TECNOLOGIAS DE LA INFORMACION Y CIBERSEGURIDAD

Inacap

Eventos e Incidentes en Seguridad de la Información

Inacap

Eventos, en seguridad de la información

Un evento se refiere a cualquier actividad o suceso significativo que ocurre dentro de un sistema, red, aplicación o infraestructura informática.

Los eventos pueden ser tanto normales como anómalos, y pueden incluir actividades que no necesariamente constituyen un ataque o incidente de seguridad, pero que deben ser monitoreadas y registradas para garantizar la integridad y seguridad de los sistemas.

Inacap

Eventos, sus características

Características	
Actividad registrada	Los eventos suelen estar registrados en logs (registros) que capturan detalles sobre la acción que ocurrió, como la fecha, hora, dirección IP, usuario involucrado, tipo de acción, entre otros.
Positiva o negativa	Algunos eventos son simplemente operaciones normales, como el inicio de sesión de un usuario, mientras que otros pueden indicar comportamientos inusuales que requieren atención, como intentos de acceso no autorizado.
Evaluación de impacto	No todos los eventos son necesariamente peligrosos, pero todos deben ser monitoreados para detectar posibles amenazas o fallos en el sistema.

Ejemplos de eventos

Ejemplos	
Inicio o cierre de sesión de un usuario	Un evento común que indica que un usuario ha accedido o salido del sistema.
Acceso a un archivo o base de datos	Cuando un usuario accede a un recurso o sistema, como un archivo importante o una base de datos.
Modificación de permisos	Cuando se realiza un cambio en los permisos de acceso a un archivo o sistema.
Uso de privilegios elevados	Cuando un usuario usa credenciales de administrador o privilegios especiales para acceder a áreas restringidas del sistema.
Fallos de autenticación	Intentos fallidos de inicio de sesión, lo que podría ser un indicio de un intento de acceso no autorizado.
Cambio de configuración del sistema	Cualquier alteración en la configuración de un sistema o aplicación, que podría ser legítima o maliciosa.
Transacciones de red	El envío o recepción de datos entre dispositivos en una red.

Importancia de los eventos

Importancia	
Identificación de patrones	Permiten identificar patrones y comportamientos normales, lo que facilita la detección de anomalías y posibles amenazas.
Investigación y análisis forense	Los eventos registrados sirven como evidencia en caso de una investigación de seguridad, ayudando a los equipos de respuesta a entender cómo ocurrió un incidente.
Cumplimiento y auditoría	En muchas industrias, la grabación y el análisis de eventos son necesarios para cumplir con regulaciones de seguridad y protección de datos.

Diferencia entre evento e incidente

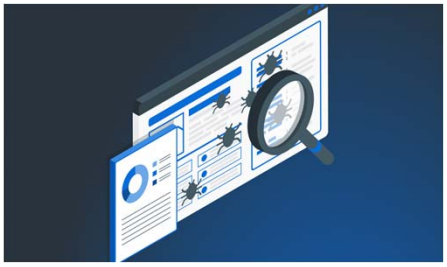
Evento	Incidente
Es cualquier suceso o acción que ocurre dentro del sistema. No todos los eventos son negativos o peligrosos. Por ejemplo, un inicio de sesión exitoso o la creación de un archivo son eventos.	Un incidente de seguridad es un evento o una serie de eventos que afecta negativamente la seguridad de los sistemas, como un acceso no autorizado, una intrusión, o la divulgación de información confidencial.

Ejemplo:
Si un servidor de base de datos registra un evento de acceso legítimo por parte de un usuario autorizado, ese es simplemente un evento. Sin embargo, si ese mismo acceso ocurre fuera del horario laboral y el usuario está accediendo a datos sensibles sin justificación, esto podría convertirse en un incidente de seguridad.

Incidente

Un incidente en seguridad de la información es cualquier evento o suceso que pone en peligro la confidencialidad, integridad o disponibilidad de los sistemas de información, los datos o los recursos tecnológicos de una organización.

Los incidentes de seguridad pueden ser intencionales o accidentales, y pueden tener consecuencias graves para la organización, como pérdidas de datos, interrupciones en los servicios, o daños a la reputación.



Tipos de incidentes

Tipos de incidentes	
Accesos no autorizados	Cuando una persona o entidad accede a sistemas, redes o datos sin la debida autorización.
Robo de datos	Cuando se sustraen datos sensibles o confidenciales, como información personal, financiera o propiedad intelectual.
Ataques de Malware	Incluyen virus, ransomware, troyanos, spyware, etc., que comprometen la seguridad de los sistemas al corromper, dañar o robar información.
Phishing	Técnicas de ingeniería social donde los atacantes intentan engañar a los usuarios para que revelen información sensible, como contraseñas o datos bancarios, haciéndose pasar por una entidad confiable.
Denegación de servicio (DDoS	Un ataque en el que los atacantes inundan un sistema o red con tráfico excesivo, lo que impide que los usuarios legítimos accedan a los servicios.
Pérdida o robo de dispositivos	Como laptops, teléfonos móviles o dispositivos de almacenamiento que contienen información confidencial de la empresa.
Errores humanos:	Acciones equivocadas de los empleados, como enviar información sensible a la persona equivocada o no seguir las políticas de seguridad.
Exposición de datos accidental	Errores o fallos en la configuración que resultan en la divulgación no autorizada de datos.

Características de un incidente

Características	
Impacto	Dependiendo de su naturaleza, un incidente puede tener diferentes grados de impacto, desde interrupciones menores hasta daños graves a la reputación o la operatividad de la empresa.
Urgencia	Algunos incidentes deben ser tratados con rapidez debido a su capacidad para propagarse rápidamente o causar daños significativos.
Recuperación	La capacidad de una organización para contener, mitigar y recuperarse de un incidente es esencial para reducir los efectos negativos.

Gestión de incidentes de seguridad

La gestión de incidentes de seguridad implica una serie de pasos para responder y mitigar los efectos de los incidentes de seguridad. Este proceso generalmente incluye:

Gestión de incidentes	
Identificación	Detectar y reconocer que un incidente ha ocurrido.
Clasificación	Evaluar la gravedad del incidente y determinar su impacto potencial.
Contención	Tomar medidas para limitar el alcance del incidente y evitar que se propague.
Erradicación	Eliminar la causa raíz del incidente (por ejemplo, eliminar malware o cerrar brechas de seguridad).
Recuperación	Restaurar los sistemas y servicios afectados a su funcionamiento normal.
Lecciones aprendidas	Analizar el incidente para comprender cómo ocurrió y mejorar las medidas de seguridad para evitar futuros incidentes.

IOC Indicadores de compromiso

Los indicadores de compromiso (en inglés, Indicators of Compromise, o IOCs) son señales o evidencias que indican que un sistema, red o dispositivo ha sido comprometido o está siendo atacado.

Estos indicadores son elementos observables que permiten a los equipos de seguridad identificar y detectar que un incidente de seguridad ha ocurrido o está ocurriendo, lo que ayuda a tomar acciones preventivas, correctivas o de respuesta ante ciberamenazas.

Tipos comunes de indicadores de compromiso (IOCs)

IOCs mas comunes	
Direcciones IP Maliciosas	Direcciones IP conocidas por estar asociadas con actividades de cibercriminales, como ataques de denegación de servicio (DDoS), malware o phishing.
URL o dominios maliciosos	Sitios web o dominios asociados con malware, ransomware, o campañas de phishing que intentan engañar a los usuarios para que descarguen software malicioso o entreguen información sensible.
Hashes de archivos	Un hash es una "huella digital" única de un archivo. Si un archivo malicioso ha sido identificado, su hash puede ser utilizado como un IOC para buscar archivos idénticos en otros sistemas.
Nombres de archivos y rutas	Los archivos maliciosos pueden tener nombres o ubicaciones específicas dentro de los sistemas. Por ejemplo, ciertos archivos con nombres sospechosos o ubicaciones inusuales pueden indicar que el sistema ha sido comprometido.
Tiempos de modificación o creación de archivos	Cambios inesperados en los timestamps de los archivos pueden indicar que un atacante ha alterado o creado nuevos archivos para llevar a cabo un ataque.
Comportamiento anómalo	Actividades inusuales, como un aumento inesperado en el tráfico de la red, acceso no autorizado a ciertos recursos, o el uso de cuentas de administrador sin justificación, son señales de posibles compromisos.
Cadenas de comandos “scripts”	Secuencias de comandos o comandos específicos que los atacantes utilizan para ejecutar ataques. Por ejemplo, comandos de PowerShell utilizados para ejecutar malware o extraer datos de una red comprometida.
Direcciones de correo o alias asociados a phishing	Las direcciones de correo electrónico que se utilizan en campañas de phishing o suplantación de identidad pueden ser un IOC útil para detectar intentos de fraude.
Certificados digitales fraudulentos	Certificados digitales que han sido manipulados o emitidos por fuentes no confiables, utilizados para cifrar comunicaciones maliciosas.

Importancia de los IOCs

Importacia	
Detección temprana	Los IOCs permiten a los equipos de seguridad identificar rápidamente las señales de un ataque o compromiso, lo que les permite actuar de manera proactiva para prevenir daños mayores.
Investigación de incidentes	Durante un análisis forense de un incidente, los IOCs pueden ayudar a rastrear el ataque, identificar cómo se llevó a cabo, qué sistemas se vieron afectados y qué datos fueron comprometidos.
Respuestas rápidas	Los IOCs permiten a los administradores de sistemas bloquear accesos maliciosos, aislar sistemas comprometidos y prevenir que los atacantes causen más daño.
Compartir inteligencia de amenazas	Los IOCs también se pueden compartir entre organizaciones y comunidades de seguridad, ayudando a crear conciencia sobre las amenazas emergentes.

Ejemplo

Ejemplo práctico:

Imagine que un sistema detecta una dirección IP maliciosa (un IOC) que está intentando acceder a los servidores internos de Inacap.

Esto puede ser una señal de un intento de ataque.

Los administradores de seguridad pueden bloquear esa IP y investigar más a fondo para determinar si se ha producido un compromiso o si se trata de un falso positivo.

¿Falso positivo?

En seguridad de la información, un falso positivo ocurre cuando un sistema de seguridad (como un software antivirus, un firewall o una herramienta de detección de intrusiones) identifica incorrectamente una actividad o evento legítimo como una amenaza o ataque. Es decir, el sistema marca algo como peligroso o malicioso cuando en realidad no lo es.

Ejemplos de falsos positivos
Antivirus que detecta un archivo legítimo como malware: A veces, un antivirus puede clasificar un archivo como un virus o troyano cuando, de hecho, el archivo es completamente seguro. Esto puede ocurrir si el archivo tiene un patrón o características similares a un malware conocido.
Sistema de detección de intrusiones (IDS) que alerta sobre un tráfico legítimo: Si un sistema IDS identifica una comunicación interna entre servidores como un intento de ataque, aunque la actividad sea completamente normal, eso sería un falso positivo.
Firewall bloqueando tráfico legítimo: Un firewall puede interpretar una solicitud de conexión desde una fuente legítima como un intento de ataque y bloquearla, interrumpiendo una acción legítima o servicio.