

PROJET 2 : BLOCAGE D'UNE ATTAQUE PAR BRUTE FORCE WAZUH EDR

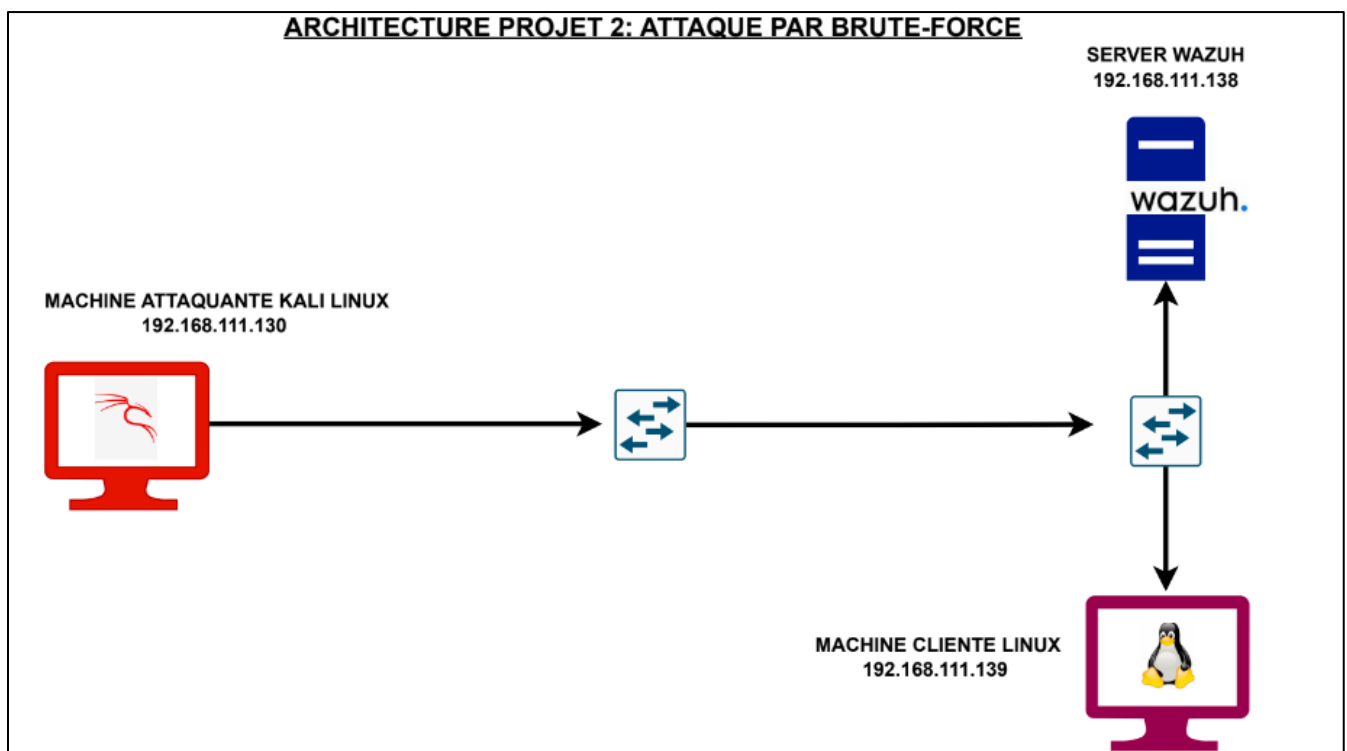
CONTEXTE

Dans ce projet nous allons tenter de bloquer une attaque de type brute-forcing avec notre EDR WAZUH.

Une attaque par force brute (brute-force attack) consiste à tester, l'une après l'autre, chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant donné afin se connecter au service ciblé.

Dans ce laboratoire nous allons lancer une attaque par brute-force en SSH depuis notre machine kali linux vers notre machine Ubuntu. Avec l'EDR WAZUH notre objectif est de détecter ce type d'attaque dans un premier temps puis d'essayer de la bloquer avec le module Active-Response de WAZUH.

ARCHITECTURE DU LAB

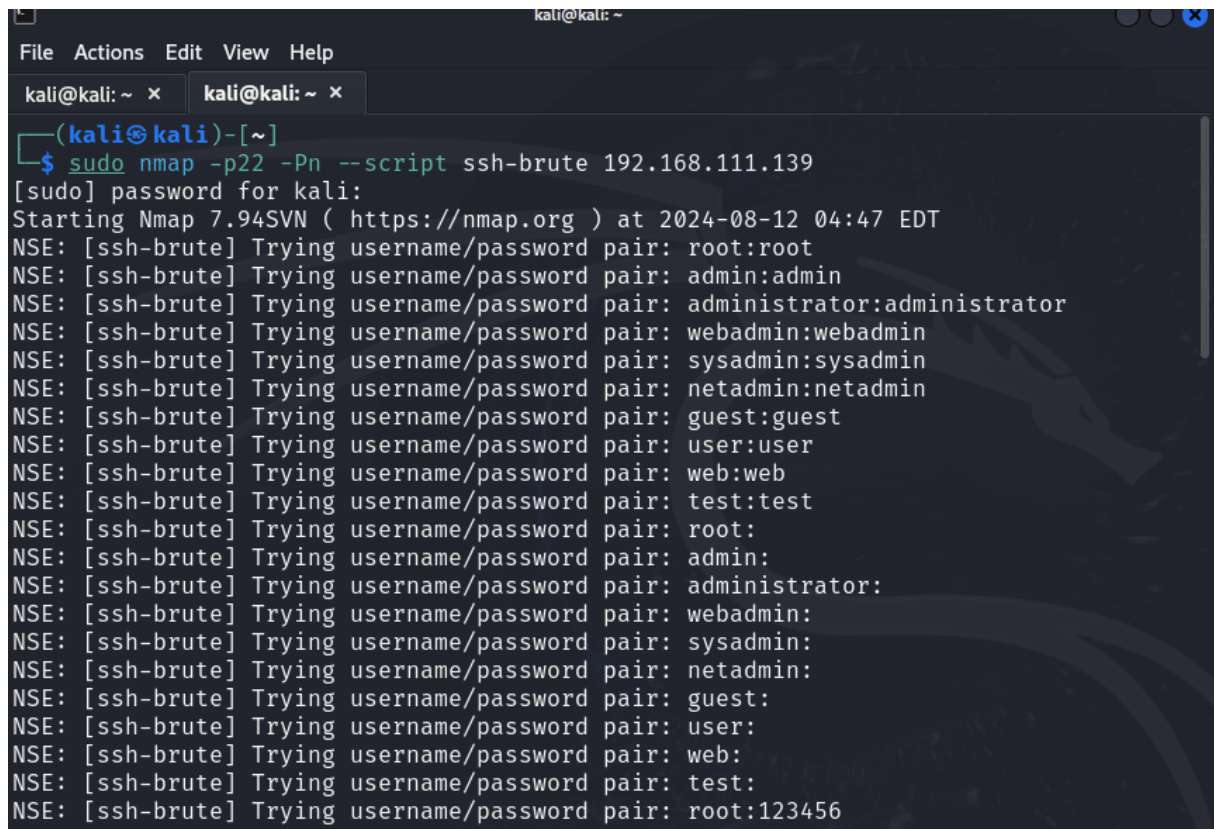


PARTIE 1 : PRÉPARATION DU SCRIPT NMAP DÉTECTION DE L'ATTAQUE

Pour lancer notre attaque nous allons utiliser un petit déjà présent sur NMAP qui nous permettra de brute-forcer la machine Ubuntu cible.

SCRIPT BRUTE-FORCE : `nmap -p 22 -Pn --script ssh-brute 192.168.111.139`

Ce script permettra de lancer une attaque par force brute en SSH qui utilise le port 22, sur la machine cible ayant l'adresse IP 192.168.111.139

A screenshot of a Kali Linux terminal window. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar, there are two tabs, both labeled 'kali@kali: ~'. The terminal shows the command `sudo nmap -p22 -Pn --script ssh-brute 192.168.111.139` being executed. The output shows the Nmap version (7.94SVN) and the start time (2024-08-12 04:47 EDT). It then lists 20 username/password pairs being tested by the ssh-brute script, including root:root, admin:admin, administrator:administrator, webadmin:webadmin, sysadmin:sysadmin, netadmin:netadmin, guest:guest, user:user, web:web, test:test, root:, admin:, administrator:, webadmin:, sysadmin:, netadmin:, guest:, user:, web:, test:, and root:123456.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
(kali@kali)-[~]  
$ sudo nmap -p22 -Pn --script ssh-brute 192.168.111.139  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 04:47 EDT  
NSE: [ssh-brute] Trying username/password pair: root:root  
NSE: [ssh-brute] Trying username/password pair: admin:admin  
NSE: [ssh-brute] Trying username/password pair: administrator:administrator  
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin  
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin  
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin  
NSE: [ssh-brute] Trying username/password pair: guest:guest  
NSE: [ssh-brute] Trying username/password pair: user:user  
NSE: [ssh-brute] Trying username/password pair: web:web  
NSE: [ssh-brute] Trying username/password pair: test:test  
NSE: [ssh-brute] Trying username/password pair: root:  
NSE: [ssh-brute] Trying username/password pair: admin:  
NSE: [ssh-brute] Trying username/password pair: administrator:  
NSE: [ssh-brute] Trying username/password pair: webadmin:  
NSE: [ssh-brute] Trying username/password pair: sysadmin:  
NSE: [ssh-brute] Trying username/password pair: netadmin:  
NSE: [ssh-brute] Trying username/password pair: guest:  
NSE: [ssh-brute] Trying username/password pair: user:  
NSE: [ssh-brute] Trying username/password pair: web:  
NSE: [ssh-brute] Trying username/password pair: test:  
NSE: [ssh-brute] Trying username/password pair: root:123456
```

Après lancement de l'attaque par brute-force, nous constatons sur le tableau de bord de WAZUH que l'attaque a été détectée avec un nombre de **611 tentatives de connexion** qui ont échoué.

Nous pouvons également constater sur les autres images du tableau de bord qu'il s'agit d'une technique de « **CREDENTIAL ACCES, LATERALE MOVEMENT** » c'est-à-dire une tentative de connexion en essayant plusieurs combinaisons de login et de mots de passe avec comme objectif un gain d'accès au système.

Dashboard Events

mdiawlinux (001)

Generate report

Search

DQL

~ a day ago → now

Refresh

manager.name: wazuh-server agent.id: 001 + Add filter

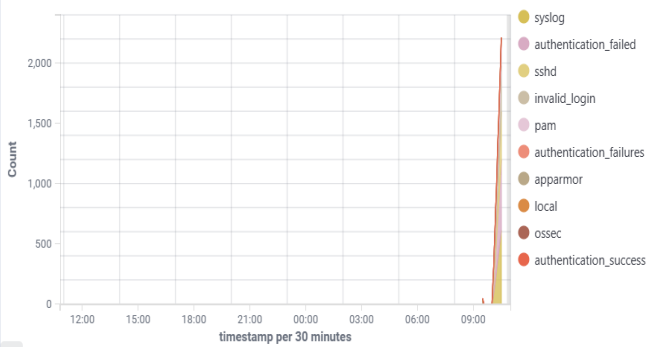
Total
631

Level 12 or above alerts
0

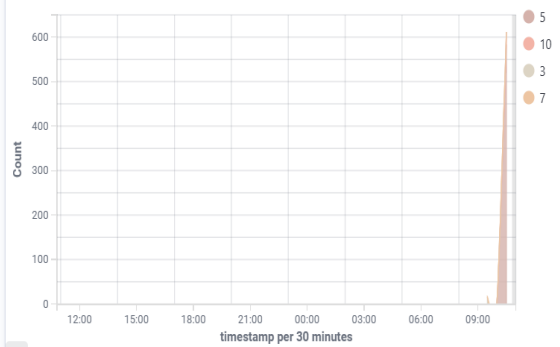
Authentication failure
611

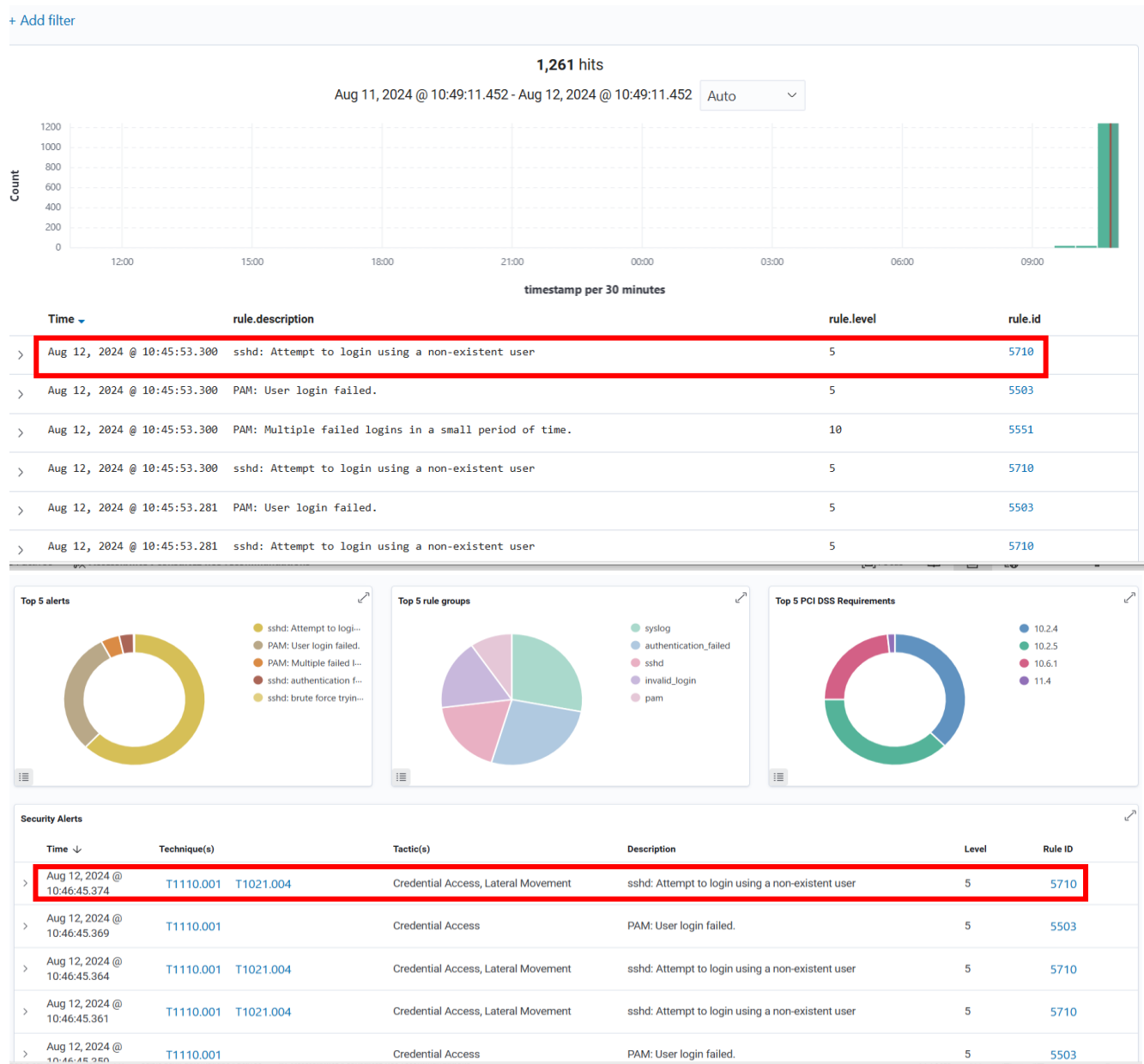
Authentication success
2

Top 10 Alert groups evolution



Alerts





PARTIE 2 : BLOCAGE DE L'ATTAQUE PAR BRUTE-FORCE AVEC UNE REGLE WAZUH

Dans la partie 2 nous avons lancer et détecter une attaque brute-force. L'objectif maintenant est créer une règle qui bloque un lancement d'une telle attaque avec le module ACTIVE-RESPONSE DE WAZUH.

Avant d'écrire la règle de blocage nous devons connaitre l'identifiant de la règle wazuh qui permet de détecter une attaque par brute force.

Pour ce faire, nous ouvrons le fichier de configuration des règles ssh sur WAZUH : 0095-sshd_rules.xml. Nous pouvons voir que l'identifiant de la règle est **5712**

```

<rule id="5712" level="10" frequency="8" timeframe="120" ignore="60">
  <it_matched_sid>5710</it_matched_sid>
  <same_source ip />
  <description>sshd: brute force trying to get access to the system. Non existent user.</description>
  <mitre>
    <id>T1110</id>
  </mitre>
  <group>authentication_failures,gdpr_IV_35.7.d,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_SI.4,nist_800_53_AU.14,nist_800_53_AC.7,pci_dss_11.4,pci_dss_10.2.4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
</rule>

```

-REGLE DE BLOCAGE WAZUH ET EXPLICATION

Une fois activée, cette règle permettra de bloquer pendant 180 secondes toute tentative d'attaque par brute-force avec SSH sur la machine cible ubuntu.

<active-response>

<command>firewall-drop</command>

<location>defined-agent</location>

<agent_id>001</agent_id>

<rules_id>5712</rules_id>

<timeout>180</timeout>

</active-response>

PARTIE 3 : VÉRIFICATION DE LA REGLE DE BLOCAGE

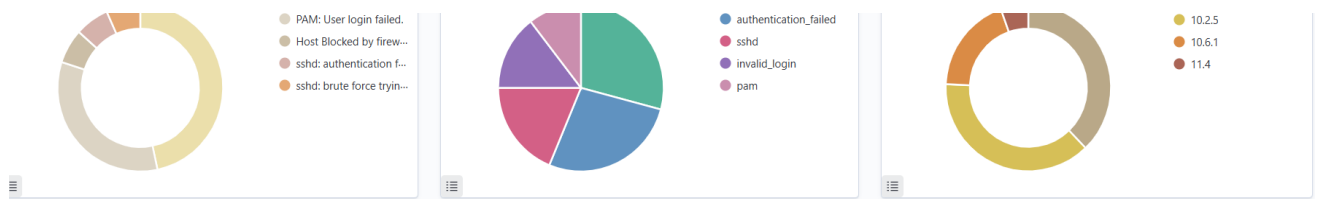
Après l'établissement de la règle de blocage, nous allons retenter une attaque par brute-force afin d'évaluer si notre règle marche ou pas.

Cette fois ci nous pouvons constater que l'attaque par brute-force a été détectée et bloquée par la règle ACTIVE-RESPONSE nous avons mis en place sur WAZUH.

Même le PING (protocole ICMP) ne passe plus, le contact entre la machine attaque et la cible est rompu.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
  
(kali@kali)-[~]  
$ sudo nmap -p22 -Pn --script ssh-brute 192.168.111.139  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 06:25 EDT  
NSE: [ssh-brute] Trying username/password pair: root:root  
NSE: [ssh-brute] Trying username/password pair: admin:admin  
NSE: [ssh-brute] Trying username/password pair: administrator:administrator  
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin  
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin  
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin  
NSE: [ssh-brute] Trying username/password pair: guest:guest  
NSE: [ssh-brute] Trying username/password pair: user:user  
NSE: [ssh-brute] Trying username/password pair: web:web  
NSE: [ssh-brute] Trying username/password pair: test:test  
NSE: [ssh-brute] Trying username/password pair: root:  
NSE: [ssh-brute] Trying username/password pair: admin:  
Stats: 0:06:16 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 94.59% done; ETC: 06:32 (0:00:21 remaining)  
Stats: 0:06:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 94.59% done; ETC: 06:32 (0:00:22 remaining)  
Stats: 0:06:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 94.74% done; ETC: 06:33 (0:00:23 remaining)
```

```
(kali@kali)-[~]  
$ ping 192.168.111.139  
PING 192.168.111.139 (192.168.111.139) 56(84) bytes of data.
```



Security Alerts

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 12, 2024 @ 12:22:50.931			Host Blocked by firewall-drop Active Response	3	651
> Aug 12, 2024 @ 12:22:50.833	T1110	Credential Access	sshd: brute force trying to get access to the system. Non existent user.	10	5712
> Aug 12, 2024 @ 12:22:50.831	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760
> Aug 12, 2024 @ 12:22:50.829	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Aug 12, 2024 @ 12:22:50.826	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
> Aug 12, 2024 @ 12:22:50.823	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

+ Add filter

15 hits

Aug 12, 2024 @ 12:21:21.060 - Aug 12, 2024 @ 12:29:21.060

Auto



Time	rule.description	rule.level	rule.id
> Aug 12, 2024 @ 12:22:50.931	Host Blocked by firewall-drop Active Response	3	651
> Aug 12, 2024 @ 12:22:50.833	sshd: brute force trying to get access to the system. Non existent user.	10	5712
> Aug 12, 2024 @ 12:22:50.831	sshd: authentication failed.	5	5760
> Aug 12, 2024 @ 12:22:50.829	sshd: Attempt to login using a non-existent user	5	5710
> Aug 12, 2024 @ 12:22:50.826	sshd: Attempt to login using a non-existent user	5	5710
> Aug 12, 2024 @ 12:22:50.823	sshd: Attempt to login using a non-existent user	5	5710

Search

DQL

Last 8 minutes

Show dates

Refresh

manager.name: wazuh-server

agent.id: 001

+ Add filter

Total

33

Level 12 or above alerts

0

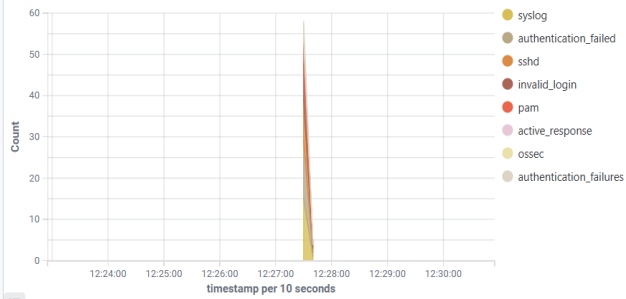
Authentication failure

30

Authentication success

0

Top 10 Alert groups evolution



Alerts

