SOC INCIDENT REPORT #2 – Ataque por Frecuencia

Fecha: 17 Nov 2025

Analista: J. Rey

Severidad: Alta

Estado: Abierto – Acción Requerida

Resumen:

Se identificó un patrón de intentos de acceso fallidos con alta frecuencia por parte de la IP 203.0.113.10.

La velocidad y repetición indican un ataque automatizado de fuerza bruta.

Una segunda IP (192.168.1.50) mostró un patrón más lento, probablemente manual.

Intentos por minuto:

- 11:00 → 3 intentos fallidos

- 11:01 → 4 intentos fallidos

- 11:02 → 4 intentos fallidos

- 11:05 → 3 intentos fallidos

- 11:06 → 2 intentos fallidos

Hallazgos:

- Total de errores detectados: 16

- IP principal atacante: 203.0.113.10 (11 intentos entre 11:00–11:02)

- IP secundaria: 192.168.1.50 (5 intentos entre 11:05–11:06)

- El primer bloque de intentos supera el ritmo humano → actividad automatizada confirmada.

Conclusión:

La IP 203.0.113.10 realizó un ataque automatizado de fuerza bruta contra el usuario “admin”.

La repetición, velocidad y consistencia confirman el uso de una herramienta automática.

Recomendaciones:

1. Bloquear inmediatamente la IP 203.0.113.10 a nivel de firewall.

2. Activar rate-limiting por intentos fallidos de login.

3. Habilitar MFA para cuentas privilegiadas como “admin”.

4. Revisar logs adicionales para actividad relacionada.