Laboratorio: El Incidente Crítico

Paso 1: Identificar el Vector de Ataque Inicial

1.1 Revisión de Indicadores Iniciales

Actividad: ¿Qué información reunirías para identificar los primeros signos del incidente?

- Mensajes de correo sospechosos.
- Usuarios reportando comportamiento extraño en sus equipos.
- Alertas del antivirus o EDR.
- Fallos en sistemas específicos sin causa aparente.
- Cambios inusuales en archivos o configuraciones.

Posibles vectores:

- Phishing (correo con enlace o archivo malicioso).
- Explotación de vulnerabilidades (software desactualizado o sin parches).
- Acceso no autorizado (uso indebido de credenciales o cuentas comprometidas).

1.2 Evaluación de la Evidencia

Actividad: ¿Qué buscar en cada caso?

- Phishing: Correos con remitentes falsificados, enlaces sospechosos, archivos adjuntos con macros, actividad inusual después de la apertura del mensaje.
- Vulnerabilidad sospechosa: Software sin parches, servicios expuestos (puertos abiertos innecesarios), logs de error de sistemas que indican explotación.
- Acceso no autorizado: Inicios de sesión fuera del horario, desde ubicaciones geográficas inusuales o IPs desconocidas.

Resultado Esperado: Identificación del vector probable de ataque, por ejemplo: phishing a través de un archivo adjunto que ejecuta un script malicioso.

Paso 2: Analizar los Logs del Sistema

2.1 Recolección de Logs

Actividad: ¿Qué logs revisar?

- Logs del servidor de correo electrónico: búsqueda de correos con adjuntos sospechosos, mensajes enviados desde cuentas comprometidas, correo entrante desde IPs con mala reputación.
- Logs del sistema de bases de datos: consultas fuera del horario habitual, accesos con usuarios con permisos elevados, intentos fallidos de autenticación.

- Logs de seguridad (firewall, antivirus, IDS): alertas de actividad maliciosa, escaneos de puertos, conexiones no autorizadas, bloqueos por reputación de IP.

2.2 Análisis de la Actividad Maliciosa

Actividad: Buscar patrones inusuales

- Inicios de sesión simultáneos desde ubicaciones distintas.
- Tráfico de red elevado hacia destinos desconocidos.
- Comandos inusuales ejecutados por scripts o servicios.

Herramientas útiles: ELK Stack, Splunk, Wireshark, SIEMs.

Paso 3: Determinar el Alcance del Compromiso

3.1 Identificación de Sistemas Comprometidos

Actividad: ¿Qué se debe hacer?

- Revisión de logs de todos los equipos conectados.
- Análisis de integridad de archivos y procesos en ejecución.
- Aislamiento de máquinas sospechosas para análisis forense.

3.2 Evaluación del Impacto

Actividad: Evaluar impacto en los tres pilares:

- Disponibilidad: ¿Qué sistemas dejaron de funcionar? ¿Se detuvieron servicios críticos?
- Integridad: ¿Se alteraron datos sin autorización? ¿Existen cambios no documentados?
- Confidencialidad: ¿Se accedió o exfiltró información sensible?

Resultado Esperado: Mapeo de sistemas afectados y el grado de daño en cada pilar de seguridad.

Paso 4: Proponer Medidas de Contención Inmediatas

4.1 Medidas de Contención Inmediatas

Actividad: Acciones recomendadas

- Desconectar los sistemas comprometidos de la red.
- Forzar el cambio de credenciales de todas las cuentas afectadas.
- Aplicar parches de seguridad en los sistemas vulnerables.

4.2 Plan de Recuperación

Actividad:

- Restaurar sistemas desde copias de seguridad confiables.
- Verificar integridad de los datos restaurados.
- Monitorear constantemente para detectar reinfecciones.
- Realizar un análisis post-incidente para entender el origen y evitar recurrencia.

4.3 Comunicación

Actividad: ¿A quién informar y cómo?

- Notificar a los equipos internos de TI y seguridad.
- Informar a la gerencia y legal si hay implicaciones regulatorias.
- Si aplica, notificar a usuarios o entidades externas afectadas.

Transparencia: Elaborar un informe claro y objetivo, sin ocultar información crítica.