**Mitigaciones clave para “Valid Accounts / Logins sospechosos”**

1. **Autenticación y seguridad de credenciales**

* **Implementar MFA (Multi-Factor Authentication)** en todas las cuentas, preferiblemente resistente a phishing (FIDO2, OTP).
* **Políticas robustas de contraseñas**: longitud mínima, complejidad, evitar reutilización.
* **Bloqueo de intentos sospechosos**: limitar número de intentos fallidos y aplicar *rate-limiting*.

1. **Gestión y ciclo de vida de cuentas**

* **Asignación de cuentas basada en roles (RBAC)** y creación de cuentas nuevas con los menores privilegios necesarios para su uso.
* **Revisión periódica de cuentas activas**: detectar inactivas, duplicadas o sospechosas.
* **Deshabilitar o eliminar cuentas** cuando no sean necesarias o tras salida de personal.
* **Impedir cuentas compartidas**: evitar que los usuarios compartan sus cuentas y notificar el uso indebido en caso de compartir cuentas.

1. **Monitoreo y detección**

* **Registro y auditoría de accesos**: guardar logs de login, Multi-Factor Authentication, cambios de privilegios.
* **Detección de anomalías**: accesos desde ubicaciones geográficas inusuales, dispositivos no reconocidos, cambios de IP o user-agent sospechosos.
* **Comprobación de IP** **entrantes** para contrastar con databases de IP sospechosas.
* **Integración de feeds de riesgo**: contraseñas comprometidas, breached credentials, IPs maliciosas (p. ej., MISP, HaveIBeenPwned).

1. **Respuesta y mitigación automatizada**

* **Bloqueo temporal de cuentas** tras detecciones de actividad sospechosa o brute force.
* **Step-up Multi-Factor Authentication** o verificación adicional en accesos riesgosos.
* **Revocación inmediata de sesiones activas** cuando se detecte compromiso.
* **Notificación a usuarios y administradores** sobre incidentes de acceso sospechoso.

1. **Herramientas y procesos de soporte**

* **Centralización** de cuentas, administración de privilegios y auditoría.
* **Playbooks de respuesta a incidentes** integrados en la app: pasos automáticos y manuales para cada tipo de incidente (ATO (robo de cuenta), brute force, phishing, DDOS).
* **Dashboards y visualización**: mostrar alertas, anomalías, historial de accesos y riesgo de cuentas.
* **Automatización de enriquecimiento**: añadir contexto (geoIP, ASN, reputación de IP/host) para priorizar alertas.