SOC INCIDENT REPORT – 17 Nov 2025

Analista: J. Rey

Severidad: Media–Alta

Estado: Abierto (requiere acción)

Resumen:

Se identificaron 6 intentos de login fallidos dentro del intervalo 10:01–10:09.
La mayoría de los intentos provinieron de la IP 203.0.113.10, la misma que generó una alerta de “actividad sospechosa”. El patrón de repetición indica un posible ataque de fuerza bruta dirigido al usuario “admin”.

Detalles relevantes:

- Total de errores: 6
- IP repetida en errores: 203.0.113.10 (4 veces)
- IP adicional involucrada: 192.168.1.50 (2 veces)
- Advertencia correlacionada: 203.0.113.10
- Usuarios atacados: “admin”, “pedro”

Recomendaciones:

1. Bloquear temporalmente la IP 203.0.113.10.
2. Revisar e implementar políticas de bloqueo por intentos fallidos (rate limiting).
3. Habilitar MFA para el usuario “admin”.
4. Monitorear actividad adicional en las próximas 24 horas.