

**Vector: Phishing**

Mensajes extraños, Archivos sospechosos, enlaces sospechosos se evalúa el encabezado de correo, el correo remitente.

**Evidencia**

Recolectar los logs del correo electrónico, bases de datos, seguridad

Revisas conexiones de red, dispositivos, aislar los sistemas comprometidos

**Alcance**

Sistemas interconectados

Conexiones de redes

Puntos de entrada

**Contención**

Desconectar los sistemas comprometidos

Desactivar cuentas comprometidas

Descargar parches y actualizaciones