Universidad de Buenos Aires

Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería
Carrera de Especialización en
Seguridad Informática

Trabajo Final

LOS PECADOS CAPITALES DEL SIEM

Autor: Ing. Alejandra Álvarez Durán
Tutora: Mg.Ing. Sabrina Jeanette
Irisarri González Deibe

Año 2018
Cohorte 2019

Declaración Jurada

Por medio de la presente, la autora manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad del contenido del documento presente es original y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido referenciados adecuadamente y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMA: Mayra Alejandra Álvarez Durán
DNI: 95842972

Resumen

A medida que nace una nueva herramienta tecnológica, el número de cibercrímenes crece y los métodos de defensa son más difíciles de implementar. Mientras un profesional de seguridad intenta corregir vulnerabilidades que pueden surgir en su entorno, el atacante se centra en una sola por lo que el profesional de seguridad se va a encontrar en desventaja.

Según el informe de ESET Latinoamérica [1]**,** hasta junio del 2018 se han detectado más de 8 mil ciberataques, y la tendencia se multiplica. Esta es una de las razones por las que las empresas, buscan implementar la herramienta **SIEM** como un mecanismo de protección.

Sin embargo, pueden surgir problemas en la implementación que crearían puntos de fuga para el atacante; por lo tanto ¿Cómo saber si se están explotando todas las capacidades del SIEM?, ¿Cómo saber si con esta herramienta estamos protegidos?

El presente trabajo final permite identificar y exponer errores que se cometen en el proceso de adquisición e implementación de la herramienta, y que disminuyen la eficiencia, basado en la experiencia personal y corroborado por estudios y reportes internacionales.

Palabras Claves: SIEM, problemas en implementación, seguridad.

Índice

Índice de figuras

Introducción.

Son las 02:05 am de un sábado, Juana analista de ventas de una empresa X establece conexión por una VPN (Virtual Protocol Network) corporativa, accede al servidor de consumidores y copia la base de datos de los clientes con información confidencial, historial de compras, registro crediticio, etc. El acceso a estos recursos se encuentra autorizado dentro de los perfiles y roles que la compañía estipula para cada usuario. Mientras se mantiene conectada guarda en un directorio del equipo un script que se activará con el siguiente reinicio del servidor; posterior a ello elimina todos los correos electrónicos de la bandeja de entrada y salida de la empresa y se desconecta; el lunes siguiente Juana renuncia justificando que posee una nueva propuesta laboral de la competencia.

Lo realizado por la misma expone a la organización a una serie de riesgos que podrían desencadenar en pérdidas de todo tipo en la empresa. Estos podrían incluir destrucción de datos, indisponibilidad del sistema de base de datos por el script incrustado, robo de información confidencial o muchas situaciones más. Las acciones que Juana ejecutó en los equipos deberían encontrarse en forma de logs con fecha y hora, pero a menudo pasan desapercibidos en una organización.

La pregunta entonces es: ¿Por qué? Y las respuestas podrían ser varias. Es importante destacar que cada sistema tiene su propio generador de logs, éstos están dispersos en cada equipo aislados unos de otros, por lo que un analista en el área de TI o Seguridad no invierte su tiempo en revisar las grandes cantidades de logs que genera y almacena cada equipo, simplemente porque no alcanzaría con su tiempo. Otra razón por la que la revisión de logs no es la tarea favorita de este personal es la sintaxis propia del log, ya que a simple vista no es amigable a su lectura porque implementa números de identificación de cada evento asociado a su propia nomenclatura y usualmente en texto plano.

La situación presentada podría ser claramente un ejemplo de robo de datos a los que día a día está expuesta una empresa y muy a menudo no tiene conocimiento, adicionalmente están los intentos de ataques por denegación de servicio, problemas de control de acceso, malwares, mala implementación de herramientas, configuraciones por defecto, etc. Todo ha provocado la necesidad de que surjan herramientas que permitan conocer y gestionar lo que sucede en la red y es por ello por lo que nacen las Herramientas SIEM.

Enfoque y relevancia.

Implementar un SIEM no significa únicamente comprar el producto, instalarlo y esperar que el dispositivo automáticamente funcione. El proceso de adopción de una nueva tecnología, más aún del SIEM, requiere la implementación sigilosa de todas sus fases, desde la fase inicial o planeamiento, seguida por una fase de diseño, elaboración de casos de uso, pruebas para evaluar el comportamiento real del SIEM frente al esperado, esto sin olvidar que todas estas fases forman parte de un circulo continuo que comprende tanto la administración de la herramienta, como así también la administración de todos sus dispositivos asociados.

Cuando el SIEM no se implementa conforme el proceso descripto anteriormente, surgen dificultades y en la actualidad es común encontrar en la internet sinnúmeros de post de usuarios con inconvenientes en fases de implementación del SIEM.
Por lo que este trabajo final pretende realizar un análisis crítico que permita evidenciar los pecados en los que incurren las empresas cuando implementan la tecnología SIEM.

Objetivo.

El objetivo general del presente Trabajo Final propuesto es realizar un análisis de los requerimientos necesarios para la implementación de la herramienta de seguridad SIEM. Investigar cuales son las principales necesidades que se plantean las empresas para adquirir la herramienta y mediante ello poder identificar y determinar los inconvenientes que surgen en cada una de las fases de implementación.

Alcance.

En el presente trabajo final de especialización se realizará una investigación exhaustiva que abarcará tanto el análisis de requerimientos necesarios para la implementación de la herramienta SIEM como así también la identificación y el descubrimiento de los inconvenientes que surgen en cada etapa de implementación desde la fase de adquisición hasta su puesta en funcionamiento.

CAPITULO 1 ¿QUÉ ES EL SIEM?

SIEM es la abreviatura de las siglas en inglés: *Security Information and Event Management*, es decir, un sistema de gestión de información y eventos de seguridad, el libro Security Information and Event Management (SIEM) define a la herramienta de la siguiente manera:

"El sistema SIEM es una colección compleja de tecnologías diseñadas para proporcionar visión y claridad sobre el sistema de TI corporativo en su conjunto, lo que beneficia a los analistas de seguridad y administradores de TI". [2]

Esta herramienta surge de la unificación de dos tecnologías SIM y SEM (Anexo A) permitiendo como resultado alcanzar una visión holística de la infraestructura y estar alerta de posibles anomalías y amenazas que podrían comprometer los activos críticos de información de la empresa mediante la recolección, centralización y análisis de registros de los diferentes equipos como firewall, IPS/IDS, antimalware, host de red, active directory, sistemas de video, antivirus, correo electrónico, etc.

Como se menciona la tecnología SIEM agrega datos de eventos producidos por dispositivos de seguridad, infraestructura de red, sistemas y aplicaciones, pero la tecnología SIEM también puede procesar otras formas de datos, como la telemetría de red (flujos y paquetes), estos eventos se combinan con información contextual sobre usuarios, activos, amenazas y vulnerabilidades.

Los datos son normalizados, de modo que la información contextual de distintas fuentes puede analizarse con fines específicos, como la supervisión de eventos de seguridad de la red, la supervisión de la actividad del usuario y la notificación de cumplimiento. La tecnología proporciona análisis en tiempo real de eventos para monitoreo de seguridad, consultas y análisis de largo alcance para realizar investigaciones o búsquedas históricas, otro soporte para la investigación y gestión de incidentes, e informes (por ejemplo, para requisitos de cumplimiento).

Las características principales de las herramientas SIEM son.

1.1 Recolección, retención y centralización de logs.

Una característica importante en el SIEM se encuentra en la capacidad de alojar grandes cantidades de registros de diversas fuentes ya sea aplicaciones de usuario, servidores, equipos de red o de seguridad informática, u otros que se efectiviza gracias al proceso de recolección.

Para el proceso de recolección es trascendental identificar el tipo de arquitectura que posee la organización, la tendencia actual es contar con servicios e infraestructura en la nube ya sea para abaratar costos, crecer en el mercado, implementar nuevas soluciones, etc. La infraestructura basada en servidores físicos llamada on-premise se está quedando cada vez más relegada frente a las plataformas en la nube como son SaaS, IaaS, Paas, ya en 2010 la empresa Magic Software publicaba un informe llamado “¿Hay algo más entre las nubes y el sótano?”, en el cual confirmaba lo mencionado [3].

Los registros contienen la sucesión de pasos o acontecimientos que afectan a un proceso y están basados en estándares, así como también en formatos dependientes de su creador por consiguiente existen diversos tipos de generadores de registros entre los cuales se identifican los siguientes.

Syslog (RFC5424): que es un estándar de facto para envío de registros en la red, lo consumen sistemas operativos como Linux, Unix, Mac, equipos de red etc. [4]
Netflow: protocolo de red elaborado por Cisco System usado para recolectar la información sobre el tráfico IP. [5]

Alertas propietarias: que son protocolos propios que generan los dispositivos como Antivirus, Windows (evt, etvx), AS400, etc.
Al igual que muchos otros como por ejemplo J-Flow de Juniper, Q-Flow de Q1labs, sFlow(RFC3176).

1.2 Definición de métodos para la recolección de logs.

1.2.1 Push method o basado en agentes:

Este método se caracteriza por la instalación previa de un agente (demonio) en cada host, el mismo que es el responsable de capturar, extraer, procesar y enviar los logs al SIEM, de esta forma el agente puede configurarse para enviar registros de manera periódica. [6]

Para el proceso de envió de registros es necesario establecer una conexión a nivel de red, por ejemplo para la herramienta SIEM de SPLUNK, cuando necesita recopilar información desde un servidor Windows, utiliza un agente llamado: “Universal Forwarder” el cual requiere instalación previa en el equipo para recolectar los eventos, y posterior envío mediante el establecimiento de una conexión utilizando los puertos recomendados TCP: 8089, 9997 [7].

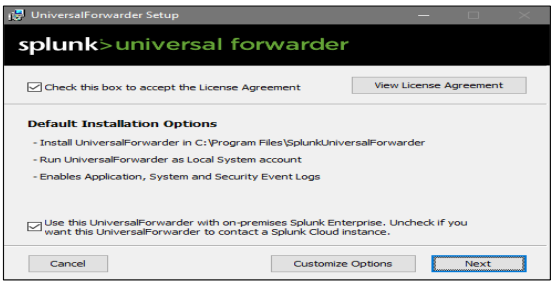

Figura 1 Ejemplo de Agente de Instalación Splunk Forwarder Fuente: [8]

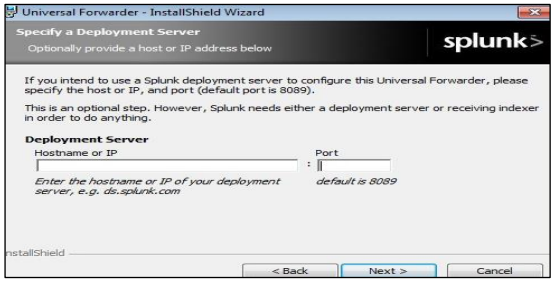

Figura 2 Ejemplo de Agente de Instalación Splunk Forwarder Fuente: [8]

1.2.2 Pull method o sin agentes:

Este proceso no requiere la instalación de ningún agente ya que es el mismo SIEM el que extrae y transporta los registros para su recolección, utilizando como recursos protocolos que se encuentren disponibles en el equipo, por ejemplo, SSH, JDBC, SNMP, CIFS, log4j, WMI, MSRPC etc. [6]

Para la implementación de este método es necesario contar con un usuario y contraseña valida (temporal o permanente) con ciertos privilegios que permita la autenticación cuando se establezca una conexión entre el SIEM y los equipos donde se alojen los eventos, al igual que la configuración del usuario es necesario establecer una configuración en base tiempo y periodicidad para la extracción de estos. [9]

Por ejemplo, si se decidiera integrar los logs de una BD Oracle con el SIEM Qradar de IBM; éste presenta la opción de realizarlo utilizando una conexión previa mediante el protocolo JDBC. Para realizar la conexión se utiliza un usuario y clave con privilegios para acceder a la tabla donde se encuentran los logs a extraer: *dba_audit_trail*.

Desde QRadar, se configura un Log Source [1] con los parámetros del usuario, la clave, el protocolo, el puerto, el destino hacia donde se van a enviar los datos de la siguiente manera:

[1] Log Source: es una característica dentro del módulo de administración del QRadar que permite configurar manualmente las fuentes de registro.

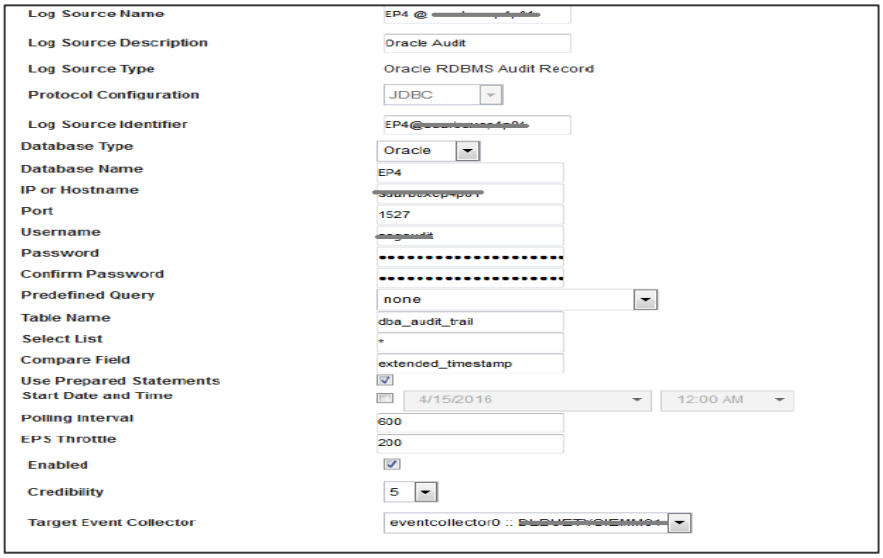

Figura 3 Modulo Log Source de QRadar.

1.3 Normalización o Parseo de logs.

Luego del proceso de recolección de logs es necesario normalizar los registros de dispositivos o aplicaciones en eventos comunes ya que inicialmente poseen diferente nomenclatura, por lo que estandarizar los registros implicaría tener un lenguaje común dentro de la herramienta.

La normalización permite un almacenamiento ordenado y predecible para todos los registros indexándolos para una búsqueda y clasificación concisa. [10]

https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/t_tuning_guide_deploy_addlsman.html#t_tuning_guide_deploy_addlsman

Por ejemplo, un evento de inicio de sesión en Windows indicaría este número de evento y tipo de log. EVENT ID: 4672

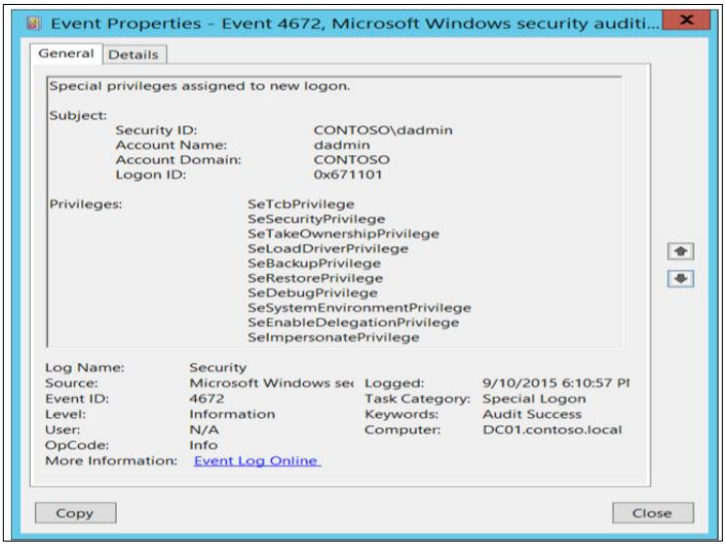

Figura 4 Visor de Eventos Windows

Sin embargo, un inicio de sesión en Linux se mostraría de esta manera.

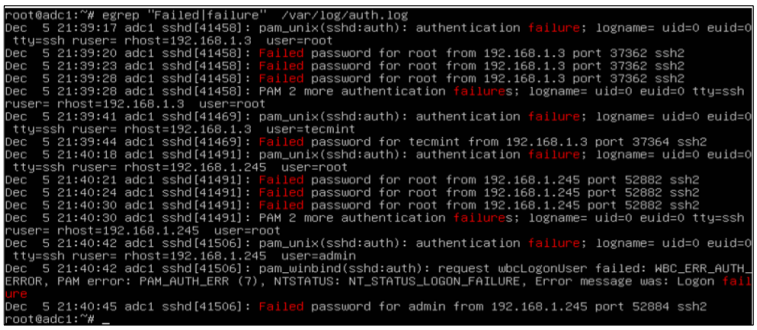

Figura 5 Captura de logs de Linux

Así como también un log del firewall seria:

		Older				Newer	
Time	Chain	Iface	Proto	Source	Src Port	Destination	Dst Port
11:47:01	DROP_INPUT	red0	TCP	200.82.232.153	4380	200.82.243.146	139
11:46:55	DROP_INPUT	red0	TCP	200.82.232.153	4380	200.82.243.146	139
11:46:52	DROP_INPUT	red0	TCP	200.82.232.153	4380	200.82.243.146	139
09:29:45	DROP_INPUT	red0	TCP	200.82.241.198	1969	200.82.243.146	139
09:29:38	DROP_INPUT	red0	TCP	200.82.241.198	1969	200.82.243.146	139
09:29:36	DROP_INPUT	red0	TCP	200.82.241.198	1969	200.82.243.146	139
03:10:53	DROP_INPUT	red0	TCP	200.82.237.157	2697	200.82.243.146	139
03:10:47	DROP_INPUT	red0	TCP	200.82.237.157	2697	200.82.243.146	139
03:10:44	DROP_INPUT	red0	TCP	200.82.237.157	2697	200.82.243.146	139
03:10:01	DROP_INPUT	red0	TCP	200.82.232.215	1785	200.82.243.146	139
03:00:01	DROP_INPUT	red0	TCP	200.82.232.215	1785	200.82.243.146	139

Figura 6 Captura logs Firewall

Todos estos registros poseen información importante que es necesaria para la gestión de la herramienta SIEM como, por ejemplo:

- Nombre de host
- Fecha y hora
- Fuente IP del tráfico
- IP de origen y destino
- Puerto de origen
- Puerto de destino
- Acción tomada por el firewall
- País de origen
- País de destino
- Aplicación descubierta

Por lo que es evidente que, para el análisis sintáctico del dato, es necesario la estandarización de la nomenclatura. [11]

Este proceso lo realiza el SIEM dependiendo de su capacidad de interpretación mediante las operaciones en su propia base de datos, parseando los tipos de formatos de logs usando expresiones regulares, así como también el procesamiento natural del lenguaje para generar un propio evento de manera que independientemente del origen se determine un propio formato ID del evento con, la descripción, hora, tipo, etc. [12]

Algunos SIEM se basan en el RDBMS que es el sistema de gestión de BD relacionales para alojar los logs y normalizarlos, otros utilizan nuevos gestores de recolección que basan su infraestructura en big data, o adoptan la tecnología Hadoop entre otras para llevar a cabo este proceso; la normalización depende mucho del proveedor y cual sea su lineamiento y oferta en el mercado. [13]

La distribución del SIEM de IBM QRadar, en su versión 7.2.6 puede reconocer el origen de 315 de fuentes de registro, sin embargo, cuando los registros no tienen una configuración coincidente, son enviados al módulo de análisis de tráfico, en el que cada evento busca coincidir con

alguno de los DSM[2] disponibles para que el SIEM pueda identificar la descripción de este. [14]

El QRadar posee una guía general de configuración de DSM donde describe las 174 fuentes de registros compatibles mediante la detección automática (análisis de tráfico) para crear orígenes de registro a partir de eventos Syslog o SNMP.

Cuando los registros no son detectados de manera automática en el QRadar, es necesario agregarlos manualmente, ya que podría suceder que, aunque Qradar soporte y analice los eventos de 174 fuentes a través de sus respectivos DSMs, exista un dispositivo con otro tipo de generación de registros y no sea compatible.

Por ejemplo, si necesitaran agregar los registros de la herramienta e-Trust Control de Acceso[3], es necesario la generación de una extensión de origen de registro (LXS), esta extensión es un archivo XML que indica cómo definir los elementos del log.

Para ello es necesario exportar previamente el registro, verificar qué campos están disponibles y son necesarios para la posterior gestión del SIEM, como el nombre del evento, dirección de origen, dirección de destino, puerto, nombre del usuario, nombre del equipo.

Una vez que se identifique la información útil, es necesario la localización de ésta mediante expresiones regulares dentro del registro. QRadar trabaja con las expresiones regulares de Java, esto es necesario conocerlo para la creación y configuración del archivo LXS. [15]

---

[2] Un *Módulo de Soporte de Dispositivos (DSM)* es un módulo de código que analiza los eventos recibidos de múltiples fuentes de registro y los convierte a un formato de taxonomía estándar que puede mostrarse como salida. ftp://ftp.software.ibm.com/software/security/products/qradar/documents/iTeam_addendum/b_dsm_guide.pdf

[3] E-Trust CA: es un administrador virtual de privilegios actualmente es conocido como PIM (Privileged Identity Management Endpoint) página web: https://www.ca.com/us/products/privileged-access-management.html

Un ejemplo de la extensión de origen del registro en formato XML basado en las expresiones regulares para e-Trust se muestra en la siguiente figura.

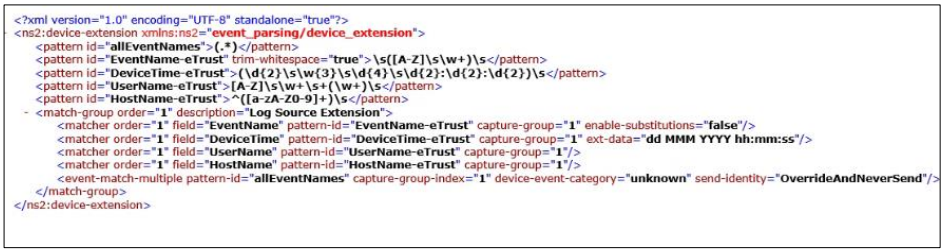

Figura 7 Formato XML de la extensión de origen de registro para e-Trust

Posteriormente se debe incorporar en el QRadar y agregar un nombre para la identificación, mediante el módulo propio de LXS; es necesario validar que la composición del archivo XML tenga la sintaxis adecuada, para evitar errores.

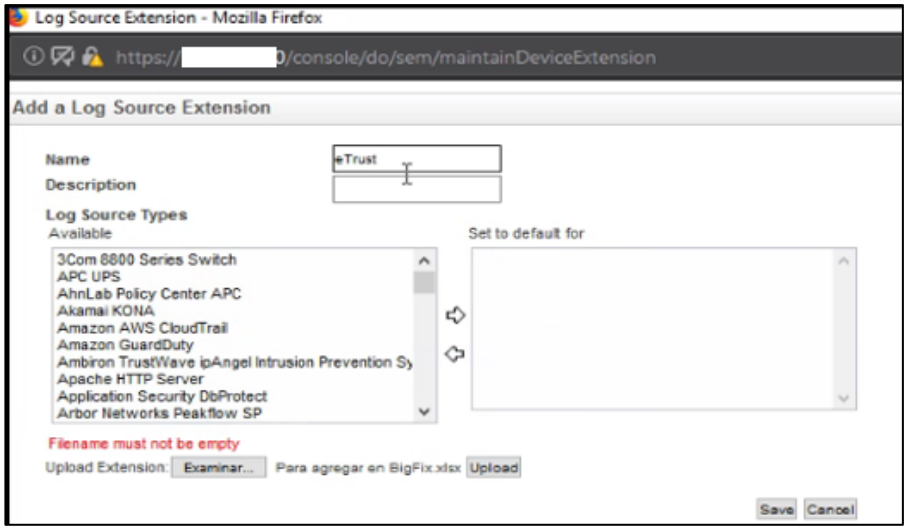

Figura 8 Modulo de la extensión de origen del registro de QRadar.

El siguiente paso es la generación del DSM Universal, que es la fuente de registro genérica ya que el DSM no lo reconoció automáticamente en un principio.

Para el ejemplo de los registros de la herramienta e-Trust la configuración se visualizaría como en la siguiente figura.

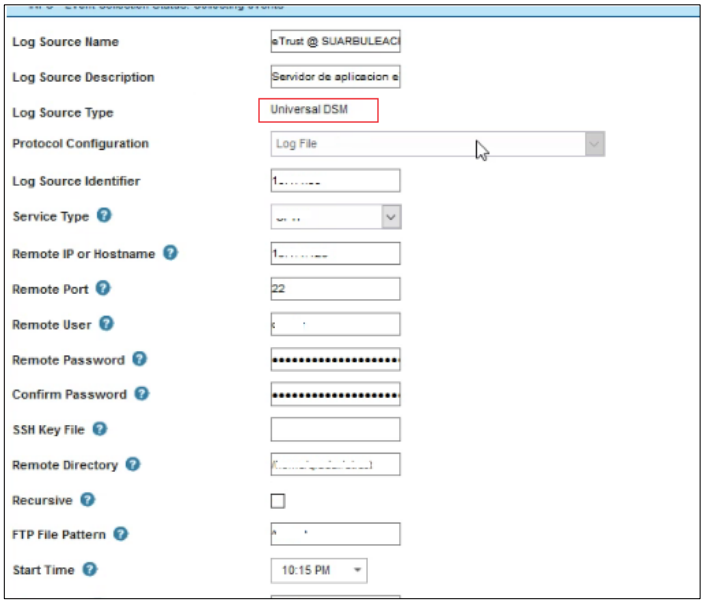

Figura 9 Modulo de Generación UDSM de QRadar

Si todo se encuentra configurado correctamente el visor de eventos del Qradar empezara a recolectar los registros con los campos coincidentes como en la siguiente figura.

Nombre de suceso	Origen de registro	Recuento de sucesos	Hora	IP de origen	IP
eTrust Login Event (permited)	eTrust @ P01	217	13 jun. 2019 14:13:31	10.1.4.88	10.
eTrust Logout Event	eTrust @ P01	215	13 jun. 2019 14:13:31	10.1.4.88	10.
eTrust Resource Access Event (permit)	eTrust @ P01	169	13 jun. 2019 14:13:29	10.1.4.88	10.
eTrust sudo Event (permited)	eTrust @ P01	25	13 jun. 2019 14:13:28	10.1.4.88	10.
eTrust Login Event (permited)	eTrust @ P01	4	13 jun. 2019 14:13:27	10.1.4.88	10.
eTrust Logout Event	eTrust @ P01	14	13 jun. 2019 14:13:27	10.1.4.88	10.

Figura 10 Visor de Eventos del QRadar

1.4 Correlación de eventos.

La correlación de eventos usa los logs alojados en el SIEM para establecer relación entre diversos sucesos que aparentemente están aislados, pero podrían estar ligados a un incidente específico.

Para lograr esto, la solución SIEM ha preestablecido un conjunto de normas basadas en los requerimientos del mercado sin embargo con frecuencia se requiere un ajuste o creación de nuevas reglas que estén de acorde al negocio particular. Dependiendo del requerimiento en la definición las reglas pueden ser simples o complejas y son definidas de forma booleana lógica para determinar si una condición especifica cumple con patrones indicados en determinados campos de datos.

Por ejemplo, para poder descubrir que están realizando un escaneo intenso de puertos a un servidor crítico, se puede configurar una regla que correlacione lo siguiente.

Ejemplo:

Regla **Posible Ataque a servidor critico**: Se deberá activar una alerta si existen 4 o más intentos de conexión en diversos puertos, desde una misma IP origen en menos de un minuto.

El atacante en una de sus fases de ataque para intentar vulnerar el sistema ejecuta un escaneo de vulnerabilidades, o un network sweep utilizando por ejemplo un nmap dirigido, en el cual como resultado encuentra un puerto habilitado y escuchando e intenta una conexión que es exitosa:

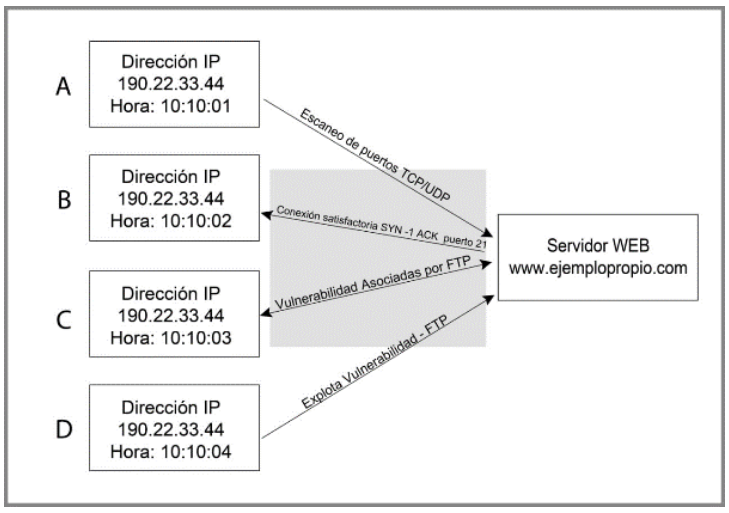

Figura 11 Ejemplo de solicitud de acceso a diversos puertos

Esta situación puede generar problemas en la infraestructura, ya que permite al atacante conocer que servicios están activos permitiéndole disponer de puertas de acceso, y facilitando la explotación vulnerabilidades, ganar accesos, provocar denegación del servicio, etc.

El motor de correlación del SIEM es importante para identificar con mayor granularidad las posibles amenazas, es por ello por lo que las empresas proveedoras han incorporado nuevos sistemas que analicen nuevos comportamientos, como por ejemplo los análisis basados en (ML) Machine Learning, otras en tecnológicas UBA o UEBA que ayudan a la gestión de modelar el comportamiento tanto de los humanos como de las máquinas dentro de la red.

1.5 Cumplimiento de regulaciones vigentes.

Con la información de eventos ocurridos en la red y almacenados de forma centralizada es posible generar procesos de auditoria validando los eventos registrados frente a lo que debió haber ocurrido. Dentro de las políticas de seguridad y las mejores prácticas que cada organización necesita o debe cumplir, existen regulaciones a obligatorias a efectuar por ejemplo PCI, SOX, 27001, FISMA, HIPAA, sin duda alguna el SIEM por sus bondades anteriormente expuestas permite cumplir con los mismos. Por ejemplo, la ISO 27001 establece procedimientos y principios generales para implementar el SGSI, y el SIEM dispone de reportes o plugins predefinidos que permiten alinearse con las normativas solicitadas.

En el caso de Splunk una distribución de SIEM, posee en sus complementos el plugin de PCI-DSS, para cumplir el estándar de seguridad de datos de la industria de tarjetas de pago [8].

1.6 Monitorización e Informes de Seguridad.

La facilidad de generar informes sobre las alertas configuradas o estándar, programar notificaciones que lleguen al correo electrónico, diario, mensual, semanal, etc. es otra característica que posee el SIEM, y que permite tener de forma tabular los resultados de eventos, mediante métricas, tablas, estimaciones, etc.

El SIEM contiene un motor de informes robusto con muchos informes definidos y la posibilidad de personalizar y crear informes con fines específicos, dependerá de la empresa distribuidora el nivel parametrización que impulse para fortalecer la generación de estos.

Las distribuciones SIEM poseen diversas interfaces amigables GUI para los usuarios, administradores, grupos de trabajo de monitoreo; así como también interface para administración por consola para procesos de actualizaciones, backups etc.

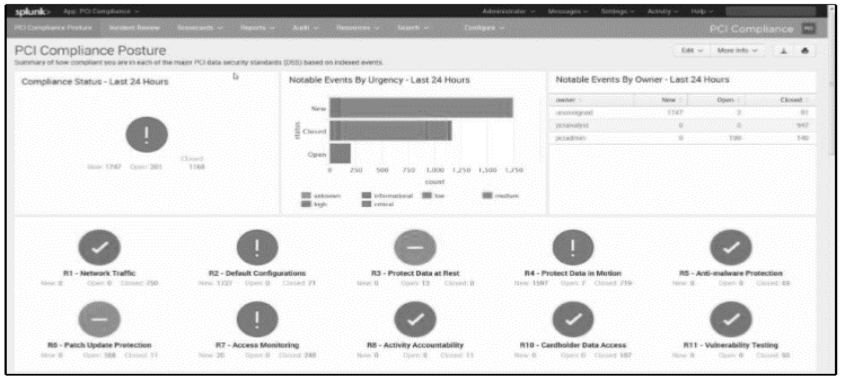

Figura 12 Ejemplo de un dashboard de SIEM Splunk Fuente: [7]

1.7 Respuesta a Incidentes.

Los componentes anteriores proporcionan la materia prima para que el SIEM explote sus capacidades y bondades. La recopilación, correlación y análisis de logs, no tendría sentido si las entidades implicadas como el SOC, CERT o CSIRT no pudieran utilizar esta información para dar respuesta inmediata a las situaciones anómalas detectadas, que podría generar en un incidente.

Un incidente de seguridad informática es una violación o amenaza inminente de violación de las políticas de seguridad informáticas.

Ya sea por un reglamento, requisito legal o la necesidad de mantener la rentabilidad de la organización, es vital proteger los activos de información. La alta gerencia generalmente impulsa el desarrollo de un programa de seguridad que se define mediante políticas y procedimientos que comunican las reglas de la organización, que podrían basarse en recomendaciones

conocidas como ISO/IEC 27035, la Guía NIST SP 800-61, ITILv3, ISO 27001 para el proceso de respuesta a incidentes.

La herramienta SIEM permite la configuración y gestión de alertas basándose en la identificación y categorización previa de los activos de tal manera que, ante un evento clasificado de riesgo alto (Anexo B), se disparen alertas, informes o advertencias que notifiquen el suceso detectado.

1.8 Análisis Forense.

En el libro de "Análisis Forense Digital" de Miguel López Delgado en el capítulo Introductorio *(pág. 5)* define:

"Al Análisis Forense Digital como un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, análisis y presentación de evidencias digitales que llegado el caso puedan ser aceptadas legalmente."

"Por evidencia digital se entiende al conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencias a éstos (metadatos) que se encuentren en los soportes físicos o lógicos del sistema atacado". [16]

El análisis se basa en encontrar patrones, comportamientos, o exposición de información que se encuentra oculta. Por tal motivo la herramienta SIEM se convierte en un arma de apoyo ya que permite la recopilación centralizada de registros, la correlación de eventos, y genera informes que evidencien patrones en datos de registro incoherentes, estas funciones son importantes para las investigaciones sospechosas y la detección violaciones de datos. [17]

Además, los registros adecuadamente almacenados y protegidos podrían ser útiles para las investigaciones de incidentes internos e incluso podrían ser admisibles como prueba ante un tribunal, para lograr esto existen recomendaciones realizadas por entidades de control como la NIST[4], que

[4] NIST: Instituto Nacional de Estándares y Tecnología https://www.nist.gov/

publicó una Guía para la gestión de registros de seguridad informática en el 2006. [18]

Algunos SIEM poseen módulos adicionales que trabajan directamente en este aspecto como lo es en IBM el módulo: IBM **Security QRadar Incident Forensics** o el **Splunk Life ITSI** dentro de la distribución Splunk.

CAPITULO 2 LOS PECADOS DEL SIEM.
INCONVENIENTES EN LA IMPLEMENTACION DEL SIEM.

En el capítulo anterior se expuso a grandes rasgos que es y cuáles son las características del SIEM, sin embargo, el valor fundamental y su nivel de eficacia como una herramienta de protección ante las amenazas en una entidad está ligada directamente a su forma de implementación, es por ello por lo que en este capítulo de investigación se expondrá cuáles son algunos de los problemas que surgen al momento de implementar la herramienta.

2.1 Dejarse engañar por la demo de un proveedor.

Un inconveniente que podría surgir cuando se toma la decisión de incorporar una herramienta SIEM, estaría en la elección de la distribución, marca y modelo, es decir, en el proceso inicial donde nace la idea, y se procede a hacer la búsqueda para adquirirla.

Este paso es fundamental tomar en consideración para todo el proceso, ya que un análisis previo podría determinar costo beneficio, evaluar el FODA[5], soporte, escalabilidad, ventajas, desventajas, etc.

Según el libro *"SIEM Implementation" de David R. Miller" en el capítulo Introductorio (pág. 39,40)* entender el modelo de negocio de la empresa, basado en los valores, línea de productos, servicios, objetivos, metas, entre otros, es primordial antes de adquirir cualquier herramienta ya que de eso dependerán los motivos por los cuales la entidad valore adquirir un SIEM frente a otro.

[5] FODA: acrónimo de Fortalezas, Oportunidades, Debilidades, y Amenazas herramienta estratégica que permite conocer la situación de una institución, empresa, o proyecto.

Como se describió en el capítulo 1 del presente trabajo, un SIEM permite alojar registros, ayudar en la gestión de incidentes de seguridad, proporcionar capacidad de informes, además mediante la configuración de reglas y la generación de alarmas ayuda a cumplir con regulaciones o certificaciones, todo esto como una medida para intentar reducir el riesgo que posee una organización frente a ataques o intentos de ataques a los que está expuesta.

Por lo tanto no es raro que el departamento de Seguridad de la Información use al SIEM como una herramienta de apoyo que le permita conocer qué actividades ocurren en su red y mediante políticas de seguridad, basadas en requerimientos del negocio cumplir con procesos regulatorios, mantener el grado de confidencialidad, promover el cumplimiento de normativas, controles de seguridad, etc.

Sin embargo, el problema está cuando se adquiere, sin analizar las necesidades de la organización, es decir, el Oficial de seguridad de la información (CISO) a cargo elige la herramienta simplemente revisando los demos[6] que las empresas proveedoras exponen, y no hace un análisis exhaustivo o pruebas de concepto adecuadas.

Por ejemplo, podría elegir un SIEM basado en que le pareció que la herramienta posee gran capacidad de procesamiento de datos por segundo, sin embargo no analizó la saturación que esta tendrá en su red, otra razón podría ser porque le permita alojar grandes cantidades logs por mucho tiempo debido a su capacidad de almacenamiento, sin tomar en consideración que la misma no posee interfaces graficas de administración amigables, o no posee soporte externo para actualización de la herramienta, etc.

Las decisiones de selección de un SIEM recomendado por Gartner deben ser impulsadas por requisitos específicos de la organización en áreas tales como [19]:

[6] Demo: demostración reducida de un programa para poder evaluarlo antes de adquirirlo.

- Importancia relativa a las capacidades básicas frente a las características avanzadas.
- Limitaciones presupuestarias.
- Escala del despliegue.
- Complejidad del producto (implementación, ejecución, uso y soporte)
- La implementación de proyectos de la organización de TI y las capacidades de soporte tecnológico.
- Integración con aplicaciones establecidas, monitoreo de datos, tipo de infraestructura.

Para las organizaciones que planean utilizar proveedores de servicios externos para el despliegue, configuración y procesos de actualización del SIEM deben considerar productos que ofrezcan soporte de servicio continuo y adecuado.

Dependiendo del motivo por el cual se pretenda la adquisición de la herramienta SIEM, el mercado oferta distintos productos (Anexo C), con diversas características, dependiendo del tamaño de la empresa, necesidades, etc.

Según el último informe de la consultora de investigación de las tecnologías de la información Gartner éstos son los SIEM abanderados en el mercado [19].

El cuadrante evalúa a los proveedores de tecnología con respecto al escenario de selección de tecnología más común:

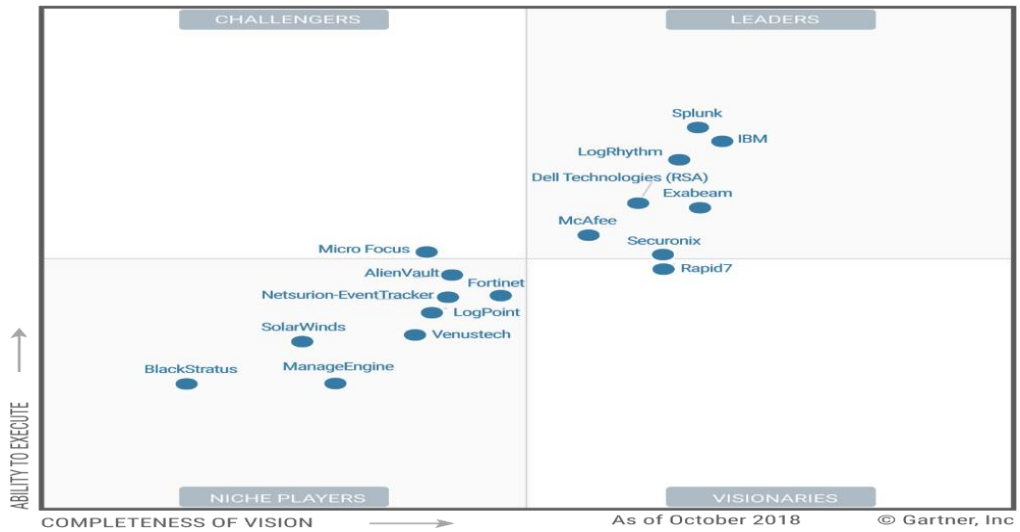

Figura 13 Cuadrante Mágico del SIEM fuente [19]

A medida que se analiza cada una de las ofertas de los proveedores, algunas empresas podrían también llegar a evaluar desarrollar su propio recurso de SIEM, para tener soluciones personalizadas a sus necesidades, definiendo que módulos o funciones necesita implementar y cuáles no.

Sin embargo, este análisis se debe tomar con mesura considerando el costo de adquirir un SIEM ya disponible en el mercado, frente al costo de contratar personal dedicado a diseñar, implementar, mantener una solución personalizada. [19]

Es necesario consensuar que postura se va a considerar cuando se plantee adquirir el SIEM, para disminuir dificultades en la implementación.

2.2 Subestimar costos.

Otro problema recurrente es subestimar el costo necesario para cumplir la implementación y funcionamiento. Cuando se evalúa el costo de la herramienta no solo se debe revisar el costo de licencias, implementación, o renovación, también la empresa necesita considerar otros costos, como por ejemplo el de capacitación para los empleados, soporte continuo, etc.

Además, resulta de suma importancia evaluar la escalabilidad basada en el número de activos (equipos) mínimos necesarios para la implementación, así como también estimar el costo de horas del personal que

va a administrar la herramienta. Toda organización debe realizar, previa adquisición de un SIEM, un estudio comparativo, o benchmark, para determinar el costo-beneficio de las soluciones disponibles en el mercado.

En el reporte de la empresa de seguridad Alert Logic se indica que, aunque se podría adquirir un SIEM por un valor de U$$100.000 dólares, es común que las implementaciones de este tipo en las empresas cuesten alrededor de U$$1 millón de dólares con tarifas de U$$30.000 solo en mantenimiento valores a los cuales es necesario sumar costos de infraestructura de red, computo, almacenamiento nuevas reglas, el monitoreo, e investigación de alertas. [20].

La inversión también está en el tiempo, tiempo que se traduce a dinero, tiempo para implementar, configurar, mantener, capacitar, y a pesar de que la tecnología SIEM está dentro de las herramientas más importantes en Seguridad Tecnológica, algunas empresas desisten de adquirirla por no contar con el presupuesto, así como otras en su gran mayoría superan presupuestos y plazos planificados. [20]

Según el estudio de investigación realizado por el Instituto Ponemon, el 25 % de los costos de SIEM están relacionados con la compra inicial, mientras que el 75 % restante se destina a la instalación, el mantenimiento y la dotación de personal, en donde se involucran los costos iniciales de la licencia, la implementación, la administración continua, la renovación, la integración de las fuentes de datos, la capacitación del personal para ejecutar el SIEM [21].

Alrededor del 78 % de las organizaciones encuestadas le dijeron a Ponemon que solo tienen un miembro del personal dedicado a su SIEM y, a pesar de esto, el 64 % informó haber pagado más de U$$$ 1M al año en los costos relacionados con SIEM, sin tomar en consideración por ejemplo las recomendaciones que Gartner hace en su publicación (“Como superar las causas comunes de fallas en la implementación de SIEM”, mayo de 2017): “Para un banco mediano típico, se requiere un personal mínimo de ocho a diez personas para ejecutar un monitoreo de eventos de seguridad (SIEM) 24/7 dedicado de operación". [22]

Continuando con la investigación de Ponemon, en promedio, las organizaciones representadas en su investigación gastaron $ 15.6 millones en inversiones para habilitar tecnologías de seguridad en el año fiscal en curso y un promedio del 25 % del total está destinado al SIEM.

En la siguiente figura se puede observar el porcentaje de asignación de gastos en la inversión de la solución SIEM, en el cual se visualiza que el mayor gasto está en la parte del capital humano, seguido del proceso de instalación, adquisición de software, mantenimiento anual y hardware.

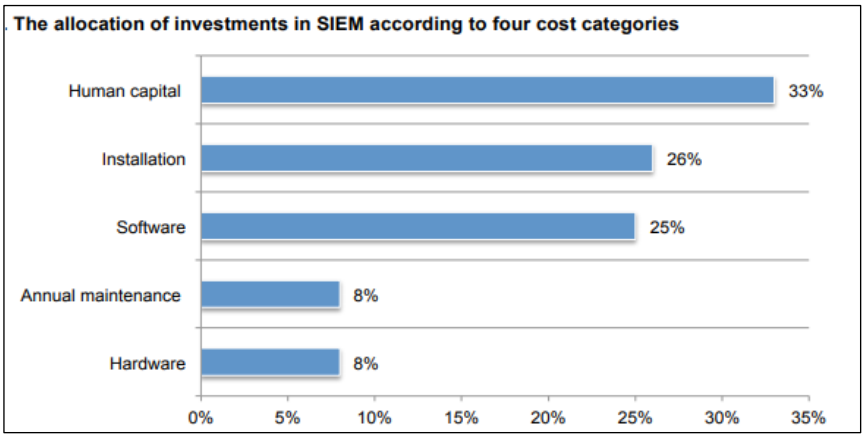

Figura 14 Asignación de gastos para un SIEM Fuente: [21]

Dentro del capital humano los gastos laborales promedian U$$1.78 millones en implementación en curso y mantenimiento, un promedio de U$$ 1.33 millones se gasta en contratistas, consultores y proveedores de servicios gestionados y se gasta un promedio de U$$ 1.10 millones en otros costos de bolsillo pagados por servicios relacionados con la instalación y el despliegue de SIEM.

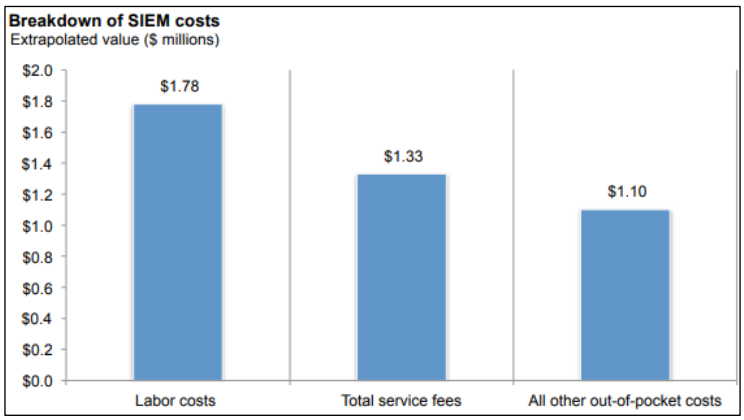

Figura 15 Indicador de Costos SIEM Fuente [21]

El subestimar los costos provoca que como cualquier proyecto con baja planificación alcance rápidamente los umbrales máximos monetarios, que fueron inicialmente delimitados y genere dificultades para continuar con el despliegue y funcionamiento, llegando a casos más radicales donde el proyecto definitivamente fracase y a la herramienta SIEM la terminen apagando.

2.3 Recolectar más registros no significa mayor visibilidad.

El grado de efectividad en detección del SIEM es proporcional a la calidad de registros que se recolecten. Alojar enormes cantidades de registros no significa tener un gran porcentaje de información válida, ya que muchos de los datos podrían ser irrelevantes. Para empezar, es necesario entender que al registro no se lo puede clasificar de forma binaria como “bueno o malo”, para ello es importante conocer el origen y el tipo de dato y posteriormente decidir si es necesario su análisis y recolección, segundo es importante entender que los datos seleccionados son siempre reactivos ya que el evento que se ha guardado en la base de datos ya sucedió.

Los resultados del informe de NETWRIX[7] indican que casi el 81% de los encuestados declararon que el SIEM contiene demasiado ruido. Al igual que indicaron que cerca del 65% de las empresas presentan dificultades para encontrar datos de registro en el SIEM, solicitado para temas de auditoria [23].

[7] Netwrix Corporation Empresa de seguridad tecnológica https://www.netwrix.com

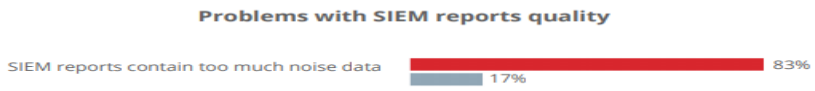

Figura 16 Resultado de Encuesta realizada por Netwrix Fuente: [23]

Bajo esta misma premisa el estudio realizado por Cisco *"¿Qué podemos perder al no implementar la seguridad adecuada en nuestro entorno de TI?* ", solo el 28 % de las alertas de seguridad investigadas resultan ser legítimas, es decir, de una muestra de 5000 alertas, 2200 no son investigadas y dentro de ellas 616 son importantes. [24]

Por ejemplo, tener un servidor con sistema operativo Windows en el que su visor de eventos evidencia grandes cantidades de logs por segundo, no significa que registre todos los logs importantes, ya que de forma predeterminada muchas actividades están desactivadas para su recolección, por ejemplo, los logs de registro de proceso, logs de línea de comando, cambio de hora, registros de cambios en controlador de Windows, etc. Activarlos proporcionaría tener información útil al igual que también incrementaría el gran volumen de logs, por lo tanto, es importante determinar los registros necesarios.

El libro *"SIEM Implementation de David R. Miller" capítulo 5 Anatomía del SIEM (pág. 80)* recomienda que una vez que se identifiquen los dispositivos a recolectar, es necesario determinar que registros se necesitan y porqué. Ya que una razón para su recopilación podría ser simplemente cumplir con tiempos de alojamiento y recolección para cumplimientos normativos como SOX, o PCI, mediante el almacenamiento de copias de los registros, así como otra razón está ligada a recolectar logs que puedan proporcionar información importante para proteger el entorno, ayudar a diagnosticar problemas a medida que surjan en la red. [2]

Hay que considerar que no se necesitan todos los registros, ya que es necesario mantener el equilibrio entre la cantidad de registros que puedan ser almacenados frente a los que puedan ser procesados por el SIEM tomando en cuenta que los recursos de almacenamiento son finitos. [23]

Los registros irrelevantes podrían contribuir con la generación de ruido, por lo que es necesario identificar y gestionar el límite de logs con los que se contará para la implementación.

El ruido se genera por los datos irrelevantes recolectados, los mismos que posteriormente disparan alertas falso-positivas; el reducir el ruido reduciría estas alertas falso-positivas.

Se podrían tomar medidas para reducir los falsos positivos, con revisiones y un alto grado de ajuste periódico a la configuración de la alerta, sin tocar el ruido, pero no sería favorable ya que afectaría y sobrecargaría el espacio de almacenamiento, así como el consumo de licencias.

En el libro *"SIEM Implementation de David R. Miller" se* recomienda que para gestionar adecuadamente los logs es necesario responderse algunas preguntas:

¿Cuánto tiempo se deben conservar los registros?

Esta primera pregunta trae consultas con respecto a la retención de datos y la destrucción de datos. Las regulaciones o leyes de la industria pueden exigir que se retengan ciertos tipos de datos durante un período de tiempo determinado, también puede tener controladores legales y funcionales que determinen cómo desechar la información después de un período de tiempo.

¿Cuánta información de registro deberá retener?

Incluso en una red pequeña, la cantidad de logs e información de eventos que puedan producirse podría agotar el almacenamiento disponible si no está limitado, ya que es de común conocimiento que se recolectan cientos de millones o incluso miles de millones de registros por día, por lo que es necesario definir la cantidad de almacenamiento razonablemente basándose en los requisitos de retención y destrucción de datos.

¿Qué tipo de registros de sistema de información debe retener?

Como se ha mencionado anteriormente existen diversas fuentes de registros dependiendo del dispositivo, su sistema operativo, funcionalidad, etc. En el presente trabajo final se hará enfoque en el estándar syslog (RFC 5424) para el envío de registros.

Por syslog se conoce tanto al protocolo de red como a la aplicación que envía los mensajes de registro. La estructura del syslog permite que el mensaje de registro disponga de una cabecera y descripción indicando su prioridad. Esta prioridad es un número de 8 bits que indica el tipo de dispositivo que ha generado el mensaje, la importancia o severidad de este, se puede visualizar en el (Anexo D) [25] cada descripción de los mensajes.

Luego de conocer los códigos de severidad, es posible identificar qué log es más indispensable que otro, ya que al disponer registros de toda clase; es necesario considerar los eventos que involucren al ámbito de la seguridad para beneficiar la gestión y rendimiento del SIEM. [26]

Es necesario eliminar la mentalidad de registrar y enviar cualquier log a la herramienta SIEM, ya que es ineficaz debido a la cantidad de registros por segundo que generan los equipos de una entidad.

2.4 Problemas en la construcción de casos de uso.

Un caso de uso dentro del SIEM es una forma formal de definir una actividad de seguridad, esta se compone de parámetros que son necesarios para la activación de alertas, los casos de uso pueden ser comerciales o del sistema.

Es importante comprender la diferencia entre los dos, un caso de uso comercial es un requisito comercial general, por ejemplo: “identificar los eventos de inicio de sesión fallidos”. Un caso de uso del sistema es el componente propio tecnológico en el SIEM, por ejemplo: “alerta en un evento de inicio de sesión Windows fallido”, y especifica de forma explícita los datos que está usando el sistema. [27]

Los proveedores del SIEM usualmente no visibilizan la diferencia entre un caso de uso comercial frente a un caso de uso de sistema que es más detallado para el SIEM. La identificación de estos casos es necesaria en el proceso de evaluación de la herramienta antes de seleccionar la solución SIEM. Ya que al analizarlo exhaustivamente con los datos disponibles que posee la organización, permite definir y desarrollar los casos de usos de forma más explícita. [27]

Los casos de uso se configuran como reglas, estas reglas son el método de respuesta para identificar las amenazas, por lo tanto, la calidad de información almacenada influencia la eficacia de los casos de uso.

En el informe del instituto SANS “*Effective Use Case Modeling for Security Information & Event Management*” se recomienda la técnica de investigación de las “Cinco W” como las 5 preguntas necesarias a responder mediante los caso de uso, las cuales son*. ¿Cuándo ocurrió el evento?, ¿Quién estuvo involucrado?, ¿Qué sucedió?, ¿Donde sucedió? y ¿Por qué ocurrió? y propone una metodología llamada* TDBUMO[8] como guía para conseguir responder las preguntas realizadas. (Anexo E). [27]

[8] TDBUMO: acrónimo en inglés: TopYDown BottomYUp MiddleYOut

La mayoría de las distribuciones del SIEM poseen configuraciones nativas sobre distintos casos de uso en forma de plantillas para su posterior gestión, las mismas están basadas en lo que los proveedores consideran relevantes; otras distribuciones por costos mayores incluso presentan su herramienta con componentes adicionales de casos de uso basados en normativas como SOX, PCI, HIPPA, etc. Por ejemplo, casos de uso que alerten sobre inicios de sesión efectivos, inicios de sesión denegados, instalación de aplicaciones, creación de usuarios, eliminación de usuarios necesario para el control etc.

Sin embargo, la mayoría de estos casos de uso carecen de campos en sus informes. Ya que, si bien los mismos identifican cuando, como ocurrió el evento, y quien realizo la acción, no se identifica adecuadamente desde donde y por lo tanto no es completamente procesable el caso de uso, lo que generara un rendimiento poco eficiente del SIEM, esto afectara a su utilidad y en última instancia afecta el retorno de la inversión de la solución. [27]

La selección y creación de casos de uso, depende exclusivamente del motivo comercial para el cual fue adquirida la herramienta, sin embargo, como guía la compañía de Software NetIQ [26], recomienda que los casos de uso deberían estar enfocados en cumplir las siguientes necesidades:

- Informes de cumplimiento:
- Detección avanzada de amenazas
- Resolución de problemas operativos de sistema, red, y operaciones.

Para la generación de los casos de uso que precisan ser configurados por necesidades de cumplimiento de normativas, el Instituto SANS recomienda una guía para una exitosa administración de los registros en el SIEM llamado "***Successful SIEM and Log Management Strategies for Audit and Compliance***". [28].

Cuando la creación de los casos de uso está basada en la detección avanzada de amenazas, o en solventar problemas operativos, es sustancial conocer las necesidades adicionales que posee la institución.
Por ejemplo, cabe preguntase, ¿Cuáles son las expectativas para intentar mitigar las vulnerabilidades que se identifiquen frente a las alertas mundiales diarias que se encuentren? Algunas recomendaciones y mejores prácticas para intentar resolver este interrogante se ilustran en el (Anexo F) [29].

Estos casos de uso no son los únicos necesarios ya que como se ha mencionado anteriormente cada empresa posee requerimientos adicionales, que deben plasmarse con la construcción de casos de uso personalizados de acuerdo con las herramientas que posee la misma para ayudar a la seguridad de la empresa.

Adicional a ello las reglas por defecto, al igual que las que se creen posteriormente requieren mantenimiento, actualización, personalización y un control de ciclo de vida continuo para reducir falsos positivos ya que necesitan contextualización de acorde a las necesidades propias de la entidad, el no hacerlo conlleva a la inundación de alarmas falsas positivo dentro del SIEM.

El punto es evitar dos problemas, el primero la falta de creación de nuevos casos de uso, así como también la construcción de casos de uso ineficientes y de poco apoyo para la institución.

No generar suficientes reglas de correlación de amenazas basadas en nuevos casos de uso significa que podría perder amenazas serias y no evolucionar.

2.5 Falta de personal adecuado administrando el SIEM.

No es un secreto la falta de personal en áreas de tecnología y seguridad cibernética en el mundo gracias al crecimiento mundial de la tecnología, el nacimiento de nuevas plataformas de comunicación, infraestructura, diversas aplicaciones, etc. Debido a ello la asociación no lucrativa más grande del mundo de profesionales certificados en seguridad (ISC)² presentó en febrero del 2019 su último informe realizado sobre "**La brecha laboral de seguridad cibernética global**" mediante encuestas investigativas desarrolladas en octubre del 2018 [30] en el cual indica que:

- Existe una brecha mundial entre ofertas de empleo y personal calificado para el área de 2,93 millones, América del Norte tiene el siguiente número más alto de brechas con 498,000, mientras que EMEA (Europa, Oriente Medio, África) y Latinoamérica contribuyen con un déficit de personal de 142,000 y 136,000, respectivamente.
- El 63% de los encuestados informa que sus organizaciones tienen una escasez de personal de TI dedicado a la ciberseguridad. El 59% dice que sus empresas están en riesgo moderado o extremo de ataques de ciberseguridad debido a esta escasez.

En el informe explicado anteriormente por parte de Cyphort y Ponemon, Franklyn Jones, director de marketing de la consultora expresó que "La cantidad de datos que posee el SIEM es demasiado alto, mientras que la calidad de los datos es demasiado baja, y que existe personal inadecuado para minimizar ese ruido y maximizar el valor subyacente ". Dentro del mismo se refleja que el 68% de los encuestados dice que su SIEM es útil, pero necesitaría personal adicional y adecuado para maximizar su valor ya que es su administración es muy compleja.

La complejidad de administrar la herramienta sabiendo que existe poca demanda de personal con experiencia técnica en este tipo de herramientas,

termina siendo un inconveniente no mencionado por las empresas distribuidoras de SIEM.

Es importante añadir que, para la administración de un SIEM, las entidades están designando poco personal, esto se valida en el mismo informe de Cyphort y Ponemon que menciona que el 78 % de los encuestados dice que existe una o menos de una persona dedicada a la administración y mantenimiento del SIEM.

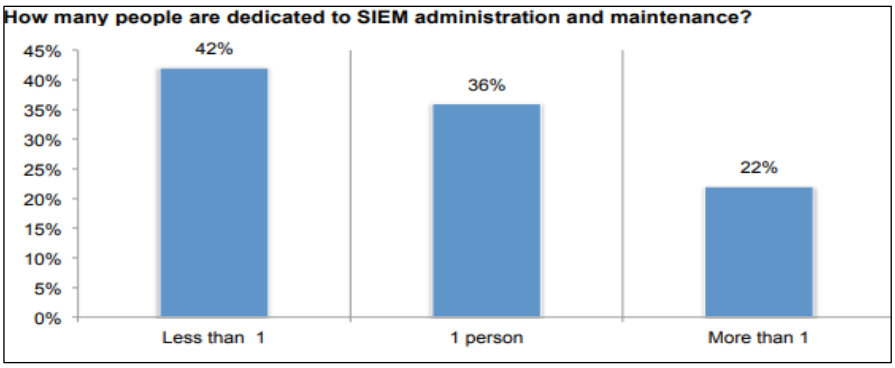

Figura 17 Indicador de # administradores de un SIEM Fuente: [21]

Un recurso que se puede adoptar como una posible salida para el departamento de seguridad es encontrar una solución SIEM que contenga interfaces de usuario amigables que se adapte al equipo de seguridad de TI y su entorno de TI.

No es recomendable como se mencionó en el primer punto seleccionar una solución a ciegas, se debe consultar y consensuar con el equipo de seguridad para que haga la valoración ya sea mediante una demostración del producto mediante pruebas reales, o con casos de uso basados en las necesidades, ambientes controlado de desarrollo, etc.

Es necesario elegir una solución que permita un desarrollo largo plazo como así también resulta indispensable que la misma incluya cursos de inducción para los profesionales.

2.6 Respuesta pasiva a las amenazas de seguridad.

Un factor crítico y a menudo pasado por alto para obtener mayor valor en el SIEM, es el requisito de interpretación y seguimiento sobre las alertas una vez que las amenazas son detectadas. Las organizaciones requieren información clara sobre los incidentes para comprender el potencial impacto, clasificarlo y responder con algún proceso de remediación.

La mayor parte del esfuerzo continuo requerido de un SIEM es monitorear e investigar las alertas identificadas. El personal de seguridad informática normalmente pierde dos tercios de su tiempo investigando sobre alertas falsas, mientras que las infracciones reales pasan desapercibidas, en un promedio de 74 días, según el informe mundial de M-Trends 2019 [31].

El incumplimiento del 2013 es el ejemplo más famoso de la importancia de revisar las alertas de seguridad. Target Corp. tuvo alertas activadas por FireEye que indicaban que estaban bajo ataque, pero no fueron investigadas y los hackers robaron información de más de 40 millones de tarjetas de crédito y débito de sus clientes [32].

En el informe de Ponemon, el 76% de los encuestados valora su SIEM como una herramienta de seguridad estratégicamente importante. Sin embargo, solo el 48% está satisfecho con la inteligencia accionable que obtiene de su SIEM ya que no toman medidas sobre lo reportado

Las alertas SIEM requieren interpretación y validación por profesionales de seguridad para determinar cómo actuar. Anton Chuvakin de Gartner manifiesta lo siguiente: “Las alertas necesitan ser revisadas a través de un proceso de selección de alertas para decidir si se convierten en un incidente”, de ser así el problema debe resolverse de inmediato; si fuese una falsa alarma se debería afinar la regla de alerta para reducir los falsos positivos [33].

Solo después de que una alerta ha sido revisada se convierte en un incidente, el cuál requerirá inmediata respuesta. El departamento de Seguridad de la Información deberá agregar personal o recursos adicionales para mantenerse al día. Con la cantidad de detección de datos, solo señalar que existe una alarma no es suficiente. El operador o analista debe ser capaz de comprender el riesgo y proporcionar recomendaciones para cada incidente, para poder priorizar la acción.

Todo método de respuesta debe tener un plan concreto, y el mismo deberá establecerse de acuerdo con las políticas que se determinen en la entidad. Para ayudar en la gestión, el NIST[9] (SP 800-61) [34] propone una guía de manejo de incidentes, con recomendaciones a tomar en cuenta para mejorar y gestionar de manera eficiente mediante siguiendo el ciclo como en la figura siguiente:

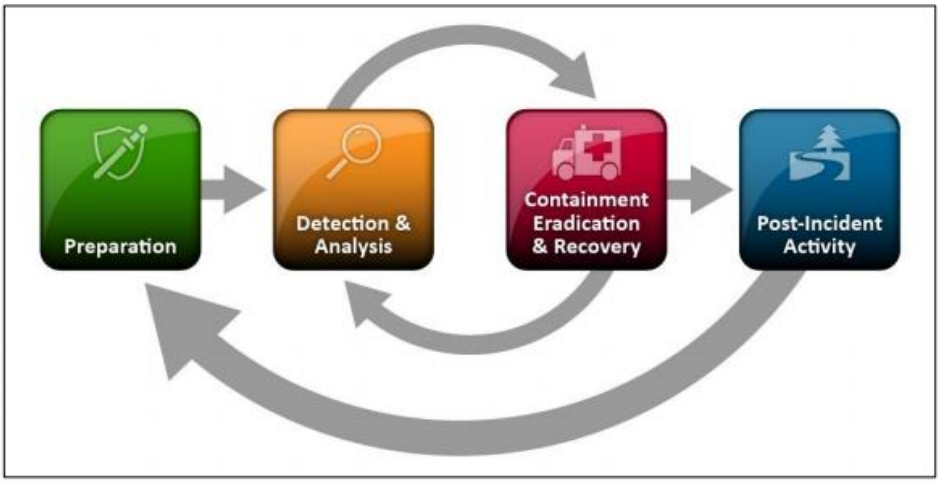

Figura 18 Ciclo de vida de la respuesta a un incidente Fuente: *[34]*

Una herramienta SIEM permite configurar los valores de prioridad de las amenazas detectadas para ayudar al analista de seguridad a enfocarse en otros temas. Sin embargo, es necesario contar con alguna guía, como la mencionada para evaluar y responder a los incidentes a medida que surgen y para refinar y ajustar las reglas de detección.

[9] NIST: National Institute of Standards and Technology

2.7 Mantenimiento inadecuado a la herramienta SIEM.

El SIEM demanda operatividad 24 horas 7 días, durante 365 días al año, no tomar en consideración aquello es crítico ya que el SIEM exige continuidad operativa, con mantenimiento y vigilancia por parte de los administradores del servicio. Cuando no se identifican las necesidades de la herramienta la efectividad y productividad disminuye.

Con la herramienta instalada, los componentes desplegados y la configuración de acuerdo con las necesidades de la empresa; el personal que administra el SIEM podría suponer que no es necesario ningún mantenimiento a priori. Sin embargo, el no contemplarlo dentro de los requerimientos afectaría el costo total del producto en un futuro, aspecto analizado previamente en el punto 2 “Subestimar Costos”.

Cuando se descubre una vulnerabilidad en algún componente del SIEM, es posible que sea necesario una actualización. Este proceso podría necesitar de soporte externo, es decir contar con proveedores que, a más de informar a los clientes sobre la disponibilidad de un parche, también gestionen y colaboren con recomendaciones necesarias para la actualización de la versión. Este proceso forma parte del mantenimiento necesario dentro del ciclo de vida del SIEM, no darle importancia implicaría asumir riesgos.

El mantenimiento y gestión del espacio donde se alojan los logs dentro del SIEM también es fundamental para evitar la saturación y perdida de registros en un futuro, así como también consumo del tráfico de red entre el SIEM y los equipos que envían los logs ya que esto no debe saturar y sobrecargar el ancho de banda que dispone la entidad.

Como los ejemplos mencionados, existen otros aspectos relacionados con las copias de seguridad, implementaciones para el cifrado de los registros que garanticen la confiabilidad de los datos y más situaciones dentro del mantenimiento del SIEM que son necesarias identificar y dar curso.

Dentro de las empresas existen políticas de control y mantenimiento avalados por el departamento de Seguridad, por lo tanto, es importante que la herramienta SIEM se alinee bajo las mismas normativas como otro activo, en el cual se incluyan controles basados en pruebas de penetración, análisis de vulnerabilidades y auditorias de seguridad entre otras.

Como una guía de los puntos importantes a tomar en cuenta en la fase de mantenimiento, el instituto SANS en el documento "*Security Development Life Cycle versión 5*" presenta los procedimientos mínimos necesarios a tomar en consideración para el mantenimiento de la herramienta SIEM. (Anexo G)

CONCLUSIONES.

Es importante poder contar con herramientas que permitan ayudar a mitigar riesgos de ciberataques a los que diariamente se enfrentan las empresas, para ello el SIEM se convierte en un arma de apoyo en búsqueda de ese propósito.

En el desarrollo de este trabajo final se analizaron algunas situaciones o pecados que se cometen cuando se adquiere la herramienta.

- Es posible que al momento de considerar que tipo de SIEM comprar el CISO se deje engañar por la demo inicial que presenta el proveedor y termine eligiendo una; sin embargo, es necesario analizar qué tipo de SIEM adquirir basándose en la cultura de la organización, identificando las necesidades del negocio y posterior a ello, poder tomar una decisión final.

- Subestimar los costos es otro pecado que se comete al momento de la adquisición, se debe tomar en cuenta que el costo de la solución no exceda el benefició que se busca de la herramienta, así como también incluir en el costo, el valor que se genere en todas y cada una de las fases de implementación del SIEM.

- La recolección de registros debe ser de calidad, es decir es necesario conocer que es lo que se va a recolectar y con qué finalidad, si se envía basura al SIEM, se procesará basura dentro de él, mayor cantidad de registros no significa mayor visibilidad de lo que sucede en la entidad.

- La selección y creación de casos de uso depende del objetivo comercial de la empresa sin embargo para cada uno de ellos es necesario contar con información de: ¿Cuándo sucedió?, ¿Quién lo realizó?, ¿Qué fue lo que ocurrió?, ¿Dónde se generó?, y ¿Por qué se ocasionó la situación?.

- La falta de personal administrando la herramienta, está ligada completamente al déficit de personal en áreas de seguridad informática a nivel

mundial, esto es un tema que compete a toda la sociedad y es necesario se siga fomentando lugares donde aprender sobre la ciberseguridad.

- El SIEM alerta sobre las situaciones encontradas, pero depende de los administradores de la herramienta realizar acciones de respuesta a las alertas detectadas ya sea para mitigar un riesgo, o afinar las alarmas. Es necesario siempre dar respuesta a las amenazadas detectadas.

- El mantenimiento del SIEM debe ser tan crítico como cualquier otro servicio o servidor indispensable dentro de la entidad, ya que el mismo solicita atención 24/7 los 365 días del año.

ANEXOS

Anexo A. DEFINICIÓN SIM Y SEM

SIM (Security Information Management), El SIM permite recopilar y alojar registros de dispositivos tecnológicos, mediante solidas capacidades de almacenamiento permitiendo el análisis gestión y administración informes de cumplimiento solicitado por la institución o entes regulatorios. [35]

SEM (Security Event Management) “Administrador de eventos de seguridad” permiten analizar amenazas en tiempo real, basadas en la gestión de eventos y respuesta a incidentes mediante la recopilación de registros de dispositivos de seguridad como por ejemplo IDS, IPS, Firewalls, WAF, Proxys, Antivirus, etc. [35]

Anexo B. CLASIFICACIÓN DE ACTIVOS CRITICOS.

Para clasificar los activos en críticos o no críticos, es necesario conocer y evaluar los riesgos a los que se encuentran expuestos los activos apoyados en la confidencialidad, integridad y disponibilidad; de lo contrario no se podrá identificar lo que se necesita proteger.

Riesgo: Posibilidad de que ocurra algún evento que tenga un impacto sobre los objetivos. (AS/NZS 4630).

Los riesgos para tener en cuenta a los que se puede enfrentar una institución son de índole económicos, financieros, operativos, tecnológicos, de reputación, cumplimiento, legal, etc. Y se miden de acuerdo con su probabilidad de ocurrencia (frecuencia) por la consecuencia (impacto) que genera (ISO/IEC 27005).

Por lo tanto, un activo tiene un nivel más crítico basado en su nivel de exposición al riesgo, para simplificar la identificación se

pueden establecer niveles de clasificación como en el ejemplo de la siguiente imagen.

ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
Base de Datos de Cobranzas	Fraude	Muy Alta	Seria	Extremo
Base de Datos de Finanzas	Incumplimiento legales	Alta	Significativa	Alto
Base de Datos de Marketing	Fuga de información	Medio	Menor	Bajo

Ilustración 1 Análisis de activos críticos

De esta manera con una clasificación se puede estimar el grado de afectación al que se expone un activo de la organización frente a cualquier situación no esperada.

La herramienta SIEM permite la configuración y gestión de alertas basándose en la identificación y clasificación previa de los activos de tal manera que, ante un evento clasificado como crítico, se disparen alertas, informes o advertencias que notifiquen el suceso detectado.

Anexo C. COMPARATIVA PRODUCTOS SIEM.

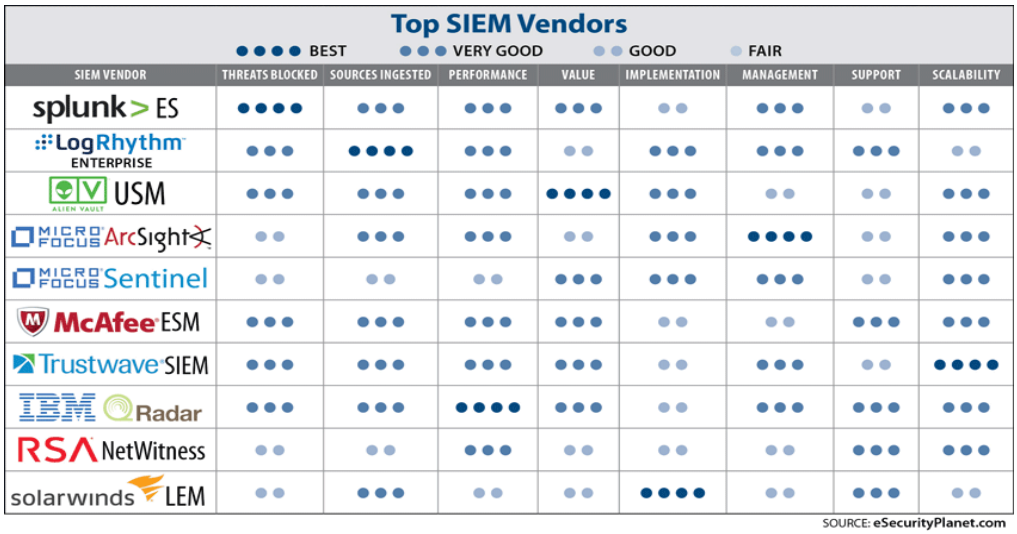

Figura 19 Comparativa de SIEM Fuente: [37]

ANEXO D. CODIGO RECURSOS SYSLOG.

Se adjuntan los códigos de recursos del Syslog RFC 5424 *[4]*

Código de Recursos:

0 mensajes del kernel
1 mensajes de nivel de usuario
2 sistema de correo
3 demonios del sistema
4 mensajes de seguridad / autorización (nota 1)
5 mensajes generados internamente por syslog
Subsistema de impresora de 6 líneas
7 subsistema de noticias de la red
8 subsistema UUCP
9 demonio de relojes
10 mensajes de seguridad / autorización
11 demonio FTP
12 subsistema NTP
13 auditoría de registro
14 alerta de registro
Demonio de 15 relojes
16 uso local 0 (local0)
17 uso local 1 (local1)
18 uso local 2 (local2)
19 uso local 3 (local3)
20 uso local 4 (local4)
21 uso local 5 (local5)
22 uso local 6 (local6)
23 uso local 7 (local7)

Ilustración 2 Tabla de Gravedad de los mensajes de Syslog *[4]*

Cada mensaje de prioridad también tiene un indicador de nivel de gravedad, estos se describen en la siguiente tabla junto con sus datos numéricos.

Código de Severidad Numérica

0 Emergencia: el sistema es inutilizable
1 Alerta: se debe tomar acción inmediatamente
2 Críticos: condiciones críticas.
3 Error: condiciones de error
4 Advertencia: condiciones de advertencia
5 Aviso: condición normal pero significativa
6 Informativo: mensajes informativos.

7 Debug: mensajes de nivel de depuración

Ilustración 3 Tabla Gravedad de los mensajes de syslog *[4]*

ANEXO E. CASOS DE USO.

A continuación, se presentan las consideraciones a tomar en cuenta al momento de elaborar un caso de uso dentro de la guía efectiva de modelado de casos de uso publicado por el instituto SANS [27]:

- Cuando: hora / fecha de la (s) prueba (s) del evento (s)
- Quien: Identificador del solicitante; Normalmente una dirección IP y / o un nombre de usuario.
- Qué: Descripción del evento (como un GET o POST a un servidor web)
- Dónde: Sistema o aplicación que generó el evento y desde donde se originó la solicitud.
- Por qué: El propósito de la acción y típicamente es lo que se está investigando.

Metodología TDBUMO: Es el método empleado para la generación de los casos de uso revisando como se genera el flujo de datos al SIEM.

Desde Arriba hacia Abajo (Top Down):

Donde se intenta identificar y agrupar los distintos dispositivos que enviaran los datos hacia el SIEM, a alto nivel es decir visualizar los tipos de servidores, o equipos de red, etc.

Desde Abajo hacia Arriba (Bottom Up): En este punto es posible identificar al revés que el primer punto, se puede empezar reconociendo los servicios propios que posee los servidores, las aplicaciones, los programas que ejecuta y para conocer los eventos que generan, tomando en consideración las 5 preguntas mencionadas al inicio de este anexo.

Intermedio (Middle Out): Cuando se llega a este paso es necesario unir los eventos que generan las aplicaciones y del (Bottom up) con los equipos identificados (Top Down) para empezar a armar los casos de uso.

ANEXO F. CONSIDERACIÓNES A TOMAR EN CUENTA EN CASOS DE USO PARA DETECCIÓN AVANZADA DE AMENAZAS.

A continuación se presentan consejos a tomar en consideración para generar casos de uso que ayuden a detectar futuros intentos de ataques y ayuden a mitigar las vulnerabilidades, basado en recomendaciones de la empresa EXABEM [29].

1) **Tomar en consideración los consejos de empresas similares o de los medios de comunicación:** buscar datos históricos de patrones de ataque o firmas similares a los ataques conocidos.
2) **Crear hipótesis basadas en riesgos conocidos:** ayudar a los analistas a enmarcar una hipótesis y probarla explorando datos de seguridad en el SIEM.
3) **Analizar activamente las anomalías del entorno:** identificar anomalías en los sistemas de TI mediante correlaciones y análisis de comportamiento.
4) **Reconocer incidentes similares:** verificar si " alguna anomalía sucedió antes": se buscan datos de seguridad en busca de patrones similares a un incidente de seguridad actual o anterior.
5) **Explorar si existen puertas traseras, rootkits y botnets:** detectar el tráfico de red a los centros de comando y control e identificar los sistemas infectados que transmiten datos a partes no autorizadas.
6) **Monitorear almacenamiento en la nube y FTP:** monitorear el tráfico de red a través de protocolos que faciliten la transferencia de datos grandes, y alertar cuando se transfieran cantidades inusuales o tipos de archivos, o cuando el objetivo es desconocido o malicioso.
7) **Considerar el movimiento lateral:** la exfiltración de datos generalmente involucra a los atacantes que intentan escalar privilegios o acceder a otros sistemas de TI, en su camino hacia un objetivo lucrativo. Los SIEM pueden detectar movimientos laterales al correlacionar datos de múltiples sistemas de TI.

8) **Seguridad de datos móviles:** un SIEM puede monitorear datos de la fuerza laboral móvil e identificar anomalías que podrían indicar una fuga de información a través de un dispositivo móvil.

ANEXO G. GUIA DE PROCEDIMIENTOS PARA MANTENIMIENTO DEL SIEM

Se adjunta los procedimientos necesarios para el mantenimiento de la herramienta SIEM recomendado por el Instituto SANS [38].

a) Diseñar un procedimiento para parchear el sistema operativo donde se alojen los servidores SIEM, en caso de ser requerido.
b) Diseñar un procedimiento de parches para la aplicación SIEM.
c) Diseñar un procedimiento que contenga los requisitos del negocio en el contenido del SIEM.
d) Diseñar un procedimiento para el desarrollo de contenido que cumpla con las necesidades y condiciones del CSIRT.
e) Diseñar un procedimiento para el almacenamiento y respaldo de los datos del SIEM.
f) Diseñar un procedimiento para la restauración de los datos del SIEM archivados para un análisis por necesidades legales u otros requisitos.
g) Diseñar un procedimiento para administrar las cuentas de usuarios en el SIEM. (creación, eliminación, bloqueo, reseteo)
h) Capacitación continua de los Administradores y Operadores de la herramienta.
i) Crear un procedimiento de retroalimentación de lecciones aprendidas sobre los procesos que involucren al SIEM basado en mejorar el manejo de incidentes.
j) Anticiparse a las necesidades de los nuevos agentes o actualizaciones de los registros, agregando nuevas fuentes

Como recomendaciones adicionales es necesario asegurarse de tener un plan para la actualización de los agentes desplegados de manera oportuna.

BIBLIOGRAFIA.

1] ESET SECURITY, «www.welivesecurity.com,» 19 06 2018. [En línea]. Available: https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region. [Último acceso: 16 05 2019].

2] McGraw Hill, David Miller, «Anatomía del SIEM,» de *SIEM Implementation*, Hollywood, Florida, 2011, pp. capítulo 5, (pág. 80).

3] M. Software, «http://www.magicsoftware.com.ar,» 22 03 2010. [En línea]. Available: http://www.magicsoftware.com.ar/ria/white_paper_platforma_cloud.pdf. [Último acceso: 01 05 2019].

4] www.ietf.org, «www.ietf.org,» 01 08 2001. [En línea]. Available: https://www.ietf.org/rfc/rfc3164.txt. [Último acceso: 22 03 2019].

5] Cisco, «www.cisco.com,» 22 05 2018. [En línea]. Available: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html. [Último acceso: 01 04 2019].

6] University of Houston, «www.uhcl.edu,» 2 08 2015. [En línea]. Available: https://www.uhcl.edu/computing/information-security/tips-best-practices/siem. [Último acceso: 30 05 2019].

7] Splunk, "www.splunk.com," 2019. [Online]. Available: https://docs.splunk.com/Documentation/Splunk/7.2.4/InheritedDeployment/Ports.

8] Splunk, «www.splunk.com,» 3 10 2018. [En línea]. Available: https://docs.splunk.com/Documentation/PCI/3.7.2/Install/PCIDSSRequirements. [Último acceso: 22 04 2019].

Universidad de Houston, «www.uhcl.edu/,» 1 11 2018. [En
9] línea]. Available: https://www.uhcl.edu/computing/information-security/tips-best-practices/siem. [Último acceso: 02 05 2019].

SECUROSIS, «www.securosis.com,» 27 05 2010. [En línea].
10] Available: https://securosis.com/blog/understanding-and-selecting-siem-lm-aggregation-normalization-and-enrichmen. [Último acceso: 01 02 2019].

IBM SECURITY INTELIGENCE,
11] «https://securityintelligence.com,» 08 01 2019. [En línea]. Available: https://securityintelligence.com/siem-event-normalization-makes-raw-data-relevant-to-both-humans-and-machines/. [Último acceso: 04 05 2019].

A. A. F. C. a. C. M. D Jaeger, «Normalizing Security Events with
12] a Hierarchical,» 20 01 2017. [En línea]. Available: https://hal.inria.fr/hal-01442546/document. [Último acceso: 7 03 2019].

Securonix, «https://www.securonix.com,» 24 06 2017. [En
13] línea]. Available: https://www.securonix.com/seven-reasons-to-replace-your-legacy-siem-with-security-analytics-2/. [Último acceso: 01 05 2019].

I. QRADAR, «https://www-01.ibm.com/,» 12 11 2018. [En línea].
14] Available: https://www-01.ibm.com/support/docview.wss?uid=swg21982361. [Último acceso: 11 03 2019].

M. Stanton, «https://www.sans.org/,» Sans Institute, 02 11 2014.
15] [En línea]. Available: https://www.sans.org/reading-room/whitepapers/logging/qradar-log-source-extension-walkthrough-35452. [Último acceso: 11 06 2019].

M. L. Delgado, “Análisis Forense Digital”, 16] http://www.gnu.org/licenses/fdl-1.3.html, 2007.

Apriorit, «https://www.apriorit.com,» 19 12 2017. [En línea]. 17] Available: https://www.apriorit.com/dev-blog/476-requirements-forensic-features-siem. [Último acceso: 04 05 2019].

NIST, «www.nist.gov,» 13 09 2006. [En línea]. Available: 18] https://www.nist.gov/publications/guide-computer-security-log-management. [Último acceso: 02 04 2019].

I. Gartner, «https://www.gartner.com/,» 3 12 2018. [En línea]. 19] Available: https://www.gartner.com/doc/reprints?id=1-5WEZABX&ct=181205&st=sb. [Último acceso: 01 02 2019].

A. Logic, «www.alertlogic.com,» 12 09 2017. [En línea]. 20] Available: https://www.alertlogic.com/resources/whitepapers/siem-solutions-for-security-what-vendors-wont-tell-you/. [Último acceso: 11 03 2019].

Ponemon Institute, «Challenges to Achieving SIEM,» *Ponemon 21] Institute© Research Report,* pp. 02-30, 01 Marzo 2017.

Gartner, «www.gartner.com,» Gartner, 30 05 2017. [En línea]. 22] Available: https://www.gartner.com/en/documents/3732517. [Último acceso: 02 03 2019].

Netwrix Corporation, «SIEM Efficiency Survey,» 23] www.netwrix.com., Irvine, CA 92618, US, 2016.

Cisco, «Annual Cybersecurity Report,» 16 marzo 2017. [En 24] línea]. Available: https://www.cisco.com/c/dam/m/sl_si/events/2017/cisco-connect/pdf/ConnectSLO_What-can-you-lose_Security_2015-03-16-v3.pdf. [Último acceso: 16 01 2019].

IETF.ORG, «ietf,» 03 2009. [En línea]. Available:
25] https://tools.ietf.org/rfc/rfc5424.txt.

A. Chuvakin, «https://www.microfocus.com,» NetIQ, 16 06
26] 2016. [En línea]. Available: https://www.microfocus.com/media/white-paper/the_complete_guide_to_log_and_event_management_wp_es.pdf. [Último acceso: 22 03 2019].

D. Frye, «https://www.sans.org/,» 21 09 2009. [En línea].
27] Available: https://www.sans.org/reading-room/whitepapers/bestprac/effective-case-modeling-security-information-event-management-33319. [Último acceso: 15 06 2019].

D. Swift, «https://www.sans.org,» GIAC GCIA Gold Certification,
28] 4 11 2010. [En línea]. Available: https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528. [Último acceso: 07 03 2019].

EXABEM, «www.exabeam.com,» 1 11 2018. [En línea].
29] Available: https://www.exabeam.com/siem-guide/siem-use-cases/. [Último acceso: 02 06 2019].

(ISC)², «https://www.isc2.org,» 17 10 2018. [En línea]. Available:
30] https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0. [Último acceso: 20 05 2019].

M.-T. 2019, «FireEye,» 01 02 2019. [En línea]. Available:
31] https://content.fireeye.com/m-trends. [Último acceso: 01 06 2019].

Reuters, «www.reuters.com,» 18 12 2013. [En línea]. Available:
32] https://www.reuters.com/article/us-target-breach/target-cyber-breach-hits-40-million-payment-cards-at-holiday-peak-idUSBRE9BH1GX20131219. [Último acceso: 21 04 2019].

A. Chuvakin, «www.gartner.com,» 14 05 2014. [En línea]. Available: https://blogs.gartner.com/anton-chuvakin/2014/05/14/popular-siem-starter-use-cases/. [Último acceso: 12 02 2019].
33]

NIST, «https://nvlpubs.nist.gov,» 01 08 2012. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf. [Último acceso: 11 01 2019].
34]

K. Agrawal, «Department of CS, Institute of Engineering & Technology, D.A.V.V., Indore, India,» 07 07 2015. [En línea]. Available: https://pdfs.semanticscholar.org/520a/39d69369a692cbca8a3bae476f604c387c4a.pdf. [Último acceso: 04 04 2019].
35]

Drew Robb, esecurityplanet, «https://www.esecurityplanet.com,» 6 11 2018. [En línea]. Available: https://www.esecurityplanet.com/products/top-siem-products.html#features. [Último acceso: 03 03 2019].
36]

SANS INSTITUTE, «www.sans.org,» 02 01 2006. [En línea]. Available: https://www.sans.org/media/score/esa-current.pdf. [Último acceso: 01 06 2019].
37]

Verizon, «https://enterprise.verizon.com,» 2018. [En línea]. Available: https://enterprise.verizon.com/resources/reports/dbir/.
38]

welivesecurity, «www.welivesecurity.com,» 18 05 2015. [En línea]. Available: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/. [Último acceso: 19 04 2019].
39]

A. Chuvakin, «www.garner.com,» 11 05 2015. [En línea]. Available: https://blogs.gartner.com/anton-chuvakin/2015/11/05/siem-use-case-discovery/. [Último acceso: 29 04 2019].
40]

I. QRADAR, «https://www.ibm.com/,» 2 11 2018. [En línea]. Available: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/c_qradar_admin_data_ingestion.html. [Último acceso: 2 02 2019].
41]

A. Chuvakin, «https://www.microfocus.com,» NetIQ, 2016. [En línea]. Available: https://www.microfocus.com/media/white-paper/the_complete_guide_to_log_and_event_management_wp_es.pdf.
42]