**Mitigaciones clave contra Fuerza Bruta**

1. **Prevención en la capa de autenticación**

* **Rate limiting / throttling**: limitar el número de intentos de login por usuario, IP o dispositivo para prevenir ataques de fuerza bruta y password spraying.
* **Protección de endpoints críticos**: asegurar login, APIs y paneles administrativos con límites de solicitudes y bloqueos temporales.
* **Autenticación multifactor (MFA)**: forzar MFA (Multi Factor Authentication) resistente a phishing (FIDO2, contraseña de un solo uso) para que la contraseña sola no permita el acceso.
* **Políticas robustas de contraseñas**: longitud mínima, complejidad, no reutilización de contraseñas y evitar passwords comunes.
* **Bloqueo automático de cuentas tras intentos sospechosos**: detectar patrones de repetición y aplicar lockout temporal o paso a verificación adicional.

1. **Educación y concienciación del usuario**

* **Formación sobre seguridad de contraseñas**: enseñar a crear contraseñas únicas y fuertes, no compartirlas y no reutilizarlas en distintos servicios.
* **Simulaciones de ataques internos**: campañas controladas para detectar cuentas con contraseñas débiles.
* **Políticas internas claras**: comunicar los límites de intentos de login, procedimientos de recuperación de contraseña y protocolos de notificación.
* **Cambio periódico de contraseñas**: obligatorio cada 2-3 meses, especialmente para cuentas privilegiadas.

1. **Detección y enriquecimiento (Data / AI)**

* **Monitoreo de intentos de login**: registrar todos los logins fallidos y exitosos, IPs de origen, dispositivos y ubicación geográfica.
* **Modelos de Machine Learning / reglas heurísticas**: detectar patrones de login sospechosos, como múltiples intentos desde la misma IP o desde IPs distribuidas (ataque de reutilización de credenciales).
* **Correlación con Threat Intelligence**: feeds de IPs maliciosas, bots conocidos o contraseñas comprometidas (HaveIBeenPwned, MISP).
* **Alertas automáticas**: reglas Sigma que disparen notificaciones cuando se detecten ataques de fuerza bruta o intentos masivos de login.

1. **Respuesta y mitigación automatizada**

* **Bloqueo temporal** de IPs o cuentas tras múltiples intentos fallidos.
* **Usar MFA** o verificación adicional en accesos sospechosos.
* **Revocación de sesiones activas** si se detecta un patrón de ataque en curso.
* **Notificación a usuarios y administradores**: alertas automáticas sobre actividad sospechosa o bloqueo de cuentas.
* **Integración con playbooks**: automatización de acciones (bloqueos, escalado, logs)

1. **Herramientas, procesos y gobernanza**

* **Dashboards y métricas**: visualizar intentos de login, cuentas bloqueadas y patrones de ataques para análisis en tiempo real.
* **Registro y auditoría**: guardar logs completos de intentos de login, cambios de privilegios, bloqueos y alertas generadas.
* **Integración con sistemas IAM (Gestión de Identidad y Accesos)**: centralizar la gestión de cuentas, roles y privilegios, aplicar lockout automático y MFA.
* **Playbooks documentados**: pasos automáticos y manuales ante ataques de brute force o ataque de reutilización de credenciales, incluyendo escalado a personal de seguridad.
* **Reentrenamiento de modelos y ajustes de umbrales**: utilizar datos históricos de ataques para mejorar la detección y reducir falsos positivos.