Threat Brief

Resumen (3 líneas):
Múltiples intentos fallidos de SSH desde 2 IPs externas entre 09:12:01 y 09:41:05
Enumeración de usuarios comunes e intentos directos contra `root`. Accesos legítimos de `alice` y `dev`.

Por qué importa:
Ataque de diccionario básico; `root` expuesto aumenta el riesgo si hay credenciales débiles.

Señales/patrones:

- IPs ofensores: 203.0.113.8 (≈9 intentos), 198.51.100.22 (≈7 intentos).
- Usuarios inventados probados: admin, test, oracle, guest, ubuntu, postgres.
- Intentos a `root`: ≈8 en <~30 min>.
- Accesos válidos: `alice` (password), `dev` (clave pública).

Cómo detectar (regla en lenguaje natural):

- Si una IP falla >5 veces en 30 min contra cualquier usuario → alertar.
- Cualquier intento a `root` desde IP externa → alertar.

Acciones inmediatas:

1. Bloquear 203.0.113.8 y 198.51.100.22 en firewall.
2. Deshabilitar login de `root` por SSH y forzar claves (sin password) para todos.
3. Activar rate-limit/Fail2Ban para `sshd`.

Siguientes pasos (próxima semana):

- Revisar contraseñas débiles y 2FA donde aplique.
- Dashboard simple de intentos fallidos por IP/usuario.
- Auditoría de `alice` / `dev` (horarios y origen esperados).