Phishing

Lo primero es identificar el medio o la forma en la que se recibió el ataque (correo, red social, etc.).

Logs:

- Un usuario reporta actividad inusual en su cuenta
- Se revisan registros de acceso a correo electrónico y sistemas internos
- Se identifican intentos de conexión desde direcciones ip desconocidas

Herramientas como Splunk detectan actividad desde ubicaciones geográficas extrañas.

Se evalúan todos los accesos con las credenciales comprometidas
Se revisa si hay más usuarios comprometidos

Evaluación del Impacto

Disponibilidad: revisar que no haya interrupción inmediata de servicios.
Integridad: verificar una posible modificación de archivos internos.
Confidencialidad: ¿qué datos sensibles podrían haber sido expuestos?

Acciones de Contención

Se bloquea la cuenta comprometida y se cambia la contraseña.
Se desconectan sistemas afectados y se refuerza la seguridad.

Recuperación

Se restauran credenciales afectadas.
Se aplica autenticación multifactor para evitar futuros ataques.
Se monitorea actividad sospechosa para prevenir más daños.

Comunicación

Se informa a los empleados sobre el ataque.
Se organizan capacitaciones sobre reconocimiento de phishing.