**Términos del glosario de la semana 1**

**Términos y definiciones del curso 6, semana 1**

**Centro de Operaciones de Seguridad** (SOC, por sus siglas en inglés): Unidad organizativa centralizada, que monitorea redes, sistemas y dispositivos en busca de amenazas o ataques a la seguridad.

**Ciclo de vida de respuesta a incidentes del Instituto Nacional de Estándares y Tecnología (NIST):** Marco para la respuesta a incidentes que consta de cuatro fases: preparación, detección y análisis; contención; erradicación y recuperación; y actividad posterior a un incidente.

**Detección y respuesta de puntos de conexión (EDR):** Aplicación que monitorea un punto de conexión para detectar actividad maliciosa.

**Diario de gestión de incidentes:** Forma de documentación utilizada en la respuesta a incidentes.

**Documentación:** Cualquier forma de contenido que se ha registrado para un propósito específico.

**Equipos de respuesta a incidentes de seguridad informática (CSIRT):** Grupo especializado de profesionales de la seguridad formados en gestión y respuesta a incidentes.

**Evento:** Acontecimiento observable en una red, sistema o dispositivo.

**Falso negativo**: Resultado de un análisis que no detecta una amenaza existente y, por lo tanto, no activa una alerta.

**Falso positivo:** Resultado de un análisis que detecta erróneamente una amenaza y dispara una alerta, cuando no existe un incidente real.

**Gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés):** Solución de seguridad que recopila y analiza los datos de registro para monitorear actividades críticas en una organización.

**Incidente:** Acontecimiento que pone en peligro de forma real o inminente, sin autoridad legal, la confidencialidad, integridad o disponibilidad de la información o de un sistema de información; o que constituye una violación o amenaza inminente de violación de la ley, las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable.

**Manual de estrategias:** Guía que proporciona detalles sobre cualquier acción operativa.

**Orquestación, automatización y respuesta de seguridad (SOAR):** Conjunto de aplicaciones, herramientas y flujos de trabajo que utilizan la automatización para responder a eventos de seguridad.

**Plan de respuesta a incidentes:** Documento que describe los procedimientos a seguir en cada paso de la respuesta a un incidente.

**Sistema de detección de intrusiones (IDS, por sus siglas en inglés):** Aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones.

**Sistema de prevención de intrusiones (IPS, por sus siglas en inglés):** Aplicación que monitorea la actividad del sistema en busca de actividades intrusivas y toma medidas para detenerlas.

**Verdadero negativo:** Resultado de un análisis o una detección en el que un sistema de seguridad identifica correctamente la inexistencia de incidentes.

**Verdadero positivo**: Resultado de un análisis o una detección en el que un sistema de seguridad identifica correctamente un incidente real.

Marcar como completo