Facultad de Ingeniería
Ingeniería de Sistemas e Informática

Programa Especial de Titulación:

“IMPLEMENTACIÓN DE UN SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PARA DETECTAR VULNERABILIDADES Y AMENAZAS EXPUESTAS EN LAS PLATAFORMAS INFORMÁTICAS Y REDES DE UNA ENTIDAD FINANCIERA”

Autor: Mariella Anabel, Estela Campos

Para optar el Título Profesional de
Ingeniero de Sistemas e Informática

Asesor: Pedro Ángel, Molina Velarde

Lima, febrero 2020

DEDICATORIA

Este trabajo y esfuerzo le dedico especialmente a mi madre quien me enseñó que se debe mantener la perseverancia para luchar bajo cualquier circunstancia, por sus ánimos para salir adelante y por ser la mujer que siempre estuvo, está y estará presente en cada lucha de mi vida.

A mi hermano quien se preocupó por mi bienestar y en mis estudios desde que era pequeña y tuve siempre su apoyo incondicional.

AGRADECIMIENTOS

Agradezco infinitamente a mi madre y a mi hermano por su apoyo incondicional en todo momento, por hacerme una persona de bien y profesional, gracias por confiar en mí.

A la universidad, a mis profesores y a mi asesor por el apoyo, enseñanza y guía a lo largo de este camino universitario y para la elaboración de esta tesis.

A mis amigos quienes nos apoyamos mutuamente compartiendo nuestros conocimientos y por los ánimos brindados para lograr esta tesis.

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

INTRODUCCION

En el presente proyecto se desarrolló bajo la necesidad de la implementación de una plataforma de gestión de información y eventos de seguridad (SIEM) para detectar vulnerabilidades y amenazas expuestas en las plataformas informáticas y redes de la entidad financiera.

En el primer capítulo, se analiza la problemática que atravesaba la entidad financiera, teniendo como principal problema la deficiencia en el control de seguridad de las plataformas que administra la entidad financiera, y de acuerdo a ello se plasma los objetivos, se plantea los alcances, limitaciones y justificación de dicho proyecto.

En el segundo capítulo, se desarrolla el marco teórico donde se brindará los conceptos teóricos con relación al proyecto, así como también el marco metodológico, donde se define la metodología a usar en el que se detalla el procedimiento para la elaboración del presente proyecto y por último el marco conceptual.

En el tercer capítulo, comprende el desarrollo del proyecto utilizando la metodología defina, con una combinación de buenas prácticas de Scrum, PMBOK y la guía de IBM, esta metodología está dividida en 5 fases que son inicio, planificación, implementación y configuración, monitoreo y control y por último la fase de cierre.

Y para finalizar, en el cuarto capítulo se precisa los resultados logrados, así como el análisis económico de la inversión para llevar a cabo el proyecto.

CAPITULO 1

ASPECTOS GENERALES

1.1. Definición del Problema

1.1.1. Descripción del Problema

Debido a los constantes ciberataques a las plataformas informáticas, cajeros y a las redes a las entidades financieras, en muchas ocasiones ha sido burlado la seguridad por atacantes de grandes bandas criminales que se aprovechan de las brechas de las plataformas de seguridad, el cual se han visto afectados perdiendo la disponibilidad de sus recursos en la red, información confidencial y sensible y grandes pérdidas económicas que ha perjudicado tanto a las entidades financieras como a los clientes de estos.

La entidad financiera que abordaré en la presente tesis no contaba con una plataforma SIEM, una centralizadora de almacenamiento e interpretación de eventos de seguridad (logs) de sus tecnologías de seguridad, servidores y cajeros automáticos que le permitiera tener un mayor control, visibilidad holística, detectar con precisión, análisis en tiempo real, priorizar las amenazas y permita al área de seguridad tomar medidas ofensivas más rápidamente ante ataques y vulnerabilidades.

Otro de los factores era la realización de configuraciones manuales, a pesar de que son personas expertas en la ciberseguridad dejaban muchas brechas, y cuando estaban siendo atacados, al SOC le tomaba mucho tiempo poder detectar por donde están logrando ingresar los hackers, debido a que cuentan con distintas tecnologías de seguridad (Firewall, EDS, IPS, EDR, DLP y AV)

que tienen que monitorear individualmente mientras que los hackers actuaban en cuestión de segundos.

Se realizó la técnica del árbol de problemas, que se muestra a continuación:

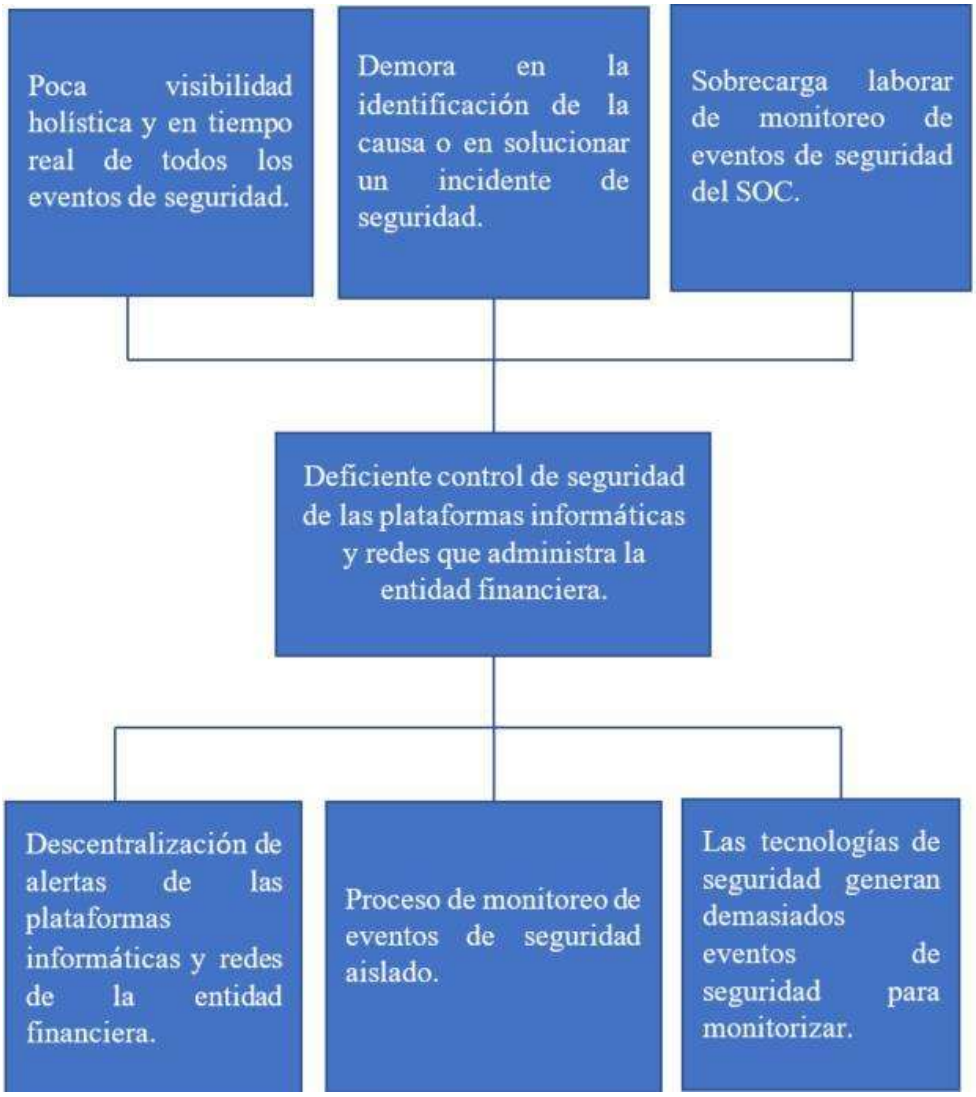


Tabla 1: Árbol de problemas

Fuente: *Elaboración Propia*

Adicionalmente se muestra la tabla de problemas:

Tabla 1: Tabla de problemas

Cuadro de problemas	
Descripción del problema: Deficiente control de seguridad de las plataformas informáticas y redes que administra la entidad financiera.	
Causas	**Efectos**
1. Descentralización de alertas de las plataformas informáticas y redes de la entidad financiera.	Poca visibilidad holística y en tiempo real de todos los eventos de seguridad.
2. Proceso de monitoreo de eventos de seguridad aislado.	Demora en la identificación de la causa o en solucionar un incidente de seguridad.
3. Las tecnologías de seguridad generan demasiados eventos de seguridad para monitorizar.	Sobrecarga laborar de monitoreo de eventos de seguridad del SOC.

Tabla 2: Tabla de Problemas
Fuente: *Elaboración Propia*

1.1.2. Formulación del Problema

➢ **General:**

¿Cómo el control de seguridad de las plataformas informáticas y redes que administra la entidad financiera dejaría de ser deficiente?

➢ **Específicos:**

- ¿De qué manera se puede mejorar la descentralización de alertas de las plataformas de seguridad de la entidad financiera para obtener una visibilidad holística?
- ¿Cómo el proceso de monitoreo de eventos de seguridad dejará de impactar en el retraso de identificación de las causas de incidentes?
- ¿Cómo la gran cantidad de eventos recibidos a monitorear ya no provocará sobrecarga laboral?

1.2. Definición de objetivos

1.2.1 Objetivo general

Implementar una solución Security Information and Event Management (SIEM) para detectar vulnerabilidades y amenazas expuestas expuestas en las plataformas informáticas y redes de una entidad financiera.

1.2.2 Objetivos específicos

- Integrar todas las plataformas de seguridad, cajeros automáticos, servidores y redes a la tecnología SIEM para obtener una visibilidad holística de todos los eventos y alertas de seguridad.
- Optimizar el tiempo de análisis de monitoreo de eventos de seguridad para identificar rápidamente la causa de un incidente de seguridad.
- Disminuir la carga laboral de monitoreo de eventos de seguridad del SOC identificando oportunamente vulnerabilidades y amenazas de seguridad.

1.3 Alcances y limitaciones

1.3.1 Alcances

Para la implementación de SIEM en la entidad financiera se ha considerado los siguiente:

- Se definió los activos de información que se integrarán con el SIEM (activos críticos) entre ellos cajeros automáticos.
- Se definió que sólo los eventos de seguridad
- Se definió las acciones de notificación de las alertas de acuerdo al requerimiento de la entidad financiera.
- Se creó 11 reglas (casos de uso) customizados de acuerdo con solicitud de la entidad.
- Desde Qradar sólo se monitorea eventos de seguridad.
- Se visualiza reportes y dashboard predefinidos.

1.3.2 Limitaciones:

Se cuenta con las siguientes limitaciones:

- El acceso a la plataforma SIEM solo es posible mediante navegadores web y CLI.
- No se realizó la integración con dispositivos finales (endpoints) de la entidad.
- Los reportes del SIEM solo se visualizan de manera gráfica.
- No se integró soluciones o sistemas operativos que no cuenten con soporte del fabricante.
- No se generó propiedades personalizadas.

- No se generó reportes customizados.
- No se incluye la arquitectura de la infraestructura de la entidad por motivos de privacidad y confidencialidad.

1.4 Justificación:

La tecnología y la digitalización de la información convierten a los datos en un activo muy importante y sensible para todas las empresas, siendo necesarios protegerlos ante vulnerabilidades y amenazas internas y externas de la organización. A pesar de que hoy en día las técnicas de seguridad hacia los datos y hacia la infraestructura de las comunicaciones están en auge, tales como tecnologías de seguridad que permiten prevenir los ataques informáticos no son absolutamente confiables y no son integrados, además, todos los equipos generan una gran cantidad de eventos de seguridad y los administradores no cuentan con el tiempo suficiente para monitorear evento por evento, es por esa razón que las organizaciones necesitan una solución que realicen este monitoreo.

Hoy en día, las entidades financieras necesitan que la información que manejan cumpla con los 3 pilares de la información: integridad, disponibilidad y confidencialidad, por lo que es necesario tener una visibilidad y un control general de todo lo eventos de seguridad que ocurren en la entidad financiera, para salvaguardar data sensible tanto de la entidad como la de sus clientes.

Con la implementación de la solución SIEM, se logró mitigar consideradamente las vulnerabilidades y amenazas de seguridad expuestos en las plataformas informáticas y redes de la entidad financiera, además que ayuda a cumplir con los estándares de seguridad PCI DSS (Estándar de Seguridad de Datos para la Industria

de Tarjeta de Pago) y la norma ISO7IEC 27001: Sistemas de gestión de seguridad de la información, proporciona un estándar de calidad; entre otros.

CAPITULO 2

FUNDAMENTO TEÓRICO

2.1 Antecedentes

2.1.1 Tesinas Nacionales

2.1.1.1 Tesina Nacional N° 1

Antonio Inoguchi, Erika Macha (2017), Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las pymes el Perú, Lima, Perú.

❖ **Objetivos**

Objetivo General

Determinar la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, 2016.

Objetivos Específicos

- Identificar los problemas de gestión de la ciberseguridad en las PYMES del Perú, 2016.
- Prevenir los riesgos de los ataques cibernéticos en las PYMES del Perú, 2016.

Síntesis de la situación problemática planteada

Gran parte de las PYMES en el Perú son consideradas las más vulnerables a los ciberataques porque desconocen el impacto que pueden tener sobre su negocio. Esto lleva a que muchas no implementen las acciones necesarias para protegerse de manera efectiva.

Metodología

Para el desarrollo de este trabajo se aplicaron las siguientes fases:

- Definición del Alcance.
- Relevamiento.
- Planificación.
- Implantación.
- Conclusiones

Conclusión

La Empresa Zavala Cargo S.A.C. tenía una falta del uso de planes contra ataques de Seguridad Cibernética, que resguarden su información cibernética permitiendo así una toma de decisiones más confiable.

Los resultados de las pruebas que se realizó a la empresa permitió saber la falta de conocimiento de seguridad de la información cibernética de todo el personal de la empresa.

2.1.1.2 Tesina Nacional N° 2

Goyo Guzmán (2015), Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica ortega, Huancayo, Perú.

❖ **Objetivos**

Objetivo General

Determinar el nivel de importancia de la metodología de seguridad de tecnologías de información y comunicaciones que permita la continuidad de

Objetivos Específicos

- Identificar las amenazas y los riesgos a los que están sometidos los procesos de información al no tener sistemas de seguridad de tecnologías de información y comunicaciones.
- Definir los aspectos críticos que debe contemplar la seguridad de las tecnologías de información y comunicaciones.

Síntesis de la situación problemática planteada

La seguridad de la empresa tiene vital importancia para las organizaciones cuyas funciones operacionales y gerenciales requieren operar en forma ininterrumpida (7X24) pudiendo desarrollar actividades dentro de cualquier sector empresarial.

procesos de la clínica Ortega cuyos servicios principales dependen de la tecnología.

Metodología

La metodología se desarrolla en las siguientes fases:

➢ Definición del Alcance.

- Relevamiento.
- Planificación.
- Implantación.

Conclusiones

- Se logró la mejora del nivel de seguridad que es medido a través de la asignación de valores, obteniéndose un valor inicial de 16 y final de 50.
- Para el desarrollo del modelo de seguridad de tecnologías de información y comunicaciones se tuvo en cuenta Normas técnicas y las recomendaciones del modelo ISO.

2.1.2 Internacional

Jorge Fernández, Juan Herrera, Juan Camilo (2019), Implementación de un Security Information and Event Management (SIEM) en el comando de la armada nacional, tesis presentada para obtener Especialización en Seguridad Informática. Universidad Piloto de Colombia, Bogotá, Colombia.

Objetivos:

Objetivo General

Implementar un SIEM para la Dirección de Tecnologías de la Información y las Comunicaciones del Comando de la Armada Nacional ("DITEL"), mediante el uso de herramientas de software libre y gratuitas, con el fin de brindar visibilidad en tiempo real de ataques a la infraestructura tecnológica.

Objetivos Específicos

- Implementar una herramienta que correlacione, priorice y asigne los riesgos informáticos potenciales por medio de la recolección de eventos de los componentes tecnológicos designados por la ARC.

- Brindar a la Armada Nacional por intermedio de la implementación de un SIEM, un panorama visible ante un eventual ataque informático.

Síntesis de la situación problemática planteada

La Armada Nacional por medio de la implementación buscan monitorear, revisar, prevenir y contrarrestar amenazas y/o vulnerabilidades que puedan atentar contra la integridad, confidencialidad y disponibilidad de la información.

Metodología

Utilizaron una metodología a criterio de los autores, que cuenta con las siguientes fases:

- Fase de descubrimiento
- Fase de diseño y análisis
- Fase de implementación
- Fase de pruebas
- Fase de documentación

Conclusiones

Se llegaron a las siguientes conclusiones:

- Se definieron los requerimientos técnicos teniendo en cuenta la documentación del fabricante y las buenas prácticas para implementación del SIEM.

- La solución implementada le permitió a la Armada contar con un Dashboard que presenta gráficamente los eventos que les permiten tomar decisiones frente ataques informáticos.

2.2 Marco Teórico

2.2.1 Seguridad Informática

Es la práctica de proteger la información mitigando los riesgos de la información. Es parte de la gestión de riesgos de la información . Por lo general, implica prevenir o al menos reducir la probabilidad de ataques cibernéticos

La seguridad informática debe garantizar:

- La Disponibilidad de los sistemas de información.
- La Integridad de la información.
- La Confidencialidad de la información.

Tipos de Seguridad

A) Seguridad de red

Este tipo de seguridad es necesario para evitar que un hacker acceda a datos dentro de la red. También evita que afecten negativamente la capacidad de sus usuarios para acceder o usar la red. Los más comunes incluyen:

- Virus, gusanos y troyanos
- Software espía y publicitario
- Ataques de hackers
- Ataques de denegación de servicio
- Intercepción o robo de datos
- Robo de identidad

B) Seguridad de Software

La seguridad de software se utiliza para proteger el software contra ataques maliciosos de hackers y otros riesgos, las buenas prácticas de ingeniería de software implican pensar en la seguridad al principio del ciclo de vida del desarrollo de software, conocer y comprender las amenazas comunes, diseñar para la seguridad y someter todos los artefactos de software a análisis de riesgo objetivos exhaustivos y pruebas

C) Seguridad de Hardware

Garantizan la confianza, integridad y autenticidad de los circuitos integrados (IC) y los sistemas electrónicos. Las soluciones de seguridad de hardware pueden venir en forma de dispositivos de red: los cortafuegos, enrutadores e incluso conmutadores pueden funcionar para proporcionar un cierto nivel de seguridad. En general, estos dispositivos son computadoras dedicadas que ejecutan software propietario.

2.2.2 Riesgos Informáticos

Los riesgos pueden ser definidos como una función de la probabilidad de que una amenaza aproveche o explote una potencial vulnerabilidad en un activo de información, y de la magnitud del daño resultante de tal evento adverso en la organización.

2.2.3 Gestión de datos de registro

La administración de datos de registro es un componente central de cualquier sistema SIEM a escala empresarial que permite:

- ✓ agrupar datos de registro de una variedad de fuentes diferentes, cada uno con su propia forma de categorizar y registrar datos.
- ✓ reconocer patrones de comportamiento malicioso y generar notificaciones para alertar al usuario para que tome medidas.

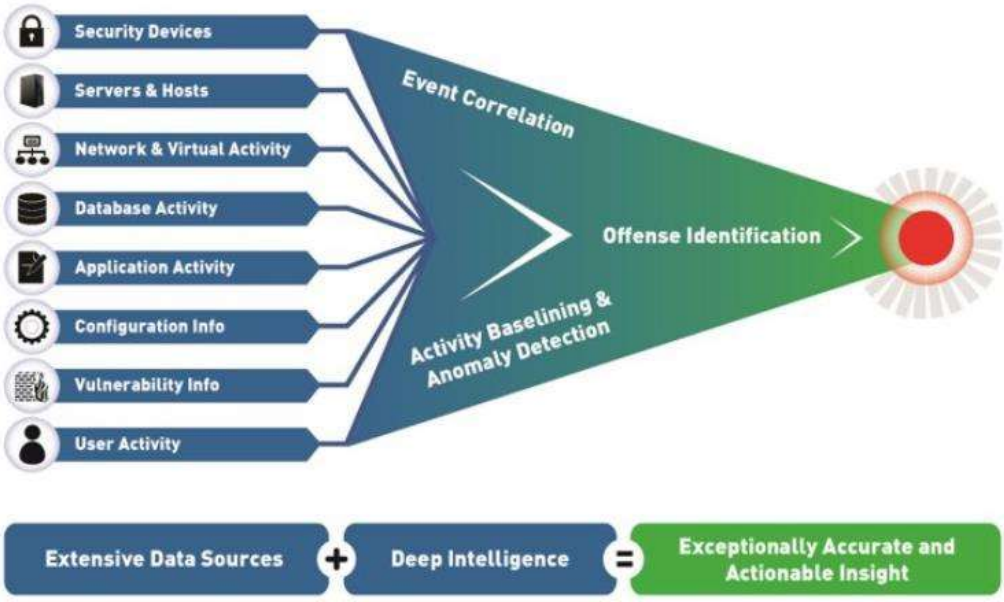


Ilustración 1: Gestión de datos de registro

2.2.4 Plataforma SIEM – Security Information and Event Management

El acrónimo inglés de SIEM corresponde a Security Information and Event Management, es decir, un sistema de gestión de eventos y seguridad de la información, son plataformas que proveen análisis en tiempo real de los eventos de seguridad generados por los equipos de comunicación, servidores y todo lo que estemos monitoreando.

Ilustración 2: Anatomía de un sistema SIEM

Principales Características	Ventajas
Alertas y Correlación de Eventos	Disminuir falsos positivos.
Monitoreo de integridad	Detección de anomalías de red y amenazas.
Agregación de Logs	Análisis antes, durante y después del ataque.
Análisis Forenses	Captura total de los paquetes en la red.
Análisis en tiempo Real	Cumplimiento de nuevas normas/leyes.
Manejo de Vulnerabilidades.	

Tabla 3: Características y Ventajas SIEM
Fuente: *Elaboración Propia*

2.2.5 Proveedores SIEM

Existe una variedad de soluciones SIEM en el mercado tecnológico.

A) ArcSight Enterprise Security Manage

Esta plataforma proporciona análisis de seguridad de información y software de inteligencia para la información de seguridad y la gestión de eventos (SIEM) y la gestión de registros. Está diseñado para apoyar a los clientes a detectar y priorizar las amenazas de seguridad, organizar y rastrear las actividades de respuesta a incidentes y simplificar las actividades de auditoría y cumplimiento. ArcSight se convirtió en una subsidiaria de Hewlett-Packard en 2010.

Características

- Potente correlación de datos en tiempo real
- Automatización del flujo de trabajo y orquestación de la seguridad
- Matriz de permisos unificada y para múltiples usuarios
- Contenido de seguridad impulsado por la comunidad.
- Compatibilidad con ArcSight Data Platform y ArcSight Investigate
- Datos enriquecidos de eventos de seguridad

B) SolarWinds SIEM

Esta plataforma obtiene el analizador de registro de eventos y el consolidador de gestión de forma gratuita como prueba. Los sistemas SolarWinds SIEM le permiten ver registros en más de un sistema Windows. Puede filtrar sus registros y patrones. Security Events Manager le brinda la capacidad de evaluar y almacenar sus datos de registro históricos.

Es una herramienta excelente para aquellos que buscan explotar los registros de eventos de Windows debido a la respuesta detallada a los incidentes y es

adecuada para aquellos que desean administrar activamente su infraestructura de red contra futuras amenazas.

C) QRadar SIEM de IBM

Es una plataforma de gestión de seguridad de la red que utiliza una combinación de conocimiento de la red basado en flujos, correlación de sucesos de seguridad y evaluación de vulnerabilidades basada en activos. Facilita a los equipos de seguridad a descubrir con exactitud y priorizar las amenazas ocurridas dentro de la organización. Mediante la consolidación de eventos de registro y datos de flujo de red de todos dispositivos integrados, y aplicaciones que se encuentran dentro de la red, QRadar correlaciona toda esta información diferente y agrega eventos relacionados a alertas únicas que aceleran el análisis y la resolución de incidentes.

Ventajas

- Visibilidad Completa y centralizado de registros, flujo y eventos
- Detección de amenazas en tiempo real
- Eliminar los procesos de seguimiento manual y permite a los analistas enfocarse en la investigación y en la respuesta.
- Gestiona fácilmente la conformidad con las normas.
- Arquitectura escalable para soportar grandes implementaciones.

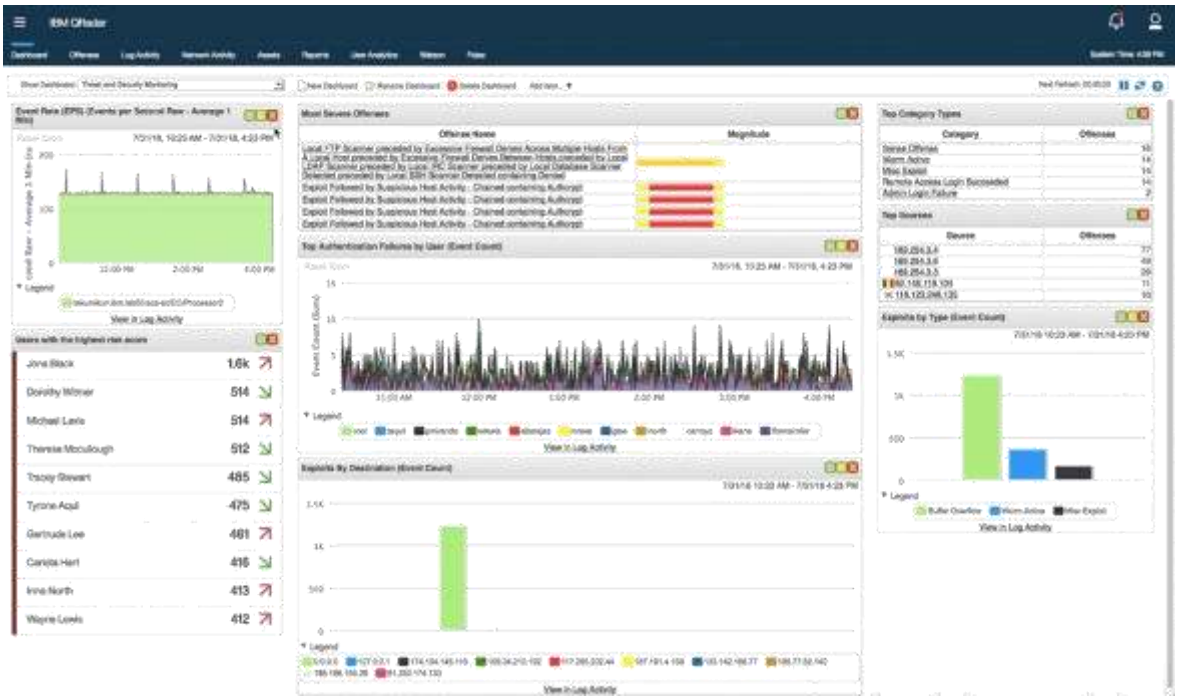


Ilustración 3: Plataforma Qradar

Principales características

- Aplica analítica integrada para detectar con precisión a las amenazas.
- Recopila eventos y flujos de red.
- Correlaciona actividades relacionadas para priorizar incidentes.
- Analiza y normaliza automáticamente los registros.
- Se integra inmediatamente con 450 tipos de soluciones.
- La arquitectura flexible puede implementarse on-premise o en la nube.
- Base de datos escalable, autogestionable y autosintonizable.
- Captura de carga útil de capa 7 hasta un número configurable de bytes del tráfico sin cifrar.
- Amplias capacidades de búsqueda.
- Notificación por correo electrónico, entre otros.

- Supervise los cambios en el comportamiento del host y de la red que podrían indicar un ataque o incumplimiento de políticas, por ejemplo:
  - Fuera de horario o uso excesivo de una aplicación o patrones de actividad de red inconsistentes con los perfiles históricos
  - Priorización de presuntos ataques e infracciones de políticas

Arquitectura

Es una plataforma de inteligencia de seguridad que facilita una arquitectura unificada para recolectar, almacenar, analizar y consultar datos de registro, flujos de red, amenazas, vulnerabilidades y riesgos. Como resultado, los operadores, analistas y auditores que utilizan cualquiera de los módulos de la Plataforma de Inteligencia de Seguridad se benefician de:

- Arquitectura unificada de colección, agregación y análisis para eventos de seguridad, datos de vulnerabilidad, datos de gestión de identidad y acceso, archivos de configuración y telemetría de flujo de red; una plataforma común para todas las funciones de búsqueda, filtrado, escritura de reglas y generación de informes.
- Una interfaz de usuario única para toda la gestión de registros, telemetría de flujo de red, modelado de riesgos, prioridades de vulnerabilidad, detección de incidentes y tareas de análisis de impacto.
- La arquitectura flexible de IBM Security QRadar, que incluye la colección, análisis y exposición de información de seguridad y de red,

permite a las organizaciones implementar una solución que se adapte a sus requisitos específicos de gestión de seguridad de red.

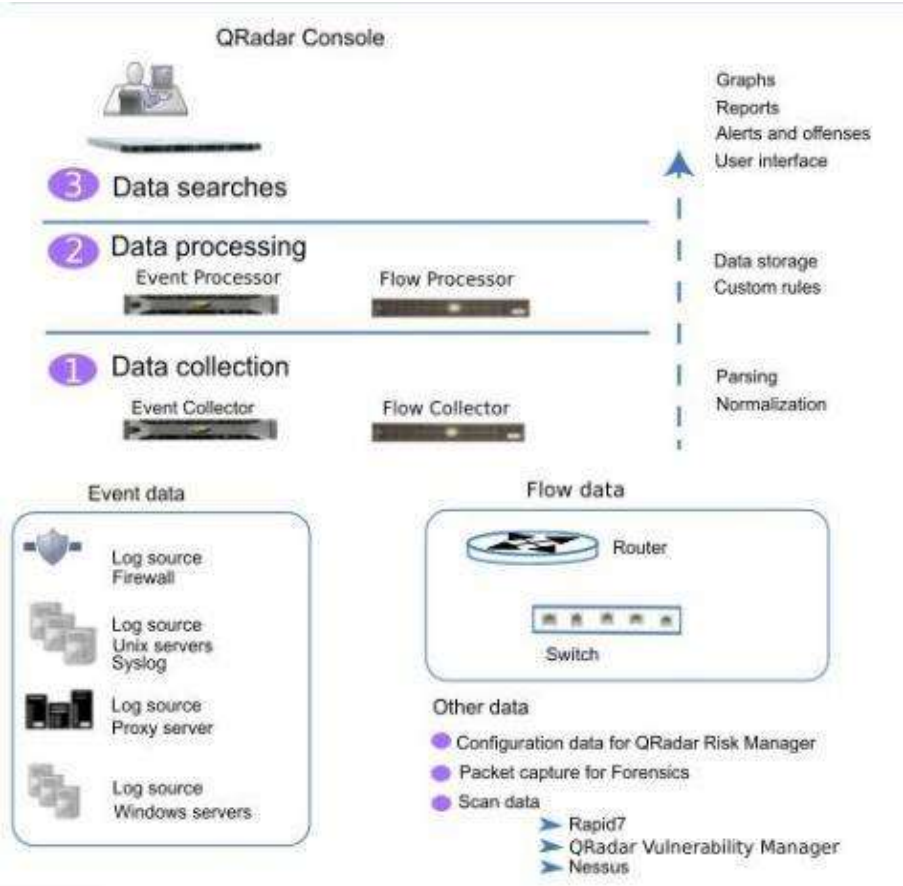


Ilustración 4: Arquitectura QRadar All In One

IBM Security QRadar 3129

IBM Security QRadar 3129 es una plataforma todo en uno que utiliza capacidades integradas de recopilación y correlación de flujos y eventos. Asimismo, son sistemas cuyas características permiten ampliarse con procesadores de eventos, procesadores de flujo, dispositivos de procesamiento de flujos y eventos combinados.

Estos sistemas pueden recopilar directamente datos de NetFlow, J-Flow, sFlow e IPFIX. Asimismo, pueden utilizar QRadar QFlow Collector para la captura de contenido y el análisis de datos de red.

El siguiente diagrama muestra un dispositivo todo en uno, que recopila datos de orígenes de eventos y flujo, procesa los datos y proporciona una aplicación web donde puede buscar, monitorear y responder a amenazas de seguridad.

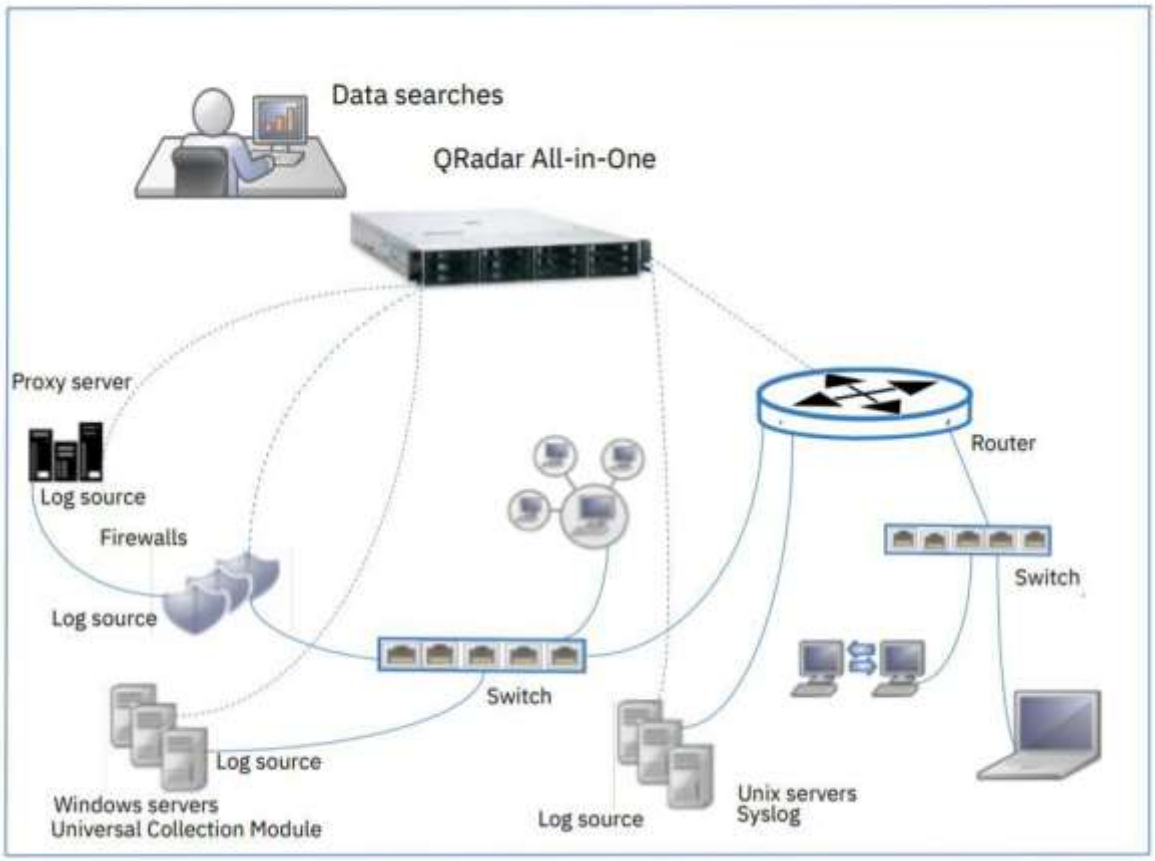


Ilustración 5: Arquitectura de Implementación QRadar 3129

2.2.6 Monitoreo de Seguridad

Es la supervisión de la seguridad en un proceso automatizado de recopilación y análisis constante de indicadores de posibles amenazas de seguridad, y luego evalúa

estas amenazas para la acción adecuada y así estar un paso por delante de las amenazas cibernéticas.

2.2.7 Marcos de trabajo

I. Framework SCRUM

Scrum es un proceso de desarrollo de software iterativo y creciente utilizado, comúnmente, en entornos basados en el desarrollo ágil de software. El trabajo es estructurado en ciclos de trabajo llamados Sprints, iteraciones de trabajo con una duración de dos a cuatro semanas.

Scrum se caracteriza por ser un modelo que define un conjunto de prácticas y roles que puede tomarse como punto de partida para definir el proceso de desarrollo que se ejecutará durante un proyecto.

ROLES SCRUM	CARACTERÍSTICAS	ACTIVIDADES
✓ Scrum Master.	✓ Resultados anticipados.	✓ Sprint planning
✓ Product Owner	✓ Flexibilidad y adaptación.	✓ Sprint
✓ Equipo Scrum.	✓ Retorno de inversión.	✓ Scrum daily meeting
	✓ Mitigación de riesgos.	✓ Sprint review
	✓ Productividad y calidad.	✓ Sprint retrospective
	✓ Alineamiento entre cliente y equipo.	
	✓ Un equipo motivado.	

Tabla 4: Roles, características y actividades Scrum

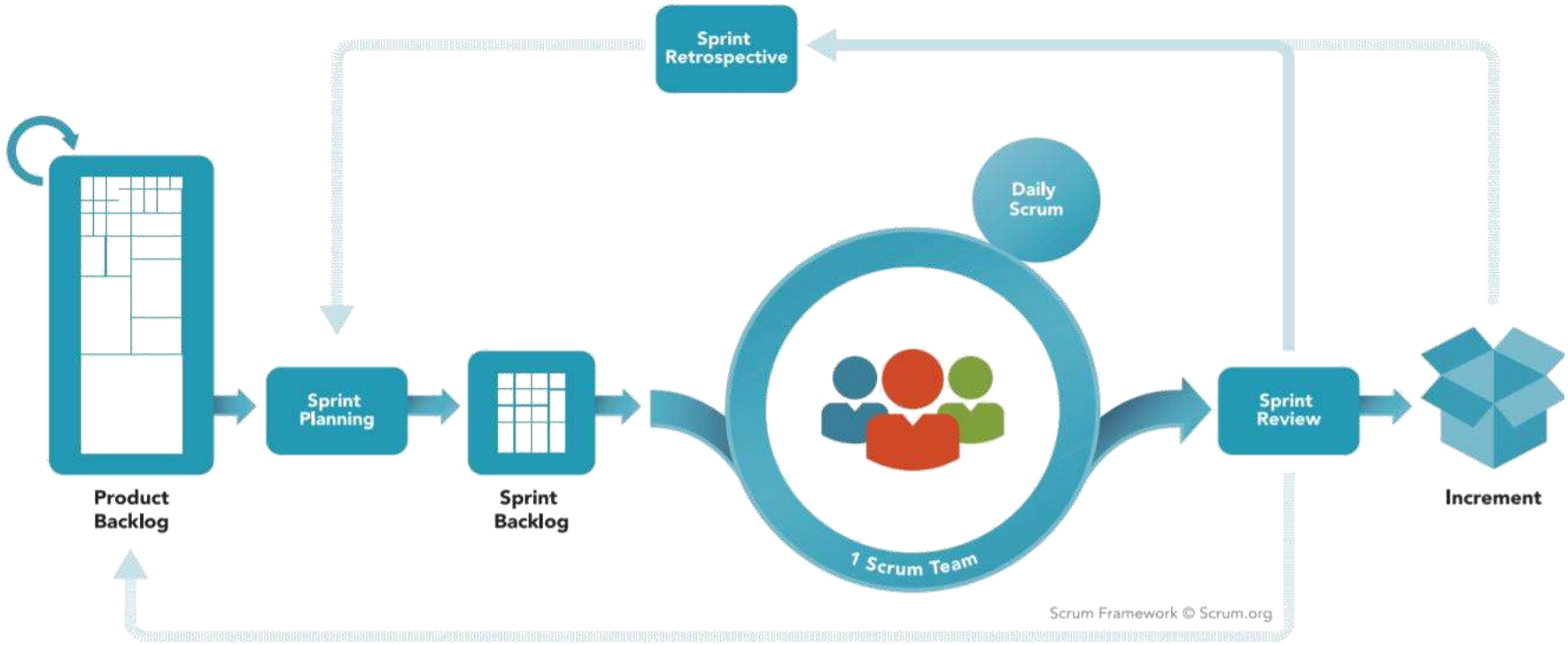


Ilustración 6: Scrum Framework
Fuente: https://www.scrum.org/

II. PMBOK GUIDE

Es una guía para de conocimientos de gestión de proyectos, la publicación principal de PMI es un recurso fundamental para la gestión eficaz de proyectos en cualquier industria. Incluye información sobre prácticas ágiles junto con los enfoques tradicionales de la sexta edición y con Agile Alliance.

La guía PMBOK - Sexta edición y la guía de práctica ágil se crearon para complementarse entre sí, juntas, estas dos publicaciones son una herramienta poderosa que permite el enfoque correcto para el proyecto correcto.

2.3 Marco Metodológico

La gestión de proyectos es la mejor práctica para el desarrollo progresivo, pero para lograrlo debe contar con las herramientas, los recursos y el apoyo necesarios para cumplir con los objetivos principales de la entidad. Actualmente se consideran dos marcos principales para los cuales se hace referencia a las mejores prácticas en la promoción de la gestión de proyectos, el PMBOK y SCRUM. Proponen desarrollar una metodología para la gestión de proyectos basada en las mejores prácticas de SCRUM y PMBOK, para proporcionar orientación a la gestión del proyecto y así reducir la probabilidad de falla del proyecto.

La esquematización del método para una mejor comprensión del método propuesto se realizó un diseño del método a manera de esquema tomando como referencia el ciclo de vida del proyecto del PMBOK, SCRUM y la guía de implementación de IBM, de tal manera que pueda ser entendido de manera conceptual, como se aprecia en la siguiente ilustración:

Ilustración 7: Esquema de la metodología
Fuente: Elaboración Propia

2.4 Marco conceptual

Términos Clave

A. Activos

Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección.

B. Amenaza

Cualquier labor que es capaz de aprovechar alguna brecha y perjudicar un sistema de información. Probabilidad de ocurrencia de un evento en un periodo de tiempo.

C. Checker ATM Security

Checker es un S.O. desarrollado para los cajeros automáticos financieros, siendo su principal objetivo proteger los procesos de transacciones financiera.

D. Confidencialidad

Implica proteger la información de tal forma que sólo sea conocida por las personas autorizadas y se la resguarde del acceso de terceros.

E. Consola QRadar

La consola de QRadar proporciona la interfaz de usuario de QRadar y vistas de eventos y flujos en tiempo real, informes, delitos, información de activos y funciones administrativas. En las implementaciones distribuidas de QRadar

se usa la Consola QRadar para administrar hosts que incluyan otros componentes.

F. Event Collector

El recopilador de sucesos recopila eventos de registro de fuentes locales y remotas, y normaliza los eventos fuente del registro primas para darles formato para su uso por QRadar. El Collector Evento haces o coalesce eventos idénticos a el uso del sistema conserve y envía los datos al procesador de eventos.

G. EPS

Eventos por segundo, los EPS es una medida que se utiliza para transmitir la rapidez con que una red genera datos a partir de los dispositivos de seguridad y/o qué tan rápido un producto SIEM puede correlacionar datos de estos dispositivos.

H. Impacto

Probabilidad de impacto, si al presentarse el vector de amenaza es exitoso.

I. Integridad

Se refiere a los métodos para garantizar que los datos sean reales, precisos y protegidos de modificaciones no autorizadas por el usuario.

J. Disponibilidad

La disponibilidad, en el contexto de un sistema informático, se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto.

K. Datos Sensibles

Son los datos privados que revelan opiniones políticas, convicciones religiosas, economía e información referente a la salud o a la vida sexual (Art.2°, de la ley peruana 29733 de protección de datos personales).

L. Logs

Un mensaje de log o registro es lo que genera un sistema de computadora, dispositivo, software, etc. en respuesta a cualquier tipo de registro. El término logs o registros realmente se usa para indicar una colección de mensajes que se usarán colectivamente para "pintar una imagen" de alguna ocurrencia. Esta es la base de información de todos los sistemas SIEM, estos logs van a ser utilizados para extraer información útil, analizando y categorizando.

M. Log Source

Son las fuentes de registro de los dispositivos que son integrados a la consola IBM Security QRadar, estos pueden ser equipos de red, de seguridad, servidores Linux y windows, entre otros.

N. Riesgo

Es el potencial de que una amenaza dada aproveche las brechas de los activos y, por lo tanto, cause daños a la empresa. Se mide en términos de una combinación de la probabilidad de ocurrencia de un evento y su consecuencia. Contingencia o proximidad a un daño.

O. SIEM

Las soluciones SIEM proporcionan una visión holística de lo que sucede en una red en tiempo real y ayudan a los equipos de TI a ser más proactivos en la lucha contra las amenazas de seguridad.

P. Vulnerabilidad

Es la falla en un sistema que puede dejarlo abierto a ataques.

Q. Wincollect

Es una función escalable de IBM Security QRadar que recopila eventos basados en Windows utilizando su API del registro de eventos de sistema para recopilar eventos y, a continuación, WinCollect envía los eventos a QRadar mediante el protocolo syslog.

CAPITULO 3

DESARROLLO DE LA SOLUCIÓN

3.1 Desarrollo

La presente tesis está dividida por 5 fases según la propuesta metodológica basada en Scrum, PMBOK y la Guía de implementación de IBM, las fases y actividades a realizar son las siguientes:

FASES	ACTIVIDADES	SALIDA
Fase de Inicio	- Identificación de Recursos del Proyecto - Identificación de Stakeholder - Identificación de Equipos - Acta de constitución del proyecto	- Lista de Recursos. - Stakeholders. - Acta de Constitución del proyecto.
Fase de Planificación	- Alcance y Limitaciones. - Diagrama de arquitectura. - Cronograma de actividades. - Identificación de riesgos. - Costo del Proyecto. - Planificación de Sprint's	- Alcance y limitaciones. - Cronograma de actividades. - Asignación de recursos. - Lista de riesgos. - Costo del Proyecto.
Fase de Implementación y Configuración	- Instalación y configuración SIEM - Integración de equipos SIEM - Configuración de reglas	- Reportes de estado - Actos de reunión - Solicitud de cambios
Fase de Monitoreo y Control	- Monitoreo de eventos y alertas.	- Reportes de estado - Acta de reunión - Solicitud de cambios
Cierre	- Manual de uso. - Capacitación. - Acta de conformidad del proyecto.	- Reporte de estado de equipos. - Reporte de configuraciones. - Acta de conformidad del proyecto.

Tabla 5: Fases de la Metodología

3.2 FASE DE INICIO DEL PROYECTO

3.2.1 Identificación de Recursos del Proyecto

3.2.1.1 Identificación de Stakeholders y Roles

Los Stakeholders son todas las personas que se han visto involucradas durante la elaboración del proyecto.

STAKEHOLDERS		
PUESTO	**NOMBRE**	**ROL**
Gerente de Operaciones	Javier O.	**Product Owner**
Jefe de Proyectos	Alf F.	**Scrum Master**
Especialista y Líder	Joel C.	**ScrumTeam** *(Implementing team)* *(Monitoring team)*
Analista de Seguridad I	Mariella E.	**ScrumTeam** *(Implementing team)* *(Monitoring team)*
Analista de Seguridad I	Fernando P.	**ScrumTeam** *(Monitoring team)*
Cliente	Entidad Financiera	**Business Owner**

Tabla 6: Stakeholders

3.2.1.2 Identificación de Equipos

Dispositivo IBM Security QRadar 3129 (todo en uno) es un sistema QRadar todo en uno que puede perfilar el comportamiento de la red e identificar las amenazas de seguridad de la red.

DESCRIPCIÓN	VALOR
Máxima capacidad	300,000 FPM 15,000 EPS
Interfaces	2 puertos HBA Fibre Channel de 8 Gbps 4 x interfaces Ethernet 10/100/1000 Base-T 1 x interfaz de módulo de gestión integrado 10/100/1000 Base-T 2 puertos Ethernet SFP + de 10 Gbps
Memoria	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Almacenamiento	12 x 3.5 pulgadas 6 TB SAS 7.2 K rpm, 60 TB en total (RAID6) 48 TB disponibles para almacenar datos de eventos y flujos.
Fuente de alimentación	Doble redundante de 900 W de CA
Dimensiones	31.5 pulgadas de profundidad x 17.5 pulgadas de ancho x 3.4 pulgadas de alto.
Componentes incluidos	Coleccionista de eventos. Procesador de eventos para procesar eventos y flujos. Almacenamiento interno para eventos y flujos.

Tabla 7: Características QRadar 3129

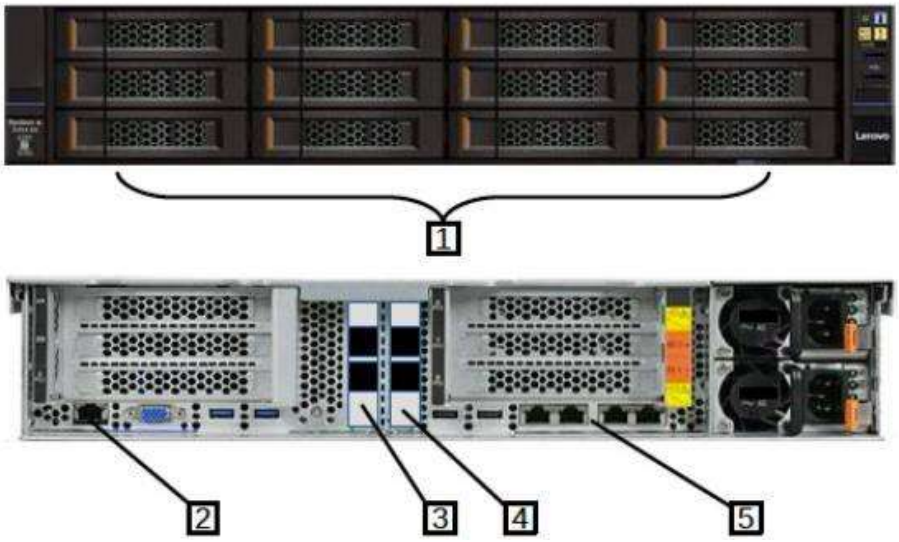


Ilustración 8:Servidor QRadar 3129

ETIQUETA	DESCRIPCIÓN
1	Almacenamiento de datos de eventos
2	Puerto IMM (TX 1GbE)
3	Puertos de administración (10 GbE SFP +)
4	Puertos de canal de fibra (8 Gb SFP +)
5	Puertos de gestión (1 GbE TX)

Tabla 8:Descripción Servidor 3129

Licencias

CANTIDAD	DESCRIPCIÓN
1	Licencia de instalación del software IBM QRadar + Suscripción SW y soporte 12 meses
1	IBM QRadar Capacidad de eventos 2.5K Eventos por segundo Licencia + Suscripción SW y soporte 12 meses

Tabla 9: Licencia QRadar 3129

3.2.2 Acta de Constitución del Proyecto

Gestión de Proyectos

Acta de Constitución

Información Inicial del Proyecto			
Código Negocio / Proyecto:	PE00205/2019	**Fecha:**	10/06/2019
Nombre del proyecto:	Servicios Profesionales plataforma IBM QRadar SIEM		
Empresa CLIENTE:	Entidad Financiera		
SPONSOR del cliente:	Carlos D.		
Jefe de Proyecto Cliente:	Juan G.		
Gte. Cuenta empresa:	Giancarlo O.		
Jefe de Proyecto empresa:	Alf F.		

Versión	Fecha	Autor	Versión
1	10/06/2019	Alf F.	Versión 1.0
2			

Requerimiento del Cliente:

La ENTIDAD FINANCIERA se encuentra en la búsqueda de un partner de IBM que le brinde el servicio de implementación de la plataforma IBM QRADAR SIEM, que implemente las licencias de EPS – Eventos por Segundo necesarios para soportar y dar la visibilidad al equipo de seguridad de lo que ocurre en la red del banco.

Propuesta de EMPRESA:

Los presentes servicios profesionales tienen por objetivo el mejoramiento, eficiencia y productividad del IBM QRadar de la Entidad Financiera, para lo cual consideramos los siguientes Servicios:

- Instalación y configuración del SIEM
- Rackeo del equipo SIEM Qradar
- Se definió que el cliente es el encargado de realizar las configuraciones a cada activo según el manual de integración de IBM.
- Integración de 134 dispositivos a correlacionar en el SIEM del listado de tecnologías por integrar.
- Correlación sólo de eventos de seguridad.
- Se definió las acciones de notificación de las alertas de acuerdo al requerimiento de la entidad financiera.
- Creación de 11 reglas (casos de uso) personalizadas.
- La visualización de reportes es predefinida por parte del equipo SIEM.
- Informes de configuración y casos de uso.
- Capacitación de 15 hrs para 10 personas que pertenecen a la entidad financiera

Acta de Constitución

Alcance del Proyecto	Entregable	Criterio de aceptación
Implementación equipo SIEM	• Equipo implementado	
Activación de licencias con nuevos EPS.	• Licencia activada.	
Integración de 134 dispositivos	• 134 dispositivos integrados.	
Creación de 11 reglas (casos de uso) personalizadas.	• 11 reglas configuradas	
Capacitación	• Capacitación realizada.	

Duración estimada inicial del Proyecto	Lugar de Ejecución
El plazo de entrega y configuración del servicio de suscripción será de noventa (90) días calendario.	Los servicios serán provistos en la sede principal de Entidad Financiera

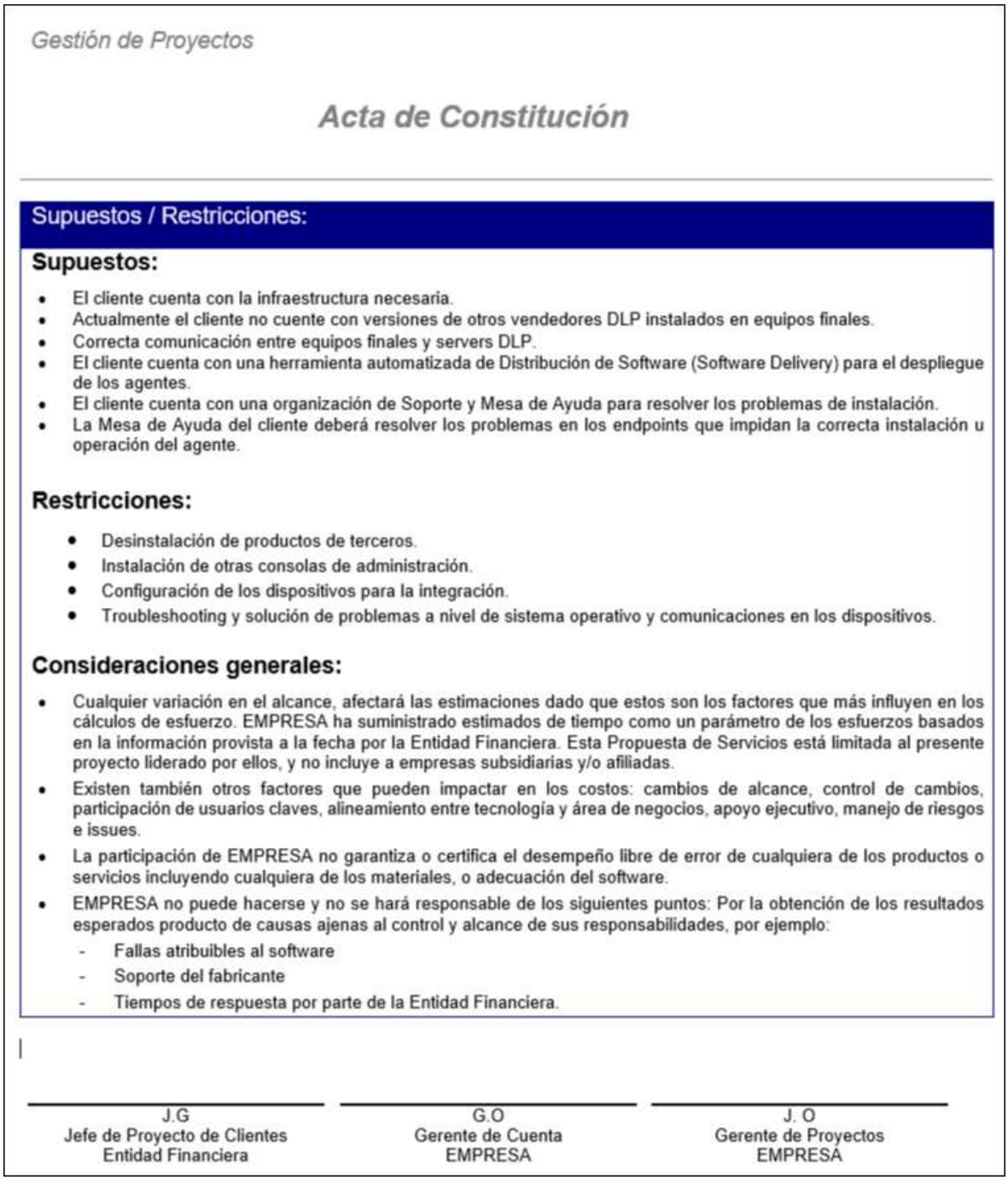
Responsabilidades:

De la **Entidad Financiera:**

- Definición de las directivas de seguridad.
- Asignar a una persona que será el punto de contacto entre EMPRESA y la Entidad Financiera para el Servicio de implementación de la solución y para el Servicio de soporte técnico.
- La persona asignada recibirá la transferencia de conocimientos en:
  - Desarrollo de la instalación
  - Directivas de seguridad configuradas
- La persona asignada debe brindar las facilidades para lograr un trabajo fluido, es decir, brindar los permisos de acceso que se requieren para poder realizar la implementación de la solución y realizar las coordinaciones con las instancias internas de la Entidad Financiera para cumplir con los requisitos de la implementación.
- Aceptación de los entregables, después del visto bueno de las pruebas realizadas la Entidad Financiera debe firmar el acta de conformidad indicando que las pruebas fueron satisfactorias.
- Espacio de trabajo (escritorio, silla, anexo telefónico, punto de red y acceso a Internet) cercano al equipo de trabajo de la Entidad Financiera.

De **EMPRESA:**

- Planificación del proyecto en lo que respecta a instalación y configuración, para ello, EMPRESA cuenta con un Jefe de Proyectos quien se encargará de llevar el control de los procesos de la implementación de la solución.
- Pruebas de las directivas configuradas.
- EMPRESA no se hace responsable en caso surjan problemas por nuevas configuraciones y/o cambios en las configuraciones realizadas por personal ajeno a la organización de EMPRESA.
- EMPRESA no se hace responsable de desconfiguraciones ocasionadas por personal ajeno a la administración de la solución de seguridad. De requerir los servicios de consultoría de EMPRESA ello tendrá un costo de USD 80 por hora hombre sin incluir los impuestos de ley.



Gestión de Proyectos

Acta de Constitución

Supuestos / Restricciones:

Supuestos:

- El cliente cuenta con la infraestructura necesaria.
- Actualmente el cliente no cuente con versiones de otros vendedores DLP instalados en equipos finales.
- Correcta comunicación entre equipos finales y servers DLP.
- El cliente cuenta con una herramienta automatizada de Distribución de Software (Software Delivery) para el despliegue de los agentes.
- El cliente cuenta con una organización de Soporte y Mesa de Ayuda para resolver los problemas de instalación.
- La Mesa de Ayuda del cliente deberá resolver los problemas en los endpoints que impidan la correcta instalación u operación del agente.

Restricciones:

- Desinstalación de productos de terceros.
- Instalación de otras consolas de administración.
- Configuración de los dispositivos para la integración.
- Troubleshooting y solución de problemas a nivel de sistema operativo y comunicaciones en los dispositivos.

Consideraciones generales:

- Cualquier variación en el alcance, afectará las estimaciones dado que estos son los factores que más influyen en los cálculos de esfuerzo. EMPRESA ha suministrado estimados de tiempo como un parámetro de los esfuerzos basados en la información provista a la fecha por la Entidad Financiera. Esta Propuesta de Servicios está limitada al presente proyecto liderado por ellos, y no incluye a empresas subsidiarias y/o afiliadas.
- Existen también otros factores que pueden impactar en los costos: cambios de alcance, control de cambios, participación de usuarios claves, alineamiento entre tecnología y área de negocios, apoyo ejecutivo, manejo de riesgos e issues.
- La participación de EMPRESA no garantiza o certifica el desempeño libre de error de cualquiera de los productos o servicios incluyendo cualquiera de los materiales, o adecuación del software.
- EMPRESA no puede hacerse y no se hará responsable de los siguientes puntos: Por la obtención de los resultados esperados producto de causas ajenas al control y alcance de sus responsabilidades, por ejemplo:
  - Fallas atribuibles al software
  - Soporte del fabricante
  - Tiempos de respuesta por parte de la Entidad Financiera.

J.G	G.O	J. O
Jefe de Proyecto de Clientes Entidad Financiera	Gerente de Cuenta EMPRESA	Gerente de Proyectos EMPRESA

Ilustración 9: Acta de Constitución del Proyecto
Fuente: *Elaboración Propia*

3.3 FASE DE PLANIFICACIÓN DEL PROYECTO

3.3.1 Definición de alcance y limitaciones

3.3.1.1 Alcance

Para la implementación de SIEM en la entidad financiera se ha considerado los siguientes puntos:

- ✓ Instalación y configuración del SIEM.
- ✓ Rackeo del equipo SIEM Qradar.
- ✓ Activación de licencias.
- ✓ Integración de 134 dispositivos a correlacionar en el SIEM del listado de tecnologías por integrar.
- ✓ Se definió que la correlación es solo de eventos de seguridad.
- ✓ Se definió las acciones de notificación de las alertas de acuerdo con el requerimiento de la entidad financiera.
- ✓ Se definió la creación de 11 reglas personalizadas.
- ✓ La visualización de reportes es predefinida por parte del equipo SIEM.
- ✓ Se hizo entrega de informes de configuración, reglas.
- ✓ Se hizo entrega del manual de uso.
- ✓ Se realizó la capacitación de 20 hrs.

3.3.1.2 Limitaciones

A continuación, se describe las limitaciones de la presente tesis:

- Se definió que el cliente es el encargado de realizar las configuraciones a cada activo según el manual de integración de IBM.

- El acceso a la plataforma SIEM solo es posible a través de navegadores web (Microsoft Internet Explorer, Google Chrome y Mozilla Firefox)
- Solo se integró activos propuestos por el cliente.
- Los dashboard son del propio SIEM solo se visualizan de manera gráfica.
- No se integró soluciones o sistemas operativos que no cuenten con soporte del fabricante.
- No se generó propiedades personalizadas.
- No se generó reportes customizados.
- No se incluye la arquitectura de red por privacidad de la entidad financiera.

3.3.2 Requisitos Pre-Implementación

La arquitectura de IBM Security QRadar admite implementaciones de diversos tamaños y topologías, desde una implementación de host único, donde todos los componentes de software se ejecutan en un solo sistema, hasta múltiples hosts, donde dispositivos tales como Event Collectors y Flow Collectors, Data Nodes, Event Los procesadores y los procesadores de flujo tienen roles específicos.

El objetivo principal del primer ejemplo de implementación es describir una única implementación de dispositivo todo en uno para una empresa, dicho ejemplo que será utilizado en el presente proyecto. Los ejemplos posteriores describen las opciones de implementación a medida que la empresa se expande.

Los requisitos para su implementación de QRadar dependen de la capacidad de su implementación elegida para procesar y almacenar todos los datos que desea analizar en su red.

Antes de planificar su implementación, se consideró las siguientes preguntas al cliente:

a) ¿Cómo usa su empresa Internet?
b) ¿Subes tanto como descargas? *(Un mayor uso puede aumentar su exposición a posibles problemas de seguridad.)*
c) ¿Cuántos eventos por segundo (EPS) y flujos por minuto (FPM) necesita monitorear? *(Los requisitos de capacidad de licencia de EPS y FPM aumentan a medida que crece la implementación.)*
d) ¿Cuánta información necesita almacenar y por cuánto tiempo?
e) ¿Conoces las zonas más vulnerables de la infraestructura T.I.?
f) ¿Las búsquedas de información específicas son sencillas?

En una implementación de QRadar de host único, tiene un dispositivo QRadar todo en uno que es un servidor único que recopila datos, como registros de datos de eventos de syslog y eventos de Windows, y también datos de flujo, desde su red.

Las implementaciones de servidor único son adecuadas para empresas que supervisan la actividad de la red y los eventos, como los servicios de autenticación y la actividad del firewall.

Consideraciones:

Para que la funcionalidad del SIEM funcionen correctamente, se debe utilizar un web compatible navegador.

La siguiente tabla enumera las versiones compatibles de los navegadores web:

Navegador Web	Versiones Soportadas
64-bit Mozilla Firefox	45.8 Versión de soporte extendido y posterior
Microsoft Internet Explorer de 64 bits con Microsoft	11.0, Edge 38.14393 y posterior
64-bit Google Chrome	Último

Tabla 10: Navegadores soportadas por Qradar

3.3.3 Diagrama de Arquitectura

3.3.3.1 La empresa fabricante despliega un único servidor QRadar

El siguiente diagrama muestra un dispositivo Todo en Uno, que recopila datos de orígenes de eventos y flujos, procesa los datos y proporciona una aplicación web donde puede buscar, monitorear y responder a amenazas de seguridad.

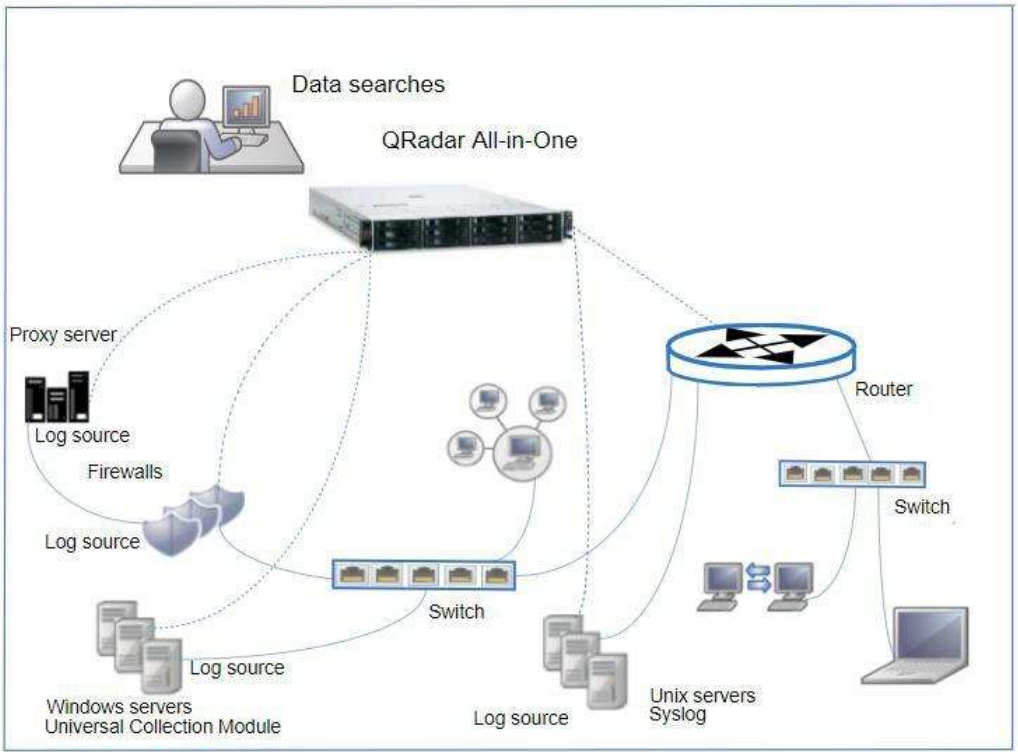


Ilustración 10: Despliegue todo en uno

El dispositivo QRadar All-in-One realiza las siguientes tareas:

- Recopila datos de eventos y flujo de red, y luego normaliza los datos en un formato de datos que QRadar puede usar.
- Analiza y almacena los datos e identifica las amenazas de seguridad.
- Proporciona acceso a la aplicación web QRadar.
- A medida que crecen sus fuentes de datos, o aumentan sus necesidades de procesamiento o almacenamiento, puede agregar dispositivos para expandir su implementación.

3.3.4 Cronograma de Actividades

La duración del proyecto duró 90 días laborales, a continuación, se muestra el cronograma con las actividades realizadas en los días definidos.

NOMBRE DE TAREA	DURACIÓN	COMIENZO	FIN
PROYECTO: Implementación de un Security Information and Event Management (SIEM)	**90 días**	**lun 03/06/19**	**vie 04/10/19**
1. FASE DE INICIO	**4 días**	**lun 03/06/19**	**jue 06/06/19**
1.1. Identificación de Recursos del Proyecto	**4 días**	**lun 03/06/19**	**jue 06/06/19**
1.1.1. Identificación de stakeholder	1 día	lun 03/06/19	lun 03/06/19
1.1.2. Identificación de equipos	1 día	mar 04/06/19	mar 04/06/19
1.2. Acta de constitución del proyecto	1 día	mié 05/06/19	mié 05/06/19
2. FASE DE PLANIFICACIÓN	**6 días**	**vie 07/06/19**	**vie 14/06/19**
2.1. Definición de alcance y limitaciones	1 día	vie 07/06/19	vie 07/06/19
2.2. Requisitos pre-implementación	1 día	vie 07/06/19	vie 07/06/19
2.3 Diagrama de Arquitectura	1 día	lun 10/06/19	lun 10/06/19
2.4 Cronograma de actividades	1 día	mar 11/06/19	mar 11/06/19
2.5 Identificación de Riesgos	1 día	mié 12/06/19	mié 12/06/19

2.6 Costo de proyecto	1 día	jue 13/06/19	jue 13/06/19
3. FASE IMPLEMENTACIÓN Y CONFIGURACIÓN	**52 días**	**lun 17/06/19**	**mar 27/08/19**
3.1 SPRINT 1: Implementación SIEM y Configuración	**7 días**	**lun 17/06/19**	**mar 25/06/19**
3.1.1 Implementación del SIEM	3 días	lun 17/06/19	mié 19/06/19
3.2.2 Instalación de licencias	1 día	jue 20/06/19	jue 20/06/19
3.2.3 Configuración en consola Qradar	1 día	vie 21/06/19	vie 21/06/19
3.2.4 Rackeo de equipo	1 día	lun 24/06/19	lun 24/06/19
3.2.5 Pruebas de configuración	1 día	mar 25/06/19	mar 25/06/19
3.2 SPRINT 2: Integració n de equipos al SIEM	**45 días**	**mié 26/06/19**	**mar 27/08/19**
3.2.1 Planeamiento	2 días	mié 26/06/19	jue 27/06/19
3.2.2 Procedimiento de integración	22 días	lun 01/07/19	mar 30/07/19
3.3 SPRINT 3: Configuración de reglas	**14 días**	**jue 01/08/19**	**mar 20/08/19**
3.3.1 Planeamiento	2 días	jue 01/08/19	vie 02/08/19
3.3.2 Configuración de reglas	10 días	lun 05/08/19	vie 16/08/19
3.3.3 Pruebas	2 días	lun 19/08/19	mar 20/08/19
4. FASE Monitoreo y Control	**15 días**	**lun 26/08/19**	**vie 13/09/19**
Monitoreo de eventos	**15 días**	**lun 26/08/19**	**vie 13/09/19**
4.1 Monitoreo de eventos	7 días	lun 26/08/19	Mar 03/09/19
4.2 Monitoreo de alertas	8 días	mie 04/09/19	vie 13/09/19
5. FASE CIERRE	**19 días**	**lun 23/09/19**	**vie 04/10/19**
5.1 Capacitación	5 días	lun 23/09/19	vie 27/09/19
5.2 Acta de conformidad	3 días	mié 02/10/19	vie 04/10/19

Tabla 11: Cronograma de actividades
Fuente: *Elaboración Propia*

3.3.5 Identificación de Riesgos

3.3.5.1 Impacto y Probabilidad

Los riesgos se calcularán multiplicando la cuantificación del impacto por la cuantificación de la probabilidad de aparición. Tanto la cuantificación del impacto como la de probabilidad de aparición, pueden tomar valores del 1 al 3 (bajo, medio y alto respectivamente). En consecuencia, la ponderación final del riesgo puede tomar valores de 1 a 9.

PROBABILIADAD	IMPACTO	PONDERACIÓN	CRITERIO
Alto	Alto	3	diario
Medio	Medio	2	semanal
Bajo	Bajo	1	Mensual

Tabla 12: Impacto y Probabilidad
Fuente: *Elaboración Propia*

3.3.5.2 Ponderación de Riesgo

RIESGO	PONDERACIÓN
Alto	7 a 9
Medio	4 a 6
Bajo	1 a 3

Tabla 13: Ponderación de Riesgo
Fuente: *Elaboración Propia*

3.3.5.3 Identificación de Riesgos

TIPO	DESCRIPCIÓN DEL RIESGO
RRHH	Cancelación de reuniones diarias
Financiero	Cancelación del proyecto
Financiero	Incumplimiento de las fechas establecidas para los entregables definidos en cada fase del proyecto
RRHH	Abandono de trabajo del personal asignado al proyecto
Tecnológico	Indisponibilidad del equipo SIEM

Tabla 14: Riesgos durante del proyecto
Fuente: *Elaboración Propia*

3.3.5.4 Matriz de Riesgo

TIPO	DESCRIPCIÓN	PROBABILIDAD	IMPACTO	RIESGO
RRHH	Cancelación de reuniones diarias	3	2	Medio
Financiero	Cancelación del proyecto	1	3	Bajo
Financiero	Incumplimiento de las fechas establecidas para los entregables definidos en cada fase del proyecto	2	2	Medio
RRHH	Abandono de trabajo del personal asignado al proyecto	1	3	Bajo
Tecnológico	Indisponibilidad del equipo SIEM	1	2	Bajo

Tabla 15: Matriz de Riesgo
Fuente: *Elaboración Propia*

Una vez definidos los riesgos del proyecto y la categoría a la que pertenecen por el tipo de impacto que causan, se creó la matriz de riesgos donde se puede apreciar el nivel de impacto, la importancia y el nivel de riesgo.

3.3.5.5 Plan de Contingencia

A continuación, se define el plan de contingencia que describe las acciones que permiten mitigar el riesgo.

DESCRIPCIÓN RIESGO	ACCIÓN PARA MITIGAR	ACCIÓN DE CONTINGENCIA
Cancelación de reuniones diarias	Optar por reprogramar la reunión para un día particular por única vez.	El cronograma de proyecto debe contemplar este tipo de escenarios para poder reprogramar la reunión sin impacto en el tiempo del proyecto.
Cancelación del proyecto	Definir cláusulas de cancelación del proyecto en el contrato.	Haciendo uso de las cláusulas se debe proceder al pago establecido de acuerdo a ley.
Incumplimiento de las fechas establecidas para los entregables definidos en cada fase del proyecto	Definir acuerdos por demora en los entregables	Duplicar los esfuerzos de los integrantes del equipo del proyecto.
Abandono de trabajo del personal asignado al proyecto	Elaborar cartera de personal en espera.	Contactar al personal de la cartera en espera y contar con el presupuesto necesario
Indisponibilidad del equipo SIEM	Definir partner alternos para la compra de equipo.	Utilizar vías alternas para lograr la comprar del equipo.

Tabla 16: Plan de Contingencia
Fuente: *Elaboración Propia*

3.3.6 Costo del Proyecto

Para poder definir el flujo de caja es fundamental detallar en primer lugar el costo de los recursos que se utilizarán en el proyecto como:

- Materiales y equipos
- Servicios de Recursos Humanos
- Equipo SIEM

3.3.6.1 Costos en Materiales y Equipos

A continuación, se detallan los materiales, insumos y equipos que se utilizaron durante el tiempo de la implementación.

Materiales	Costo Total
Uso de espacio	S/ 800.00
Uso de recursos depreciables (Laptop, mouse, celular, impresora)	S/ 200.00
S.O. Windows 10 Pro	S/ 200.00
Papel Bond A4	S/ 12.00
Tinta para impresora	S/ 150.00
Electricidad	S/ 150.00
Internet y teléfono	S/ 150.00
TOTAL:	**S/ 1,662.00**

Tabla 17: Costos en Materiales y Equipos
Fuente: *Elaboración Propia*

3.3.6.2 Costo de Recursos Humanos

A continuación, se detallan los gastos de recursos humanos para el proyecto:

- Las semanas de esfuerzo.
- El costo semanal.
- El sueldo total.

Cargo	Cant	Semanas	Costo Semanal	Total
Gerente de Operaciones	1	1/2	1,000.00	1,000.00
Jefe de proyecto	1	9	950.00	8,550.00
Especialista	1	9	750.00	6,750.00
Analista de Seguridad I	2	9	550.00	9,900.00
TOTAL:				**26,200.00**

Tabla 18: Costo de Recursos Humanos
Fuente: *Elaboración Propia*

3.3.6.3 Costo en Equipo

A continuación, se detallan el gasto del equipo SIEM para el proyecto:

Cargo	Cant	Costo Semanal	Total
IMB SIEM QRadar + Licencia 1.5k eventos	1	300,800.00	300,800.00
TOTAL:			**300,800.00**

Tabla 19 Costo en Equipo
Fuente: *Elaboración Propia*

3.3.7 Planificación de SPRINT's

Para el desarrollo de cada Sprint se han planificado revisiones y entregables para validar los avances logrados y así generar de manera retrospectiva las acciones de mejora para los siguientes sprints.

SPRINT N° 1

SPRINT N° 1: Implementación y Configuración SIEM	
Fecha de Inicio	17/06/2019
Fecha de Fin	25/06/2019
Revisión de los avances	Este SPRINT dura solo 1 semana, por lo que la única fecha de revisión será el día 21/06/2019
Tareas a desarrollar	Definición de Requisitos Pre-Implementación
	Implementación del SIEM
	Instalación de licencias
	Configuración en consola QRadar
	Rackeo del equipo
	Pruebas de configuración

Tabla 20: Planificación del Sprint N° 1
Fuente: *Elaboración Propia*

SPRINT N° 2

SPRINT N° 2: Integración de activos al SIEM	
Fecha de Inicio	26/06/2019
Fecha de Fin	27/08/2019
Revisión de los avances	Este SPRINT dura 3 semanas, las fechas de revisión serán las siguientes: - 10/07/2019 - 31/07/2019 - 23/07/2019
Tareas a desarrollar	Configuración de activos (tarea realizada por el cliente)
	Integración de activos al QRadar
	Pruebas de recepción de syslog

Tabla 21: Planificación del Sprint N° 2
Fuente: *Elaboración Propia*

SPRINT N° 3

SPRINT N° 3: Configuración de reglas	
Fecha de Inicio	01/08/2019
Fecha de Fin	20/08/2019
Revisión de los avances	Este SPRINT dura 3 semanas, las fechas de revisión serán las siguientes: - 09/08/2019 - 16/08/2019
Tareas a desarrollar	Análisis de 11 reglas
	Configuración de 11 reglas
	Pruebas de alertas

Tabla 22: Planificación del Sprint N°3
Fuente: *Elaboración Propia*

3.3.7.1 Definición de TaskBoard

TaskBoard Inicial

Se presenta el Taskboard de desarrollo inicial del proyecto con todas las historias y la condición inicial de cada uno de los Sprint.

INICIO: 17/06/2019				
FIN: 25/06/2019				
Sprint's	**Historia de Usuario**	**Pendiente**	**En Curso**	**Hecho**
Sprint 1	Definición de Requisitos Pre-Implementación	✓		
	Implementación del SIEM	✓		
	Instalación de licencias	✓		
	Configuración en consola QRadar	✓		
	Rackeo del equipo	✓		
	Pruebas de configuración	✓		
Sprint 2	Validaciones de recepción de paquetes de logsource	✓		
	Integración de activos al QRadar	✓		

Sprint 3	Análisis de 11 reglas	✓		
	Configuración de 11 reglas	✓		

Tabla 23: TaskBoard Inicial
Fuente: *Elaboración Propia*

3.3.7.2 Pruebas de Sprint's

Se definió pruebas al finalizar cada Sprint completando el siguiente formulario, para asegurar la calidad de cada sprint.

PRUEBA FUNCIONAL						
PRUEBA				**VERSIÓN**		
				FECHA EJECUCIÓN		
TAREA						
Descripción del caso de prueba						
1. Caso de pruebas						
a. Precondiciones						
b. Pasos de pruebas						
Datos de entrada			**Respuesta esperada de la aplicación**	**Coincide**		**Respuesta del Sistema**
Campo	**Valor**	**Tipo Escenario**		**SI**	**NO**	

Tabla 24: Formato de Pruebas de Sprint's
Fuente: *Elaboración Propia*

3.4 FASE IMPLEMENTACIÓN Y CONFIGURACIÓN

3.4.1 SPRINT 1: Implementación y Configuración de SIEM

3.4.1.1 Implementación SIEM

I. Backlog

Lista de historias de usuario por orden de importancia (BACKLOG)			
Historia de Usuario	**Prioridad**	**Importancia**	**Tiempo Estimado**
Definición de Requisitos Pre-Implementación	Alta	5	1 día
Implementación del SIEM	Alta	5	1 día
Instalación de licencias	Alta	4	1 día
Configuración en consola QRadar	Alta	5	1 día
Rackeo de equipo	Alta	5	1 día
Pruebas de configuración	Alta	5	2 días

Tabla 25: Backlog
Fuente: *Elaboración Propia*

II. Historia de Usuario

HISTORIA DE USUARIO	
ID: HU01	**NOMBRE HISTORIA:** Implementación y Configuración de SIEM
Stakeholders: Jefe de proyecto, líder del equipo, equipo implementador y cliente	
Prioridad en el Negocio: Alto	**Importancia del Desarrollo:** 100
Tiempo Estimado: 7 días	**Modulo Asignado:** Implementación
Descripción: Definición de Requisitos Pre-Implementación Implementación del SIEM Instalación de licencias Configuración en consola Qradar Rackeo de equipo Pruebas de configuración	
Observaciones: Se debe tomar en cuentas las consideraciones pre-implementación.	

Tabla 26:Historia de Usuario 01
Fuente: *Elaboración Propia*

III. Daily Scrum 1

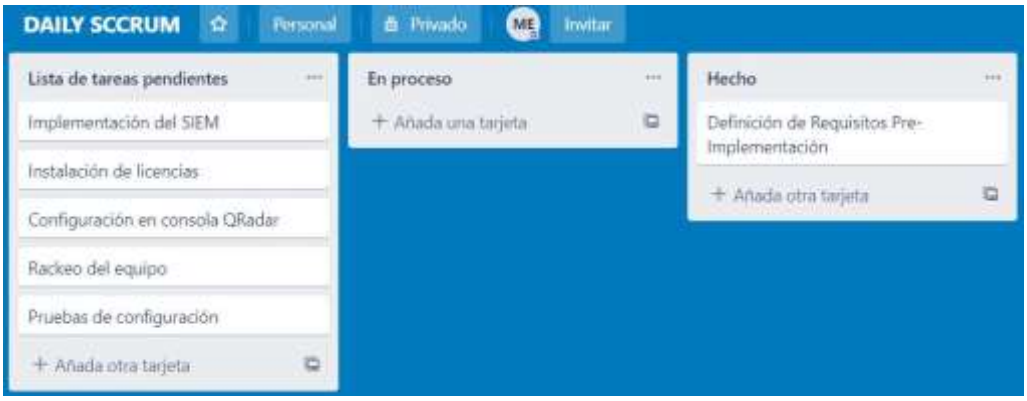


Ilustración 11: Daily Scrum 1 - Sprint 1
Fuente: *Elaboración Propia*

IV. Proceso de Instalación SIEM

1. Seleccionar Instalar Red Hat Enterprise Linux 7.3 cuando se le presente un menú de opciones, como en la siguiente imagen:

Ilustración 12: Instalando Red Hat Enterprise Linux 7.3

2. Seleccionar el tipo de instalación, el hardware y el software que vienen de IBM (comprado como un dispositivo).

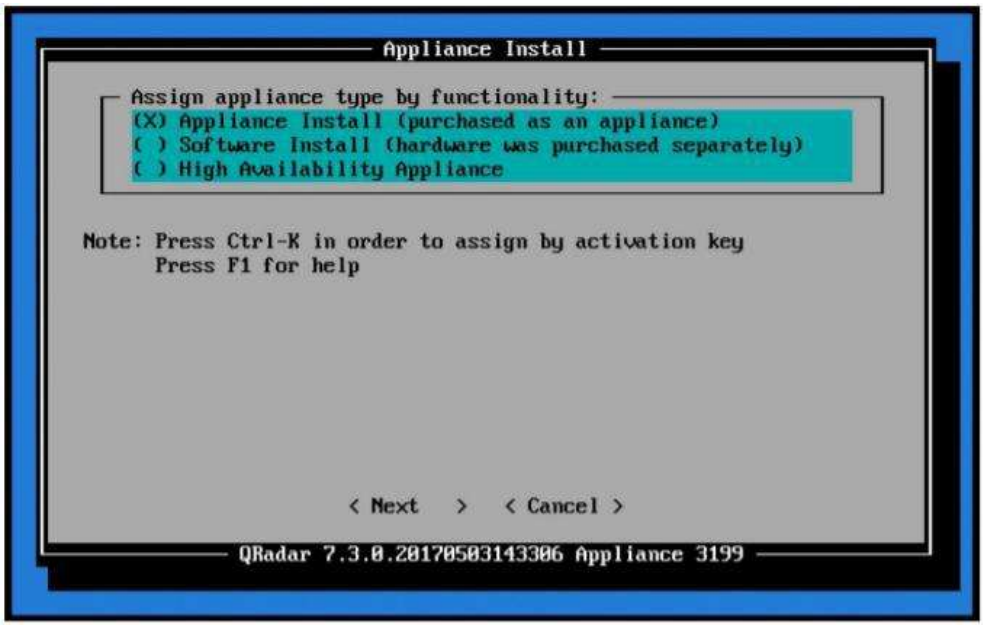


Ilustración 13: Appliance Install

3. Luego seleccione el tipo de configuración, en este caso es una instalación normal

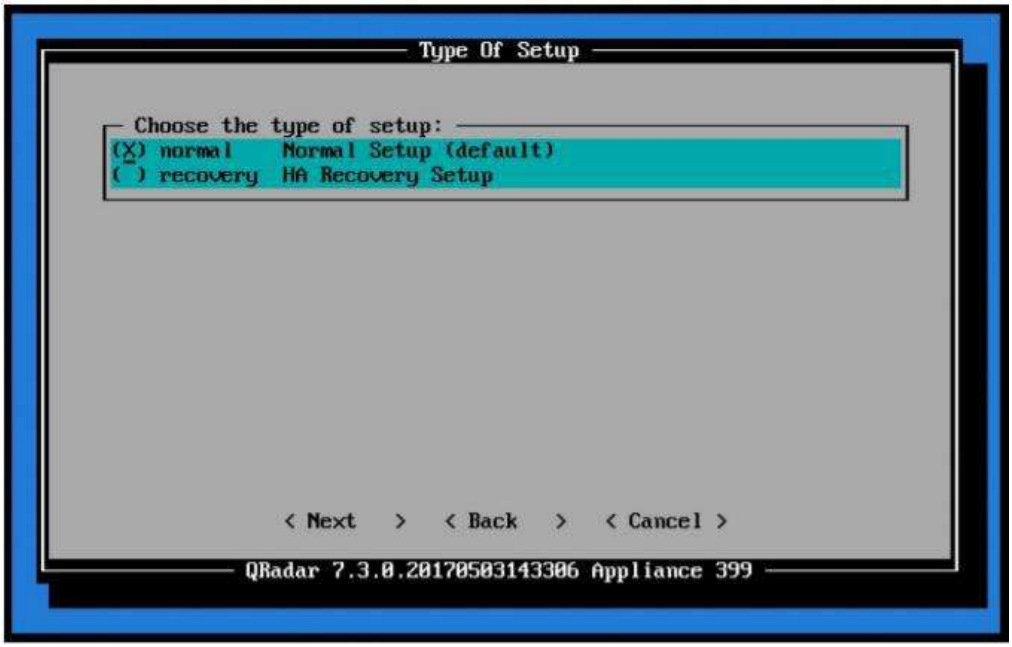


Ilustración 14: Tipo de instalación

4. Luego, se configura la fecha y la hora manualmente. También puede configurar el servidor horario, ya sea por hostname o IP.

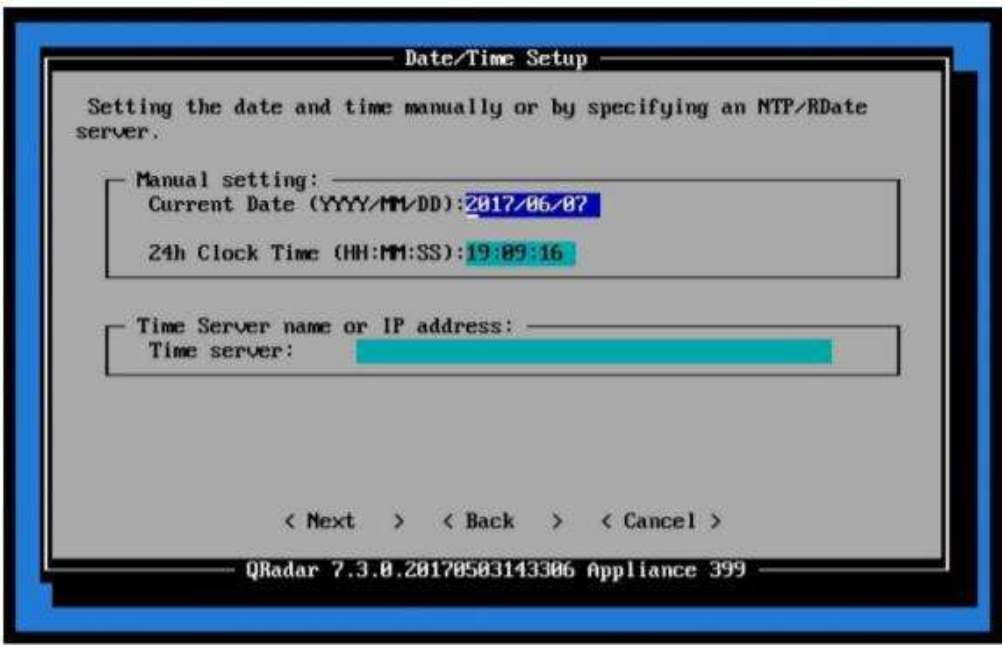


Ilustración 15: Configuración de fecha, hora e IP

5. Luego se configura la zona horaria del dispositivo

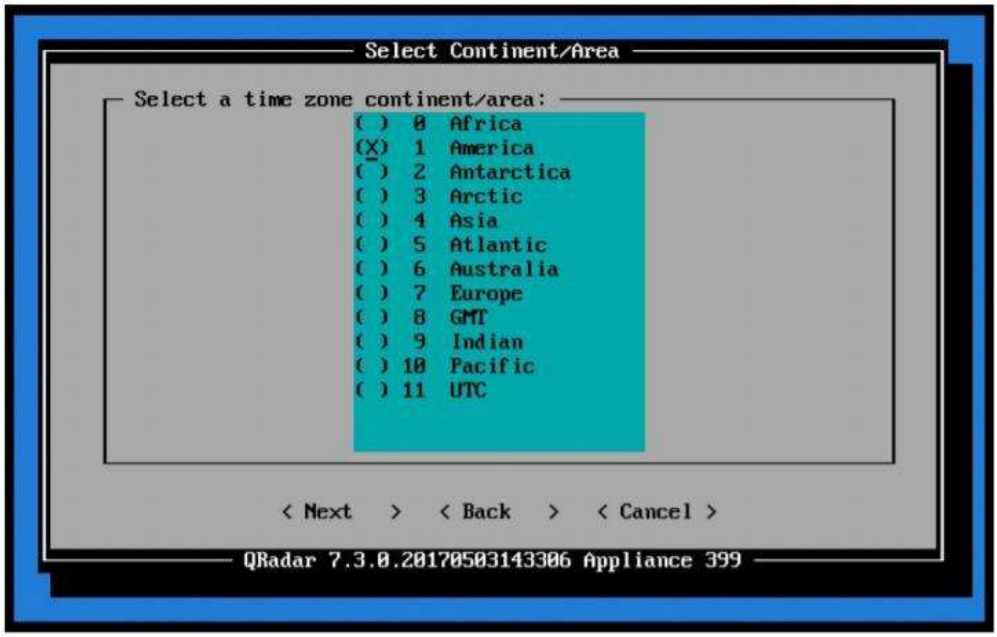


Ilustración 16: Selección de zona horaria

6. Luego se configura la interfaz de red

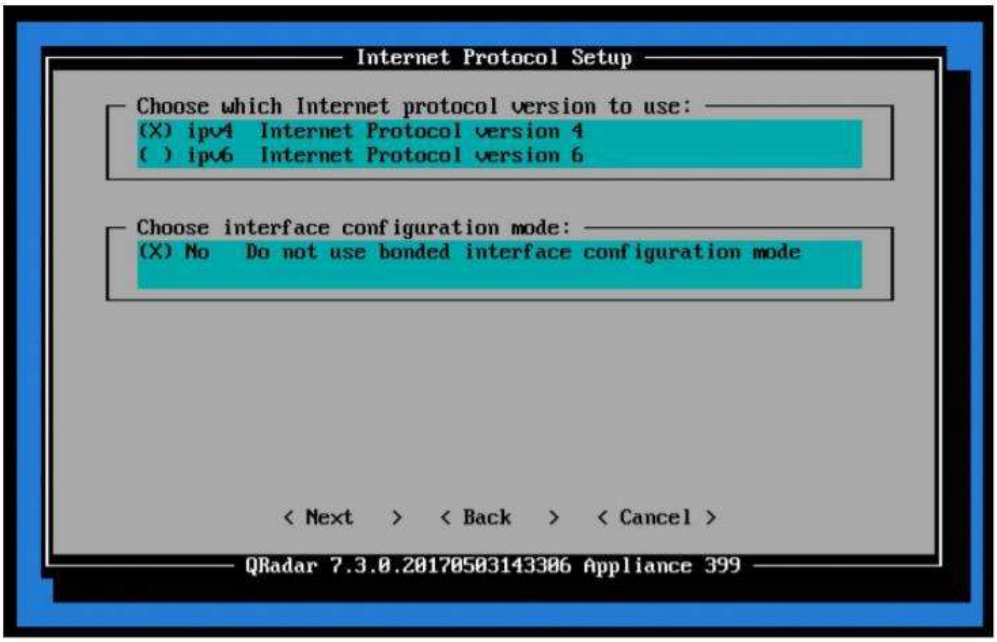


Ilustración 17: Interfaz de red

7. Luego, se selecciona la interfaz de administración. En este caso, solo tenemos una NIC,

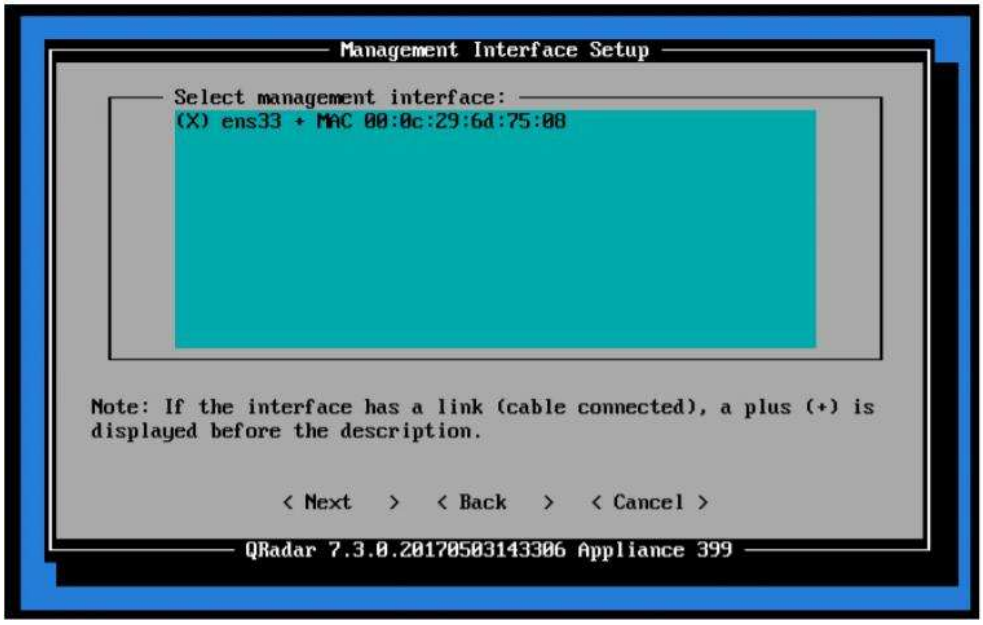


Ilustración 18: Configuración de la interfaz de administración

8. Se ingresa la información de red (como la dirección IP, el nombre de host, la máscara de red, etc.), se debe completar el dominio.

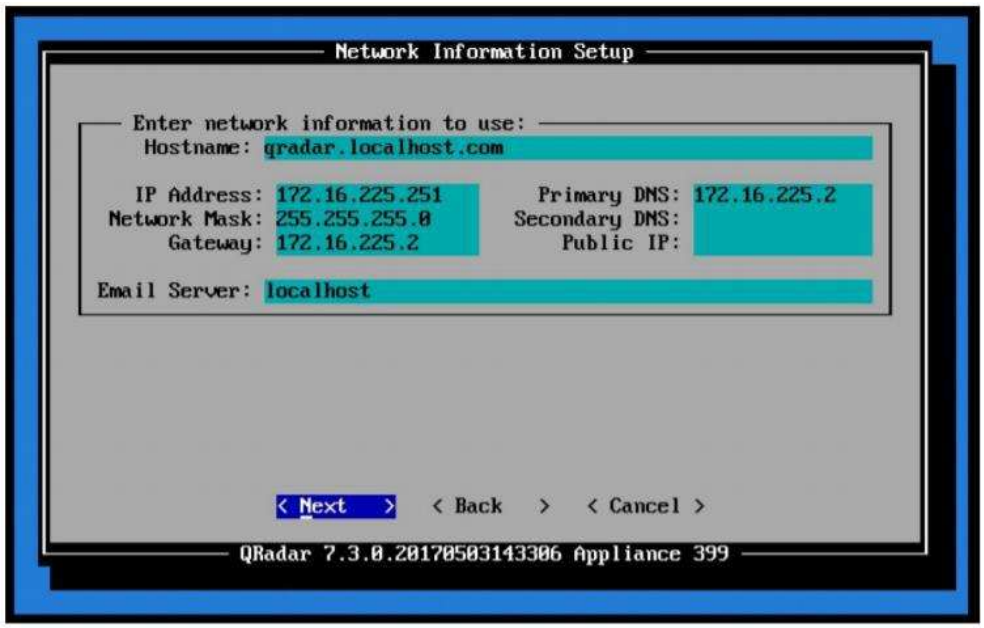


Ilustración 19: Configuración de Red

9. Se ingresa la contraseña de administrador, que es la contraseña para el administrador del usuario y se utiliza para iniciar sesión a través del acceso web. Luego se configura la contraseña de root. Esta contraseña raíz es el usuario para el acceso SSH (CLI)

Ilustración 20: Configuración de credencial

10. En este punto, el instalador continúa su proceso automáticamente.

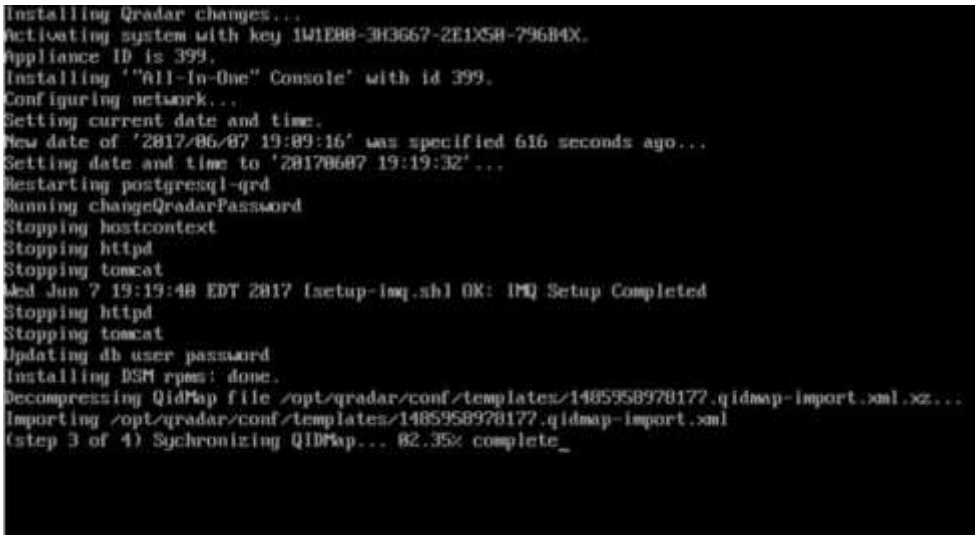


Ilustración 21: Carga de configuración

11. Cuando se completa el proceso de instalación, recibe la notificación que se muestra en la Figura.

Ilustración 22: Proceso de instalación completa

V. Daily Scrum 2

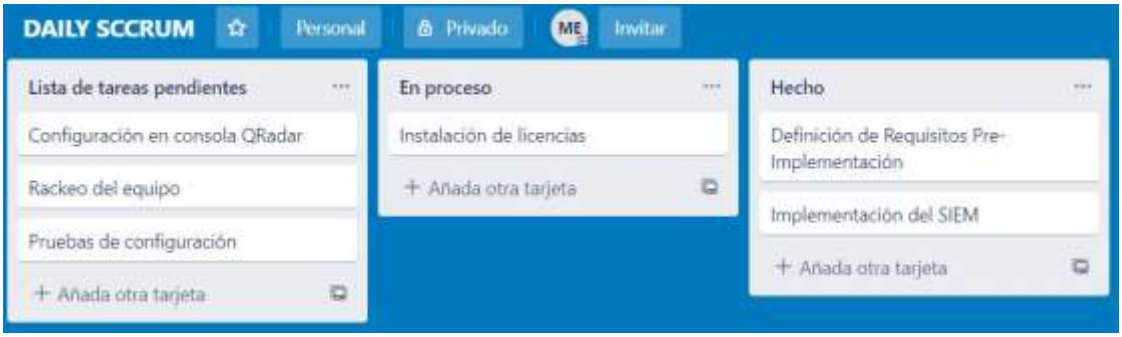


Ilustración 23: Daily Scrum 2 - Sprint 1

3.4.1.2 Instalación de Licencias

Una vez que se completa el proceso de instalación, debe aplicar la licencia.

Procedimiento para aplicar la licencia:

1. Se inició sesión en la consola web de QRadar. Usamos la IP que configuró en la consola de QRadar:

   https: // <dirección IP de la consola>

2. Luego, se inicia sesión con el administrador de usuario y las credenciales establecidas durante la instalación.

Ilustración 24: Pagina de Logueo

3. Ingresamos a la pestaña administrador y entramos a “System and License Managment”

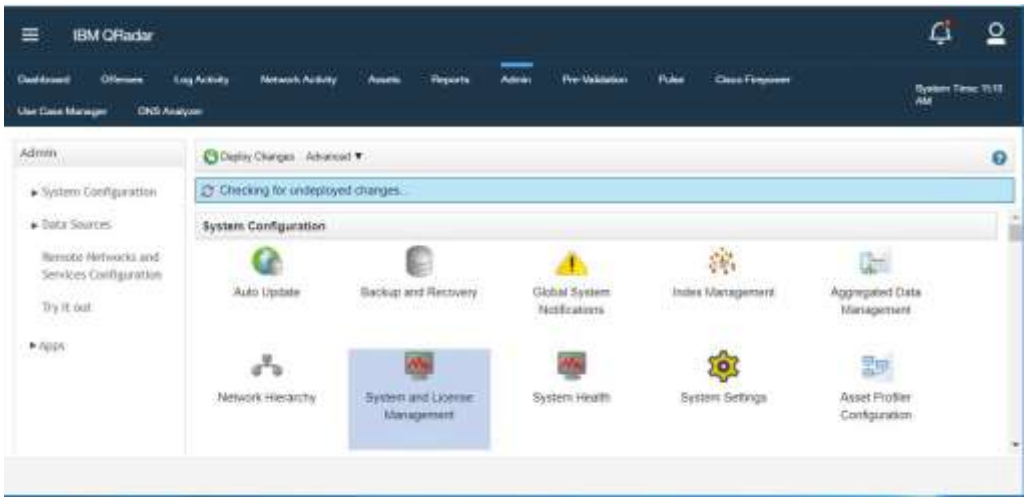


Ilustración 25: Pestaña Administrador Qradar

4. Desde la ventana emergente, hacemos clic en el menú Cargar licencia.

Ilustración 26: System and License Managment

5. Examinamos para seleccionar el archivo de licencia para el dispositivo deseado, en este caso es para una consola. Después de seleccionar, damos clic en el botón “Cargar licencia”.

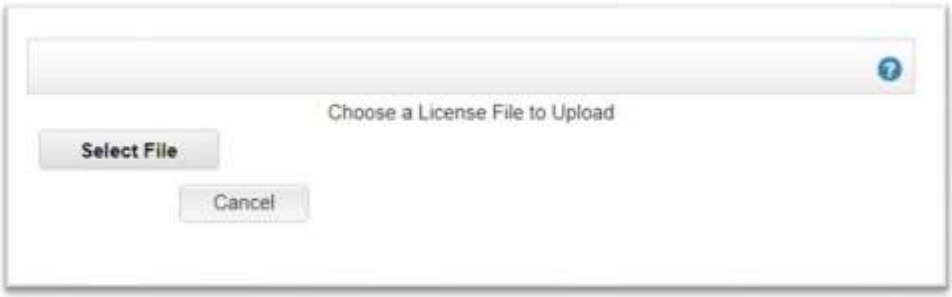


Ilustración 27: Integración de equipos al SIEM

6. Después de cargar la licencia en la consola, debe asignarla al dispositivo correcto. En el menú Sistema y Administración de licencias, seleccionamos la pantalla de licencias, haga clic en la licencia y luego haga clic en Asignar licencia al sistema.

Ilustración 28: Carga de Licencia

7. Después de aplicar y asignar la licencia al dispositivo correcto, haga clic en Implementar cambios de licencia y luego en Continuar.

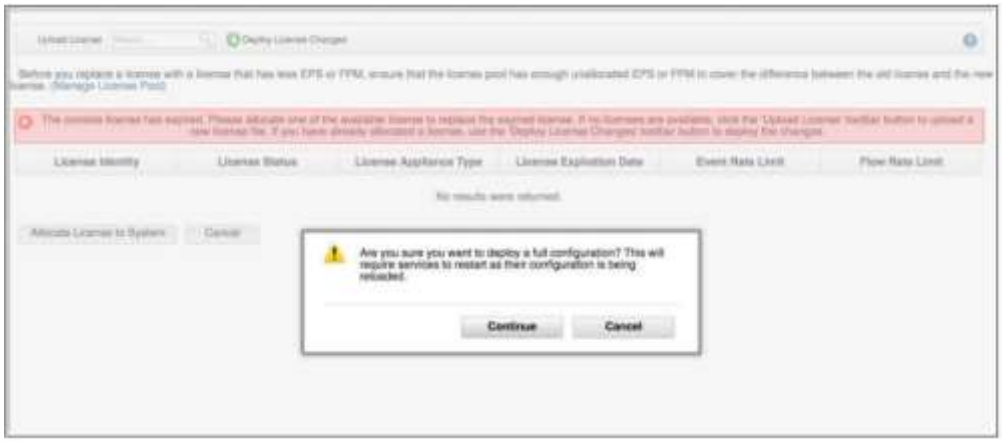


Ilustración 29: Activación de Licencia

8. En este punto, el dispositivo ya está listo para comenzar a funcionar. Aparece el mensaje "No hay cambios para implementar" desde la pestaña Administrador.

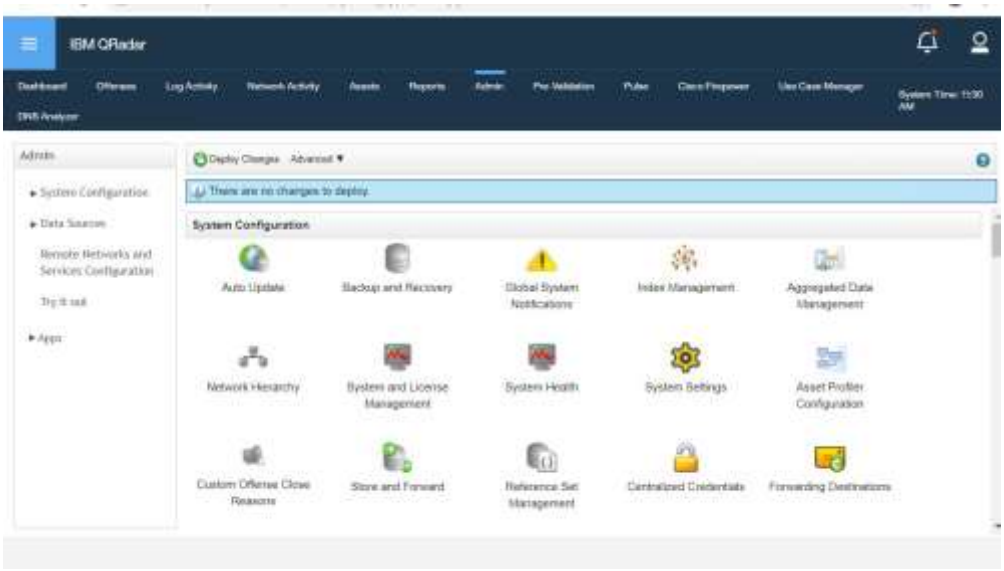


Ilustración 30: Licencia activada

VI. Daily Scrum 2

Ilustración 31:Daily Scrum 3 - Sprint 1
Fuente: *Elaboración Propia*

3.4.1.3 Configuración en Consola Qradar

Se realizó el siguiente procedimiento para realizar la configuración de la consola QRadar.

1) Ingresar a la consola de QRadar e ir al Menu y seleccionar Admi

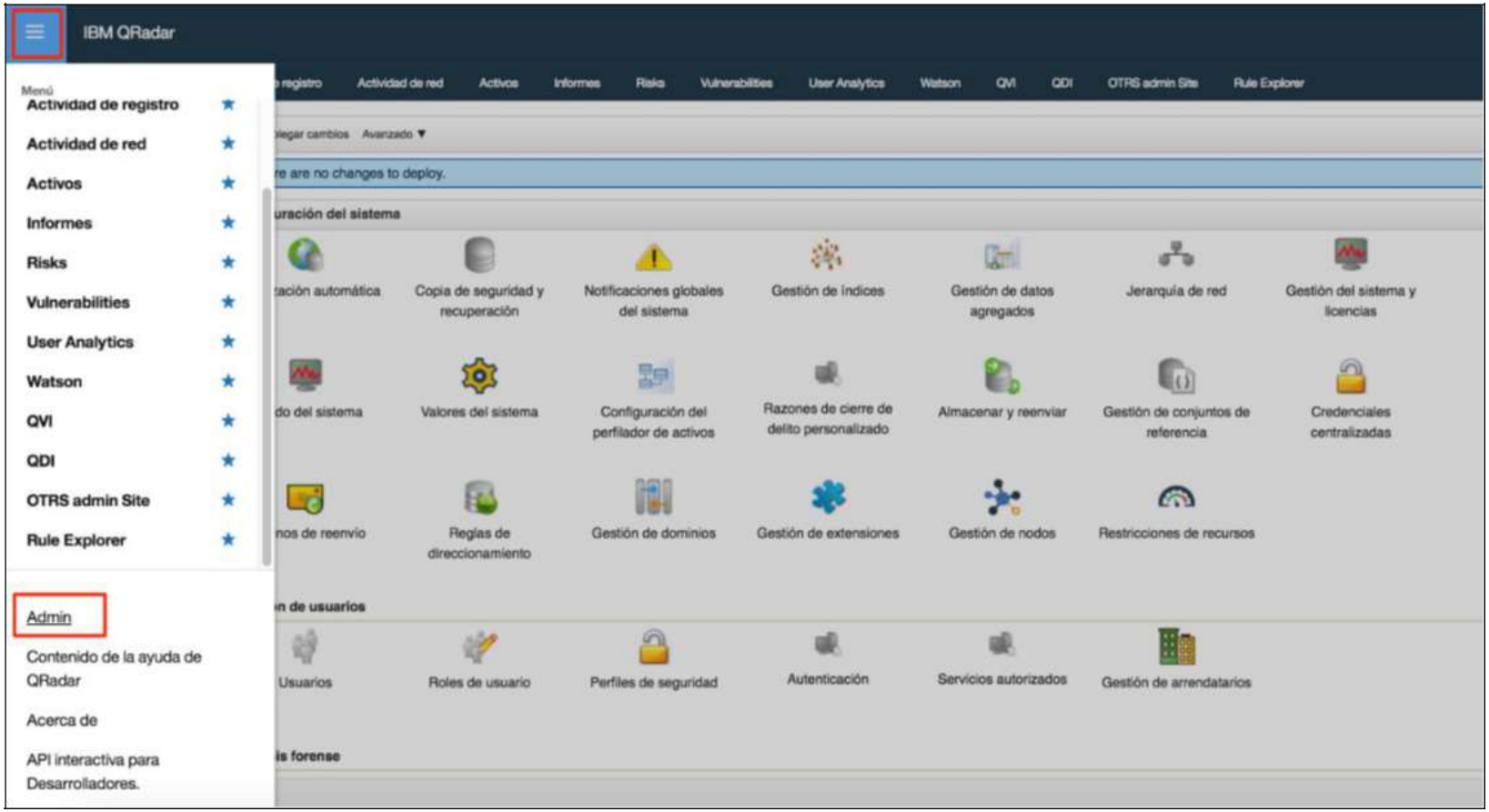


Ilustración 32: Ingreso a consola de Qradar

2) Ingresar en Tenant Management para crear o editar algún Tenant.

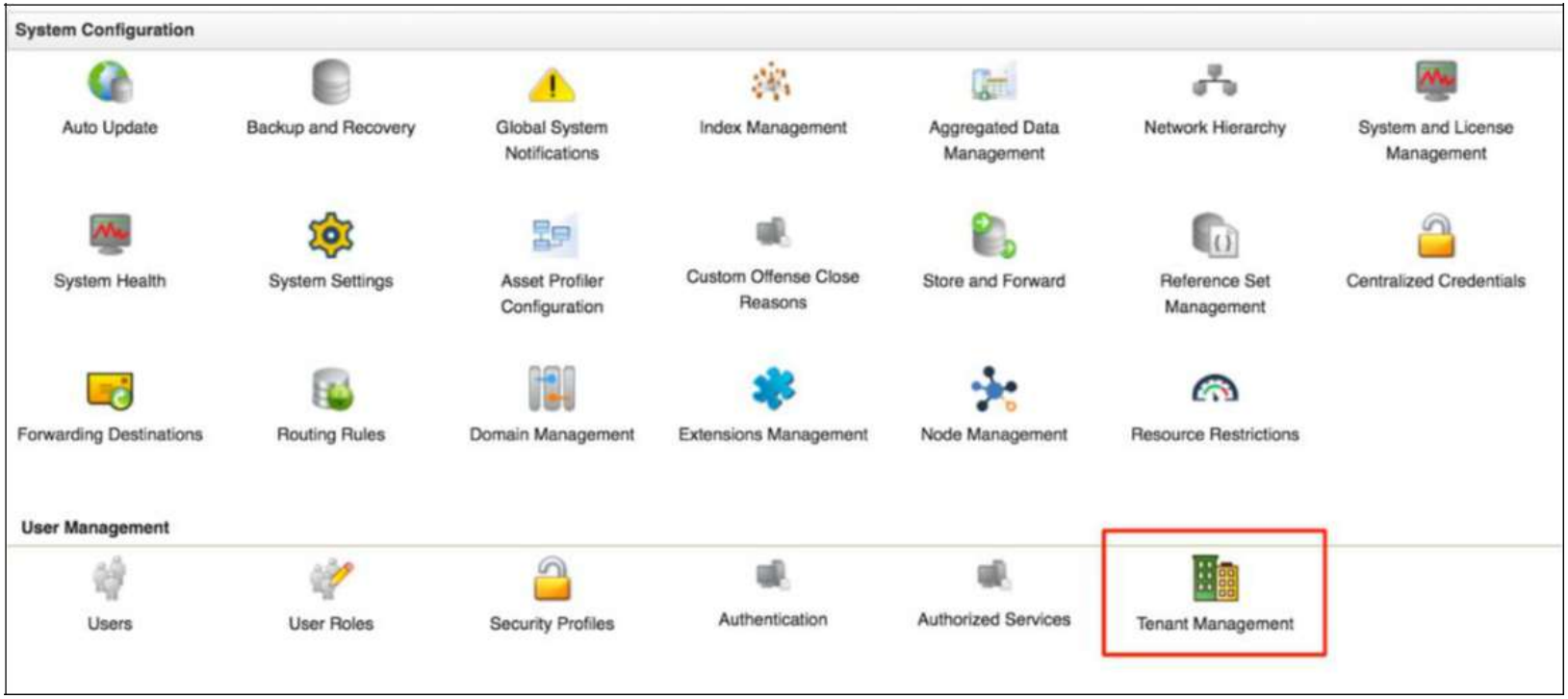


Ilustración 33: Panel de Administración para agregar Tenant

3) En la ventana, hacer click en “Add”, llenar con los datos del cliente como Nombre y Descripción, y finalizar con Crear.

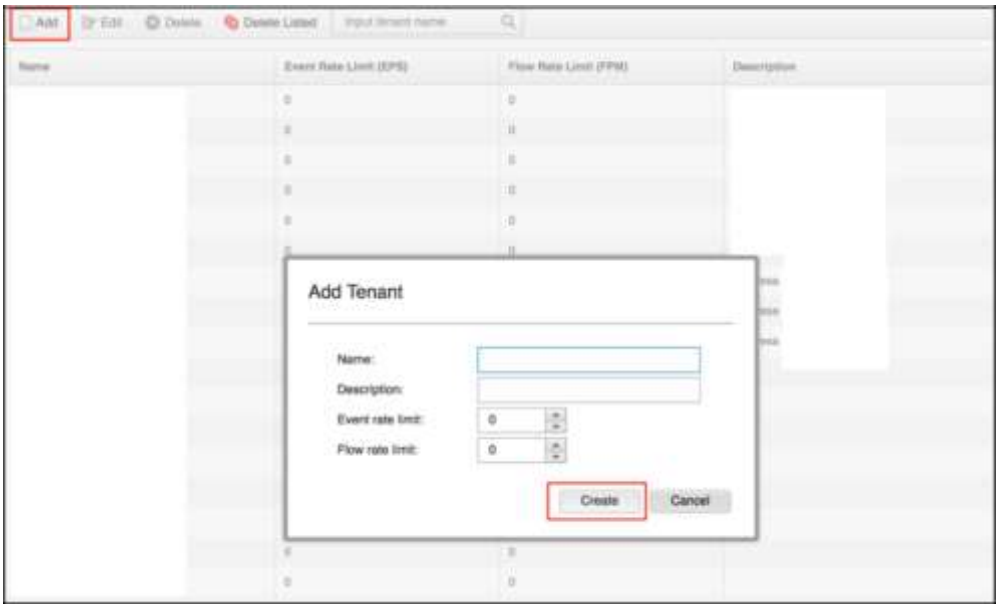


Ilustración 34: Ventana para configurar Tenant

4) Luego, se debe crear un Log Source, ingresando donde indica la imagen.

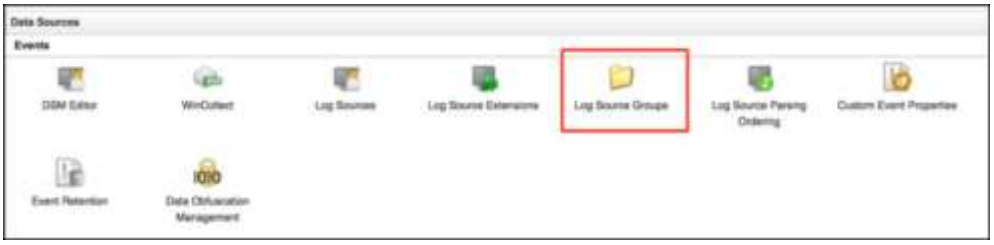


Ilustración 35: Panel de Administración para agregar Log Source

5) Hacer click en “New Group” y nuevamente llenar con los datos del cliente, Nombre y Descripción. Click en Ok.

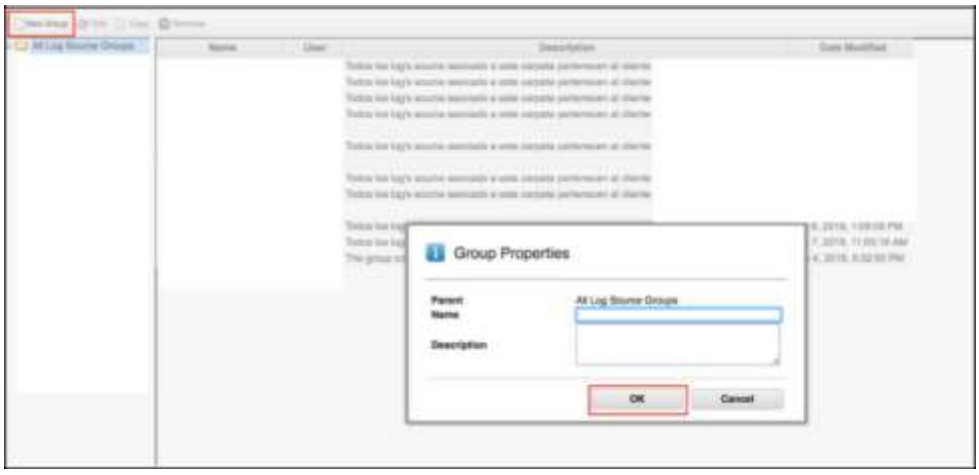


Ilustración 36: Ventana para configurar Log Source

6) Volver al panel de administración e ingresar en el Gestor de Dominios.

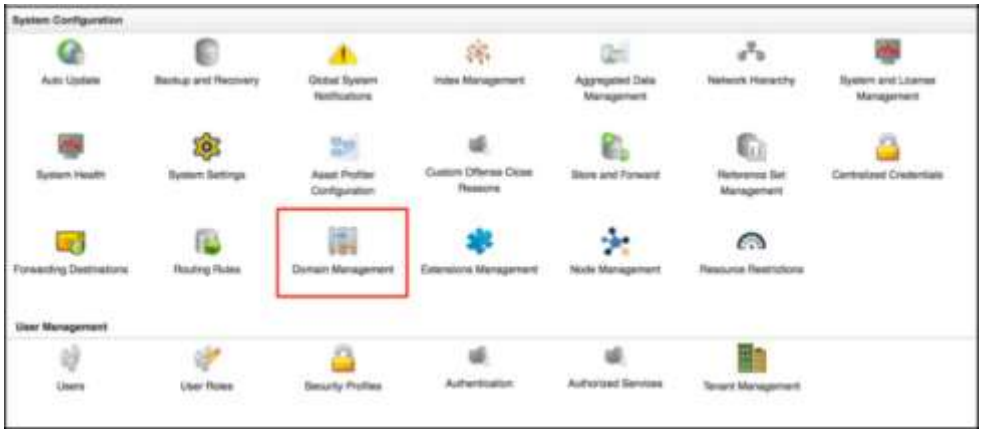


Ilustración 37: Panel de Administración para agregar Dominio

7) Crear un nuevo dominio ingresando en “Add”, completar con el nombre del cliente y descripción, ir a la pestaña “Events” y luego a “Log Sources”, seleccionar la carpeta asociada al cliente y click en “Add”. Finalizar con “Create”.

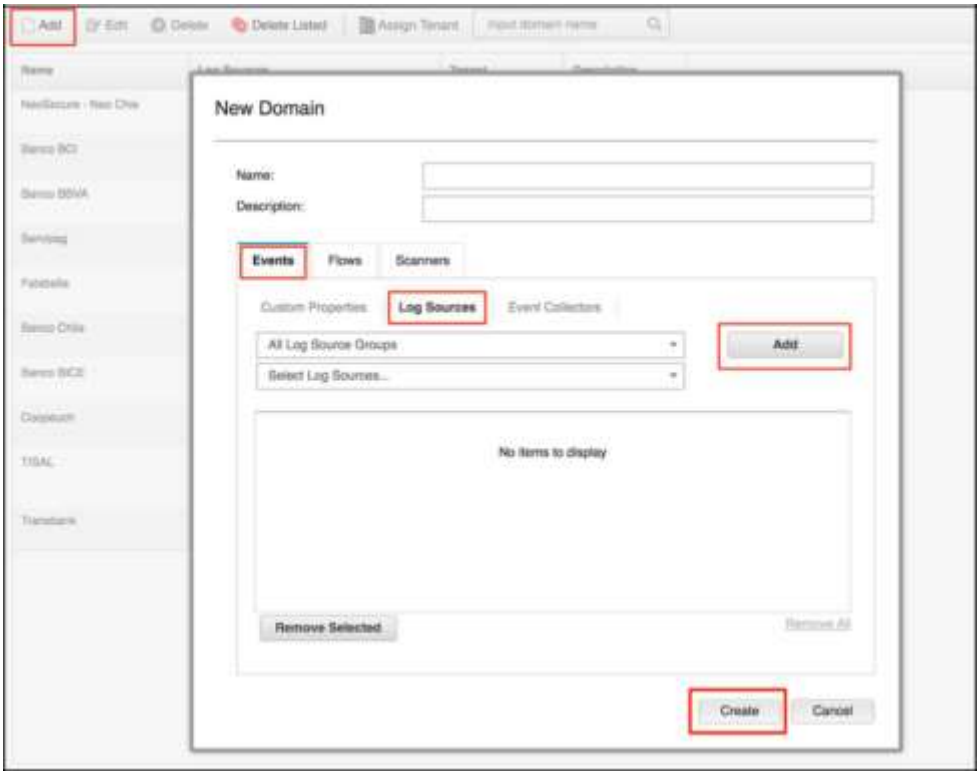


Ilustración 38: Ventana para asociar Log Source al dominio del Cliente

8) Finalmente, se asocia el Tenant creado al dominio del cliente. Seleccionar el cliente específico en la lista de dominios e ingresar en “Assign Tenant”. Seleccionar el Tenant correspondiente y Guardar.

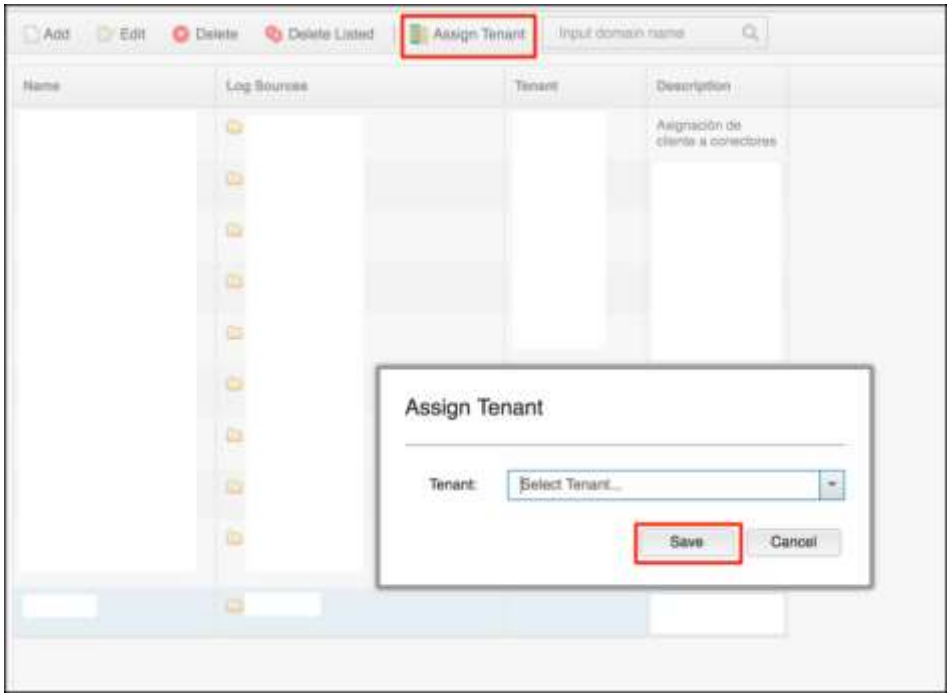


Ilustración 39: Ventana para asociar Tenant a Cliente

VII. Daily Scrum

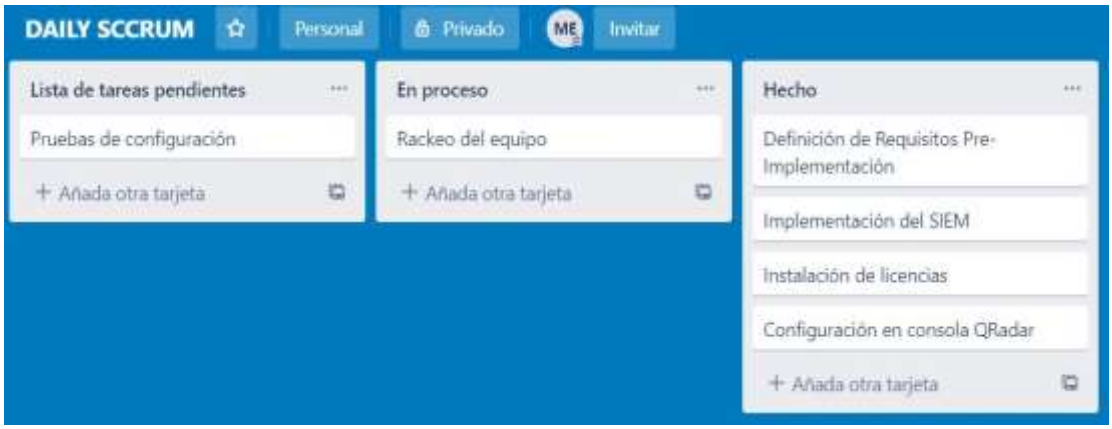


Ilustración 40: Daily Scrum 4 - Sprint 1
Fuente: *Elaboración Propia*

3.4.1.4 Rackeo del Equipo

Para realizar el rackeo correctamente y evitar lesiones personales o daños al equipo se tomó las siguientes consideraciones:

1) La instalación se realizó entre 2 personas con implementos adecuados de seguridad (Botas punta de acero, Cascos y guantes) y las herramientas para el rackeo (Destornillador, Tuercas y Tornillos).
2) Las personas se aseguraron de que el equipo de QRadar se coloque sobre una superficie estable antes de la instalación de montaje en rack.
3) Se revisó que el tipo de Rack que posee el cliente (debe ser un rack de comunicaciones).
4) Se colocó las cuatro tuercas de soporte en la unidad de Rack asignada, dejando un espacio de por medio.

Ilustración 41: Colocación de tuercas

5) Se Fijó los soportes de montaje del SIEM a los lados de la unidad con los tornillos suministrados. Los mangos deben estar alineados con la parte frontal de la unidad.

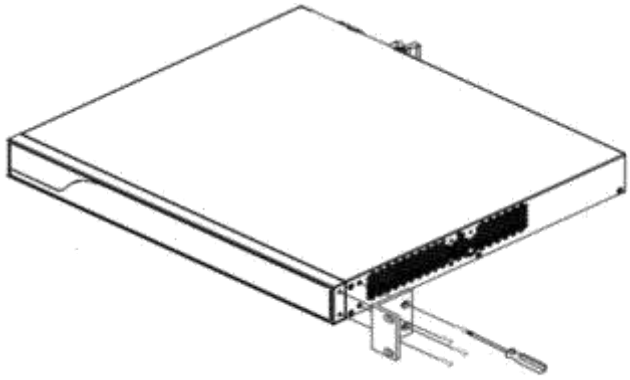


Ilustración 42: Soporte de montajes

6) Se colocó el equipo SIEM en el Rack. asegurándonos de que haya suficiente espacio en torno al equipo para permitir el flujo de aire suficiente.
7) Se alineó el equipo con los orificios del soporte en el rack y asegurándonos de que el equipo este nivelado.

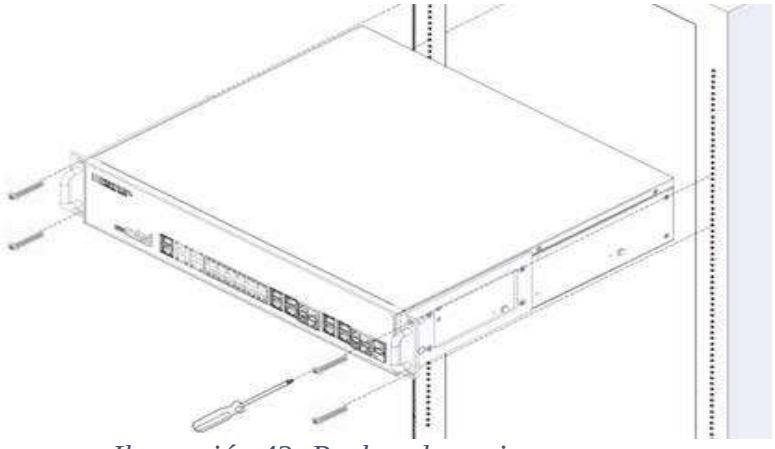


Ilustración 43: Rackeo de equipo

8) Se apretó los cuatro tornillos de montaje en rack para conectar la unidad.
9) Con el cable de alimentación suministrado, se conectó el cable en la parte trasera del equipo y luego a una toma eléctrica.

10) Se validó el tipo de conector de energía eléctrica que posee el Rack, los equipos SIEM de QRadar viene con el conector siguiente:

Ilustración 44: Conector de energía eléctrica

11) El equipo SIEM tiene una fuente de alimentación redundante, cada cable de alimentación se conectó a una fuente de alimentación diferente. De esta forma, si una fuente de poder falla, la otra puede seguir siendo operativa y el equipo no se apaga.

12) Se encendió la unidad con el interruptor "on" en la parte posterior del dispositivo.

3.4.1.5 Pruebas de Configuración del ECM

Se ejecutan los siguientes comandos para comprobar la correcta instalación de NRPE, SNMP y Firewall.

Antes de iniciar las pruebas, es necesario reiniciar el equipo.

1. **Qradar Deploy status**

   Loguearse en la consola Qradar, ir a la opción QDI y seleccionar el ECM a validar. El recuadro debe estar en color verde.

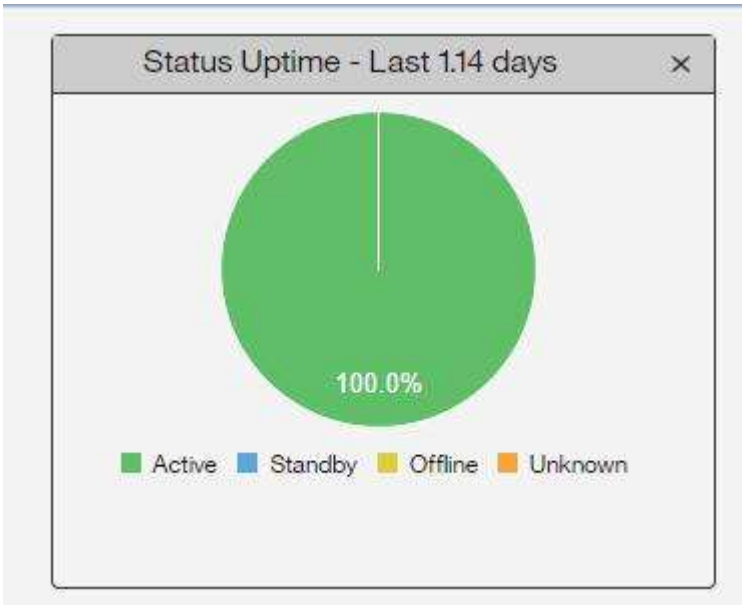


Ilustración 45: Estado del ECM

2. **Conectividad al iniciar ECM**

   Revisar que al iniciar el ECM, la interfaz de red levante automáticamente y se pueda generar conectividad hacia el ECM. Desde otra máquina generar ping al ECM.

3. **SNMP**

   Ejecutar el siguiente comando:

   snmpwalk -v 2c -c neo-cp <IP MAQUINA>

   Si el script funciona, se asume que está bien instalado.

4. **Firewall**

Se debe validar que exista la regla para el NAT de salida con la VPN, que esté permitido el ping y el acceso SSH.

Donde "X" → Octeto del site [187(TMX) | 186 (TIC)

] Donde "Y" → Octeto del cliente

En el archivo:

cat /opt/qradar/conf/iptables-nat.post

Debe existir la regla:

-A OUTPUT -p tcp -d 10.4.0.68 --dport 22 -j DNAT --to-destination 10.X.Y.68:22

En el archivo:

cat /opt/qradar/conf/iptables.pre

Debe existir la regla

-I INPUT -p tcp --dport 22 -j ACCEPT'

-A INPUT -p icmp --icmp-type 8 -s 10.187.Y.0/24 -j ACCEPT

-A INPUT -p icmp --icmp-type 0 -s 10.187.Y.0/24 -j ACCEPT

-A INPUT -p icmp --icmp-type 8 -s 10.186.Y.0/24 -j ACCEPT

-A INPUT -p icmp --icmp-type 0 -s 10.186.Y.0/24 -j ACCEPT

Validar que dichas reglas estén aplicadas en el iptables:

Iptables –nL –t nat

5. **Backup**

   Ejecutar los siguientes scripts en el ECM:

   /backup/backup-in-rcm-fisico.sh

   /backup/backup-in-rcm-virtual.sh

   De operar correctamente, se creará un archivo en la ruta /backup/ si el ecm es físico o /store/backup/ecm si el ecm es virtual con el siguiente nombre ***backup.HOSTNAME.FECHA.tar.gz***

6. **Llave SSH NAS**

   Validar que esté el archivo con llave de conexión desde el NAS. ***less /root/.ssh/authorized_keys***

7. **RSYNC**

   Validar que el RSYNC esté instalado.
   rsync

8. **TELNET**

   Validar que el TELNET esté instalado. ***telnet***

9. **TCPDUMP**

   Validar que el TCPDUMP esté instalado.

   Tcpdump

10. Editor de Texto

Validar que los editores de texto estén instalados.

Nano y luego vim

11. Traceroute

Validar que el TRACEROUTE esté

instalado. ***traceroute***

12. NTP

Validar que el NTP esté

instalado. ***ntpd***

13. Zona horaria

Validar que la hora y zona horaria esté configurada correctamente

Date

VIII. Daily Scrum

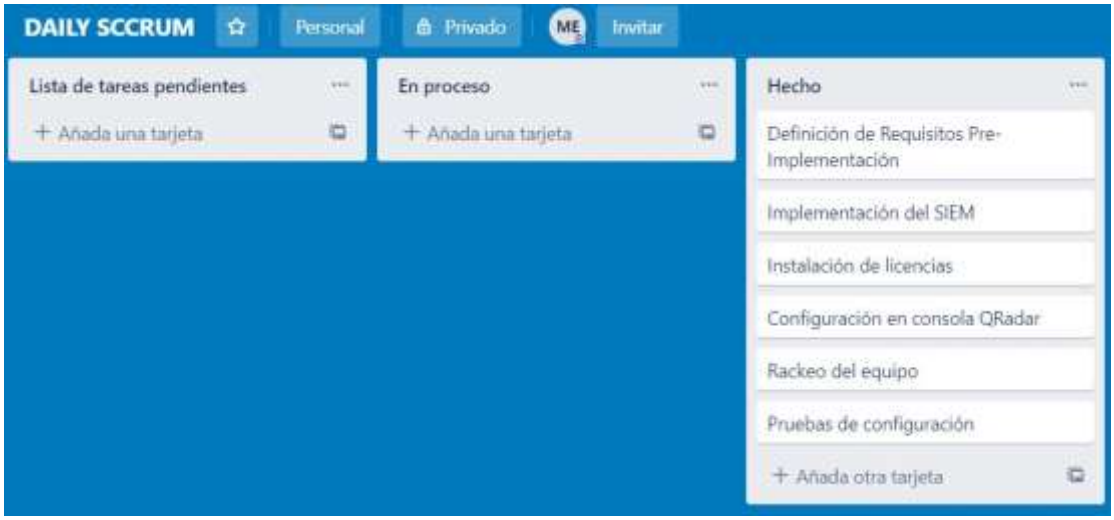


Ilustración 46: Daily Scrum 5 - Sprint 1

3.4.1.5.1 Informe de Prueba Funcional

PRUEBA FUNCIONAL			
PRUEBA N° 1	Prueba de Funcionalidad N° 1	**VERSIÓN DE**	PF-001
		FECHA	20/06/2019
TAREA	Implementación y Configuración del SIEM		
Descripción del caso de prueba	Se realizó las pruebas de configuración		
1. Caso de pruebas			
a. Precondiciones			
Reiniciar el equipo			
Contar con las credenciales			
b. Pasos de pruebas			
1. Qradar Deploy status			
2. Conectividad al iniciar ECM			
3. Conectividad SSH			
4. Validar SNMP			
5. Validar Firewall			
6. Validar Backup			
7. Validar Llave SSH NAS			
8. Validar RSYNC			
9. Validar TELNET			
10. Validar TCPDUMP			
11. Validar Editor de Texto			
12. Validar Traceroute			
13. Validar NTP			
14. Validar Zona horaria			

Datos de entrada			Respuesta esperada de la aplicación	Coincide		Respuesta del Sistema
Campo	Valor	Tipo Escenario		SI	NO	
.....	.....	.....	Status Uptime en verde			Status 100% activo
.....	.....	.....	Conectividad (PING) desde otra maquina hacia el SIEM			Conectividad correcta
.....	.....	.....	funcionalidad de SNMP			funcionalidad satisfactoria
.....	.....	.....	accesos ping y SSH permitidos			accesos satisfactorio
.....	.....	.....	ruta de backup existente			ruta creada
.....	.....	.....	Llave SSH de conexión desde el NAS			Conectividad correcta
.....	.....	.....	RSYNC instalado			RSYNC instalado
.....	.....	.....	TELNET instalado			TELNET instalado
.....	.....	.....	Editor de texto instalado			Editor de texto instalado
.....	.....	.....	Traceroute instalado			Traceroute instalado
.....	.....	.....	NTP instalado			NTP instalado
.....	.....	.....	Zona horaria correcta			Zona horaria correcta

Ilustración 47: Informe de Prueba Funcional

Fuente: *Elaboración Propia*

3.4.1.6 Revisión de Sprint – Semana 1

Nombre del Proyecto	Implementación de un Security Information and Event Management (SIEM) para mitigar vulnerabilidades y riesgos cibernéticos expuestas en las plataformas informáticas y redes de una entidad financiera	
Lugar	Entidad Financiera	
Fecha	20/06/2019	
Número de Sprint	N° 1	
Personas convocadas a la reunión	Jefe de proyecto	
	Líder del equipo	
	Analista de Seguridad I	
¿Qué salió bien en el Sprint? (aciertos)	**¿Qué no salió bien en el Sprint? (errores)**	**Lecciones aprendidas (Recomendaciones)**
Definición de Requisitos Pre-Implementación **Implementación del SIEM** **Instalación de licencias** **Configuración en consola Qradar** **Rackeo de equipo** **Pruebas de configuración**	El tiempo de ejecución de la cuarta historia de usuario tomo más tiempo de lo esperado, lo cual, genero un retraso en el avance de las siguientes historias pero al final del sprint se logró terminar en el tiempo estimado.	Se sugiere siempre mantener actualizado el Taskboard para mantener informado al equipo y el mismo debe ser divulgado a todos los involucrados para no generar retrasos o se malinterpreten las necesidades y prioridades del desarrollo.

Tabla 27: Revisión de Sprint S1

3.4.2 SPRINT 2: Integración de equipos SIEM

3.4.2.1 Planeamiento de Integración

I. Backlog

Historia de Usuario	Prioridad	Importancia	Tiempo Estimado
Definición de Requisitos Pre-Integración	Alta	3	2 días
Procedimiento de integración	Alta	4	19 días
Pruebas de recepción de syslog	Alta	5	19 días

Tabla 28: Backlog Sprint 2

II. Historia de Usuario

HISTORIA DE USUARIO	
ID: HU02	**NOMBRE HISTORIA:** Integración de equipos SIEM
Stakeholders: Jefe de proyecto, líder del equipo, equipo implementador y cliente	
Prioridad en el Negocio: Medio	**Importancia del Desarrollo:** 90
Tiempo Estimado: 45 días	**Modulo Asignado:** Administración
Descripción: Definición de Requisitos Pre-Integración Procedimiento de integración Pruebas de recepción de syslog	
Observaciones: Se debe tomar en cuentas las consideraciones pre-implementación.	

Ilustración 48: Historia de Usuario 02

III. TaskBoard

Sprint's	Historia de Usuario	Pendiente	En Curso	Hecho
SPRINT 1	Definición de Requisitos Pre-Implementación			✓
	Implementación del SIEM			✓
	Instalación de licencias			✓
	Configuración en consola QRadar			✓
	Rackeo del equipo			✓
	Pruebas de configuración			✓
SPRINT 2	Validaciones de recepción de paquetes de logsource	✓		
	Integración de activos al QRadar	✓		
	Pruebas de configuración	✓		
SPRINT 3	Configuración de 11 reglas	✓		
	Configuración de 03 reglas PCI	✓		
	Pruebas de alertas	✓		

Tabla 29: TaskBoard 02

IV. Daily Scrum 1

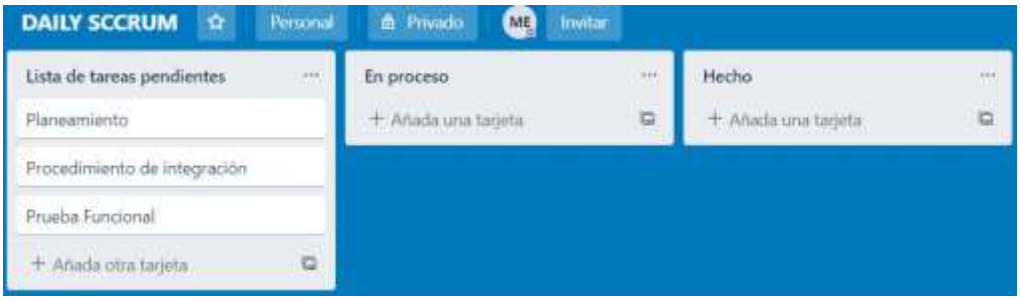


Ilustración 49: Daily Scrum 1 - Sprint 2
Fuente: *Elaboración Propia*

3.4.2.2.1 Definición de Requisitos Pre-Integración

Requisitos técnicos para el inicio de integración a producción

En la definición de las fuentes a integrar se considera que el log source tiene las siguientes características:

El log source está incluido en el listado de la guía de configuración DSM, disponible en el siguiente sitio web:

http://public.dhe.ibm.com/software/security/products/qradar/documents/iT

eam_addendum/b_dsm_guide.pdf

El log contiene los datos que se requieren y mensajes que permiten identificar las entradas y/o secuencias para el desarrollo de casos de uso, por ejemplo, códigos; para mayor información consulte el diccionario de datos del fabricante del log Source.

Lista de Log Source

En la siguiente tabla se muestran los dispositivos log source a integrar en IBM Security QRadar y la referencia al capítulo en donde se encuentran los requisitos y procedimientos sugeridos para la configuración de la fuente.

ÍTEM	CANTIDAD	TECNOLOGÍA	MARCA	MODELO
1	50	Checker ATM	GMV	Linux Kernel 2.6
1	3	Firewall (NGFW)	Cisco	Firepower 4120
2	1	Antiespam	Cisco	ESA-C390
3	2	Router	Cisco	Catalyst 9300-48T
4	1	Switch	Cisco	Nexus 7000
5	1	Router	Cisco	2900
6	2	Router	Cisco	4331
7	2	Controlador Wifi	Cisco	WLC_2504
9	1	Antivirus	McAfee	EPO
10	20	Servidor	Windows	Win 2012/2012 R2/2016
11	30	Servidor	Linux	Red Hat 5.8/6.5/ 6.8
12	11	Servidor	Solaris	Solaris 10 /11
	134	**TOTAL:**		

Ilustración 50: Lista de Log Source

V. Daily Scrum 2

Ilustración 51: Daily Scrum 2 - Sprint 2

3.4.2.2.2 Manual de procedimiento de configuración de equipos

Con este manual los administradores de los equipos y servidores podrán guiarse para realizar las configuraciones siguiendo los pasos de acuerdo con cada tecnología

A) Cisco Firepower Management Center

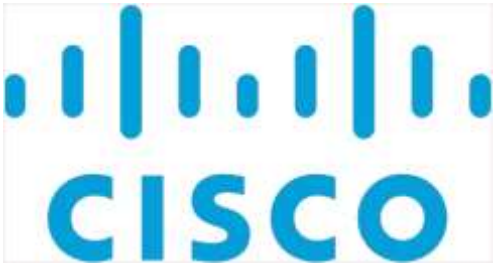


Ilustración 52: Logo Cisco

Se debe generar certificados en la interfaz Firepower y agregarlos en Qradar:

1. Inicie sesión en su interfaz de Cisco Firepower Management Center.

   a. Si está utilizando la versión 5.x, seleccione Sistema> Local> Registro.

   b. si. Si está utilizando la versión 6.x, seleccione Sistema> Integración.

2. Click en el botón eStreamer. 3. Seleccionar los tipos de eventos que desea que Cisco Firepower Management Center envíe a QRadar y luego haga clic en Guardar. La siguiente imagen enumera los tipos de eventos que Cisco Firepower Management Center envía a QRadar.

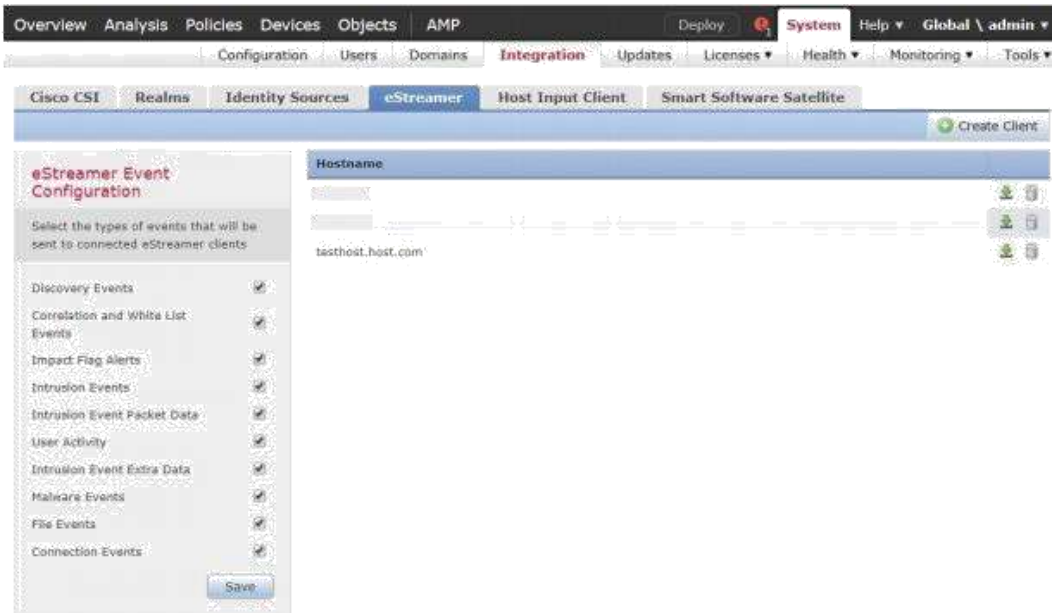


Ilustración 53: Cisco Firepower Management Center Event Configuration

4. Click en crear cliente en la parte superior derecha de la ventana.

5. En el Hostname field, tipear la IP o el nombre, dependiendo de cuál de las siguientes condiciones se aplica a sus entornos.

- Si usa una Consola QRadar o usa un dispositivo Todo en Uno QRadar para recopilar eventos de eStreamer, escriba la dirección IP o el nombre de host de su Consola QRadar.

- Si utiliza un QRadar Event Collector para recopilar eventos de eStreamer, escriba la dirección IP o el nombre de host del Event Collector.

- Si usa QRadar High Availability (HA), escriba la dirección IP virtual.6.

En el campo Contraseña, escriba una contraseña para su certificado. Si elige proporcionar una contraseña, se requiere la contraseña para importar el certificado.

7. Clic en Guardar. El nuevo cliente se agrega a la lista de clientes de eStreamer y el host puede comunicarse con la API de eStreamer en el puerto 8302.

8. Haga clic en Descargar certificado para su host para guardar el certificado pkcs12 en una ubicación de archivo.

9. Haga clic en Aceptar para descargar el archivo.

B) Cisco Catalyst

1. Inicie sesión en su interfaz de usuario de Cisco CatOS.

2. Escriba el siguiente comando para acceder al modo EXEC privilegiado: habilitar

3. Configure el sistema para los mensajes de marca de tiempo: establecer la marca de tiempo de registro habilitar

4. Escriba el siguiente comando con la dirección IP de IBM QRadar:

configurar el servidor de registro <dirección IP>

5. Limite los mensajes que se registran seleccionando un nivel de gravedad:

establecer la gravedad del servidor de registro <nivel de gravedad del servidor>

6. Configure el nivel de instalación que se utilizará en el mensaje. El valor predeterminado es local7.

establecer la instalación del servidor de registro <parámetro de la instalación del servidor>

7. Active el interruptor para enviar mensajes de syslog al QRadar. configurar el servidor de registro habilitar

C) Linux

Ilustración 54: Logo Linux

1. Ingresar al equipo Linux OS, como usuario root.
2. Editar el archivo /etc/syslog.conf.
3. Agregar la siguiente información: ***authpriv.* @{ ip del ecm}***
4. Guardar el archivo.
5. Reiniciar el proceso de syslog con el siguiente comando: ***service syslog restart***.

D) Windows

Ilustración 55: Logo Windows

Se deben tener las siguientes consideraciones:

Se debe contar con las credenciales de un usuario que pertenezca al grupo de “Lectores del registro de eventos”. Para agregar al usuario en el grupo requerido:

1. Ejecutar desde cmd el comando: ***lusrmgr.msc***
2. Click en “grupos”.
3. Click derecho en “Lectores del registro de eventos”. Click en “propiedades”.
4. Click en “agregar” y escoger el usuario.
5. Click en “Aplicar”.
6. Click en “Aceptar”.

✓ Habilitar la Opción “Administración remota de registro de eventos”, check en dominio y doméstica.

1. Dirigirse a “Panel de control”.
2. Click en “Sistema y seguridad”.
3. En el apartado de “Firewall de Windows” dar click en “Permitir un programa a través de Firewall de Windows”.
4. Check en “Administración remota de registro de eventos”,
5. Check en las columnas “Dominio” y “Doméstica/Trabajo”.
6. Click en “Aceptar”

✓ Validar que no existan reglas de bloqueo del Firewall entre el host y el WinCollect. (Validarlo con el administrador)

Se detalla en el Anexo 01 el manual de configuración de envío de syslog de las demás tecnologías que fueron integradas al SIEM.

3.4.2.2 Procedimiento de integración

QRadar SIEM puede descubrir automáticamente Log Sources en su implementación cuando envían mensajes solo de syslog a una dirección IP del Event Collector.

Nos dirigimos a la pestaña “Admin”, buszamos la zona de “Data Sources” y entramos a la opción “Log Sources”

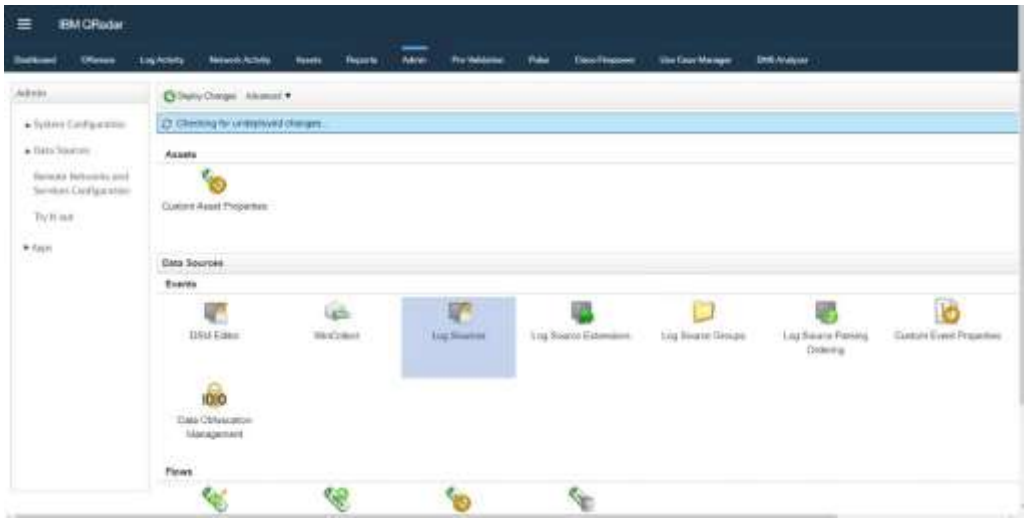


Ilustración 56: Configuración Log Source

1. Nos mostrará una ventana emergente donde se registran todos los logsource de acuerdo con el tipo de tecnología, para agregar un logsource hacemos clic en “Add”

Ilustración 57: Añadir Log Source

2. Nos mostrará la siguiente ventana, donde procederemos a registrar el logsource, de acuerdo con el manual de configuraciones de tecnologías a integrar en Qradar de IBM se completa los campos.

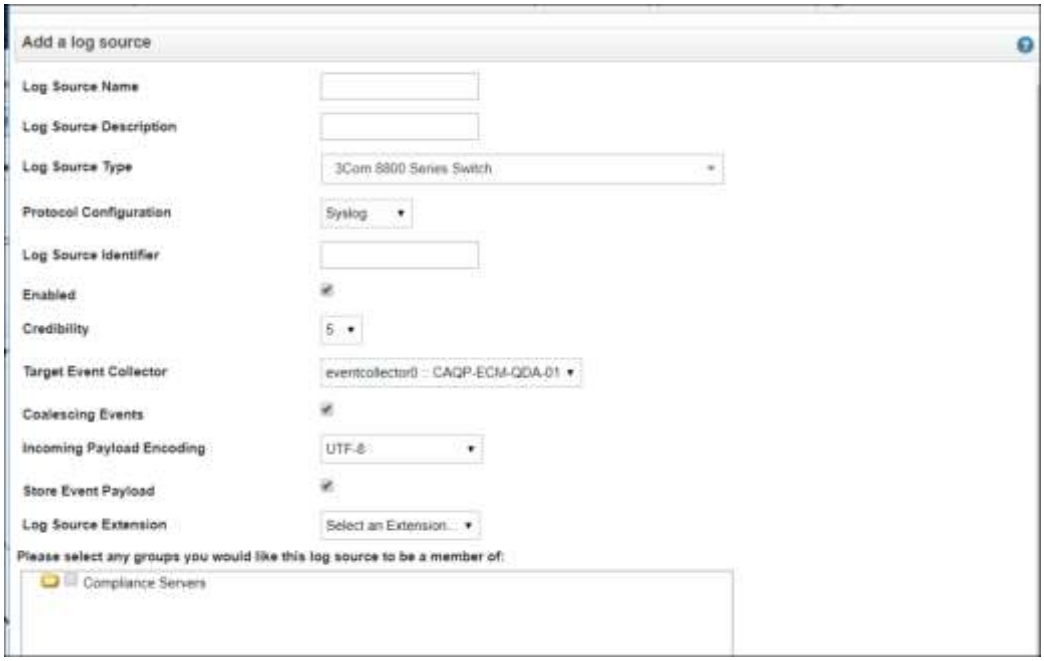


Ilustración 58: Configuración ventana Log Source

3. Una vez completados los campos, guardamos.

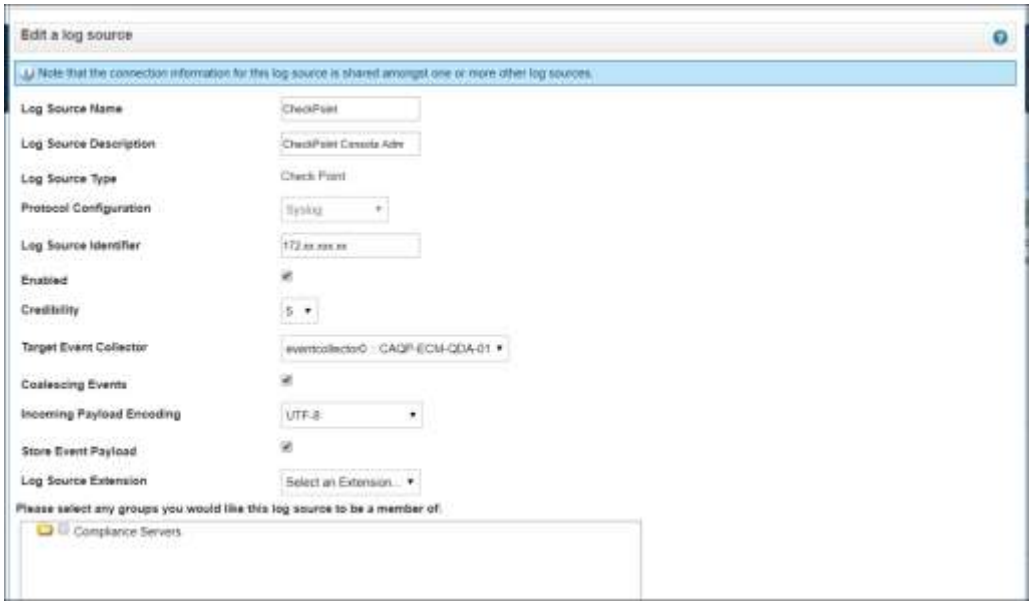


Ilustración 59: Configuración completada de Log Source

4. Seleccionamos el logsource y deshabilitamos y volvemos a habilitarlo.

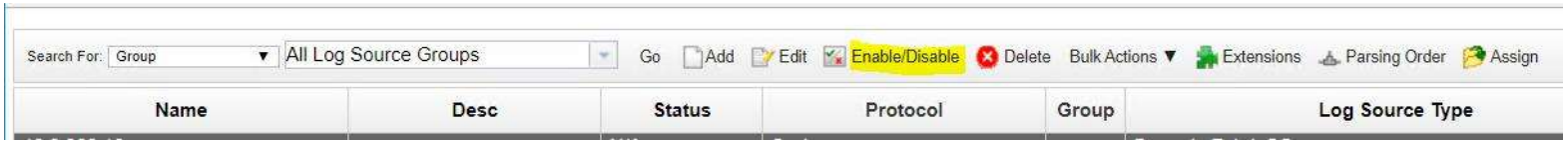


Ilustración 60: Habilitar Log Source

5. Cerramos la pestaña emergente, y nos dirigimos a la pestaña "admin" de la consola web y damos clic en "Deploy Changes" para implementar los cambios configurados.

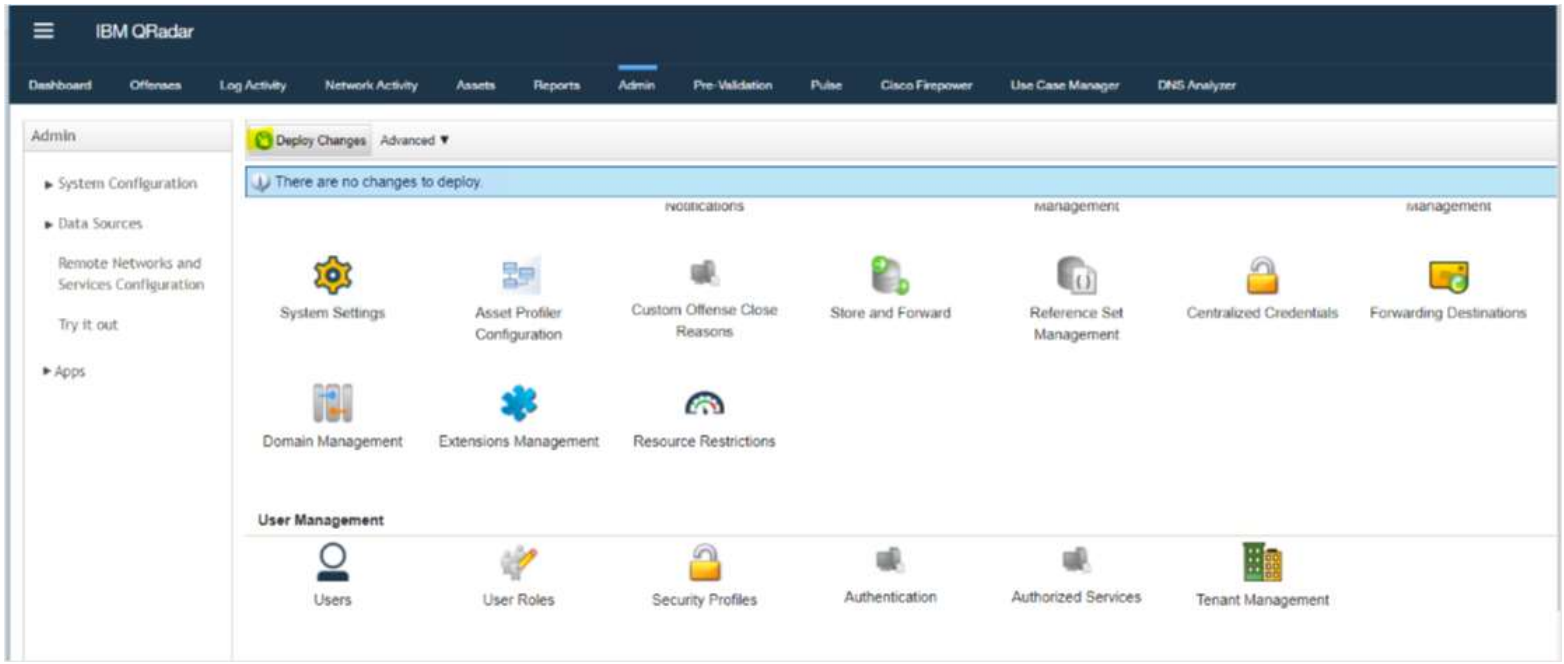


Ilustración 61: Deployar cambios

6. Nos dirigimos a la pestaña “Log Activity” para visualizar los eventos que recepciona el SIEM en tiempo real.

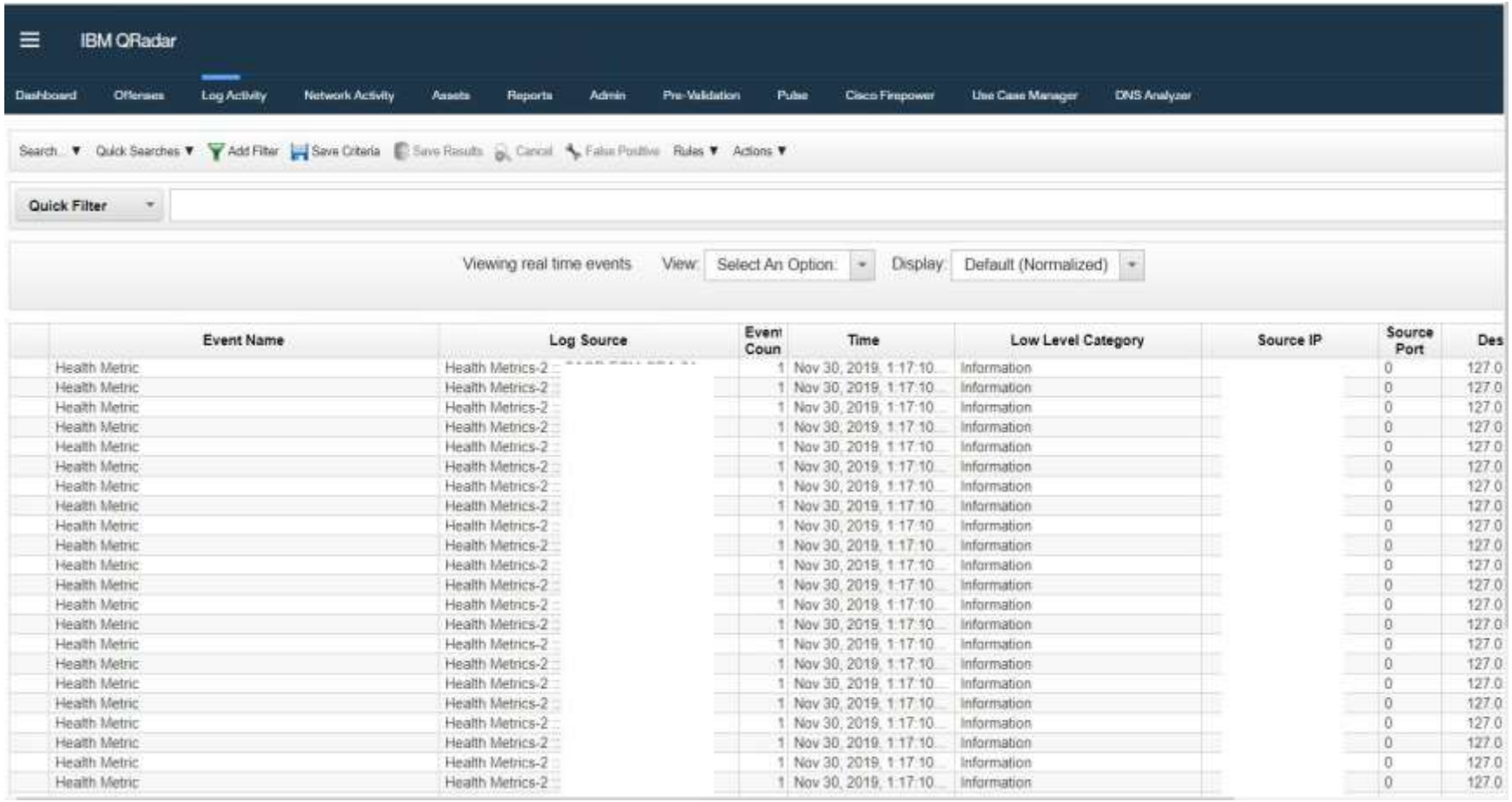


Ilustración 62: Sector Log Activity

3.4.2.3 Informe de Prueba Funcional

PRUEBA FUNCIONAL			
PRUEBA	Prueba de Funcionalidad N° 2	**VERSIÓN**	PF-002
		FECHA	15/07/2019
TAREA	Implementación y Configuración del SIEM		
Descripción del caso de prueba	Se realizó las pruebas de configuración		

1. Caso de pruebas						
a. Precondiciones						
Reiniciar el equipo						
Contar con las credenciales						
b. Pasos de pruebas						
1. Validación de recepción de syslog para Cisco Firepower 4120						
1. Validación de recepción de syslog para Cisco ESA-C390						
1. Validación de recepción de syslog para Cisco Catalyst 9300-48T						
1. Validación de recepción de syslog para Cisco Nexus 7000						
1. Validación de recepción de syslog para Cisco 2900						
1. Validación de recepción de syslog para Cisco 4331						
1. Validación de recepción de syslog para Cisco WLC_2504						
1. Validación de recepción de syslog para CheckPoint 5800						
1. Validación de recepción de syslog para McAfee EPO						
1. Validación de recepción de syslog para Windows 2012/2012 R2/2016						
1. Validación de recepción de syslog para Linux Red Hat 5.8/6.5/ 6.8						
1. Validación de recepción de syslog para Solaris 10 /11						

Datos de entrada			Respuesta esperada de la aplicación	Coincide		Respuesta del Sistema
Campo	Valor	Tipo Escenario		SI	NO	
----------	----------	CLI Y WEB	Recepción correcta de syslog de Cisco Firepower 4120	X		Recepción satisfactoria
----------	----------	CLI Y WEB	Recepción correcta de syslog de Cisco ESA-C390	X		Recepción satisfactoria
----------	----------	CLI Y WEB	Recepción correcta de syslog de Cisco Catalyst 9300-48T	X		Recepción satisfactoria
----------	----------	CLI Y WEB	Recepción correcta de syslog de Cisco Nexus 7000	X		Recepción satisfactoria
----------	----------	CLI Y WEB	Recepción correcta de syslog de Cisco 2900	X		Recepción satisfactoria
----------	----------	CLI Y WEB	Recepción correcta de syslog de Cisco 4331	X		Recepción satisfactoria
----------	----------	CLI Y WEB	Recepción correcta de syslog de Cisco WLC_2504	X		Recepción satisfactoria
----------	----------	CLI Y WEB	Recepción correcta de syslog de CheckPoint 5800	X		Recepción satisfactoria
----------	----------	CLI Y WEB	Recepción correcta de syslog de McAfee EPO	X		Recepción satisfactoria
----------	----------	CLI Y WEB	Recepción correcta de syslog de Windows	X		Recepción satisfactoria
----------	----------	CLI Y WEB	Recepción correcta de syslog de Linux	X		Recepción satisfactoria
----------	----------	CLI Y WEB	Recepción correcta de syslog de Solaris	X		Recepción satisfactoria

Ilustración 63: Informe de Prueba Funcional

VI. Daily Scrum

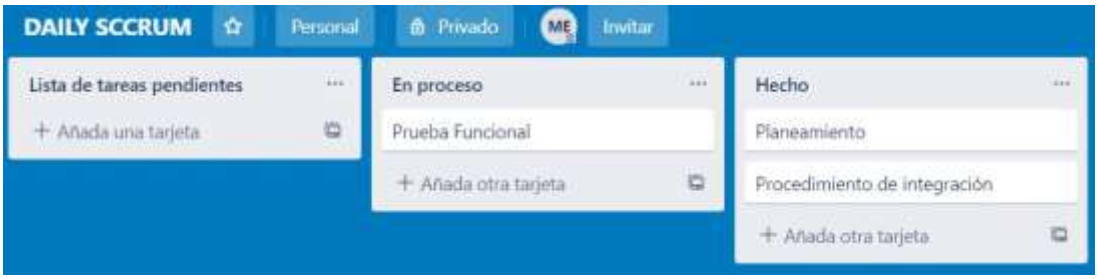


Ilustración 64: Daily Scrum 3 - Sprint 2

3.4.2.4 Revisión de Sprint – Semana 2

Nombre del Proyecto	Implementación de un Security Information and Event Management (SIEM) para mitigar vulnerabilidades y riesgos cibernéticos expuestas en las plataformas informáticas y redes de una entidad financiera	
Lugar	Entidad Financiera	
Fecha	26/06/2019	
Número de Sprint	N° 2	
Personas convocadas a la reunión	Jefe de proyecto	
	Líder del equipo	
	Analista de Seguridad I	
	Cliente	
¿Qué salió bien en el Sprint? (aciertos)	**¿Qué no salió bien en el Sprint? (errores)**	**Lecciones aprendidas (Recomendaciones)**
Definición de Requisitos Pre-Integración **Procedimiento de integración** **Pruebas de recepción de syslog**	El tiempo de ejecución de la segunda historia de usuario tomo más tiempo de lo esperado, lo cual, generó un retraso en el avance de las siguientes historias.	Se sugiere siempre mantener actualizado el Taskboard para mantener informado al equipo y el mismo debe ser divulgado a todos los involucrados para no generar retrasos o se malinterpreten las necesidades y prioridades del desarrollo.

Tabla 30: Revisión de Sprint S2

3.4.3 Configuración de Reglas

3.4.3.1 Planeamiento

I. TaskBoard

Sprint's	Historia de Usuario	Pendiente	En Curso	Hecho
SPRINT 1	Definición de Requisitos Pre-Implementación			✓
	Implementación del SIEM			✓
	Instalación de licencias			✓
	Configuración en consola QRadar			✓
	Rackeo del equipo			✓
	Pruebas de configuración			✓
SPRINT 2	Validaciones de recepción de paquetes de log Source			✓
	Integración de activos al QRadar			✓
	Pruebas de configuración			✓
SPRINT 3	Análisis de 11 reglas	✓		
	Configuración de 11 reglas	✓		
	Pruebas de alertas	✓		

Tabla 31: TaskBoard 2

VII. Daily Scrum

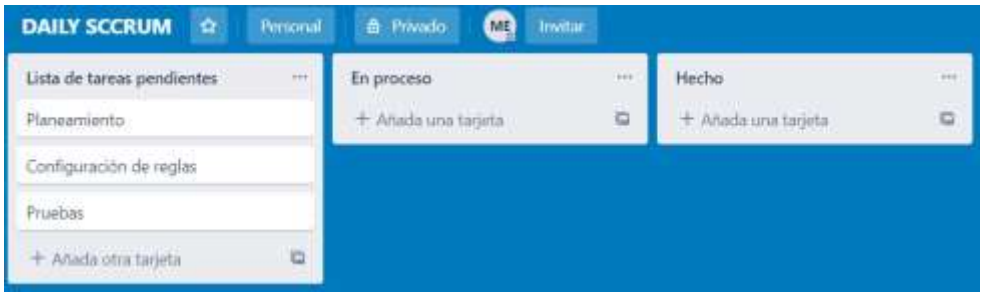


Ilustración 65: Daily Scrum 1 - Sprint 3
Fuente: *Elaboración Propia*

3.4.3.1.1 Definición de Requisitos Pre-Configuración

1. Para iniciar con la configuración de reglas primero se debe definir los casos de uso en una lista, en conjunto con el sponsor de acuerdo a las necesidades prioritarias que tengan.

ITEM	REPORTE	CASO DE USO	FUENTE
1	SI	Múltiples fallas de inicio de sesión en el mismo destino	Servidores
2	SI	Cargar ISO2700 Bulding Blocks	Equipos
3	SI	Correo electrónico que contiene archivos confidenciales enviados a un host potencialmente hostil.	Equipos
4	SI	Detectar ataques DDoS	Firewall
5	SI	Fuente de ataque de múltiples vectores	Servidores
6	SI	Denegaciones excesivas en el firewall desde un local host	Firewall
7	SI	Limpieza fallida de Malware o Virus	Equipos
8	SI	Usuario de alto privilegio que realiza acciones sospechosas	Servidores
9	SI	Informa un inicio de sesión exitoso en un host después de que se haya realizado el reconocimiento en la red	Servidores
10	SI	Fuente vulnerable a cualquier exploit	Servidores
11	SI	Comportamiento de Ransomware de los registros de eventos de seguridad de Microsoft Windows	Servidores

Tabla 32: Pre Requisitos de Configuración

3.4.3.2 Configuración de reglas

Las reglas, a veces llamadas reglas de correlación, se aplican a eventos, flujos u ofensas para buscar o detectar anomalías. Si se cumplen todas las condiciones de una prueba, la regla genera respuesta.

Las reglas personalizadas prueban eventos, flujos y delitos para detectar actividades inusuales en la red. Se puede crear nuevas reglas utilizando combinaciones AND y OR de pruebas de reglas existentes. Las reglas de detección de anomalías prueban los resultados de búsquedas guardadas de flujo o eventos para detectar cuándo ocurren patrones de tráfico inusuales en su red. Las reglas de detección de anomalías requieren una búsqueda guardada que se agrupa alrededor de un parámetro común.

Las reglas recopilan eventos de fuentes locales y remotas, normalizan esto normalizan estos eventos y los clasifican en categorías de bajo y alto nivel.

El motor de reglas (CRE) procesa eventos y los compara con reglas definidas para buscar anomalías. Cuando se cumple una condición de regla, el procesador de eventos genera una acción que se define en la respuesta de la regla. La CRE rastrea los sistemas que están involucrados en incidentes, contribuye eventos a ofensas y genera notificaciones.

QRadar crea un delito cuando los eventos, los flujos o ambos cumplen con los criterios de prueba que se especifican en las reglas.

QRadar analiza la siguiente información:

- Eventos y flujos entrantes
- Información de activos
- Vulnerabilidades conocidas

La regla que creó el delito determina el tipo de delito.

El magistrado prioriza los delitos y asigna el valor de magnitud en función de varios factores,

incluyendo número de eventos, severidad, relevancia y credibilidad.

Bulding Blocks

Un bloque de construcción es una colección de pruebas que no dan como resultado una respuesta o una acción.

Un bloque de construcción agrupa las pruebas de uso común para construir una lógica compleja para que pueda reutilizarse en las reglas.

VIII. Daily Scrum

Ilustración 66: Daily Scrum 2 - Sprint 3

Fuente: *Elaboración Propia*

3.4.3.3.1 Procedimiento de creación de reglas

1. Para la configuración de reglas, nos ubicamos en la pestaña "Ofensas" de la plataforma y entramos al segmento "Reglas"

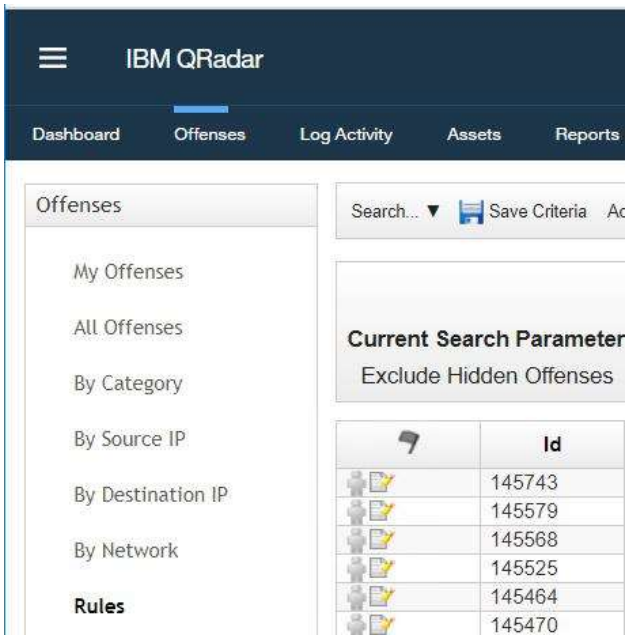


Ilustración 67: Pestaña reglas del SIEM

2. En la lista Acciones, seleccione un tipo de regla.

   Cada tipo de regla prueba contra datos entrantes de diferentes fuentes en tiempo real. Por ejemplo, evento

   las reglas prueban los datos de origen de registro entrantes y las reglas de delito prueban los parámetros de un delito para desencadenar.

   Por defecto el SIEM viene configurado más de 400 reglas que ayudan para identificar vulnerabilidades, comportamiento sospechoso de usuarios y amenazas de seguridad, de la cual se deben afinar de acuerdo al entorno de la entidad financiar.

3. En la página Editor de pila de prueba de reglas, en el panel Regla, escriba un nombre único al que desee asignar esta regla en el cuadro de texto Aplicar.
4. En el cuadro de lista, seleccionar Local o Global.
5. Si las pruebas de una regla coinciden, la regla genera las acciones y respuestas configuradas, como estos ejemplos:
    - Crear una ofensa
    - Agregar una anotación
    - Enviando un correo electrónico
    - Generando notificaciones del sistema que se muestran en el dashboard.

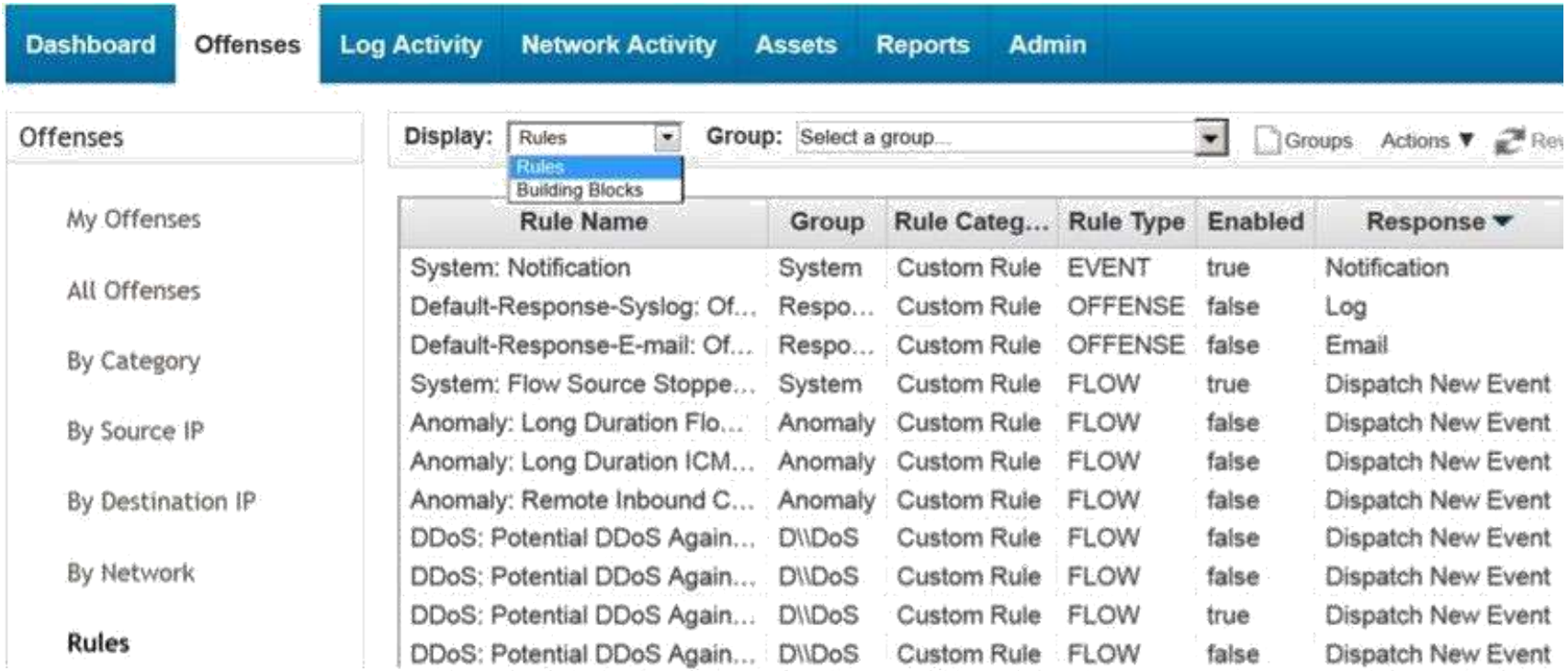


Ilustración 68: Lista de reglas predeterminadas

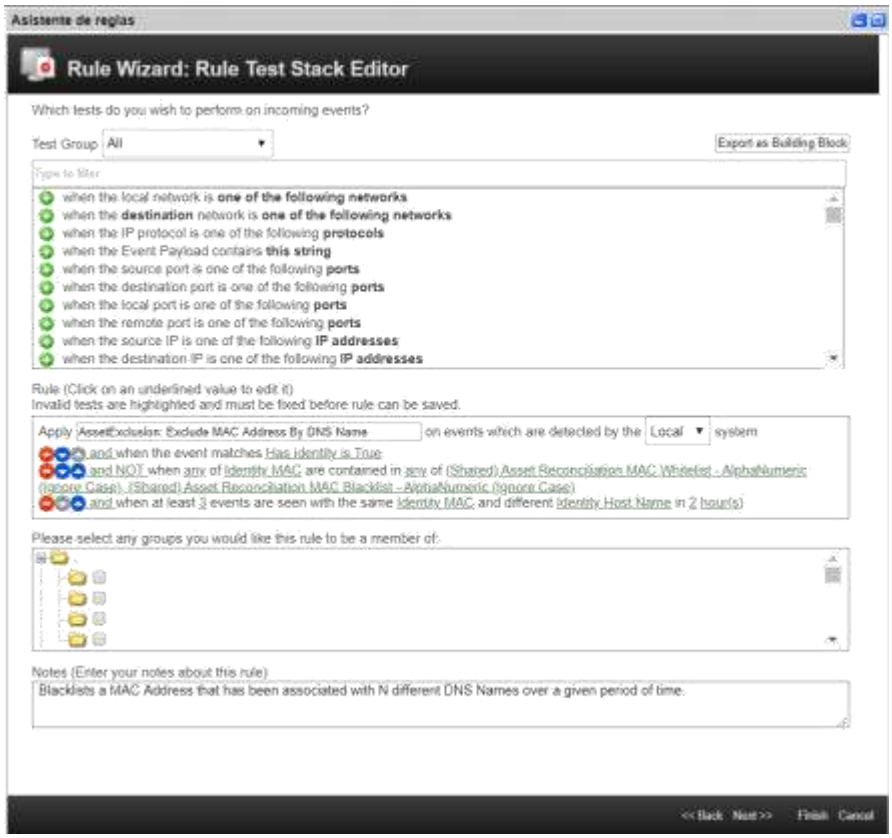


Ilustración 69: Asistente de regla

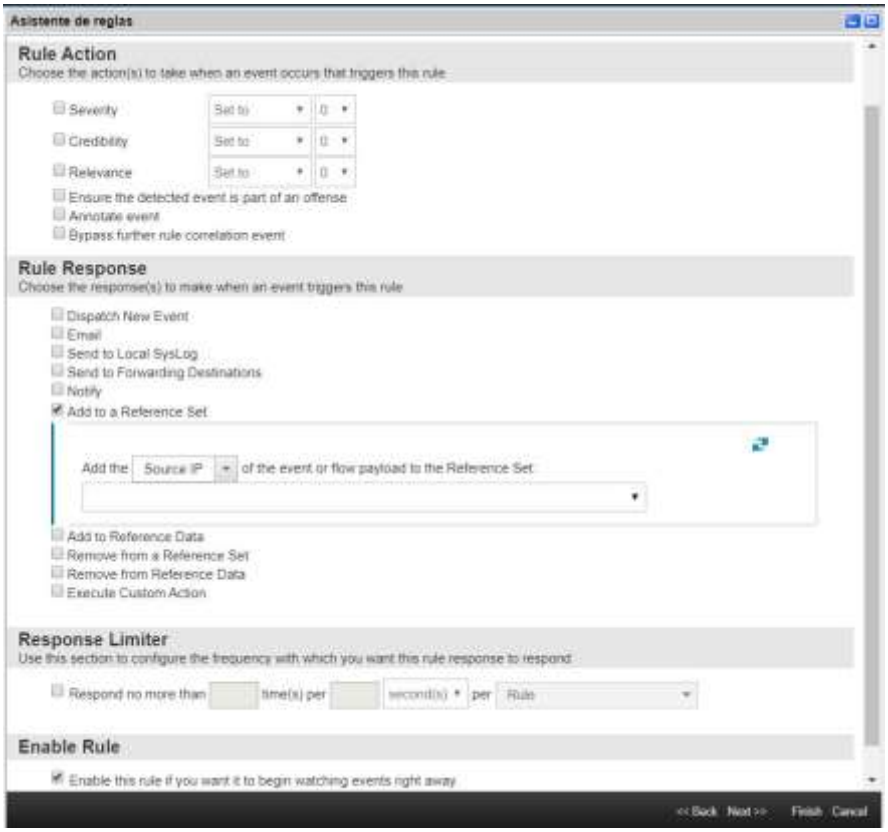


Ilustración 70: Configuración de acción de regla

3.4.3.3.2 Lista de reglas configuradas

Se detalla las 11 reglas que fueron configuradas.

1) Múltiples fallas de inicio de sesión en el mismo destino.

Informa cuando ocurre un evento de falla de autenticación al menos 10 veces en la misma dirección IP de destino desde una dirección IP y un nombre de usuario diferentes en 5 minutos.

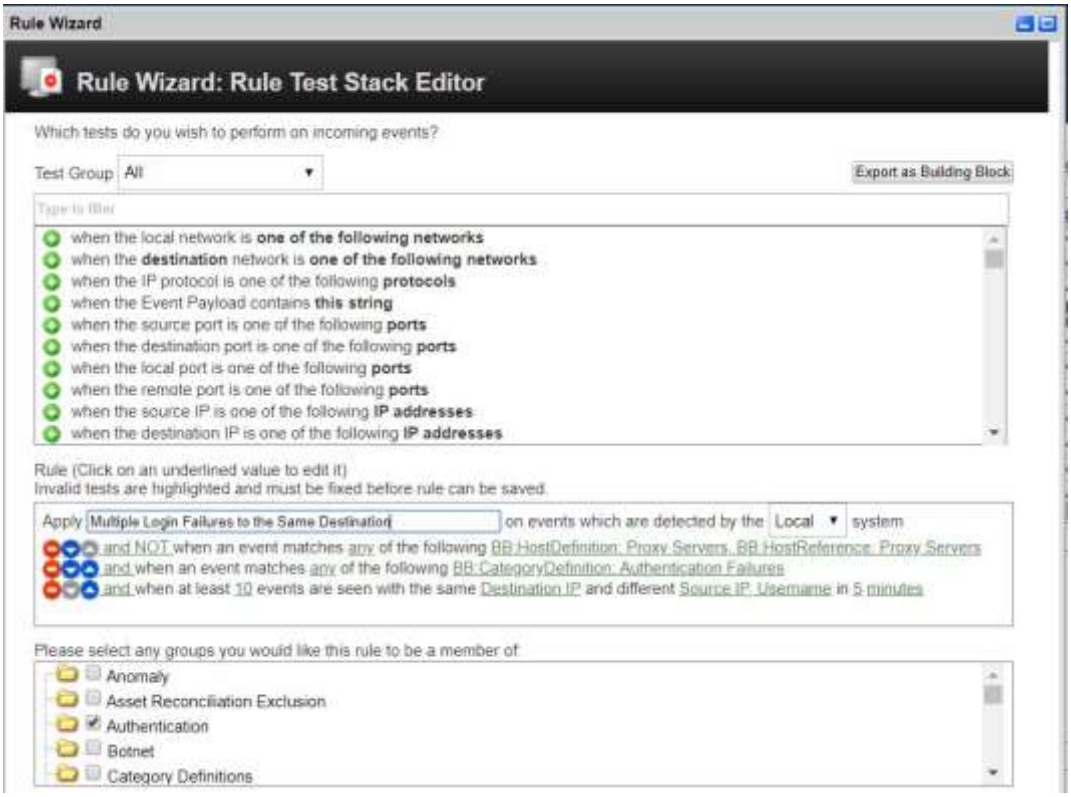


Ilustración 71: Reglas 1

2) Cargar ISO2700 Bulding Blocks

Esta regla carga los componentes básicos necesarios para completar los informes ISO 27001: 2013

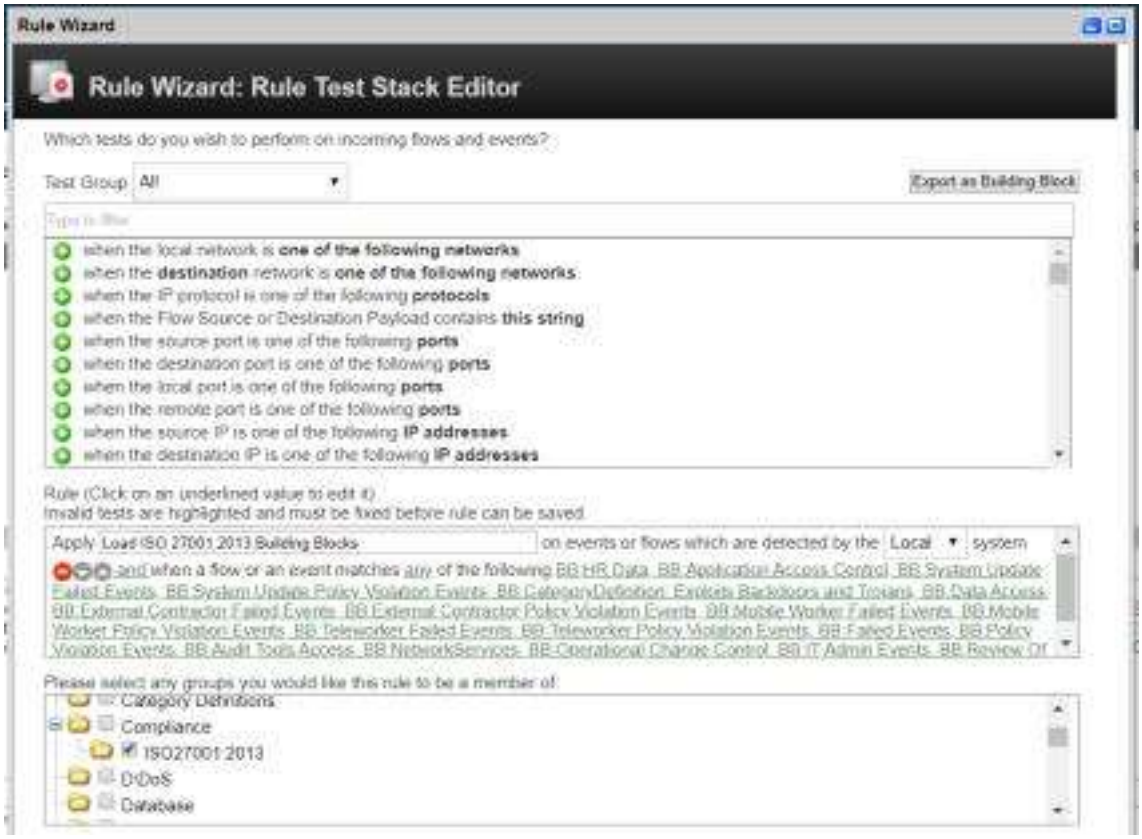


Ilustración 72: Reglas 2

3) Correo electrónico que contiene archivos confidenciales enviados a un host potencialmente hostil.

Esta regla se activa cuando se envía un correo electrónico que contiene un archivo confidencial a un host que es conocido por actividades hostiles, como phishing, spam, malware, botnet command and control, o cryptocurrency mining. El conjunto de referencia archivos en directorios confidenciales se completa con la regla archivos en directorios de archivos confidenciales.

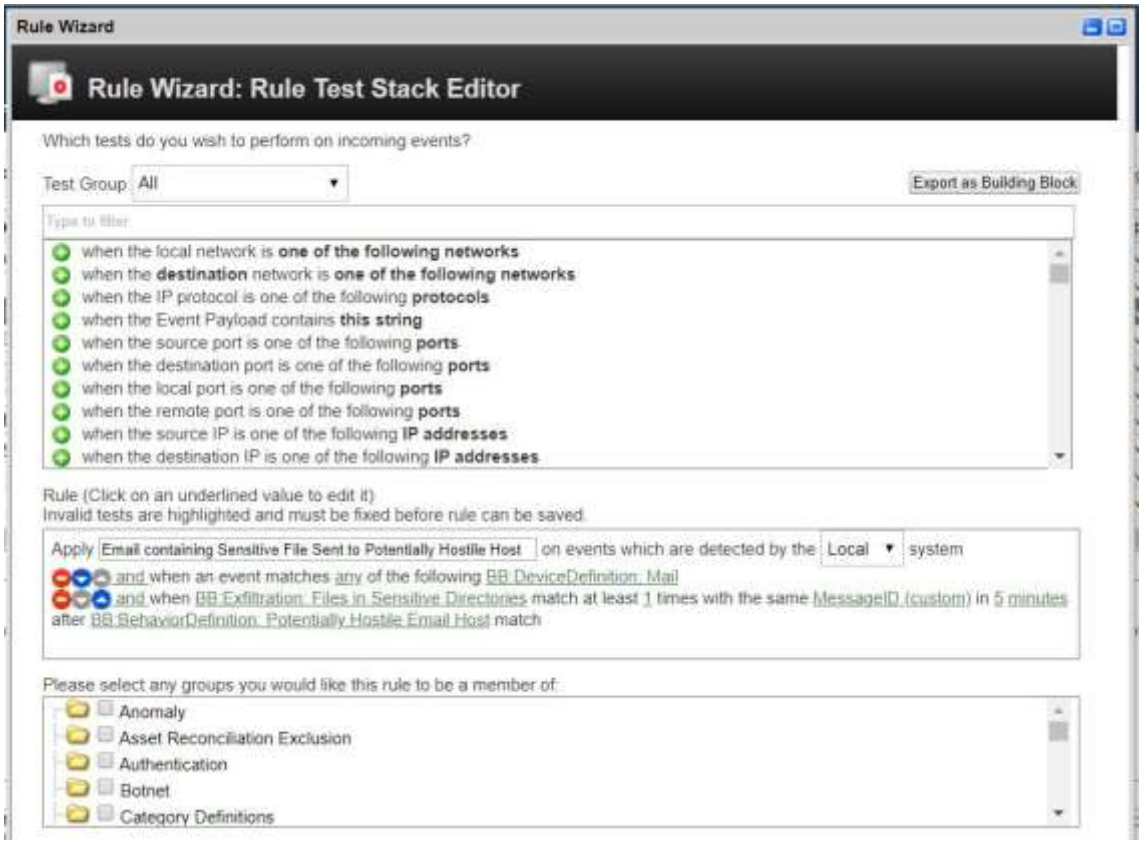


Ilustración 73: Reglas 3

4) Detectar ataques DDoS

Informa sobre ataques denegados del servicio (DoS) de red en un sistema.

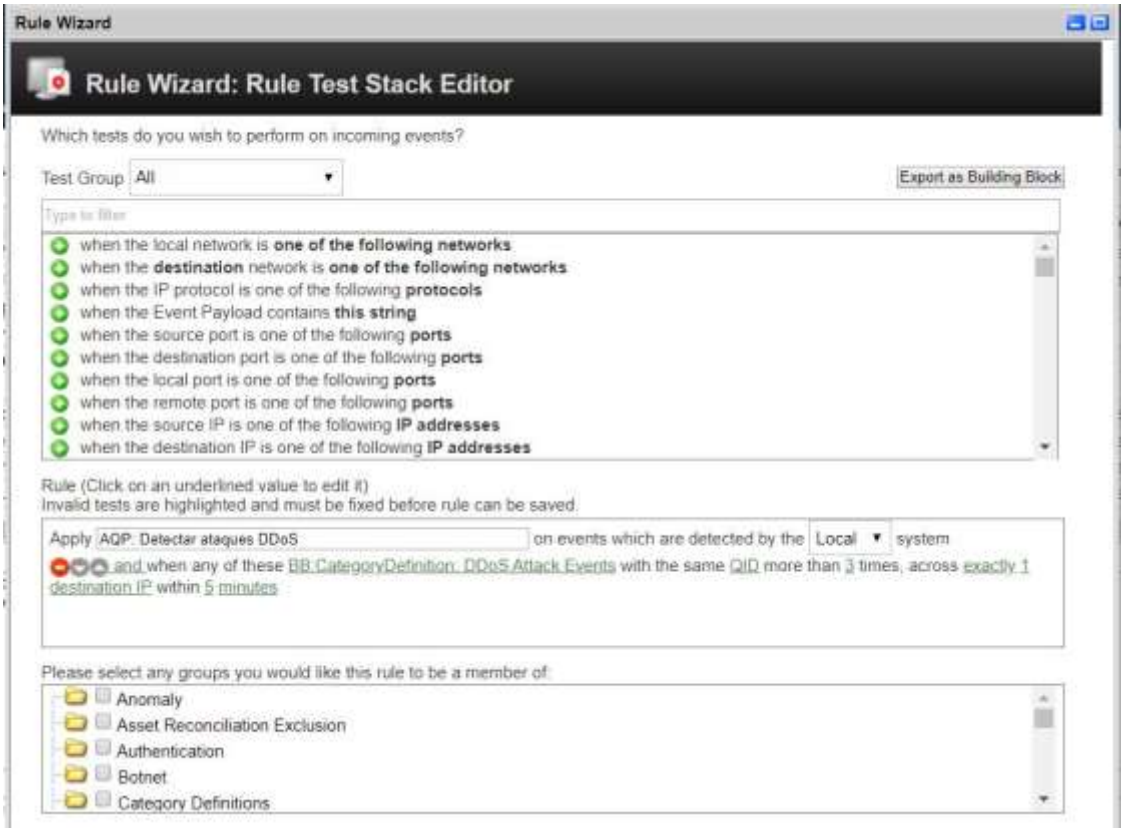


Ilustración 74: Reglas 4

5) Fuente de ataque de múltiples vectores

Esta regla detecta cuando un host de origen intenta múltiples vectores de ataque, esto puede indicar que el host de origen se dirige específicamente a un activo.

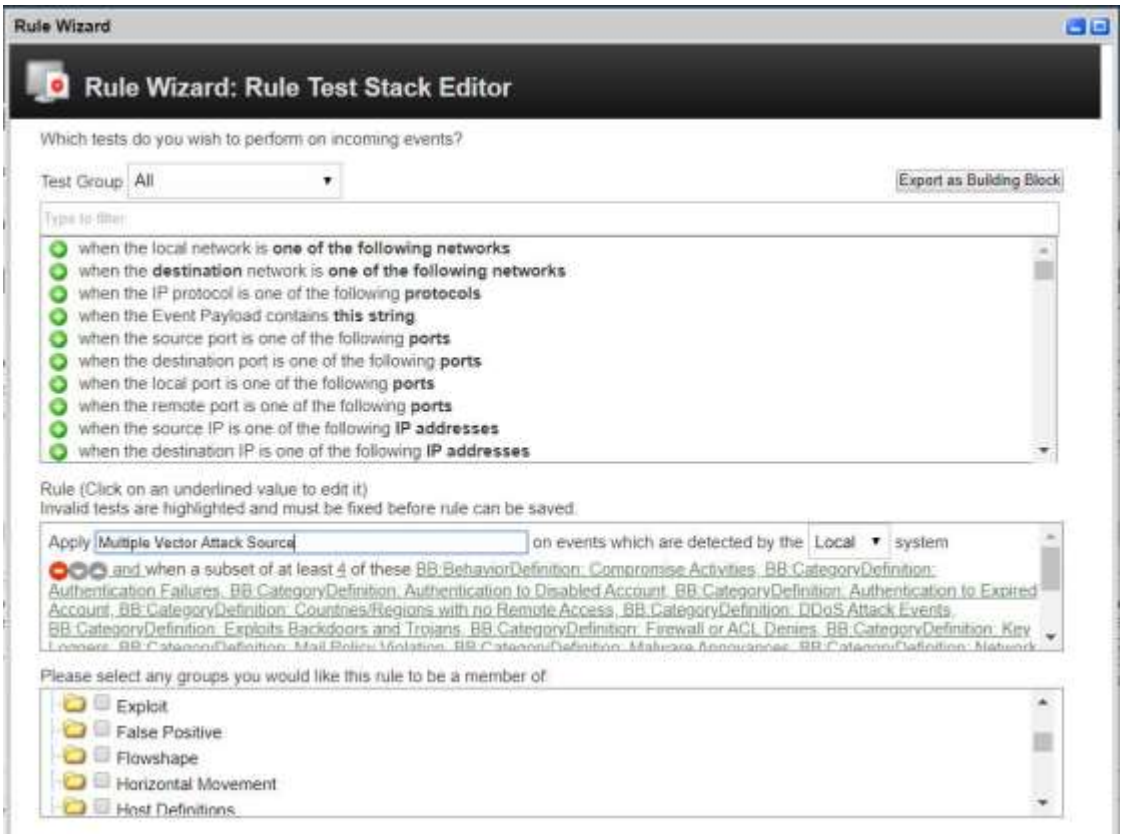


Ilustración 75: Reglas 5

6) Denegaciones excesivas en el firewall desde un localhost

Reporta intentos excesivos desde un host local, a través de múltiples hosts, para acceder al firewall y se deniega el acceso. Se detectan más de 40 intentos en al menos 40 direcciones IP de destino en 5 minutos.

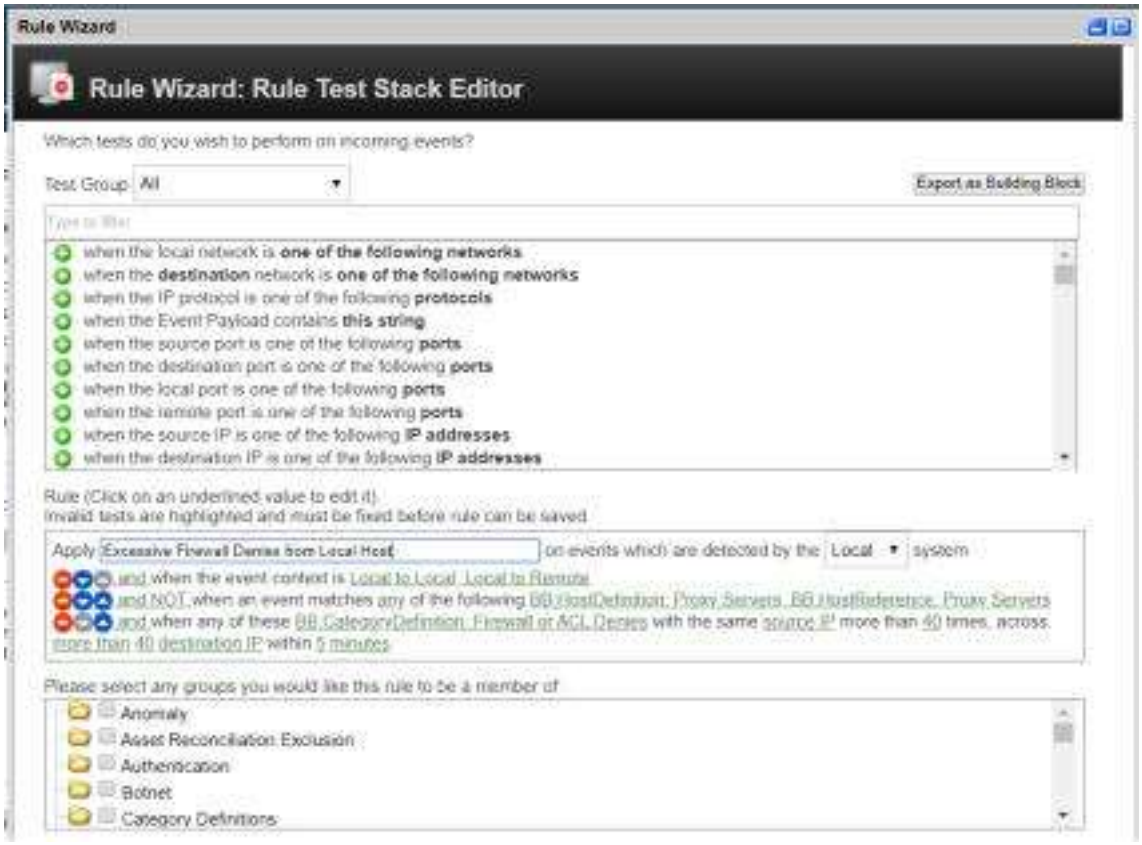


Ilustración 76: Reglas 6

7) Limpieza fallida de Malware o Virus

El sistema detectó un virus y no pudo limpiarlo o alejarlo

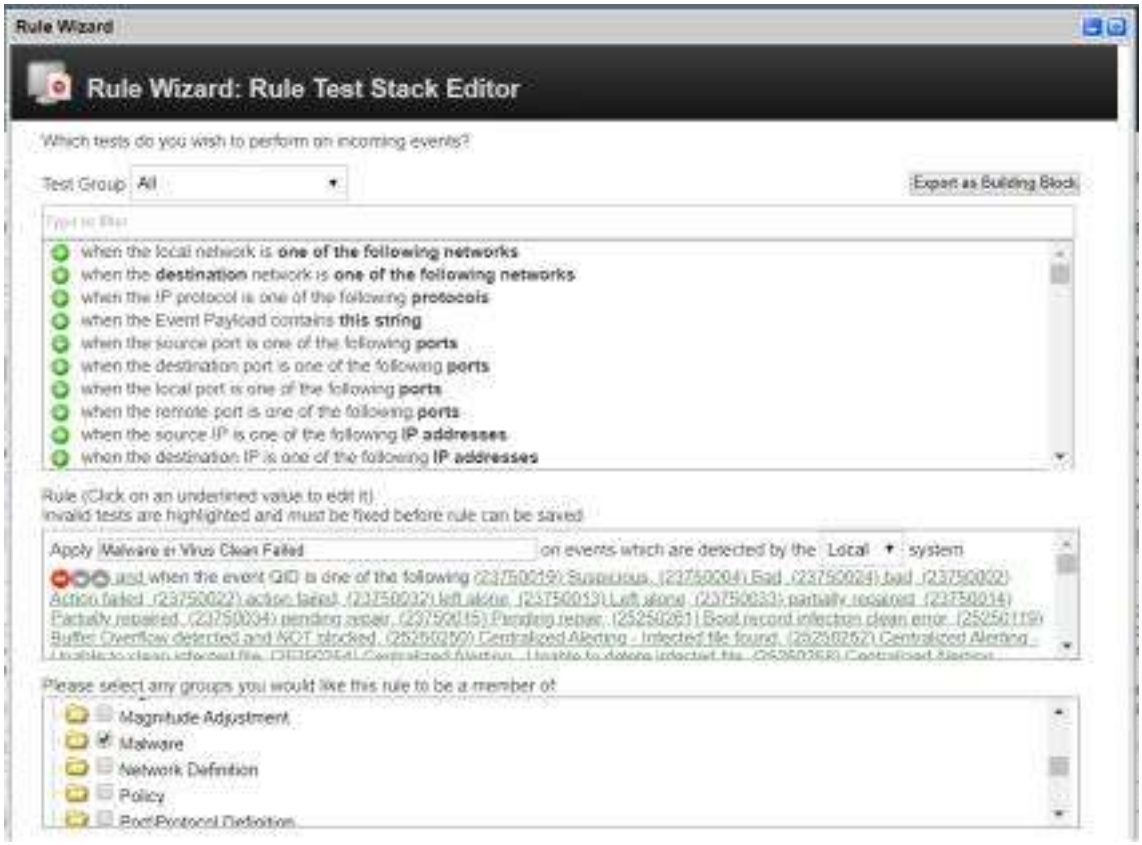


Ilustración 77:Reglas 7

8) Usuario de alto privilegio que realiza acciones sospechosas

Esta regla se activa cuando un rol de usuario cambia en un privilegio superior (por ejemplo, Administrador), seguido de actividades sospechosas. Esta acción puede indicar que un usuario cambia los permisos para realizar acciones maliciosas o accede a máquinas no autorizadas.

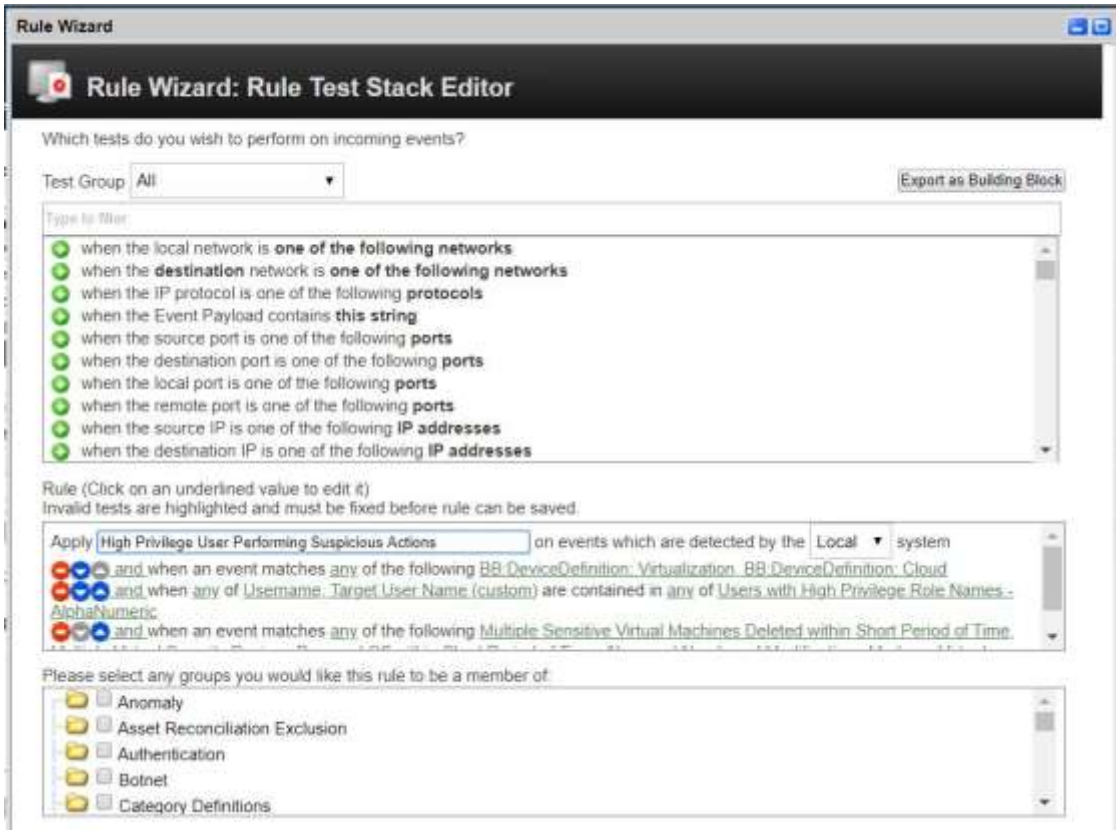


Ilustración 78: Reglas 8

9) Informa un inicio de sesión exitoso en un host después de que se haya realizado el reconocimiento en la red.

Informa un inicio de sesión exitoso en un host después de que se haya realizado el reconocimiento en la red.

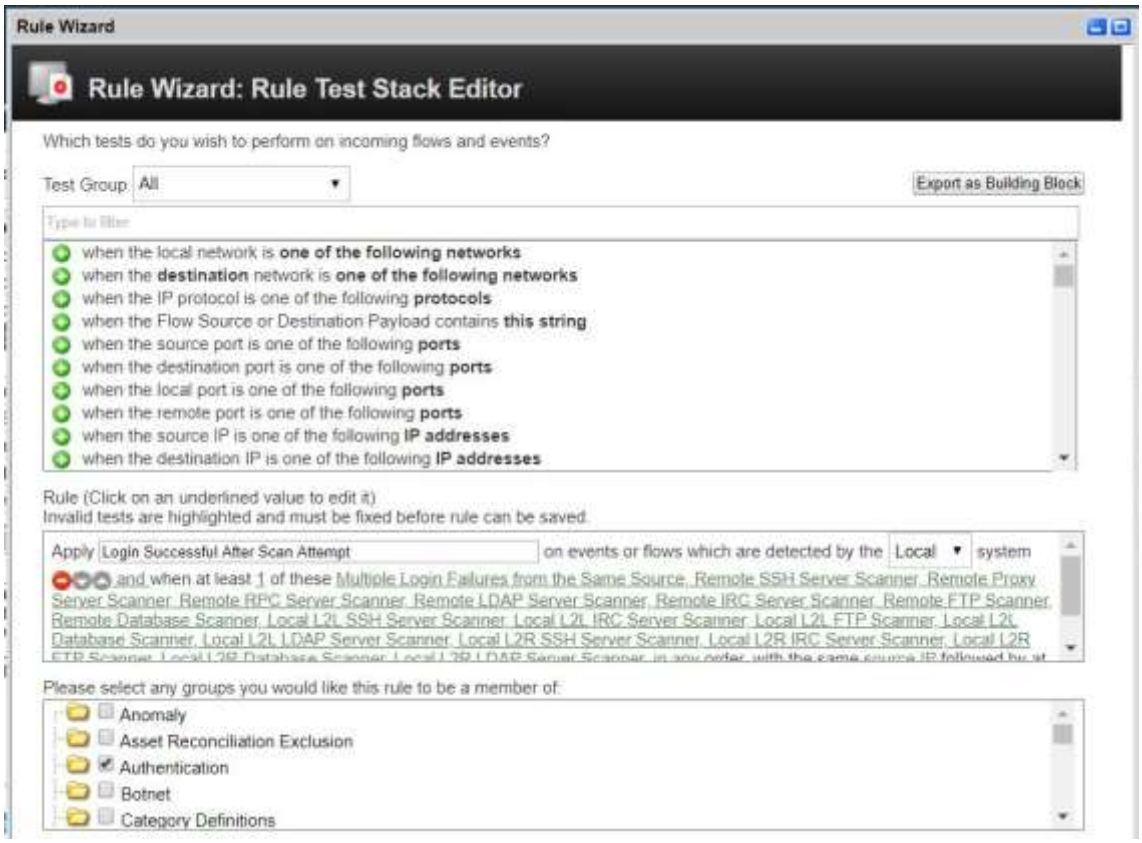


Ilustración 79: Reglas 9

10) Fuente vulnerable a cualquier exploit.

Informa un ataque desde un host local donde la fuente tiene al menos una vulnerabilidad. Es posible que la fuente haya sido atacada en un delito anterior.

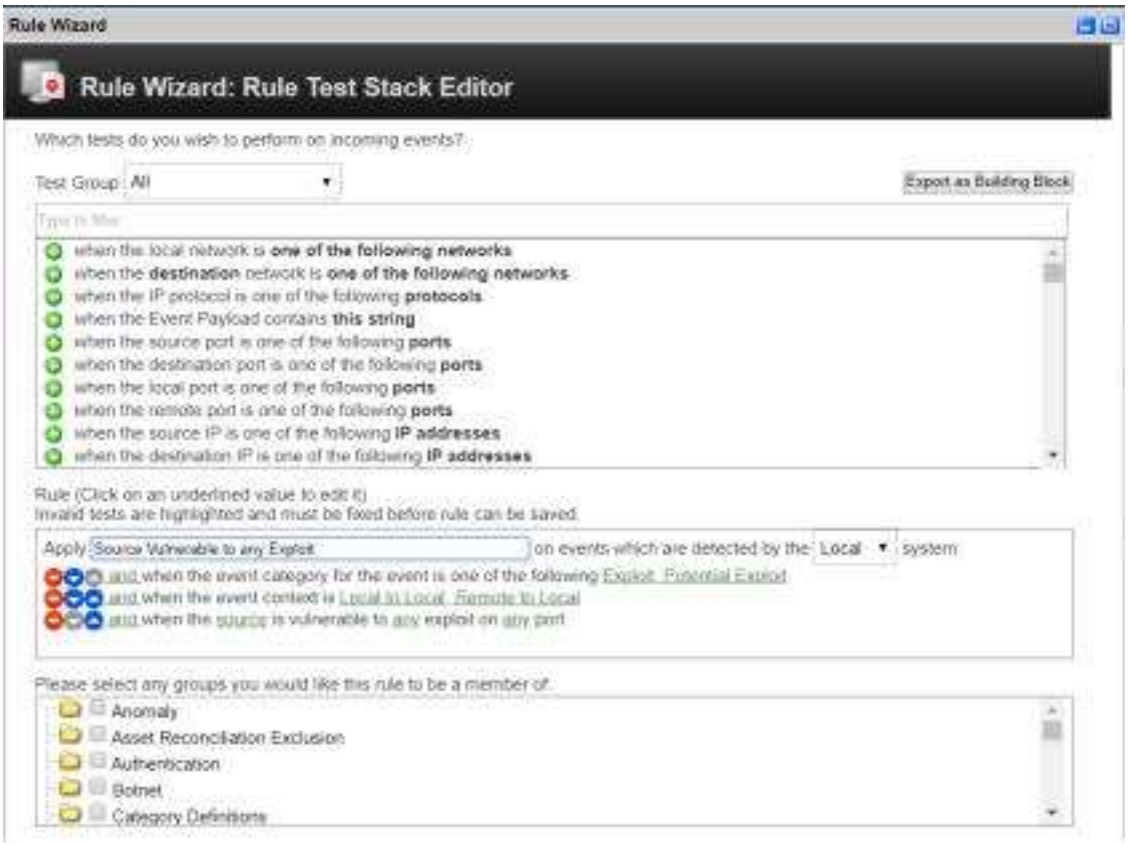


Ilustración 80: Reglas 10

11) Comportamiento de Ransomware de los registros de eventos de seguridad de Microsoft Windows

Esta regla se activa cuando los eventos de acceso / modificación de archivos que provienen del sistema Microsoft Windows se observan a una velocidad muy alta en un corto período de tiempo. La activación de esta regla indica un posible comportamiento de ransomware en el sistema

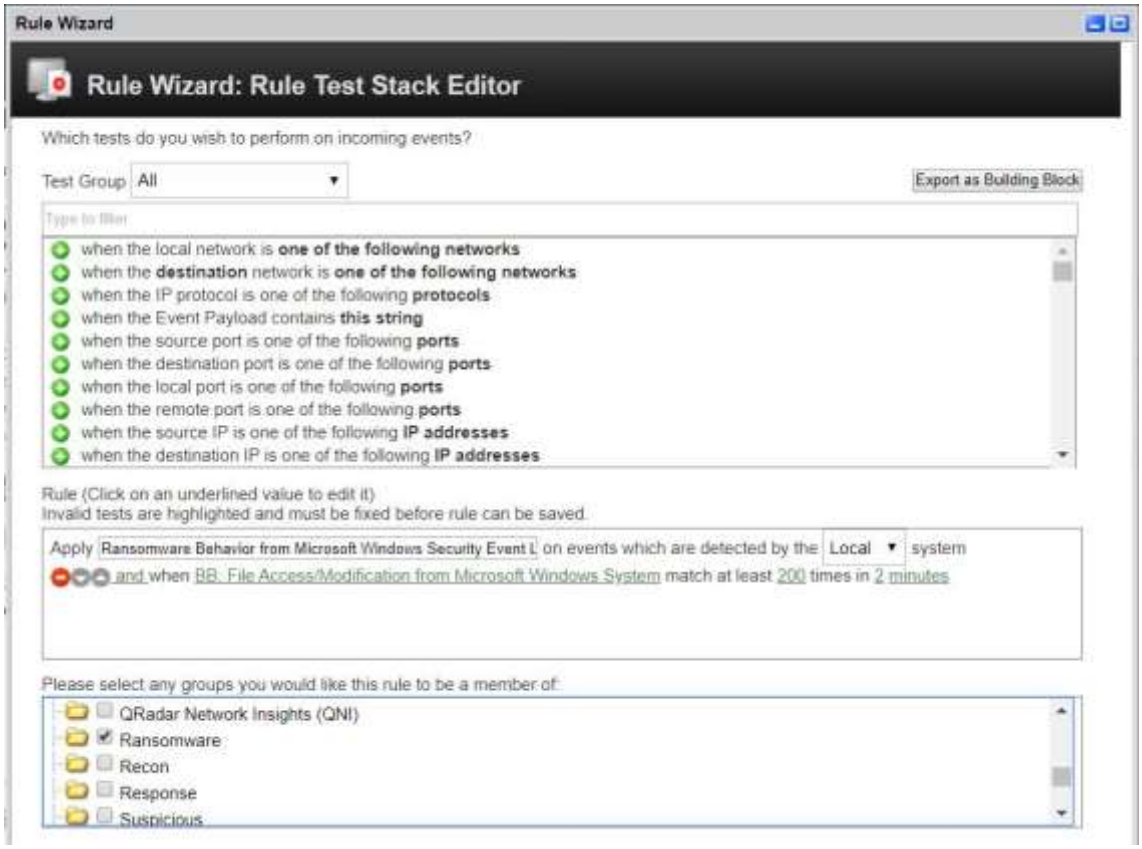


Ilustración 81: Reglas 11

3.4.3.3 Pruebas

PRUEBA FUNCIONAL					
PRUEBA	Prueba de Funcionalidad N° 3		**VERSIÓN**	PF-003	
			FECHA EJECUCIÓN	19/08/2019	
TAREA	Configuración de reglas				
Descripción del caso de prueba	Se realizó las pruebas de configuración				
1. Caso de pruebas					
a. Precondiciones					
Debe estar los equipos debidamente implementados					
b. Pasos de pruebas					
Generar ofensas para cada regla.					
Generar eventos de seguridad en los equipos					
Datos de entrada			**Respuesta esperada de la aplicación**	**Coincide**	**Respuesta del Sistema**
Campo	**Valor**	**Tipo Escenario**		**SI** / **NO**	
---	---	Consola Web	Las reglas deben generar las ofensas	X	Alerta y ofensa generada
---	---	Equipos integrados	Las reglas deben generar las ofensas	X	Alerta y ofensa generada

Tabla 33: Prueba de Funcionalidad 03

IX. Daily Scrum

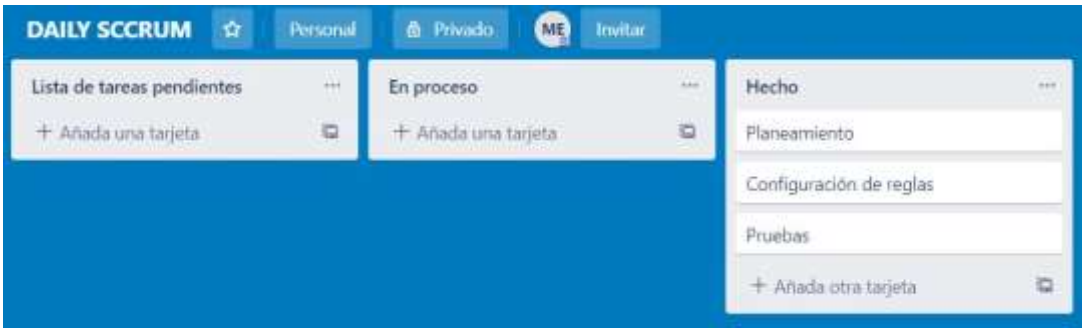


Ilustración 82: Daily Scrum 3 - Sprint 3
Fuente: *Elaboración Propia*

3.5 FASE MONITOREO Y CONTROL

3.5.1 Monitoreo de Eventos

El análisis realizado de los eventos genéricos de los logs Source en el SIEM, ayuda a que varios eventos puedan ser agrupados y analizados como uno solo, esto debido a que representan diferentes tipos de acciones que pueden llegar a generar un evento en común, cada evento maneja un ID único.

El modo de transmisión le permitirá ver los datos de eventos que ingresan a su sistema. Este modo te proporciona una vista en tiempo real de la actividad de su evento actual al mostrar los últimos 50 eventos.

La correlación de eventos permite diseñar alarmas que puedan aumentar el análisis del riesgo, esto debido a que al relacionar dos eventos se puede llegar a disminuir en gran medida los falsos positivos, como es el caso puntual de un login fallido, por si sólo no representa un riesgo alto a no ser que después de varios intentos fallido o de fuerza bruta se logre ingresar al sistema operativo, por lo que al realizar la correlación con un evento de login exitoso se asegura que hay un riesgo crítico.

Si aplica algún filtro en la pestaña Actividad de registro o en sus criterios de búsqueda antes de habilitar el modo de transmisión, Los filtros se mantienen en modo de transmisión.

Sin embargo, el modo de transmisión no admite búsquedas que incluyen eventos agrupados. Si habilita el modo de transmisión en eventos agrupados o criterios de

búsqueda agrupados, la pestaña Actividad de registro muestra los eventos normalizados.

Procedimiento

1. Haga clic en la pestaña Actividad de registro.

2. En el cuadro de lista Ver, seleccione Tiempo real (transmisión).

3. Opcional. Pausa o reproduce los eventos de transmisión. Elige una de las siguientes opciones:

• Para seleccionar un registro de evento, hacer clic en el icono "stop" para detener la transmisión.

• Para reiniciar el modo de transmisión, haga clic en el icono Reproducir.

La normalización implica analizar datos de eventos sin procesar y preparar los datos para mostrar información legible sobre la pestaña. Cuando los eventos se normalizan, el sistema también normaliza los nombres. Por lo tanto, el nombre que se muestra en la pestaña Actividad de registro podría no coincidir con el nombre que se muestra en el evento.

Con la pestaña Actividad de registro, puede ver los eventos agrupados por varias opciones de la lista de "Display" puede seleccionar el parámetro por el que desea agrupar eventos.

A continuación, se muestra los eventos de seguridad que llegan de las tecnologías integradas al SIEM en la pestaña **"Log Activity".**

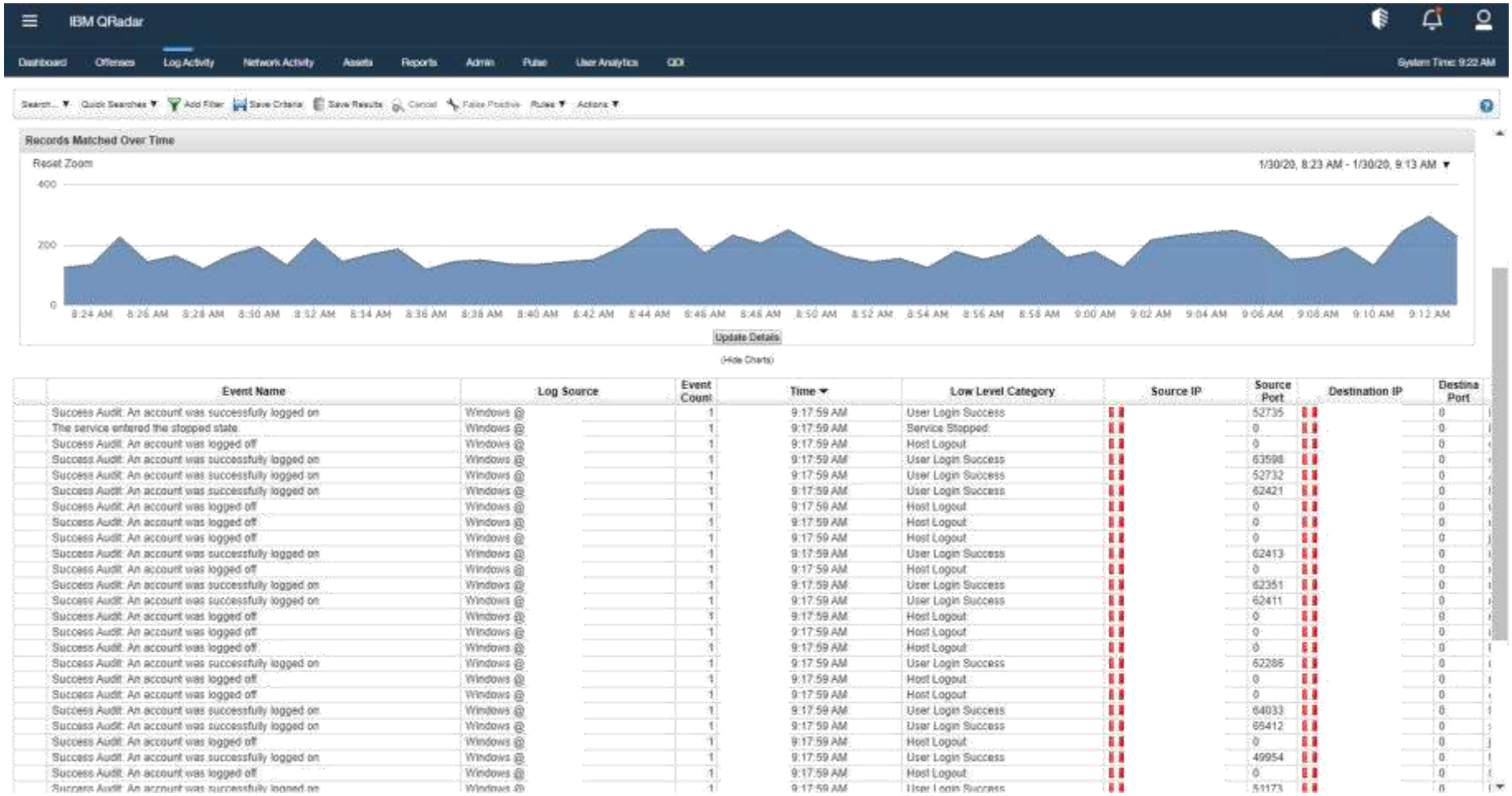
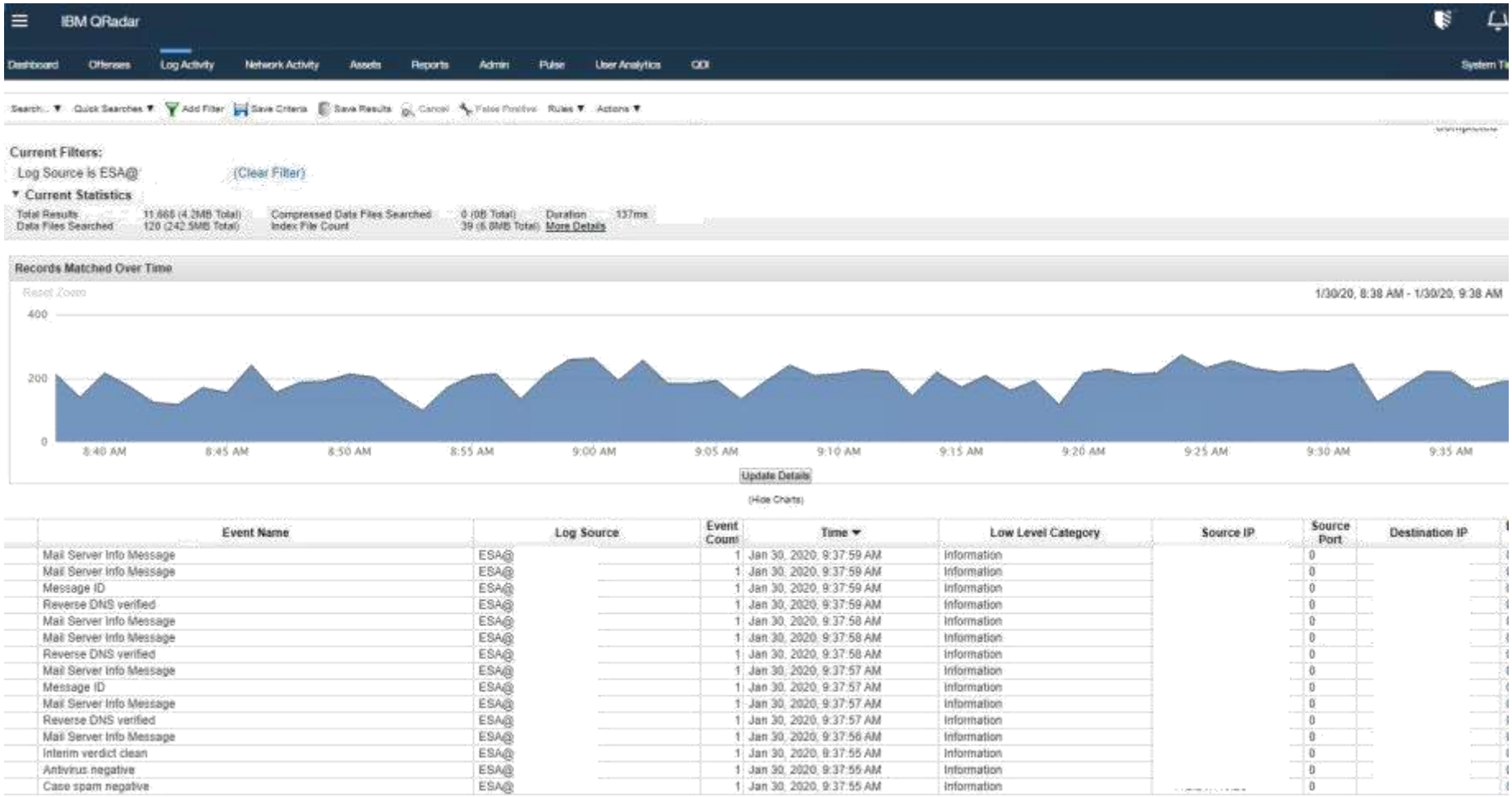


Ilustración 83: Log Activity



Event Name	Log Source	Event Coun	Time	Low Level Category	Source IP	Source Port	Destination IP
Mail Server Info Message	ESA@	1	Jan 30, 2020, 9:37:59 AM	Information		0	
Mail Server Info Message	ESA@	1	Jan 30, 2020, 9:37:59 AM	Information		0	
Message ID	ESA@	1	Jan 30, 2020, 9:37:59 AM	Information		0	
Reverse DNS verified	ESA@	1	Jan 30, 2020, 9:37:59 AM	Information		0	
Mail Server Info Message	ESA@	1	Jan 30, 2020, 9:37:58 AM	Information		0	
Mail Server Info Message	ESA@	1	Jan 30, 2020, 9:37:58 AM	Information		0	
Reverse DNS verified	ESA@	1	Jan 30, 2020, 9:37:58 AM	Information		0	
Mail Server Info Message	ESA@	1	Jan 30, 2020, 9:37:57 AM	Information		0	
Message ID	ESA@	1	Jan 30, 2020, 9:37:57 AM	Information		0	
Mail Server Info Message	ESA@	1	Jan 30, 2020, 9:37:57 AM	Information		0	
Reverse DNS verified	ESA@	1	Jan 30, 2020, 9:37:57 AM	Information		0	
Mail Server Info Message	ESA@	1	Jan 30, 2020, 9:37:56 AM	Information		0	
Interim verdict clean	ESA@	1	Jan 30, 2020, 9:37:55 AM	Information		0	
Antivirus negative	ESA@	1	Jan 30, 2020, 9:37:55 AM	Information		0	
Case spam negative	ESA@	1	Jan 30, 2020, 9:37:55 AM	Information		0	

Ilustración 84: Log Activity 1

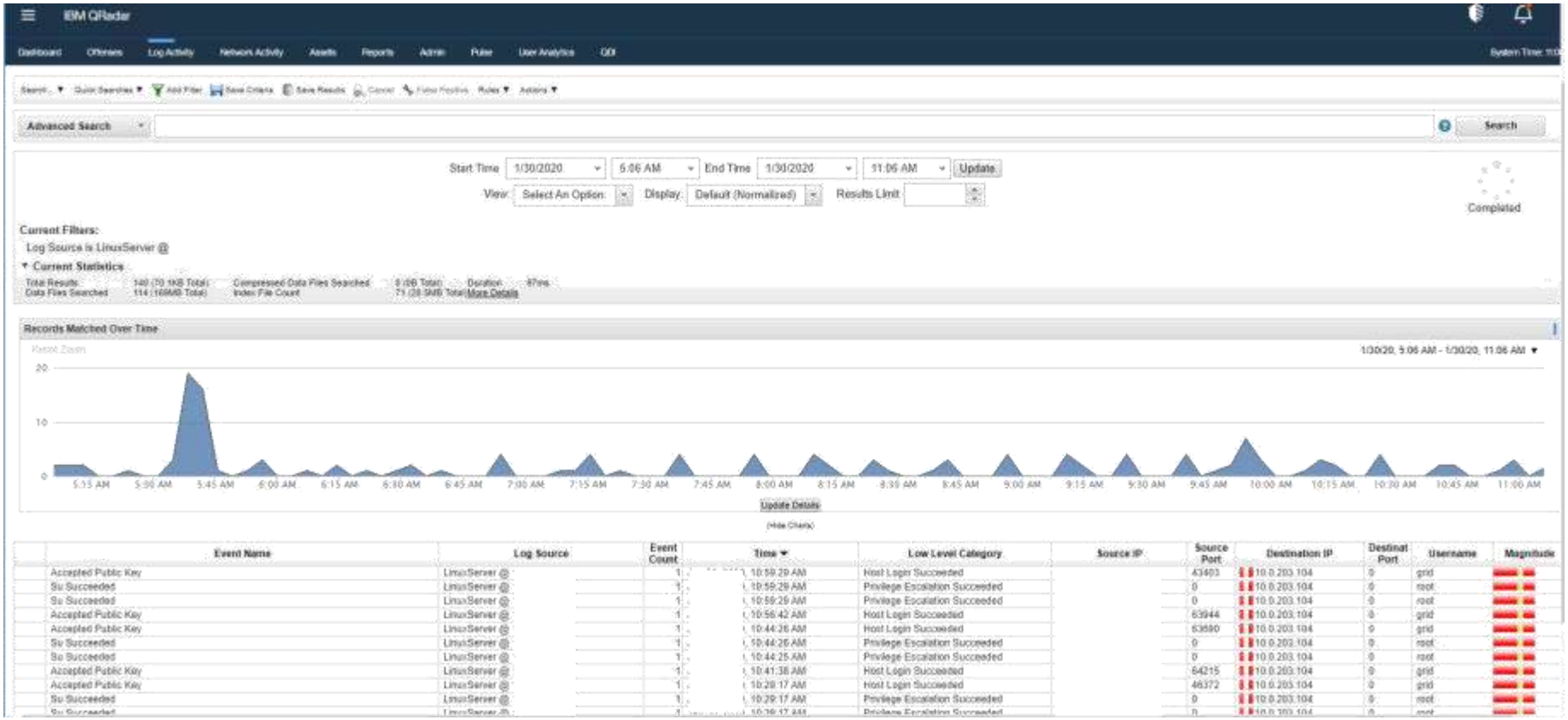


Ilustración 85: Log Activity 2

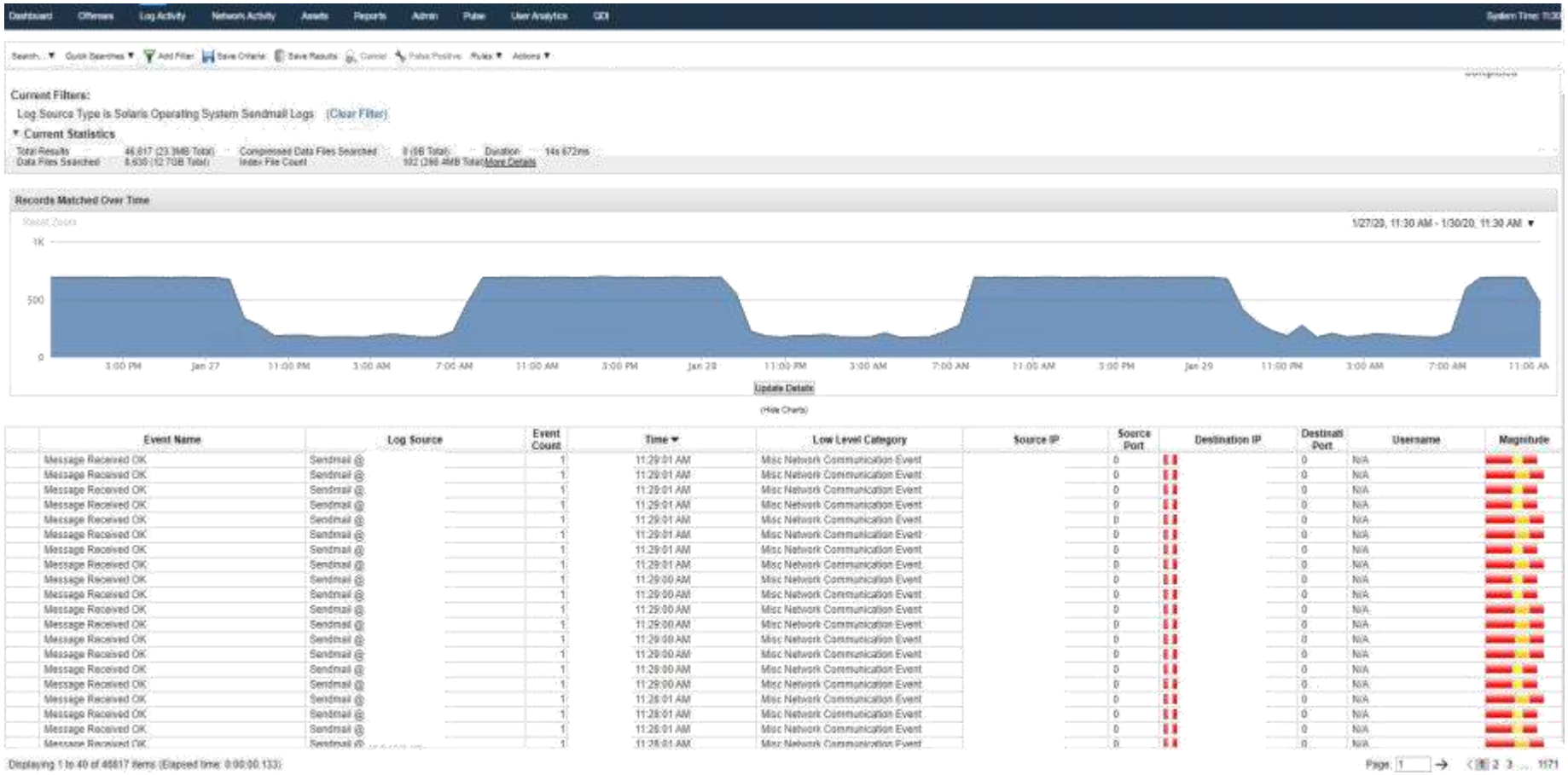
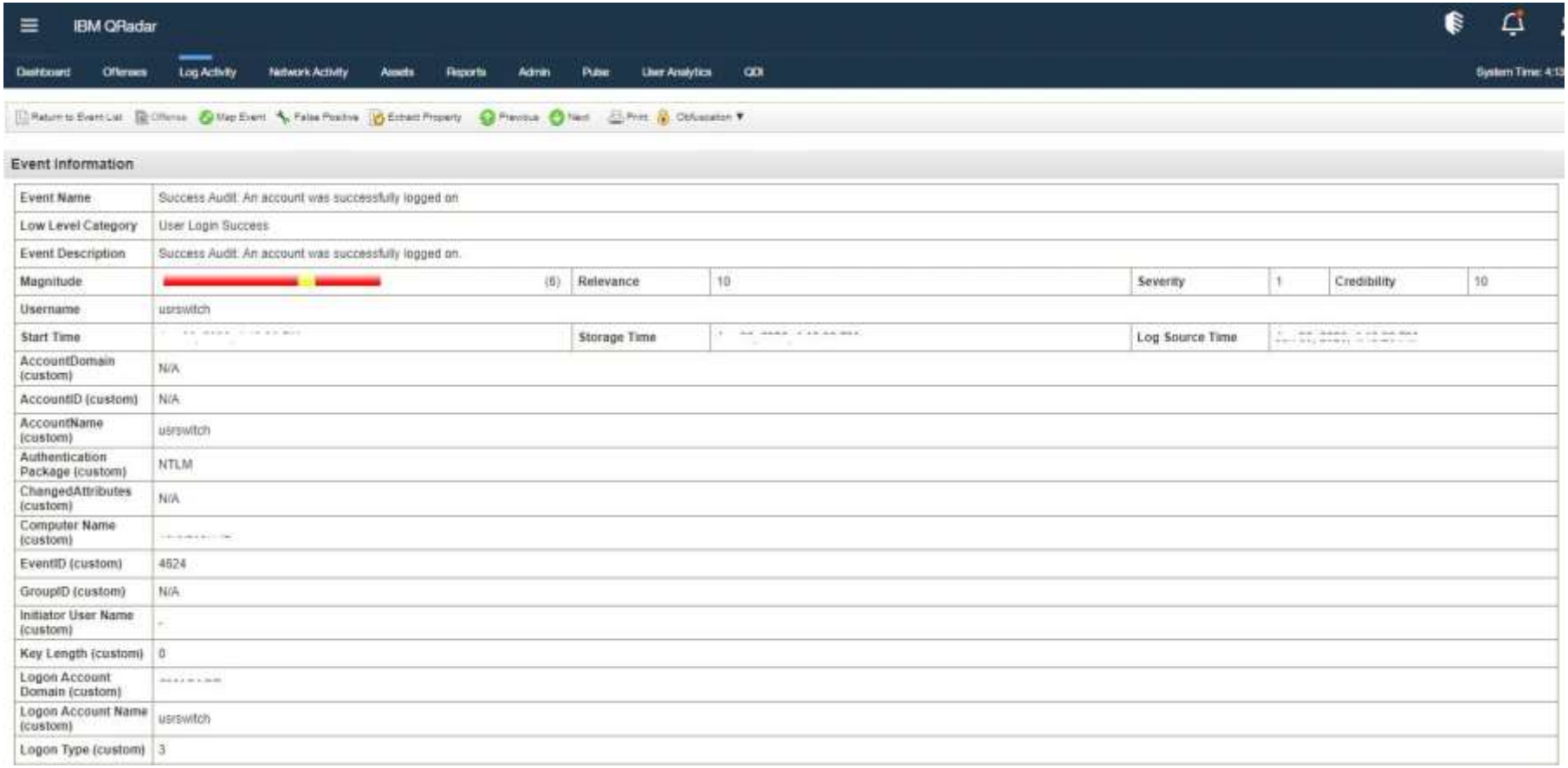


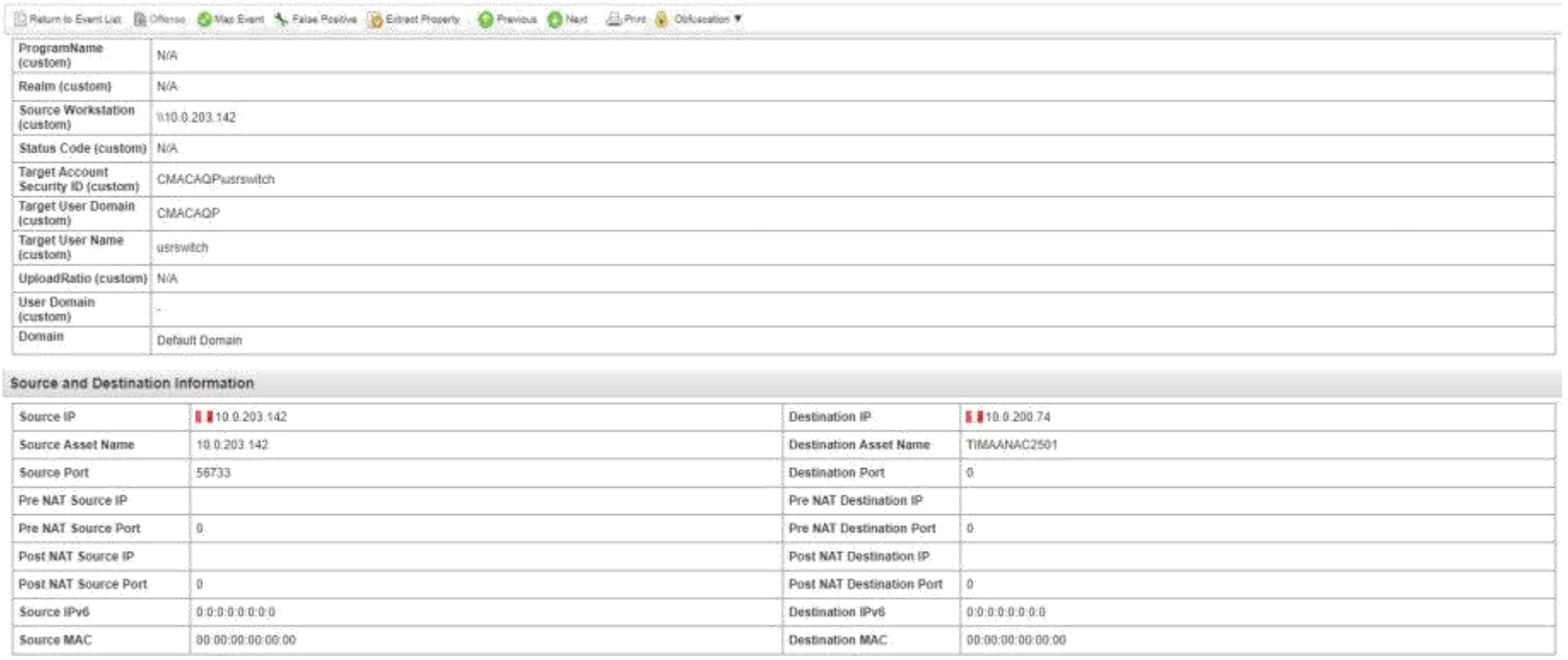
Ilustración 86: Log Activity 3

Cuando desee seleccionar un evento para ver detalles o realizar una acción, debe pausar la transmisión antes de hacer doble clic en un evento, luego de dar doble clic se visualizará la siguiente ventana, donde detalla toda la información de los eventos.



Event Name	Success Audit: An account was successfully logged on						
Low Level Category	User Login Success						
Event Description	Success Audit: An account was successfully logged on.						
Magnitude	[redacted] (6)	Relevance	10	Severity	1	Credibility	10
Username	usrswitch						
Start Time	[redacted]	Storage Time	[redacted]	Log Source Time	[redacted]		
AccountDomain (custom)	N/A						
AccountID (custom)	N/A						
AccountName (custom)	usrswitch						
Authentication Package (custom)	NTLM						
ChangedAttributes (custom)	N/A						
Computer Name (custom)	[redacted]						
EventID (custom)	4624						
GroupID (custom)	N/A						
Initiator User Name (custom)	-						
Key Length (custom)	0						
Logon Account Domain (custom)	[redacted]						
Logon Account Name (custom)	usrswitch						
Logon Type (custom)	3						

Ilustración 87: Log Activity 4


Return to Event List | Offense | Map Event | False Positive | Extract Property | Previous | Next | Print | Obfuscation ▼

ProgramName (custom)	N/A
Realm (custom)	N/A
Source Workstation (custom)	\\10.0.203.142
Status Code (custom)	N/A
Target Account Security ID (custom)	CMACAQP\usrswitch
Target User Domain (custom)	CMACAQP
Target User Name (custom)	usrswitch
UploadRatio (custom)	N/A
User Domain (custom)	-
Domain	Default Domain

Source and Destination Information

Source IP	[redacted]10.0.203.142	Destination IP	[redacted]10.0.200.74
Source Asset Name	10.0.203.142	Destination Asset Name	TIMAANAC2501
Source Port	56733	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Ilustración 88: Log Activity 5

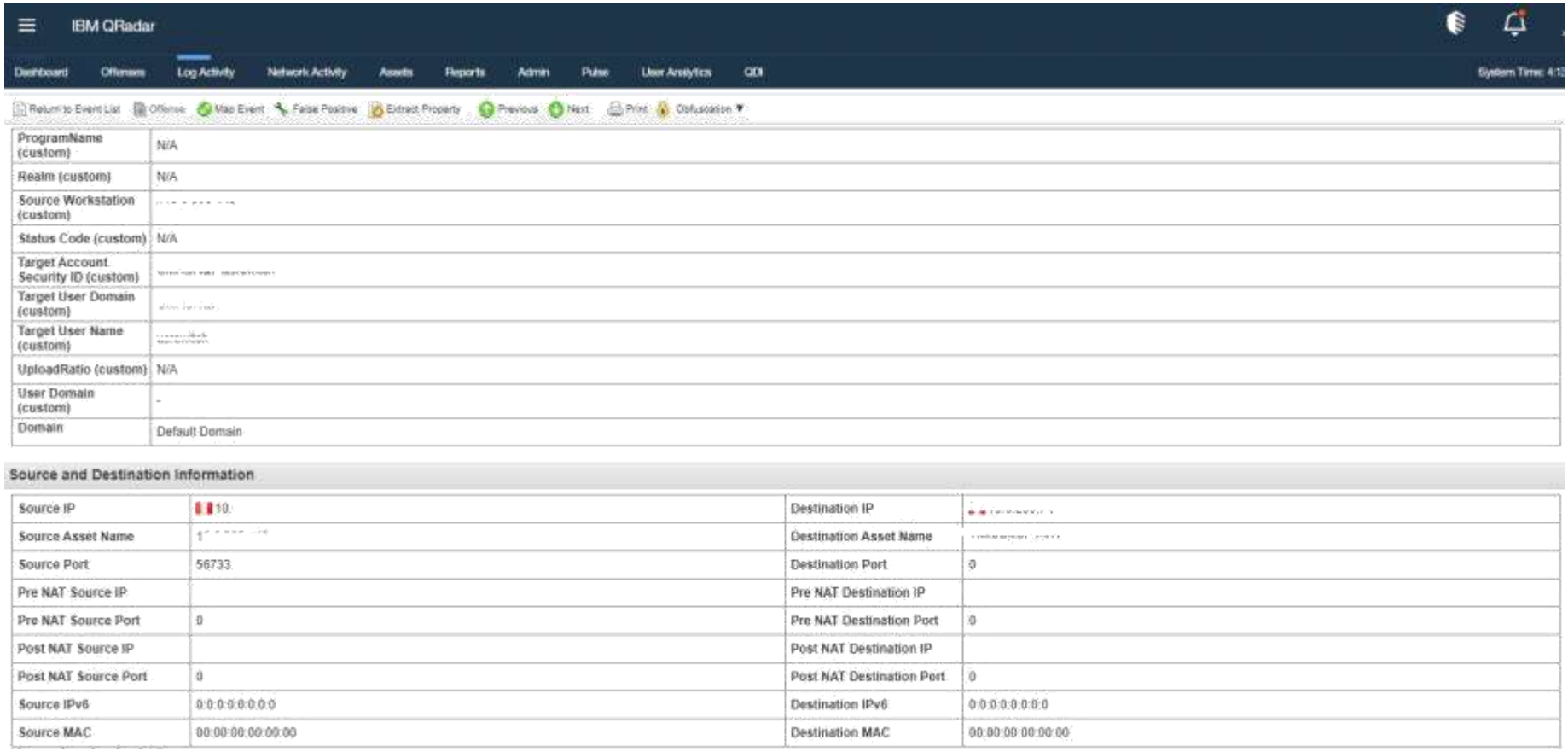


Ilustración 89: Log Activity 6

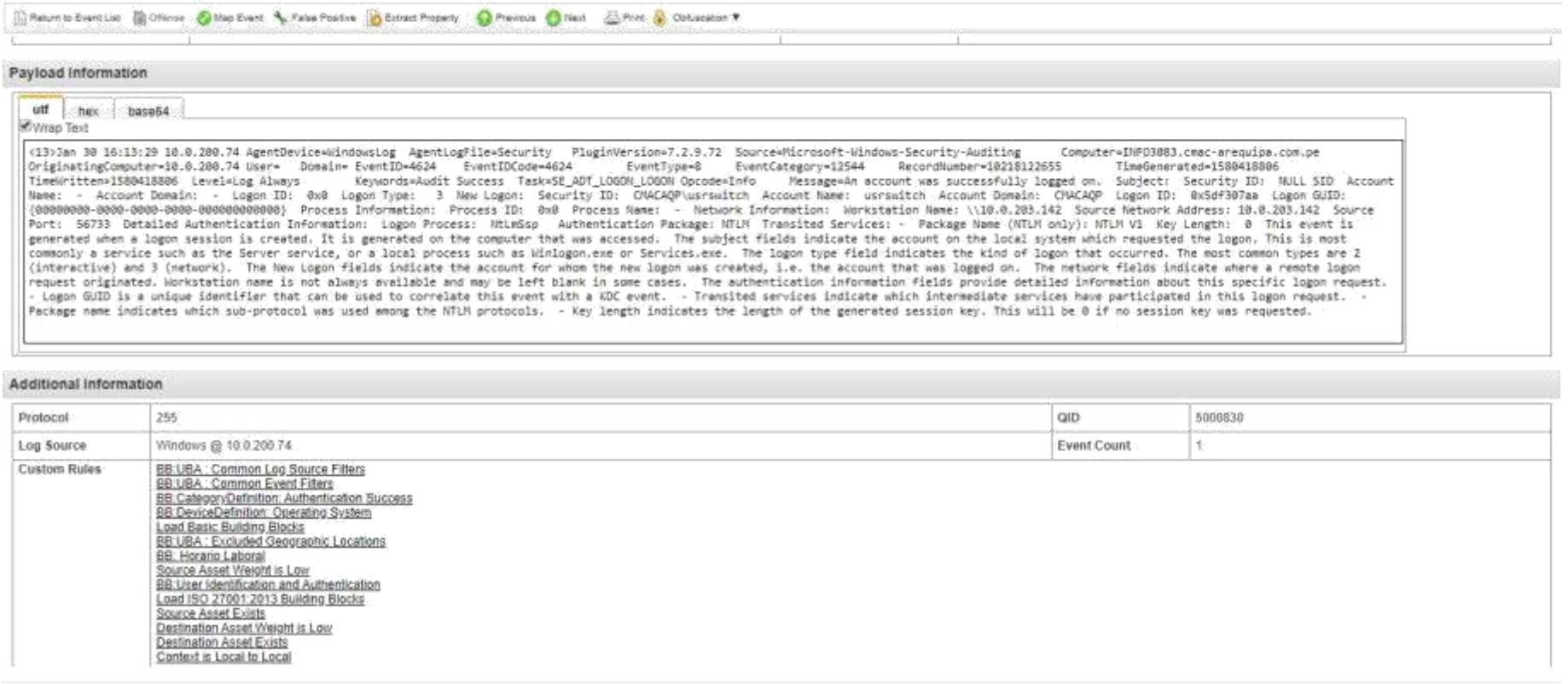


Ilustración 90: Log Activity 7

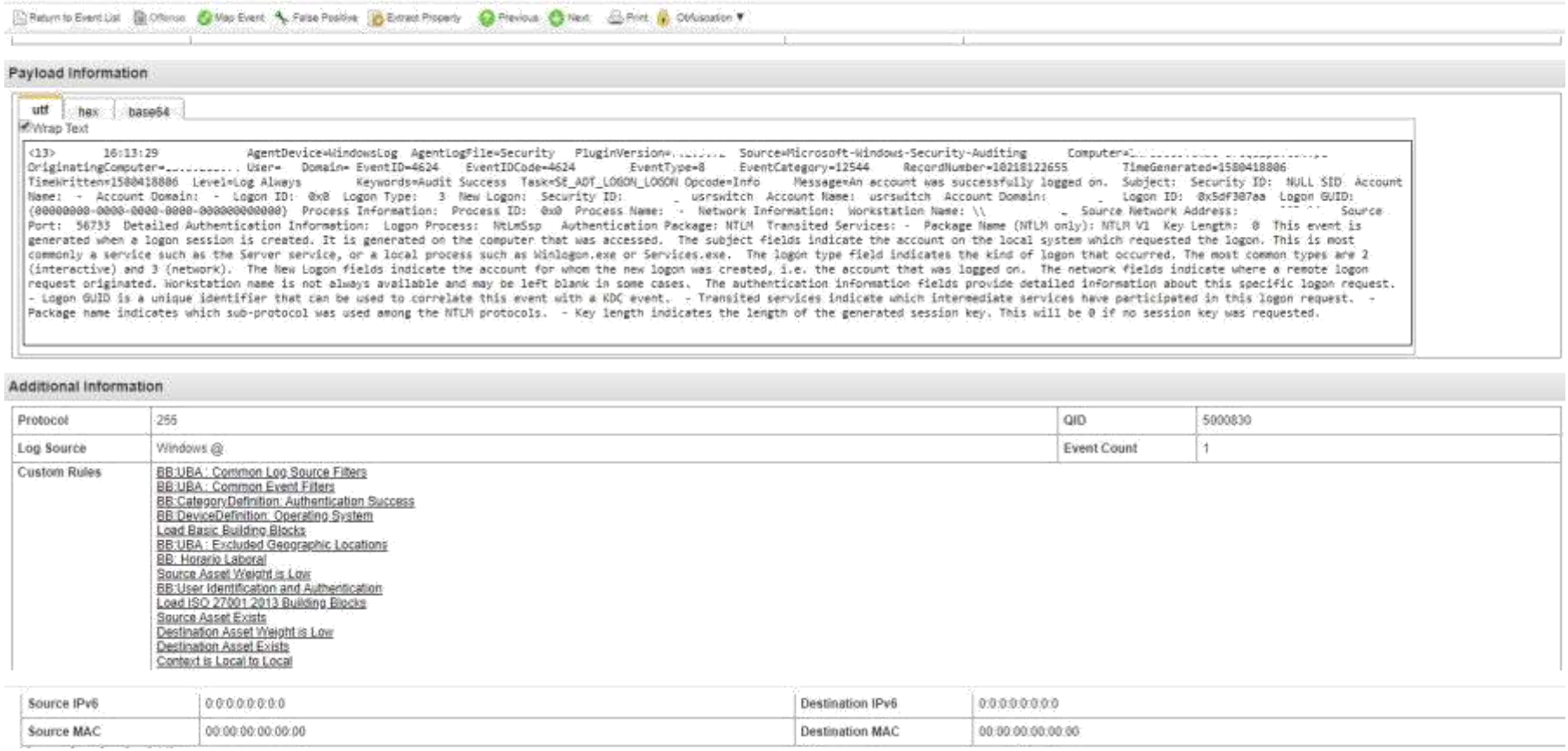


Ilustración 91: Log Activity 8

Se puede evidenciar que durante el tiempo que se realizó el monitoreo de eventos después de realizar la integración al SIEM, se está recibiendo eventos de seguridad satisfactoriamente y sin ninguna pérdida de información de eventos.

3.5.2 Monitoreo de Alertas

3.5.2.1 Dashboard

QRadar SIEM muestra la pestaña Dashboard cuando inicia sesión, para monitorear el comportamiento de su evento de seguridad. Proporciona un entorno de espacio de trabajo que admite múltiples paneles en los que puede mostrar las vistas de seguridad de red, actividad o datos que se recopilan. Los dashboard permiten organizar los elementos de panel de control en vistas funcionales, que le permiten enfocarse en áreas específicas de su red. Dentro de esta sección se visualiza 8 dashboards puede, también se puede crear múltiples dashboard, cada Dashboard puede contener elementos que proporcionan información resumida y detallada.

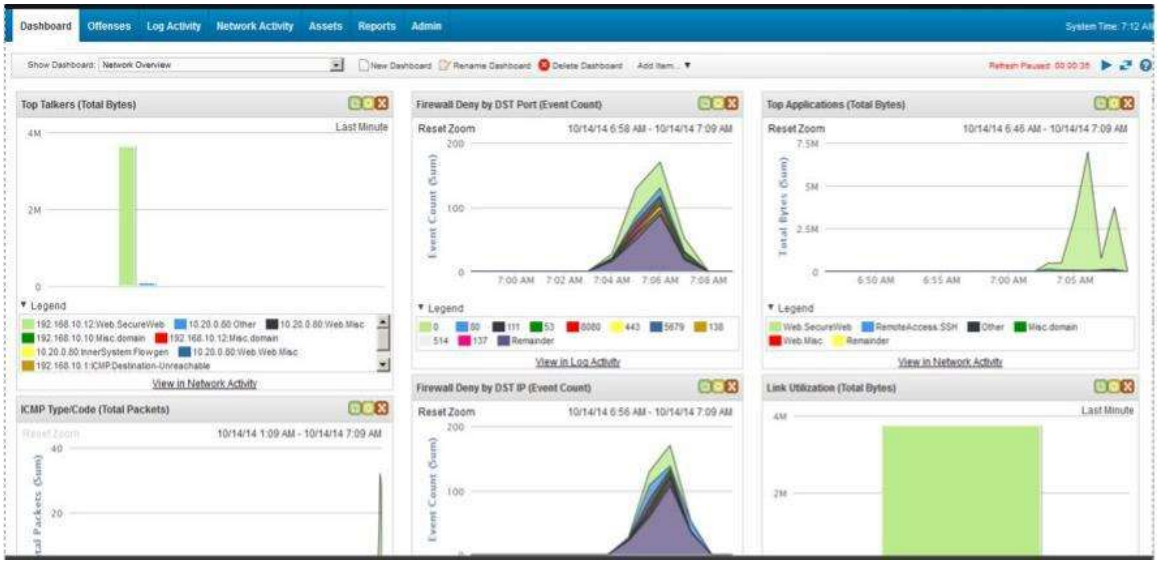


Ilustración 92: Dashboard

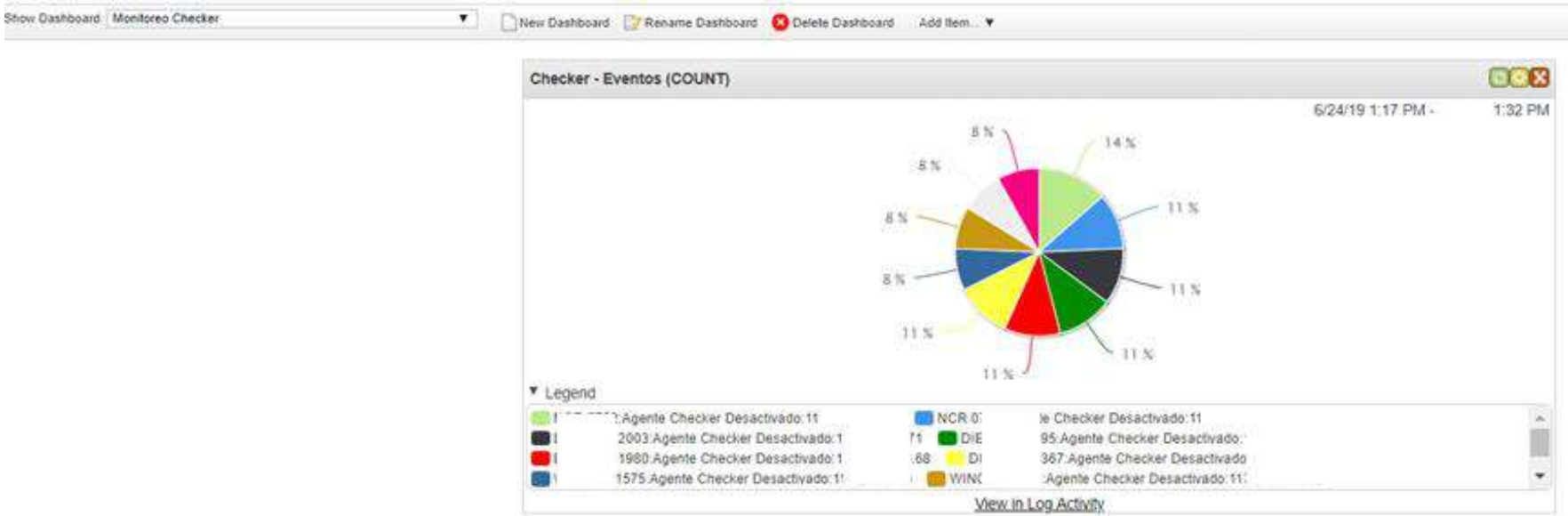


Ilustración 93: Dashboard Checker

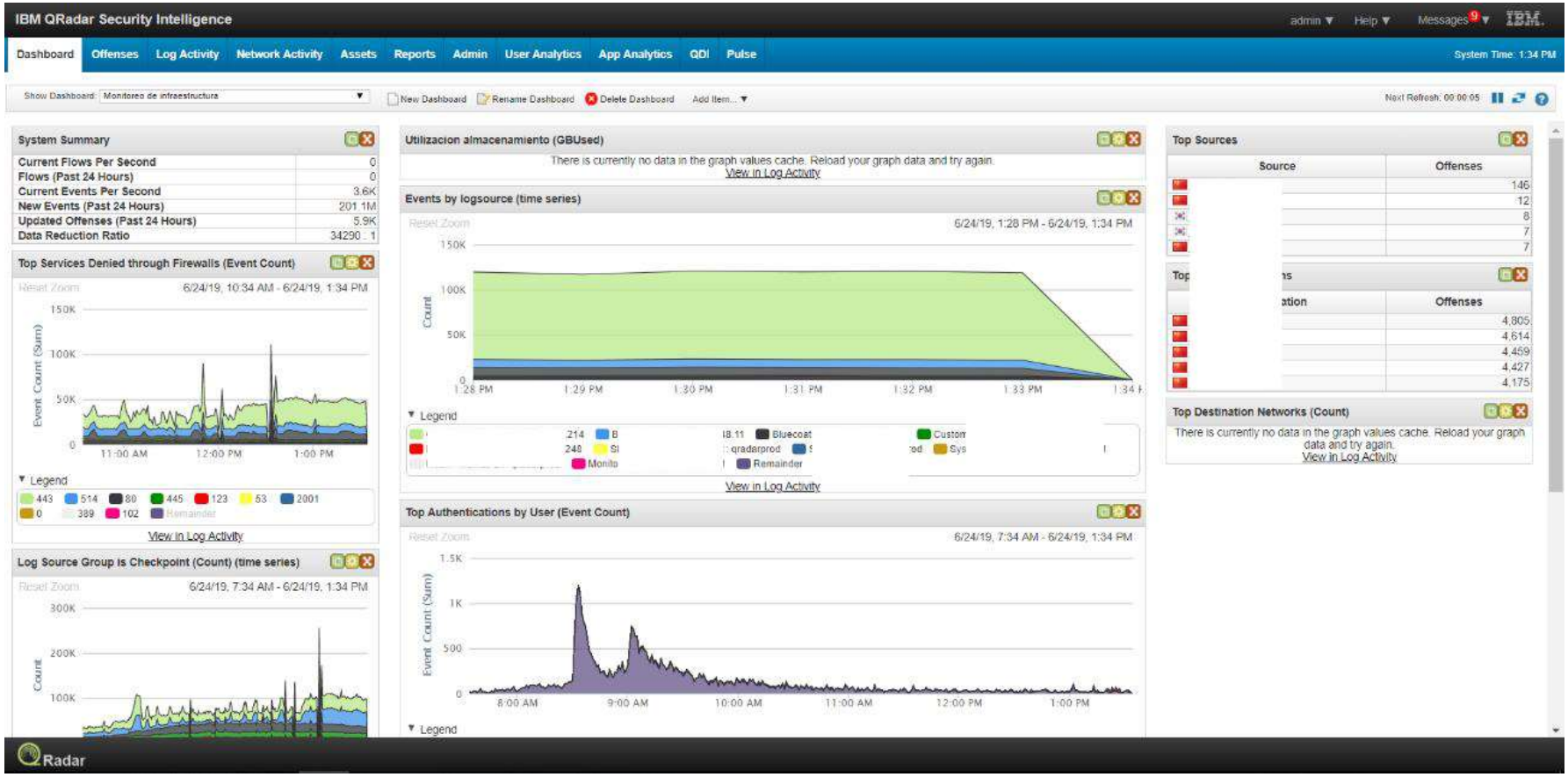


Ilustración 94: Dashboard Monitoreo de Infraestructura

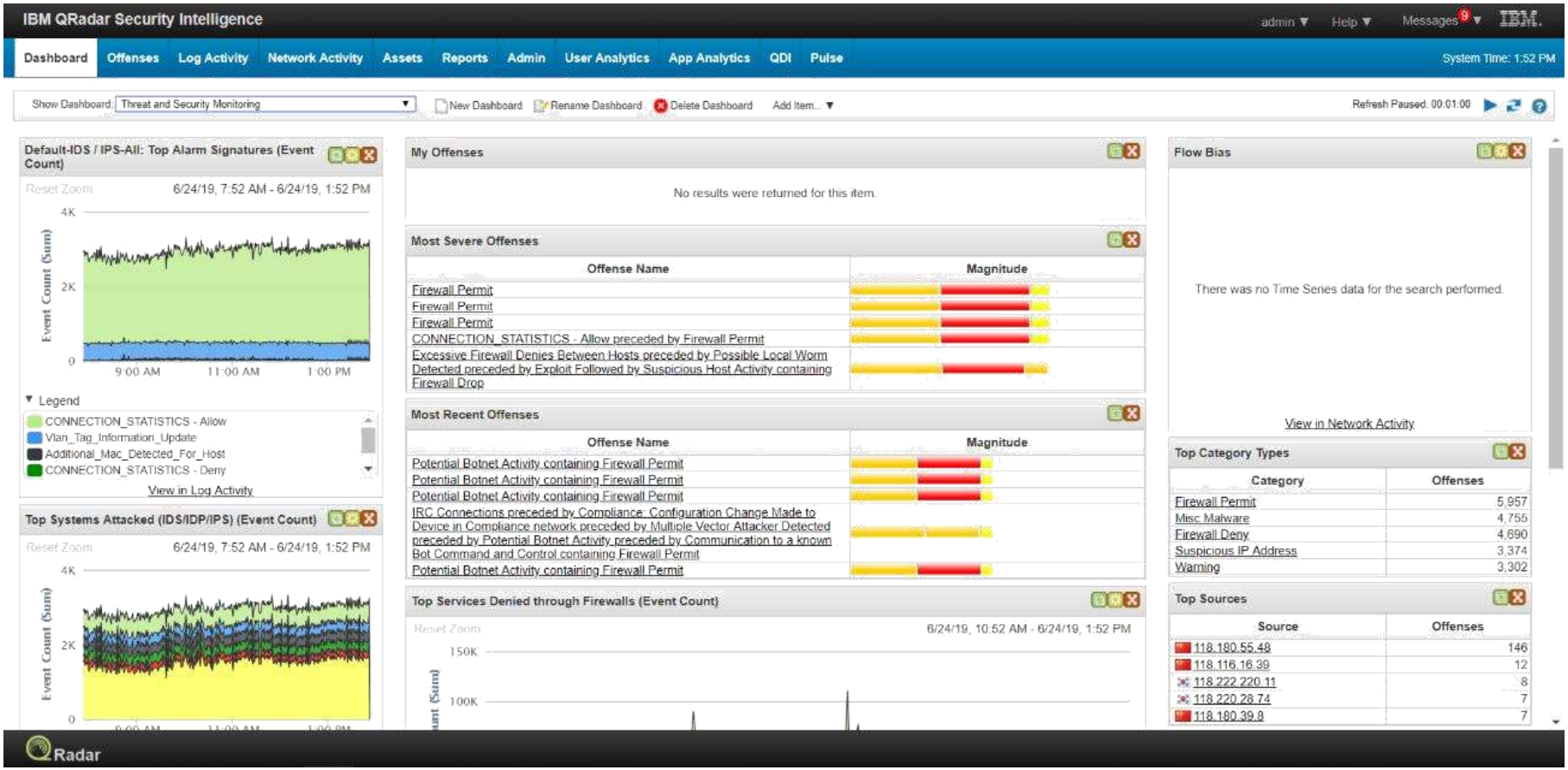


Ilustración 95: Dashboard Threat and Security Monitoriing

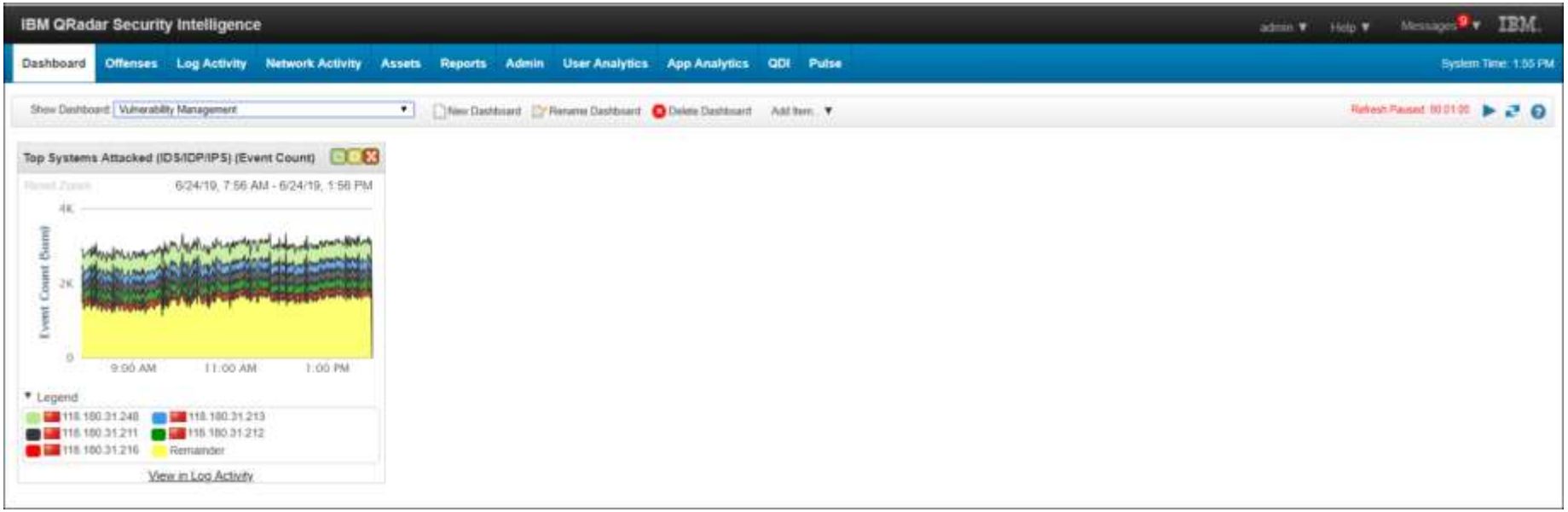


Ilustración 96: Dashboard Vulnerability Management

3.5.2.2 Reporte

La pestaña de reportes o también llamados informes permite crear, distribuir y gestionar informes para los datos en QRadar.

➢ **Características:**

- Permite crear informes personalizados para uso operativo y ejecutivo. Para crear un informe, puede combinar la información (por ejemplo, seguridad o red) en un único informe.
- Permite utilizar plantillas de informe preinstaladas que se incluyen con QRadar.
- Permite marcar los informes con logotipos personalizados. Esta personalización es beneficiosa para distribuir informes a diferentes públicos.
- Unas opciones de creación de informes detalladas y flexibles satisfacen diversos estándares normativos como, por ejemplo, la conformidad con PCI.
- Un informe puede constar de varios elementos de datos y puede representar datos de red y de seguridad en diversos estilos, tales como tablas, gráficos de línea, gráficos circulares y gráficos de barras. Al seleccionar el diseño de un informe, tenga en cuenta el tipo de informe que desea crear. Por ejemplo, no elija un contenedor de gráfico pequeño para un contenido de gráfico que muestra muchos objetos.

➢ **Tipos de Gráfico**

Cuando se crea un informe, se debe elegir un tipo de gráfico para cada gráfico que incluya en el informe. El tipo de gráfico determina cómo aparecen en el informe generado los datos y objetos de red. Se puede utilizar cualquiera de los siguientes tipos de gráficos:

Tipo de gráfico	Descripción
Ninguno	Utilice esta opción si necesita un espacio en blanco en el informe. Si selecciona la opción Ninguno para cualquier contenedor, no es necesario realizar ninguna configuración adicional para dicho contenedor.
Vulnerabilidades de activos	Utilice este gráfico para ver los datos de vulnerabilidad para cada activo definido en el despliegue. Puede generar gráficos de vulnerabilidad de activos cuando una exploración de VA ha detectado vulnerabilidades. Este gráfico está disponible después de instalar IBM Security QRadar Vulnerability Manager.
Conexiones	Esta opción de gráfico solo se visualiza si ha adquirido IBM Security QRadar Risk Manager y dispone de la licencia correspondiente. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Risk Manager*.
Reglas de dispositivo	Esta opción de gráfico solo se visualiza si ha adquirido IBM Security QRadar Risk Manager y dispone de la licencia correspondiente. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Risk Manager*.
Objetos no utilizados de dispositivo	Esta opción de gráfico solo se visualiza si ha adquirido IBM Security QRadar Risk Manager y dispone de la licencia correspondiente. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Risk Manager*.
Sucesos/Registros	Utilice este gráfico para ver información de suceso. Puede basar un gráfico en datos de búsquedas guardadas en la pestaña **Actividad de registro**. Puede configurar el gráfico para trazar datos durante un periodo de tiempo configurable para detectar tendencias de sucesos. Para obtener más información sobre las búsquedas guardadas, consulte Búsquedas de datos.
Orígenes de registro	Utilice este gráfico para exportar o informe sobre los orígenes de registro. Seleccione los orígenes de registro y los grupos de orígenes de registro que desea que aparezcan en el informe. Ordene los orígenes de registro por columnas de informe. Incluya orígenes de registro de los que no se ha informado durante un periodo de tiempo definido. Incluya orígenes de registro que se han creado en un periodo de tiempo especificado.

Tipo de gráfico	Descripción
Flujos	Utilice este gráfico para ver información de flujo. Puede basar un gráfico en datos de búsquedas guardadas en la pestaña **Actividad de red**. Puede configurar el gráfico para trazar datos de flujo durante un periodo de tiempo configurable para detectar tendencias de flujo. Para obtener más información sobre las búsquedas guardadas, consulte Búsquedas de datos.
IP de destino principales	Utilice este gráfico para visualizar las direcciones IP de destino principales en las ubicaciones de red que seleccione.
Delitos principales	Utilice este gráfico para visualizar los delitos principales que se producen en el momento actual para las ubicaciones de red que seleccione.
Delitos a lo largo del tiempo	Utilice este gráfico para visualizar todos los delitos cuya hora de inicio está dentro de un intervalo de tiempo definido para las ubicaciones de red que seleccione.
IP de origen principales	Utilice este gráfico para visualizar y ordenar los principales orígenes de delito (direcciones IP) que atacan la red o los activos de la empresa.
Vulnerabilidades	La opción Vulnerabilidades sólo se visualiza cuando se ha adquirido IBM Security QRadar Vulnerability Manager y se dispone de licencia para el mismo. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

Tipo de gráfico	Descripción
Ninguno	Utilice esta opción si necesita un espacio en blanco en el informe. Si selecciona la opción Ninguno para cualquier contenedor, no es necesario realizar ninguna configuración adicional para dicho contenedor.
Vulnerabilidades de activos	Utilice este gráfico para ver los datos de vulnerabilidad para cada activo definido en el despliegue. Puede generar gráficos de vulnerabilidad de activos cuando una exploración de VA ha detectado vulnerabilidades. Este gráfico está disponible después de instalar IBM Security QRadar Vulnerability Manager.
Vulnerabilidades	La opción Vulnerabilidades sólo se visualiza cuando se ha adquirido IBM Security QRadar Vulnerability Manager y se dispone de licencia para el mismo. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

Ilustración 97: Tipos de gráficos de reportes
Fuente: Guía de IBM

➢ **Proceso de visualización de reporte:**

1) Una vez ubicados en la pestaña reportes se puede buscar y ordenar los reportes de manera similar a los eventos y flujos, como se puede ver en la (IBM, 2019)siguiente imagen.

Ilustración 98: Ventana de reportes

2) Verificar reportes en la distribución de grupos.

Ilustración 99: Grupo de reportes

3) Ejecutar un reporte, para poder visualizar la información.

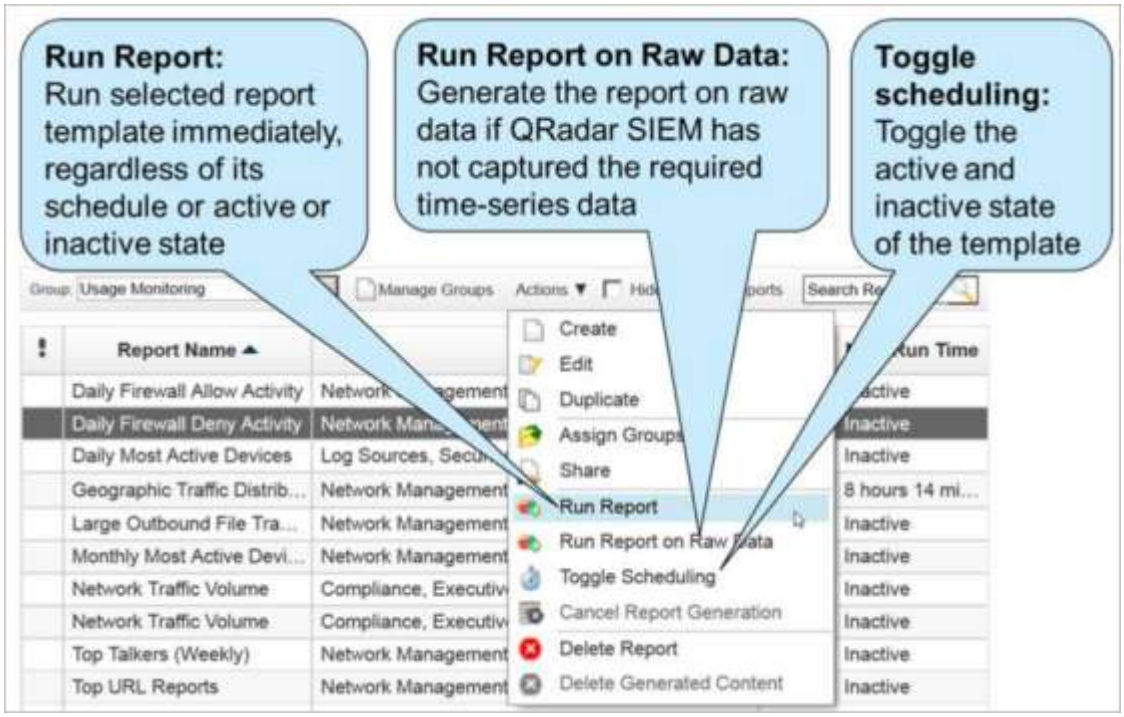


Ilustración 100: Ejecución de reporte

4) Seleccionar el reporte generado.

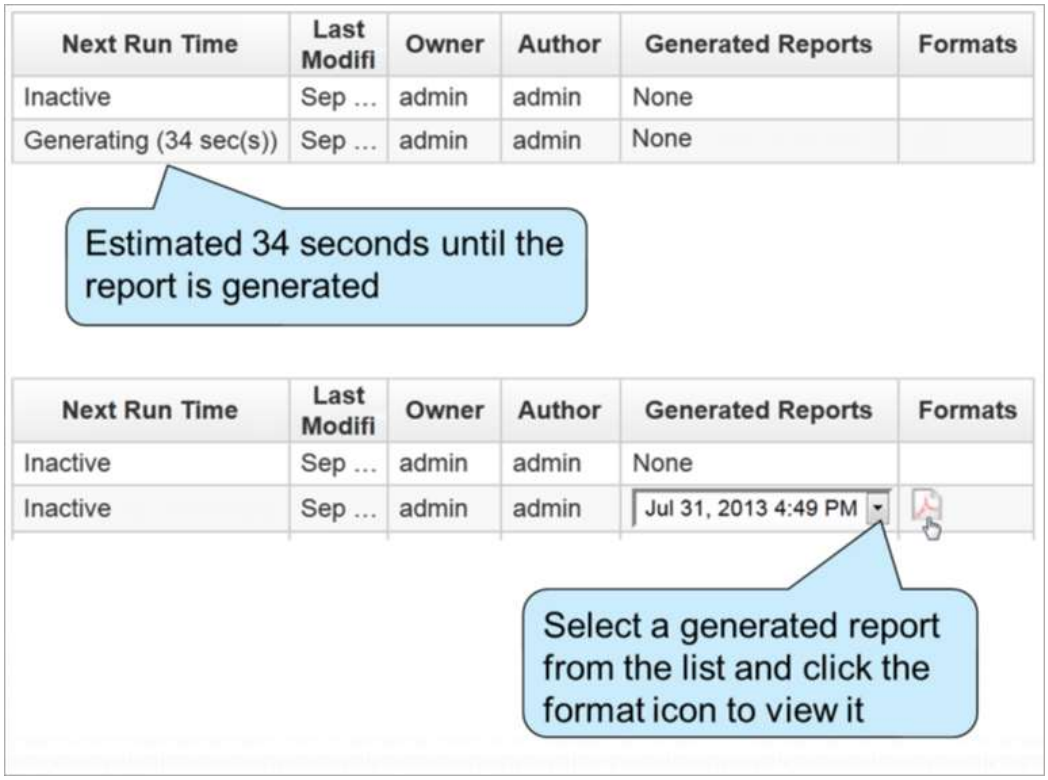
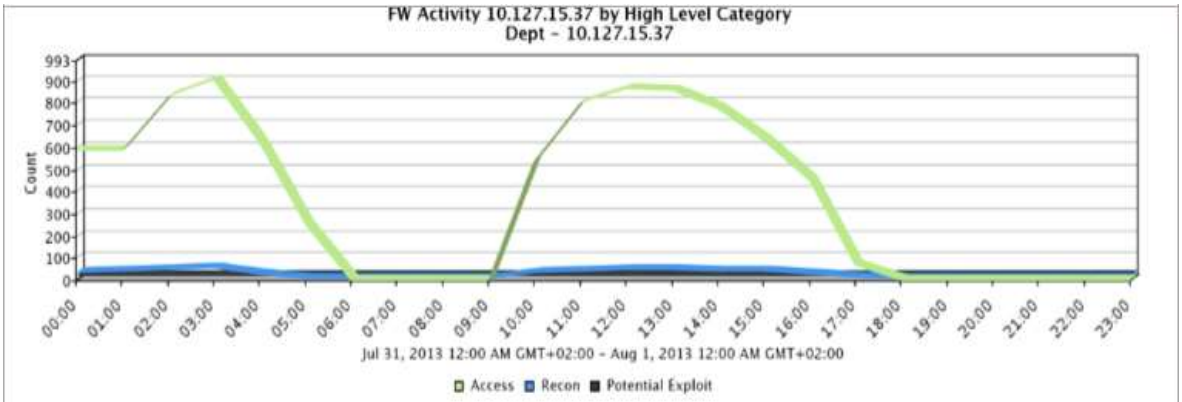


Ilustración 101: Generación de reporte

5) Ver el informe generado



FW Watch
Top Services/Ports Through Firewalls
Jul 31, 2013 12:00:00 AM - Aug 1, 2013 12:00:00 AM

Destination Port	Log Source	Event Name	Low Level Category	Source IP	Destination IP	Username	Event Count	Count
443	CheckPoint @ FW-1Machine	Firewall Permit	Firewall Permit	Multiple (4,961)	Multiple (22)	N/A	409,974	407,503
0	CheckPoint @ FW-1Machine	Firewall Permit	Firewall Permit	Multiple (4,791)	Multiple (451)	N/A	246,956	246,872
80	CheckPoint @ FW-1Machine	Firewall Permit	Firewall Permit	Multiple (3,547)	Multiple (74)	N/A	190,056	189,528
25	CheckPoint @ FW-1Machine	Firewall Permit	Firewall Permit	Multiple (530)	Multiple (5)	N/A	15,115	15,109
161	CheckPoint @ FW-1Machine	Firewall Permit	Firewall Permit	Multiple (4)	Multiple (57)	N/A	9,139	9,139

Ilustración 102: Visualización de reporte

➢ **Mejores prácticas al crear informes**

✓ Para comparación y revisión, presente diagramas de tráfico de red y tablas de eventos juntos.

✓ Considerar el propósito del informe y elija el menor número de contenedores de páginas que sea necesario para comunicar los datos.

✓ No elegir una división de página pequeña para un gráfico que pueda contener una gran cantidad de objetos.

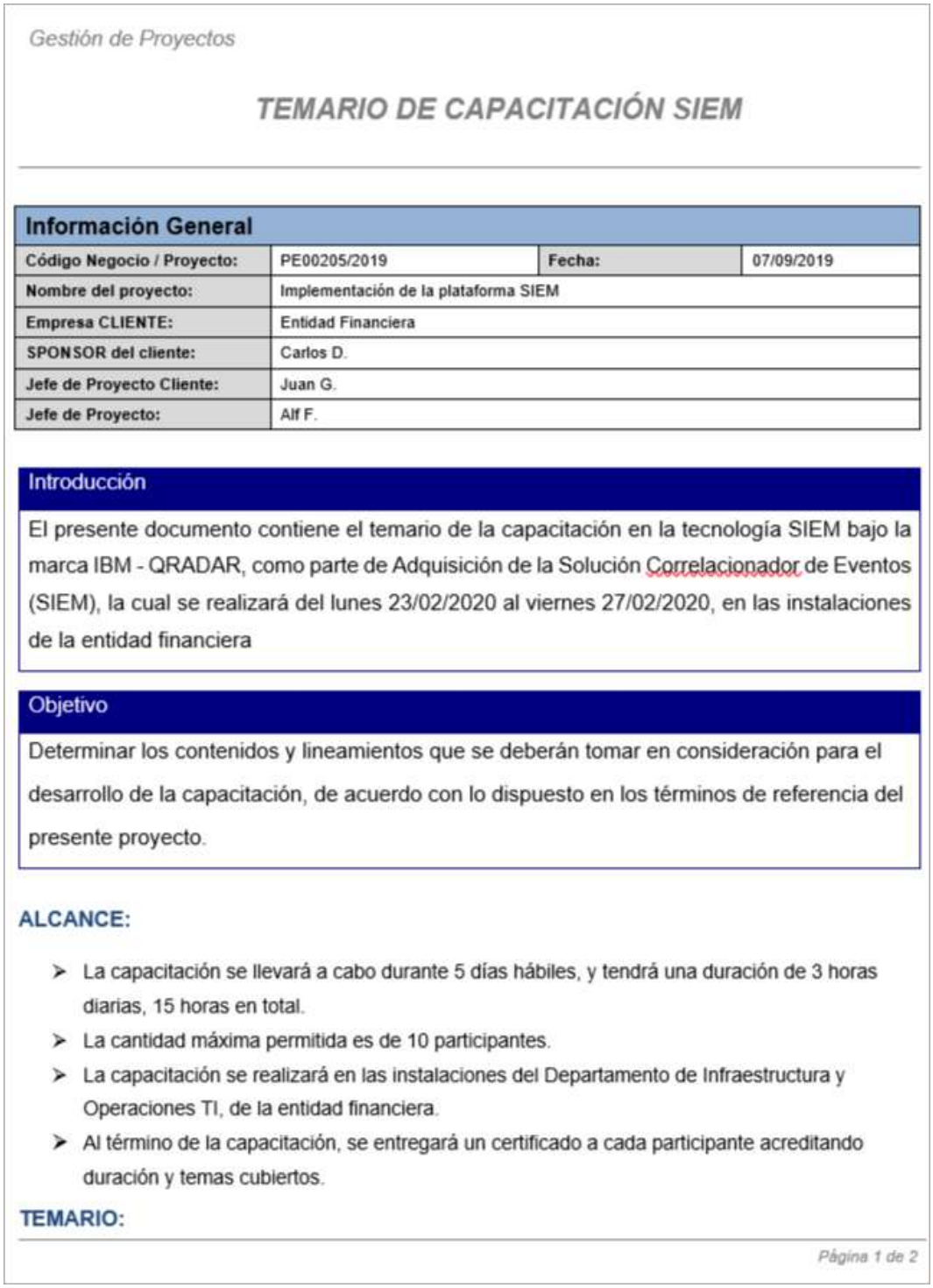
✓ Los informes de resumen ejecutivo utilizan divisiones de una o dos páginas para simplificar el enfoque del informe.

3.6 FASE CIERRE

3.6.1 Capacitación

3.6.1.1 Temario

A continuación, se detalla el temario de la capacitación realizada a los usuarios que usarán la plataforma SIEM.



Gestión de Proyectos

TEMARIO DE CAPACITACIÓN SIEM

Información General			
Código Negocio / Proyecto:	PE00205/2019	**Fecha:**	07/09/2019
Nombre del proyecto:	Implementación de la plataforma SIEM		
Empresa CLIENTE:	Entidad Financiera		
SPONSOR del cliente:	Carlos D.		
Jefe de Proyecto Cliente:	Juan G.		
Jefe de Proyecto:	Alf F.		

Introducción

El presente documento contiene el temario de la capacitación en la tecnología SIEM bajo la marca IBM - QRADAR, como parte de Adquisición de la Solución Correlacionador de Eventos (SIEM), la cual se realizará del lunes 23/02/2020 al viernes 27/02/2020, en las instalaciones de la entidad financiera

Objetivo

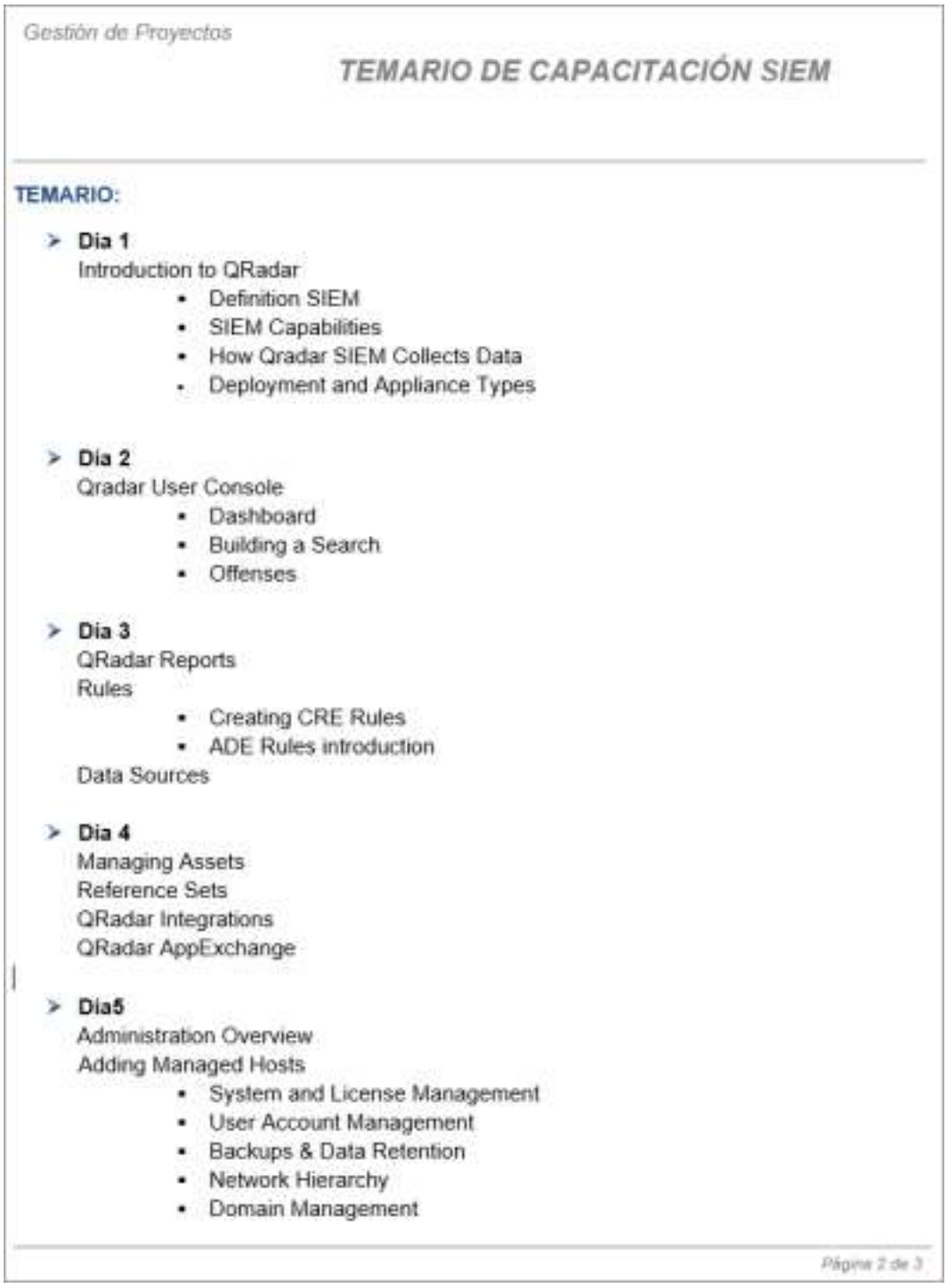
Determinar los contenidos y lineamientos que se deberán tomar en consideración para el desarrollo de la capacitación, de acuerdo con lo dispuesto en los términos de referencia del presente proyecto.

ALCANCE:

- La capacitación se llevará a cabo durante 5 días hábiles, y tendrá una duración de 3 horas diarias, 15 horas en total.
- La cantidad máxima permitida es de 10 participantes.
- La capacitación se realizará en las instalaciones del Departamento de Infraestructura y Operaciones TI, de la entidad financiera.
- Al término de la capacitación, se entregará un certificado a cada participante acreditando duración y temas cubiertos.

TEMARIO:

Página 1 de 2



Gestión de Proyectos

TEMARIO DE CAPACITACIÓN SIEM

TEMARIO:

- **Dia 1**
  Introduction to QRadar
  - Definition SIEM
  - SIEM Capabilities
  - How Qradar SIEM Collects Data
  - Deployment and Appliance Types

- **Dia 2**
  Qradar User Console
  - Dashboard
  - Building a Search
  - Offenses

- **Dia 3**
  QRadar Reports
  Rules
  - Creating CRE Rules
  - ADE Rules introduction

  Data Sources

- **Dia 4**
  Managing Assets
  Reference Sets
  QRadar Integrations
  QRadar AppExchange

- **Dia5**
  Administration Overview
  Adding Managed Hosts
  - System and License Management
  - User Account Management
  - Backups & Data Retention
  - Network Hierarchy
  - Domain Management

Página 2 de 3

Ilustración 103: Temario de Capacitación

Fuente: Elaboración Propia

3.6.2 Acta de conformidad del proyecto

Acta de Conformidad

Fecha: Viernes, 04 de octubre del 2019
Cliente: Entidad Financiera
Proyecto: Implementación y configuración del SIEM.

Mediante el presente documento se deja constancia de la conformidad por el cumplimiento de lo siguiente:

- Implementación del SIEM
  - Instalación del SIEM
  - Configuración inicial.
  - Rackeo en la data center del cliente.
- Instalación y activación de la licencia SIEM
- Afinamiento de reglas configuradas en la plataforma según el siguiente detalle:

Item	Reporte	Caso de uso
1	SI	Múltiples fallas de inicio de sesión en el mismo destino
2	SI	Cargar ISO2700 Bulding Blocks
3	SI	Correo electrónico que contiene archivos confidenciales enviados a un host potencialmente hostil
4	SI	Detectar ataques DDoS
5	SI	Fuentes de ataque de múltiples vectores
6	SI	Denegaciones excesivas en el firewall desde un localhost
7	SI	Limpieza fallida de malware o virus
8	SI	Usuario de alto privilegio que realiza acciones sospechosas
9	SI	Informa un inicio de sesión exitoso en un host después de que se haya realizado el reconocimiento en la red
10	SI	Fuente vulnerable a cualquier exploit
11	SI	Comportamiento de ransomware de los registros de eventos de seguridad de Microsoft Windows

Acta de Conformidad

- Capacitación de 15 horas en la administración, soporte técnico, establecimiento de reglas y reportes de auditoría de base de datos a través del software IBM QRadar.

  Al respecto, y como sustento de lo anteriormente descrito, se adjuntan a la presente acta los siguientes documentos:

  - Lista de asistencia de personal que participó en la capacitación presencial.
  - Presentación de la capacitación ofertada.
  - UN (CD) conteniendo la siguiente información:
  - Actualizaciones y revisiones del producto ofertado que el fabricante libere durante el período de ejecución del contrato. (Backups de configuración de la plataforma al término de la actualización) o Toda bibliografía necesaria para utilizar la solución ofrecida, que el fabricante libere durante el período de ejecución del servicio. (Enlace público del fabricante a la bibliografía disponible y la presentación impresa y en medio electrónico de la capacitación ofertada).

Finalmente, se confirma que la empresa no ha incurrido en penalidades durante el desarrollo de lo ofrecido. En constancia de aceptación se firma la presente acta.

----------	----------
Oficial de Seguridad de la Información	Project Manager
Entidad Financiera	Empresa

Ilustración 104: Acta de conformidad del proyecto

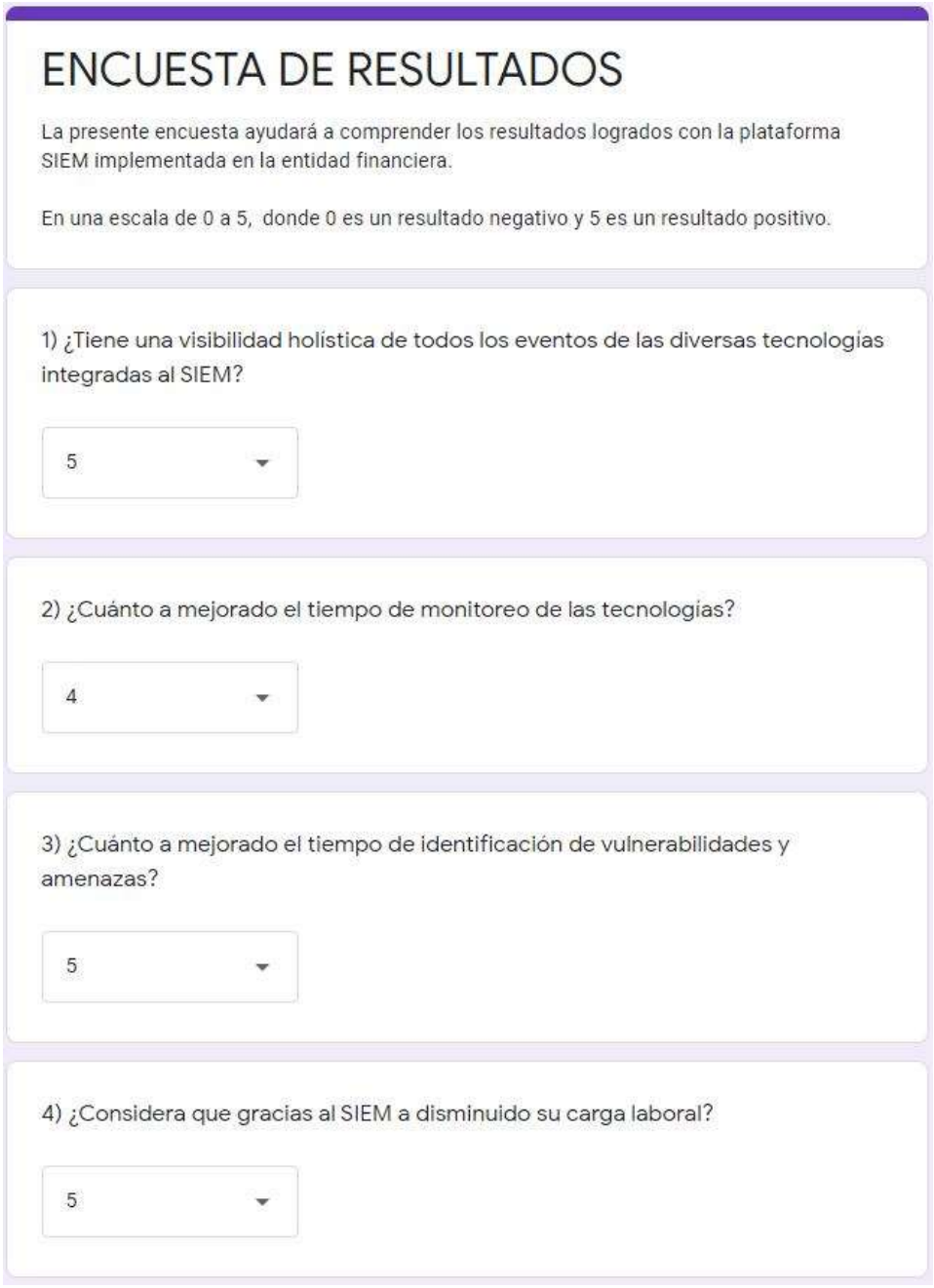
Fuente: *Elaboración Propia*

CAPITULO 4

RESULTADOS

4.1 RESULTADOS

Después de haber realizado la integración de todas las tecnologías brindadas por el cliente se ha realizado una encuesta a 10 usuarios para evaluar si se ha logrado cumplir con los objetivos para el presente proyecto.



ENCUESTA DE RESULTADOS

La presente encuesta ayudará a comprender los resultados logrados con la plataforma SIEM implementada en la entidad financiera.

En una escala de 0 a 5, donde 0 es un resultado negativo y 5 es un resultado positivo.

1) ¿Tiene una visibilidad holística de todos los eventos de las diversas tecnologías integradas al SIEM?

5

2) ¿Cuánto a mejorado el tiempo de monitoreo de las tecnologías?

4

3) ¿Cuánto a mejorado el tiempo de identificación de vulnerabilidades y amenazas?

5

4) ¿Considera que gracias al SIEM a disminuido su carga laboral?

5

5) ¿El SIEM le alerta oportunamente eventos sospechosos?

5

6) ¿El SIEM le permite realizar reportes personalizados de manera sencilla?

5

7) ¿La búsqueda de información específica son más sencillas y rápidas de encontrar?

4

8) ¿Le permite realizar alertas personalizadas complejas de seguridad de una manera sencilla?

4

9) ¿Los informes de eventos y alertas son fáciles de entender?

5

10) ¿Tiene mayor control de eventos de seguridad de las tecnologías integradas?

5

Tabla 34: Cuestionario de Resultados

El resumen de los resultados fueron los siguientes, considerando que 5 es un alto nivel de satisfacción y 0 es un bajo nivel de satisfacción.

Ilustración 105: Logro de resultados
Fuente: *Elaboración Propia*

Gracias a los resultados obtenidos en la evaluación de la implementación del SIEM QRadar, ayudaron a mitigar vulnerabilidades y riesgos cibernéticos expuestas en las plataformas informáticas y redes de una entidad financiera entre los siguientes resultados:

- ✓ La plataforma SIEM centraliza el almacenamiento y la interpretación de los eventos y permite un análisis casi en tiempo real que permite al SOC tomar medidas defensivas más rápidamente.
- ✓ Visibilidad en tiempo real de las tecnologías integradas, que facilitan la detección y priorización de las amenazas.
- ✓ Reducción y priorización de alertas, logrando que las investigaciones del analista de seguridad se focalicen en una lista procesable de incidentes sospechosos de alta probabilidad.
- ✓ Se integró correctamente toda la lista de activos críticos definidos por la entidad financiera.
- ✓ La plataforma SIEM notifica brechas de seguridad dentro de las plataformas informáticas y redes.
- ✓ La plataforma SIEM informa sobre amenazas potenciales y eventos sospechosos en la red.
- ✓ Se puede monitorear la actividad de red y gestión de riesgo de una manera optimizada.
- ✓ Se obtuvo, se analizó y se preparó reportes de eventos de los activos integrados.

Se visualiza que la plataforma se encuentra activo y en funcionamiento, en la siguiente ventana que se muestra.

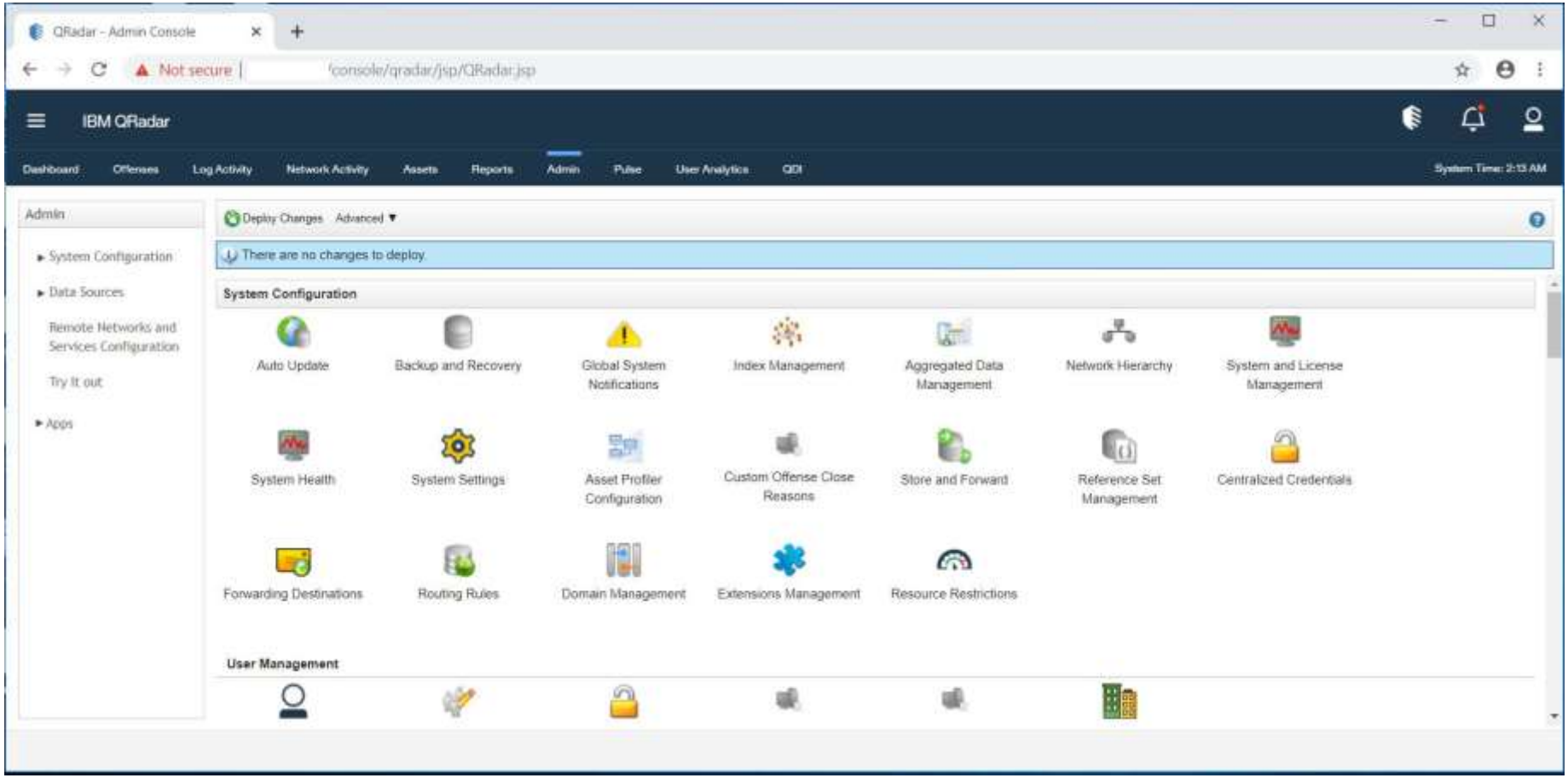


Ilustración 106: Ventana Administrador de la plataforma SIEM

4.1.1 Estado General De La Plataforma

4.1.1.1 Salud

A continuación, se presenta el dashboard de Monitoreo del sistema

Ilustración 107: Dashboard

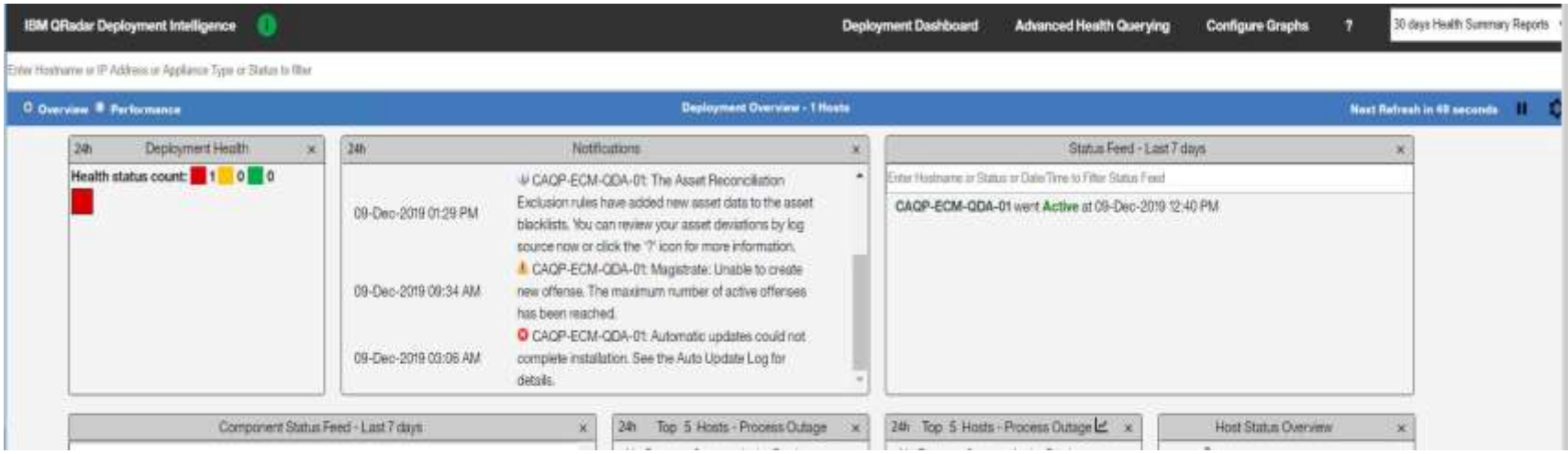
A nivel de deployment la plataforma se encuentra correctamente funcionando.

```
[root@CAQP-ECM-QDA-01 support]# ./validate_deployment.sh
GOOD: No instances of hostid=0 found in deployment history
GOOD: All hosts have a valid masterlist
GOOD: All hosts have a valid token in their masterlist
GOOD: All managed host IDs are correct.
GOOD: All deployed components have valid component references.
GOOD: All managedhostcapabilityxref entries appear valid.
GOOD: All deployment.xml components exist in the database.
GOOD: All deployed_component IDs exist in deployment.xml.
GOOD: All connections in deployment.xml appear to have valid references.
GOOD: All tunnels map back to valid hosts.
GOOD: All server hosts have valid managed hosts
GOOD: All managed hosts have valid server hosts
GOOD: All managed hosts have valid primary_host entries in the serverhost table
GOOD: All flow source connections have valid flow source entries
```

Tabla 35: Deploymentt

4.1.1.2 DashBoards QRadar Deployment Intelligence (QDI)

Se ha implementado una aplicación de monitoreo de Salud desarrollado por IBM, el cual entrega una vista completa de la salud de todas las componentes del Qradar (consola y colectores). Navegando por la aplicación se puede obtener una vista general de la arquitectura completa o revisar por componente individual, sólo basta con seleccionar la vista a revisar, tal como muestra la imagen abajo.



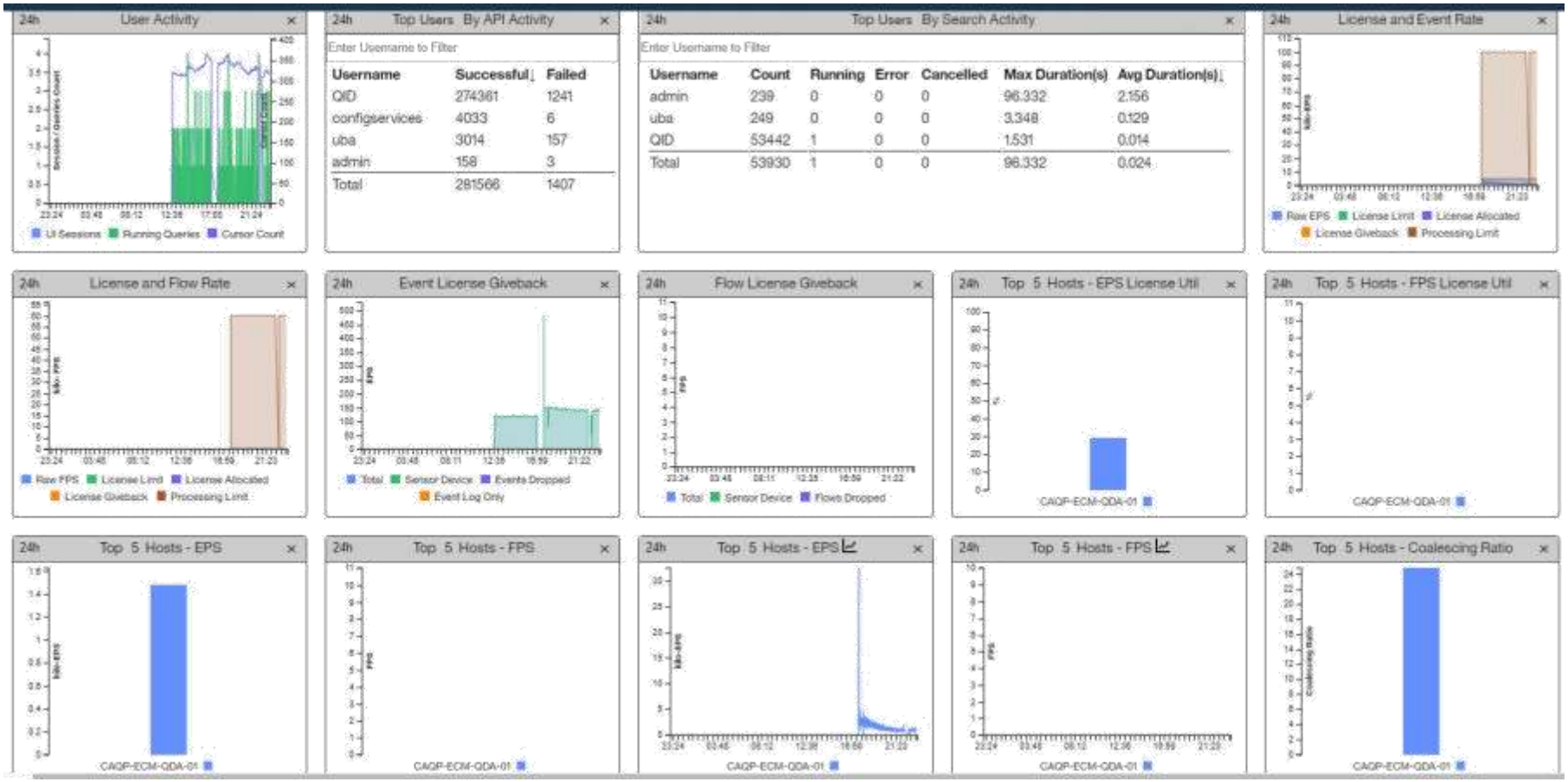


Ilustración 108: DashBoards QRadar Deployment Intelligence

4.1.1.3 Alertas

A nivel de alertas del SIEM se presenta la siguiente tabla:

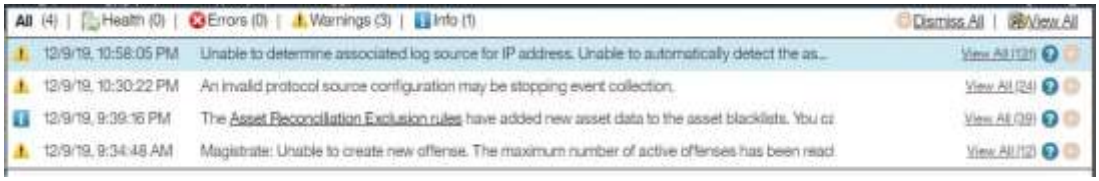


Ilustración 109: Informe de alertas

4.1.1.4 Políticas de retención de datos

Se realizó la configuración de retención de eventos por 3 meses. Esta configuración no asegura que los eventos se almacenarán 3 meses, esto depende de la cantidad de logs que generen los equipos y/o servidores del cliente.

Ilustración 110: Políticas de retención de datos

4.2 PRESUPUESTO

4.2.1 Costo de la Implementación

Cargo	Total
RRHH	S/ 26,200.00
Software	S/ 140.00
Hardware	S/ 300,800.00
TOTAL:	**327,140.00**

Tabla 36: Costo de implementación

4.2.2 Costos Variables

Materiales	Costo Total
Uso de espacio	S/ 800.00
Uso de recursos depreciables (Laptop, mouse, celular, impresora)	S/ 200.00
S.O. Windows 10 Pro	S/ 200.00
Papel Bond A4	S/ 12.00
Tinta para impresora	S/ 150.00
Electricidad	S/ 150.00
Internet y teléfono	S/ 150.00
TOTAL:	**S/ 1,662.00**

Tabla 37: Costos Variables

Costo total del proyecto: S/ 328,802.00

4.3 ANÁLIS DE RIESGO

El riesgo puede ser definido como una probabilidad de que una amenaza explote una brecha en un activo informático, y de la magnitud del daño resultante de tal evento adverso en la entidad.

Debido a que el monitoreo tiene como objetivo aquellos dispositivos cuyo ataque represente un alto nivel de riesgo para la entidad, inicialmente se realiza un análisis de riesgo completo para los activos.

Cuando la amenaza es real, el contador del coste puede ponerse en marcha en cualquier momento. Gastos asociados a la investigación, la paliación, la notificación, la reparación o el abono de sanciones y multas. Costes generados por el tiempo de interrupción causado por la brecha de seguridad y el negocio perdido como consecuencia de sus efectos. Y, por supuesto, también esos otros gastos más difíciles

de calcular, pero igual de reales, como son la repercusión del evento en términos de reputación, la pérdida de posicionamiento o los derivados de demandas colectivas.

4.3.1 Identificación de los activos de información

En esta etapa, se definen los límites del sistema en estudio a la vez que se detallan los recursos y la información que constituyen el sistema, que se denominarán activos de información

4.3.2 Clasificación de activos

Para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información.

CONFIDENCIALIDAD	VALOR
Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera de la Entidad	0
Información que puede ser conocida y utilizada por todos los agentes de la Entidad.	1
Información que sólo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo	2
Información que sólo puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio a la Entidad. o terceros	3

Tabla 38: Escala de clasificación de confidencialidad

INTEGRIDAD	VALOR
Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades de la Entidad.	0
Información cuya modificación no autorizada puede repararse, aunque podría ocasionar un perjuicio para la Entidad o terceros	1
Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para la Entidad o terceros	2
Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades	3

Tabla 39: Escala de clasificación de Integridad

DISPONIBILIDAD	VALOR
Información cuya inaccesibilidad no afecta la actividad normal de la Entidad.	0
Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para la Entidad.	1
Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades de la Entidad.	2
Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la Entidad.	3

Tabla 40: Escala de clasificación de Disponibilidad

4.3.3 Identificación de vulnerabilidades y amenazas

En esta sección se pretenden identificar las diferentes vulnerabilidades y sus respectivas

amenazas potenciales que son aplicables al sistema en el activo evaluado. Se entiende por vulnerabilidad toda debilidad presente en un activo de información, dada comúnmente por la inexistencia o ineficacia de un control, por otro lado.

VULNERABILIDAD	AMENAZA
Asignación errada de los derechos de acceso	Abuso de los derechos
Software nuevo inmaduro	Mal funcionamiento del software
Descarga y uso no controlado de software	Manipulación con software
Disponibilidad innecesaria de puertos	Exposición a malware o robo de archivos
Deshabilitación de software	Manipulación de software
Acceso no contralado	Acceso no autorizado
Control sobre los posibles errores del sistema	No aplica
Brechas de seguridad	Robo de información y/o monetaria

Tabla 41: Identificación de vulnerabilidades y amenazas

Fuente: *Elaboración Propia*

4.3.4 Valoración de amenazas y determinación del impacto

Para cada activo y amenaza debe estimarse la degradación, es decir el porcentaje en que la amenaza daña al activo en estudio estableciendo un valor entre 0 % (no lo daña) y 100 % (lo daña absolutamente) para cada una de las características de confidencialidad, integridad y disponibilidad.

4.3.5 Evaluación del riesgo

La evaluación del riesgo se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz

denominada “Matriz de Calificación, Evaluación y respuesta a los Riesgos”, con la cual se presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen:

Matriz de valoración de riesgos		Consecuencias			
		Insignificante	Moderado	Dañino	Extremo
Probabilidad	Muy alta	Medio	Alto	Crítico	Crítico
	Alta	Medio	Alto	Alto	Crítico
	Media	Bajo	Medio	Alto	Alto
	Baja	Bajo	Bajo	Medio	Medio

Tabla 42: Ejemplo Matriz de Calificación, Evaluación y respuesta a los Riesgos

Donde:

Bajo: Zona de riesgo baja: Asumir riesgo.

Medio: Zona de riesgo moderado: Asumir el riesgo, reducir el riesgo.

Alto: Zona de riesgo alto: Reducir el riesgo, evitar, compartir o transferir.

Crítico: Zona de riesgo crítico: Reducir el riesgo, evitar, compartir o transferir.

Una vez identificados los activos de información, de acuerdo a las tablas de confidencialidad, integridad y disponibilidad se determina su respectiva criticidad. Para desarrollar el monitoreo son seleccionados aquellos con más alto nivel de riesgo.

TIPO	ADICIONALES	SISTEMA OPERATIVO	C	I	D	CRITICIDAD
Checker ATM	Cajeros automáticos	Linux kernel 2.6	3	3	3	3
Servidores	Servidores encargados de monitorear la información de transacciones con número tarjeta.	Win 2012/2012 R2/2016	3	3	3	3
Firewall	Dispositivo que protege los equipos individuales, servidores o equipos conectados en la red contra accesos no deseados.	Firepower 4120	3	2	3	3
Desktop	Equipo escritorio (endpoint)	Win 2016	3	3	2	3

Tabla 43: Tecnologías críticos

Fuente: *Elaboración Propia*

Un ataque de ciberseguridad a nivel de criticidad 3 puede generar grandes pérdidas económicas, las empresas tardan aproximadamente 46 días en corregir las consecuencias de un ataque cibernético y gastan un promedio de **US$ 32,000** por día".

Según la empresa Prey Project, empresa que brinda servicios web freemium, elaboró estadísticas de riesgos de seguridad informática del año 2019:

Estadísticas en Seguridad Informática

Estadísticas en Seguridad Informática
43% de los ciberataques afectan a pequeños negocios. (Small Business Trends)
230,000 nuevos malware son producidos cada día, y se predice que este número crecerá. (Panda Security)
A una compañía le toma entre 6 meses, o 197 días, detectar una brecha de seguridad. (ZD Net)
Hubo más de 3 millones de golpes de crypto jacking entre enero y mayo del 2018. (Quick Heal)

Tabla 44: Estadísticas en Seguridad Informática

Costos de la Seguridad Informática

Costos de la Seguridad Informática
El mercado de la seguridad informática crecerá un 8.7% en el 2019, llegando a los $124 billones. (Computer Weekly)
El costo total de un ciberataque exitoso es de más de 5 millones, o 301 por empleado. (Ponemon)
El componente más caro de un ataque virtual es la pérdida de datos, que representa un 43% de los costos. (Accenture)
Se proyecta que el daño relacionado a ciberataques llegará a los $6 trillones de dólares anuales para el 2021. (CyberSecurity Ventures)
Los dos ataques más frecuentes son los ataques de malware y aquellos basados en la web. Las empresas gastan un estimado de $2.4 millones en defensa. (Accenture)

Tabla 45: Costos de la Seguridad Informática

Ataques Ransomware

Ataques Ransomware
Ocurren más de 4,000 ataques de ransomware por día. (FBI)
75% de las organizaciones infectadas con ransomware tenían protección activa. (Sophos)
Los daños globales relacionados a ataques de ransomware llegarán a $11.5 billones en el 2019. (Cybersecurity Ventures)
Se estima que habrá un ataque de ransomware cada 14 segundos para el fin del 2019. Esto no incluye ataques a individuos, que ocurren con mayor frecuencia. (Cybersecurity Ventures)

Tabla 46: Ataques Ransomware

Ataques Phishing

Ataques Phishing
En una encuesta realizada a más de 1300 profesionales de TI se descubrió que 56% de las organizaciones identificaron al phishing como su mayor riesgo de seguridad informática. (CyberArk)
76% de los negocios reportaron ser víctimas de ataques phishing en el último año. (Wombat Security)

Tabla 47: Ataques Phishing

4.4 ANÁLISIS DE BENEFICIO

4.4.1 Beneficios Tangibles

Se definen como beneficios tangibles a todo lo que se puede medir en valor monetario, los cuales se producen tras la implementación del proyecto. La tabla que se muestra a continuación señala los beneficios tangibles de mayor relevancia del proyecto:

BENEFICIOS TANGIBLES	SIN SISTEMA			CON SISTEMA			TOTAL BENEFICIO
Descripción	**Tiempo trabajado**	**RRHH**	**Costo**	**Tiempo trabajado**	**RRHH**	**Costo**	**Total**
Monitoreo de alertas de seguridad	160 hrs	6	S/10,800.00	160 hrs	3	S/ 5,400.00	S/ 5,400.00
Proceso de análisis de eventos	160 hrs	4	S/ 7,200.00	160 hrs	2	S/ 3,600.00	S/ 3,600.00
Elaboración de reportes	35 hrs	4	S/ 1,440.00	35 hrs	1	S/ 360.00	S/ 1080.00
TOTAL							**S/10,080.00**

Tabla 48: Relación de beneficios tangibles del proyecto

Fuente: *Elaboración Propia*

4.4.2 Beneficios intangibles

Se denominan beneficios intangibles a todo lo que no se puede medir en valor monetario, sin embargo, otorgan mejoras a la empresa y son producidas tras la implementación del proyecto. En consecuencia, se indican a continuación los beneficios intangibles de mayor importancia del proyecto.

ITEM	BENEFICIOS INTANGIBLES
1	Cumplir con los estándares, normas y leyes de seguridad informática y evitar las multas:
	a. Estándar internacional **ISO/IEC 27032,** que facilita la colaboración segura y fiable para proteger la privacidad de las personas en todo el mundo. De esta manera, puede ayudar a prepararse, detectar, monitorizar y responder a los ataques.
	b. Norma **ISO 27001,** es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.
	c. **La norma ISO/IEC 17799** persigue que se proporcione una base común con la que poder llevar a cabo normas de seguridad dentro de las empresas y convertirse en una práctica eficaz de gestión de la seguridad.
	d. **Ley N° 29733:** Ley de Protección de Datos Personales
	e. **Ley N° 30096** y su modificatoria **Ley 30171:** Ley de Delitos Informáticos
	f. **Decreto Legislativo N° 1353**, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses.
2	Concientización sobre seguridad informática.
3	Disminución carga laboral.
4	Aumento de productividad.

Tabla 49: Beneficios Intangibles
Fuente: *Elaboración Propia*

4.5 ANALISIS DE FLUJO DE CAJA, VAN Y TIR

4.5.1 FLUJO DE CAJA

En el periodo cero se están considerando los gastos que están relacionados directamente con la implementación de la solución SIEM QRadar, a partir del primer mes en cuál ya se encuentra implementado el software se realiza el cálculo de la cantidad de costos y beneficios que este generará a la entidad financiera.

Meses	0	1	2	3
Costo de implementación	S/ 327,140.00			
Costo de personal		S/ -	S/ -	S/ -
Costo variables		S/ 554.00	S/ 554.00	S/ 554.00
Costos acumulados	**S/ 327,140.00**	**S/ 327,694.00**	**S/ 328,248.00**	**S/ 328,802.00**
Beneficios Tangibles		S/ 3,360.00	S/ 3,360.00	S/ 3,360.00
Beneficios Prevención			S/ 5,032,000.00	S/ 32,000.00
Beneficios Acumulados			**S/ 5,035,360.00**	**S/ 10,070,720.00**
Flujo de caja (ingreso neto)	-S/ 327,140.00	-S/ 554.00	S/ 5,034,806.00	S/ 10,070,166.00
Costo - Beneficio	**S/ 327,140.00**	**-S/ 327,694.00**	**S/ 4,707,112.00**	**S/ 9,741,918.00**

Tabla 50: Flujo de caja del proyecto
Fuente: *Elaboración Propia*

La tabla expone el flujo de caja, el cual se proyecta para 3 meses. Además, se puede notar que durante el segundo mes se está previendo pérdidas económicas ante un ataque de ciberseguridad.

CONCLUSIONES

- La integración de las distintas tecnologías de seguridad y cumplimiento de normativas es más eficaz que el funcionamiento aislado de cada tecnología, además de que la falta de integración genera complejidades. Esta complejidad es la causa por la que la seguridad a menudo es una cuestión táctica, en lugar de estratégica y alineada con las prioridades de la entidad financiera.

- La entidad financiera llegó a la conclusión de que mediante el empleo de la plataforma SIEM junto con controles de endpoints, redes y checkers, podía mitigar los riesgos de forma más eficaz y evitar pérdidas económicas y de información.

- La solución SIEM es una herramienta de gran importancia para la seguridad, capaz de demostrar el cumplimiento de las normativas, garantizar la disponibilidad de los activos y, en definitiva, asegurar la continuidad del servicio y velar por la por la confidencialidad, integridad y disponibilidad de los diferentes activos de la información

- La entidad financiera redujo carga laboral, costos empresariales mensuales y logró economías de escala.

- Gracias a la implementación del SIEM Qradar se priorizó las alertas de seguridad, logrando que las investigaciones del SOC se focalicen en los incidentes sospechosos de alta probabilidad.

RECOMENDACIONES

- Se recomienda contratar un servicio gestionado de monitoreo de disponibilidad y seguridad 24x7 para una mejor gestión de eventos de seguridad debido a la alta experiencia que cuentan.

- Para un mejor aprovechamiento de la plataforma Qradar, se recomienda implementar la solución de análisis de comportamiento del usuario (IBM Qradar UBA).

- Se sugiere integrar los activos crítico-faltantes y también lo activos no críticos para un mejor control y monitoreo de seguridad.

- Se sugiere agregar reglas customizados para afinar el monitoreo de seguridad.

- Se recomienda integrar al SIEM una tecnología de monitoreo de base de datos para tener un mayor control de seguridad de data sensible que se maneja en la entidad.

BIBLIOGRAFÍA

Antonio Inoguchi, E. M. (2017). *Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las pymes en el Perú.* Lima.

Fernandez, J. (2019). *Implementación de un Security Information and Event Management (SIEM) en el comando de la armada nacional, tesis presentada para obtener Especialización en Seguridad Informática.* Bogotá.

GMV. (26 de 05 de 2016). *checker ATM Security*. Obtenido de https://www.gmv.com/DocumentosPDF/checker/Checker_ESP_26_05_2016.pdf

Guzmán, G. (2015). *Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica Ortega.* Huancayo.

IBM. (2019). *Installation Guide*. Obtenido de IBM Security QRadar: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_siem_inst.pdf

PMI. (2017). *La Guía del PMBOK 6ta Edición*. Obtenido de https://www.pmi.org.pe/

Scrum. (2020). *Scrum.org*. Obtenido de La guía de Scrum: https://www.scrum.org/