Gestión Integral de un Incidente Crítico de Seguridad en Codearts Solutions

---

🔹 Fase 1: Detección y análisis forense inicial

- Revisión de logs críticos: /var/log/syslog, /var/log/auth.log, /var/log/apache2/, journalctl.
- Identificación de IoC (Indicadores de Compromiso):
    - IPs externas con accesos frecuentes.
    - Actividad en directorios sospechosos (/tmp, /dev/shm).
    - Cambios en /etc/passwd, usuarios no autorizados.
- Trazado de sesiones y puertos con: who, last, netstat, ss, lsof.

Error común:
No guardar los logs antes de apagar el sistema.
Solución: Copiar logs importantes antes de reiniciar o cortar tráfico.

🔹 Fase 2: Aislamiento y preservación de evidencia

- Desconexión del servidor afectado (iptables, deshabilitar interfaces).
- Imagen forense del disco con dd o dcfldd.
- Montaje de la copia en modo solo lectura.
- Verificación de integridad con SHA256 del disco.

Error común:
Realizar el análisis directamente sobre el disco afectado.
Solución: Trabajar siempre sobre la copia forense.

🔹 Fase 3: Análisis profundo y cronología

- Detección de rootkits y malware con chkrootkit, rkhunter, clamav.
- Verificación de persistencia: crontab, .bashrc, /etc/rc.local.
- Creación de línea de tiempo con eventos críticos y órdenes ejecutadas.
- Evaluación de escaladas de privilegios o movimientos laterales.

Error común:
Omitir la revisión de scripts de usuario modificados.
Solución: Revisar .bash_history y archivos ocultos por usuario.

🔹 Fase 4: Erradicación y reconstrucción

- Eliminación completa de archivos binarios sospechosos y cuentas comprometidas.
- Reinstalación limpia de servicios afectados.
- Hardening inmediato del sistema (SSH, fail2ban, renovación de claves).
- Aplicación de parches pendientes.

Error común:
Confiar en una limpieza sin reinstalar servicios.
Solución: Siempre reinstalar desde fuentes oficiales si hay dudas.

🔹 Fase 5: Reforzamiento y respuesta futura

- Activación de 2FA, segmentación de red y control por VLAN si aplica.
- Instalación de IDS como OSSEC o Wazuh.
- Creación de un **Playbook de Respuesta** con:
    - Listas de comprobación por fases.
    - Roles asignados y tiempos estimados.
    - Herramientas a utilizar en cada fase.

Error común:
No registrar el incidente de forma documentada.
Solución: Centralizar los pasos, evidencias y decisiones para referencia futura.