**Términos del glosario de la semana 4**

**Términos y definiciones del Curso 6, Semana 4**

**Análisis basado en anomalías:** Método de detección que busca identificar comportamientos atípicos a partir del análisis de un conjunto de datos.

**Análisis de firmas:** Método de detección que busca identificar eventos sospechosos o maliciosos.

**Análisis de registros:** Proceso de examinar los registros para identificar eventos de interés.

**Archivo de configuración:** Archivo utilizado para configurar los parámetros de una aplicación.

**Array:** Tipo de dato estructurado que permite almacenar un conjunto de datos homogéneo, es decir, del mismo tipo y relacionados, en una lista ordenada separada por comas.

**Comodín**: Carácter especial que puede sustituir a cualquier otro.

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

**Día cero:** Vulnerabilidad recién descubierta.

**Falso positivo:** Alerta que detecta erróneamente la presencia de una amenaza.

**Firma:** Patrón asociado a una actividad maliciosa.

**Formato de evento común (CEF):** Formato de registro que utiliza parejas clave-valor para estructurar los datos e identificar los campos y sus valores correspondientes.

**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.

**Gestión de registros:** Proceso de recopilación, almacenamiento, análisis y eliminación de datos de registro.

**Lenguaje de procesamiento de búsqueda (SPL):** Lenguaje de consulta de Splunk.

**Objeto:** Tipo de datos, en JavaScript, que almacena datos en una lista separada por comas de parejas clave-valor.

**Pareja clave-valor:** Conjunto de datos que representa dos elementos vinculados: una clave y su valor correspondiente.

**Punto de conexión (endpoint):** Cualquier dispositivo conectado a una red.

**Registro (Log):** Inventario de eventos que tienen lugar dentro de los sistemas de una organización.

**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 detección de intrusiones basado en la red (NIDS, por sus siglas en inglés):** Aplicación que recopila y monitorea el tráfico y los datos de la red.

**Sistema de detección de intrusiones basado en host (HIDS, por sus siglas en inglés):** Aplicación que monitorea la actividad del host en el que está instalada.

**Suricata**: Sistema de monitoreo de redes de código abierto para la detección y prevención de amenazas.

**Telemetría:** Recopilación y transmisión de datos para su análisis.

**YARA-L:** Lenguaje informático utilizado para crear reglas de búsqueda en los datos de registro ingeridos.