**Términos del glosario de la semana 3**

**Términos y definiciones del curso 6, semana 3**

**Actividad posterior a un incidente:** Proceso de revisión de un incidente para identificar áreas de mejora.

**Análisis:** Investigación y validación de alertas.

**Cadena de custodia:** Procedimiento documentado que permite constatar la posesión y el control de la evidencia obtenida durante el ciclo de vida de un incidente.

**Caza de amenazas:** Búsqueda proactiva de amenazas en una red.

**Contención:** Acto de limitar que un incidente se extienda para prevenir los daños adicionales que pudiera causar.

**Crowdsourcing:** Práctica de colaboración colectiva que consiste en recopilar información con base en aportes del público, con el fin de resolver un problema o llevar adelante una tarea.

**Detección:** Descubrimiento oportuno de eventos de seguridad.

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

**Erradicación:** Eliminación completa de los elementos de un incidente en todos los sistemas afectados.

**Estándares:** Referencias sobre los objetivos y controles exigibles en lo referente a la seguridad de la información.

**Honeypot:** Sistema o recurso vulnerable a los ataques creado como señuelo para atraer a posibles intrusos.

**Indicadores de ataque (IoA):** Serie de eventos observados que indican un incidente en tiempo real.

**Indicadores de compromiso (IoC):** Evidencia observable que sugiere indicios de un posible incidente de seguridad.

**Informe final:** Documentación que proporciona una revisión exhaustiva de un incidente.

**Inteligencia de fuentes abiertas (OSINT):** Recopilación y análisis de información procedente de fuentes de acceso público para generar inteligencia utilizable.

**Inteligencia sobre amenazas:** Información basada en evidencia que proporciona contexto sobre amenazas existentes o emergentes.

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

**Plan de continuidad del negocio (BCP):** Documento que describe los procedimientos para mantener las operaciones comerciales durante y después de una interrupción significativa.

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

**Recuperación:** Proceso por el que los sistemas afectados vuelven a funcionar con normalidad.

**Resiliencia**: Capacidad de prepararse, responder y recuperarse de las perturbaciones.

**Reunión sobre lecciones aprendidas:** Reunión en la que participan todas las partes implicadas tras un incidente grave.

**Ruptura de la cadena de custodia:** Inconsistencias en la recopilación y el registro de pruebas en la cadena de custodia.

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

**Triaje**: Clasificación y priorización de incidentes en función de su nivel de importancia o urgencia.

**VirusTotal:** Servicio que permite a cualquier persona analizar archivos, dominios, URL y direcciones IP sospechosas en busca de contenido malicioso.

Marcar como completo

Me gusta

No me gusta

Informar de un problema