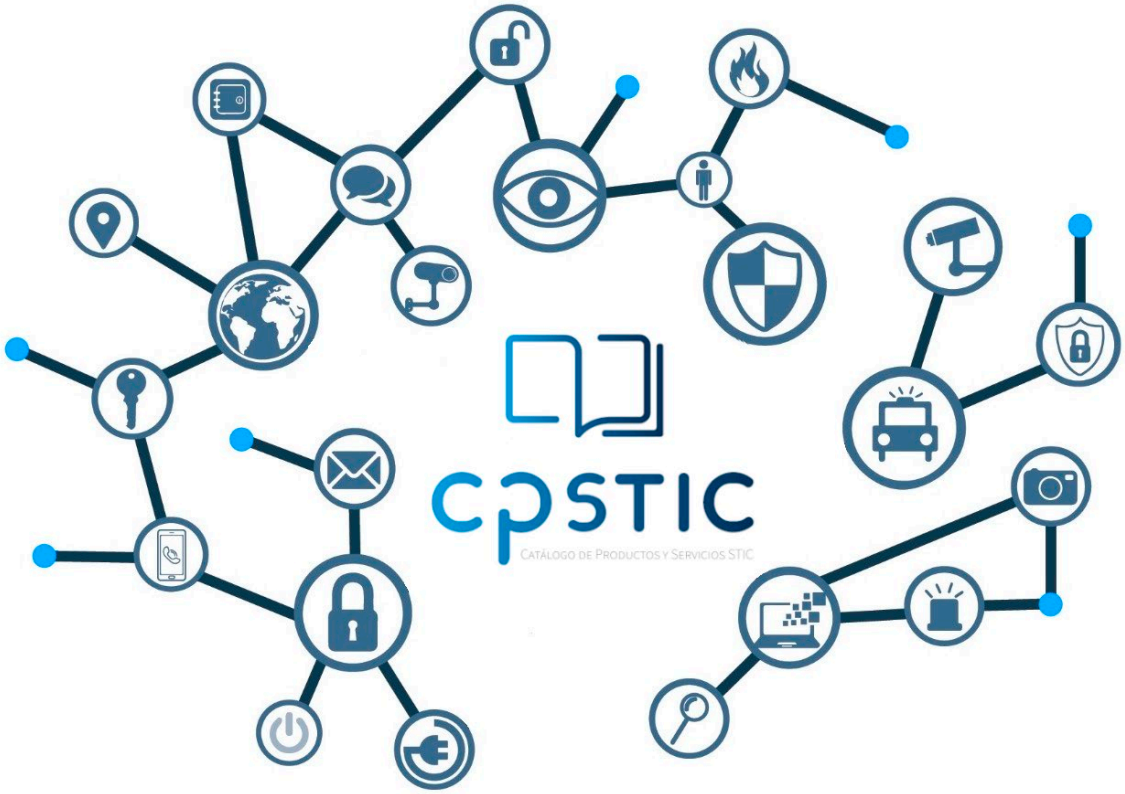
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1203

Procedimiento de empleo seguro
IBM QRadar *Security Intelligence Platform*



Enero de 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.02.01 12:36:18 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-038-0.
Fecha de Edición: enero de 2024.

ÍNDICE

1 INTRODUCCIÓN

1. *IBM QRadar Security Intelligence Platform*, también conocido *como IBM QRadar Security Information and Event Management* (SIEM), es una solución de gestión de la seguridad de la red, que proporciona un conocimiento global de la situación en cuanto a la seguridad, y da soporte a las necesidades de cumplimientos normativos. Para ello, utiliza una combinación de conocimientos basados en los flujos de red, la correlación de sucesos de seguridad procedentes de diversas fuentes de log, y la evaluación de vulnerabilidades de los activos.

2. Algunas de sus características principales son:

   a) Recolección de información de sucesos de seguridad (*Events*) y de flujos de red (*Flows*) que proporcionan información sobre el tráfico de red. Los sucesos se generan en las fuentes de sucesos (*firewalls*, *routers*, etc.) y se envían a QRadar. Los flujos de red se recogen haciendo uso de puertos SPAN. La principal diferencia entre los sucesos y los flujos es que los sucesos son acciones específicas en un momento determinado del tiempo, como un inicio de sesión de un usuario o una conexión VPN. Mientras que los flujos de red son conjuntos de datos de actividad de red que puede durar desde pocos segundos, hasta días, como la descarga de ficheros.

   b) Definición de reglas e infracciones (*Offenses*). El producto utiliza las reglas para monitorizar los sucesos y flujos en la red, y detectar amenazas a la seguridad. Cuando un suceso o flujo cumple las condiciones definidas en una regla, se crea una infracción para indicar que existe sospecha de ataque o de infracción de la política de seguridad.

   c) Actividad de logs. Permite monitorizar y visualizar los sucesos de seguridad producidos en la red en tiempo real, así como realizar búsquedas avanzadas.

   d) Actividad de la red. Permite investigar las sesiones establecidas entre los dispositivos de la red. Si la opción de capturar el contenido está habilitada, proporciona información sobre cómo se están estableciendo estas comunicaciones y qué se está comunicando a través del tráfico de red.

   e) *Profiling* de Activos. Permite crear de forma automática, perfiles de los activos detectados en la red. Estos perfiles proporcionan información de los activos, incluyendo qué servicios está ejecutando, lo cual se utiliza para propósitos de correlación, y ayuda a evitar falsos positivos.

   f) Generación de informes. Permite crear informes personalizados o utilizar informes predefinidos.

3. La siguiente imagen muestra el entorno para un *appliance "All-in-one*". Se trata de un despliegue en un solo dispositivo en el cual se ejecuta todo el software. La Consola QRadar proporciona la interfaz de usuario, las vistas de sucesos y flujos en tiempo

real, los informes, las infracciones, la información de activos y las funciones administrativas.

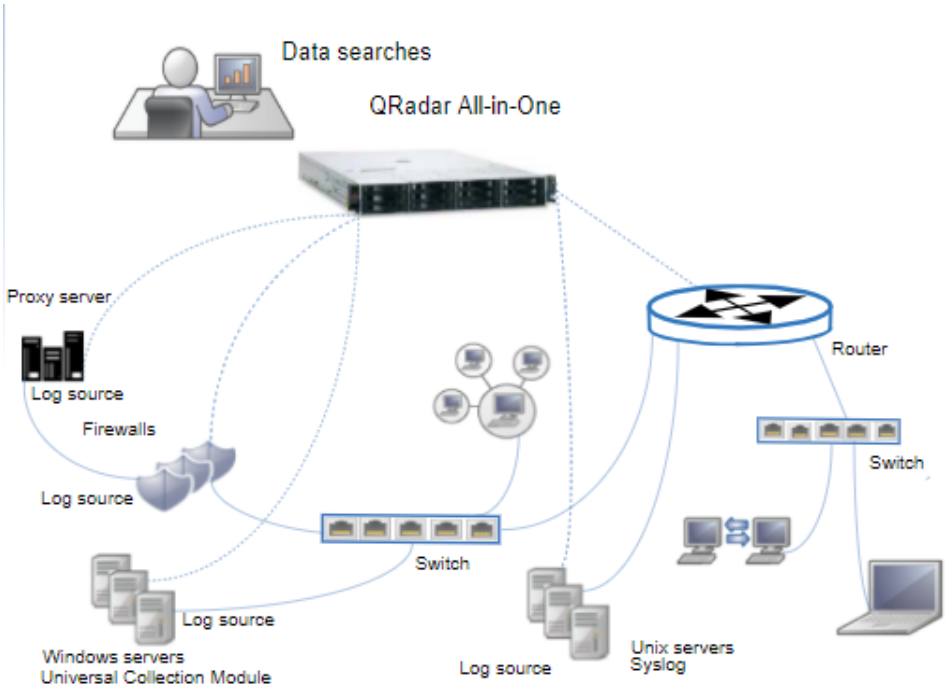


Ilustración 1-1. Entorno del dispositivo *"All-in-one"*

4. Las comunicaciones con los diferentes componentes de la red se realizan a través canales de comunicación protegidos por TLS, con autenticación a través certificados X509v3.
5. La administración del producto se puede llevar a cabo mediante GUI usando HTTPS o mediante CLI protegido por SSH.

2 OBJETO Y ALCANCE

7. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución ***IBM QRadar Security Intelligence Platform versión 7.5.***

8. El presente documento aplica al dispositivo "*All-in-one*" formado por:

    a) Modelo *hardware*: *IBM Model 3129,* con arquitectura x86 64 bit CPU.
    b) Versiones *software*: Sistema operativo *Red Hat RHEL 7.9* y *QRadar Security Intelligence Platform,* versión 7.5.

9. El producto mencionado en esta guía ha sido cualificado e incluido en el **Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC)** para categoría ALTA en la familia de "***Sistemas de Gestión de Eventos de Seguridad***". Se recomienda consultar el Catálogo para conocer la versión cualificada en cada momento.

3 ORGANIZACIÓN DEL DOCUMENTO

10. El documento se compone de los siguientes apartados:

    a) Apartado 4. En este apartado se recogen recomendaciones a tener en cuenta durante la fase previa a la instalación del producto.

    b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto

    c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

    d) Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

    e) Apartado 8.Incluye un listado de la documentación que ha sido referenciada a lo largo del presente documento.

    f) Apartado 9. Incluye un listado de las abreviaturas empleadas a lo largo del presente documento.

    g) ANEXO A. Incluye una tabla con los eventos auditables y ejemplos de estos.

    h) ANEXO B. Incluye una tabla con los distintos roles de usuarios disponibles.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

11. Tras la entrega del dispositivo, es necesario asegurarse de que no ha sido manipulado, lo que podría suponer un problema de seguridad. Para asegurarse de la autenticidad e integridad del producto, siga estos pasos:

    a) El número de seguimiento, número de pedido y número de serie obtenidos al realizar el pedido, deben coincidir con los incluidos en el producto recibido.

    b) Verificar que el paquete no ha sido dañado durante el transporte y que no tiene signos de haber sido abierto y/o manipulado.

    c) Los productos deben venir debidamente embalados, con su envoltorio sellado.

12. Posteriormente, se debe comprobar que el hardware coincide con el acordado. Esto se debe confirmar en las etiquetas del producto.

13. El hardware no contiene el software instalado, por lo que debe realizarse la descarga e instalación manualmente. La descarga del *software* de QRadar se realiza **a través de la página web de Fixcentral** (https://www.ibm.com/support/fixcentral/). Seleccionar el fichero .iso correcto de QRadar Security Intelligence Platform, versión **7.5.**

14. Junto al enlace de descarga del fichero .iso, se encuentra un fichero con su *hash* SHA256. Tras descargar el fichero, realizar el *hash* SHA256 y comprobar que coincide con el publicado en la página, para verificar la integridad del fichero descargado.

1.

Ilustración 4-1. *Hash* instalador QRadar.

15. En un sistema operativo Red Hat Linux, se puede obtener el *hash* SHA256 del fichero con el siguiente comando:

    sha256sum <QRadar>.iso

5 FASE DE INSTALACIÓN

16. Para la instalación en el *appliance* no es necesario configurar el sistema operativo RHEL, ya que este viene incluido en el fichero .iso de QRadar.
17. Una vez descargado el fichero de la página web de *Fixcentral* (https://www.ibm.com/support/fixcentral) y verificada la integridad del mismo, crear un USB de arranque siguiendo los pasos descritos en el capítulo *USB flash drive installations* de la guía *IBM Security QRadar Version 7.5 – Installation Guide* [REF2].
18. Para iniciar la instalación, introducir el USB de arranque en el puerto USB del *appliance*. Cuando se muestre el menú de *Red Hat Enterprise Linux*, seleccionar una de las siguientes opciones:
    a) Si se ha conectado un monitor y un teclado, seleccionar ***Install Red Hat Enterprise Linux 7.9***.
    b) Si se ha conectado mediante una conexión serial, seleccionar ***Install Red Hat Enterprise Linux 7.9 using Serial console without format prompt*** o ***Install Red Hat Enterprise Linux 7.9 using Serial console with format prompt***.
19. Escribir *SETUP* para iniciar la instalación de QRadar. Seguir los siguientes pasos:
    a) Cuando se muestre el mensaje de inicio de sesión, introducir *root* como usuario y *password* como contraseña. Aceptar el "acuerdo de licencia de usuario final" (*End User License Agreement)*.
    b) Seleccionar el tipo de *appliance*: *Appliance Install,* en caso de una instalación *stand-alone* o *High Availability Appliance*, en caso de instalación en alta disponibilidad *(*ver apartado 6.14 ALTA DISPONIBILIDAD).
    c) Seleccionar la funcionalidad ***"All-In-One" Console***.
    d) Seleccionar el tipo de instalación: ***Normal Setup (default)***, en caso de una instalación *stand-alone* o *HA Recovery Setup,* en caso de una instalación en alta disponibilidad.
    e) Seleccionar la versión del protocolo IP: *ipv4* o *ipv6*.
    f) Seleccionar la interfaz de gestión.
    g) Introducir una dirección IP estática.
    h) Introducir una nueva contraseña para la cuenta *root*. Esta contraseña sustituye a la contraseña "password" utilizada para iniciar el proceso de instalación. El usuario *root* se utilizará para el acceso y configuración inicial mediante CLI, conectando con SSH.
    i) Introducir la contraseña para el usuario *admin*. **Con la cuenta *admin* se llevará a cabo el acceso y la configuración de usuarios y características iniciales del producto a través de la GUI.**

j) Hacer clic en *Finish*.

20. Para las contraseñas de los usuarios *root* y *admin*, deberá seguirse la política de contraseñas definida en el apartado 6.3.5.
21. Una vez realizada la instalación, se puede verificar la versión del *software* siguiendo los siguientes pasos:
    a) Para comprobar la versión del *software* instalada, iniciar sesión en la Consola QRadar.
    b) Desde el menú de navegación, seleccionar *Help > About.*
    c) La versión del *software* se muestra en la ventana *Help*.
    d) También puede comprobarse la versión del *software* ejecutando el siguiente comando:

sudo /opt/qradar/bin/myver –v

5.1 CREACIÓN DEL USUARIO ADMINISTRADOR

22. Una vez finalizado el proceso de instalación, se recomienda dejar de utilizar el usuario *root* para la gestión del producto mediante CLI.
23. El su lugar, crear un usuario *administrador* con acceso al comando *sudo* (se trata de una utilidad de los sistemas operativos basados en Unix que permite a los usuarios ejecutar programas y comandos con los privilegios del usuario *root* de forma segura), para poder realizar tareas administrativas mediante CLI.
24. Para crear el usuario utilizar los siguientes comandos:

useradd –c 'Admin User' –d /home/administrador –m –s /bin/bash administrador

psswd administrador

25. La contraseña deberá seguir la política de contraseñas definida en el apartado 6.3.5
26. Para dar acceso al comando sudo al usuario, editar el fichero */etc/sudoers*:
    a) Añadir al final del fichero:

Administrador ALL=(ALL) ALL

    b) Comentar con "#" todas las líneas que contengan *NOPASSWD*.

5.2 INSTALACIÓN CLAVES DE LICENCIA

27. Para instalar las claves de licencia:
    a) Iniciar sesión en la GUI de QRadar como usuario *admin,* con las credenciales creadas en el proceso de instalación:

https://<Direccion_IP_QRadar>

b) En el menú de navegación ir a *Admin > System Configuration > System and License Management*. De la lista desplegable seleccionar *Upload License* y subir la licencia.

c) Una vez subida la licencia, es necesario asignarla al sistema. Seleccionar la licencia no asignada y hacer clic en *Allocate System to License*. De la lista de sistemas, seleccionar el deseado y pulsar *Allocate System to License*.

6 FASE DE CONFIGURACIÓN

6.1 DESPLIEGUE DE CAMBIOS EN LA CONFIGURACIÓN

28. Al realizar cambios en la configuración de QRadar, utilizando la GUI, estos se guardan en un área de transferencia mientras no se hayan aplicado. Se activará un *banner* de despliegue de la pestaña *Admin* indicando que es necesario desplegar los cambios. Generalmente, los cambios requieren un reinicio de los servicios afectados.

29. QRadar dispone de dos (2) métodos para desplegar los cambios en el sistema: *Deploy Changes* y *Deploy Full Configuration*.

    a) En el proceso de ***Deploy changes***, sólo los servicios que requieren actualización son reiniciados en los *appliances*. En esta opción no se reinicia nunca, por ejemplo, el servicio "*Event Collection*", por lo que la recolección o el procesamiento de sucesos continúan funcionando.

    b) En el proceso de ***Deploy Full Configuration*** se envía una petición para reconstruir todos los ficheros de configuración del sistema. Cada *appliance* tiene su propio archivo de configuración y todos los servicios son reiniciados para asegurarse que la nueva configuración es cargada. Todos los procesos de recolección y procesamiento son reiniciados.

30. Se recomienda usar, cuando sea posible, el despliegue de cambios mediante ***Deploy Changes***, utilizando *Deploy Full Configuration* solo cuando sea necesario, para los cambios en la arquitectura y las licencias.

31. Ejemplos de cambios que requieren *Deploy Full Configuration*:

    a) Añadir o eliminar un dispositivo.

    b) Añadir, eliminar o editar los valores de un *Event Collector* o *Event Processor*.

    c) Añadir o actualizar una licencia.

    d) Añadir o eliminar el cifrado para un dispositivo gestionado.

32. Ejemplos de cambios para los que es suficiente un Deploy Changes:

    a) Añadir o editar un nuevo usuario o rol.

    b) Añadir o actualizar la jerarquía de red.

    c) Añadir nuevos perfiles de seguridad.

    d) Crear un *token* de servicio.

    e) Añadir una nueva fuente de log.

    f) Cambio de contraseñas.

33. A lo largo del documento, cuando se indique que se deben desplegar los cambios realizados, seleccionar el método más adecuado según lo indicado en este apartado.

6.2 AUTENTICACIÓN

34. QRadar permite la autenticación local y remota de usuarios. La autenticación local se utiliza por defecto y hace uso de credenciales de usuario/contraseña para permitir el acceso.

35. En el caso de los usuarios con permisos de administrador, si se habilita la autenticación remota, debe mantenerse también la autenticación local. De tal forma que si la autenticación remota falla, los usuarios con permisos de administrador puedan acceder al sistema.

36. Cuando se habilite la autenticación remota, los usuarios sin permisos de administración no podrán autenticarse en el sistema de forma local si esta falla.

37. Se soportan los siguientes tipos de autenticación remota de usuarios:

    a) **Autenticación RADIUS**. Se autentica a los usuarios a través de un servidor RADIUS. Cuando un usuario intenta iniciar sesión, QRadar cifra la contraseña y envía el nombre y la contraseña al servidor para la autenticación.

    b) **Autenticación TACACS**. Se autentica a los usuarios a través de un servidor TACACS. Cuando un usuario intenta iniciar sesión, QRadar cifra el nombre de usuario y la contraseña y los envía al servidor para la autenticación.

    c) **LDAP.** Los usuarios se autentican a través de un usuario LDAPS nativo o Directorio Activo de Microsoft

    d) **Autenticación "*single sign-on*" SAML.** Se puede integrar QRadar con el servidor de autenticación de la organización, eliminando la necesidad de mantener usuarios locales en QRadar. Los usuarios que inician sesión en el servidor de autenticación pueden entrar en QRadar sin necesidad de mantener contraseñas o credenciales separadas.

38. En el capítulo *User Authentication* de la guía *IBM Security QRadar Version 7.5 – Administration Guide* [REF1] se encuentran detallados los diferentes tipos de autenticación y cómo configurarlos.

6.3 ADMINISTRACIÓN

6.3.1 ADMINISTRACIÓN REMOTA

39. La administración remota de QRadar mediante CLI, se lleva a cabo conectando con SSH (ver apartado 6.5.1 CONFIGURACIÓN DE SSH), utilizando preferentemente la cuenta *administrador* creada en el proceso de instalación (ver apartado 5.1 CREACIÓN DEL USUARIO ADMINISTRADOR).

40. La administración remota de QRadar mediante la interfaz Web GUI, está protegida por HTTPS/TLS1.2 (ver apartado 6.5.2 CONFIGURACIÓN TLS DEL SERVIDOR WEB). Para acceder a esta GUI, introducir en el navegador la dirección *https://<Direccion IP QRadar>* e iniciar sesión con la cuenta *admin* creada durante la instalación de la solución (ver apartado 5 FASE DE INSTALACIÓN).
41. A lo largo del documento, cuando no se especifique que una configuración se realiza mediante SSH, se utilizará la GUI.
42. En el capítulo *Supported web browsers* de la guía *IBM Security QRadar Version 7.5 – Administration Guide* [REF1] se encuentran los distintos navegadores web soportados y sus respectivas versiones.

6.3.2 PERFILES DE SEGURIDAD

43. QRadar permite crear perfiles de seguridad que definen a qué redes, fuentes de sucesos y dominios pueden acceder los usuarios. Existe un perfil de seguridad para usuarios administradores definido por defecto que tiene acceso a todos los recursos.
44. **Se recomienda crear los perfiles de seguridad, junto a los roles de usuario, antes de la creación de cuentas de usuarios para delimitar correctamente a qué datos tienen acceso los distintos usuarios.**
45. La prioridad de permiso determina qué sucesos y flujos puede ver el usuario. Pueden definirse las siguientes prioridades de permiso:
    a) ***No Restrictions***: Esta opción no aplica restricciones sobre los sucesos que se visualizan.
    b) ***Network Only***: Esta opción hace que el usuario pueda ver solamente los sucesos y flujos que están asociados con las redes especificadas en el perfil de seguridad.
    c) ***Log Sources Only***: Esta opción hace que el usuario pueda ver solamente los sucesos que están asociados con las fuentes de sucesos especificadas en el perfil de seguridad.
    d) ***Networks AND Log Sources***: Esta opción hace que el usuario pueda ver solamente los sucesos y flujos asociados con las fuentes de sucesos y las redes especificadas en el perfil de seguridad.
    e) ***Networks OR Log Sources***: Esta opción hace que el usuario pueda ver los sucesos y flujos que están asociados con las fuentes de sucesos o las redes especificadas en el perfil de seguridad.
46. Para visualizar las alertas por infracciones de políticas o sospechas de ataque, se aplica siempre el permiso "*Networks OR Log Sources*".
47. Para crear un perfil de seguridad seguir los siguientes pasos:

a) Ir a la pestaña *Admin > System Configuration > User Management > Security Profiles*.

b) En la barra de herramientas *Security Profile Management window* hacer clic en *New*.

c) Introducir un nombre en el campo *Security Profile Name*.

d) En la pestaña *Permission Precedence* elegir la prioridad de permiso.

e) Escoger las redes, fuentes de sucesos y dominios a los que puede acceder el perfil de seguridad y hacer clic en *Save*.

f) Desplegar los cambios.

48. En el capítulo *Security profiles* de la guía *IBM Security QRadar Version 7.5 – Administration Guide* [REF1] se encuentra detallado el procedimiento para crear, editar y eliminar perfiles de seguridad.

6.3.3 CUENTAS Y ROLES DE USUARIOS

49. Durante la instalación de QRadar se definen dos roles de usuario por defecto, *Admin* y *All*. **Se recomienda definir roles de usuarios con permisos específicos antes de crear usuarios.**

50. Para crear un rol de usuario seguir los siguientes pasos:

a) Ir a *Admin > System Configuration > User Management > User Roles*.

b) Hacer clic en *New*.

c) En el campo *User Role Name* asignar un nombre único al rol.

d) Seleccionar los permisos para el rol de usuario. Los diferentes permisos que se pueden asignar a los roles se encuentran descritos en ANEXO B – ROLES DE USUARIO. En el área de *Dashboards*, seleccionar aquellos paneles de control a los que debe poder acceder el rol de usuario.

e) Hacer clic en *Save*.

f) Desplegar los cambios.

51. **Se deben crear roles de usuario que se ajusten a las tareas que desempeñarán los diferentes usuarios, limitando de esta forma las tareas que pueden realizar a las mínimas indispensables para desempeñar el trabajo.**

52. Cuando se crea una cuenta de usuario, deben asignarse credenciales, un rol de usuario y un perfil de seguridad al usuario. Los **roles de usuario** definen las acciones que un usuario tiene permiso para realizar, mientras que los **perfiles de seguridad** definen a qué datos pueden acceder los usuarios.

53. Para crear un usuario local, seguir los siguientes pasos:

a) Ir a *Admin > User Management > Users*.

b) Hacer clic en *Add*.

c) Introducir los valores de los siguientes parámetros:

- *User Name*: Nombre de usuario único.
- *User description*: Descripción del usuario.
- *Email*: Dirección de email asociada al usuario.
- *New Password*: Introducir la contraseña del usuario. Debe cumplir con la política de contraseñas definida. Los usuarios deberán cambiar la contraseña tras su primer acceso.
- *Confirm New Password*: Repetir la contraseña del usuario.
- *User Role*: Seleccionar un rol de usuario de la lista.
- *Security Profile*: Seleccionar un perfil de seguridad desde la lista.

d) Hacer clic en *Save*.

e) Cerrar la ventana de *User Management*.

f) Desplegar los cambios.

6.3.4 SEGMENTACIÓN EN DOMINIOS

54. Segmentar la red en diferentes dominios puede ayudar a asegurar que la información solo se encuentra disponible para aquellos usuarios que la necesitan para desempeñar sus funciones. QRadar permite asignar los dominios a los distintos perfiles de seguridad, como se ha visto en el anterior apartado, de forma que se limita la información disponible para un grupo de usuarios dentro de un dominio.
55. También se pueden usar los dominios para gestionar las direcciones IP solapadas, en aquellos casos en que la organización conste de diferentes redes. Creando dominios para representar cada red, dispositivos en distintos dominios pueden tener asignada la misma dirección IP y seguir siendo tratados como dispositivos separados.
56. Para crear un dominio seguir los siguientes pasos:

a) Ir a *Admin > System Configuration > Domain Management.*

b) Para añadir un dominio, pulsar *Add* y escribir un nombre exclusivo para el dominio y una descripción.

c) Pulsar la pestaña correspondiente al criterio de dominio que se vaya a definir:

- Para definir el dominio basado en una propiedad personalizada, grupo de fuentes de sucesos, fuentes de sucesos o recopiladores de sucesos, pulsar la pestaña *Events*.
- Para definir el dominio basado en un origen de flujos o un recopilador de flujos, pulsar la pestaña *Flows*.
- Para definir el dominio basado en un escáner de vulnerabilidades, pulsar la pestaña *Scanners*.

d) Para asignar una propiedad personalizada a un dominio:

- Ir al recuadro *Capture Result*.
- Escribir la expresión regular que hará de filtro para la propiedad.

e) En la lista, seleccionar el criterio del dominio y pulsar Add.

f) Pulsar Create.

57. QRadar permite configurar reglas de creación de alertas de ataques e infracciones de seguridad para dominios concretos, ajustando el campo And *Domain Is* de dichas reglas.
58. El detalle de la configuración de dominios en QRadar se puede consultar en el capítulo *Domain segmentation* de la guía *IBM Security QRadar Version 7.5 – Administration Guide* [REF1].

6.3.5 POLÍTICA DE CONTRASEÑAS DE USUARIOS LOCALES

59. QRadar permite configurar la política de contraseñas para las cuentas de usuario locales. Si se modifica o configura por primera vez la política de contraseñas, el sistema pide a todos los usuarios cuya contraseña no cumpla con esta, que la cambien la primera vez que inician sesión después de la actualización.
60. Cuando sea posible, se recomienda alinear las políticas de contraseñas de los métodos de autenticación remotos, con la política de contraseñas local.
61. Se debe configurar una **política de contraseñas** para que cumplan, al menos, los siguientes requisitos:

a) Un mínimo de 12 caracteres (parámetro *Minimum Password Length)*

b) No usar palabras que puedan encontrarse en diccionarios.

c) Utilizar, al menos 3 de estos 4 grupos: letras mayúsculas, minúsculas, caracteres alfanuméricos y caracteres especiales como “!”,“@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“ y “) (parámetros *Contain an uppercase character , Contain an lowercase carácter, Contain a digit*, *Contain a special carácter y Use Complexity Rules).*

d) No deberá permitirse la repetición de, al menos, las 5 últimas contraseñas utilizadas (parámetro *Unique password count*).

e) El valor recomendado para la vigencia y expiración de contraseñas no debe superar los 6 meses (parámetro *Days before password will expire).*

f) No deberá realizarse un nuevo cambio de contraseña en los 4 días posteriores al último cambio.

62. Para configurar la política de contraseñas para los usuarios locales, seguir los siguientes pasos:

a) *Admin > System Configuration > User Management > Authentication.*

b) Hacer *clic* en *Local Password Policy Configuration*.

c) Especificar la configuración de la política, los valores disponibles son:

- ***Minimum Password Length***: Especifica el número mínimo de caracteres que debe tener una contraseña.
- ***Use Complexity Rules***: Requiere que las contraseñas cumplan varias reglas de complejidad, por ejemplo, contener caracteres en mayúscula, minúscula, caracteres especiales y números.
- ***Number of rules required***: El número de reglas de complejidad que deben cumplir las contraseñas. Debe estar entre uno y el número de reglas habilitadas.
- ***Contain an uppercase character***: Habilita la regla que requiere que las contraseñas contengan, al menos, un carácter en mayúsculas.
- ***Contain a lowercase character***: Habilita la regla que requiere que las contraseñas contengan, al menos, un carácter en minúsculas.
- ***Contain a digit***: Habilita la regla que requiere que las contraseñas contengan, al menos, un número.
- ***Contain a special character***: Habilita la regla que requiere que las contraseñas contengan, al menos, un carácter especial.
- ***Not contain repeating characters***: Habilita la regla que no permite más de dos caracteres repetidos. Por ejemplo, *abbc* está permitido, pero *abbbc* no.
- ***Password History***: Impide que las contraseñas se reutilicen durante un número de días. El número de días se calcula multiplicando los valores *Unique password count* por *Days before password will expire*.

- ***Unique password count***: El número de cambios de contraseña antes de poder reutilizar una contraseña anterior.
- ***Days before password will expire***: El número de días antes de que se deba cambiar una contraseña.

d) Hacer clic en *Update Password Policy.*

63. El detalle de la configuración de políticas de contraseñas se puede consultar en el capítulo *Configuring system authentication* de la guía *IBM Security QRadar Version 7.5 – Administration Guide* [REF1].

6.4 PARÁMETROS DEL SISTEMA

64. En QRadar se pueden configurar, desde la sección *Admin > System Configuration > System Settings*, varios parámetros relacionados con funciones de seguridad del producto. Para configurar los ajustes del sistema, seguir los siguientes pasos:

a) Ir a la pestaña *Admin*.

b) En la sección *System Configuration*, hacer clic en *System Settings.*

c) Configurar los ajustes del sistema.

d) Hacer clic en *Save*.

e) Desplegar los cambios.

65. En la pestaña *Ariel Database Settings*, se recomienda configurar los siguientes parámetros:

a) ***Hashing Algorithm***: Determina el algoritmo de hash utilizado en el apartado 6.4.3 INTEGRIDAD DE LOS DATOS. La función hash que se debe utilizar es SHA-256 o superior. Se recomienda activar el parámetro *HMAC Encryption* y seleccionar SHA-256, SHA-384 o SHA-512.

66. En la pestaña *SNMP Settings*, se recomienda configurar los siguientes parámetros:

a) ***SNMP Version***: Indica la versión de SNMP que usará QRadar. Se debe desactivar esta opción si no se desea usar SNMP. En caso de ser necesario el uso de SNMP, se debe configurar **versión 3 (SNMPv3)**.

67. En la pestaña *Authentication Settings*, se recomienda configurar los siguientes parámetros:

a) ***Persistent Session Timeout (in days):*** Cantidad de tiempo en días que se mantiene una sesión de usuario. Se configurará este valor para establecer un tiempo máximo en días mayor que 0 (se recomienda 1).

b) ***Inactivity Timeout (in minutes):*** Cantidad de tiempo en minutos antes de que QRadar cierre la sesión de usuario. Un valor '0' indica que la sesión

permanecerá activa mientras la ventana de exploración siga abierta. Por tanto, se recomienda introducir un valor lo más bajo posible.

c) ***Allow Logon Password Autocomplete***: El auto completado es una característica proporcionada por los navegadores que recuerda y rellena automáticamente los formularios de inicio de sesión. QRadar permite activar y desactivar esta característica en su página de *login*. Se debe mantener esta opción desactivada para aumentar la seguridad de las credenciales y evitar inicios de sesión no deseados.

d) ***Display Login History:*** Cuando se encuentra activado, se muestra al usuario el historial de inicio de sesión, que contiene la fecha y hora del último inicio de sesión correcto y el número de inicios de sesión erróneos desde que se cerró por última vez sesión. Se recomienda activar esta opción.

e) ***Concurrent Login Limit (all hosts):*** Introducir el número de sesiones activas que un usuario puede mantener abiertas simultáneamente. Se debe configurar este ajuste con un valor de 1 para prevenir que QRadar autentique al mismo usuario más de una vez.

68. Para evitar la modificación no deseada de los ficheros de configuración, se recomienda desactivar las actualizaciones automáticas de los ficheros de configuración:

    a) Ir a *Admin > System Configuration > Auto update*.

    b) Hacer clic en *Change settings*.

    c) En la sección *Update types* bajo *Configuration updates*, cambiar *Update type* a *Disable*.

6.4.1 LOGIN BANNER

69. Se debe configurar un mensaje de aviso y consentimiento (***Login banner***) que el usuario debe aceptar antes de iniciar sesión:

    a) Ir a *Admin > System Configuration > System Settings* y hacer *clic* en *Authentication Settings*.

    b) Para editar el mensaje del banner hacer clic en *Edit*, en el campo *Login Message.*

    c) Escribir el mensaje del banner en la ventana *Edit Login Message*.

    d) Para forzar a los usuarios a aceptar esta política antes de poder iniciar sesión, activar la casilla.

    e) Hacer clic en *Save*.

    f) Desplegar los cambios.

6.4.2 PARÁMETROS DE SESIÓN

70. A continuación, se indica cómo configurar los parámetros de sesión más relevantes.
71. Se recomienda configurar un número máximo de intentos fallidos de autenticación, tras el cual la cuenta de usuario se bloqueará**. El número máximo de intentos fallidos de autenticación no debe ser superior a cinco (5) intentos**.
72. Para configurar el bloqueo de las cuentas de usuario seguir los siguientes pasos:
    a) Ir a *Admin > System configuration > Authentication settings.*
    b) En el campo *Maximum Login Attemts,* especificar el número de inicios de sesión erróneos que pueden llevarse a cabo antes del bloqueo de la cuenta.
    c) En el campo *Login Failure Attempt Window (in minutes)* especificar el periodo de tiempo en minutos en el cual deben suceder los fallos de inicio de sesión.
    d) En el campo *Login Failure Block Time (in minutes)* especificar el tiempo que permanece bloqueada la cuenta.
    e) Desplegar los cambios.
73. Cuando se da el número indicado de fallos de inicio de sesión dentro del tiempo especificado (*Login Failure Block Time)*, la cuenta de usuario se bloquea. El desbloqueo debe realizarse, siempre que sea posible, a través de acción del administrador.
74. Deberá configurarse un **periodo de inactividad de sesión remota**, tras el cual expire la sesión del usuario remoto y sea necesario volver a iniciar sesión:
    a) En la pestaña *Admin > System Configuration > System Settings hacer clic en Authentication Settings.*
    b) En el campo *Inactivity Timeout* especificar el número de minutos de inactividad antes de que QRadar cierre la sesión de un usuario.
    c) Hacer clic en *Save*.
    d) Desplegar los cambios.
75. Deberá configurarse un **periodo de inactividad de sesión local**, tras el cual expire la sesión del usuario local y sea necesario volver a iniciar sesión:
    a) Usar SSH para iniciar sesión en la Consola de QRadar.
    b) Ir al fichero de configuración ubicado en */etc/profile.*
    c) Cambiar el valor de TMOUT al número de segundos tras se cerrará la sesión de los usuarios.
    d) Guardar el fichero.

6.4.3 INTEGRIDAD DE LOS DATOS

76. Cuando se encuentra activada la opción *log hashing* todos los sistemas que registran datos de sucesos y flujos, crean ficheros *hash* de los datos recolectados para poder verificar posteriormente su integridad.

77. Se recomienda activar la opción ***log hashing*** desde la pestaña de configuración del sistema, *Admin > System Configuration > System Settings.*

78. Para verificar la integridad de los datos, se deben seguir los siguientes pasos:

    a) Usar SSH para iniciar sesión en QRadar como administrador.

    b) Escribir el siguiente comando. En la tabla se detallan los diferentes parámetros que acepta el comando:

        - */opt/qradar/bin/check_ariel_integrity.sh –d <duración> -n <nombre base datos> [-t <tiempo finalización>] [-a <algoritmo de hash>] [-r <directorio raíz del hash>] [-k <clave hmac>]*

Parámetro	Descripción
-d	Longitud en minutos de los datos del archivo de registro a explorar. Es el periodo de tiempo que precede inmediatamente a la hora final especificada mediante el parámetro –t. Por ejemplo, si se especifica –d 5, se exploran todos los datos de registro recopilados cinco minutos antes de la hora final –t.
-n	La base de datos de QRadar a explorar. Las opciones válidas son Sucesos y Flujos.
-t	La hora final de la exploración. El formato de la hora final es aaaa/mm/dd hh:mm, con HH especificado en formato de 24 horas. Si no se especifica hora final, se utiliza la hora actual.
-a	Algoritmo hash a utilizar. Este algoritmo debe ser el mismo que se utilizó para crear los hashes. Si no se especifica ningún algoritmo, se utiliza SHA-1.
-r	La ubicación de los ficheros hash. Este argumento solo es necesario cuando estos ficheros no están en la ubicación especificada en el archivo de configuración */opt/qradar/conf/arielConfig.xml*
-k	La clave utilizada para el cifrado HMAC. Si no se especifica ninguna clave y el sistema está habilitado para el cifrado HMAC, el *script* toma de forma predeterminada la clave especificada en los valores del sistema.

79. Si se devuelve un mensaje de *ERROR* o *FAILED*, el valor *hash* generado de los datos actualmente guardados no coincide con el valor *hash* creado cuando los datos se guardaron.

6.4.4 IMB X-FORCE

80. QRadar permite la integración con **IMB X-Force**. Se trata de un conjunto de datos globales formados por muestras de *malware*, análisis de páginas web y URLs y análisis de direcciones IP maliciosas.
81. Activar la integración del intercambio de datos con **X-Force** permite detectar amenazas en el entorno de la organización antes de que amenacen la estabilidad de la red.
82. Para activar ***X-Force Thread Intelligence*** seguir los siguientes pasos:
    a) Ir a la pestaña *Admin*.
    b) En la sección *System Configuration*, hacer clic en *System Settings.*
    c) Seleccionar Yes en el campo *Enable X-Force Thread Intelligence F*eed.
83. El detalle de la configuración de *IBM X-Force* se puede consultar en el capítulo *IBM X-Force integration* de la guía *IBM Security QRadar Version 7.5 – Administration Guide* [REF1].

6.5 PROTECCIÓN DE LAS COMUNICACIONES

84. La administración remota de QRadar se realiza a través del protocolo SSH para la administración CLI y a través de HTTPS/TLS1.2 para el GUI.
85. Las comunicaciones internas entre los dispositivos gestionados de QRadar se protegen mediante SSH (ver apartado 6.9 DISPOSITIVOS GESTIONADOS).
86. Las comunicaciones con las fuentes de eventos (*log sources*) y con los destinos de reenvío (*forwarding destination*) utilizarán el protocolo TLS *Syslog* con TLS 1.2 siempre que la fuente o destino lo permitan.
87. En el apartado 6.6 GESTIÓN DE CERTIFICADOS se detalla la instalación de los certificados necesarios para las comunicaciones descritas.

6.5.1 CONFIGURACIÓN DE SSH

88. Se debe configurar SSH para que solo acepte autenticación de clave pública RSA. Para ello:
    a) El equipo o *workstation* que utilizaremos para la administración remota, debe disponer de una pareja de claves pública/privada RSA. Se deben utilizar claves de longitud, al menos, 3072 bits.
    b) Copiar la clave pública del equipo o *workstation* en la carpeta *~/.ssh/authorized_keys* del *appliance*.
    c) Repetir este punto para cada equipo o *workstation* que vayamos a usar para la administración remota SSH de QRadar.

d) En la línea de comandos del *appliance* editar el fichero */etc/ssh/sshd_config.*

- Establecer *PubkeyAuthentication* a *Yes*.
- Establecer *PasswordAuthentication* a *No*.
- Descomentar la línea de *HostKey* que hace referencia a la clave RSA. Dejar el resto de las líneas comentadas.

  HostKey /etc/ssh/ssh_host_rsa_key

- Reiniciar el servicio SSHD introduciendo el comando:

  service sshd restart

89. Se recomienda configurar SSH para usar AES en modo CRT o GCM para cifrado, y como método de intercambio de clave algunas de las siguientes *suites*:

a) ecdh-sha2-nistp256

b) ecdh-sha2-nistp384

c) ecdh-sha2-nistp521

d) diffie-hellman-group16-sha512

e) diffie-hellman-group17-sha512

diffie-hellman-group18-sha512

90. Para ello:

a) Editar el fichero */etc/ssh/sshd_config.*

- Al final del fichero, comprobar que la línea Ciphers y KeyAlgorithms contienen lo siguiente:

  Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com, aes256-ctr,aes192-ctr,aes128-ctr

  KexAlgorithms ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group16-sha512,diffie-hellman-group17-sha512 ,diffie-hellman-group18-sha512

b) Reiniciar el servicio SSHD introduciendo el comando:

service sshd restart

91. Las claves de las sesiones SSH están configuradas para regenerarse tras una hora o un intercambio de 1Gb de datos, lo que suceda primero. Esta configuración no puede cambiarse.

6.5.2 CONFIGURACIÓN TLS DEL SERVIDOR WEB

92. Deberán configurarse las TLS *cipher suites* que se usarán en el servidor web http (Apache) para las conexiones de los usuarios con la interfaz GUI, de tal forma que se **permitan solo los cipher suites aprobados por el CCN-STIC-807**:

    a) Ir al fichero */etc/httpd/conf.d/ssl.conf* y comprobar que la línea de texto *SSLCipherSuite* contiene lo siguiente:

    SSLCipherSuite ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384

    b) Escribir el siguiente comando para reiniciar el servicio:

    service httpd restart

6.5.3 CONFIGURACIÓN TLS DE JAVA

93. QRadar utiliza la seguridad de Java para todas las comunicaciones seguras TLS con otros dispositivos (dispositivos gestionados y destinos de reenvío).

94. Deberán excluirse las *cipher suites* inseguras de TLS, de la política de seguridad de Java. Para ello:

    a) Escribir el siguiente comando:

    sudo cp /opt/ibm/java-x86_64-80/jre/lib/security/policy/unlimited/local_policy.jar /opt/ibm/java-x86_64-80/jre/lib/security/

    b) Editar el fichero de configuración de java ubicado en /opt/ibm/java-x86_64-80/jre/lib/security/java.security y reemplazar la línea de texto:

    *jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, RC4, DES, MD5withRSA, DH keySize < 1024, DESede, *

    EC keySize < 224, 3DES_EDE_CBC, anon, NULL, DES_CBC

    por

    *jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, RC4, DES, MD5withRSA, DH keySize < 3072, DESede, *

    EC keySize < 224, 3DES_EDE_CBC, anon, NULL, DES_CBC

    c) Por último, reiniciar el *appliance*.

6.6 GESTIÓN DE CERTIFICADOS

95. Para llevar a cabo la autenticación de servidor cuando los usuarios se conecten a QRadar mediante HTTPS, es necesario instalar en QRadar un certificado SSL de servidor. Por defecto, QRadar dispone de un certificado autofirmado, que deberá sustituirse por **un certificado emitido por una autoridad de certificación (CA) de confianza.** A su vez, el certificado raíz de la CA emisora (*root* CA) deberá instalarse en todos los equipos de usuario para que confíen en el certificado del servidor.

96. En las conexiones mediante TLS con otros componentes, cuando sea posible, QRadar utiliza autenticación mutua. Los componentes con los que se comunica que deberán disponer de un certificado son:

    a) Fuente de sucesos (*Log sources*). Actúan como cliente TLS.

    b) Destino de reenvío (*forwarding destination*). Actúan como servidor TLS.

97. Con las fuentes de sucesos, QRadar actuará como servidor TLS. Con los destinos de reenvío, QRadar actuará como cliente TLS. Será necesario instalar el certificado CA *root* de la CA emisora del certificado de QRadar en los componentes con los que se comunique. Del mismo modo, los certificados raíz de las CAs emisoras de los certificados de los componentes, deberán ser instalados en QRadar.

98. A continuación, se indican los aspectos para tener en cuenta a la hora de instalar y configurar los certificados.

6.6.1 CREAR UNA PETICIÓN CSR

99. QRadar permite crear peticiones CSR (*Certificate Signing Request*), para enviar a una CA. Para ello:

    a) Iniciar sesión en QRadar mediante un cliente SSH.

    b) Generar una clave RSA privada usando el siguiente comando:

        openssl genrsa –out qradar.key 3072

        La longitud de clave RSA debe ser de, al menos, 3072 bits.

    c) Generar la petición de firma del certificado (CSR). Ejecutar el siguiente comando:

        openssl req –new –key qradar.key –out qradar.csr

    d) Se solicitará en la línea de comandos información para el certificado. Se recomienda proporcionar, al menos, los siguientes parámetros:

        - *Country Name.*
        - *State or Province Name.*
        - *Locality Name.*

- *Organization Name.*
- *Organizational Unit Name.*
- *Common Name.*
- *Email Address.*

e) Verificar la información introducida en la petición CSR, utilizando el siguiente comando:

openssl req –noout –text –in qradar.csr

f) Enviar el fichero CSR a la autoridad de certificación (CA) para su firma. El formato del fichero CSR es formato Apache.

6.6.2 INSTALAR UN CERTIFICADO DE SERVIDOR HTTPS EN QRADAR

100. El certificado de servidor a instalar en QRadar debe ser X.*509 PEM base64 encoding*, y la extensión del fichero tiene que ser: *.cert, .crt, .pem o .der.*

101. Una vez obtenido el certificado que se utilizará como certificado de servidor HTTPS para la conexión al interfaz gráfico GUI, se instala siguiendo los siguientes pasos:

a) Ejecutar el siguiente *script*:

/opt/qradar/bin/install-ssl-cert.sh

En el campo *Path to Public Key File* (*SSLCertificateFile*), introducir la ubicación del fichero del certificado. Por ejemplo, */root/new.certs/cert.cert*.

En el campo *Path to Private Key File* (*SSLCertificateKeyFile*), introducir la ubicación del fichero de clave privada. Por ejemplo, */root/new.certs/qradar.key*.

b) Desplegar los cambios.

102. En el capítulo *Installing a new SSL Certificate* de la guía *IBM Security QRadar Version 7.5 – Administration Guide* [REF1] se encuentra detallado el proceso de instalación de certificados.

6.6.3 INSTALAR CERTIFICADOS PARA OTRAS COMUNICACIONES TLS

103. A continuación, se describe el procedimiento para instalar los certificados necesarios para las comunicaciones TLS seguras entre QRadar y otros componentes del sistema.

104. Para instalar en QRadar, tanto el certificado de servidor o cliente TLS, como los certificados de las CA raíz (*root* CA) de los componentes con los que se comunicará, se utiliza la REST API proporcionada por QRadar.

105. A la REST API se accede enviando solicitudes HTTPS a un API *Endpoint* desde la consola QRadar, o utilizando un cliente REST API de terceros. Cada solicitud que se realice deberá contener credenciales de autenticación y los parámetros necesarios.

106. El API *Endpoint* contiene la URL del recurso al que se quiera acceder. La solicitud indicará, a través del método HTTP usado, qué acción se quiere realizar sobre el recurso: GET, POST, PUT o DELETE.

107. Tras la solicitud API (*API request*), el servidor devuelve una respuesta HTTP. Esta respuesta contiene un código que indica si la petición ha sido correcta, junto con el detalle en formato JSON (*JavaScript Object Notation*).

6.6.3.1 CERTIFICADOS CA RAÍZ

108. Para instalar los certificados CA raíz (*root* CA) de las CAs emisoras de los certificados de los clientes TLS (fuentes de sucesos) y los servidores TLS (destinos de reenvío) en QRadar, seguir los siguientes pasos.

109. Utilizar la REST API:

a) Crear una petición HTTPS con los siguientes ajustes:

Parámetro	Valor
URL	*https://<Direccion_IP_QRadar>/api/staged_config/ca_certs*
Protocolo	*POST*
Cabecera	*"allow-hidden: true"*
Content-type	*Multipart/form-data*
Autorización	*Basic* *Usermane: admin* *Password: <Contraseña admin>*
Multipart/form-data	*Filename="<Nombre de fichero de la CA raíz>*

b) Enviar la petición y verificar que la respuesta JSON muestra la información correcta.

c) Desplegar los cambios.

110. Una vez instalados los certificados CA raíz de los componentes, si la CA emisora del certificado de QRadar es distinta de la CA emisora del certificado del componente, debe instalarse el certificado CA Raíz de QRadar, siguiendo los mismos pasos que el caso anterior.

6.6.3.2 INSTALAR EL CERTIFICADO DE QRADAR

111. Una vez instalados los certificados CA raíz, deberá instalarse el certificado que utilizará QRadar en las comunicaciones TLS. Este certificado será tipo servidor para la comunicación TLS *Syslog* entrante, con fuentes de sucesos (*log sources*) y será de tipo cliente para la comunicación TLS saliente de reenvío de datos a otros componentes (*forwarding destination*).

112. Se creará un recurso para el certificado, para lo cual, deberán seguirse los siguientes pasos:

    a) Crear una petición HTTPS con los siguientes ajustes:

Parámetro	Valor
URL	*https://<Direccion_IP_QRadar>/api/staged_config/certificates*
Protocolo	*POST*
Cabecera	*"allow-hidden: true"*
Content-type	*Application/json*
Autorización	*Basic* *Usermane: admin* *Password: <Contraseña admin>*
Body	*{ "component_id": 4, "name": "nombre del certificado con el que lo vamos a identificar", "purpose": "SERVER /CLIENT (según corresponda)"*

    b) Guardar el ID que se devuelve en la respuesta JSON.

113. A continuación, se importará el fichero de clave, para lo cual deberán seguirse los siguientes pasos.

    a) Crear una petición HTTPS con los siguientes ajustes:

Parámetro	Valor
URL	*https://<Direccion_IP_QRadar>/api/staged_config/certificates/<ID>(devuelto_en_el_paso_anterior)>/key_file*
Protocolo	*PUT*
Cabecera	*"allow-hidden: true"*
Content-type	*Application/json*
Autorización	*Basic* *Usermane: admin* *Password: <Contraseña admin>*
Body	*{"private key": "-----BEGIN PRIVATE KEY --- <fichero de clave codificado en PEM y en formato PKCS8 > ----- END PRIVATE KEY--- "*

    b) Verificar que la respuesta HTTP es un código 204.

114. Una vez importado el fichero de clave, se importará el fichero intermedio, para lo cual se seguirán los siguientes pasos:

a) Crear una petición HTTPS con los siguientes ajustes:

Parámetro	Valor
URL	*https://<Direccion_IP_QRadar>/api/staged_config/certificates/<ID>(devuelto_en_el_paso_anterior)>/ca_chain_file*
Protocolo	*PUT*
Cabecera	*"allow-hidden: true"*
Content-type	*Text/plain*
Autorización	*Basic* *Usermane: admin* *Password: <Contraseña admin>*
Body	*:-----BEGIN CERTIFICATE --- <fichero intermedio en formato PEM> ----- END CERTIFICATE---*

b) Verificar que la respuesta HTTP es un código 204.

115. Por último, deberá importarse el certificado, para lo cual deberán seguirse los siguientes pasos:

a) Crear una petición HTTPS con los siguientes ajustes:

Parámetro	Valor
URL	*https://<Direccion_IP_QRadar>/api/staged_config/certificates/<ID>(devuelto_en_el_paso_anterior)>/cert_file*
Protocolo	*PUT*
Cabecera	*"allow-hidden: true"*
Content-type	*Text/plain*
Autorización	*Basic* *Usermane: admin* *Password: <Contraseña admin>*
Body	*:-----BEGIN CERTIFICATE --- <fichero del certificado en formato PEM> ----- END CERTIFICATE---*

b) Verificar que la respuesta HTTP es un código 204.

c) Desplegar los cambios.

6.7 GESTIÓN DE LOS DATOS

116. QRadar recibe y almacena datos de sucesos de seguridad (*events*) y flujos de red (*flows*) y utiliza reglas para monitorizar estos datos y detectar amenazas de seguridad.

117. La información sobre flujos de red se recibe a través de las conexiones de red de QRadar, haciendo uso de puertos espejo SPAN o TAPs de red. La información de sucesos se recoge mediante las fuentes de sucesos.

118. Además, para mejorar cómo se visualiza la información y poder detectar amenazas de seguridad con mayor confianza, QRadar genera perfiles de activos, a los cuales se asocian los eventos y flujos, y permite añadir información de seguridad de otras fuentes.

6.7.1 AÑADIR FUENTES DE SUCESOS

119. Una fuente de sucesos (*log source*) es un dispositivo externo, sistema o servicio en la nube, configurado para enviar sucesos de seguridad a QRadar.

120. Un DSM (*Device Support Module*) es un módulo de *software* que analiza los sucesos recibidos de las distintas fuentes de sucesos, y los convierte a un formato estándar. Cada tipo de fuente de sucesos tiene un DSM correspondiente en QRadar.

121. Para poder recibir los sucesos de los dispositivos, debe completarse la instalación y configuración del módulo DSM tanto en la fuente de sucesos, como en el sistema QRadar. Algunos de estos dispositivos requieren pasos extra, como configurar certificados para habilitar las comunicaciones con QRadar, o el uso de agentes.

122. El proceso para instalar una fuente de sucesos es el siguiente:

    a) Leer las instrucciones de integración del dispositivo concreto disponibles en la base de datos de conocimiento:

    https://www.ibm.com/docs/en/qsip/7.5.

    b) Descargar e instalar el paquete DSM RPM (RPM es un programa para instalar y gestionar paquetes de *software* en un sistema) para el dispositivo. Los RPMs se encuentran disponibles para su descarga en la página de soporte de IBM (*https://www.ibm.com/support*).

    c) Configurar el dispositivo para enviar los sucesos a QRadar.

    d) Por lo general, tras recibir cierto número de sucesos de un dispositivo, QRadar detecta y crea automáticamente la fuente de sucesos.

    e) Si QRadar no detecta automáticamente la fuente de sucesos, es posible añadirla manualmente.

    f) Desplegar los cambios.

123. En la base de datos de conocimiento se pueden ver los dispositivos soportados *(https://www.ibm.com/docs/en/qsip/7.5?topic=configuration-qradar-supported-dsms*). También se pueden añadir dispositivos no soportados de forma manual, haciendo uso del DSM Universal.

124. En el momento de añadir una fuente de sucesos, si el DSM específico no se descubre automáticamente, es posible instalarlo manualmente:

    a) Descargar el fichero RPM DSM desde la página de soporte de IBM (https://www.ibm.com/support).

    b) Copiar el fichero en QRadar.

    c) Usar SSH para iniciar sesión como administrador.

    d) Ir al directorio donde se ha copiado el fichero y escribir el siguiente comando:

    yum –y install <fichero_RPM>

    e) Iniciar sesión en la interfaz web de QRadar.

    f) Desplegar los cambios.

125. Para configurar la detección automática de fuentes de sucesos concretas, seguir los siguientes pasos:

    a) En el menú de navegación, hacer clic en *Admin*.

    b) Ir a *Data Sources > DSM Editor*.

    c) Seleccionar el tipo de fuente de sucesos.

    d) En la pestaña *Configuration*, hacer clic en *Enable Log Source Autodetection*.

    e) Configurar los siguientes parámetros:

        - *Log Source Name Template*: Plantilla para el nombre de las fuentes detectadas automáticamente. Puede usarse el nombre del tipo de fuente o la dirección de la fuente.
        - *Log Source Description Template*: Plantilla para la descripción de las fuentes detectadas automáticamente.
        - *Minimum Succesful Events for Autodetection*: Número mínimo de sucesos que deben analizarse correctamente desde una fuente desconocida, para que ocurra la detección automática.
        - *Minimum Success Rate for Autodetection*: Porcentaje mínimo de éxito en el análisis de sucesos de una fuente desconocida, para detectarla automáticamente.
        - *Attempted Parse Limit*: Número máximo de sucesos analizados de una fuente desconocida, antes de abandonar el intento de detección automática.

- *Consecutive Failed Parse Limit*: Número de sucesos consecutivos analizados sin éxito de una fuente desconocida, antes de abandonar el intento de detección automática.

f) *Hacer clic en Save.*

g) Desplegar los cambios.

h) Una vez configurada la detección automática de fuentes de sucesos, configurar el dispositivo correspondiente para enviar los sucesos a QRadar.

126. Para configurar una fuente de sucesos de forma manual, seguir los siguientes pasos:

a) Ir a *Admin > Data Sources > Log Sources*.

b) En la barra de tareas, hacer clic en *Add* e introducir los siguientes datos:

- *Name*.
- *Description*.
- *Log Source Type*: seleccionar el tipo de dispositivo si existe un DSM específico, o *Universal DSM* en caso de no haberlo.
- *Protocol Configuration*: seleccionar el protocolo de comunicación. Seleccionar ***TLS Syslog*** cuando sea posible.
- *Log Source identifier*: introducir la dirección IPv4 de la fuente.
- *TLS Listen Port*: elegir un puerto o dejar el puerto 6514 por defecto.
- *Authentication mode*: seleccionar el tipo de autenticación, seleccionar ***TLS and Client Authentication*** cuando sea posible.

  Al activar la autenticación de cliente, QRadar autenticará las fuentes de sucesos que traten de enviar datos. Para ello es necesario instalar el certificado de la CA raíz emisora (e intermedias) de las fuentes de sucesos en QRadar (ver apartado 6.6.3.1 CERTIFICADOS CA RAÍZ).

- *Client Certificate Issuer ID*: introducir el *Authority Key Identifier*. Este campo del certificado del cliente, contiene el identificador del certificado de la CA emisora firmante.
- *Certificate CN Whitelist*: introducir una lista de los CN (*Common Names*) de los certificados del cliente.
- *Certificate Type*: seleccionar *Provide Certificate*.
- Seleccionar *Check Client Certificate Revocation*.

- Seleccionar *Check Client Certificate Usage*.
- *Server Certificate Resource ID*: introducir el **ID** obtenido de la llamada a la RestAPI cuando se creó el recurso del certificado de servidor para esta comunicación.
- *Maximum connections*: introducir el número máximo de conexiones permitidas.
- *TLS Protocols*: seleccionar los protocolos TLS que se usarán. Se debe seleccionar ***TLS 1.2 and above***.
- *Credibility*: seleccionar un nivel de credibilidad que asignaremos a los eventos generados por la fuente de log.
- Seleccionar *Coalescing Events* para relacionar los sucesos entre sí y no verlos de forma individual.

c) Hacer clic en Save.

d) Desplegar los cambios.

127. Una vez configurada de forma manual la fuente de sucesos en QRadar, configurar el dispositivo correspondiente para enviar los sucesos a QRadar.

6.7.2 RETENCIÓN DE DATOS

128. Los grupos de retención (*Retention Buckets*) permiten definir durante cuánto tiempo se mantienen almacenados los datos de flujos de red y sucesos de seguridad, en QRadar.

129. Cuando QRadar recibe datos, los compara con los criterios de los diferentes grupos de retención configurados. Cuando los datos coinciden con alguno de los filtros de un grupo, se almacenan en este hasta que se alcanza la fecha de borrado definida en dicho grupo.

130. El valor por defecto de los grupos de retención es de 30 días, tras los cuales se eliminan los datos. Se deberá configurar el periodo de retención de datos para que sea acorde a lo definido en la Política de Seguridad de cada organización.

131. Los grupos se ordenan por prioridad (de la fila superior a la fila inferior, tal como se muestran en la interfaz de QRadar), de tal forma que un dato se almacena en el grupo de mayor prioridad en la que cumpla los criterios de filtrado. En caso de no cumplir ningún requisito para los grupos, se almacena en el grupo por defecto.

132. Para configurar un grupo de retención seguir los siguientes pasos:

a) Ir a *Admin > Data sources*.

b) Hacer clic en *Event Retention* o *Flow Retention* para configurar la retención de datos de sucesos o flujos, respectivamente.

c) Hacer *doble-clic* en la primera fila vacía de la tabla para abrir la ventana *Retention Properties.*

d) Introducir los parámetros del grupo*:*

- *Name:* Nombre identificativo del grupo.
- *Keep data placed in this bucket for:* Periodo durante el cual se mantendrán almacenados los datos.
- *Delete data in this bucket*: Define cuándo eliminar los datos del grupo una vez alcanzado el periodo de retención. Seleccionar *Immediately after the retention period has expired* para eliminarlos inmediatamente. Seleccionar *When data storage is required* para mantener los datos almacenados hasta que el sistema necesite espacio de almacenamiento (cuando quede menos del 15% del espacio total).
- *Description*: Descripción del grupo.
- *Current Filters*: Configurar los criterios con los que se compararán los datos para pertenecer al grupo.

e) Para editar un grupo existente. Seleccionar la fila de la tabla correspondiente y hacer clic en *Edit*.

f) Para eliminar un grupo existente. Seleccionar la fila de la tabla correspondiente y hacer clic en *Delete*.

g) Hacer clic en *Save*.

133. Definir la prioridad en la que se comprueba la pertenencia a los grupos:

a) Ir a *Admin > Data sources*.

b) Hacer clic en *Event Retention* o *Flow Retention*.

c) Seleccionar la fila correspondiente al grupo y pulsar los botones *Up* y *Down* para aumentar o disminuir la prioridad respectivamente.

d) Hacer clic en *Save*.

134. El detalle de la configuración de retención de datos en QRadar se puede consultar en el capítulo *Data retention* de la guía I*BM Security QRadar Version 7.5 – Administration Guide* [REF1].

6.7.3 GESTIÓN DE ACTIVOS

135. QRadar crea activos y perfiles de activo para servidores y dispositivos de red, a partir de la información de identidad que absorbe pasivamente de los datos de sucesos y flujos que recibe.

136. Utilizando los datos de activos se pueden relacionar las infracciones desencadenadas en el sistema, con activos físicos o virtuales.

137. Se puede visualizar la información de activos unificada en la pestaña *Assets*. Esta información se actualiza conforme QRadar descubre más información sobre cada activo o nuevos activos.

138. QRadar recopila datos sobre los activos y se los proporciona a la base de datos de activos. Estos datos generalmente provienen de uno de los siguientes orígenes:

    a) Sucesos (*Events*): Los datos de sucesos a menudo tienen información de inicios de sesión de usuarios, direcciones IP, nombres de dispositivos, direcciones MAC y otros tipos de información sobre activos.

    b) Flujos (*Flows*): Los datos de flujos contienen información como la dirección IP, el puerto y el protocolo de comunicaciones. Los datos de flujos recopilados se asocian a los activos mediante la dirección IP.

    c) Exploradores de vulnerabilidades (*Vulnerability Scanners*): QRadar puede integrarse con exploradores de vulnerabilidades de IBM o de terceros. Estos pueden proporcionar ciertos datos sobre los activos como el sistema operativo, *software* instalado e información de parches.

    d) Interfaz de usuario (*User Interface*): Los usuarios con el rol de *Assets* pueden importar o proporcionar información de activos directamente a la base de datos de activos.

139. Cuando un origen de datos tiene configurada información de dominio, todos los datos de activos que provengan de dicho origen se etiquetan automáticamente con el dominio.

140. Cada activo debe contener al menos un dato identificativo. Las actualizaciones posteriores que contengan dicho dato identificativo irán asociadas al mismo activo. Los datos que se utilizan para identificar a los activos son los siguientes (de mayor a menos prioridad):

    a) Dirección MAC.

    b) Nombre de dispositivo NetBIOS.

    c) Nombre de dispositivo DNS.

    d) Dirección IP.

141. QRadar guarda por defecto los datos de activos durante 120 días después de la última vez que se hayan observado. Los nombres de usuario se conservan durante 30 días. Los datos añadidos manualmente se conservan indefinidamente.

142. El periodo de retención de activos puede configurarse siguiendo los siguientes pasos:

    a) Ir a *Admin > System Configuration > Asset Profiler Configuration*.

b) Hacer clic en *Asset Profiler Retention Configuration*.

c) Ajustar los valores y hacer clic en *Save*.

d) Desplegar los cambios en el entorno.

143. En el capítulo *Asset Management* de la guía I*BM Security QRadar Version 7.5 – Administration Guide* [REF1] se encuentra detallada toda la información sobre la gestión de activos en Qradar.

6.7.4 CONTENIDO DE SEGURIDAD

144. Se utilizan las herramientas de gestión de contenido para importar contenido de seguridad adicional en QRadar, como por ejemplo reglas, informes, paneles de control y aplicaciones. El contenido de seguridad puede proceder de otros sistemas QRadar, o puede desarrollarse de forma independiente para ampliar las capacidades de QRadar existentes.

145. QRadar permite la importación de dos tipos diferentes de contenidos de seguridad:

a) **Paquetes de contenido (*Content Packs*):** Contienen mejoras para tipos específicos de contenido de seguridad. A menudo incluyen contenido para integraciones o sistemas operativos de terceros. Por ejemplo, un paquete de contenido de seguridad para la integración de ciertas fuentes de sucesos podría contener nuevas propiedades *custom* que se encuentran dentro de los eventos que generan este tipo de fuentes, de forma que QRadar podría usar estas propiedades para realizar búsquedas e informes.

b) **Extensiones (*Extensions*):** Las extensiones de QRadar son elementos que mejoran o extienden las capacidades de QRadar. Una extensión puede contener aplicaciones, reglas personalizadas, plantillas de informes, búsquedas guardadas o contener actualizaciones de los elementos de contenido ya existentes.

146. El contenido de QRadar está disponible en *IBM Security App Exchange* y en *IBM Fix Central.*

147. En el capítulo *Security content de IBM Security QRadar Version 7.5 – Administration Guide* [REF1] se pueden encontrar todos los detalles sobre el contenido de seguridad.

6.7.5 ENVÍO DE DATOS A SISTEMAS EXTERNOS

148. QRadar puede enviar los datos normalizados a sistemas de alertas o *ticketing*, o a otros sistemas QRadar a través de TLS.

149. El primer paso es instalar los certificados de los dispositivos a los que se enviarán los datos (que actuarán como servidor TLS) y del sistema QRadar (que actuará como cliente TLS). Ver apartado 6.6 GESTIÓN DE CERTIFICADOS.

150. Para añadir un destino de reenvío (*forwarding destination*), seguir los siguientes pasos:

a) Ir a *Admin > System Configuration > Forwarding Destinations.*

b) En la barra de herramientas pulsar *Add*.

c) En el campo *Name*, escribir un nombre descriptivo para el destino de reenvío.

d) En el campo *Destination Address*, escribir la dirección IP o el *Host Name* del sistema al que quieren enviarse los datos.

e) En la lista *Event Format* se puede seleccionar:

- ***Payload***: Usará el formato original de la fuente de sucesos o de los flujos. Se recomienda utilizar este formato.
- ***Normalized***: Datos analizados y preparados como información presentable en la interfaz de usuario.
- ***JSON***: Formato de intercambio de datos de Java.

f) En el cuadro *Destination Port*, escribir el número de puerto al que se enviarán los datos.

g) En la lista *Protocol*, **se debe seleccionar *TCP over TLS 1.2 or above***.

h) Seleccionar la casilla *Enable hostname verification*.

i) Seleccionar la casilla *Enable client authentication.*

j) En la lista *Client Certificate*, seleccionar el certificado de cliente que se quiere utilizar para la conexión con este destino de reenvío.

k) Seleccionar la casilla *Prefix* a *syslog header if it is missing or invalid*. Cuando se usa el formato *Payload*, esta casilla asegura que se verifique que la cabecera *syslog* es correcta antes del envío.

l) Hacer clic en *Save.*

151. Una vez configurados los destinos, se definen diferentes reglas de enrutado para concretar cómo serán enviados los datos. Los detalles para la configuración de las reglas de enrutado se encuentran en el capítulo *Configuring routing rules to forward data* de la guía *IBM Security QRadar Version 7.5 – Administration Guide* [REF1].

152. Las reglas pueden reenviar los sucesos en dos (2) modos diferentes:

a) **Modo *Online***: Los datos permanecen actualizados y el reenvío se produce en tiempo real. Si el destino fuese inalcanzable por algún error, los datos enviados no serían entregados, lo que provocaría una falta de datos en el destino. Para asegurar la entrega de datos habría que usar el modo *Offline*.

b) **Modo *Offline***: Los datos son almacenados primero en la base de datos y después reenviados al destino. Este modo asegura que no se pierden datos, pero provoca un retraso en el reenvío de los datos.

6.8 PROTECCIÓN DE DATOS CONFIDENCIALES

153. QRadar permite ofuscar o enmascarar datos que pueden resultar sensibles, en propiedades personalizadas, propiedades normalizadas (por ejemplo, nombres de usuario) o en el contenido de paquetes (*payload*) (por ejemplo, números de tarjeta o seguridad social). Se recomienda utilizar este proceso de ofuscación de datos para impedir el acceso no autorizado a la información confidencial o que permita identificar a los usuarios.

154. Para ofuscar los datos, QRadar utiliza perfiles de ofuscación. Estos determinan qué claves se utilizarán para ofuscar los datos, un almacén de claves, donde se ubicarán las claves utilizadas para cifrar/descifrar los datos y expresiones de ofuscación que definirán a qué datos se aplica el perfil.

155. La ofuscación de datos es una utilidad que ofrece el producto para enmascarar datos. No obstante, deberá tenerse en cuenta que no proporciona la fortaleza de cifrado que se exige en la guía CCN-STIC-807, al no utilizar los algoritmos de cifrado admitidos en esa guía. Por ello, y aunque las técnicas de ofuscación ofrezcan una protección adicional, estos datos deberán tratarse en todo momento como datos sensibles cuya confidencialidad debe ser protegida.

156. Para crear un perfil de ofuscación de datos y un almacén de claves seguir los siguientes pasos:

    a) Ir a *Admin > Data Sources > Data Obfuscation Management.*

    b) Para crear un nuevo perfil, hacer clic en *Add* e introducir un nombre único y una descripción.

    c) Para crear un nuevo almacén de claves para el perfil:

        - Hacer clic en *System generate keystore*.
        - En la lista *Provider*, seleccionar *IBMJCE*.
        - En la lista *Algorithm*, seleccionar *JCE* y elegir el tamaño de las claves de cifrado (512 o 1024 bits).
        - En el cuadro *Keystore password*, introducir la contraseña para el almacén de claves. La contraseña debe tener al menos 8 caracteres de longitud.
        - En el cuadro *Verify keystore password*, repita la contraseña.

    d) En caso de usar un almacén de claves existente, seguir los siguientes pasos:

        - Hacer clic en *Upload keystore*.

- Hacer clic en *Browse* y seleccionar el almacén.
- En el cuadro *Keystore password* introducir la contraseña del almacén.

e) Hacer clic en *Submit*.

f) Por último, eliminar el almacén en el sistema y trasladarlo a una ubicación segura a la que solo tengan acceso los usuarios autorizados a acceder a los datos ofuscados de QRadar.

157. Para crear una expresión de ofuscación seguir los siguientes pasos:

a) Ir a *Admin > Data Sources > Data Obfuscation Management.*

b) Hacer clic en el perfil que desea configurarse y pulsar *View Contents*.

c) Hacer clic en *Add* e introducir la expresión contra la que se comparará el tipo de datos a ofuscar.

d) Seleccionar la casilla *Enabled* para habilitar la expresión.

e) Hacer clic en *Save*.

158. Cuando se crea un perfil de ofuscación, los datos se comprueban (*match*) contra la expresión de ofuscación definida, si los datos coinciden, se ofuscan.

159. Cuando el perfil de ofuscación de datos está habilitado, el sistema enmascara los datos de cada suceso o evento conforme se reciben, si cumplen el perfil configurado. Los sucesos ya existentes antes de la creación del perfil de ofuscación no se enmascaran. Cuando la ofuscación de datos está configurada, los activos acumulan datos enmascarados, pero los datos que ya tenían, tampoco se enmascaran.

160. Cuando se habilita un perfil de ofuscación y comienza a ofuscar los datos, se bloquea automáticamente para evitar modificaciones en la expresión de ofuscación. Solo los usuarios con la clave privada del perfil pueden desbloquearlo para modificar la expresión de ofuscación o inhabilitarlo.

161. Para desofuscar los datos es necesario tener el rol administrador y seguir los siguientes pasos:

a) Para desofuscar datos basados en identidad:

- En la página *Event Details*, buscar los datos que se desean desofuscar. Hacer clic en el icono de candado que aparece al lado de los datos.
- En la sección *Upload Key*, hacer clic en *Select File* y seleccionar el almacén de claves correspondiente.
- En el cuadro *Password* introducir la contraseña. Hacer clic en *Upload*.

b) Para desofuscar datos basados en contenido de paquetes (*payload*):

- En la página *Event Details*, hacer clic en *Obfuscation > Deobfuscation keys*.
- En la sección *Upload Key*, hacer clic en *Select File* y seleccionar el almacén de claves correspondiente.
- En el cuadro *Password* introducir la contraseña y hacer clic en *Upload*.
- En el cuadro *Payload information*, seleccionar y copiar el texto ofuscado.
- En la página *Event Details*, hacer clic en *Obfuscation > Deobfuscation*.
- Pegar el texto ofuscado en el cuadro de diálogo.
- Seleccionar el perfil de ofuscación de la lista y hacer clic en *Deobfuscate*.

162. En el capítulo *Sensitive data protection* de la guía *IBM Security QRadar Version 7.5 – Administration Guide* [REF1] se encuentra detallada toda la información de ofuscación de datos en QRadar.

6.9 DISPOSITIVOS GESTIONADOS

163. QRadar permite añadir dispositivos gestionados al despliegue All-in-one para añadir mayor flexibilidad a la recolección de datos y eventos, y al procesamiento de los flujos de red. Estos dispositivos gestionados, serán normalmente colectores, procesadores o nodos de datos. Estos dispositivos suelen añadirse, también, en caso de necesitar recolectar sucesos y flujos de una ubicación distinta a la del *appliance All-in-one*.

164. Los dispositivos que pueden añadirse son los siguientes:

a) ***Event Collector***: Recolecta sucesos de fuentes de log locales y remotas y normaliza los datos de sucesos para que puedan ser usados por QRadar.

b) ***Event Processor***: Procesa los sucesos que han sido recolectados por *Event Collectors*. Si el suceso coincide con una de las reglas configuradas en la consola, se sigue la acción definida en la respuesta de la regla.

c) ***QRadar QFlow Collector***: Recolecta flujos de red de los dispositivos. Se incluyen los detalles de red, escaneos de puertos y registros de flujo de TAP de red o puertos SPAN.

d) ***Flow Processor***: Procesa los flujos que han sido recolectados por uno o más *Flow Collectors*. Puede, además, procesar flujos externos como NetFlow, J-Flow y sFlow proporcionados por routers de la red.

e) ***Data Node***: Reciben los sucesos de seguridad y flujos de red desde los *Event and Flow Processors* y almacenan los datos. Siempre deben estar conectados a un *Event Processor* o *Flow Processor*.

f) ***App Host***: Dispositivos dedicados a la ejecución de aplicaciones. Aportan almacenamiento, memoria y recursos CPU extra al entorno. Solo se puede tener un App Host en el despliegue, y debe encontrarse en la misma subred que el *appliance All-in-one*.

165. QRadar permite proteger las comunicaciones entre los dispositivos gestionados y la consola mediante túneles SSH. Por ejemplo, las comunicaciones entre un *Event Collector* y un *Event Processor*.

166. Para añadir un dispositivo gestionado seguir los siguientes pasos:

a) Ir a *Admin > System Configuration > System and License Management.*

b) En la lista *Display*, seleccionar *Systems*.

c) En el menú *Deployment Actions*, hacer clic en *Add Host*.

d) Configurar los ajustes para el dispositivo, fijando una dirección IP y las credenciales *root* para acceder a la *Shell* del sistema operativo en el appliance.

e) Hacer clic en *Add*.

f) Desplegar los cambios.

167. Se debe habilitar la comunicación segura con los dispositivos gestionados, para ello seguir los siguientes pasos:

a) Ir a *Admin > System Configuration > System and License Management.*

b) En la lista *Display*, seleccionar *Systems*.

c) Seleccionar el dispositivo que va a configurarse y en el menú *Deployment Actions* hacer clic en *Edit Host.*

d) Para crear un túnel SSH en el puerto 22 del dispositivo, seleccionar la casilla ***Encrypt Host***.

e) Hacer clic en *Save*.

f) Desplegar los cambios.

168. En el capítulo *Managed hosts* de la guía I*BM Security QRadar Version 7.5 – Administration Guide* [REF1] se encuentran todos los detalles de configuración de los dispositivos gestionados.

6.10 CONFIGURACIÓN DEL RELOJ DEL SISTEMA

169. QRadar permite configurar el reloj del sistema manualmente o mediante un servidor NTP. Se recomienda el uso de un servidor NTP. El reloj del sistema se sincroniza automáticamente entre la consola de QRadar y los dispositivos gestionados.

170. Para configurar el reloj de QRadar:

a) Ir a *Admin > System configuration* y hacer clic en *System and License Management*.

b) En la lista *Display* seleccionar *Systems*.

c) Seleccionar el dispositivo para el que se quiere configurar el reloj.

d) Desde el menú *Actions* hacer clic en *View and Manage System*

e) Ir a la pestaña *System Time*.

f) Para configurar un servidor NTP:

- Hacer clic en *Specify NTP Servers* y pulsar *Add More*.
- En el campo *Server 1 Address*, introducir la dirección IP para el servidor NTP.

g) Hacer clic en *Save* y después en *OK*.

6.11 ACTUALIZACIONES

6.11.1 ACTUALIZACIONES MANUALES

171. Para actualizar QRadar manualmente, es necesario que un administrador aplique las actualizaciones. Los ficheros de actualizaciones de seguridad de QRadar están firmados.

172. Para descargar e instalar una actualización seguir los siguientes pasos:

a) Descargar la actualización en https://www.ibm.com/support/fixcentral/
b) Copiar el fichero en el sistema.

c) Usar el siguiente comando para verificar la firma del fichero descargado. Para ello utilizará la clave pública de IBM que se encuentra preinstalada en el dispositivo QRadar y creará el fichero de actualización (extensión .sfs):

sudo chmod 755 <Fichero_descargado>

sudo <Fichero descargado>

d) Ejecutar las actualizaciones usando los siguientes comandos:

sudo mkdir /media/updates

sudo mount –o loop ./<Fichero de actualización>.sfs /media/updates

sudo /media/updates/installer

e) Utilizar el siguiente comando para verificar la versión del parche instalada:

sudo /opt/qradar/bin/myver -v

6.11.2 ACTUALIZACIONES AUTOMÁTICAS

173. Si QRadar tiene acceso a Internet, se puede automatizar la descarga e instalación de las actualizaciones. Por defecto, la frecuencia con la que se comprueba si hay nuevas actualizaciones y se instalan es diaria, pero puede ajustarse a la frecuencia deseada.

174. En el capítulo *Automatic updates* de la guía *IBM Security QRadar Version 7.5 – Administration Guide* [REF1] se encuentran todos los detalles y posibles configuraciones para las actualizaciones automáticas de QRadar.

175. Se recomienda seleccionar como método de actualización *Auto Integrate*, en la pestaña *Admin > System Configuration > Auto Update > Basic*. Con este método se evita que las actualizaciones sobrescriban configuraciones a medida que se hayan podido realizar.

6.12 AUTO-CHEQUEOS

176. QRadar lleva a cabo auto-chequeos de las funciones y métodos criptográficos durante el arranque. Los algoritmos criptográficos aportados por L*inux Kernel Crypto API* son comprobados usando un test de “respuesta conocida” para verificar que funcionan de forma correcta.

177. Un fallo en cualquiera de las pruebas bloquea el arranque, siendo necesario reiniciar el dispositivo. Si el reinicio no resuelve el problema, el sistema podría estar comprometido y debe reinstalarse QRadar.

6.13 ENTORNO MULTI ARRENDATARIO

178. Los entornos multi arrendatario permiten a una organización proporcionar servicios de seguridad a diferentes divisiones desde un único despliegue de QRadar compartido. No es necesario desplegar una instancia de QRadar para cada división.

179. En un despliegue multi arrendatario, se asegura que los usuarios solo ven los datos que corresponden a su división mediante el uso de dominios basados en los orígenes de entrada en QRadar. Creando perfiles de seguridad y roles de usuarios basados en estos dominios, se garantiza que los usuarios solo tengan acceso a la información que están autorizados a ver.

180. En el capítulo *Multitenant management* de la guía *IBM Security QRadar Version 7.5 – Administration Guide* [REF1] se encuentran detalladas las diferentes configuraciones y opciones para los entornos multi arrendatario.

6.14 ALTA DISPONIBILIDAD

181. QRadar permite configuraciones de Alta Disponibilidad. Es necesario disponer de un dispositivo secundario con, al menos, la misma capacidad de almacenamiento que el dispositivo principal.

182. Cuando se configura alta disponibilidad, si falla el dispositivo principal, QRadar puede continuar recolectando, almacenando y procesando los sucesos y flujos haciendo uso del dispositivo secundario.

183. Para habilitar la Alta Disponibilidad, QRadar conecta el dispositivo primario con el secundario, formando un clúster de Alta Disponibilidad. El dispositivo secundario hereda la licencia del primario, no es necesario aplicar licencias separadas. Para crear un clúster seguir los siguientes pasos:

    a) Ir a la pestaña *Admin > System and License Management*.

    b) Seleccionar el dispositivo para el cual desea habilitarse la configuración de Alta Disponibilidad.

    c) Desde el menú *Actions*, seleccionar *Add HA Host* y hacer clic en *OK*.

    d) Leer el texto introductorio y hacer clic en *Next*.

    e) Introducir los valores de los parámetros:

        - *Primary Host IP address*: Nueva dirección IP para el dispositivo principal, ya que la dirección IP previa pasará a ser la dirección del clúster.
        - *Secondary HA host IP address*: Dirección IP para el dispositivo secundario.
        - *Enter the root password of the host*: Contraseña para el usuario *root* del dispositivo secundario. Esta contraseña no puede contener caracteres especiales.
        - *Confirm the root password of the host*: Confirmar la contraseña del usuario *root* del dispositivo secundario.

    f) Configurar los parámetros avanzados, desde la pestaña *Show Advanced Options.* La lista completa de parámetros se encuentra en el capítulo *Creating an HA cluster de la guía IBM Security QRadar Version 7.5 – High Availability Guide* [REF3].

    g) Hacer clic en Next y en *Finish*.

h) Desplegar los cambios.

184. Al crear un clúster de Alta Disponibilidad, la dirección IP del dispositivo primario se reasigna automáticamente como dirección IP virtual del clúster.

185. Los despliegues de Alta Disponibilidad aseguran la consistencia de los datos entre ambos dispositivos. La sincronización de los datos sucede en las siguientes situaciones:

a) Cuando se configura inicialmente un clúster.

b) Cuando el dispositivo primario se restaura después de un fallo.

c) Durante las operaciones normales. Los datos se sincronizan en tiempo real entre los dispositivos primario y secundario.

186. Cuando el dispositivo primario falla, se continúa con el almacenamiento y la operación en el host secundario en tiempo real. Una vez se restaura el dispositivo primario, los datos recolectados por el secundario se sincronizan. Es necesario activar manualmente el dispositivo primario para que retome la operación del sistema.

187. En los despliegues de Alta Disponibilidad, cuando se realizan actualizaciones en el dispositivo primario, o se modifican los ficheros de configuración, y se despliegan los cambios, las actualizaciones se hacen automáticamente en el dispositivo secundario. En caso de no desplegar los cambios, las actualizaciones se hacen en el dispositivo secundario mediante un proceso automático que se ejecuta cada hora.

188. Los detalles sobre la gestión, configuración y restauración de los despliegues de Alta Disponibilidad se encuentran en la guía *IBM Security QRadar Version 7.5 – High Availability Guide* [REF3].

6.15 AUDITORÍA

189. Los registros de auditoría (*logs*) generados, son almacenados de forma local en el dispositivo "*All-in-one*" en texto plano.

190. El fichero de logs más reciente tendrá el nombre de audit.log. Cuando este alcance los 200 MB, será comprimido y renombrado como *audit.log.1.gz.* El número del fichero incrementa cada vez que se archiva un nuevo fichero.

191. QRadar puede almacenar hasta 50 ficheros de logs. Si se alcanza el límite de ficheros, se sobrescriben los más antiguos para almacenar los más recientes.

192. Para revisar los logs de auditoría:

a) Iniciar una sesión SSH con el usuario *administrador* en QRadar:

b) Los logs se encuentran en la carpeta */var/log/audit*.

193. Para más detalles sobre el contenido de los logs en QRadar, consultar el capítulo *Audit logs de la guía IBM Security QRadar Version 7.5 – Administration Guide* [REF1].

194. En el ANEXO A– ACCIONES AUDITABLES se encuentran detalladas las diferentes acciones que generan logs de auditoría.

195. Para poder hacer un mejor seguimiento sobre las acciones que se han producido en QRadar, pueden crearse informes sobre los logs de auditoría.

196. Para crear un informe seguir los siguientes pasos:

    a) Ir a *Log Activity > Add Filter*.

    b) En la ventana *Add Filter*, configurar los siguientes ajustes:

        - *Parameter: Log Source [Indexed].*
        - *Operator: Equals.*
        - *Log Source: SIM Audit-2.*

    c) Hacer clic en *Add Filter*.

    d) Si se encuentran sucesos transmitiéndose a la pestaña *Log Activity*, pulsar *Pause*.

    e) Desde la lista *View*, seleccionar un intervalo de tiempo.

    f) Para salvar los criterios de búsqueda, hacer clic en *Save Criteria*, introducir un nombre para la búsqueda y hacer clic en *OK*.

    g) Para generar un informe a partir de los resultados de la búsqueda, seguir los siguientes pasos:

        - Desde la pestaña *Reports*, hacer clic en *Actions > Create*.
        - Seguir el asistente de informes.
        - En el campo *Saved Searches*, escribir el nombre de la búsqueda creada.
        - Hacer clic en *Save Container Details*.
        - Terminar las páginas del asistente de informes.

6.16 COPIAS DE SEGURIDAD

197. QRadar permite la creación de copias de seguridad, tanto de los ficheros de configuración del sistema, como de los datos. Las copias de seguridad de datos incluyen: información de direcciones IP de origen y destino, información de activos, información de categorías de sucesos, datos de vulnerabilidades, datos de flujos y datos de sucesos.

198. Permite también realizar restauraciones manuales de los datos de sucesos y flujos y de los ficheros de configuración del sistema.

199. QRadar genera, por defecto, un *backup* diario a media noche, que solo incluye los ficheros de configuración. Se recomienda personalizar este *backup* diario para incluir datos de la consola QRadar y de los dispositivos gestionados que se considere.

200. Para customizar la copia de seguridad diaria seguir los siguientes pasos:

    a) Ir a la pestaña *Admin*.

    b) En la sección *System Configuration*, hacer clic en *Backup and Recovery*.

    c) En la barra de herramientas, hacer clic en *Configure.*

    d) En la ventana *Backup Recovery Configuration:*

        - *Backup Repository* Path: ruta donde se quiere almacenar el fichero de *backup* (por defecto es */store/backup*).
        - *Backup Retention Period (days*): tiempo durante el que se guarda la copia de *backup* (2 días por defecto).
        - *Nightly Backup Schedule*: elegir el tipo de copia de seguridad que desea realizarse: datos, configuración o ambos (*Configuration and Data Backups*).
        - *Managed hosts*: en caso de seleccionar la opción *Configuration and Data Backups*, permite seleccionar de una lista, los dispositivos gestionados de los que queremos hacer el backup de datos.

    e) Hacer clic en *Save*.

    f) Desplegar los cambios.

201. En el capítulo *Backup QRadar configurations and data de* la guía *IBM Security QRadar Version 7.5 – Installation Guide* [REF2] se encuentran detallados los diferentes ajustes disponibles para las copias de seguridad.

7 FASE DE OPERACIÓN

202. Durante la fase de operación de QRadar se recomienda llevar a cabo, al menos, las siguientes tareas para una gestión segura del producto:

a) Comprobar periódicamente el software para asegurar que no se ha introducido software no autorizado.

b) Revisar que las copias de seguridad automáticas se realizan correctamente para los datos y los archivos de configuración.

c) Revisar periódicamente los logs de auditoría. Comprobar el límite de almacenamiento, eliminando (y si fuese oportuno, almacenando en una ubicación alternativa) los logs más antiguos para evitar que el sistema los sobrescriba.

d) Comprobar que los ficheros de auditoría están protegidos frente al borrado o la modificación no autorizados.

e) Controlar el acceso a la información de auditoría, de tal forma que únicamente el personal designado pueda acceder a ella.

f) Comprobar que se reciben correctamente las notificaciones de las actualizaciones y mantener el sistema actualizado siempre a la última versión.

g) Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

h) En caso de habilitar la ofuscación de datos, comprobar que las claves son protegidas correctamente.

8 REFERENCIAS

REF1 *IBM Security QRadar Version 7.5 – Administration Guide*
https://www.ibm.com/docs/en/SS42VS_7.5/pdf/b_qradar_admin_guide.pdf

REF2 *IBM Security QRadar Version 7.5 – Installation Guide*
https://www.ibm.com/docs/en/SS42VS_7.5/pdf/b_siem_inst.pdf

REF3 *IBM Security QRadar Version 7.5 – High Availability Guide*
https://www.ibm.com/docs/en/SS42VS_7.5/pdf/b_qradar_ha_guide.pdf

9 ABREVIATURAS

API	*Application Programming Interface*
CA	Autoridad de Certificación (*Certification Authority*)
CCN	Centro Criptológico Nacional
CLI	*Command-Line Interface*
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
CPU	*Central Processing Unit*
CSR	*Certificate Signing Request*
DNS	*Domain Name System*
DSA	*Digital Signature Algorithm*
ENS	Esquema Nacional de Seguridad
GUI	*Graphical User Interface*
HA	*High Availability*
HTTPS	*Hypertext Transfer Protocol Secure*
LDAP	*Lightweight Directory Access Protocol*
MAC	Media Access Control
NetBIOS	*Network Basic Input/Output System*
NTP	*Network Time Protocol*
RADIUS	*Remote Authentication Dial-In User Service*
RHEL	*Red Hat Enterprise Linux*
SAML	*Security Assertion Markup Language*
SFTP	*Secure File Transfer Protocol*
SIEM	*Security Information and Event Management*
SNMP	*Simple Network Management Protocol*
SPAN	*Switched Port Analyzer*
SSH	*Secure Shell*
TACACS	*Terminal Access Controller Access Control System*
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*

ANEXO A – ACCIONES AUDITABLES

203. A continuación, se muestran las diferentes acciones auditables en QRadar:

a) Autenticación de los administradores:

- Inicio / fin de sesión.

b) Activos:

- Eliminar un activo.
- Eliminar todos los activos.

c) Acceso a los logs de auditoría:

- Búsquedas que incluyen sucesos que tienen un suceso de alto nivel de auditoría.

d) Copias de seguridad y *restore*:

- Editar la configuración.
- Iniciar una copia de seguridad.
- Completar una copia de seguridad.
- Error al realizar una copia de seguridad.
- Sincronización de una copia de seguridad.
- Cancelación de una copia de seguridad.
- Actualización de una copia de seguridad.
- Actualización de una copia de seguridad no válida.
- Inicio de una restauración del sistema.
- Purga de una copia de seguridad.

e) Configuración de gráficos:

- Guardar la configuración de gráficos de sucesos o flujos.

f) Gestión del contenido:

- Exportación de contenido iniciada.
- Exportación de contenido completa.
- Importación de contenido iniciada.
- Importación de contenido completada.

- Actualización de contenido iniciada.
- Actualización de contenido completada.
- Aplicaciones añadidas.
- Aplicaciones modificadas.
- Acciones personalizadas añadidas.
- Acciones personalizadas modificadas.
- Propiedad Ariel añadida.
- Propiedad Ariel modificada.
- Propiedad de expresión Ariel añadida.
- Propiedad de expresión Ariel modificada.
- Regla CRE añadida.
- Regla CRE modificada.
- Panel de control añadido.
- Panel de control modificado.
- Extensión de dispositivo añadida.
- Extensión de dispositivo modificada.
- Asociación de extensión de dispositivo modificada.
- Grupo añadido.
- Grupo modificado.
- Perfil de correlación histórica añadido.
- Perfil de correlación histórica modificado.
- Entrada de QID map añadida.
- Entrada de QID map modificada.
- Referencia de datos añadida.
- Referencia de datos modificada.
- Perfil de seguridad añadido.
- Perfil de seguridad modificado.
- Dispositivo sensor añadido.

- Dispositivo sensor modificado.

g) Propiedades personalizadas:

- Añadir una propiedad de suceso personalizada.
- Editar una propiedad de suceso personalizada.
- Eliminar una propiedad de suceso personalizada.
- Editar una propiedad de flujo personalizada.
- Eliminar una propiedad de flujo personalizada.

h) Expresiones personalizadas:

- Añadir una expresión de suceso personalizada.
- Editar una expresión de suceso personalizada.
- Eliminar una expresión de suceso personalizada.
- Editar una expresión de flujo personalizada.
- Eliminar una expresión de flujo personalizada.

i) Fuentes de flujos:

- Añadir una fuente de flujos.
- Editar una fuente de flujos.
- Eliminar una fuente de flujos.

j) Grupos:

- Añadir un grupo.
- Editar un grupo.
- Eliminar un grupo.

k) Correlación Histórica:

- Añadir un perfil de correlación histórica.
- Modificar un perfil de correlación histórica.
- Eliminar un perfil de correlación histórica.
- Habilitar un perfil de correlación histórica.
- Deshabilitar un perfil de correlación histórica.
- Un perfil de correlación histórica se está ejecutando.

- Un perfil de correlación histórica ha sido cancelado.

l) Licencias:

- Añadir una clave de licencia.
- Eliminar una clave de licencica.
- Eliminar una ubicación de claves de licencia.
- Actualizar una ubicación de claves de licencia.

m) Extensión de fuentes de logs:

- Añadir una extensión de fuentes de logs.
- Editar una extensión de fuentes de logs.
- Eliminar una extensión de fuentes de logs.
- Actualizar una extensión de fuentes de logs.
- Actualizar satisfactoriamente una extensión de fuentes de logs.
- Actualizar una extensión de fuentes de logs incorrecta.
- Descargar una extensión de fuentes de logs.
- Reportar una extensión de fuentes de logs.
- Modificar la asociación de fuentes de logs a un dispositivo o tipo de dispositivos.

n) Infracciones:

- Crear una infracción.
- Ocultar una infracción.
- Cerrar una infracción.
- Cerrar todas las infracciones.
- Añadir una nota de destino.
- Añadir una nota de origen.
- Añadir una nota de red.
- Añadir una nota de infracción.
- Añadir una razón para el cierre de infracciones.
- Editar una razón para el cierre de infracciones.

o) Configuración de protocolos:
   - Añadir una configuración de protocolos.
   - Editar una configuración de protocolos.
   - Eliminar una configuración de protocolos.

p) *QIDmap:*
   - Añadir una entrada de *QIDmap*.
   - Editar una entrada de *QIDmap*.

q) *IBM QRadar Vulnerability Manager:*
   - Crear una programación de escáner.
   - Actualizar una programación de escáner.
   - Eliminar una programación de escáner.
   - Inicio de un escáner programado.
   - Pausa de un escáner programado.
   - Resumen de un escáner programado.

r) Sets de referencia:
   - Crear un set de referencia.
   - Editar un set de referencia.
   - Purgar elementos de un set de referencia.
   - Eliminar un set de referencia.
   - Añadir elementos a un set de referencia.
   - Eliminar elementos de un set de referencia.
   - Eliminar todos los elementos de un set de referencia.
   - Importar elementos de un set de referencia.
   - Exportar elementos de un set de referencia.

s) Informes:
   - Añadir una plantilla.
   - Eliminar una plantilla.
   - Editar una plantilla.

- Generar un informe.
- Eliminar el contenido generado.
- Ver un informe generado.
- Mandar por email un informe generado.

t) *"Bucket Retention":*

- Añadir un "bucket".
- Eliminar un "bucket".
- Editar un "bucket".
- Habilitar o deshabilitar un "bucket".

u) Inicio de sesión de *root*:

- Iniciar sesión en QRadar como usuario *root*.
- Cerrar sesión en QRadar como usuario *root.*

v) Reglas:

- Añadir una regla.
- Borrar una regla.
- Editar una regla.

w) Escáner:

- Añadir un escáner.
- Editar un escáner.
- Eliminar un escáner.

x) Programación horaria de escáner:

- Añadir una programación.
- Editar una programación.
- Eliminar una programación.

y) Autenticación de sesión:

- Crear una sesión de administración.
- Terminar una sesión de administración.
- Denegar la autenticación de sesión a un usuario incorrecto.

- Expirar la autenticación de sesión.
- Crear una autenticación de sesión.
- Terminar una autenticación de sesión.

z) SIM:

- Vaciar un modelo SIM.

aa) Almacenamiento y reenvío:

- Añadir una programación de almacenamiento y reenvío.
- Editar una programación de almacenamiento y reenvío.
- Eliminar una programación de almacenamiento y reenvío

bb) Reenvío de *Syslog*:

- Añadir un reenvío de Syslog.
- Editar un reenvío de Syslog.
- Eliminar un reenvío de Syslog.

cc) Gestión del sistema:

- Apagar un sistema.
- Reiniciar un sistema.

dd) Cuentas de usuario:

- Añadir una cuenta de usuario.
- Editar una cuenta de usuario.
- Eliminar una cuenta de usuario.

ee) Autenticación de usuarios:

- Inicio de sesión en la interfaz de usuario.
- Cierre de sesión en la interfaz de usuario.

ff) Autenticación Ariel de usuarios:

- Denegar un intento de inicio de sesión.
- Añadir una propiedad Ariel.
- Eliminar una propiedad Ariel.
- Editar una propiedad Ariel.

- Añadir una extensión de propiedad Ariel.
- Eliminar una extensión de propiedad Ariel.
- Editar una extensión de propiedad Ariel.

gg) Roles de usuarios:

- Añadir un rol.
- Editar un rol.
- Eliminar un rol.

hh) VIS:

- Descubrir un nuevo dispositivo.
- Descubrir un nuevo sistema operativo.
- Descubrir un nuevo puerto.
- Descubrir una nueva vulnerabilidad.

ANEXO B – ROLES DE USUARIO

Permiso	Descripción
Admin	Otorga acceso administrativo a la interfaz de usuario. Puede otorgar permisos administrativos específicos. Los usuarios con permiso ***Admin*** del sistema pueden acceder a todas las áreas de la interfaz de usuario. Los usuarios que tienen este acceso no pueden editar otras cuentas de administrador.
Delegated Administration	Otorgar permisos de usuarios para realizar funciones administrativas limitadas. En un entorno de varios arrendatarios los usuarios de arrendatario con permisos de ***Delegated Administration*** solo pueden ver datos de su propio entorno de arrendatario. Si se asignan otros permisos administrativos que no forman parte de la Administración delegada, los usuarios del arrendatario pueden ver datos para todos los arrendatarios.
Offenses	Otorga acceso a todas las funciones de la pestaña ***Offenses***. Los roles de usuario deben tener permiso ***Maintain Custom Rules*** para crear y editar reglas personalizadas.
Log Activity	Otorga acceso a las funciones de la pestaña ***Log Activity***. También puede otorgar permisos específicos: • ***Maintain Custom Rules.*** Otorga permiso para crear o editar reglas que se muestran en la pestaña ***Log Activity.*** • ***Manage Time Series.*** Otorga permiso para configurar y ver gráficas de datos de series temporales. • ***User Defined Event Properties.*** Otorga permiso para crear propiedades de suceso personalizadas. • ***View Custom Rules.*** Otorga permiso para ver reglas personalizadas. Si se otorga a un rol de usuario que no tenga asimismo el permiso ***Maintain Custom Rules,*** el rol de usuario no puede crear ni editar reglas.
Assets	**Nota**: Este permiso solamente se visualiza si IBM QRadar Vulnerability Manager está instalado en el sistema. Otorga acceso a la función de la pestaña ***Assets***. Puede otorgar permisos específicos: • ***Perform VA Scans.*** Otorga permiso para realizar exploraciones de evaluación de vulnerabilidades. • ***Remove Vulnerabilties.*** Otorga permiso para eliminar las vulnerabilidades de los activos. • ***Server Discovery.*** Otorga permiso para descubrir servidores. • ***View VA Data.*** Otorga permiso para los datos de evaluación de vulnerabilidades.

Permiso	Descripción
Network Activity	Otorga acceso a todas las funciones de la pestaña ***Network Activity***. Puede otorgar acceso específico a los permisos siguientes. • ***Maintain Custom Rules.*** Otorga permiso para crear o editar reglas que se muestran en la pestaña ***Network Activity.*** • ***Manage Time Series.*** Otorga permisos para configurar y ver gráficas de datos de series temporales. • ***User Defined Flow Properties.***Otorga permiso para crear propiedades de flujo personalizadas. • ***View Custom Rules.*** Otorga permiso para ver reglas personalizadas. Si el rol de usuario no tiene también el permiso **Maintain Custom Rules,** el rol de usuario no puede crear ni editar reglas personalizadas. • ***View Flow Content.***Otorga permiso para acceder a los datos de flujo.
Reports	Otorga permiso para acceder a todas las funciones en la pestaña ***Reports***. • ***Distribute Reports via Email.*** Otorga permiso para distribuir informes a través del correo electrónico. • ***Maintain Templates.*** Otorga permiso para editar las plantillas del informe.
Vulnerability Manager	Otorga permiso para la función *QRadar Vulnerability Mamager. QRadar Vulnerability Manager* debe estar activado.
Forensics	Otorga permiso para las prestaciones de ***QRadar Incident Forensics.*** • **Create cases in Incident Forensics.** Otorga permiso para crear casos para recopilaciones de archivos pcap y de documentos importados.
IP Right Click Menu Extensions	Otorga permiso para las opciones añadidas al menú contextual.
Platform Configuration	Otorga permiso para los servicios de ***Plataform Configuration***. • ***Dismiss System Notifications.*** Otorga *permiso* para ocultar las notificaciones del sistema en la pestaña **Messages.** • **View Reference Data.** Otorga permiso para ver datos de referencia cuando está disponible en los resultados de la búsqueda. • ***View System Notifications.*** Otorga permiso para ver las notificaciones del sistema en la pestaña ***Messages*.**

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL