Gestión Integral de un Incidente Crítico de Seguridad en Codearts Solutions

---

🔹 Fase 1: Detección y análisis forense inicial

journalctl -xe

cat /var/log/syslog

cat /var/log/auth.log

cat /var/log/apache2/access.log

who

last

netstat -tulpn

ss -tulnp

lsof -i

find /tmp /dev/shm -type f -executable -ls

grep -E 'useradd|passwd' /var/log/auth.log

🔹 Fase 2: Aislamiento y preservación de evidencia

ip link set eth0 down

ufw deny out

dd if=/dev/sda of=/mnt/usb/forensic-image.img bs=4M status=progress

sha256sum /mnt/usb/forensic-image.img > /mnt/usb/hash.txt

mkdir /mnt/forensic

mount -o ro,loop /mnt/usb/forensic-image.img /mnt/forensic

🔹 Fase 3: Análisis profundo y cronología

chkrootkit

rkhunter --check

clamscan -r /

crontab -l

cat /etc/rc.local

grep bash /home/*/.bashrc

ls -la /home/*/.ssh/

cat /home/*/.bash_history

🔹 Fase 4: Erradicación y reconstrucción

userdel usuario_sospechoso

rm -rf /usr/local/bin/backdoor

apt reinstall openssh-server

apt update && apt upgrade

systemctl restart ssh

systemctl restart fail2ban

passwd usuario_afectado

🔹 Fase 5: Reforzamiento y respuesta futura

apt install libpam-google-authenticator

google-authenticator

apt install ossec-hids

ufw enable

ufw default deny incoming

ufw allow ssh

vim /etc/ossec.conf

touch /opt/incident_response_playbook.md