives provenant du réseau interne (192.168.1.*) seront considérées comme des faux positifs. La recherche vise également à identifier les comptes utilisateurs et les ordinateurs impliqués dans ces tentatives de connexion infructueuses.

Recherche Splunk :

```
index=* EventCode=4625 "Adresse du réseau source"!="192.168.1.*" ("Type d'ouverture de session"=3 OR "Type d'ouverture de session"=10)
| stats  count by "Adresse du réseau source",ComputerName, Nom_du_compte, Domaine_du_compte | search Nom_du_compte!="-" AND Domaine_du_compte!="-"
| sort  - count
```

Adresse du réseau source	ComputerName	Nom_du_compte	Domaine_du_compte	count
192.168.50.9	USER-IRON.IRON4SOFTWARE.LAB	info	IRON4SOFTWARE.LAB	63
192.168.50.9	DC-IRON.IRON4SOFTWARE.LAB	Administrator	WORKGROUP	11
192.168.50.9	DC-IRON.IRON4SOFTWARE.LAB	emilio.massafra@iron4software@lab	WORKGROUP	4
192.168.50.9	USER-IRON.IRON4SOFTWARE.LAB	Info	IRON4SOFTWARE	4

La recherche agrège les événements d'échec de connexion (EventCode=4625) en se basant sur les champs suivants :

- "Adresse du réseau source" : L'adresse IP d'où provient la tentative de connexion.
- ComputerName : Le nom de l'ordinateur cible.
- Nom_du_compte : Le nom du compte utilisateur utilisé pour la tentative de connexion.
- Domaine_du_compte : Le domaine auquel appartient le compte utilisateur.

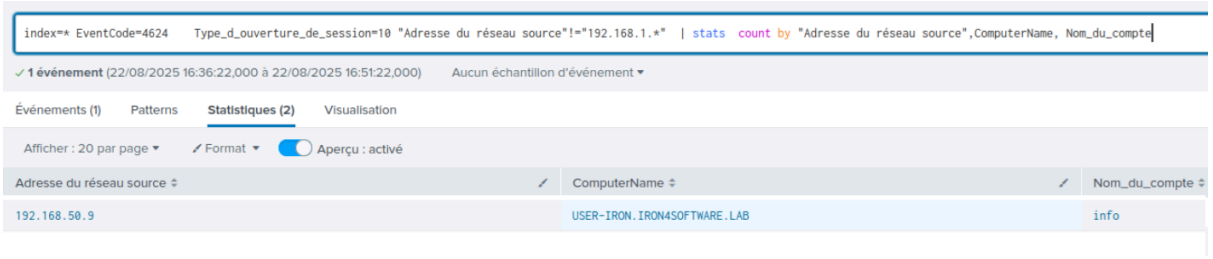
Les résultats sont triés par le nombre d'occurrences (count) par ordre décroissant, affichant ainsi les tentatives d'échec les plus fréquentes en premier. La recherche exclut également les noms de compte et de domaine vides ("-").

Cela correspond à la technique **MITRE ATT&CK T1021.001 : Remote Desktop Protocol (RDP).**

1.2.2. Accès RDP autorisé mais surveillé : connexion réussie depuis une machine distante (externe)

L'objectif de cette recherche Splunk est d'identifier et de compter les connexions réussies depuis des machines distantes (externes) qui ne proviennent pas du sous-réseau interne (192.168.1.*). Cela permet de surveiller l'accès externe et de détecter d'éventuelles activités suspectes ou non autorisées.

Recherche Splunk :



La recherche agrège les résultats et affiche le nombre de connexions réussies par :

- "Adresse du réseau source" : L'adresse IP de la machine distante d'où provient la connexion.
- "ComputerName" : Le nom de l'ordinateur sur lequel la connexion a été établie.
- "Nom_du_compte" : Le nom du compte utilisateur utilisé pour la connexion.
- "Count" : le nombre de connexions réussies

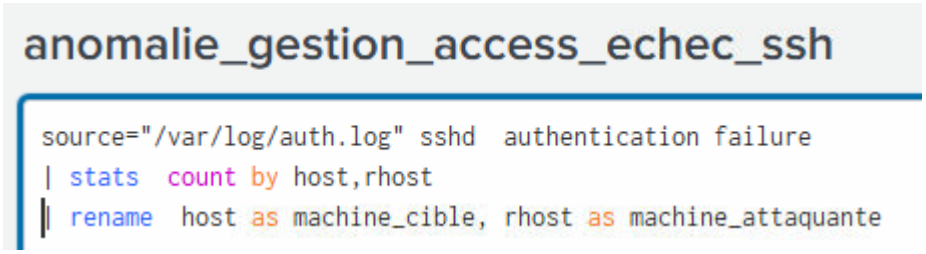
En clair, pour chaque connexion externe réussie, on verra de quelle adresse IP elle est venue, sur quel ordinateur elle s'est connectée, et avec quel compte. Le count indique combien de fois cette combinaison spécifique d'adresse source, nom d'ordinateur et nom de compte s'est produite.

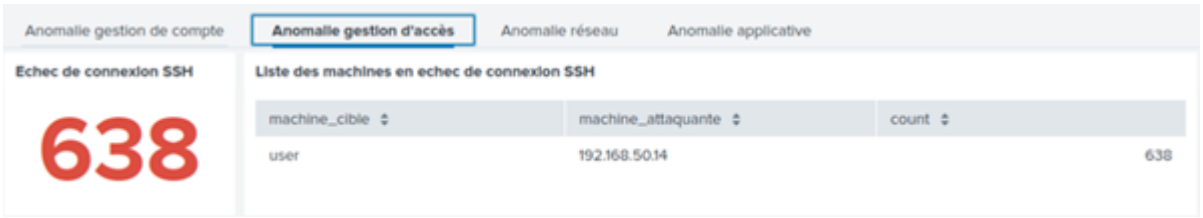
Cela correspond à la technique **MITRE ATT&CK T1078 : Valid Accounts**

1.2.3. Accès ssh non autorisé

L'objectif est de détecter les tentatives d'authentification SSH échouées.

Recherche Splunk :





Un tableau affichant le nombre d'échecs d'authentification SSH, regroupés par machine cible et machine attaquante.

Cela correspond à la technique **MITRE ATT&CK T1110 : Brute force**

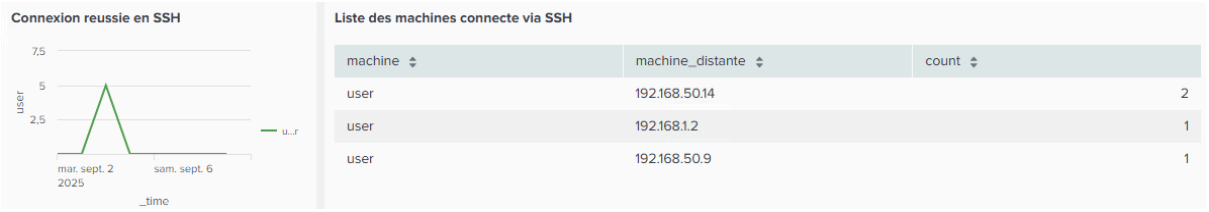
1.2.4. Accès ssh autorisé mais surveillé

L'objectif de cette recherche Splunk est d'identifier et de compter les tentatives de connexion SSH réussies, en regroupant les résultats par machine hôte et adresse IP distante.

Recherche Splunk :

anomalie_gestion_access_sshreussie

```
source=/var/log/auth.log sshd Accepted password
| stats count by host,auth_ip
|  sort - count
|  rename auth_ip as machine_distante, host as machine
```



La recherche produira un tableau avec les colonnes suivantes :

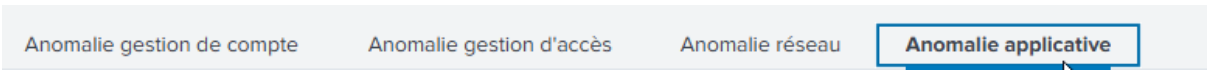
- **machine_distante :** L'adresse IP de la machine à partir de laquelle la connexion SSH a été tentée.
- **machine :** Le nom d'hôte de la machine sur laquelle la connexion SSH a été acceptée.
- **count :** Le nombre de tentatives de connexion SSH réussies depuis l'adresse IP distante vers la machine spécifiée.

Les résultats seront triés par ordre décroissant du nombre de connexions, affichant en premier les combinaisons machine/IP distante avec le plus grand nombre de connexions acceptées.

Cela correspond à la technique **MITRE ATT&CK T1078 : Valid Accounts**

1.3. Anomalie applicative

Onglet du tableau de bord :

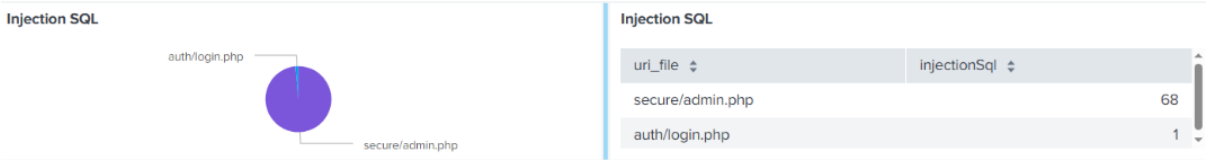


1.3.1. Anomalie injection SQL

L'objectif est de détecter les tentatives d'injection SQL en recherchant des mots-clés et des fonctions couramment utilisés dans les attaques d'injection SQL au sein des logs d'accès.

Recherche Splunk :

```
sourcetype="access-too_small" ("information_schema" OR "union+select" OR "union+all+select" OR "or+1%3D1" OR "or+1%3D0" OR "and+1%3D1" OR "and+1%3D0" OR "order+by"  OR  "group+by"  OR
    "information_schema" OR "version" OR "database" OR "user()" OR "current_user"
 OR "sleep" OR "benchmark" OR "concat" OR "char(" OR "load_file" OR "into+outfile" OR "into+dumpfile"
 OR "xp_cmdshell" OR "sp_executesql" OR "exec" OR "cast" OR "convert")
| stats count as injectionSql by uri_file
    | sort - injectionSql
```



Un tableau qui liste les fichiers URI (uri_file) où des tentatives d'injection SQL ont été détectées, trié par le nombre de détections (injectionSql) par ordre décroissant. Le fichier URI avec le plus grand nombre de détections d'injection SQL apparaît en premier.

Cela correspond à la technique **MITRE ATT&CK T1190 : Exploit Public-Facing Application**

1.3.2. Anomalie erreur HTTP : **Scan / reconnaissance active (dirb ... 400,403,404,414)**

L'objectif est de détecter les tentatives de scan ou de reconnaissance active (comme dirb, hydra) sur les systèmes en identifiant les requêtes HTTP avec des codes d'erreur spécifiques.

Recherche Splunk :

Code(s) HTTP	Signification
404	Not Found – l'attaquant énumère des chemins inexistants.
400	Bad Request – payload volontairement cassé (fuzzing).
414	URI Too Long – fuzzing, payloads très longs.

Le tableau horaire (timechart) affichera le nombre de ces erreurs regroupées par adresse IP du client (clientip), ce qui permettra de visualiser quelles adresses IP génèrent le plus de ces erreurs sur une période donnée, et potentiellement d'identifier les sources des scans.

Pour information le tableau des erreurs HTTP:

Code	Nom	Description
400	Bad Request	La requête envoyée par le client est mal formée ou invalide.
403	Forbidden	Le serveur comprend la requête mais refuse d'y répondre (accès interdit).
404	Not Found	La ressource demandée n'existe pas ou n'est pas disponible.

414	URI Too Long	L’URL (URI) est trop longue pour être traitée par le serveur.

Cela correspond aux techniques :

- **MITRE ATT&CK T1595 : Active Scanning**
- **MITRE ATT&CK T1083 : File and Directory Discovery**

1.3.3. Anomalie erreur HTTP : Nombre élevé d'erreurs d'authentification (401,403,429 en erreur)

L'objectif de cette recherche Splunk est d'identifier les tentatives d'attaques par force brute actives. Elle se concentre sur la détection des adresses IP clientes qui génèrent un nombre élevé d'erreurs d'authentification (statut 401), d'accès refusé (statut 403) ou de requêtes trop nombreuses (statut 429).

Recherche Splunk :

```
index=*  host=user   source="/var/log/apache2/access.log"  (status="401" OR status="403" OR  status="429")
| timechart  count by clientip
```

Le résultat de cette recherche sera un tableau temporel (timechart) affichant le nombre de ces erreurs regroupées par adresse IP cliente (`clientip`). Cela permet de visualiser les adresses IP qui sont les plus actives dans la génération de ces types d'erreurs, indiquant potentiellement une tentative de force brute.

En résumé, la recherche permet de **surveiller** les erreurs 401, 403 et 429 , d'**identifier** les adresses IP clientes qui déclenchent ces erreurs de manière répétée et enfin de **visualiser** l'évolution dans le temps de ces tentatives par adresse IP.

Pour information le tableau des erreurs HTTP:

Code(s) HTTP	Signification
401	Unauthorized – mot de passe/méthode auth invalide (bruteforce).
403	Forbidden – accès refusé (compte bloqué ou IP interdite).
429	Too Many Requests – rate-limit activé (preuve de brute-force/spray).

Cela correspond à la technique **MITRE ATT&CK T1110 : Brute force**

1.3.4. Anomalie: **Détection de LFI (Local File Inclusion) et Remote Code Execution**

L'objectif est de détecter les tentatives d'inclusion de fichiers locaux et RCE en analysant les paramètres d'URL suspects qui pourraient permettre l'accès non autorisé à des fichiers système sensibles.

Recherche Splunk :

```
index=* host=user (uri_query="*../*" OR uri_query="*/etc/passwd*" OR uri_query="*file=*" OR uri_query="*include=*")
| timechart count by clientip
```

Le résultat de cette recherche sera un tableau temporel (timechart) affichant le nombre de tentatives regroupées par adresse IP du client (clientip), ce qui permettra de visualiser quelles adresses IP génèrent le plus de ces tentatives sur une période donnée.

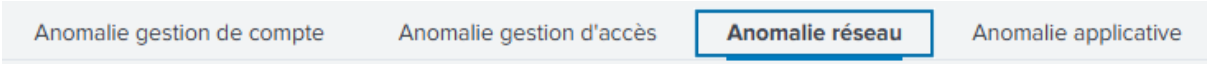
En résumé, la recherche permet de détecter les tentatives d'inclusion de fichiers locaux et RCE en surveillant les patterns caractéristiques (../, /etc/passwd, file=, include=) dans les paramètres d'URL et permet de visualiser l'évolution dans le temps de ces tentatives par adresse IP.

Cela correspond aux techniques :

- ➢ **MITRE ATT&CK T1083 : File and Directory Discovery**
- ➢ **MITRE ATT&CK T1190 : Exploit Public-Facing Application**
- ➢ **MITRE ATT&CK T1059 : Command and Scripting Interpreter**

1.4 Anomalie réseau

Onglet du tableau de bord :



1.4.1 Anomalie réseau : Détection IPS SNORT via PFsense

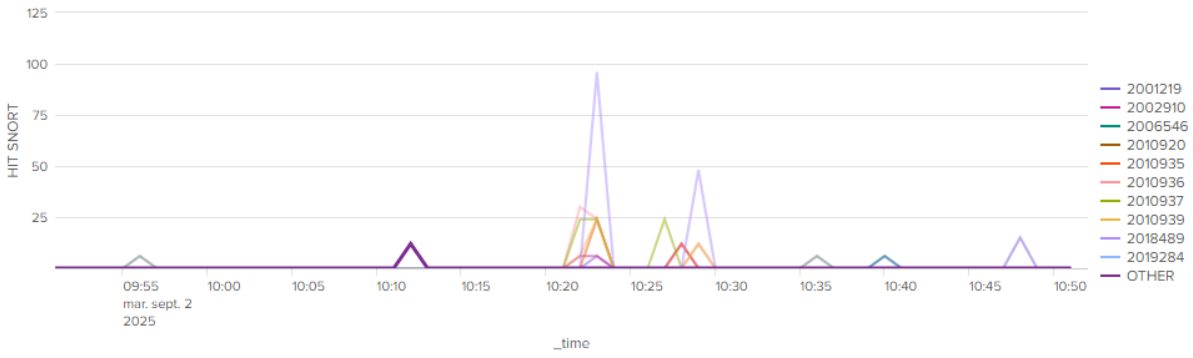
L'objectif de ce rapport est de **surveiller et analyser l'activité réseau détectée par Snort**, en mettant en évidence :

- Les règles Snort qui se sont déclenchées
- Le volume et la récurrence des alertes dans le temps
- L'identification d'éventuelles anomalies ou comportements suspects sur le réseau

Cela permet d'évaluer l'exposition aux menaces, de repérer des scans ou attaques, et de vérifier l'efficacité des mécanismes de détection mis en place sur pfSense.

Recherche splunk associée :

```
index="firewall"  sourcetype=firewall  "snort["
| eval norm=replace(_raw,"(Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec)","\n\\1")
| makemv delim="\n" norm
|  mvexpand norm
| rex "snort\[\d+\]: \[(?<gid>\d+):(?<sid>\d+):(?<rev>\d+)\]"
|  timechart count by sid usenull=false
```



Ce rapport de surveillance contient une série d'alertes de sécurité, principalement axées sur les activités de scan et les tentatives d'exploitation.

Les alertes couvrent les points suivants :

- Scans de ports courants : Détection des tentatives de scan des ports par défaut des bases de données (MSSQL, Oracle SQL, MySQL, PostgreSQL) et du service SSH, qui peuvent indiquer une recherche de vulnérabilités ou de services ouverts.
- Détection du système d'exploitation : Alerte sur les sondes NMAP utilisées pour identifier le système d'exploitation des cibles.
- Tentatives d'injection et d'exploitation web : Identification d'attaques d'injection PHP suspectes et de la présence de commandes exécutées sur le serveur HTTP (comme la commande id, qui pourrait révéler des informations sur l'utilisateur du serveur).

- Attaques par force brute SSH : Détection de connexions SSH fréquentes et suspectes basées sur LibSSH, suggérant une attaque par force brute pour deviner les identifiants.

  2001219 SCAN Potential SSH Scan
  2010935 SCAN Suspicious inbound to MSSQL port 1433
  2010936 SCAN Suspicious inbound to Oracle SQL port 1521
  2010937 SCAN Suspicious inbound to mySQL port 3306
  2010939 SCAN Suspicious inbound to PostgreSQL port 5432
  2018489 SCAN NMAP OS Detection Probe
  2010920 WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)
  2019284 ATTACK_RESPONSE Output of id command from HTTP server
  2006546 SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack
  2060630 INFO TeamViewer RMM Domain

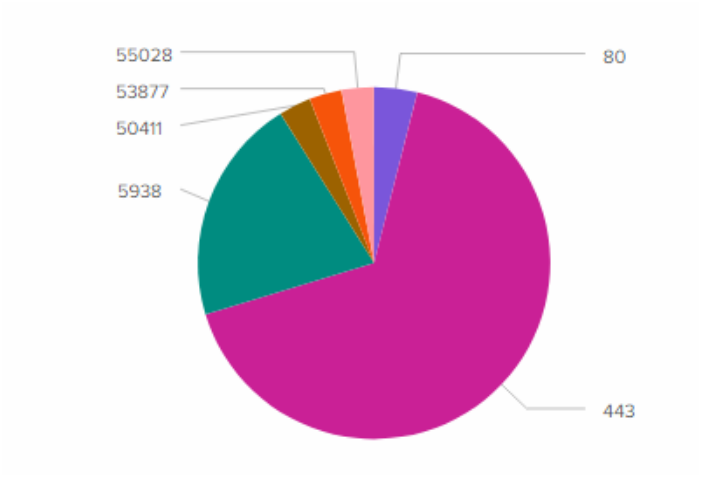
Cela correspond aux techniques :

- ➢ **MITRE ATT&CK T1595 : Active Scanning**
- ➢ **MITRE ATT&CK T1110 : Brute Force**
- ➢ **MITRE ATT&CK T1071 : Application Layer Protocol**
- ➢ **MITRE ATT&CK T1083 : File and Directory Discovery**
- ➢ **MITRE ATT&CK T1190 : Exploit Public-Facing Application**
- ➢ **MITRE ATT&CK T1059 : Command and Scripting Interpreter**

1.4.2 Anomalie réseau : Port utilisés par les postes Windows

Ce graphique circulaire issu de Splunk présente une analyse des événements réseau capturés par Sysmon (Microsoft Windows Sysmon, EventCode=3 qui correspond à une connexion réseau). La commande Splunk affichée agrège le nombre d'événements selon les ports de destination (« DestinationPort »).

```
index="*" sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=3| chart count by DestinationPort
```



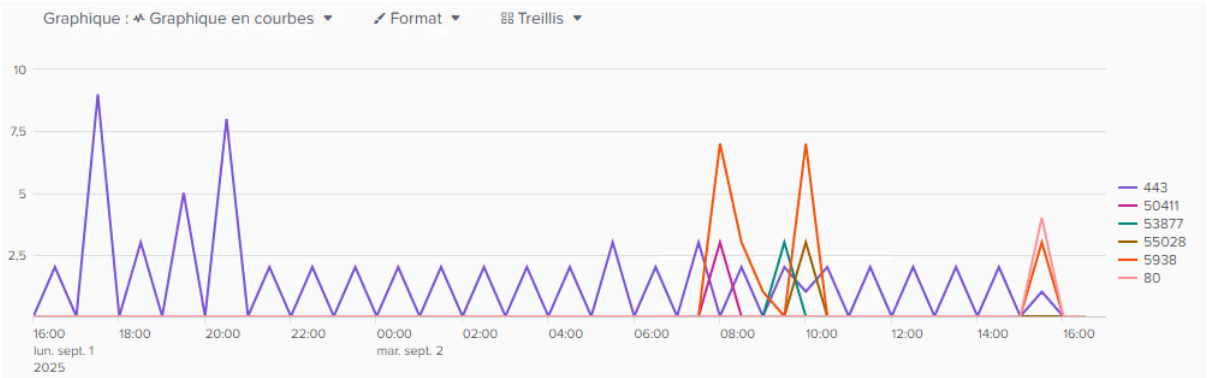
Le port 5938 est utilisé par Teamviewer, les ports élevés (50441, 53877 et 55028) sont souvent liés à des applications spécifiques ou des communications internes/dynamiques.

Cette alerte vise donc à surveiller et à détecter d'éventuels flux inhabituels ou non autorisés sur les ports utilisés, permettant l'analyse proactive de comportements anormaux ou potentiellement malveillants via le suivi des ports de destination.

1.4.3 Anomalie réseau : Port utilisés par les postes Windows par heure

Cette requête analyse les journaux d'événements Windows générés par Sysmon (événements de type 3), ce qui correspond à des connexions réseau détectées sur une machine Windows. Un graphique en courbes affiche le nombre d'événements détectés pour chaque port de destination (comme 443, 80, 50411, etc.) sur une période de temps donnée de 24h.

```
index="*" sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=3| timechart count by DestinationPort
```



Ce type de recherche permet d'identifier facilement des pics d'activité inhabituels ou des comportements suspects (par exemple, échanges soudains sur des ports non standards), utiles pour la supervision de la sécurité ou le dépannage réseau.

2. Gestion des alertes

2.1 Sévérité des alertes

Niveau de sévérité	Nom de l'alerte
Critique	Local File Inclusion
Elevé	Pfsense Blocked List : Machine bloqué par l'IPS
Moyenne	Echec de connexion SSH important /min
Moyenne	Echec de connexion de RDP important /min

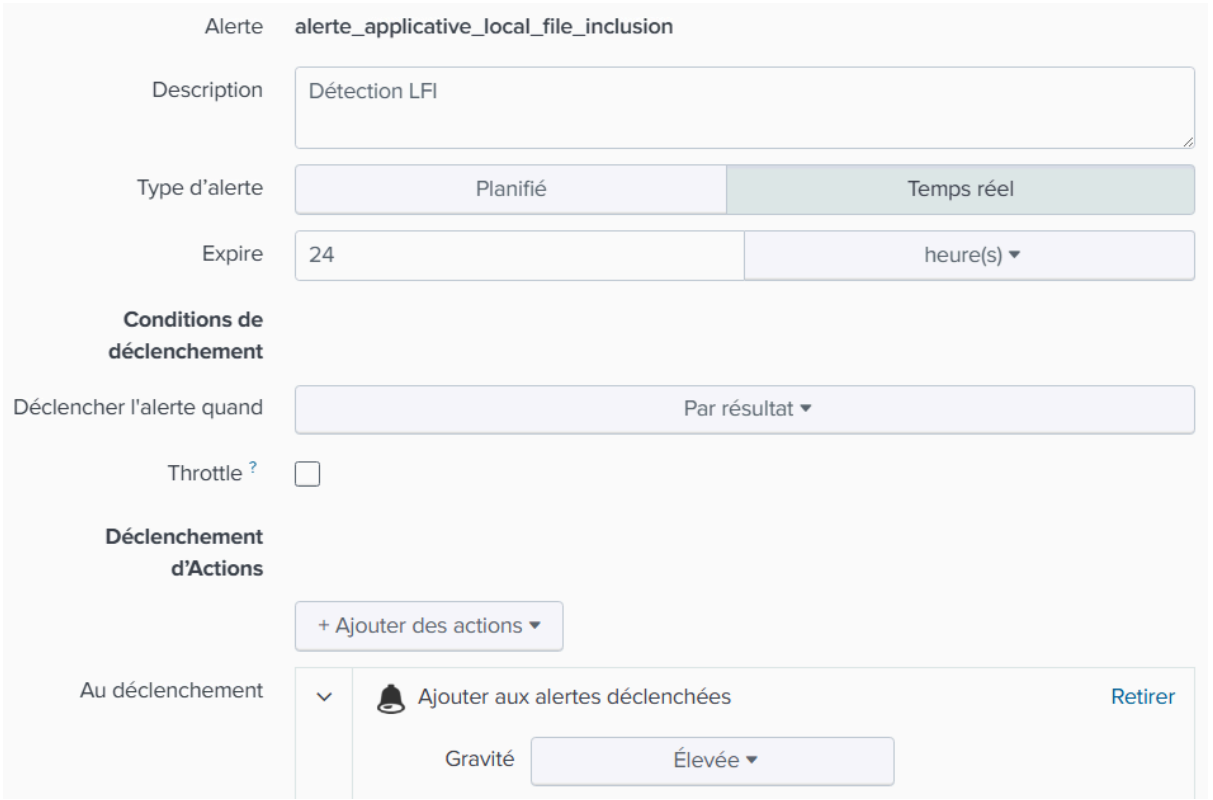
2.2 Liste des alertes

2.2.1 Alerte applicative : Local File Inclusion - Sévérité Critique

Cette alerte vise à détecter des tentatives d'attaque de type Local File Inclusion (LFI) dans les journaux web, par exemple des requêtes contenant include= ou des chemins sensibles comme /etc/passwd dans le paramètre uri_query, afin d'identifier rapidement une exfiltration potentielle de fichiers locaux du serveur et d'y répondre sans délai.

Recherche splunk associée :

Les paramètres de l'alerte Splunk sont :

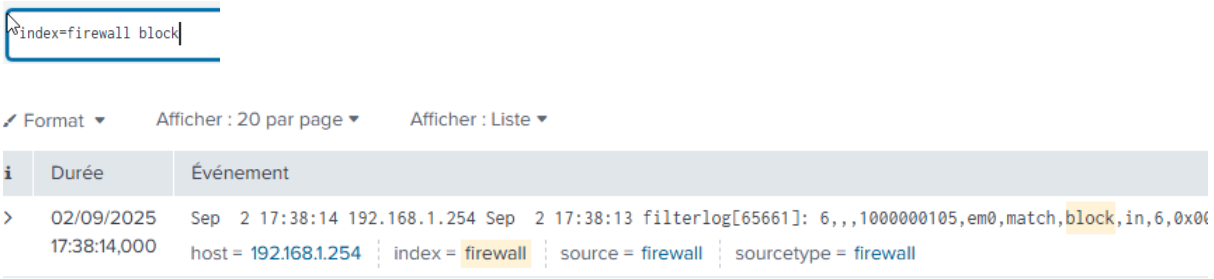


L'alerte se déclenche lorsqu'un résultat a été détecté afin de pouvoir agir rapidement.

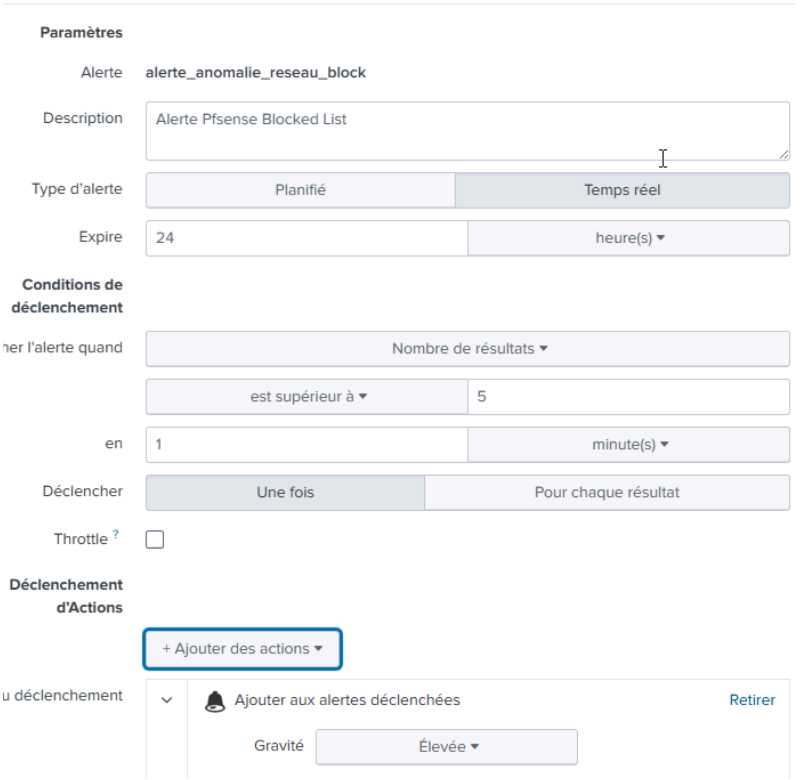
2.2.2 Alerte Pfsense Blocked List : Machine bloqué par l'IPS - Sévérité Elevé

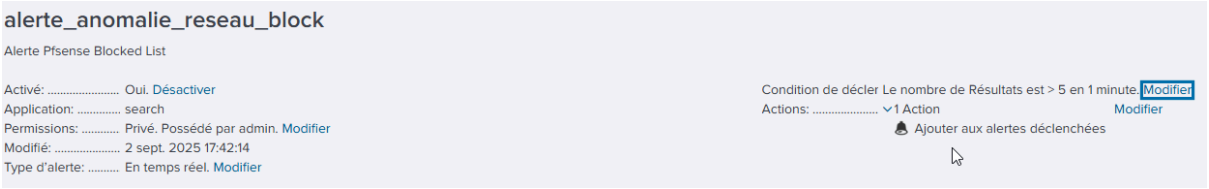
L'objectif de cette alerte Splunk est de détecter un nombre important de blocage par l'IPS Pfsense.

Recherche splunk associée :



Les paramètres de l'alerte Splunk sont :





L'historique du déclenchement de l'alerte :

L'alerte se déclenche lorsqu'un nombre trop important de blocage est enregistré par minute.(> 5 par minute)

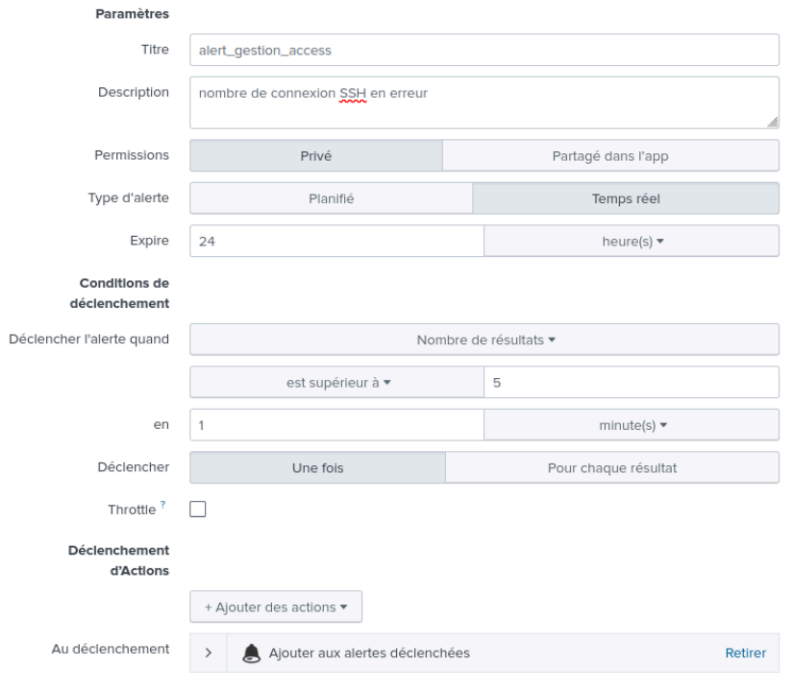
2.2.3 Alerte SSH : Echec de connexion SSH important /min - Sévérité Moyenne

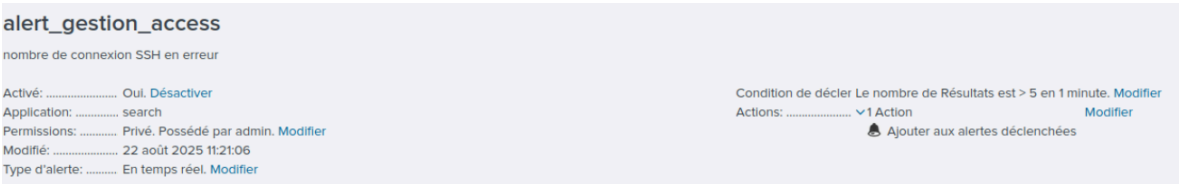
L' objectif de l'alerte Splunk est de détecter les tentatives de connexion SSH infructueuses excessives, potentiellement indicatives d'attaques par force brute.

Recherche splunk associée :

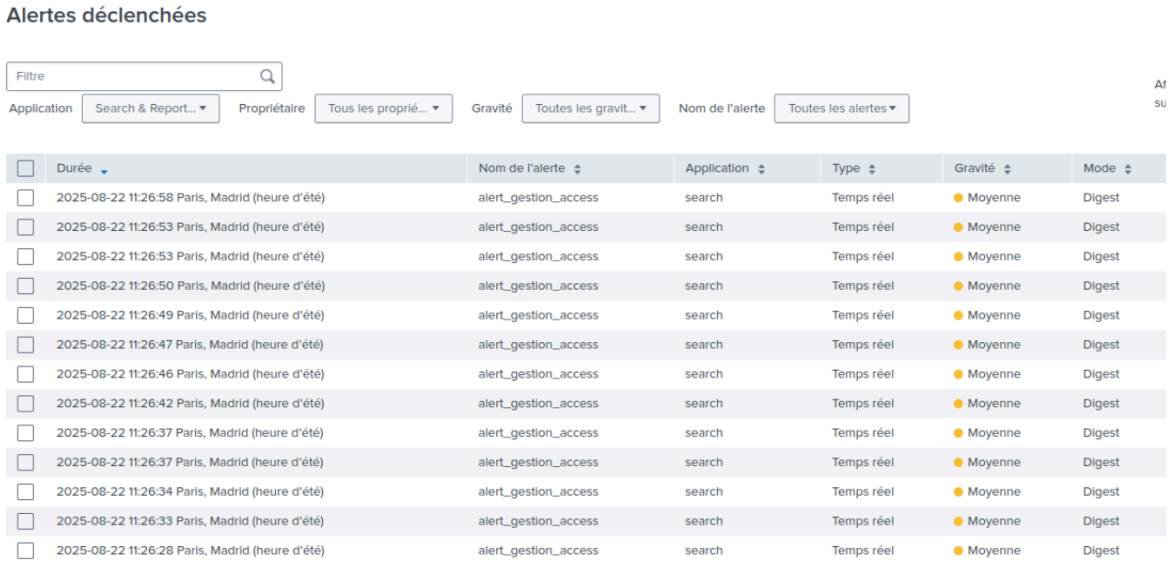
```
source=/var/log/auth.log sshd authentication failure
```

Les paramètres de l'alerte Splunk sont :





L'historique de l'alerte est ci-dessous :

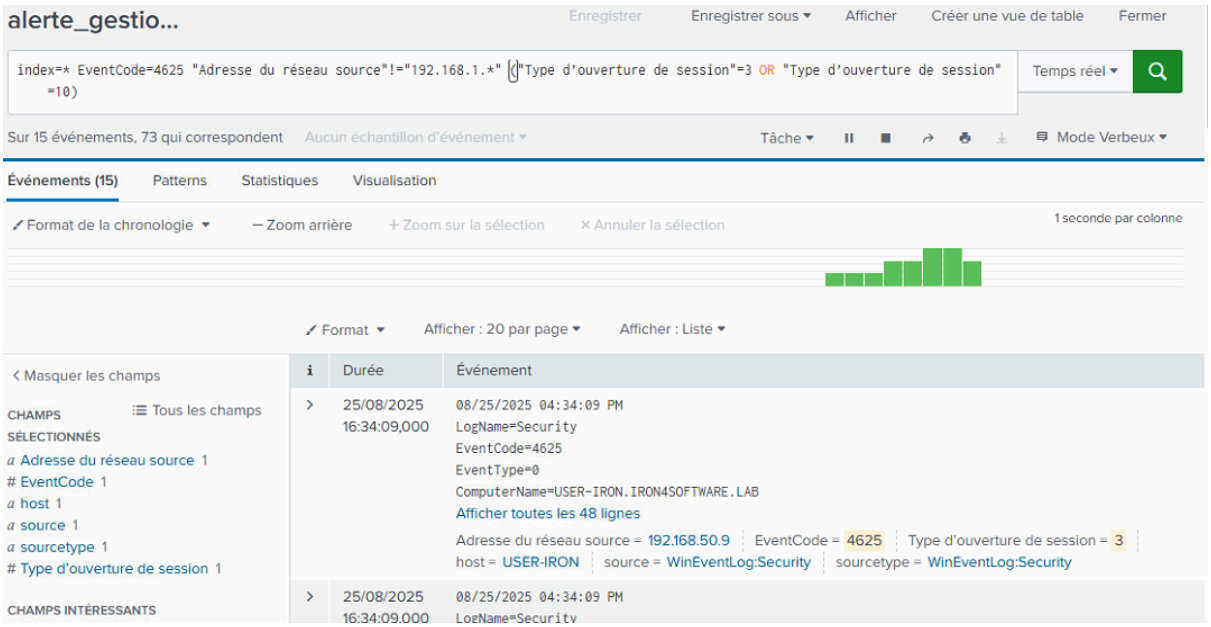


L'alerte se déclenche lorsqu'un nombre trop important d'échecs de connexion SSH est enregistré par minute, indiquant une attaque par force brute SSH.

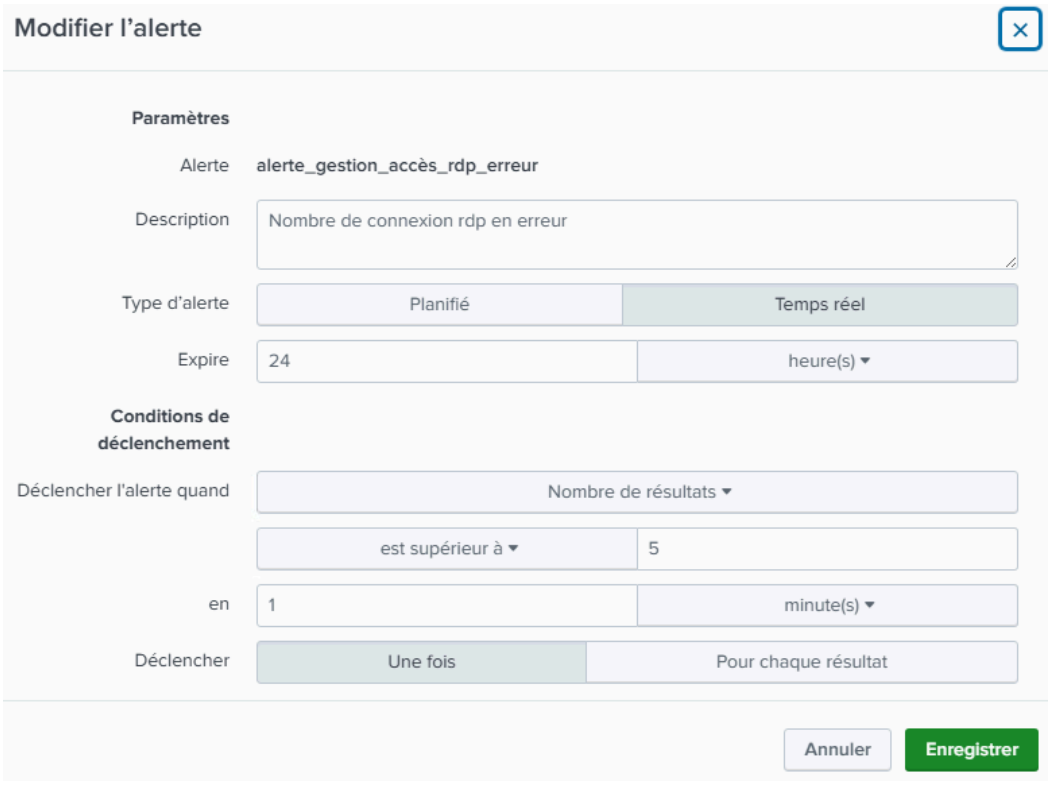
2.2.4 Alerte RDP : Echec de connexion de RDP important /min - Sévérité moyenne

L'objectif de cette alerte Splunk est de détecter et de rapporter les tentatives de connexion RDP échouées provenant d'adresses IP externes (non internes au réseau 192.168.1.*) pour des types de session d'ouverture de session 3 ou 10. Cela permet d'identifier des activités suspectes qui pourraient indiquer des tentatives d'accès non autorisées via RDP.

Recherche splunk associée :



Les paramètres de l'alerte Splunk sont :



alerte_gestion_accès_rdp_erreur

Nombre de connexion rdp en erreur

Activé:	Oui. Désactiver	Condition de déclen	Le nombre de Résultats est > 5 en 1 minute. Modifier
Application:	search	Actions:	1 Action
Permissions:	Privé. Possédé par admin. Modifier		Ajouter aux alertes déclenchées
Modifié:	25 août 2025 16:12:15		Modifier
Type d'alerte:	En temps réel. Modifier		

L'historique du déclenchement de l'alerte :

Historique de déclenchement

20 par page

	Heure de déclenchement	Actions
1	2025-08-25 16:35:38 Paris, Madrid (heure d'été)	Vue Résultats
2	2025-08-25 16:35:34 Paris, Madrid (heure d'été)	Vue Résultats
3	2025-08-25 16:35:33 Paris, Madrid (heure d'été)	Vue Résultats
4	2025-08-25 16:35:31 Paris, Madrid (heure d'été)	Vue Résultats
5	2025-08-25 16:35:31 Paris, Madrid (heure d'été)	Vue Résultats
6	2025-08-25 16:35:29 Paris, Madrid (heure d'été)	Vue Résultats
7	2025-08-25 16:35:29 Paris, Madrid (heure d'été)	Vue Résultats
8	2025-08-25 16:35:29 Paris, Madrid (heure d'été)	Vue Résultats
9	2025-08-25 16:35:24 Paris, Madrid (heure d'été)	Vue Résultats
10	2025-08-25 16:35:21 Paris, Madrid (heure d'été)	Vue Résultats

L'alerte se déclenche lorsqu'un nombre trop important d'échecs de connexion RDP est enregistré par minute.

Conclusion

Ce rapport met en évidence la robustesse du système de détection Splunk Enterprise Security d'Iron4Software. Il permet une identification proactive des menaces (anomalies de gestion de compte, accès non autorisés, attaques applicatives, menaces réseau via Snort) grâce à des tableaux de bord et alertes détaillés.

Les seuils et configurations des alertes sont ajustés pour une réactivité maximale et une minimisation des faux positifs. La classification des alertes par sévérité assure une priorisation efficace des incidents.

Ce système de surveillance permet de réduire les risques d’impact sur les actifs et opérations d’Iron4software, et fera l'objet d'améliorations régulières.