☐ Minimo 10 controles hardening

- **SELinux en modo enforcing**

getenfoce

```
[ile@localhost hips-so2]$ getenforce
Enforcing
[ile@localhost hips-so2]$
```

- **firewalld con zona restrictiva**

sudo firewall-cmd –list-all || true

sudo systemctl status firewalld

```
[ile@localhost hips-so2]$ sudo firewall-cmd --list-all || true
public (active)
  target: DROP
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[ile@localhost hips-so2]$ sudo systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
     Active: active (running) since Fri 2026-07-10 14:24:57 -03; 14min ago
       Docs: man:firewalld(1)
   Main PID: 869 (firewalld)
      Tasks: 4 (limit: 60668)
     Memory: 47.2M (peak: 47.5M)
        CPU: 970ms
     CGroup: /system.slice/firewalld.service
             └─869 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid
```

- **SSH con acceso restringido**

sudo sshd -T | grep -E 'permitrootlogin|passwordauthentication|pubkeyauthentication'

```
maxauthtries 3
permitrootlogin no
pubkeyauthentication yes
passwordauthentication no
kbdinteractiveauthentication no
permitemptypasswords no
banner /etc/issue.net
```

- **/tmp montado con noexec, nosuid, nodev**

  Evita que scripts o binarios dejados por un atacante en /tmp se ejecuten fácilmente.

cat /etc/fstab

```
[ile@localhost hips-so2]$ cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Tue Jul  7 14:28:07 2026
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
/dev/mapper/rl-root     /                       xfs     defaults        0 0
UUID=b4a3fcd8-5c03-4d73-8ef1-f23f6dd19b5a /boot                   xfs     defaults        0 0
/dev/mapper/rl-swap     none                    swap    defaults        0 0
tmpfs /tmp tmpfs defaults,noexec,nosuid,nodev,mode=1777 0 0
[ile@localhost hips-so2]$
```

- **auditd activo con reglas personalizadas**

  Audita cambios o accesos importantes, especialmente en /etc/passwd, /etc/shadow, /etc/sudoers y comandos privilegiados.

sudo systemctl status auditd

sudo auditctl -l

```
[ile@localhost hips-so2]$ sudo systemctl status auditd
[sudo] contraseña para ile:
● auditd.service - Security Auditing Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: enabled)
     Active: active (running) since Fri 2026-07-10 14:24:55 -03; 39min ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
   Main PID: 782 (auditd)
      Tasks: 4 (limit: 60668)
     Memory: 12.0M (peak: 13.1M)
        CPU: 316ms
     CGroup: /system.slice/auditd.service
             ├782 /sbin/auditd
             └784 /usr/sbin/sedispatch

jul 10 14:24:55 localhost augenrules[803]: enabled 1
jul 10 14:24:55 localhost augenrules[803]: failure 1
jul 10 14:24:55 localhost augenrules[803]: pid 782
jul 10 14:24:55 localhost augenrules[803]: rate_limit 0
jul 10 14:24:55 localhost augenrules[803]: backlog_limit 8192
jul 10 14:24:55 localhost augenrules[803]: lost 0
jul 10 14:24:55 localhost augenrules[803]: backlog 0
jul 10 14:24:55 localhost augenrules[803]: backlog_wait_time 60000
jul 10 14:24:55 localhost augenrules[803]: backlog_wait_time_actual 0
jul 10 14:24:55 localhost systemd[1]: Started Security Auditing Service.
[ile@localhost hips-so2]$ sudo auditctl -l
-w /etc/passwd -p wa -k hips_identity
-w /etc/shadow -p wa -k hips_identity
-w /etc/sudoers -p wa -k hips_sudoers
-w /etc/sudoers.d -p wa -k hips_sudoers
-w /var/log/hips -p wa -k hips_logs
-a always,exit -F arch=b64 -S execve -F euid=0 -F key=hips_privileged_exec
-a always,exit -F arch=b32 -S execve -F euid=0 -F key=hips_privileged_exec
[ile@localhost hips-so2]$
```

- **Principio de mínimo privilegio**

El servicio HIPS corre con usuario dedicado y permisos limitados, no como root. También se verifica que no haya cuentas extra con UID 0.

sudo systemctl status hips

```
[ile@localhost hips-so2]$ sudo systemctl status hips
● hips.service - HIPS - deteccion y prevencion automatica
     Loaded: loaded (/etc/systemd/system/hips.service; static)
     Active: activating (start) since Fri 2026-07-10 15:11:11 -03; 26ms ago
TriggeredBy: ● hips.timer
   Main PID: 5695 (python3)
      Tasks: 1 (limit: 60668)
     Memory: 4.7M (peak: 4.7M)
        CPU: 16ms
     CGroup: /system.slice/hips.service
             └5695 /usr/bin/python3 /home/ile/hips-so2/hips.py --guardar-db --enviar-email --prevenir --json

jul 10 15:11:11 localhost.localdomain systemd[1]: Starting HIPS - deteccion y prevencion automatica...
```

En un servicio oneshot, eso está bien. No debe quedar “active running”; corre una vez, termina correctamente y el timer lo vuelve a ejecutar.

- **Servicios innecesarios deshabilitados**

Se deshabilitan servicios que no hacen falta, como avahi-daemon, cups, bluetooth, nfs y rpcbind.

systemctl status avahi-daemon cups bluetooth nfs-server rpcbind

```
[ile@localhost hips-so2]$ systemctl status avahi-daemon cups bluetooth nfs-server rpcbind
Unit nfs-server.service could not be found.
Unit rpcbind.service could not be found.
○ avahi-daemon.service - Avahi mDNS/DNS-SD Stack
     Loaded: loaded (/usr/lib/systemd/system/avahi-daemon.service; disabled; preset: enabled)
     Active: inactive (dead)
TriggeredBy: ○ avahi-daemon.socket

○ cups.service - CUPS Scheduler
     Loaded: loaded (/usr/lib/systemd/system/cups.service; disabled; preset: enabled)
    Drop-In: /usr/lib/systemd/system/cups.service.d
             └─10-foomaticrip-upgrade.conf, server.conf
     Active: inactive (dead)
TriggeredBy: ○ cups.socket
       Docs: man:cupsd(8)

○ bluetooth.service - Bluetooth service
     Loaded: loaded (/usr/lib/systemd/system/bluetooth.service; disabled; preset: enabled)
     Active: inactive (dead)
       Docs: man:bluetoothd(8)

jul 10 14:25:13 localhost.localdomain systemd[1]: Bluetooth service was skipped because of an unmet condition check (ConditionPathIsDirectory=/sys/class/bluetooth).
Tiene correo nuevo en /var/spool/mail/ile
[ile@localhost hips-so2]$
[ile@localhost hips-so2]$
```

- **Banner de login y aviso legal**

Se configura un mensaje de advertencia en /etc/issue.net o /etc/motd para accesos no autorizados.

sudo sshd -T | grep banner

cat /etc/issue.net

```
[ile@localhost hips-so2]$ sudo sshd -T | grep banner
[sudo] contraseña para ile:
banner /etc/issue.net
Tiene correo nuevo en /var/spool/mail/ile
[ile@localhost hips-so2]$ cat /etc/issue.net
ACCESO RESTRINGIDO - Sistema HIPS
Solo personal autorizado. Toda actividad puede ser monitoreada y registrada.
[ile@localhost hips-so2]$
```

- **Actualizaciones automáticas de seguridad**

Uso de dnf-automatic para aplicar parches de seguridad automáticamente.

rpm -q dnf-automatic

systemctl status dnf-automatic.timer

```
[ile@localhost hips-so2]$ rpm -q dnf-automatic
dnf-automatic-4.14.0-34.el9_8.rocky.0.1.noarch
Tiene correo nuevo en /var/spool/mail/ile
[ile@localhost hips-so2]$ systemctl status dnf-automatic.timer
● dnf-automatic.timer - dnf-automatic timer
     Loaded: loaded (/usr/lib/systemd/system/dnf-automatic.timer; enabled; preset: disabled)
     Active: active (waiting) since Fri 2026-07-10 14:31:09 -03; 58min ago
      Until: Fri 2026-07-10 14:31:09 -03; 58min ago
    Trigger: Sat 2026-07-11 06:50:31 -03; 15h left
   Triggers: ● dnf-automatic.service

jul 10 14:31:09 localhost.localdomain systemd[1]: Started dnf-automatic timer.
```

grep -E 'apply_updates|upgrade_type' /etc/dnf/automatic.conf

```
[ile@localhost hips-so2]$ grep -E 'apply_updates|upgrade_type' /etc/dnf/automatic.conf
upgrade_type = security
apply_updates = yes
```

- **Permisos restrictivos en archivos críticos**

Permisos seguros para /etc/passwd, /etc/shadow, /etc/sudoers y /var/log/hips/.

ls -l /etc/passwd /etc/shadow /etc/sudoers

```
[ile@localhost hips-so2]$ ls -l /etc/passwd /etc/shadow /etc/sudoers
-rw-r--r--. 1 root root 2054 jul  9 15:43 /etc/passwd
----------. 1 root root 1114 jul  9 15:43 /etc/shadow
-r--r-----. 1 root root 4328 may 19 21:55 /etc/sudoers
Tiene correo nuevo en /var/spool/mail/ile
[ile@localhost hips-so2]$
```

ls -ld /var/log/hips

```
[ile@localhost hips-so2]$ ls -ld /var/log/hips
drwxr-x---. 2 hips_svc hips_group 76 jul  8 16:42 /var/log/hips
```

ls -l /var/log/hips

```
[ile@localhost hips-so2]$ ls -l /var/log/hips
ls: no se puede abrir el directorio '/var/log/hips': Permiso denegado
```

☐ Postgres sql Instalado Y Configurado

rpm -q postgresql-server

```
[ile@localhost hips-so2]$ rpm -q postgresql-server
postgresql-server-13.23-2.el9_7.x86_64
```

☐ 7 buenas practicas Hardening (CIS) en la base de datos

- **Usuario de aplicación sin superusuario**

La app usa hips_app, con permisos limitados solo sobre hips_db. No se usa postgres desde la aplicación.

PGPASSWORD="hips_app_local_123" psql -h 127.0.0.1 -U hips_app -d hips_db -c "SELECT current_user, current_database(); SELECT usename, usesuper FROM pg_user WHERE usename='hips_app';"

```
[ile@localhost hips-so2]$ PGPASSWORD="hips_app_local_123" psql -h 127.0.0.1 -U hips_app -d hips_db -c "SELECT current_user, current_database(); SELECT usename, usesuper FROM pg_user WHERE usename='hips_app';"
 usename  | usesuper
----------+----------
 hips_app | f
(1 fila)
```

- **SSL activo**

PostgreSQL tiene ssl = on, para cifrar conexiones cliente-servidor.

sudo -u postgres psql -d hips_db -c "SHOW ssl;"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "SHOW ssl;"
could not change directory to "/home/ile/hips-so2": Permiso denegado
 ssl
-----
 on
(1 row)
```

- **Registro de conexiones y desconexiones**

Se activan logs para saber quién se conecta y cuándo se desconecta.

sudo -u postgres psql -d hips_db -c "SELECT name, setting FROM pg_settings WHERE name IN ('log_connections','log_disconnections') ORDER BY name;"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "SELECT name, setting FROM pg_settings WHERE name IN ('log_connections','log_disconnections') ORDER BY name;"
could not change directory to "/home/ile/hips-so2": Permiso denegado
        name        | setting
-------------------+---------
 log_connections    | on
 log_disconnections | on
(2 rows)
```

- **listen_addresses restringido a localhost**

PostgreSQL solo escucha en localhost, no en interfaces externas.

sudo -u postgres psql -d hips_db -c "SHOW listen_addresses;"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "SHOW listen_addresses;"
could not change directory to "/home/ile/hips-so2": Permiso denegado
 listen_addresses
------------------
 localhost
(1 row)
```

- **password_encryption = scram-sha-256**

Las contraseñas se almacenan con SCRAM-SHA-256, más seguro que MD5.

sudo -u postgres psql -d hips_db -c "SHOW password_encryption;"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "SHOW password_encryption;"
could not change directory to "/home/ile/hips-so2": Permiso denegado
 password_encryption
---------------------
 scram-sha-256
(1 row)
```

- **Registro de errores de autenticación**

Se registran errores de conexión/autenticación para alimentar la detección de intentos inválidos.

sudo -u postgres psql -d hips_db -c "SHOW log_min_error_statement;"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "SHOW log_min_error_statement;"
could not change directory to "/home/ile/hips-so2": Permiso denegado
 log_min_error_statement
-------------------------
 error
(1 row)
```

- **pg_hba.conf solo local con SCRAM**

Solo se permite conexión desde 127.0.0.1/32 usando scram-sha-256; cualquier otra fuente queda restringida.

sudo grep -Ev '^\s*#|^\s*$' /var/lib/pgsql/data/pg_hba.conf

```
[ile@localhost hips-so2]$ sudo grep -Ev '^\s*#|^\s*$' /var/lib/pgsql/data/pg_hba.conf
host    hips_db      hips_app      127.0.0.1/32      scram-sha-256
host    hips_db      hips_app      ::1/128           scram-sha-256
local   all             all                                     peer
host    all             all             127.0.0.1/32            ident
host    all             all             ::1/128                 ident
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            ident
host    replication     all             ::1/128                 ident
```

☐ Permisos de acceso de datos a la bd restringidos

- **Ver los privilegios sobre la base de datos**

sudo -u postgres psql -c "\l+"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -c "\l+"
[sudo] contraseña para ile:
could not change directory to "/home/ile/hips-so2": Permiso denegado
                                                    List of databases
   Name    |  Owner   | Encoding |   Collate   |    Ctype    |   Access privileges   |  Size   | Tablespace |                Description
-----------+----------+----------+-------------+-------------+-----------------------+---------+------------+-------------------------------------------
 hips_db   | hips_app | UTF8     | es_PY.UTF-8 | es_PY.UTF-8 |                       | 8959 kB | pg_default |
 postgres  | postgres | UTF8     | es_PY.UTF-8 | es_PY.UTF-8 |                       | 8231 kB | pg_default | default administrative connection database
 template0 | postgres | UTF8     | es_PY.UTF-8 | es_PY.UTF-8 | =c/postgres          +| 8081 kB | pg_default | unmodifiable empty database
           |          |          |             |             | postgres=CTc/postgres |         |            |
 template1 | postgres | UTF8     | es_PY.UTF-8 | es_PY.UTF-8 | =c/postgres          +| 8081 kB | pg_default | default template for new databases
           |          |          |             |             | postgres=CTc/postgres |         |            |
(4 rows)

Tiene correo nuevo en /var/spool/mail/ile
[ile@localhost hips-so2]$
```

- **solo para hips_db:**

sudo -u postgres psql -c "\l+ hips_db"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -c "\l+ hips_db"
could not change directory to "/home/ile/hips-so2": Permiso denegado
                                                    List of databases
  Name   |  Owner   | Encoding |   Collate   |    Ctype    | Access privileges |  Size   | Tablespace | Description
---------+----------+----------+-------------+-------------+-------------------+---------+------------+-------------
 hips_db | hips_app | UTF8     | es_PY.UTF-8 | es_PY.UTF-8 |                   | 8959 kB | pg_default |
(1 row)
```

Ahí vas a ver quién tiene permisos sobre la base de datos.

- **Ver los privilegios del usuario hips_app**

sudo -u postgres psql -d hips_db -c "\du hips_app"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "\du hips_app"
could not change directory to "/home/ile/hips-so2": Permiso denegado
           List of roles
 Role name | Attributes | Member of
-----------+------------+-----------
 hips_app  |            | {}

[ile@localhost hips-so2]$
```

```
sudo -u postgres psql -c "
SELECT rolname,
       rolsuper,
       rolcreatedb,
       rolcreaterole,
       rolreplication
FROM pg_roles
WHERE rolname='hips_app';"
```

```
 rolname  | rolsuper | rolcreatedb | rolcreaterole | rolreplication
----------+----------+-------------+---------------+----------------
 hips_app | f        | f           | f             | f
(1 row)
```

☐ Ninguna contrasena expuesta en el código fuente

```
grep -RniE 'password|passwd|pwd|secret|token|api[_-]?key|PGPASSWORD' . \
  --exclude-dir=.git \
  --exclude='*.png' \
  --exclude='*.jpg'
```

Checklist de esta medida

Verificación	Estado	Evidencia
La contraseña de BD no está hardcodeada	✅	`db/connection.py` usa `os.environ.get("HIPS_DB_PASSWORD")`. Pasted text
La contraseña web no está hardcodeada	✅	`HIPS_WEB_PASSWORD` se obtiene desde variable de entorno. Pasted text
La clave secreta web no está hardcodeada	✅	`HIPS_WEB_SECRET_KEY` se obtiene desde variable de entorno y si falta lanza error. Pasted text
Los archivos de ejemplo no contienen secretos reales	✅	`hips.env.example` usa placeholders tipo `CAMBIAR_ESTA_CONTRASENA`. Pasted text
Los valores en tests son ficticios	✅	Aparecen valores como `"clave-test"` y `"secreto"` en pruebas, no credenciales productivas. Pasted text

Copy table

☐ en particion o carpeta encriptada o en bd

La configuración de módulos, umbrales e intervalos del HIPS se almacena en la base de datos PostgreSQL, no en archivos planos del sistema. Además, las credenciales sensibles fueron movidas fuera del repositorio a /etc/hips/hips.env con permisos restrictivos.

sudo -u postgres psql -d hips_db -c "SELECT modulo, habilitado, intervalo_segundos, umbral, configuracion FROM configuracion_modulos ORDER BY modulo;"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "SELECT modulo, habilitado, intervalo_segundos, umbral, configuracion FROM configuracion_modulos ORDER BY modulo;"
[sudo] contraseña para ile:
could not change directory to "/home/ile/hips-so2": Permiso denegado
       modulo        | habilitado | intervalo_segundos | umbral |                configuracion
---------------------+------------+--------------------+--------+----------------------------------------------
 auth_failures       | t          |                 60 |      5 | {}
 cron_monitor        | t          |                 60 |        | {}
 ddos_monitor        | t          |                 30 |     50 | {}
 integridad_archivos | t          |                 60 |        | {}
 mail_queue          | t          |                 60 |     20 | {}
 process_monitor     | t          |                 60 |        | {}
 sniffers            | t          |                 60 |        | {}
 system_logs         | t          |                 60 |        | {}
 tmp_monitor         | t          |                 60 |        | {}
 user_monitor        | t          |                 60 |        | {"login_hora_fin": 23, "login_hora_inicio": 0}
(10 rows)

Tiene correo nuevo en /var/spool/mail/ile
[ile@localhost hips-so2]$
```

☐ Baseline de binarios generado y guardado de forma segura

sudo -u postgres psql -d hips_db -c "\dt"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "\dt"
[sudo] contraseña para ile:
could not change directory to "/home/ile/hips-so2": Permiso denegado
                 List of relations
 Schema |          Name           | Type  |  Owner
--------+-------------------------+-------+----------
 public | acciones_prevencion     | table | hips_app
 public | alarmas                 | table | hips_app
 public | baseline_archivos       | table | hips_app
 public | configuracion_modulos   | table | postgres
 public | eventos_sistema         | table | hips_app
 public | usuarios_web            | table | hips_app
(6 rows)
```

sudo -u postgres psql -d hips_db -c "\d baseline_archivos"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "\d baseline_archivos"
could not change directory to "/home/ile/hips-so2": Permiso denegado
                                      Table "public.baseline_archivos"
     Column     |            Type             | Collation | Nullable |                   Default
----------------+-----------------------------+-----------+----------+-----------------------------------------------
 id             | integer                     |           | not null | nextval('baseline_archivos_id_seq'::regclass)
 ruta_archivo   | text                        |           | not null |
 hash_original  | text                        |           | not null |
 fecha_registro | timestamp without time zone |           | not null | CURRENT_TIMESTAMP
 activo         | boolean                     |           | not null | true
Indexes:
    "baseline_archivos_pkey" PRIMARY KEY, btree (id)
    "baseline_archivos_ruta_archivo_key" UNIQUE CONSTRAINT, btree (ruta_archivo)
```

grep -E '"/etc/passwd"|"/etc/shadow"|"/bin/|"/usr/bin/' config/baseline_archivos.json 2>/dev/null

```
[ile@localhost hips-so2]$ grep -E '"/etc/passwd"|"/etc/shadow"|"/bin/|"/usr/bin/' config/baseline_archivos.json 2>/dev/null
  "/etc/passwd": {
  "/etc/shadow": {
  "/bin/bash": {
  "/bin/sh": {
  "/usr/bin/sudo": {
  "/usr/bin/su": {
  "/usr/bin/passwd": {
  "/usr/bin/ssh": {
  "/usr/bin/systemctl": {
  "/usr/bin/firewall-cmd": {
  "/usr/bin/python3": {
  "/usr/bin/ps": {
```

☐ Deteccion de modificacion de binarios vs baseline

cd /home/ile/hips-so2 && sudo env PYTHONPATH="$PWD" python3 -c 'from copy import deepcopy; from detection.file_integrity import cargar_baseline, verificar_integridad; b=deepcopy(cargar_baseline("config/baseline_archivos.json")); f="/bin/bash" if "/bin/bash" in b else next(iter(b)); b[f]["sha256"]="HASH_FALSO"; a=verificar_integridad(b, registrar_alertas=False); print("archivo_probado =", f); print("alertas_detectadas =", len(a)); print("tipo =", a[0]["tipo"] if a else "SIN_ALERTAS"); print("detalle =", a[0]["detalle"] if a else "SIN_DETALLE")'

ID	Fecha	Tipo	Módulo	Severidad	IP origen	Resuelta	Descripción	Acción
109	2026-07-11 16:19:11.499078	archivo_modificado	integridad_archivos	MEDIA	N/A	True	El archivo /usr/local/bin/hips_test_bin fue modificado	Resuelta

1. Compara el archivo actual contra el baseline.
2. Si el hash cambió, genera alarma: archivo_modificado.
3. Guarda la alarma en PostgreSQL.
4. Ejecuta acción preventiva segura: documentar_integridad_archivo.
5. Marca la alarma como resuelta automáticamente.

☐ Detección de modificaciones en /etc/passwd

cd /home/ile/hips-so2 && sudo env PYTHONPATH="$PWD" python3 -c 'from copy import deepcopy; from detection.file_integrity import cargar_baseline, verificar_integridad; b=deepcopy(cargar_baseline("config/baseline_archivos.json")); b["/etc/passwd"]["sha256"]="HASH_FALSO"; a=verificar_integridad(b, registrar_alertas=False); print("archivo_probado = /etc/passwd"); print("alertas_detectadas =", len(a)); print("tipo =", a[0]["tipo"] if a else "SIN_ALERTAS"); print("detalle =", a[0]["detalle"] if a else "SIN_DETALLE")'

```
[ile@localhost hips-so2]$ cd /home/ile/hips-so2 && sudo env PYTHONPATH="$PWD" python3 -c 'from copy import deepcopy; from detection.file_integrity import cargar_baseline, verificar_integridad; b=deepcopy(cargar_baseline("config/baseline_archivos.json"));
 b["/etc/passwd"]["sha256"]="HASH_FALSO"; a=verificar_integridad(b, registrar_alertas=False); print("archivo_probado = /etc/passwd"); print("alertas_detectadas =", len(a)); print("tipo =", a[0]["tipo"] if a else "SIN_ALERTAS"); print("detalle =", a[0]["d
etalle"] if a else "SIN_DETALLE")'
archivo_probado = /etc/passwd
alertas_detectadas = 2
tipo = archivo_modificado
detalle = El archivo /etc/passwd fue modificado
```

120	2026-07-11 16:37:01.832263	archivo_modificado	integridad_archivos	MEDIA	N/A	True	El archivo /etc/passwd fue modificado

☐ Detección de modificaciones en /etc/shadow

cd /home/ile/hips-so2 && sudo env PYTHONPATH="$PWD" python3 -c 'from copy import deepcopy; from detection.file_integrity import cargar_baseline, verificar_integridad; b=deepcopy(cargar_baseline("config/baseline_archivos.json")); b["/etc/shadow"]["sha256"]="HASH_FALSO"; a=verificar_integridad(b, registrar_alertas=False); print("archivo_probado = /etc/shadow"); print("alertas_detectadas =", len(a)); print("tipo =", a[0]["tipo"] if a else "SIN_ALERTAS"); print("detalle =", a[0]["detalle"] if a else "SIN_DETALLE")'

```
[ile@localhost hips-so2]$ cd /home/ile/hips-so2 && sudo env PYTHONPATH="$PWD" python3 -c 'from copy import deepcopy; from detection.file_integrity import cargar_baseline, verificar_integridad; b=deepcopy(cargar_baseline("config/baseline_archivos.json"));
 b["/etc/shadow"]["sha256"]="HASH_FALSO"; a=verificar_integridad(b, registrar_alertas=False); print("archivo_probado = /etc/shadow"); print("alertas_detectadas =", len(a)); print("tipo =", a[0]["tipo"] if a else "SIN_ALERTAS"); print("detalle =", a[0]["d
etalle"] if a else "SIN_DETALLE")'
[sudo] contraseña para ile:
archivo_probado = /etc/shadow
alertas_detectadas = 1
tipo = archivo_modificado
detalle = El archivo /etc/shadow fue modificado
```

ID	Fecha	Tipo	Módulo	Severidad	IP origen	Resuelta	Descripción
127	2026-07-11 16:42:11.612220	archivo_modificado	integridad_archivos	MEDIA	N/A	True	El archivo /etc/shadow fue modificado

☐ Accion de prevencion implementada

sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id = a.id ORDER BY a.id DESC LIMIT 5;"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id = a.id ORDER BY a.id DESC LIMIT 5;"
could not change directory to "/home/ile/hips-so2": Permiso denegado
 id  |     tipo_alarma      |      modulo       |              descripcion              | resuelta |           accion           | resultado
-----+----------------------+-------------------+---------------------------------------+----------+----------------------------+-----------
 127 | archivo_modificado   | integridad_archivos | El archivo /etc/shadow fue modificado | t        | documentar_integridad_archivo | ejecutado
 126 | archivo_modificado   | integridad_archivos | El archivo /etc/passwd fue modificado | t        | documentar_integridad_archivo | ejecutado
 125 | archivo_modificado   | integridad_archivos | El archivo /etc/shadow fue modificado | t        | documentar_integridad_archivo | ejecutado
 124 | archivo_modificado   | integridad_archivos | El archivo /etc/passwd fue modificado | t        | documentar_integridad_archivo | ejecutado
 123 | archivo_modificado   | integridad_archivos | El archivo /etc/shadow fue modificado | t        | documentar_integridad_archivo | ejecutado
(5 rows)
```

☐ Prueba/Demo funcionando

cd /home/ile/hips-so2 && sudo env HIPS_DB_NAME="hips_db" HIPS_DB_USER="hips_app" HIPS_DB_PASSWORD="$(sudo grep '^HIPS_DB_PASSWORD=' /etc/hips/hips.env | cut -d= -f2-)" HIPS_DB_HOST="127.0.0.1" HIPS_ADMIN_EMAIL="ile@localhost" HIPS_SENDMAIL_PATH="/usr/sbin/sendmail" PYTHONPATH="$PWD" python3 hips.py --guardar-db --prevenir --json && sudo -u postgres psql -d hips_db -c "SELECT id, timestamp, tipo_alarma, modulo, severidad, descripcion, resuelta FROM alarmas ORDER BY id DESC LIMIT 5;" && sudo tail -n 20 /var/log/hips/alarmas.log && sudo tail -n 20 /var/log/hips/prevencion.log

```
 id  |        timestamp        |     tipo_alarma      |      modulo       | severidad |              descripcion              | resuelta
-----+-------------------------+----------------------+-------------------+-----------+---------------------------------------+----------
 127 | 2026-07-11 16:42:11.61222 | archivo_modificado | integridad_archivos | MEDIA     | El archivo /etc/shadow fue modificado | t
 126 | 2026-07-11 16:42:11.479351 | archivo_modificado | integridad_archivos | MEDIA     | El archivo /etc/passwd fue modificado | t
 125 | 2026-07-11 16:40:11.561262 | archivo_modificado | integridad_archivos | MEDIA     | El archivo /etc/shadow fue modificado | t
 124 | 2026-07-11 16:40:11.444186 | archivo_modificado | integridad_archivos | MEDIA     | El archivo /etc/passwd fue modificado | t
 123 | 2026-07-11 16:38:11.591207 | archivo_modificado | integridad_archivos | MEDIA     | El archivo /etc/shadow fue modificado | t
(5 rows)

11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
11/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: sin_ip
{"timestamp": "2026-07-11T16:00:11.636407", "modulo": "prevention_actions", "severidad": "alta", "evento": "finalizar_proceso", "detalle": "Acción de prevención para finalizar proceso 3577", "extra": {"accion": "finalizar_proceso", "pid": 3577, "senal":
15, "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:19:11.652235", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /usr/local/bin/hips_test_bin", "extra": {"ac
cion": "documentar_integridad_archivo", "archivo": "/usr/local/bin/hips_test_bin", "motivo": "El archivo /usr/local/bin/hips_test_bin fue modificado", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:20:19.246439", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /usr/local/bin/hips_test_bin", "extra": {"ac
cion": "documentar_integridad_archivo", "archivo": "/usr/local/bin/hips_test_bin", "motivo": "El archivo /usr/local/bin/hips_test_bin fue modificado", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:21:44.985372", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /usr/local/bin/hips_test_bin", "extra": {"ac
cion": "documentar_integridad_archivo", "archivo": "/usr/local/bin/hips_test_bin", "motivo": "El archivo /usr/local/bin/hips_test_bin fue modificado", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:23:11.609020", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /usr/local/bin/hips_test_bin", "extra": {"ac
cion": "documentar_integridad_archivo", "archivo": "/usr/local/bin/hips_test_bin", "motivo": "El archivo /usr/local/bin/hips_test_bin fue modificado", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:25:11.594584", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /usr/local/bin/hips_test_bin", "extra": {"ac
cion": "documentar_integridad_archivo", "archivo": "/usr/local/bin/hips_test_bin", "motivo": "El archivo /usr/local/bin/hips_test_bin fue modificado", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:27:11.628726", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /usr/local/bin/hips_test_bin", "extra": {"ac
cion": "documentar_integridad_archivo", "archivo": "/usr/local/bin/hips_test_bin", "motivo": "El archivo /usr/local/bin/hips_test_bin fue modificado", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:29:03.005247", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /usr/local/bin/hips_test_bin", "extra": {"ac
cion": "documentar_integridad_archivo", "archivo": "/usr/local/bin/hips_test_bin", "motivo": "El archivo /usr/local/bin/hips_test_bin fue modificado", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:30:11.604021", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /usr/local/bin/hips_test_bin", "extra": {"ac
cion": "documentar_integridad_archivo", "archivo": "/usr/local/bin/hips_test_bin", "motivo": "El archivo /usr/local/bin/hips_test_bin fue modificado", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:32:01.565530", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /usr/local/bin/hips_test_bin", "extra": {"ac
cion": "documentar_integridad_archivo", "archivo": "/usr/local/bin/hips_test_bin", "motivo": "El archivo /usr/local/bin/hips_test_bin fue modificado", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:33:11.601128", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /usr/local/bin/hips_test_bin", "extra": {"ac
cion": "documentar_integridad_archivo", "archivo": "/usr/local/bin/hips_test_bin", "motivo": "El archivo /usr/local/bin/hips_test_bin fue modificado", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:34:24.338322", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /usr/local/bin/hips_test_bin", "extra": {"ac
cion": "documentar_integridad_archivo", "archivo": "/usr/local/bin/hips_test_bin", "motivo": "El archivo /usr/local/bin/hips_test_bin ya no existe", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:37:01.944739", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /etc/passwd", "extra": {"accion": "documenta
r_integridad_archivo", "archivo": "/etc/passwd", "motivo": "El archivo /etc/passwd fue modificado", "dry_run": false, "ejecutado": true}}
{"timestamp": "2026-07-11T16:37:01.944848", "modulo": "prevention_actions", "severidad": "alta", "evento": "documentar_integridad_archivo", "detalle": "Acción preventiva documentada para integridad de archivo: /etc/shadow", "extra": {"accion": "documenta
r_integridad_archivo", "archivo": "/etc/shadow", "motivo": "El archivo /etc/shadow fue modificado", "dry_run": false, "ejecutado": true}}
```

☐ Verificación de usuarios conectados y origen

echo "=== usuarios conectados y origen ==="
who -uH
w -i
last -ai | head -n 10

cd /home/ile/hips-so2
sudo env HIPS_DB_NAME="hips_db" HIPS_DB_USER="hips_app" HIPS_DB_PASSWORD="$(sudo grep '^HIPS_DB_PASSWORD=' /etc/hips/hips.env | cut -d= -f2-)" HIPS_DB_HOST="127.0.0.1" PYTHONPATH="$PWD" python3 hips.py --guardar-db --json

sudo -u postgres psql -d hips_db -c "SELECT id, timestamp, tipo_alarma, modulo, ip_origen, descripcion, resuelta FROM alarmas WHERE modulo='user_monitor' ORDER BY id DESC LIMIT 5;"

sudo -u postgres psql -d hips_db -c "SELECT id, timestamp, modulo, evento, detalle FROM eventos_sistema ORDER BY id DESC LIMIT 10;"

```
=== usuarios conectados y origen ===
NOMBRE   LÍNEA       TIEMPO                  PID COMENTARIO
ile      tty2         2026-07-11 15:57 01:23        2637 (local)
 17:20:35 up  1:23,  1 user,  load average: 1,28, 1,19, 0,87
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
ile      tty2     local            15:57    1:23m  0.02s  0.02s /usr/libexec/gnome-session-binary
ile      tty2         Sat Jul 11 15:57   still logged in    0.0.0.0
ile      tty2         Sat Jul 11 15:57 - 15:57  (00:00)     0.0.0.0
reboot   system boot  Sat Jul 11 15:57   still running      0.0.0.0
ile      tty2         Fri Jul 10 21:35 - crash  (18:21)     0.0.0.0
ile      tty2         Fri Jul 10 21:35 - 21:35  (00:00)     0.0.0.0
reboot   system boot  Fri Jul 10 21:35   still running      0.0.0.0
ile      tty2         Fri Jul 10 20:47 - crash  (00:48)     0.0.0.0
ile      tty2         Fri Jul 10 20:47 - 20:47  (00:00)     0.0.0.0
reboot   system boot  Fri Jul 10 20:46   still running      0.0.0.0
ile      tty2         Fri Jul 10 14:25 - crash  (06:21)     0.0.0.0
```

```
 id  |         timestamp          |     tipo_alarma     |    modulo    | ip_origen |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                
 101 | 2026-07-09 15:43:50.239806 | login_fuera_horario | user_monitor |           | Usuario hips_user_monitor_154347 inició sesión fuera del horario permitido | extra={"usuar
  77 | 2026-07-09 00:01:46.823432 | login_fuera_horario | user_monitor |           | Usuario conectado fuera del horario esperado: 00:01
(2 rows)

could not change directory to "/home/ile/hips-so2": Permiso denegado
 id  |         timestamp          |       modulo        |             evento              |                           detalle
-----+----------------------------+---------------------+---------------------------------+-----------------------------------------------------------------
 352 | 2026-07-11 16:42:11.657373 | prevention_engine   | alarma_resuelta_automaticamente | Alarma 127 marcada como resuelta automáticamente por prevención
 351 | 2026-07-11 16:42:11.657373 | prevention_engine   | alarma_resuelta_automaticamente | Alarma 126 marcada como resuelta automáticamente por prevención
 350 | 2026-07-11 16:42:11.615175 | integridad_archivos | alerta_registrada               | Se registró alerta archivo_modificado con id 127
 349 | 2026-07-11 16:42:11.609562 | integridad_archivos | alerta_registrada               | Se registró alerta archivo_modificado con id 126
 348 | 2026-07-11 16:40:11.597274 | prevention_engine   | alarma_resuelta_automaticamente | Alarma 125 marcada como resuelta automáticamente por prevención
 347 | 2026-07-11 16:40:11.597274 | prevention_engine   | alarma_resuelta_automaticamente | Alarma 124 marcada como resuelta automáticamente por prevención
 346 | 2026-07-11 16:40:11.563468 | integridad_archivos | alerta_registrada               | Se registró alerta archivo_modificado con id 125
 345 | 2026-07-11 16:40:11.558713 | integridad_archivos | alerta_registrada               | Se registró alerta archivo_modificado con id 124
 344 | 2026-07-11 16:38:11.634668 | prevention_engine   | alarma_resuelta_automaticamente | Alarma 123 marcada como resuelta automáticamente por prevención
 343 | 2026-07-11 16:38:11.634668 | prevention_engine   | alarma_resuelta_automaticamente | Alarma 122 marcada como resuelta automáticamente por prevención
(10 rows)
```

☐ Detección de conexiones desde origenes inusuales

```
┌──(kali㉿kali)-[~]
└─$ ssh ile@192.168.40.198
The authenticity of host '192.168.40.198 (192.168.40.198)' can't be established.
ED25519 key fingerprint is: SHA256:7M7sUBnnHoiBer3xrSknTqIMlx05pgFg9sx5ybgReQQ
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.40.198' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
ACCESO RESTRINGIDO - Sistema HIPS
Solo personal autorizado. Toda actividad puede ser monitoreada y registrada.
ile@192.168.40.198: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

134	2026-07-11 17:47:45.859982	origen_login_inusual	user_monitor	MEDIA	N/A	False	Usuario conectado desde origen no permitido: 192.168.40.105

☐ Detección de conexiones fuera de horario esperado

ID	Fecha	Tipo	Módulo	Severidad	IP origen	Resuelta	Descripción
161	2026-07-11 18:13:55.499486	login_fuera_horario	user_monitor	MEDIA	N/A	False	Usuario conectado fuera del horario esperado: 17:32

☐ Acción de prevención implementada

sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.ip_origen, a.descripcion, a.resuelta, COALESCE(ap.accion,'SIN_ACCION') AS accion, COALESCE(ap.resultado,'SIN_RESULTADO') AS resultado FROM alarmas a LEFT JOIN acciones_prevencion ap ON ap.alarma_id = a.id WHERE a.modulo='user_monitor' ORDER BY a.id DESC LIMIT 5;"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.ip_origen, a.descripcion, a.resuelta, COALESCE(ap.accion,'SIN_ACCION') AS accion, COALESCE(ap.resultado,'SIN_RESULTADO') AS resultado FROM alarmas a L
FT JOIN acciones_prevencion ap ON ap.alarma_id = a.id WHERE a.modulo='user_monitor' ORDER BY a.id DESC LIMIT 5;"
[sudo] contraseña para ile:
could not change directory to "/home/ile/hips-so2": Permiso denegado
 id  |      tipo_alarma       |    modulo    | ip_origen |                                                
```

☐ Prueba/demo funcionando

```
cd /home/ile/hips-so2 && \
sudo env \
  HIPS_DB_NAME="hips_db" \
  HIPS_DB_USER="hips_app" \
  HIPS_DB_PASSWORD="$(sudo grep '^HIPS_DB_PASSWORD=' /etc/hips/hips.env | cut -d= -f2-)" \
  HIPS_DB_HOST="127.0.0.1" \
  PYTHONPATH="$PWD" \
  python3 hips.py --guardar-db --prevenir --json && \
sudo -u postgres psql -d hips_db -c "SELECT id, timestamp, tipo_alarma, modulo, severidad, ip_origen, descripcion, resuelta FROM alarmas WHERE modulo='user_monitor' ORDER BY id DESC LIMIT 5;" && \
sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, COALESCE(ap.accion,'SIN_ACCION') AS accion, COALESCE(ap.resultado,'SIN_RESULTADO') AS resultado FROM alarmas a LEFT JOIN acciones_prevencion ap ON ap.alarma_id = a.id WHERE a.modulo='user_monitor' ORDER BY a.id DESC LIMIT 5;" && \
sudo tail -n 20 /var/log/hips/alarmas.log && \
sudo tail -n 20 /var/log/hips/prevencion.log
```

☐ Detección de interfaz en modo promiscuo

```
 id  |         timestamp          |    tipo_alarma     |  modulo  |                 descripcion                 | resuelta
-----+----------------------------+--------------------+----------+---------------------------------------------+----------
 162 | 2026-07-11 18:49:11.940103 | interfaz_promiscua | sniffers | Interfaz en modo promiscuo detectada: enp0s3 | t
  90 | 2026-07-09 13:22:27.573464 | sniffer_detectado  | sniffers | Se detectó posible sniffer activo: tcpdump   | t
  79 | 2026-07-09 10:03:35.058357 | interfaz_promiscua | sniffers | Interfaz en modo promiscuo detectada: enp0s3 | t
  67 | 2026-07-08 23:31:43.36872  | sniffer_detectado  | sniffers | Se detectó posible sniffer activo: tcpdump   | t
  65 | 2026-07-08 23:30:31.888153 | sniffer_detectado  | sniffers | Se detectó posible sniffer activo: tcpdump   | t
(5 rows)
```

☐ Detección de tcpdump / wireshark / ethereal en ejecución

sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id = a.id WHERE a.modulo='sniffers' ORDER BY a.id DESC LIMIT 10;"

```
 id  |         timestamp          |    tipo_alarma     |  modulo  |                 descripcion                 | resuelta
-----+----------------------------+--------------------+----------+---------------------------------------------+----------
 165 | 2026-07-11 19:59:32.142349 | sniffer_detectado  | sniffers | Se detectó posible sniffer activo: ethereal  | t
 164 | 2026-07-11 19:47:50.952906 | sniffer_detectado  | sniffers | Se detectó posible sniffer activo: wireshark | t
 163 | 2026-07-11 18:53:23.662822 | sniffer_detectado  | sniffers | Se detectó posible sniffer activo: tcpdump   | t
 162 | 2026-07-11 18:49:11.940103 | interfaz_promiscua | sniffers | Interfaz en modo promiscuo detectada: enp0s3 | t
  90 | 2026-07-09 13:22:27.573464 | sniffer_detectado  | sniffers | Se detectó posible sniffer activo: tcpdump   | t
  79 | 2026-07-09 10:03:35.058357 | interfaz_promiscua | sniffers | Interfaz en modo promiscuo detectada: enp0s3 | t
  67 | 2026-07-08 23:31:43.36872  | sniffer_detectado  | sniffers | Se detectó posible sniffer activo: tcpdump   | t
  65 | 2026-07-08 23:30:31.888153 | sniffer_detectado  | sniffers | Se detectó posible sniffer activo: tcpdump   | t
```

165	2026-07-11 19:59:32.142349	sniffer_detectado	sniffers	ALTA	N/A	True	Se detectó posible sniffer activo: ethereal	Resuelta
164	2026-07-11 19:47:50.952906	sniffer_detectado	sniffers	ALTA	N/A	True	Se detectó posible sniffer activo: wireshark	Resuelta
163	2026-07-11 18:53:23.662822	sniffer_detectado	sniffers	MEDIA	N/A	True	Se detectó posible sniffer activo: tcpdump	Resuelta

☐ Prevención: bloqueo o eliminación de la herramienta

sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id = a.id WHERE a.modulo='sniffers' ORDER BY a.id DESC LIMIT 10;"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resul
.id DESC LIMIT 10;"
could not change directory to "/home/ile/hips-so2": Permiso denegado
 id  |     tipo_alarma      |  modulo  |                descripcion                | resuelta |          accion           | resultado
-----+----------------------+----------+-------------------------------------------+----------+---------------------------+-----------
 164 | sniffer_detectado    | sniffers | Se detectó posible sniffer activo: wireshark | t        | finalizar_proceso         | ejecutado
 163 | sniffer_detectado    | sniffers | Se detectó posible sniffer activo: tcpdump   | t        | finalizar_proceso         | ejecutado
 162 | interfaz_promiscua   | sniffers | Interfaz en modo promiscuo detectada: enp0s3 | t        | desactivar_modo_promiscuo | ejecutado
  90 | sniffer_detectado    | sniffers | Se detectó posible sniffer activo: tcpdump   | t        | finalizar_proceso         | ejecutado
  79 | interfaz_promiscua   | sniffers | Interfaz en modo promiscuo detectada: enp0s3 | t        | desactivar_modo_promiscuo | ejecutado
  67 | sniffer_detectado    | sniffers | Se detectó posible sniffer activo: tcpdump   | t        | finalizar_proceso         | ejecutado
  65 | sniffer_detectado    | sniffers | Se detectó posible sniffer activo: tcpdump   | t        | finalizar_proceso         | ejecutado
(7 rows)
```

```
OK: no quedan sniffers activos
```

☐ Failed Password / Auth Failure

Últimas alarmas

ID	Fecha	Tipo	Módulo	Severidad	IP origen	Resuelta	Descripción
167	2026-07-11 20:03:40.215145	sudo_fallido	system_logs	ALTA	N/A	False	Se detectó un intento fallido de sudo

☐ Errores repetidos desde una IP en `access.log`

cd /home/ile/hips-so2 && sudo mkdir -p /var/log/httpd && sudo bash -c 'for i in $(seq 1 25); do echo "198.51.100.25 - - [11/Jul/2026:18:20:$i -0300] \"GET /ruta_inexistente_$i HTTP/1.1\" 404 123"; done >> /var/log/httpd/access.log' && sudo env HIPS_DB_NAME="hips_db" HIPS_DB_USER="hips_app" HIPS_DB_PASSWORD="$(sudo grep '^HIPS_DB_PASSWORD=' /etc/hips/hips.env | cut -d= -f2-)" HIPS_DB_HOST="127.0.0.1" PYTHONPATH="$PWD" python3 hips.py --guardar-db --prevenir --json && sudo -u postgres psql -d hips_db -c "SELECT id, timestamp, tipo_alarma, modulo, severidad, ip_origen, descripcion, resuelta FROM alarmas WHERE modulo='system_logs' AND tipo_alarma='scanner_http' ORDER BY id DESC LIMIT 10;"

```
could not change directory to "/home/ile/hips-so2": Permiso denegado
 id  |         timestamp          | tipo_alarma  |   modulo    | severidad |   ip_origen   |                        descripcion                        | resuelta
-----+----------------------------+--------------+-------------+-----------+---------------+-----------------------------------------------------------+----------
 170 | 2026-07-11 20:18:14.858926 | scanner_http | system_logs | ALTA      | 198.51.100.25 | Se detectaron 26 errores HTTP 404 desde la IP 198.51.100.25 | t
 104 | 2026-07-09 17:09:14.342916 | scanner_http | system_logs | ALTA      | 203.0.113.111 | Se detectaron 3 errores HTTP 404 desde la IP 203.0.113.111  | t
(2 rows)
```

```
 id  | tipo_alarma  |   modulo    |   ip_origen   |                        descripcion                        | resuelta |   accion    | resultado
-----+--------------+-------------+---------------+-----------------------------------------------------------+----------+-------------+-----------
 170 | scanner_http | system_logs | 198.51.100.25 | Se detectaron 26 errores HTTP 404 desde la IP 198.51.100.25 | t        | bloquear_ip | ejecutado
 104 | scanner_http | system_logs | 203.0.113.111 | Se detectaron 3 errores HTTP 404 desde la IP 203.0.113.111  | t        | bloquear_ip | ejecutado
(2 rows)
```

☐ Envío masivo de mails

bash -lc 'cd /home/ile/hips-so2; echo "=== PRUEBA ENVIO MASIVO DE MAILS ==="; sudo systemctl stop hips.timer || true; sudo systemctl reset-failed postfix || true; sudo systemctl start postfix || true; BACKUP="/tmp/maillog_backup_hips_$(date +%H%M%S)"; sudo cp -a /var/log/maillog "$BACKUP" 2>/dev/null || true; sudo bash -c ": > /var/log/maillog"; TAG="HIPS_ENVIO_MASIVO_$(date +%H%M%S)"; REMITENTE="spamtest_${TAG}@local"; for i in 1 2 3 4 5 6; do sudo bash -c "echo \"Jul 11 18:30:0$i localhost postfix/smtp[222$i]: ABC00$i: from=<$REMITENTE>, to=<destino$i@example.com>, status=sent $TAG\" >>

/var/log/maillog"; done; sudo env HIPS_DB_NAME="hips_db" HIPS_DB_USER="hips_app" HIPS_DB_PASSWORD="$(sudo grep "^HIPS_DB_PASSWORD=" /etc/hips/hips.env | cut -d= -f2-)" HIPS_DB_HOST="127.0.0.1" PYTHONPATH="$PWD" python3 hips.py --guardar-db --prevenir --json; echo "=== ALARMA ==="; sudo -u postgres psql -d hips_db -c "SELECT id, timestamp, tipo_alarma, modulo, severidad, descripcion, resuelta FROM alarmas WHERE tipo_alarma='\"envio_masivo_correo'\" ORDER BY id DESC LIMIT 3;"; echo "=== ACCION PREVENTIVA ==="; sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, ap.accion, ap.resultado FROM alarmas a LEFT JOIN acciones_prevencion ap ON ap.alarma_id=a.id WHERE a.tipo_alarma='\"envio_masivo_correo'\" ORDER BY a.id DESC LIMIT 3;"; sudo sed -i "/$TAG/d" /var/log/maillog; sudo systemctl start hips.timer; echo "postfix=$(systemctl is-active postfix)"; echo "hips_timer=$(systemctl is-active hips.timer)"; echo "backup_maillog=$BACKUP"; echo "=== FIN ==="'

```
 id  |         timestamp          |     tipo_alarma     |   modulo   | severidad |                                  descripcion                                  | resuelta
-----+----------------------------+---------------------+------------+-----------+-------------------------------------------------------------------------------+----------
 178 | 2026-07-11 21:06:22.522183 | envio_masivo_correo | mail_queue | ALTA      | Se detectaron 6 envios de correo desde spamtest_hips_envio_masivo_210622@local    | t
 177 | 2026-07-11 21:04:41.722695 | envio_masivo_correo | mail_queue | ALTA      | Se detectaron 6 envios de correo desde spamtest_hips_envio_masivo_210441@local    | t
 176 | 2026-07-11 20:49:08.323855 | envio_masivo_correo | mail_queue | ALTA      | Se detectaron 6 envios de correo desde spamtest_hips_envio_masivo_ok_204908@local | t
(3 rows)

=== ACCION PREVENTIVA ===
could not change directory to "/home/ile/hips-so2": Permiso denegado
 id  |     tipo_alarma     |   modulo   |      accion       | resultado
-----+---------------------+------------+-------------------+-----------
 178 | envio_masivo_correo | mail_queue | reiniciar_postfix | ejecutado
 177 | envio_masivo_correo | mail_queue | reiniciar_postfix | ejecutado
 176 | envio_masivo_correo | mail_queue | reiniciar_postfix | ejecutado
(3 rows)
```

☐ Acción: bloqueo de IP

sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.ip_origen, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id = a.id WHERE ap.accion ILIKE '%bloquear%' OR ap.accion ILIKE '%firewall%' ORDER BY a.id DESC LIMIT 10;" && echo "=== FIREWALL RICH RULES ===" && sudo firewall-cmd --list-rich-rules && echo "=== FIREWALL GENERAL ===" && sudo firewall-cmd --list-all

```
 id  |       tipo_alarma        |   modulo    |  ip_origen   |                                                
```

☐ Acción: cambio de contraseña de usuario

sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id=a.id WHERE a.tipo_alarma='password_comprometida' ORDER BY a.id DESC LIMIT 10;"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id=a.id WHERE a.tipo_alarma='password_comprome
tida' ORDER BY a.id DESC LIMIT 10;"
could not change directory to "/home/ile/hips-so2": Permiso denegado
 id  |      tipo_alarma      |   modulo    |                          descripcion                          | resuelta |          accion          | resultado
-----+-----------------------+-------------+-------------------------------------------------------------+----------+--------------------------+----------
 179 | password_comprometida | system_logs | Se detectó posible contraseña comprometida del usuario hips_pass_test | t        | cambiar_password_usuario | ejecutado
(1 row)
```

☐ Acción: bloqueo de usuario

sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id = a.id WHERE ap.accion ILIKE '%bloquear_usuario%' OR ap.accion ILIKE '%lock%' OR ap.accion ILIKE '%usuario%' ORDER BY a.id DESC LIMIT 10;"

```
 id  |      tipo_alarma      |    modulo    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                descripcion                                                                                                                                                                                                                                                                                                                
```

☐ Umbral definido para envío masivo

sudo -u postgres psql -d hips_db -c "SELECT modulo, habilitado, intervalo_segundos, umbral, configuracion FROM configuracion_modulos WHERE modulo='mail_queue';"

```
[ile@localhost hips-so2]$ sudo -u postgres psql -d hips_db -c "SELECT modulo, habilitado, intervalo_segundos, umbral, configuracion FROM configuracion_modulos WHERE modulo='mail_queue';"
[sudo] contraseña para ile:
could not change directory to "/home/ile/hips-so2": Permiso denegado
   modulo   | habilitado | intervalo_segundos | umbral | configuracion
------------+------------+--------------------+--------+---------------
 mail_queue | t          |                 60 |     20 | {}
(1 row)
```

☐ Prevención: bloqueo de IP o usuario generador

cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id=a.id WHERE a.modulo='mail_queue' AND a.tipo_alarma='envio_masivo_correo' AND ap.accion='bloquear_usuario' ORDER BY a.id DESC LIMIT 5;"

```
 id |     tipo_alarma     |   modulo   |                                                  descripcion                                                  | resuelta |      accion      | resultado
----+---------------------+------------+-------------------------------------------------------------------------------------------------------+----------+------------------+-----------
 181 | envio_masivo_correo | mail_queue | Se detectaron 6 envios de correo desde el usuario local hips_mail_224528 (hips_mail_224528@local) | t        | bloquear_usuario | ejecutado
(1 fila)
```

☐ Monitoreo de % de memoria por proceso

cd /home/ile/hips-so2 && python3 -c 'from detection.process_monitor import detectar_procesos_sospechosos; txt="PID USER %CPU %MEM COMMAND ARGS\n1234 test 0.0 85.5 python python memtest"; a=detectar_procesos_sospechosos(txt, memoria_umbral=80.0); print(a)'

```
[ile@localhost hips-so2]$ cd /home/ile/hips-so2 && python3 -c 'from detection.process_monitor import detectar_procesos_sospechosos; txt="PID USER %CPU %MEM COMMAND ARGS\n1234 test 0.0 85.5 python python memtest"; a=detectar_procesos_sospechosos(txt, memo
ria_umbral=80.0); print(a)'
[{'tipo': 'memoria_alta', 'pid': '1234', 'usuario': 'test', 'comando': 'python', 'detalle': 'Proceso con memoria alta: 85.5%', 'proceso': '1234 test 0.0 85.5 python python memtest'}]
[ile@localhost hips-so2]$
```

183	2026-07-12 12:58:00.346523	cpu_alta	process_monitor	MEDIA	N/A	True	Proceso con CPU alta: 80.8%	Resuelta

☐ Criterio de tiempo de consumo excesivo

sudo -u postgres psql -d hips_db -c "SELECT modulo, habilitado, intervalo_segundos, umbral, configuracion
FROM configuracion_modulos
WHERE modulo='process_monitor';"

```
[ile@localhost tmp]$ sudo -u postgres psql -d hips_db -c "SELECT modulo, habilitado, intervalo_segundos, umbral, configuracion
FROM configuracion_modulos
WHERE modulo='process_monitor';"
     modulo      | habilitado | intervalo_segundos | umbral |                                                  configuracion
-----------------+------------+--------------------+--------+-------------------------------------------------------------------------------------------------------------------------
 process_monitor | t          |                 60 |     80 | {"criterio": "consumo mayor al umbral durante al menos 120 segundos", "tiempo_excesivo_segundos": 120}
(1 fila)
```

☐ Lógica normal vs. anómalo

```
cd /home/ile/hips-so2 && python3 - <<'PY'
from detection.process_monitor import detectar_procesos_sospechosos

normal = "PID USER %CPU %MEM COMMAND ARGS\n1111 test 1.0 2.0 python python normal"
anomalo = "PID USER %CPU %MEM COMMAND ARGS\n2222 test 1.0 85.5 python python consumo_alto"

print("=== PROCESO NORMAL ===")
print(detectar_procesos_sospechosos(normal, memoria_umbral=80.0))
```

print("=== PROCESO ANOMALO ===")
print(detectar_procesos_sospechosos(anomalo, memoria_umbral=80.0))
PY

```
[ile@localhost tmp]$ cd /home/ile/hips-so2 && python3 - <<'PY'
from detection.process_monitor import detectar_procesos_sospechosos

normal = "PID USER %CPU %MEM COMMAND ARGS\n1111 test 1.0 2.0 python python normal"
anomalo = "PID USER %CPU %MEM COMMAND ARGS\n2222 test 1.0 85.5 python python consumo_alto"

print("=== PROCESO NORMAL ===")
print(detectar_procesos_sospechosos(normal, memoria_umbral=80.0))

print("=== PROCESO ANOMALO ===")
print(detectar_procesos_sospechosos(anomalo, memoria_umbral=80.0))
PY
=== PROCESO NORMAL ===
[]
=== PROCESO ANOMALO ===
[{'tipo': 'memoria_alta', 'pid': '2222', 'usuario': 'test', 'comando': 'python', 'detalle': 'Proceso con memoria alta: 85.5%', 'proceso': '2222 test 1.0 85.5 python python consumo_alto'}]
[ile@localhost hips-so2]$
```

☐ Prevención: terminar proceso

cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id = a.id WHERE a.modulo='process_monitor' ORDER BY a.id DESC LIMIT 10;"

```
[ile@localhost hips-so2]$ cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.res
onitor' ORDER BY a.id DESC LIMIT 10;"
 id  |     tipo_alarma      |     modulo      |            descripcion             | resuelta |      accion       | resultado
-----+----------------------+-----------------+------------------------------------+----------+-------------------+-----------
 183 | cpu_alta             | process_monitor | Proceso con CPU alta: 80.8%        | t        | finalizar_proceso | ejecutado
 182 | cpu_alta             | process_monitor | Proceso con CPU alta: 93.7%        | t        | finalizar_proceso | ejecutado
 108 | cpu_alta             | process_monitor | Proceso con CPU alta: 90.5%        | t        | finalizar_proceso | ejecutado
 107 | cpu_alta             | process_monitor | Proceso con CPU alta: 81.1%        | t        | finalizar_proceso | ejecutado
 106 | cpu_alta             | process_monitor | Proceso con CPU alta: 81.6%        | t        | finalizar_proceso | ejecutado
 102 | cpu_alta             | process_monitor | Proceso con CPU alta: 89.5%        | t        | finalizar_proceso | ejecutado
  89 | proceso_sospechoso   | process_monitor | Proceso sospechoso detectado: nmap | t        | finalizar_proceso | ejecutado
  88 | proceso_sospechoso   | process_monitor | Proceso sospechoso detectado: nmap | t        | finalizar_proceso | ejecutado
  83 | cpu_alta             | process_monitor | Proceso con CPU alta: 85.2%        | t        | finalizar_proceso | ejecutado
  82 | cpu_alta             | process_monitor | Proceso con CPU alta: 132.0%       | t        | finalizar_proceso | ejecutado
(10 filas)
```

☐ Detección de nombres extraños o scripts ejecutables en `/tmp`

cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id=a.id WHERE a.modulo='tmp_monitor' AND ap.resultado='ejecutado' ORDER BY a.id DESC LIMIT 10;"

```
[ile@localhost hips-so2]$ cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevenc
' AND ap.resultado='ejecutado' ORDER BY a.id DESC LIMIT 10;"
[sudo] contraseña para ile:
 id  |       tipo_alarma        |   modulo    |                                                    descripcion                                                    | resuelta |        accion        | resultado
-----+--------------------------+-------------+-------------------------------------------------------------------------------------------------------------------+----------+----------------------+-----------
 192 | extension_sospechosa_tmp | tmp_monitor | Archivo con extensión sospechosa en tmp: /tmp/.x_hidden_tmp.sh                                                   | t        | archivo_ya_prevenido | ejecutado
 191 | archivo_oculto_tmp       | tmp_monitor | Archivo oculto detectado en tmp: /tmp/.x_hidden_tmp.sh                                                           | t        | cuarentenar_archivo  | ejecutado
  87 | ejecutable_en_tmp        | tmp_monitor | Archivo ejecutable detectado en tmp: /tmp/hips_prueba_tmp_monitor_130740.sh                                      | t        | archivo_ya_prevenido | ejecutado
  86 | extension_sospechosa_tmp | tmp_monitor | Archivo con extensión sospechosa en tmp: /tmp/hips_prueba_tmp_monitor_130740.sh                                  | t        | cuarentenar_archivo  | ejecutado
  59 | ejecutable_en_tmp        | tmp_monitor | Archivo ejecutable detectado en tmp: /tmp/hips_prueba2_fix_doble_alerta.sh                                       | t        | archivo_ya_prevenido | ejecutado
  58 | extension_sospechosa_tmp | tmp_monitor | Archivo con extensión sospechosa en tmp: /tmp/hips_prueba2_fix_doble_alerta.sh                                   | t        | cuarentenar_archivo  | ejecutado
  45 | extension_sospechosa_tmp | tmp_monitor | Archivo con extensión sospechosa en tmp: /tmp/hips_prueba2_malware_auto.sh                                       | t        | cuarentenar_archivo  | ejecutado
   2 | nombre_sospechoso_tmp    | tmp_monitor | Nombre sospechoso detectado en tmp: /tmp/hips_logs_backup_pre_tests_20260708_214425/prevencion.log               | t        | cuarentenar_archivo  | ejecutado
(8 filas)
```

☐ Prevención: eliminación o cuarentena

cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id=a.id WHERE a.modulo='tmp_monitor' AND ap.accion IN ('cuarentenar_archivo','archivo_ya_prevenido') ORDER BY a.id DESC LIMIT 10;" && echo "=== buscar cuarentena ===" && sudo find /var /tmp -iname '*quarantine*' -o -iname '*cuarentena*'

2>/dev/null | head -n 20

```
[ile@localhost tmp]$ cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevenci
 ap.accion IN ('cuarentenar_archivo','archivo_ya_prevenido') ORDER BY a.id DESC LIMIT 10;" && echo "=== buscar cuarentena ===" && sudo find /var /tmp -iname '*quarantine*' -o -iname '*cuarentena*
 id  |       tipo_alarma        |   modulo    |                                                    descripcion                                                    | resuelta |        accion        | resultado
-----+--------------------------+-------------+-------------------------------------------------------------------------------------------------------------+----------+----------------------+-----------
 192 | extension_sospechosa_tmp | tmp_monitor | Archivo con extensión sospechosa en tmp: /tmp/.x_hidden_tmp.sh                                             | t        | archivo_ya_prevenido | ejecutado
 191 | archivo_oculto_tmp       | tmp_monitor | Archivo oculto detectado en tmp: /tmp/.x_hidden_tmp.sh                                                     | t        | cuarentenar_archivo  | ejecutado
  87 | ejecutable_en_tmp        | tmp_monitor | Archivo ejecutable detectado en tmp: /tmp/hips_prueba_tmp_monitor_130740.sh                                | t        | archivo_ya_prevenido | ejecutado
  86 | extension_sospechosa_tmp | tmp_monitor | Archivo con extensión sospechosa en tmp: /tmp/hips_prueba_tmp_monitor_130740.sh                            | t        | cuarentenar_archivo  | ejecutado
  59 | ejecutable_en_tmp        | tmp_monitor | Archivo ejecutable detectado en tmp: /tmp/hips_prueba2_fix_doble_alerta.sh                                 | t        | archivo_ya_prevenido | ejecutado
  58 | extension_sospechosa_tmp | tmp_monitor | Archivo con extensión sospechosa en tmp: /tmp/hips_prueba2_fix_doble_alerta.sh                             | t        | cuarentenar_archivo  | ejecutado
  45 | extension_sospechosa_tmp | tmp_monitor | Archivo con extensión sospechosa en tmp: /tmp/hips_prueba2_malware_auto.sh                                 | t        | cuarentenar_archivo  | ejecutado
   2 | nombre_sospechoso_tmp    | tmp_monitor | Nombre sospechoso detectado en tmp: /tmp/hips_logs_backup_pre_tests_20260708_214425/prevencion.log         | t        | cuarentenar_archivo  | ejecutado
(8 filas)

=== buscar cuarentena ===
/var/quarantine
/var/quarantine/hips/hips_prevencion_test.sh.1f14947d37e0.quarantine
/var/quarantine/hips/matriz_modulos_prevencion.md.bak_hips_parte7.5eb73863bd9f.quarantine
/var/quarantine/hips/prevencion.log.b5fecddc726d.quarantine
/var/quarantine/hips/hips_prueba2_malware_auto.sh.718a96249b8d.quarantine
/var/quarantine/hips/hips_prueba2_fix_doble_alerta.sh.7d423084a913.quarantine
/var/quarantine/hips/hips_prueba_tmp_monitor_130740.sh.d701bd34c9ce.quarantine
/var/quarantine/hips/.x_hidden_tmp.sh.eaaf32141e86.quarantine
[ile@localhost tmp]$
```

☐ Detección calibrada con muestra de log DNS

cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.ip_origen, a.resuelta, ap.accion, ap.resultado FROM alarmas a JOIN acciones_prevencion ap ON ap.alarma_id=a.id WHERE a.modulo='ddos_monitor' AND a.tipo_alarma='dns_query_flood' ORDER BY a.id DESC LIMIT 5;"

```
 id  |    tipo_alarma    |    modulo    |  ip_origen   | resuelta |   accion    | resultado
-----+-------------------+--------------+--------------+----------+-------------+-----------
 213 | dns_query_flood   | ddos_monitor | 203.0.113.55 | t        | bloquear_ip | ejecutado
(1 fila)
```

ID	Fecha	Tipo	Módulo	Severidad	IP origen	Resuelta	Descripción	Acción
213	2026-07-12 14:17:22.542849	dns_query_flood	ddos_monitor	CRITICA	203.0.113.55	True	Se detectaron 80 consultas DNS desde la IP 203.0.113.55	Resuelta

☐ Prevención: bloqueo de IP o baja del servicio

+Consultá la acción preventiva:

sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.ip_origen, a.descripcion, a.resuelta,
    ap.accion, ap.resultado
FROM alarmas a
JOIN acciones_prevencion ap ON ap.alarma_id = a.id
WHERE a.modulo='ddos_monitor'
ORDER BY a.id DESC
LIMIT 10;"

```
could not change directory to "/home/ile/hips-soc": Permiso denegado
 id  |    tipo_alarma    |    modulo    |  ip_origen   |                      descripcion                      | resuelta |   accion    | resultado
-----+-------------------+--------------+--------------+-------------------------------------------------------+----------+-------------+-----------
 213 | dns_query_flood   | ddos_monitor | 203.0.113.55 | Se detectaron 80 consultas DNS desde la IP 203.0.113.55 | t        | bloquear_ip | ejecutado
 100 | posible_syn_flood | ddos_monitor | 203.0.113.99 | Se detectaron 8 conexiones SYN desde la IP 203.0.113.99 | t        | bloquear_ip | ejecutado
(2 rows)
```

+Verificá firewall:

echo "=== FIREWALL ==="
sudo firewall-cmd --list-rich-rules
sudo firewall-cmd --list-all

```
=== FIREWALL ===
rule family="ipv4" source address="192.168.40.105" reject
rule family="ipv4" source address="198.51.100.25" reject
rule family="ipv4" source address="203.0.113.10" reject
public (active)
  target: DROP
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services:
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv4" source address="192.168.40.105" reject
        rule family="ipv4" source address="198.51.100.25" reject
        rule family="ipv4" source address="203.0.113.10" reject
[ile@localhost hips-so2]$
```

☐ Revisión de tareas cron del sistema

cd /home/ile/hips-so2 && sudo systemctl stop hips.timer || true && echo "=== crear cron falso de prueba ===" && echo '* * * * * root /tmp/.update.sh' | sudo tee /etc/cron.d/hips_prueba_cron_monitor >/dev/null && sudo chmod 644 /etc/cron.d/hips_prueba_cron_monitor && sudo env HIPS_DB_NAME="hips_db" HIPS_DB_USER="hips_app" HIPS_DB_PASSWORD="$(sudo grep '^HIPS_DB_PASSWORD=' /etc/hips/hips.env | cut -d= -f2-)" HIPS_DB_HOST="127.0.0.1" PYTHONPATH="$PWD" python3 hips.py --guardar-db --prevenir --json && cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT id, timestamp, tipo_alarma, modulo, severidad, descripcion, resuelta FROM alarmas WHERE modulo='cron_monitor' ORDER BY id DESC LIMIT 10;" && echo "=== limpiar prueba ===" && sudo rm -f /etc/cron.d/hips_prueba_cron_monitor && cd /home/ile/hips-so2 && sudo systemctl start hips.timer && systemctl is-active hips.timer

```
 id  |         timestamp          |    tipo_alarma     |    modulo    | severidad |                  descripcion                  | resuelta
-----+----------------------------+--------------------+--------------+-----------+-----------------------------------------------+----------
 216 | 2026-07-12 15:47:55.146246 | ejecucion_tmp_cron | cron_monitor | MEDIA     | Cron ejecuta o referencia archivos temporales | f
 215 | 2026-07-12 15:47:54.953489 | cron_cada_minuto   | cron_monitor | MEDIA     | Cron configurado para ejecutarse cada minuto  | f
  93 | 2026-07-09 13:44:58.88988  | ejecucion_tmp_cron | cron_monitor | MEDIA     | Cron ejecuta o referencia archivos temporales | t
  92 | 2026-07-09 13:44:58.797412 | cron_cada_minuto   | cron_monitor | MEDIA     | Cron configurado para ejecutarse cada minuto  | t
(4 filas)
```

ID	Fecha	Tipo	Módulo	Severidad	IP origen	Resuelta	Descripción
216	2026-07-12 15:47:55.146246	ejecucion_tmp_cron	cron_monitor	MEDIA	N/A	False	Cron ejecuta o referencia archivos temporales
215	2026-07-12 15:47:54.953489	cron_cada_minuto	cron_monitor	MEDIA	N/A	False	Cron configurado para ejecutarse cada minuto

☐ Identificación de tareas con rutas/nombres sospechosos

cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a LEFT JOIN acciones_prevencion ap ON ap.alarma_id=a.id WHERE a.modulo='cron_monitor' ORDER BY a.id DESC LIMIT 10;"

```
 id  |          timestamp          |    tipo_alarma     |    modulo    | severidad |                  descripcion                  | resuelta
-----+-----------------------------+--------------------+--------------+-----------+-----------------------------------------------+----------
 216 | 2026-07-12 15:47:55.146246 | ejecucion_tmp_cron | cron_monitor | MEDIA     | Cron ejecuta o referencia archivos temporales | f
 215 | 2026-07-12 15:47:54.953489 | cron_cada_minuto   | cron_monitor | MEDIA     | Cron configurado para ejecutarse cada minuto  | f
  93 | 2026-07-09 13:44:58.88988  | ejecucion_tmp_cron | cron_monitor | MEDIA     | Cron ejecuta o referencia archivos temporales | t
  92 | 2026-07-09 13:44:58.797412 | cron_cada_minuto   | cron_monitor | MEDIA     | Cron configurado para ejecutarse cada minuto  | t
(4 filas)
```

☐ Detección de intentos repetidos de un mismo usuario

Generar logs de prueba

sudo bash -c 'cat >> /var/log/secure <<EOF
Jul 12 15:10:01 localhost sshd[5001]: Failed password for invalid user admin from 203.0.113.80 port 5001 ssh2
Jul 12 15:10:02 localhost sshd[5002]: Failed password for invalid user admin from 203.0.113.80 port 5002 ssh2
Jul 12 15:10:03 localhost sshd[5003]: Failed password for invalid user admin from 203.0.113.80 port 5003 ssh2
Jul 12 15:10:04 localhost sshd[5004]: Failed password for invalid user admin from 203.0.113.80 port 5004 ssh2
Jul 12 15:10:05 localhost sshd[5005]: Failed password for invalid user admin from 203.0.113.80 port 5005 ssh2
EOF'

Verificar alarma

sudo -u postgres psql -d hips_db -c "SELECT id, timestamp, tipo_alarma, modulo, severidad, ip_origen, descripcion, resuelta
FROM alarmas
WHERE modulo IN ('auth_failures','system_logs')
ORDER BY id DESC
LIMIT 10;"

```
 id  |          timestamp          |          tipo_alarma          |    modulo     | severidad |   ip_origen   |                                  descripcion                                  | resuelta
-----+-----------------------------+-------------------------------+---------------+-----------+---------------+-------------------------------------------------------------------------------+----------
 221 | 2026-07-12 15:59:41.07491   | multiples_intentos_fallidos   | auth_failures | ALTA      | 203.0.113.80  | Se detectaron 23 intentos fallidos de autenticación desde 203.0.113.80 | t
 220 | 2026-07-12 15:58:35.061306  | multiples_intentos_fallidos   | auth_failures | ALTA      | 203.0.113.80  | Se detectaron 12 intentos fallidos de autenticación desde 203.0.113.80 | t
 219 | 2026-07-12 15:57:37.536293  | multiples_intentos_fallidos   | auth_failures | ALTA      | 203.0.113.80  | Se detectaron 6 intentos fallidos de autenticación desde 203.0.113.80  | t
 180 | 2026-07-11 22:09:51.136819  | password_comprometida         | system_logs   | ALTA      |               | Se detectó posible contraseña comprometida del usuario hips_pwd_220950 | t
 179 | 2026-07-11 21:26:21.746307  | password_comprometida         | system_logs   | ALTA      |               | Se detectó posible contraseña comprometida del usuario hips_pass_test  | t
 171 | 2026-07-11 20:21:45.692508  | scanner_http                  | system_logs   | ALTA      | 198.51.100.25 | Se detectaron 25 errores HTTP 404 desde la IP 198.51.100.25            | t
 170 | 2026-07-11 20:18:14.858926  | scanner_http                  | system_logs   | ALTA      | 198.51.100.25 | Se detectaron 26 errores HTTP 404 desde la IP 198.51.100.25            | t
 169 | 2026-07-11 20:18:12.787377  | multiples_intentos_fallidos   | auth_failures | ALTA      | sin_ip        | Se detectaron 10 intentos fallidos de autenticación desde sin_ip       | f
 168 | 2026-07-11 20:07:45.673528  | multiples_intentos_fallidos   | auth_failures | ALTA      | sin_ip        | Se detectaron 9 intentos fallidos de autenticación desde sin_ip        | f
 167 | 2026-07-11 20:03:40.215145  | sudo_fallido                  | system_logs   | ALTA      |               | Se detectó un intento fallido de sudo                                  | f
(10 rows)
```

❑ Detección de credential stuffing

cd /home/ile/hips-so2 && sudo systemctl stop hips.timer || true && TAG="HIPS_CRED_STUFF_$(date +%H%M%S)" && for u in admin oracle postgres backup test; do sudo bash -c "echo \"Jul 12 15:20:01 localhost sshd[6001]: Failed password for invalid user $u from 203.0.113.90 port 6001 ssh2 $TAG\" >> /var/log/secure"; done && sudo bash -c ': > /var/log/maillog' && sudo env HIPS_DB_NAME="hips_db" HIPS_DB_USER="hips_app" HIPS_DB_PASSWORD="$(sudo grep '^HIPS_DB_PASSWORD=' /etc/hips/hips.env | cut -d= -f2-)" HIPS_DB_HOST="127.0.0.1" PYTHONPATH="$PWD" python3 hips.py --guardar-db --prevenir --json && cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT a.id, a.tipo_alarma, a.modulo, a.severidad, a.ip_origen, a.descripcion, a.resuelta, ap.accion, ap.resultado FROM alarmas a LEFT JOIN acciones_prevencion ap ON ap.alarma_id=a.id WHERE a.modulo='auth_failures' AND (a.tipo_alarma='credential_stuffing' OR a.ip_origen='203.0.113.90' OR a.descripcion ILIKE '%203.0.113.90%') ORDER BY a.id DESC LIMIT 10;" && cd /home/ile/hips-so2 && sudo systemctl start hips.timer && systemctl is-active hips.timer

```
 id  |          tipo_alarma          |    modulo     | severidad |   ip_origen   |                                 descripcion                                 | resuelta |   accion    | resultado
-----+-------------------------------+---------------+-----------+---------------+-----------------------------------------------------------------------------+----------+-------------+-----------
 224 | credential_stuffing           | auth_failures | ALTA      | 203.0.113.90  | Se detectaron intentos contra 5 usuarios distintos desde la IP 203.0.113.90  | t        | bloquear_ip | ejecutado
 223 | multiples_intentos_fallidos   | auth_failures | ALTA      | 203.0.113.90  | Se detectaron 10 intentos fallidos de autenticación desde 203.0.113.90       | t        | bloquear_ip | ejecutado
 103 | credential_stuffing           | auth_failures | MEDIA     | 203.0.113.110 | Se detectaron intentos contra 4 usuarios distintos desde la IP 203.0.113.110 | t        | bloquear_ip | ejecutado
(3 filas)

active
[ile@localhost hips-so2]$ sudo firewall-cmd --permanent --remove-rich-rule='rule family="ipv4" source address="203.0.113.90" reject' || true && sudo firewall-cmd --reload
success
success
[ile@localhost hips-so2]$
```

sudo firewall-cmd --permanent --remove-rich-rule='rule family="ipv4" source address="203.0.113.90" reject' || true && sudo firewall-cmd --reload

☐ Criterio de distinción: intrusión real vs. comportamiento normal

Módulo	Comportamiento normal	Comportamiento anómalo / intrusión	Criterio usado
Integridad de archivos	Archivos críticos sin cambios respecto al baseline	Cambio de hash en /etc/passwd, /etc/shadow o binarios protegidos	Comparación de hash actual vs. baseline
Usuarios conectados	Usuario conectado desde origen permitido y horario válido	Login desde IP no permitida o fuera de horario	Origen permitido + ventana horaria configurada
Sniffers	Interfaces sin modo promiscuo y sin herramientas de captura	Interfaz en modo promiscuo o proceso tcpdump, wireshark, ethereal	Estado de interfaz + nombres de procesos conocidos
Análisis de logs	Algunos errores aislados en logs	Muchos errores repetidos desde la misma IP o autenticaciones fallidas	Cantidad de eventos por IP/usuario
Cola de correo	Cola vacía o pocos correos pendientes	Envío masivo o acumulación superior al umbral	Umbral configurado en mail_queue
Procesos con alto consumo	Picos breves de CPU/memoria	Consumo superior al umbral durante tiempo excesivo	Umbral + tiempo_excesivo_segundos
/tmp	Archivos temporales normales no ejecutables	Scripts ejecutables, ocultos o con nombres sospechosos	Extensión, permisos de ejecución y ubicación
DDoS	Consultas DNS normales distribuidas	Muchas consultas desde una misma IP	Cantidad de consultas por IP
Cron	Tareas conocidas del sistema	Cron cada minuto o apuntando a /tmp	Frecuencia + ruta sospechosa
Accesos no válidos	Fallos aislados de login	Múltiples intentos del mismo usuario o varios usuarios desde una IP	Conteo de intentos y diversidad de usuarios

❑ Email al admin por cada alarma detectada

echo "=== ULTIMAS ALARMAS EN POSTGRESQL ===" && cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT id, timestamp, tipo_alarma, modulo, severidad, descripcion FROM alarmas ORDER BY id DESC LIMIT 5;" && echo "=== EMAIL LOCAL RECIBIDO POR ADMIN ile ===" && sudo grep -iE 'Subject: \[HIPS\]|Alerta del sistema HIPS|ddos_monitor|auth_failures|dns_query_flood|credential_stuffing|multiples_intentos' /var/spool/mail/ile | tail -n 40 && echo "=== ESTADO POSTFIX ===" && systemctl is-active postfix

```
=== ULTIMAS ALARMAS EN POSTGRESQL ===
[sudo] contraseña para ile:
 id  |         timestamp          |         tipo_alarma          |    modulo     | severidad |                                  descripcion
-----+----------------------------+------------------------------+---------------+-----------+-------------------------------------------------------------------------------------
 225 | 2026-07-12 16:40:59.911426 | dns_query_flood              | ddos_monitor  | CRITICA   | Se detectaron 80 consultas DNS desde la IP 203.0.113.56
 224 | 2026-07-12 16:03:26.665353 | credential_stuffing          | auth_failures | ALTA      | Se detectaron intentos contra 5 usuarios distintos desde la IP 203.0.113.90
 223 | 2026-07-12 16:03:26.535303 | multiples_intentos_fallidos | auth_failures | ALTA      | Se detectaron 10 intentos fallidos de autenticación desde 203.0.113.90
 222 | 2026-07-12 16:00:45.06688  | multiples_intentos_fallidos | auth_failures | ALTA      | Se detectaron 24 intentos fallidos de autenticación desde 203.0.113.80
 221 | 2026-07-12 15:59:41.07491  | multiples_intentos_fallidos | auth_failures | ALTA      | Se detectaron 23 intentos fallidos de autenticación desde 203.0.113.80
(5 filas)

=== EMAIL LOCAL RECIBIDO POR ADMIN ile ===
  * multiples_intentos_fallidos: Se detectaron 7 intentos fallidos de autenticación desde 192.168.40.105
  * multiples_intentos_fallidos: Se detectaron 12 intentos fallidos de autenticación desde 203.0.113.10
Subject: [HIPS] 3 alerta(s) detectada(s) en localhost.localdomain
Alerta del sistema HIPS
- auth_failures: 3 alerta(s)
  * multiples_intentos_fallidos: Se detectaron 10 intentos fallidos de autenticación desde sin_ip
  * multiples_intentos_fallidos: Se detectaron 7 intentos fallidos de autenticación desde 192.168.40.105
  * multiples_intentos_fallidos: Se detectaron 12 intentos fallidos de autenticación desde 203.0.113.10
Subject: [HIPS] 3 alerta(s) detectada(s) en localhost.localdomain
Alerta del sistema HIPS
- auth_failures: 3 alerta(s)
  * multiples_intentos_fallidos: Se detectaron 10 intentos fallidos de autenticación desde sin_ip
  * multiples_intentos_fallidos: Se detectaron 7 intentos fallidos de autenticación desde 192.168.40.105
  * multiples_intentos_fallidos: Se detectaron 12 intentos fallidos de autenticación desde 203.0.113.10
Subject: [HIPS] 3 alerta(s) detectada(s) en localhost.localdomain
Alerta del sistema HIPS
- auth_failures: 3 alerta(s)
  * multiples_intentos_fallidos: Se detectaron 10 intentos fallidos de autenticación desde sin_ip
  * multiples_intentos_fallidos: Se detectaron 7 intentos fallidos de autenticación desde 192.168.40.105
  * multiples_intentos_fallidos: Se detectaron 12 intentos fallidos de autenticación desde 203.0.113.10
Subject: [HIPS] 3 alerta(s) detectada(s) en localhost.localdomain
Alerta del sistema HIPS
- auth_failures: 3 alerta(s)
  * multiples_intentos_fallidos: Se detectaron 10 intentos fallidos de autenticación desde sin_ip
  * multiples_intentos_fallidos: Se detectaron 7 intentos fallidos de autenticación desde 192.168.40.105
  * multiples_intentos_fallidos: Se detectaron 12 intentos fallidos de autenticación desde 203.0.113.10
Subject: [HIPS] 8 alerta(s) detectada(s) en localhost.localdomain
Alerta del sistema HIPS
- auth_failures: 3 alerta(s)
  * multiples_intentos_fallidos: Se detectaron 24 intentos fallidos de autenticación desde 203.0.113.80
  * multiples_intentos_fallidos: Se detectaron 10 intentos fallidos de autenticación desde 203.0.113.90
  * credential_stuffing: Se detectaron intentos contra 5 usuarios distintos desde la IP 203.0.113.90
- ddos_monitor: 1 alerta(s)
  * dns_query_flood: Se detectaron 80 consultas DNS desde la IP 203.0.113.56
=== ESTADO POSTFIX ===
activating
```

❑ Email al admin por cada acción de prevención

echo "=== EMAIL POR ACCION DE PREVENCION ===" && sudo grep -iE 'HIPS PREVENCION|Accion preventiva ejecutada|Accion preventiva:|Resultado: ejecutado|IP:|bloquear_ip|cuarentenar_archivo' /var/spool/mail/ile | tail -n 40 && echo "=== LOG

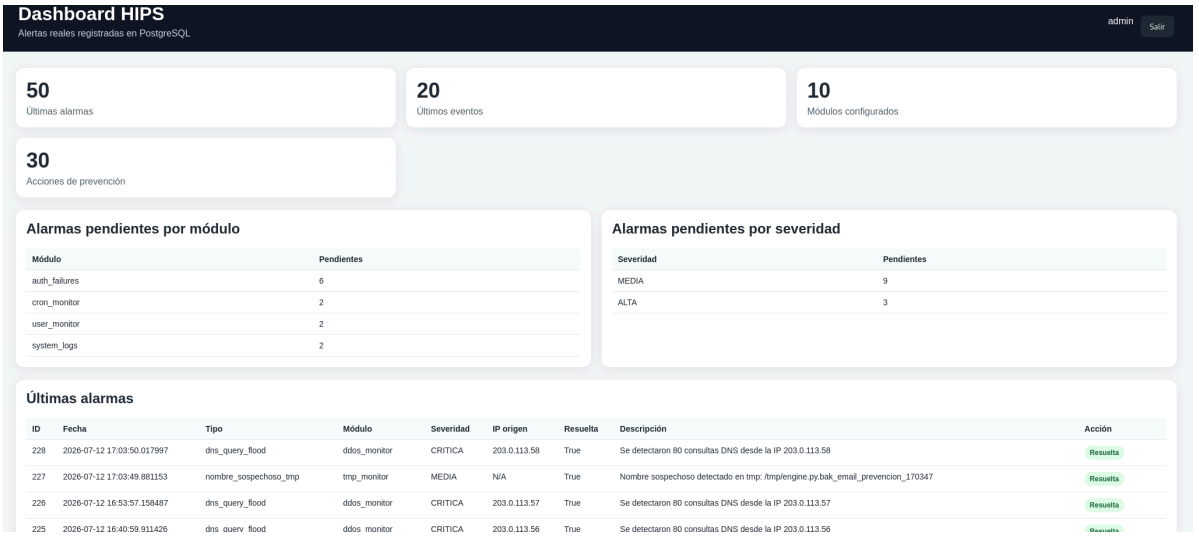
EMAIL PREVENCION ===" && sudo tail -n 10 /var/log/hips/prevencion_email.log

```
[ile@localhost hips-so2]$ echo "=== EMAIL POR ACCION DE PREVENCION ===" && sudo grep -1E 'HIPS PREVENCION|Accion preventiva ejecutada|Accion preventiva:|Resultado: ejecutado|IP:|bloquear_ip|cuarentenar_archivo' /var/spool/mail/ile | tail -n 40 && echo "=
== LOG EMAIL PREVENCION ===" && sudo tail -n 10 /var/log/hips/prevencion_email.log
=== EMAIL POR ACCION DE PREVENCION ===
Subject: [HIPS PREVENCION] bloquear_ip ejecutada en localhost.localdomain
Accion preventiva ejecutada por HIPS
Accion preventiva: bloquear_ip
Resultado: ejecutado
IP: 203.0.113.80
{"accion": "bloquear_ip", "ip": "203.0.113.80", "dry_run": false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.80\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}
Subject: [HIPS PREVENCION] bloquear_ip ejecutada en localhost.localdomain
Accion preventiva ejecutada por HIPS
Accion preventiva: bloquear_ip
Resultado: ejecutado
IP: 203.0.113.90
{"accion": "bloquear_ip", "ip": "203.0.113.90", "dry_run": false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.90\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}
Subject: [HIPS PREVENCION] bloquear_ip ejecutada en localhost.localdomain
Accion preventiva ejecutada por HIPS
Accion preventiva: bloquear_ip
Resultado: ejecutado
IP: 203.0.113.90
{"accion": "bloquear_ip", "ip": "203.0.113.90", "dry_run": false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.90\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}
Subject: [HIPS PREVENCION] cuarentenar_archivo ejecutada en localhost.localdomain
Accion preventiva ejecutada por HIPS
Accion preventiva: cuarentenar_archivo
Resultado: ejecutado
{"accion": "cuarentenar_archivo", "origen": "/tmp/engine.py.bak_email_prevencion_170347", "destino": "/var/quarantine/hips/engine.py.bak_email_prevencion_170347.e2334daa424d.quarantine", "sha256": "e2334daa424ddd7cc6f7858d016232070 7e814034d7fcd4edb1f9dd4
e3d4a44c", "dry_run": false, "ejecutado": true}
Subject: [HIPS PREVENCION] bloquear_ip ejecutada en localhost.localdomain
Accion preventiva ejecutada por HIPS
Accion preventiva: bloquear_ip
Resultado: ejecutado
IP: 203.0.113.58
{"accion": "bloquear_ip", "ip": "203.0.113.58", "dry_run": false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.58\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}
=== LOG EMAIL PREVENCION ===
{"timestamp": "2026-07-12T17:04:48.389709", "evento": "email_accion_prevencion", "accion": "reiniciar_postfix", "modulo": "mail_queue", "tipo": "rebote_correo", "ip": "", "admins": ["ileanasanabria14@gmail.com", "eliasleonardo11@gmail.com"], "returncode"
: 0, "stderr": ""}
{"timestamp": "2026-07-12T17:04:49.254174", "evento": "email_accion_prevencion", "accion": "reiniciar_postfix", "modulo": "mail_queue", "tipo": "rebote_correo", "ip": "", "admins": ["ileanasanabria14@gmail.com", "eliasleonardo11@gmail.com"], "returncode"
: 0, "stderr": ""}
{"timestamp": "2026-07-12T17:04:49.999131", "evento": "email_accion_prevencion", "accion": "reiniciar_postfix", "modulo": "mail_queue", "tipo": "rebote_correo", "ip": "", "admins": ["ileanasanabria14@gmail.com", "eliasleonardo11@gmail.com"], "returncode"
: 0, "stderr": ""}
{"timestamp": "2026-07-12T17:04:50.946608", "evento": "email_accion_prevencion", "accion": "reiniciar_postfix", "modulo": "mail_queue", "tipo": "rebote_correo", "ip": "", "admins": ["ileanasanabria14@gmail.com", "eliasleonardo11@gmail.com"], "returncode"
: 0, "stderr": ""}
{"timestamp": "2026-07-12T17:04:51.847815", "evento": "email_accion_prevencion", "accion": "reiniciar_postfix", "modulo": "mail_queue", "tipo": "rebote_correo", "ip": "", "admins": ["ileanasanabria14@gmail.com", "eliasleonardo11@gmail.com"], "returncode"
: 0, "stderr": ""}
{"timestamp": "2026-07-12T17:04:58.415970", "evento": "email_accion_prevencion", "accion": "reiniciar_postfix", "modulo": "mail_queue", "tipo": "rebote_correo", "ip": "", "admins": ["ileanasanabria14@gmail.com", "eliasleonardo11@gmail.com"], "returncode"
: 0, "stderr": ""}
{"timestamp": "2026-07-12T17:04:59.082703", "evento": "email_accion_prevencion", "accion": "reiniciar_postfix", "modulo": "mail_queue", "tipo": "rebote_correo", "ip": "", "admins": ["ileanasanabria14@gmail.com", "eliasleonardo11@gmail.com"], "returncode"
: 0, "stderr": ""}
{"timestamp": "2026-07-12T17:04:59.695310", "evento": "email_accion_prevencion", "accion": "reiniciar_postfix", "modulo": "mail_queue", "tipo": "rebote_correo", "ip": "", "admins": ["ileanasanabria14@gmail.com", "eliasleonardo11@gmail.com"], "returncode"
: 0, "stderr": ""}
{"timestamp": "2026-07-12T17:05:00.133655", "evento": "email_accion_prevencion", "accion": "reiniciar_postfix", "modulo": "mail_queue", "tipo": "rebote_correo", "ip": "", "admins": ["ileanasanabria14@gmail.com", "eliasleonardo11@gmail.com"], "returncode"
: 0, "stderr": ""}
{"timestamp": "2026-07-12T17:05:00.669085", "evento": "email_accion_prevencion", "accion": "reiniciar_postfix", "modulo": "mail_queue", "tipo": "rebote_correo", "ip": "", "admins": ["ileanasanabria14@gmail.com", "eliasleonardo11@gmail.com"], "returncode"
: 0, "stderr": ""}
Tiene correo en /var/spool/mail/ile
[ile@localhost hips-so2]$
```

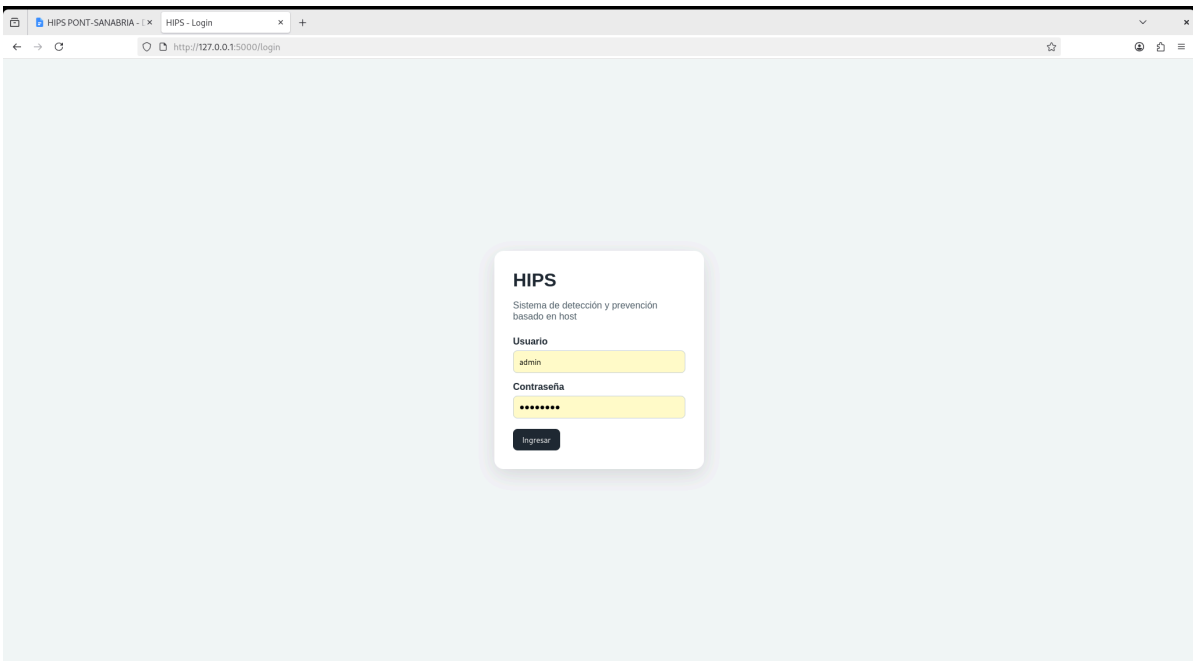
☐ Dashboard visible con las alarmas

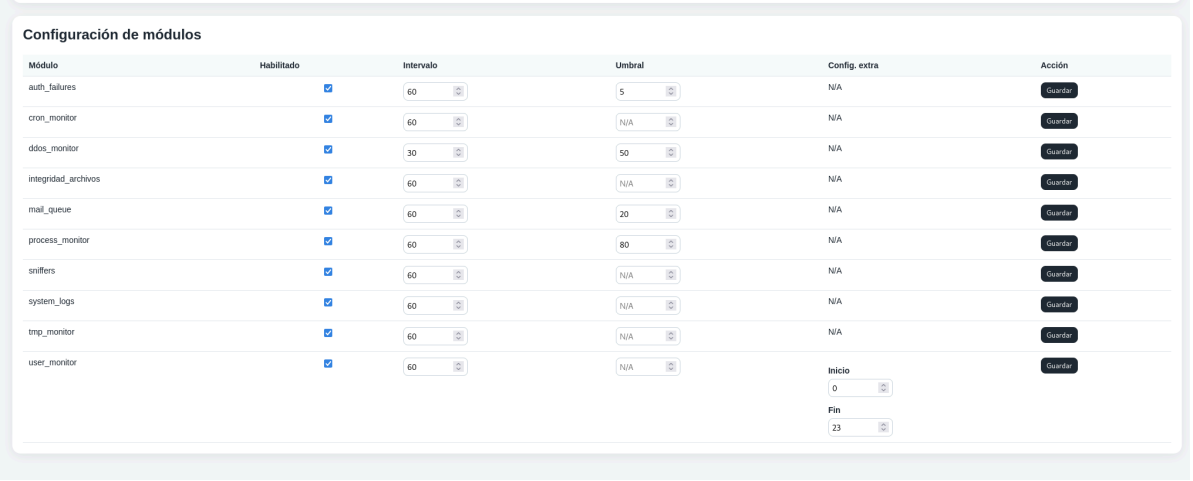
echo "=== SERVICIO WEB HIPS ===" && systemctl is-active hips-web.service && curl -s -o /dev/null -w "HTTP_CODE=%{http_code}\n" http://127.0.0.1:5000/login && echo "=== ULTIMAS ALARMAS ===" && cd /tmp && sudo -u postgres psql -d hips_db -c "SELECT id, timestamp, tipo_alarma, modulo, severidad, descripcion, resuelta FROM alarmas ORDER BY id DESC LIMIT 10;"

```
=== SERVICIO WEB HIPS ===
active
HTTP_CODE=200
=== ULTIMAS ALARMAS ===
 id  |         timestamp          |         tipo_alarma         |    modulo     | severidad |                                descripcion                                 | resuelta
-----+----------------------------+-----------------------------+---------------+-----------+----------------------------------------------------------------------------+----------
 228 | 2026-07-12 17:03:50.017997 | dns_query_flood             | ddos_monitor  | CRITICA   | Se detectaron 80 consultas DNS desde la IP 203.0.113.58                    | t
 227 | 2026-07-12 17:03:49.881153 | nombre_sospechoso_tmp       | tmp_monitor   | MEDIA     | Nombre sospechoso detectado en tmp: /tmp/engine.py.bak_email_prevencion_170347 | t
 226 | 2026-07-12 16:53:57.158487 | dns_query_flood             | ddos_monitor  | CRITICA   | Se detectaron 80 consultas DNS desde la IP 203.0.113.57                    | t
 225 | 2026-07-12 16:40:59.911426 | dns_query_flood             | ddos_monitor  | CRITICA   | Se detectaron 80 consultas DNS desde la IP 203.0.113.56                    | t
 224 | 2026-07-12 16:03:26.665353 | credential_stuffing         | auth_failures | ALTA      | Se detectaron intentos contra 5 usuarios distintos desde la IP 203.0.113.90 | t
 223 | 2026-07-12 16:03:26.535303 | multiples_intentos_fallidos | auth_failures | ALTA      | Se detectaron 10 intentos fallidos de autenticación desde 203.0.113.90      | t
 222 | 2026-07-12 16:00:45.06688  | multiples_intentos_fallidos | auth_failures | ALTA      | Se detectaron 24 intentos fallidos de autenticación desde 203.0.113.80      | t
 221 | 2026-07-12 15:59:41.07491  | multiples_intentos_fallidos | auth_failures | ALTA      | Se detectaron 23 intentos fallidos de autenticación desde 203.0.113.80      | t
 220 | 2026-07-12 15:58:35.061306 | multiples_intentos_fallidos | auth_failures | ALTA      | Se detectaron 12 intentos fallidos de autenticación desde 203.0.113.80      | t
 219 | 2026-07-12 15:57:37.536293 | multiples_intentos_fallidos | auth_failures | ALTA      | Se detectaron 6 intentos fallidos de autenticación desde 203.0.113.80       | t
(10 filas)
```



☐ Login con usuario y contraseña en interfaz web





Configuración de módulos

Módulo	Habilitado	Intervalo	Umbral	Config. extra	Acción
auth_failures	☑	60	5	N/A	Guardar
cron_monitor	☑	60	N/A	N/A	Guardar
ddos_monitor	☑	30	50	N/A	Guardar
integridad_archivos	☑	60	N/A	N/A	Guardar
mail_queue	☑	60	20	N/A	Guardar
process_monitor	☑	60	80	N/A	Guardar
sniffers	☑	60	N/A	N/A	Guardar
system_logs	☑	60	N/A	N/A	Guardar
tmp_monitor	☑	60	N/A	N/A	Guardar
user_monitor	☑	60	N/A	Inicio 0 Fin 23	Guardar

☐ Directorio /var/log/hips/ creado

echo "=== DIRECTORIO /var/log/hips ===" && sudo ls -ld /var/log/hips && echo "=== ARCHIVOS DE LOG HIPS ===" && sudo ls -l /var/log/hips

```
/log/hips && echo "=== ARCHIVOS DE LOG HIPS ===" && ls -l /var/log/hips
=== DIRECTORIO /var/log/hips ===
drwxr-x---. 2 hips_svc hips_group 104 jul 12 17:03 /var/log/hips
=== ARCHIVOS DE LOG HIPS ===
ls: no se puede abrir el directorio '/var/log/hips': Permiso denegado
[ile@localhost hips-so2]$ echo "=== DIRECTORIO /var/log/hips ===" && sudo ls -ld
 /var/log/hips && echo "=== ARCHIVOS DE LOG HIPS ===" && sudo ls -l /var/log/hip
s
=== DIRECTORIO /var/log/hips ===
[sudo] contraseña para ile:
drwxr-x---. 2 hips_svc hips_group 104 jul 12 17:03 /var/log/hips
=== ARCHIVOS DE LOG HIPS ===
total 17420
-rw-r--r--. 1 root     root       14357910 jul 12 18:27 alarmas_detalle.jsonl
-rw-r-----. 1 hips_svc hips_group   908409 jul 12 18:27 alarmas.log
-rw-r--r--. 1 root     root         251713 jul 12 18:28 prevencion_email.log
-rw-r-----. 1 hips_svc hips_group   762607 jul 12 18:28 prevencion.log
[ile@localhost hips-so2]$
```

☐ alarmas.log con todas las alarmas

cd /home/ile/hips-so2 && sudo systemctl stop hips.timer || true && sudo bash -c ': > /var/log/maillog' && sudo mkdir -p /var/log/named && sudo bash -c ': > /var/log/named/query.log' && for i in $(seq 1 80); do echo "12-Jul-2026 18:50:00.$i client 203.0.113.60#53$i (example.com): query: example.com IN A +E" | sudo tee -a /var/log/named/query.log >/dev/null; done && for i in $(seq 1 6); do sudo bash -c "echo \"Jul 12 18:50:0$i localhost sshd[700$i]: Failed password for invalid user admin from 203.0.113.61 port 700$i ssh2\" >> /var/log/secure"; done && sudo env HIPS_DB_NAME="hips_db" HIPS_DB_USER="hips_app" HIPS_DB_PASSWORD="$(sudo grep '^HIPS_DB_PASSWORD=' /etc/hips/hips.env | cut -d= -f2-)" HIPS_DB_HOST="127.0.0.1" HIPS_ADMIN_EMAIL="ile" PYTHONPATH="$PWD" python3 hips.py --guardar-db --prevenir --json && echo "=== alarmas.log ===" && sudo grep -iE 'dns_query_flood|multiples_intentos|credential|ddos|auth|mail|correo|tmp|cron|sniffer|scanner' /var/log/hips/alarmas.log | tail -n 40 && sudo systemctl start hips.timer

```
}
=== alarmas.log ===
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.80
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.90
12/07/2026 :: CREDENTIAL_STUFFING :: 203.0.113.90
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.61
12/07/2026 :: ARCHIVO_OCULTO_TMP :: N/A
12/07/2026 :: EXTENSION_SOSPECHOSA_TMP :: N/A
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.80
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.90
12/07/2026 :: CREDENTIAL_STUFFING :: 203.0.113.90
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.61
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.80
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.90
12/07/2026 :: CREDENTIAL_STUFFING :: 203.0.113.90
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.61
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.80
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.90
12/07/2026 :: CREDENTIAL_STUFFING :: 203.0.113.90
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.61
```

☐ prevencion.log con todas las acciones

echo "=== prevencion.log con acciones preventivas ===" && sudo grep -iE 'bloquear_ip|bloquear_usuario|finalizar_proceso|cuarentenar_archivo|reiniciar_postfix|cambiar_password_usuario|limpiar_cola_correo|Acción de prevención' /var/log/hips/prevencion.log | tail -n 30

```
=== prevencion.log con acciones preventivas ===
{"timestamp": "2026-07-12T18:51:24.562979", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.90", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.90", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.90\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
{"timestamp": "2026-07-12T18:51:25.040993", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.90", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.90", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.90\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
{"timestamp": "2026-07-12T18:53:20.936806", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.80", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.80", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.80\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
{"timestamp": "2026-07-12T18:53:21.658051", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.90", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.90", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.90\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
{"timestamp": "2026-07-12T18:53:22.282021", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.90", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.90", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.90\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
{"timestamp": "2026-07-12T18:54:24.274423", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.80", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.80", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.80\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
{"timestamp": "2026-07-12T18:54:24.898952", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.90", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.90", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.90\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
{"timestamp": "2026-07-12T18:54:25.504943", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.90", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.90", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.90\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
{"timestamp": "2026-07-12T18:56:24.034932", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.80", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.80", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.80\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
{"timestamp": "2026-07-12T18:56:24.645533", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.90", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.90", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.90\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
{"timestamp": "2026-07-12T18:56:25.188715", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.90", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.90", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.90\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
{"timestamp": "2026-07-12T18:56:34.078724", "modulo": "prevention_actions", "severidad": "alta", "evento": "bloquear_ip", "detalle": "Acción de prevención para bloquear IP 203.0.113.80", "extra": {"accion": "bloquear_ip", "ip": "203.0.113.80", "dry_run":
 false, "comandos": ["sudo firewall-cmd --permanent --add-rich-rule=rule family=\"ipv4\" source address=\"203.0.113.80\" reject", "sudo firewall-cmd --reload"], "ejecutado": true}}
```

☐ Formato exacto: dd/mes/yyyy :: Tipo :: IP origen

echo "=== FORMATO alarmas.log ===" && sudo tail -n 10 /var/log/hips/alarmas.log && echo "=== VALIDAR FORMATO dd/mm/yyyy :: Tipo :: IP ===" && sudo grep -E '^[0-9]{2}/[0-9]{2}/[0-9]{4} :: [A-Z0-9_]+ :: .+' /var/log/hips/alarmas.log | tail -n 10

```
=== FORMATO alarmas.log ===
12/07/2026 :: CREDENTIAL_STUFFING :: 203.0.113.90
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.61
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.80
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.90
12/07/2026 :: CREDENTIAL_STUFFING :: 203.0.113.90
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.61
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.80
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.90
12/07/2026 :: CREDENTIAL_STUFFING :: 203.0.113.90
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.61
=== VALIDAR FORMATO dd/mm/yyyy :: Tipo :: IP ===
12/07/2026 :: CREDENTIAL_STUFFING :: 203.0.113.90
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.61
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.80
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.90
12/07/2026 :: CREDENTIAL_STUFFING :: 203.0.113.90
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.61
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.80
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.90
12/07/2026 :: CREDENTIAL_STUFFING :: 203.0.113.90
12/07/2026 :: MULTIPLES_INTENTOS_FALLIDOS :: 203.0.113.61
[ile@localhost hips-so2]$
```

☐ Manual de instalación y uso — digital

☐ Manual de instalación y uso — impreso

☐ Código fuente comentado y documentado

☐ Justificación del lenguaje elegido

Se eligió Python para el desarrollo del HIPS debido a su facilidad para automatizar tareas del sistema, analizar logs, interactuar con procesos, ejecutar comandos del sistema operativo, conectarse con PostgreSQL y desarrollar una interfaz web liviana. Además, Python permite una implementación modular, rápida de probar y adecuada para un sistema de detección y prevención basado en host.

☐ Batería de pruebas automatizadas por módulo

Batería de pruebas automatizadas por módulo

Se prepararon pruebas por módulo para validar detecciones y acciones preventivas del HIPS. Las pruebas permiten verificar integridad de archivos, usuarios conectados, sniffers, análisis de logs, cola de correo, procesos, /tmp, DDoS, cron y accesos no válidos.

☐ Escenario de pruebas completo preparado

Se preparó un escenario de pruebas integral sobre Rocky Linux, incluyendo PostgreSQL, Postfix, firewalld, logs del sistema, interfaz web, módulos del HIPS y datos de prueba controlados. Este entorno permite demostrar el funcionamiento completo del sistema desde la detección hasta la prevención y notificación.

☐ Evidencia de cada módulo

Se recopilaron capturas, salidas de comandos, registros de PostgreSQL, bitácoras y evidencias del dashboard para cada módulo del HIPS. Esto permite demostrar que cada requisito fue probado y documentado individualmente.

Correr la demo

./scripts/demo_maestra.sh

Al terminar, siempre limpiar

./scripts/limpiar_demo_maestra.sh