UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Evaluación y gestión de vulnerabilidades: Cómo sobrevivir en el mundo de los ciberataques.

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática

Autor: Borja Villora Divino

Tutor: David de Andrés Martínez
Juan Carlos Ruiz García

Curso 2017-2018

Resum

Fa ja prou temps que ningú no discuteix la necessitat de tindre cura de la ciberseguretat a empreses de totes les mides o simplement en qualsevol negoci que oferisca un servei a través de la xarxa; així i tot, són poques les que han implementat una política de seguretat adequada. És per això que aquest document se centrarà a instruir respecte a l'avaluació i gestió de vulnerabilitats, així com els principals vectors d'atac usats pels cibercriminals en l'actualitat. També es tractarà la incidència de les principals normatives com la llei de Protecció de Dades de Caràcter Personal (LOPD) i el Reglament General de Protecció de Dades europeu (GDPR). Per a concloure, es durà a terme un estudi de mercat de les principals empreses que ofereixen productes relacionats amb l'avaluació de vulnerabilitats (Vulnerability Assessment) i s'analitzaran les seues distintes solucions oferides.

Paraules clau: Ciberatac, Vulnerabilitat, OWASP Top 10, LOPD, GDPR, Gestió d'actius, Escàner de vulnerabilitats, Polítiques de seguretat

Resumen

Hace ya tiempo que nadie discute la necesidad de cuidar la ciberseguridad en empresas de todos los tamaños o simplemente en cualquier negocio que ofrezca un servicio a través de la red; sin embargo, son pocas las que han implementado una política de seguridad adecuada. Es por ello que este documento se centrará en instruir en cuanto a la evaluación y gestión de vulnerabilidades, así como los principales vectores de ataque usados por los cibercriminales en la actualidad. También se tratará la incidencia de las principales normativas, como la ley de Protección de Datos de Carácter Personal (LOPD) y el Reglamento General de Protección de Datos europeo (GDPR). Para concluir, se llevará a cabo un estudio de mercado de las principales empresas que ofrecen productos relacionados con la evaluación de vulnerabilidades (Vulnerability Assessment) y se analizarán sus distintas soluciones ofertadas.

Palabras clave: Ciberataque, Vulnerabilidad, OWASP Top 10, LOPD, GDPR, Gestión de activos, Escáner de vulnerabilidades, Políticas de seguridad

Abstract

For some time now nobody has discussed the need to take care of cybersecurity in companies of all sizes or simply in any business that offers a service through the network; however, few have implemented an adequate security policy. That is why this document will focus on instructing in the assessment and management of vulnerabilities, as well as the main attack vectors used by cybercriminals today. The incidence of the main regulations will also be discussed, such as the law on the Protection of Personal Data (LOPD) and the European General Data Protection Regulation (GDPR). To conclude, a market study of the main

companies that offer products related to the assessment of vulnerabilities (Vulnerability Assessment) will be carried out and their different offered solutions will be analyzed.

Key words: Cyberattack, Vulnerability, OWASP Top 10, LOPD, GDPR, Assets management, Vulnerability scanner, Security policies

Índice general

Índice de figuras

Índice de tablas

CAPÍTULO 1
Introducción

Ya no sorprende a mucha gente la afirmación de que los datos son el nuevo oro[1] . La información es poder y como tal no son pocas las entidades que intentan hacerse con ella de manera más o menos legítima.

Se trata de un bien valioso y de una producción cada vez mayor, donde generan grandes bases de datos desde la mayor multinacional en ventas online hasta la más humilde aplicación gratuita de la Play Store. Este no es un tema baladí para empresas que manejan grandes cantidades de información, la cual podría ser considerada verdaderamente valiosa más allá del valor que tiene para la propia empresa.
Y lo que suele ocurrir cuando se pueden generar datos de una forma relativamente sencilla es que la seguridad de estos no está al nivel de las amenazas hacia dicha información, ya sea por falta de concienciación o conocimiento técnico.

Son estos dos últimos aspectos en los que pretende incidir este estudio, como bien se explicará en los objetivos y posteriormente se desarrollará a lo largo de todo el documento.

1.1 Motivación

La motivación para la realización de este trabajo surge en primer lugar de mi fascinación por la ciberseguridad, un campo de la informática que a la vez es una parte importante de todas las ramas que componen esta ciencia.

No solo porque se trate de una variante muy transversal y que requiere un alto grado de especialización en tecnologías muy distintas, sino por la volatilidad de un ecosistema siempre cambiante.
Lo que ayer servía para tomar el control de un sistema te servirá esta semana pero probablemente la semana que viene ya no tendrá un uso real, y ello exige al profesional de la ciberseguridad estar en un proceso continuo de renovación y aprendizaje.

[1] *Monica Atwal, «Data is fast becoming more valuable than gold».*

También ha supuesto un aliciente el hecho de que muchos de los últimos ciberataques más mediáticos se llevaron a cabo mediante vulnerabilidades conocidas y es por ello que no hubiera sido muy difícil contrarrestarlos con sencillas medidas de seguridad, que se asumen implementadas pero a menudo no lo están ni en empresas de carácter multinacional.

Por todo esto considero que sería de utilidad un documento donde se exponga la problemática de estos ataques y un estudio de mercado comparando diferentes productos que podrían haber prevenido estas brechas de la seguridad con un esfuerzo mínimo.

1.2 Objetivos

El principal objetivo es instruir al lector sobre las prácticas de la evaluación y gestión de vulnerabilidades, así como concienciar de la importancia de poner estas políticas en uso para estar a salvo de los cibercriminales, proporcionando al lector una serie de soluciones concretas que cubren esta problemática.

Para lograr esto se cumplirán una serie de subobjetivos como son:

- Mostrar las amenazas más comunes e importantes en la actualidad
- Exposición del marco legal en cuanto a la seguridad de la información
- Diferenciar los distintos tipos de evaluación y gestión de vulnerabilidades
- Análisis de mercado en soluciones de evaluación y gestión de vulnerabilidades

1.3 Estructura de la memoria

En primer lugar se presentará al lector la escena actual de la ciberseguridad a nivel mundial. Para ello se hará uso de noticias y eventos relacionados con la seguridad informática, así como de una explicación técnica de las principales y más recientes amenazas.
En esta escena también se incluirá el marco legal para explicar cómo las diferentes herramientas mostradas posteriormente pueden ayudar a un mejor cumplimiento de la legalidad vigente, centrando el foco a nivel nacional en la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) y a nivel europeo en la General Data Protection Regulation (GDPR).

Seguidamente también se expondrá parte de la joven historia de la ciberseguridad y se procederá a explicar un compendio de ataques reseñables producidos a lo largo de los años.

A continuación, se procederá a exponer en qué consiste la evaluación y gestión

de vulnerabilidades, así como los diferentes tipos de esta que existen, explicando las cualidades y características destacadas de cada uno.

Para mostrar de una manera ordenada y detallada los diferentes productos que existen actualmente para llevar a cabo una correcta evaluación y gestión de vulnerabilidades, se realizará un estudio de mercado donde se presentarán las fortalezas y debilidades de cada solución, así como la facilidad de implementación de cada uno. Este análisis concluirá con una tabla comparativa para las distintas soluciones analizadas y unos ejemplos de elección de solución por parte de hipotéticas empresas.

Para finalizar se condensará todo el documento en un sucinto resumen donde se relacionan todos los conceptos tratados a modo de conclusión final.

CAPÍTULO 2
La ciberseguridad en la actualidad

La ciberseguridad según el diccionario de Oxford es el estado de estar protegido contra el uso no autorizado o criminal de datos electrónicos, o las medidas tomadas para lograr esto[1].
Sin embargo este es un término relativamente nuevo y no hay un gran consenso en torno a su alcance, para el ámbito de este trabajo se adecua más la propuesta de The Economic Times: "La ciberseguridad o seguridad de las tecnologías de la información son las técnicas para proteger computadoras, redes, programas y datos de accesos no autorizados o ataques orientados a la explotación."[2]

Pese a ser un tema novedoso para el público general la ciberseguridad lleva siendo la mayor preocupación para los gestores de riesgo desde hace tres años[3]. No parece ser para menos cuando estudios como el realizado por el Centro para Estudios Estratégicos e Internacionales (CSIS) y la multinacional especializada en seguridad informática McAfee estima en 600,000 millones de dólares el peaje que cobra anualmente el cibercrimen a la economía global[4].

Y como cabría esperar si se fortalece y aumenta la inversión en los atacantes, también se fortalecen a la fuerza las defensas. En España la ciberseguridad representó el 22 % del presupuesto de las empresas del sector de tecnologías de la información en 2017 y movió alrededor de 1,000 millones de euros anuales, con una previsión de crecimiento del 5 % hasta 2020[5].

Entre el segundo semestre de 2017 y el primero de 2018 la ciberseguridad ha ocupado la cabecera de muchos telediarios con casos de gran relevancia a nivel internacional. Desde las supuestas injerencias del ciberejército ruso en la elecciones estadounidenses y otros conflictos internos de países europeos [6], hasta la posible vulneración de los datos de millones de usuarios de Facebook por parte de Cambridge Analytica, que pese a recibir una gran atención mediática no ha impedido que el gigante tecnológico siga disparando sus benficios[7].

Aunque estos ataques no se limitan solo a países o grandes empresas. En los últimos tiempos se ha popularizado el priorizar una mayor cantidad de ataques sobre objetivos de bajo valor en vez de un menor número de objetivos con un

gran valor. Se ha visto con las campañas de ransomware[1] de 2017 y la creciente amenaza del minado de criptomonedas, con soluciones para equipos de usuario, smartphones, servidores y dispositivos IoT, como recoge el Centro Seguridad TIC de la Comunidad Valenciana (CSIRT-CV) en su último informe sobre *malware*[2] de minado de criptomonedas [8].

Sin embargo y pese a todos los avances y supuesta profesionalización del ciber-criminal el grueso de los ataques se basan en vulnerabilidades que ya han sido publicadas y mayormente poseen sus correspondientes parches de seguridad publicados por el proveedor.
Estas afirmaciones no vienen de cualquier profesional de la seguridad, sino del presidente de la Agencia de Seguridad Nacional estadounidense (NSA) en la conferencia RSA 2018[3]:

'Cada día luchamos contra una nueva ciberamenaza, pero cuanto más cambian las cosas más se mantienen igual.'
'Tenemos a sofisticados adversarios usando medios poco sofisticados para causar un gran daño. De hecho, os diré como supervisor de los equipos de operaciones de la NSA que no hemos respondido a una vulnerabilidad de día cero [4] en más de 24 meses.'
'Nuestros adversarios se están metiendo en nuestras redes usando medios no técnicos, aprovechándose de tecnologías hardware y software que no cumplen con las últimas actualizaciones, y aprovechándose de malas prácticas de seguridad como hacer uso de soluciones que ya no están soportadas por el vendedor.' [9]

Es por ello que este documento pretende instruir al lector sobre como prevenir este tipo de ataques, que serán a los que se van a tener que enfrentar todas las organizaciones en un futuro próximo, si no inmediato.
A continuación se procederá a explicar las mayores amenazas actuales a través del OWASP Top 10.

El Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP en inglés) es una comunidad abierta dedicada a permitir que las organizaciones desarrollen, adquieran y mantengan aplicaciones y APIs en las que se pueda confiar[5].
Para ello proporciona de forma gratuita y abierta desde libros completos de seguridad hasta conferencias alrededor de todo el mundo, pasando por herramientas y estándares de seguridad en aplicaciones entre otros recursos ofrecidos.

Nos centraremos en un proyecto en concreto de esta organización, el famoso OWASP Top 10, creado gracias a los datos de vulnerabilidades cedidos por más de 40 empresas (datos abiertos al público) y a encuestas de opinión de más de 500 profesionales del sector de la seguridad[10].
En este documento se pretende formar un ránking de los riesgos de seguridad de

[1] *Ransomware: Software malicioso que restringe o cifra el acceso a archivos del sistema afectado, pidiendo un rescate a cambio de quitar esas restricciones.*
[2] *Malware: Tipo de software malicioso para causar daños en el sistema o red que es ejecutado.*
[3] *Conferencia RSA,https://www.rsaconference.com/*
[4] *Vulnerabilidad día cero o zero-day: Una nueva vulnerabilidad para la cual no se han creado parches o revisiones, y que se emplea para llevar a cabo un ataque.*
[5] *La Fundación OWASP,https://www.owasp.org/*

aplicaciones con mayor impacto en la actualidad de todas las organizaciones.
Este proyecto cuenta con 6 ediciones previas a la que se analizará (2003, 2004, 2007, 2010, 2013, 2016) y cuenta con reconocimiento por la comunidad a nivel mundial.
A continuación se procederá a desglosar y explicar punto por punto la edición de OWASP Top 10 2017 para luego acabar mostrando la normativa legal vigente respecto a la protección de datos, un tema clave para las empresas y de rigurosa actualidad.

2.1 Inyección

Los fallos por inyección suceden cuando el atacante mediante un comando o consulta es capaz de enviar datos no confiables al intérprete. De entre las diferentes inyecciones destacan las SQL, NoSQL, OS y LDAP.
Esta inyección de datos puede forzar al intérprete a ejecutar los comandos deseados por el atacante o incluso acceder a datos para los que no tiene autorización.

Esta vulnerabilidad se muestra cuando los datos insertados por el usuarios no son filtrados ni validados antes de invocar estas consultas y además estos datos son concatenados o usados directamente, produciendo un comando con consultas dinámicas, procedimientos almacenados u otros comandos.
Para evitar las inyecciones es recomendable validar la entrada de datos en el servidor mediante 'listas blancas' y sanitizar las consultas escapando los caracteres especiales para el intérprete usado. También se recomienda el uso de controles SQL en las consultas para evitar grandes fugas de datos en caso de que se dé una inyección.

2.2 Pérdida de Autenticación y Gestión de Sesiones

Una implementación incorrecta de las funciones de autenticación y gestión de sesiones permiten a un atacante comprometer usuarios y contraseñas, token de sesiones, o hacer uso de otras vulnerabilidades para suplantar la identidad de otros usuarios de carácter temporal o permanentemente.

Los errores de implementación más comunes son permitir ataques automatizados con una lista de pares usuario/contraseña o de fuerza bruta[6], permitir el uso de contraseñas por defecto o débiles, procesos inseguros de recuperación de credenciales como preguntas de seguridad, almacenado de contraseñas en texto plano o con un cifrado débil o no hacer uso de un sistema de autenticación multifactor.

[6] *Ataque de fuerza bruta: Ataque de recuperación de clave basado en probar todas las combinaciones posibles hasta obtener la correcta.*

Las malas implementaciones mostradas son fácilmente salvables aplicando una sencilla batería de medidas de precaución:
Para evitar los ataques automatizados basta con limitar o incrementar el tiempo de respuesta tras cada intento fallido de inicio de sesión. Otra manera que además contribuye a aumentar la seguridad general de la aplicación es implementar un sistema de autenticación multi-factor, evitando depender totalmente en credenciales que pueden ser fácilmente robados.
Para mejorar la fortaleza de las contraseñas de los usuarios se recomienda implementar una buena política de contraseñas, sin permitir el uso de credenciales por defecto o que se encuentren la lista del 'Top 10,0000 de peores contraseñas'[7].
También es recomendable establecer una longitud y complejidad mínima de estas para que no sean vulnerables a ataques automatizados y forzar al usuario a cambiar la contraseña en unos tiempos razonables.

2.3 Exposición de Datos Sensibles

En muchos casos la información financiera, de salud o Información Personalmente Identificable (PII) no se protege como cabría esperar debido al trato de los datos por parte de aplicaciones web y APIs.
El resultado es que se dejan estos datos al alcance de atacantes, que posteriormente usan para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Este tipo de datos requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.

La exposición de datos a menudo se produce cuando se envían datos sensibles en protocolos que trabajan sin cifrado, como podrían ser TELNET, SMTP, FTP y HTTP. A la hora de realizar el cifrado también supone un problema del uso de algoritmos criptográficos obsoletos como podrian ser MD5 y SHA1 entre otros.
Para solucionar estos problemas se recomienda realizar una clasificación de los datos transmitidos, almacenados o procesados y que se le aplique una seguridad de acuerdo a la sensibilidad de los datos, priorizando el cifrado de los datos en tránsito aunque pudieran parecer de menor valor.
Se recomienda reducir al mínimo el almacenaje de datos de valor innecesariamente (incluso en cache) y cuando hay que hacerlo que sea siempre cifrado, utilizando funciones de *hashing*[8] con un factor de trabajo además de *SALT*[9] para las contraseñas.

[7] *Top 10,000 Worst Passwords,https://github.com/skyzyx/bad-passwords*
[8] *Hashing: Función resumen, que a partir de un conjunto de elementos como entrada los convierte en un rango de salida finito.*
[9] *SALT: Dato aleatorio que se añade como entrada a una función hash para dificultar los ataques por diccionario.*

2.4 Entidad Externa de XML (XXE)

Si la aplicación dispone de procesadores XML antiguos o mal configurados que evalúan referencias a entidades externas en documentos XML entonces esta es vulnerable a un gran número de ataques.
El atacante puede aprovecharse de esta funcionalidad para escanear puertos de la LAN, realizar ataques de denegación de servicio (DoS), revelar archivos internos mediante la URI o archivos internos en servidores no actualizados y ejecutar código de forma remota.

La aplicación es vulnerable cuando carga XML desde fuentes no confiables, inserta datos no confiables en documentos XML o acepta XML directamente.
Para evitar este tipo de debilidad en la aplicación se recomienda encarecidamente actualizar los procesadores y bibliotecas XML de la aplicación o el sistema subyacente así como el uso de validadores de dependencias. También es recomendable deshabilitar las entidades externas de XML y procesamiento DTD en todos los analizadores sintácticos XML de la aplicación.

2.5 Pérdida de Control de Acceso

Los atacantes pueden utilizar una mala gestión sobre las restricciones de los usuarios autenticados para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc.

Para poder prevenir este tipo de accesos ilegítimos la política en caso de dudas debe ser denegar predeterminadamente y el personal involucrado en los test de calidad deberían incluir pruebas de control de acceso en sus pruebas.

2.6 Configuración de Seguridad Incorrecta

La configuración de seguridad incorrecta es un problema que ocurre en todo tipo de tecnologías y se debe a una mala configuración de forma manual, por omisión o simplemente por la falta de esta.
Como ejemplos de esta debilidad podríamos clasificar desde mensajes de error que dan demasiada información, pasando por ausencia de parches y actualizaciones, hasta dependencias y componentes desactualizados.

El abanico de malas prácticas que caerían bajo esta vulnerabilidad es demasiado amplio, pero los más comunes podrían ser:
Software desactualizado o que tiene vulnerabilidades conocidas sin parchear.

Para los sistemas actualizados, cuando las nuevas funciones de seguridad se encuentran desactivadas o no se encuentran configuradas de forma adecuada o segura.
Instalar o habilitar características innecesarias, como podrían ser puertos, cuentas o servicios, y dejar en estos las cuentas predeterminadas activadas con sus contraseñas por defecto.

Estos defectos se podrían evitar haciendo uso de una plataforma minimalista sin funcionalidades más allá de las extrictamente necesarias o componentes que puedan significar una mayor exposición.
Se recomienda la automatización de los procesos de actualización de los componentes y un proceso automatizado para verificar la efectividad de los ajustes y configuraciones en todos los ambientes.

2.7 Secuencia de Comandos en Sitios Cruzados (XSS)

Los XSS se dan cuando una aplicación acepta datos de fuentes no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con estos datos a través de una API del navegador que ejecuta JavaScript. Hay tres tipos de *Cross Site Scripting*:

XSS Reflejado: La aplicación o API utiliza datos obtenidos del usuario sin validar y son codificados como parte del HTML o Javascript de salida. Un ataque exitoso permite al atacante ejecutar comandos arbitrarios (HTML y Javascript) en el navegador de la víctima.
XSS Almacenado, la aplicación o API almacena datos proporcionados por el usuario que a posteriori son visualizados o utilizados por otro usuario o administrador. Este suele ser el más peligroso de los tres tipos.
XSS Basado en DOM, *frameworks* en JavaScript, aplicaciones de página única o APIs incluyen datos dinámicamente, controlables por un atacante.

Para prevenir ataques XSS se recomienda usar *frameworks* que por diseño codifiquen el contenido, como Ruby 3.0 o React JS.
Contra el XSS Reflejado y el XSS Almacenado bastaría con codificar los datos de requerimientos HTTP no confiables en los campos de salida HTML, mientras que para evitar el DOM XSS al modificar el documento en el navegador cliente hay que aplicarle codificación sensitiva del texto.

2.8 Deserialización Insegura

Sucede cuando una aplicación recibe objetos serializados maliciosos con el objetivo de realizar ataques de repetición, inyecciones, elevar sus privilegios de

ejecución o incluso puede desembocar en la ejecución remota de código en el servidor.

Para evitar este tipo de ataques se recomienda utilizar medios de serialización que solo permitan datos primitivos o no aceptar objetos serializados de fuentes no confiables.
Si esto último no es posible se recomienda aislar y verificar el tipo de dato durante la deserialización y antes de la creación del objeto.

2.9 Uso de Componentes con Vulnerabilidades Conocidas

Los componentes como bibliotecas, *frameworks* y otros módulos suponen un vector de ataque al ejecutarse con los mismos privilegios que la aplicación.
Si un solo componente es vulnerable puede provocar una pérdida de datos o que el atacante tome el control del servidor. Las aplicaciones y API que utilizan estos componentes con vulnerabilidades son por extensión también vulnerables.

Una aplicación es con alta probabilidad vulnerable si no conoce las versiones de todos sus componentes, si su software es vulnerable o se encuentra desactualizado, si no se actualiza la plataforma subyacente, los *frameworks* y sus dependencias o si no se asegura la configuración de componente correctamente, como se vio en Configuración de Seguridad Incorrecta.

Para prevenir esto es fundamental eliminar dependencias de funcionalidades, componentes, archivos y documentación innecesaria, así como inventariar las versiones de los componentes en uso y estar al tanto de las nuevas vulnerabilidades para los dispositivos soportados, pero sobre todo para retirar los descontinuados.
Todo esto último podría realizarse mediante evaluadores y gestores de vulnerabilidades, que este documento se encargará mostrar en los siguientes capítulos.

2.10 Registro y Monitorización Insuficientes

El registro y monitorización insuficiente, junto a la falta de respuesta ante incidentes explica en gran medida los históricos ciberataques que se expondrán en el siguiente capítulo.
La falta de esta monitorización permite a los atacantes mantener en el tiempo una intrusión exitosa, allanando el terreno del atacante para manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es superior a 200 días, siendo detectado normalmente por terceros, en

lugar de por procesos internos.

Con el fin de poder detectar y prevenir estas brechas a tiempo se recomienda registrar cuentas sospechosas con errores de inicio de sesión, de control de acceso y de validación de entradas de datos del lado del servidor. También establecer una monitorización de actividades sospechosas para todos los efectivos.
Asegurarse de que las transacciones de gran valor son trazables a posteriori y de tener un plan de respuesta o recuperación de incidentes en caso de que el ciberataque ya haya ocurrido.

2.11 Normativa

Hoy en día cualquier empresa por pequeña que sea tiene una página web, la cual de normal también tiene un formulario de contacto. Contando solamente con esta funcionalidad tan simple ya se está obteniendo datos personales e información privada del usuario, y esta se va a tener que gestionar de una forma correcta y con una seguridad adecuada para estos datos recolectados.
Un formulario de contacto es una cantidad ínfima de información si lo comparamos con negocios que operan directamente a través de internet, los cuales pueden llegar a albergar contenido del usuario tan sensible como fotos o datos de la tarjeta de crédito o contraseñas. Cuanto mayor es el valor de esta información mayor es la probabilidad de que hayan ciberatacantes buscando conseguirla, y por ende mayor riesgo en general para la compañía.

Si la seguridad de la propia empresa y los ciberatacantes acechando no fueran suficiente motivación para implementar medidas de seguridad como la evaluación y gestión de vulnerabilidades, también están las leyes.
Las leyes en torno a la protección de datos han estado en la palestra durante estos últimos años debido a las prácticas abusivas de múltiples empresas tecnológicas y los continuos ciberataques que publican la información de los usuarios del producto, como se verá en algunos ciberataques históricos. También se ha dado una mayor concienciación por parte del usuario medio de internet del poder que tienen estos datos que ceden de forma gratuita.
Como resultado de este cambio de mentalidad en la sociedad y una necesidad por parte de los estados de regular la situación de estos datos, los legisladores se pusieron manos a la obra tanto a nivel europeo como a nivel nacional en España. Las leyes más importantes en cuanto a protección de datos son la LOPD y la GDPR, a nivel nacional y europeo respectivamente, que se explicarán en los siguientes puntos.

2.11.1. GDPR

El Reglamento General de Protección de Datos (RGPD o GDPR) es una normativa europea que afecta con carácter obligatorio desde el 25 de mayo de 2018 a todas las empresas que traten datos de ciudadanos europeos.

La tramitación y aprobación de la GDPR se hizo en 2016, pudiendo aplicarse desde entonces, pero se concedió un amplio plazo de implementación de dos años para no entorpecer a las empresas.

Estas restricciones se aplican a todas aquellas entidades que traten datos de carácter personal de usuarios que se encuentren dentro de la Unión Europea. Esto incluye a responsables y encargados no establecidos en Europa pero con datos de ciudadanos de la UE.
La GDPR contempla que la actuación cuando ya se ha dado la infracción no es suficiente como estrategia, ya que esta puede suponer unos daños a los interesados difícilmente compensables o reparables. Es por ello que estas empresas que tratan datos tienen que llevar a cabo un análisis de riesgo de sus procedimientos para determinar qué medidas han de aplicar y cómo hacerlo.

Para obtener los datos de carácter personal se incide en que la obtención de estos debe de sustentarse en un consentimiento por parte del usuario libre, informado, específico e inequívoco; no aceptándose un consentimiento tácito que servía en anteriores normativas como la antigua LOPD.
A la hora de obtener este consentimiento las empresas tienen la obligación de informar de una manera concisa, transparente e inteligible, de una forma clara y concisa en torno a la base legal para el tratamiento de los datos, los períodos de retención de los mismos y otros aspectos. También es obligatorio informar al titular de los datos cómo puede ejercer sus derechos sobre estos, como el derecho de portabilidad, por el cual la organización debe proporcionar al titular la información que tiene suya en un formato estructurado y de uso común.

La GDPR introduce un nuevo cargo en la organización, el Delegado de Protección de Datos (DPD), encargado de velar por el cumplimiento de las normativas para la protección de datos.
Este cargo será de carácter obligatorio en autoridades y organismos públicos, empresas responsables del tratamiento de datos de carácter sensible a gran escala y empresas responsables de datos que requieran una observación habitual y sistemática de interesados a gran escala.

Se establece como responsabilidad de la organización el realizar una valoración del riesgo de los tratamientos que se van a realizar para poder definir las medidas a aplicar y cómo deben hacerse.
Respecto al tratamiento de los datos se deberá dar cuenta de un registro de actividades de tratamiento, incluyendo la finalidad del tratamiento de datos, categoría de los datos usados, los sistemas de tratamiento y las medidas de seguridad aplicadas durante el proceso para organizaciones de más de 250 empleados o cuando se traten datos sensibles.

Como ya se ha mencionado con anterioridad la GDPR contempla una protección de datos desde el diseño, forzando a las empresas a a analizar la seguridad en términos de protección de datos de cualquier proceso que implique el tratamiento de datos personales.
Para garantizar esta seguridad se deberán establecer las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función

de los riesgos detectados.

Finalmente en esta normativa europea se obliga a la notificación de violaciones de seguridad, exigiendo que las brechas en la seguridad que puedan afectar a los datos personales sean notificadas en un plazo máximo de 72 horas a la Autoridad de Control correspondiente, en el caso de España la Agencia Española de Protección de Datos. Si algunos de los datos afectados son de carácter sensible y de gran repercusión, también se lo deberá notificar a los afectados.

2.11.2. LOPD

La Ley Orgánica de Protección de Datos de Carácter Personal se encuentra vigente en España desde el 14 de Diciembre de 1999 con objeto de *'garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar'*[10] que se sustenta en el artículo 18 de la Constitución Española que enuncia: *'La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos'*.

Principalmente esta ley obliga a dar de alta los ficheros con datos de clientes en la Agencia Española de Protección de Datos, elaborar y mantener actualizado el Documento de Seguridad, en el cual se deben incluir las medidas de seguridad a nivel técnico y organizativo de la empresa, y obtener la legitimidad de los datos por parte de los afectados.
Hasta el 25 de mayo de 2018 estaba vigente exclusivamente la LOPD, pero a partir de esta fecha entró en vigor la GDPR, derogando parte de esta normativa. Por esta razón era necesaria una nueva LOPD que se centrara en complementar la ley europea, a la par que profundizando en temas que no incide tanto la GDPR.

Es por ello que el pasado 10 de noviembre de 2017, se aprobó el proyecto de la nueva Ley Orgánica de Protección de Datos, con el fin de modificar y complementar el marco general que establece la GDPR. Esta nueva ley sustituye a la anterior LOPD y en ella encontramos diversos cambios que afectan a una gran parte de las empresas que caen bajo esta ley.
Están obligadas a cumplir esta ley tanto las empresas, organizaciones públicas o privadas que almacenen, utilicen o traten datos de clientes, trabajadores y grabaciones de cámaras de vigilancia.
De las nuevas medidas casi todas están ya implementadas en la GDPR y destacan:

- Solo se puede pedir consentimiento para solicitar los datos que sean exclusivamente necesarios para el servicio y/o producto prestado al usuario.
- El consentimiento para la cesión de datos por parte del usuario debe ser activo y verificable, teniendo que ser registrado para posteriores comprobaciones.
- Los avisos de seguridad al usuario deberán tener la base legal del tratamiento de datos especificada, al igual que informar del tiempo que se retendrán

[10] *BOE núm. 298 de 14 de Diciembre de 1999*

los datos. Todo esto debe de ser expuesto de una forma clara y concisa para facilitar la comprensión del lector.

- El usuario tendrá derecho a solicitar la eliminación de sus datos si estos se han recogido de forma ilícita, si ha retirado de forma adecuada su consentimiento o si estos ya no son necesarios.
- El alcance de esta ley se extiende a fuera de la Unión Europea, siendo aplicable cuando el producto y/o servicio sea ofrecido a ciudadanos que pertenezcan al territorio europeo.
- Todas las empresas con bases de datos de organismos públicos o dedicadas al tratamiento masivo de datos tendrán que nombrar un Delegado de Protección de Datos (DPD) que se encargará de supervisar las prácticas de la empresa para el cumplimiento de las normativas actuales. Este empleado debe poseer conocimientos jurídicos en la materia.
- Cuando se vaya a realizar una modificación significativa sobre cualquier aspecto que tenga incidencia en los datos deberá realizarse un análisis de riesgos y viabilidad para evitar que los datos puedan ser expuestos.

Las empresas que no actúen conforme a estas dos normativas desde el 26 de mayo de 2018 pueden ser objeto de sanción.
Estas sanciones pueden llegar hasta los 20 millones de euros u oscilar entre el 2 % y el 4 % del volumen de negocio en función de la gravedad y cantidad de infracciones cometidas.

Tanto la GDPR como la LOPD de 2018, inciden mucho más en la proactividad por parte de las empresas en la protección de los datos, haciendo uso de estas sanciones para mostrar a las empresas la importancia de implementar unos sistemas de seguridad apropiados, pero sobre todo para tener una planificación y evaluación de riesgos apropiada en cuanto al tratamiento de datos personales.

CAPÍTULO 3
Ataques históricos

Ya se ha hablado de la situación actual del mundo de la ciberseguridad, y no merece menos atención la causa última por la que esta seguridad es tan importante: los ciberataques.
El término ciberataque abarca un abanico demasiado grande de acciones por parte del atacante que no deja lugar a una definición concreta de este.
Un ciberataque se puede definir como el proceso mediante el cual un atacante hace uso de sus habilidades o herramientas para modificar sistemas de información informática, infraestructuras, redes informáticas y/o dispositivos informáticos personales del objetivo con el fin de destruir, alterar o robar estos activos.

La perspectiva de futuro respecto de los ciberataques no es halagüeña, como se muestra en el informe Winning the Game, llevado a cabo por McAfee, donde el 46 % de los profesionales de la ciberseguridad encuestados afirman que en el año venidero les costaría o directamente sería imposible manejar el incremento esperado en ciberamenazas para defender sus sistemas[11].
Tampoco dan muchas esperanzas encuestas como la realizada por el Departamento para Digital, Cultura, Medios y Deportes donde se deja en evidencia que en 2017 dos quintos de las firmas británicas sufrieron ciberataques exitosos[12], o, mirando al futuro, previsiones de proveedores mundiales de inteligencia de mercado como International Data Corporation España (IDC), que prevee para 2021 que el 25 % de nuestros datos personales habrán sido comprometidos[13].

Recientemente también se han dado noticias que invitan a un punto de vista más optimista. Los funcionarios de Europol han cerrado la página WebStresser y procedido a arrestar a los administradores y benefactores de esta web. En ella se ofrecían como servicio ataques DDos[1] desde 2015 y había conseguido erigirse como líder de mercado en este tipo de actividad criminal[14].

Pero para comprender realmente dónde estamos hay que saber de dónde venimos. Y es que han tenido lugar ciberataques que han costado millones a grandes empresas, o incluso la quiebra debido a la pérdida de toda la credibilidad que pudieran tener.

[1] *Distributed Denial of Service: Ataque de denegación de servicio distribuido, el cual impide el acceso de usuarios legítimos a un recurso o servicio mediante una sobrecarga de los recursos del sistema atacado al generar un gran flujo de datos desde diversos puntos hacia este sistema.*

Por ello y para mostrar los casos reales que se dan cuando no se adoptan políticas correctas en cuanto a la evaluación y gestión de vulnerabilidades, se procederá en los siguientes puntos a exponer en orden cronológico los casos más significativos que se han dado en la historia de esta joven rama de la informática:

3.1 Stuxnet - 2010

Fue el ciberataque pionero en la posteriormente denominada ciberguerra. Stuxnet es el nombre de la pieza de *malware* que la NSA usó como ciberarma para retrasar el programa nuclear iraní.

El virus se transmitió haciendo uso de cuatro vulnerabilidades de día cero o 0-day de Windows, infectando cada equipo Windows en el que se insertaba el dispositivo de almacenamiento USB con el virus. Este nuevo sistema infectado se ocupaba de infectar a toda su red privada y cualquier USB que se conectara en un futuro a cualquiera de estos sistemas. El virus no fue detectado en un primer momento gracias a que le fueron implementadas firmas de aplicaciones benignas, haciéndole pasar bajo el radar de los antivirus.

El objetivo de este ataque era la central nuclear Natanz, en Irán. Stuxnet tenía como objetivo los controladores industriales Siemens S7-315, usados por los iraníes en sus centrifugadoras. El *malware* se encargaba de hacer grandes variaciones en la velocidad de los rotores de las centrifugadoras, reduciendo drásticamente su vida útil debido a la vibración de estos y retrasando el programa nuclear iraní.

Aunque no se pueden establecer fechas concretas parte de los componentes de Stuxnet datan de Junio de 2009 y el *malware* fue finalmente descubierto posteriormente gracias a su descontrolado contagio de sistemas por la compañía VirusBlokAda en Junio de 2010; asegurándole a este ciberataque como mínimo unos meses de máximo impacto[15].

3.2 Saudi Aramco - 2012

El 15 de Agosoto de 2012 un técnico del equipo de informática de esta empresa saudí accedió desde su correo a un enlace fraudulento, a continuación la red de ordenadores de Saudi Aramco fue infectada con un virus auto-replicado que infectó sus 35,000 máquinas basadas en Windows.
Este ataque provocó una caída total de la red de la petrolera, que aunque su producción petrolera automatizada no dependía de estos sistemas, toda la logística y el resto de operaciones sí. No es de extrañar que la petrolera haya mantenido este ataque en la más absoluta discreción dado que por aquél entonces suministraba el 10 % del petróleo mundial y se vio obligada a trabajar usando faxes y máquinas de escribir.

Sin embargo, pese a la gravedad del ciberataque podría haber sido mucho peor según la investigación de FireEye. Aseguran que el objetivo del ataque era en realidad el Sistema de Seguridad Instrumentado (SIS), encargado de la protección del proceso de manufactura. El *malware* falló y como efecto colateral dejó inutilizable la red de Aramco, pero se presume que los daños hubieran sido ostensiblemente mayores de haber funcionado correctamente.

Como efecto colateral Saudi Aramco se vio obligada a comprar un gran volumen de discos duros inmediatamente, por ello el precio de estos entre Septiembre de 2012 y Enero de 2013 a nivel mundial fue ligeramente superior a su verdadero valor[16].

3.3 Yahoo - 2013/2014

La mayor brecha de seguridad conocida en la historia de los ciberataques. Según las declaraciones de Yahoo se produjo en dos fases en 2013 y 2014 respectivamente, ascendiendo a 3,000 millones las cuentas afectadas por el ataque.

Datos como nombre, fecha de nacimiento, números de teléfono y contraseñas de usuario cifradas con una seguridad débil. Esta información fue la que obtuvieron los atacantes de cada usuario. Las cifras definitivas del ataque no fueron reveladas hasta que Yahoo concretó su conveniente venta al gigante de las telecomunicaciones Verizon por 4,480 millones.

La autoría y método del ataque no han sido confirmados, aunque las investigaciones del FBI apuntan a hackers rusos haciendo uso de ingeniería social[17].

3.4 Ashley Madison - 2015

Ashley Madison, la página para poner en contacto a gente que busca una relación extra-marital, fue expuesta en 2015 por el autoproclamado grupo de hacktivistas[2] Impact Team. El caso no supuso un gran escándalo por la nada desdeñable cifra de 32 millones de usuarios afectados, con información financiera incluida, sino por la información que se descubrió sobre las políticas de la empresa tras ser expuesta.

Los datos se expusieron en dos tandas, tras la primera Ashley Madison afirmó que los datos eran falsos pero quedaron en evidencia tras el segundo volcado de datos, que incluía mails de personal de la empresa, incluido el CEO.

[2] *Hacktivista: Persona que realiza ciberataques con objeto de la defensa de unos ideales o fines políticos.*

El caso no quedó ahí, ya que se descubrió que pese a cobrar por borrar totalmente los datos de los usuarios registrados, ese borrado nunca llegaba a tener lugar, y también se descubrió un número significativo de *bots*[3] entre las supuestas usuarias femeninas.

Nunca se llegó a confirmar cómo se realizó el ataque aunque todo parece indicar que se trató de una filtración de datos por parte de un trabajador de la empresa. Contra todo pronóstico la empresa sobrevivió tras pagar 11,2 millones de dólares a las víctimas del filtrado y la página sigue ofreciendo sus servicios[18].

3.5 Hacking Team - 2016

Este caso no es tan destacable por el impacto real del ciberataque sino por la víctima que cayó con él.
Hacking Team, empresa italiana dedicada a la venta de herramientas de vigilancia e intrusión ofensiva a gobiernos, empresas y agencias de aplicación de la ley, fue totalmente expuesta por el hacktivista que opera bajo el seudónimo de Phineas Fisher.

El ataque que logró controlar todos los sistemas de la empresa de ciberseguridad que mueve millones de euros al año fue realizado por un solo hacker, lo cual es sin duda uno de los hitos en la historia de los ciberataques.

Todo parece indicar que P.F. encontró una vulnerabilidad 0-day y creó una pieza de *malware* que hacía uso de esa vulnerabilidad, siendo este diseñado para evitar los sistemas de detección de la empresa italiana. A continuación consiguió extraer todo el código fuente de Hacking Team gracias a sus propios backups y eludiendo todas las medidas de seguridad de sus sistemas, lo que es sin lugar a dudas una proeza histórica en el mundo de la seguridad informática[19].

3.6 Banco Central de Bangladesh - 2016

Si hay un sector al que se le asume una sobresaliente ciberseguridad este es sin duda el bancario. Por lo general esta afirmación es verdadera, pero en este caso no fue así, y podría haber tenido unas consecuencias desastrosas de no haber sido por la torpeza del atacante y la astucia de los oficiales bancarios.

La víctima del ataque fue el Banco Central de Bangladesh y el objetivo se limitaba al robo de dinero. El atacante hizo uso de un sofisticado *malware* para obtener acceso al software de SWIFT Alliance Access, ejecutado en la infraestructura del

[3] *Bot: Programa informático autónomo que es capaz de llevar a cabo tareas concretas e imitar el comportamiento humano*

banco. SWIFT es el proveedor global de servicios seguros de mensajería financiera, el cual es usado para transferir cientos de millones cada hora.

Aunque SWIFT negó el impacto de el *malware* en sus servicios de mensajería el atacante llegó a robar 81 millones de dólares, que podrían haber sido hasta mil millones de no ser por un error ortográfico que el cibercriminal cometió en una transacción e hizo saltar todos los sistemas de detección.
Todavía no se ha identificado cómo se pudo llegar a cometer el ataque ni se ha podido recuperar la mayor parte de esos 81 millones que fueron transferidos a Filipinas[20].

3.7 Wannacry - 2017

Finalmente no se podía acabar con un ataque que no fuera de la especialidad del cibercrimen en 2017: *Ransomware*.
El *ransomware*, como ya se ha explicado, es un tipo de *malware* que cifra los archivos del equipo infectado y que posteriormente pide un 'rescate' a la víctima para descifrar y recuperar sus propios archivos.

Este tipo de ataques fueron lanzados por oleadas durante todo el año pero la campaña Wannacry destaca sobre el resto.
El ciberataque fue lanzado a nivel mundial con un origen desconocido y afectó a casi todos los países del mundo; grandes empresas españolas como Gas Natural, Iberdrola o Telefónica cayeron víctimas de este *ransomware*.
El alcance del ataque podría haber sido mucho mayor si Marcus Hutchins, experto en ciberseguridad británico, no se hubiera dado cuenta de que el *malware* primero hacía una petición a un dominio inexistente antes de cifrar los archivos. Una vez Marcus adquirió este dominio el *ransomware* dejó de cifrar los archivos.

Pero lo más grave del caso es que Wannacry hacía uso de EternalBlue como *exploit*[4] para difundirse, una vulnerabilidad ya conocida y publicada que había sido solucionada en el parche de seguridad de Microsoft MS17-010, disponible desde el 14 de Marzo de 2017.
La campaña de Wannacry fue lanzada el 12 de Mayo de 2017, prácticamente un mes después del lanzamiento del parche de Windows[22] y logró llegar a sacudir los cimientos de grandes multinacionales[21].

[4] *Exploit: Software que hace uso de una vulnerabilidad informática para provocar un comportamiento no deseado en el sistema que se ejecuta.*

CAPÍTULO 4
Evaluación y Gestión de Vulnerabilidades

Una vez mostrado el panorama de la ciberseguridad en la actualidad, revisados los ciberataques que nos han hecho aprender y mejorar hasta el día de hoy; y teniendo en cuenta la normativa vigente de protección de datos, se van a responder las preguntas que probablemente se hace el lector llegados a este punto del documento.

¿ Qué es la evaluación y gestión de vulnerabilidades ?

¿ Cómo puede ayudarme a estar más seguro ?

La primera no es una pregunta fácil de responder ya que no hay un consenso en cuanto a los términos. A menudo te puedes encontrar empresas donde la evaluación de vulnerabilidades, o *vulnerability assessment*, es ofrecida como lo que la mayoría de empresas venden como gestión de vulnerabilidades, o *vulnerability management*.

Generalmente se define la evaluación de vulnerabilidades como el proceso de catalogar recursos, identificar, cuantificar y priorizar vulnerabilidades; mientras que la gestión de vulnerabilidades se entiende como el proceso de buscar, identificar, verificar y mitigar amenazas.
Pese al hecho de que estas dos definiciones que se superponen están muy extendidas, no consiguen evitar que las empresas que ofrecen estos servicios les cambien el nombre o que ofrezcan ambas bajo el nombre de una, todo esto sin criterio alguno y solo respondiendo a la *buzzword*[1] del momento en el sector de la ciberseguridad.

Es por ello que en este documento de aquí en adelante se referirá a ambos conjuntos en un pack indivisible de uno solo. Más allá de los procedimientos que tienen en común a la hora de conseguir su objetivo, no sería concebible el uso de un conjunto de técnicas sin el otro, ya que sería a todas luces dejar el trabajo inacabado.
La evaluación de vulnerabilidades se alimenta de los procesos de la gestión de

[1] *Buzzword: Palabra que se hace muy popular por un periodo de tiempo.*

vulnerabilidades y viceversa, produciendo un resultado mucho más potente en términos de seguridad por un poco más de esfuerzo respecto del trabajo necesario para realizar uno de los procesos solo.

Se puede definir la evaluación y gestión de vulnerabilidades como el proceso de catalogar recursos, cuantificar la importancia de los recursos, identificar las vulnerabilidades de estos, verificar estas vulnerabilidades y realizar un plan para mitigar o eliminar estas amenazas en función de la importancia del recurso.

A continuación, para responder a la segunda pregunta se procederá a explicar la evaluación y gestión de vulnerabilidades en detalle.

4.1 Objetivos y Fases

El objetivo último de la evaluación y gestión de vulnerabilidades es resaltar los puntos vulnerables de un sistema y proporcionar las directrices necesarias para solventar estas vulnerabilidades de acuerdo a la criticidad del recurso.

Este gran objetivo puede desglosarse en otros objetivos menos ambiciosos que se tienen que ejecutar por fases y en orden, ya que cada uno de estos procesos depende de los datos generados como salida del proceso anterior.

Las fases que contribuyen a este gran objetivo se dividen en:

1. Catalogación de activos del sistema a auditar.

   En primer lugar hay que realizar un listado de todos los activos que se desean incluir en el proceso.
   Estos activos pueden ser de cualquier tipo, desde redes enteras hasta PCs individuales. Los activos dependerán del tipo de evaluación, como se explicará más adelante.

2. Descubrimiento de las vulnerabilidades para cada activo.

   Este es un proceso crítico, ya que un óptimo resultado final de la evaluación dependerá de la calidad y la cantidad de información recolectada durante esta fase.
   Escáneres de vulnerabilidades, *fuzzers*[2] y diccionarios de contraseñas para ataques de fuerza bruta son tan solo unas pocas de las herramientas necesarias para realizar el descubrimiento de vulnerabilidades.
   Cuanto mejores sean las herramientas integradas también serán mejores los resultados, y por ende, más probabilidad de que no se trate de falsos positivos.

3. Verificación de las vulnerabilidades descubiertas para cada activo.

[2] *Fuzzer: Técnica de pruebas de software que implica proporcionar datos inválidos, inesperados o aleatorios a las entradas de un programa de ordenador.*

No todas las vulnerabilidades encontradas lo son realmente.
En ciertas ocasiones los sistemas responden de una manera que nos puede sugerir que es vulnerable a cierto tipo de ataque cuando en realidad no lo es. Estos son los denominados falsos positivos.
El objetivo de esta fase es descartar la mayoría de estos falsos positivos generados en el descubrimiento de vulnerabilidades, asegurando que casi todas las vulnerabilidades que pasan a la siguiente fase no constituirán una pérdida de tiempo para el plan.

4. Cuantificación de la importancia de cada activo para el sistema.

   Una vez tenemos catalogados todos los activos sobre los que trabajaremos y las vulnerabilidades explotables, se procederá a realizar una evaluación de cada dispositivo en el contexto del sistema.
   Es importante contextualizar con todo el sistema, ya que activos que pueden parecer no críticos y con vulnerabilidades que sí lo son pueden llegar a hacer caer el sistema en función del rol que estos jueguen en el conjunto.

5. Elaboración de un plan de acción en función de la criticidad del activo y vulnerabilidad.

   Llegados a este punto ya tenemos todas las piezas para elaborar un plan de acción.
   Una vez que ya contamos con un listado de activos con su respectiva importancia para el sistema y vulnerabilidades ya filtradas solo queda que unir todas las piezas.
   Se priorizarán las vulnerabilidades en función de su criticidad para el sistema completo en vez de para el propio activo, buscando dar una mayor seguridad al sistema en conjunto.

6. Solución o mitigación de vulnerabilidades.

   Una vez establecida la hoja de ruta no queda más que seguirla.
   Dependiendo de quién o para quién se haga esta evaluación y gestión de vulnerabilidades como resultado obtendremos un informe ejecutivo, un informe técnico, una serie de cambios a realizar o directamente todo lo anterior.
   El resultado final de la evaluación y gestión de vulnerabilidades siempre será aplicar sobre nuestro sistema las recomendaciones o los cambios sugeridos por el documento final de acuerdo al orden de prioridades.

4.2 Tipos

La evaluación y gestión de vulnerabilidades no es una técnica que deje mucho lugar a la variación o la innovación, sin embargo sí que se pueden encontrar diferencias basándose en dos aspectos.

Por un lado se clasificaría por el origen de la evaluación, la zona desde donde

se lanzan todos los procesos relacionados con los tests, mientras que por otro lado se diferencia en función del alcance del escaneo, pudiendo tener como objetivo una sola máquina, una red, una aplicación, etc.

4.2.1. Origen

Externo

El test externo o *black box* es realizado desde fuera del sistema a analizar, sin un conocimiento previo de las características de este o de cualquier información privilegiada y con la intención de comprometer el sistema desde el exterior.

Se suele comenzar con un trabajo de reconocimiento a través de OSINT[3] para conseguir un poco de información extra que pudiera ayudar en las siguientes fases del test, que son iguales a las explicadas previamente.

En este tipo de evaluación se obtendrá el punto de vista de un atacante sin acceso al sistema, por ello la información recolectada será presumiblemente menor a la obtenida en una evaluación de tipo interno pero más crítica al ser accesible directamente desde el exterior.

Interno

El test interno o *white box* es realizado desde el interior del sistema a analizar, en este tipo de evaluación es usual contar con información previa de la estructura del sistema y se asume el rol de alguien de dentro en el que se confía, o directamente es realizado desde un agente instalado en un activo.

También es habitual en este tipo de evaluaciones que se otorgue al evaluador un nivel de privilegios moderado, de cara a analizar qué problemas podría causar un usuario malicioso con esos privilegios o incluso si se podría llegar a elevar esos privilegios iniciales de manera fraudulenta.

Cuando se realiza la evaluación desde esta situación se enfoca más a los riesgos respecto de un atacante que ha conseguido un acceso limitado al sistema o un agente supuestamente confiable del sistema que está actuando contra este.

Sin embargo la evaluación y gestión de vulnerabilidades bien implementada realiza ambos tipos de evaluación a la vez, beneficiándose cada tipo de los resultados obtenidos del otro y otorgando una visión más completa de las vulnerabilidades del sistema.

4.2.2. Alcance

Como también se ha explicado en los tipos de evaluación según el origen, un test completo de evaluación y gestión de vulnerabilidades combinará los cinco

[3] *Open Source Intelligence: Inteligencia de fuentes abiertas*

tipos de alcance que se exponen a continuación, obteniendo así una evaluación del sistema lo más completa posible.

Red

Los escaneos basados en red combinan el descubrimiento de *hosts* y servicios con la enumeración de vulnerabilidades.

En este tipo de evaluación se identificarán los distintos dispositivos que componen la red, determinando su importancia en el sistema y posibles vulnerabilidades.

Una característica de este tipo de evaluación es el uso de la técnica del *fingerprinting*, mediante la cual se averigua el tipo y versión del dispositivo a partir de las respuestas que este proporciona, pudiendo luego buscar vulnerabilidades específicas para ese tipo de dispositivo.

Host

Los escaneos basados en *host* se centran solamente en un dispositivo, del que se puede tener un usuario y contraseña proporcionados con anterioridad para tener una vía acceso a la máquina.

Es por esto último que este escaneo puede aportar una mejor imagen de las configuraciones establecidas y parches aplicados en cada dispositivo.

Una desventaja de este tipo de tests es que debido a la gran cantidad de configuraciones y características a las que tiene acceso el tiempo de análisis de estas también será superior, prolongando la duración total del escaneo.
Por ello es muy importante encontrar un buen equilibrio entre el alcance deseado y el tiempo que estamos dispuestos a asumir.

Wireless

Los escaneos basados en *wireless* son similares a los de red, ya que también presentan primero un descubrimiento de dispositivos y *fingerprinting*, pero esta vez mediante Wi-Fi.

Principalmente se ocupa de revisar las configuraciones de seguridad del Wi-Fi como pueden ser el uso de un cifrado estándar seguro o que el WPS se encuentra deshabilitado.

También detecta puntos de acceso maliciosos o posibles entradas a la red interna desde de la red de invitados.

Aplicación

Los escaneos de aplicación se suelen concentrar en los sitios web para detectar malas configuraciones o vulnerabilidades del software usado.

Este tipo de tests suelen tratar las vulnerabilidades típicas de la web, que ya se han explicado en el OWASP Top 10, como pueden ser las inyecciones SQL, ataques XSS o la exposición de datos sensibles entre otros.

Debido a la batería de pruebas realizadas por este tipo de escaneos se recomienda realizarlos en un entorno que no sea de producción o hacer uso de pruebas no intrusivas, ya que algunas de estas vulnerabilidades pueden llevar a un cambio permanente no deseado en la web auditada.

Base de datos

Los escaneos de base de datos se centran en las vulnerabilidades características de las bases de datos, como pueden ser las inyecciones SQL o los troyanos de base de datos.

Al igual que en los escaneos de aplicación es recomendable no realizar estos tests en un entorno de producción a no ser que se conozca perfectamente la batería de pruebas realizadas y los posibles efectos que estas tienen sobre la base de datos.

4.3 Herramientas

Todo lo explicado hasta ahora no sería realizable si no se contara con las aplicaciones de más bajo nivel necesarias para hacer estos descubrimientos.
No es la intención de este apartado realizar un análisis exhaustivo de todas ellas, ya que se saldría del alcance del documento, sino explicar brevemente qué uso se les dan en cada fase de la evaluación y gestión de vulnerabilidades.

4.3.1. Catalogación de activos

Para catalogar activos del sistema se hace uso de soluciones de descubrimiento automatizado y gestión de activos.

Estas herramientas realizan un escaneo del sistema a evaluar para registrar todos los dispositivos que se encuentren. Estos activos se pueden ver, gestionar y editar a posteriori, así como actualizar los activos tras nuevos escaneos.

En el mercado podemos encontrar herramientas especializadas en la gestión de activos como pueden ser Endpoint Manager, ManageEngine AssetExplorer, MMSoft Pulseway o Asset Panda entre otros.

4.3.2. Descubrimiento y verificación de vulnerabilidades

Para descubrir los agujeros de seguridad en el sistema se hace uso de escáneres de vulnerabilidades. Esta es la herramienta más importante de todo el proceso, además de por ser la que aporta el grueso de información de la evaluación, se trata de una herramienta que realiza diversas funcionalidades al mismo tiempo. El escáner de vulnerabilidades está compuesto por otras herramientas para funcionalidades más específicas, como pueden ser pruebas de fuerza bruta con diccionarios de contraseñas por defecto, fuzzers para descubrir dominios no bloqueados a usuarios sin autenticar o el archiconocido escáner de puertos Nmap[4].

Al ser aplicaciones con soluciones tan específicas también se pueden dividir prácticamente en los mismos tipos presentados para el alcance de la evaluación. Cada uno de ellos se especializa en vulnerabilidades y fallos de configuración de su tipo en concreto.
A continuación se muestran unos pocos ejemplos de las clases más usuales:

- Escáner de vulnerabilidades de red: Nessus, Qualys, Acunetix, OpenVAS, Nexpose, etc.
- Escáner de vulnerabilidades de aplicaciones web: Nikto, Qualys, OWASP ZAP, w3af, Burp Suite, etc.
- Escáner de vulnerabilidades de bases de datos: Scuba, AppDetectivePro, McAfee Vulnerability Manager for Databases, AuditPro Enterprise, Microsoft Baseline Security Analyzer, etc.

4.3.3. Cuantificación de la importancia

La cuantificación de la importancia de una vulnerabilidad se suele llevar a cabo también por los escáneres de vulnerabilidades, que ya cuentan con sus propias puntuaciones para cada vulnerabilidad, como podrían ser Qualys, Nessus o Acunetix.

Pero si el escáner no tiene un ránking propio también puede hacerse uso del de terceros como Arcsight o idealmente del Common Vulnerability Scoring System (CVSS), un estándar de industria abierto y gratuito para evaluar la peligrosidad de la vulnerabilidad. Actualmente se encuentra bajo la custodia del NIST [5] y las puntuaciones oscilan entre 0 y 10, calificando de 0 a 3.9 como Bajo, de 4 a 6.9 como Medio y de 7 a 10 como Alto.

4.3.4. Elaboración de un plan de acción

A la hora de generar el documento final la mayoría de soluciones ya proporcionan un generador de informes automatizado, el cual no suele ser incorrecto pero es recomendable no usarlo como documento final.

[4] *Escáner de puertos Nmap,https://nmap.org/*
[5] *National Institute of Standards and Technology, https://www.nist.gov/*

A la hora de realizar los informes manualmente habrá que tener en cuenta varios aspectos en cuanto a la forma y el contenido, como bien se explica en el siguiente punto.

4.4 Informes

El informe es una parte fundamental de la evaluación y gestión de vulnerabilidades, ya que es el encargado de mostrar el trabajo realizado de una forma clara y comprensible.
Este documento debe contener toda la información útil adquirida en las diferentes fases y usar esta como justificación en la hoja de ruta propuesta para mejorar la seguridad del sistema.

Generalmente para una misma evaluación se generan dos tipos diferentes de informe final:

4.4.1. Ejecutivo

El informe ejecutivo está orientado a lectores que carecen de conocimiento técnico, centrándose en las consecuencias que podría ocasionar la explotación de las vulnerabilidades más que en el descubrimiento de las mismas.

Este documento, cuyo *target* suele ser personal ejecutivo, expone una visión general de la seguridad en el sistema auditado pasando por encima de las vulnerabilidades en cada dispositivo. También se explica el por qué de las vulnerabilidades cuya solución es prioritaria y finaliza con unas conclusiones generales extraídas de la evaluación.

La extensión de este documento tiene que ser significativamente menor al informe técnico y reducir al mínimo las tecnicidades usando un lenguaje asequible para poder llegar al mayor número de personal no especializado posible. No tendría mucho sentido presentar el informe ejecutivo sin uno técnico que lo respalde.

4.4.2. Técnico

El informe técnico está orientado a lectores con cierto nivel técnico o directamente a los profesionales encargados de llevar a cabo las modificaciones enumeradas en este documento. Es aquí donde sí que se tiene que mostrar absolutamente toda la información obtenida durante la evaluación.

Listado de dispositivos con una valoración de su importancia en el sistema, vulnerabilidades de cada dispositivo, vulnerabilidades del sistema en general, etc. Toda la información recopilada y que se considere de utilidad tiene cabida en este informe. Las dos partes más importantes de este documento son el listado de vulnerabilidades y el plan de acción.

En el listado de vulnerabilidades se mostrarán estas ordenadas en función del riesgo que suponen, detallando cada una explicando en qué consiste y el por qué de su prioridad, en muchas ocasiones incluso enlazando a parches del propio fabricante.

En el plan de acción se debe establecer un orden de prioridad a seguir en la mitigación de las vulnerabilidades para que se lleve a cabo con la mayor eficiencia en términos de seguridad inmediata. Esta hoja de ruta va destinada al profesional que se encargará de solucionar las vulnerabilidades y por ello puede ser de un nivel técnico alto.

Este informe es de una gran importancia ya que en última instancia es el único justificante de todo el trabajo realizado y por ello debe de dejar constancia de cada descubrimiento.

CAPÍTULO 5
Análisis de mercado

La evolución del mercado de las herramientas de evaluación y gestión de vulnerabilidades ha sido vertiginosa pese a tratarse de una práctica que cuenta con apenas 25 años de historia.

Los comienzos no fueron precisamente halagüeños. Con la inspiración del Gusano Morris[1], el investigador Dan Farmer desarrollaría la primera herramienta automatizada de evaluación de vulnerabilidades llamada Security Administration Tool for Analyzing Networks[2] (SATAN). Esta herramienta no fue bien acogida en la comunidad, ni siquiera en su versión ligeramente modificada SAINT.[3] Fue condenada por muchos, incluyendo al Departamento de Justicia de los EUA.

Para mediados de los 1990 y principios de los 2000 la empresas comenzaron a ver el nicho de mercado para las herramientas de estas características. Esta etapa coincidió con el repunte de los test de penetración o *pentesting*, que se popularizaron pese a la falta de buenos profesionales en el, por aquél entonces, joven sector.

A finales de los 1990 y gracias a la introducción de los escaneos con autenticado se produjeron dos grandes avances en el terreno de la evaluación y gestión de vulnerabilidades.
El primero fue un aumento significativo en la precisión de los escaneos, ya que estos tenían acceso para monitorizar todo el software y servicios instalados directamente en cada activo, en vez de tener que deducirlos a través de técnicas de *fingerprinting*.
En segundo lugar y como consecuencia del primero se llego a lograr la *endpoint security* o seguridad de terminal, proveyendo a las empresas de una visión más exacta de cada activo para evitar los principales ataques al *endpoint* como pueden ser los efectuados a través de Java y Flash.

Una vez que se iban madurando las soluciones ya existentes se comenzaron a desarrollar soluciones para las tecnologías emergentes y que más requerían de la

[1] *Gusano Morris: Datado en 1988 fue la primera muestra de malware autorreplicable, haciendo uso de exploits y contraseñas por defecto para propagarse por la red*

[2] *Security Administration Tool for Analyzing Networks: Herramienta de Administración de Seguridad para Analizar Redes*

[3] *Juego de palabras en inglés, cambiando el nombre para obtener las siglas SAINT o santo en vez de SATAN o satán.*

seguridad.

A finales de los 2000 se integraron los primeros escáneres de vulnerabilidades web a través de módulos de *fuzzing* o del mismo Nikto. Estos módulos se hicieron como respuesta a la creciente importancia de las inyecciones, las cuales se mantienen hasta día de hoy como se ha podido observar con el OWASP Top 10.

No fue hasta Octubre de 2016 cuando se inició la última tendencia. Con la adquisición de FlawCheck por parte de Tenable, se añadió a la solución de estos el escaneo de vulnerabilidades durante el proceso de desarrollo de contenedores.
Este movimiento supuso un puñetazo encima de la mesa por parte de la empresa de Maryland, al ser los primeros en proporcionar evaluación de vulnerabilidades para la popular tecnología de Docker.

Actualmente y desde que las empresas se orientan más a la nube la inercia es orientar todas estas soluciones a servicios ofrecidos desde y para la nube.

Pese a todas estas nuevas tecnologías hay otras muchas con un mayor recorrido y con las que cuentan la mayoría de las empresas de este sector.
A día de hoy casi todas la soluciones ofrecen escaneo autenticado, auditoria de la configuración y priorización de vulnerabilidades basadas en el contexto del negocio. Hay otras tecnologías menos comunes como el agente de sistema y la priorización basada en inteligencia de amenazas, acabando con las más exclusivas como el análisis de los registros de contenedores.

Sin embargo, aunque hayan empresas que tengan en común estas tecnologías, unas las logran potenciar más que otras debido a la combinación con herramientas de terceros o a una gran personalización de las mismas. Estos puntos se detallarán a la hora de exponer las soluciones de cada empresas en puntos posteriores.

Son estas pequeñas diferencias en la personalización y en la implementación de las soluciones que hacen tan importante la elección del producto que más se adapte a las necesidades únicas de cada empresa. Es por ello que antes de decidirse por una es recomendable contemplar los siguientes aspectos de cada solución:

- La gestión de activos, de esta enumeración de activos dependerán las siguientes fases del proceso y por ello es importante tener una buena base para obtener los mejores resultados posibles sin dejar fuera ningún activo.

- La calidad de la enumeración de vulnerabilidades, teniendo en cuenta los falsos positivos y falsos negativos, el uso de detección por escaneo activo y/o pasivo, el tipo de escaneo autenticado y/o no autenticado o incluso si la solución cuenta con un agente de sistema multiplataforma para realizar un escaneo más minucioso en cada equipo.

- La rapidez y la calidad de las actualizaciones, cuanto menor sea el tiempo de reacción del producto para incluir nuevas vulnerabilidades en su base de datos, más segura estará la infraestructura de la empresa.

- El soporte para servicios basados en la nube y contenedores, con la vista en un futuro donde todo parece orientado a la nube se antoja imprescindible el poder detectar malas configuraciones en herramientas que hagan uso de estos servicios, así como contenedores, que ya son una realidad más extendida.

- La compatibilidad de la solución tanto con distintos sistemas operativos como con herramientas de terceros, es imprescindible que aspectos tan críticos de la solución como puede ser la base de datos de firmas cubra todos los sistemas operativos y componentes de la infraestructura del sistema protegido, así como la posibilidad de integrarse con soluciones de terceros para obtener una mayor y más variada cantidad de información.

- La priorización, ya se ha hablado en puntos anteriores de la importancia de priorizar las amenazas. Hay que tener en cuenta el algoritmo de priorización del producto y ver si se acopla a las necesidades del sistema.

- La evaluación de la conformidad, es un gran añadido que el producto proporcione soporte para la conformidad con los diferentes estándares o normativas que se apliquen sobre el sistema, proporcionando información de las no conformidades e informes que las detallan.

- Los informes de remediación, hay que tener constancia de los documentos que genera la solución y ver si estos se adecuan a las necesidades de la empresa.

- La usabilidad de la solución, en última instancia la solución tendrá que se gestionada por personal de la empresa y cuanto menor sea la curva de aprendizaje y mayor usabilidad de la plataforma, mejores resultados se obtendrán.

- El soporte que ofrece el vendedor, un aspecto importante en cualquier producto y más aún si de este depende la seguridad de el sistema.

Como hemos podido observar, son muchos los aspectos a tener en cuenta a la hora de elegir la solución óptima para nuestra empresa.
Es por ello que en las siguientes páginas se explicarán en detalle los productos más diferenciados del mercado basándose en algunas empresas de The Forrester Wave o la Ola de Forrester, un estudio realizado por la multinacional de investigación de mercados Forrester, que evalúa el mercado de Gestión de Vulnerabilidades de Riesgo a fecha del primer cuatrimestre de 2018[23].

En este informe se clasifican las empresas en función de su oferta de soluciones actual y la fortaleza de su estrategia de futuro, teniendo también en cuenta su actual presencia en el mercado.
Una vez son situadas en la gráfica de acuerdo a sus calificaciones se dividen en Líderes, Actores Fuertes, Competidores y Desafiadores. Para obtener una visión general del mercado de la evaluación y gestión de vulnerabilidades también se han tenido en cuenta el informe 'Market Guide for Vulnerability Assessment' de Gartner [24] y 'Vendor Landscape: Vulnerability Management, 2017' de Forrester[25].

Figura 5.1: Vulnerability Risk Management Q1 2018 Forrester Wave

A continuación se procederá a detallar por separado las diferentes soluciones de cada empresa en los siguientes puntos para posteriormente realizar una comparativa objetiva de todas ellas en función de los servicios ofrecidos.

5.1 Líderes

5.1.1. Rapid7

Rapid7, Inc.[26] es una empresa fundada en el año 2000 que provee soluciones analíticas para operaciones de seguridad e información. Esta empresa con sede en

Boston ofrece estas soluciones mediante cuatro diferentes productos capaces de integrarse entre sí.

insightAppSec se encarga de comprobar la seguridad de las aplicaciones mientras se desarrollan para garantizar la seguridad una vez finalizada la aplicación, insigtIDR detecta intrusos en las primeras fases de los ciberataques, insightOps facilita la gestión de *logs* para conseguir un mayor conocimiento del estado de los activos e insightVM para la evaluación y gestión de vulnerabilidades completa.

metasploit merece una mención a parte entre los productos de Rapid7, al tratarse del famoso software para tests de penetración de equipos de seguridad ofensiva. Este producto es considerado sin lugar a dudas el mejor en su área y es utilizado por todo el mundo por su gran base de datos de *exploits* proveniente de Rapid7 y su versatilidad para realizar ataques.

El producto que interesa analizar en este caso es insightVM. Esta solución ofrece por si sola todas las fases que cabrían esperar en una implementación correcta de la evaluación y gestión de vulnerabilidades.
Para la catalogación de activos hace uso de los agentes instalados en cada punto. Estos agentes también ayudarán al escaneo de vulnerabilidades, el cual se realiza con otro exitoso producto de Rapid7, el escáner Nexpose, también líder en el sector del escaneo de vulnerabilidades gracias a la extensa y actualizada base de datos de vulnerabilidades de Rapid7.

Una vez obtenidos todos los datos de la red se procederá a validar y cuantificar la importancia de las vulnerabilidades según el sistema de puntuación propio de insightVM.

Con todo esto, insightVM proporciona una forma de recolectar datos de vulnerabilidades de una forma disponible en todo momento, escalable y eficiente a la hora de minimizar riesgos. Utiliza las últimas tecnologías analíticas en el activo para descubrir las vulnerabilidades en tiempo real, establecer su localización, priorizarlas de acuerdo al sistema y facilitar su solución.
Pero los dos apartados en los que se ha centrado Rapid7 es en proporcionar la mejor visibilidad de la red y facilitar una remediación los más eficiente posible.

Para asegurar una mejor visibilidad se apuesta por la monitorización de los activos continua gracias a Insight Agent. Este agente recolecta automáticamente datos de todos los activos, incluso de los trabajadores que se conectan en remoto, incluyendo los activos con información sensible que no son alcanzables mediante los escaneos activos o los que forman parte de la red empresarial solo temporalmente.

El impacto de Insight Agent en la red es mínimo ya que envía una captura con los datos del activo tras la instalación y posteriormente solo envía los cambios que se dan en este. Los datos que se obtienen de este agente se pueden unificar con los datos obtenidos de las soluciones insightIDR e insightOps, necesitando un único agente para usar los tres productos a la vez.

Figura 5.2: InsightVM panel de activos

Este agente se puede desplegar fácilmente sobre activos Windows, Mac y Linux, gestionando automáticamente las actualizaciones necesarias para este sin necesidad de configuración adicional.
Insight Agent también se puede incrustar en diferentes tecnologías como las imágenes de nube y virtuales para que estas sean detectadas tan pronto como se activen.

También con la intención de aumentar la visibilidad de la red se incorporan los insightVM Liveboards, unos paneles creados a partir de la información recolectada en vivo y que es interactiva de cara al usuario.
Estos paneles son altamente personalizables y pueden ser creados fácilmente mediante un lenguaje de consultas simple que filtra entre parámetros tan significativos como son el sistema operativo del activo o el tiempo desde el descubrimiento de la vulnerabilidad. La carga del procesamiento de datos se realiza en la nube de Rapid7, evitando la sobrecarga de procesamiento de paneles en vivo sobre la infraestructura del cliente.
Estos paneles creados se pueden compartir entre miembros del equipo de remediación en esta misma plataforma.

Por último, en cuanto a la visibilidad, se ha realizado un enfoque orientado a adaptarse a los cambios constantes de las redes modernas. Para ello insightVM se integra con servicios web (Amazon Web Services, Microsoft Azure), infraestructuras virtuales (VMware) y repositorios de contenedores (Docker) con el fin de detectar nuevos activos en el momento que se crean o que se desactivan y no perderse ningún activo de la empresa.
Estas integraciones permiten obtener una visión completa del riesgo en la infrestructura física, virtual, de nube y de aplicación. De todas estas funcionalidades destaca la evaluación de vulnerabilidades y malas configuraciones para contenedores, pudiendo incluso correlar estos con los activos donde se encuentran desplegados, securizando ambos con una mayor precisión.

También es posible sincronizar los registros públicos o privados de contenedores para evaluar sus vulnerabilidades antes de desplegarlos.

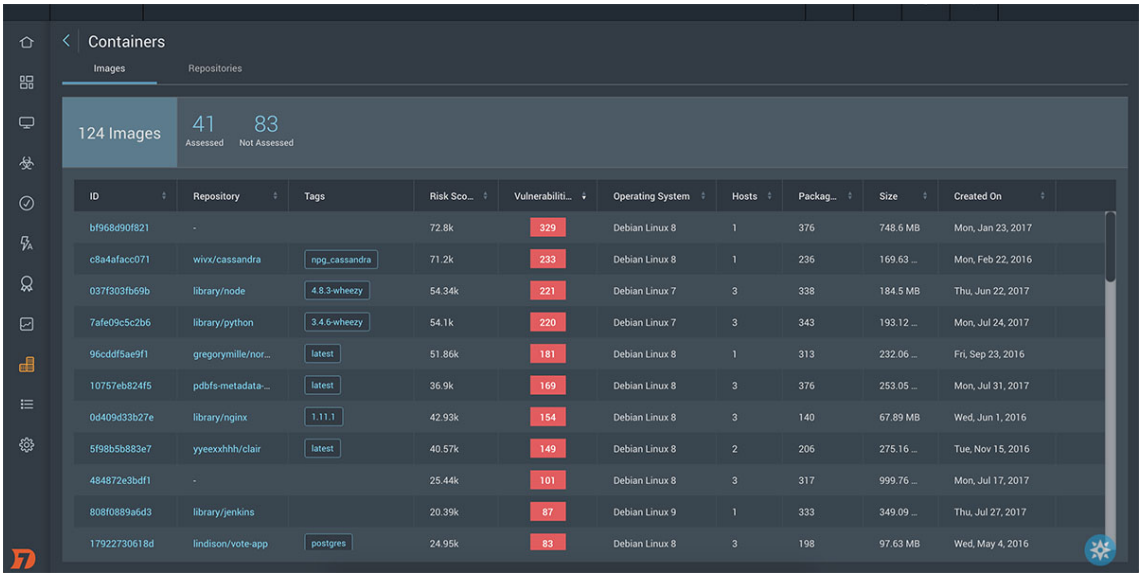

Figura 5.3: InsightVM evaluación de contenedores

En cuanto a la remediación de vulnerabilidades esta solución sorprende por lo básicos que son los informes generados. A cambio propone una planificación de la remediación en vivo, mediante la asignación y seguimiento del progreso de las tareas de remediación en tiempo real gracias a Remediation Workflows.
Esta funcionalidad también proporciona soluciones desde la plataforma para reducir el riesgo de las vulnerabilidades encontradas y hace uso de los paneles de remediación para ofrecer visibilidad sobre la eficacia del programa de remediación, pudiendo observar desde el progreso de estos, los datos de proyectos pasados y hasta el trabajo restante.

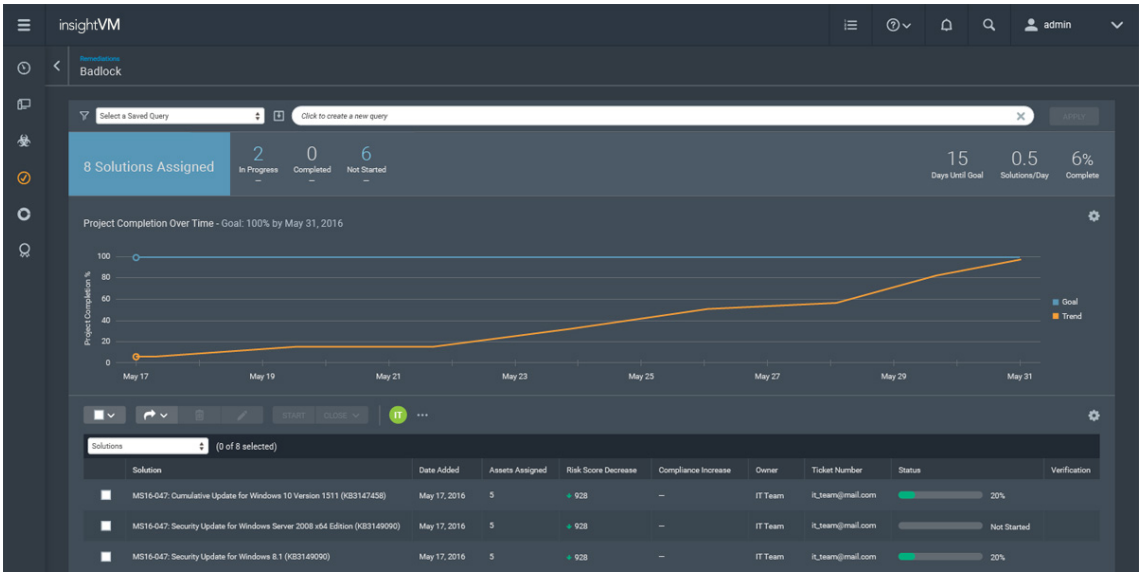

Figura 5.4: InsightVM panel de Remediation

insightVM se puede integrar con soluciones de gestión de tickets por parte de terceros como pueden ser Atlassian Jira y ServiceNow, por si se considerase insuficiente la gestión desde la plataforma. También se puede integrar con el producto de la misma casa Rapid7 Komand, el cual permite la automatización de tareas relacionadas con la seguridad de la empresa.

Por último, para hacer una remediación eficiente de las vulnerabilidades se realiza un análisis de riesgo basado en el atacante, priorizando como este lo haría.
Para cada vulnerabilidad se obtiene una puntuación granular Real Risk valorada entre 1 y 1,000 que tiene en cuenta las puntuaciones CVSS, la exposición del *malware*, la exposición del *exploit* y la facilidad de uso de este, y el tiempo que lleva en activo la vulnerabilidad.
Gracias a ello se obtiene una priorización de vulnerabilidades más precisa que las obtenidas en la competencia. Estos análisis se alimentan de bases de datos públicas de amenazas y de otras en propiedad basadas en la inteligencia de los equipos de investigación de Rapid7.
Adicionalmente insightVM cuenta con un sistema de etiquetado para que el usuario pueda realizar una asignación en función de la criticidad del activo, impactando el valor de esta etiqueta en la priorización de vulnerabilidades.
Combinando estas dos características insightVM se encargará de valorar la prioridad de cada amenaza en el proyecto de remediación general de toda la red, para que sea securizada de la forma más eficiente posible.

Figura 5.5: InsightVM panel de priorización general

Características destacables:

- Evaluación de vulnerabilidades de contenedores, nube y máquina virtual
- Plataforma altamente integrada, con capacidades de gestionar casi todos los aspectos de la seguridad de una empresa
- Cuenta con extensas bases de datos de vulnerabilidades y un eficiente sistema de puntuación propio

- Interfaz muy usable e intuitiva

Áreas de mejora:

- Despliegue inicial separado en muchos paquetes de precios en función del tamaño de la red
- No se centra en la calidad de los informes generados

5.1.2. BeyondTrust

BeyondTrust[27] es una empresa de ciberseguridad global fundada en 1985 y con sede en Phoenix, Arizona.
Sus soluciones de seguridad son muy conocidas y usadas en el sector, incluyendo entre sus clientes a más de la mitad de las empresas del Fortune 100 [4].

El producto estrella de la empresa es el PowerBroker PAM Platform[5], una solución orientada al control de privilegios y actividad de usuarios.
Entre el abanico de servicios ofrecidos por BeyondTrust también se encuentran diversos escáneres de vulnerabilidades especializados en tecnologías como Retina Web Security Scanning, especializado en amenazas para sitios y aplicaciones web, Beyond SaaS Cloud-Based Scanning, que es una solución basada en la nube para el escaneo de red interno, externo y de aplicaciones web, o Retina Network Security Scanner, que es el escáner para red tanto interna como de perímetro usado por la solución que se va a observar.

El producto a analizar se vende bajo el nombre de Retina CS. Esta solución proporciona un servicio de evaluación, gestión y remediación de vulnerabilidades a grande escala y multiplataforma.
Mediante el uso de módulos extra también puede llegar a realizar la gestión de vulnerabilidades para dispositivos móviles (Retina CS for Mobile), la gestión de parches (Retina Patch Management Module), la gestión de configuraciones (Retina Configuration Compliance Module) y la generación de informes de conformidad (Retina Configuration Compliance Module).

La evaluación comienza realizando un descubrimiento de la infraestructura tanto de red, como web, móvil, de nube, de dispositivos virtuales y del internet de las cosas o IoT. Todos estos activos se perfilan con su configuración y riesgo potencial, para luego escanear sus vulnerabilidades, *malware* descubierto o posibles ataques.

En este momento se vuelve a evaluar cada activo con sus respectivas vulnerabilidades encontradas y se establece el potencial de las amenazas gracias a un análisis combinado con la inteligencia de BeyondTrust.
Para la remediación se comienza aplicando los parches pertinentes si se dispone

[4] Fortune 100: Ránking anual de las 100 mejores empresas del mundo elaborado por la revista Fortune
[5] Privileged Access Management: Gestión del Acceso Privilegiado

del módulo de gestión de parches.
En cualquier caso se finaliza generando los informes de vulnerabilidades, conformidad, o los que se le indique a la plataforma.

Esta solución está altamente orientada a obtener resultados, por ello lo primero que hay que realizar antes de cada proceso de evaluación es especificar los objetivos a conseguir, ya sea un informe de conformidad del sistema o un informe sobre la seguridad de un activo en concreto.
Por ello se cuenta con más de 260 informes destinados a lectores técnicos y no técnicos, y se pueden programar evaluaciones y configurar alertas por mail derivadas de estos procesos.

También se hace mucho hincapié en el contexto del activo en el sistema. Se tiene una consciencia del daño colateral que podría causar una vulneración de la confidencialidad, la integridad o la disponibilidad de un solo dispositivo en el total de la red.

Una parte esencial de cualquier solución de evaluación y gestión de vulnerabilidades es el análisis y la inteligencia de amenazas, y en Retina CS este aspecto lo aporta BeyondInsight.
BeyondInsight señala amenazas avanzadas persistentes (APTs) y otros posibles ataques mediante el conteo de vulnerabilidades, el nivel de las vulnerabilidades, el puntaje de riesgo, las aplicaciones, los servicios, el software y los puertos entre otros parámetros. También tiene capacidades de análisis de *malware* y una base de datos de *malware* propia continuamente actualizada por parte del equipo de BeyondTrust.
Es gracias a estos datos de los activos que una vez agregados y centralizados BeyondInsight puede correlar en las vulnerabilidades más críticas y priorizar su mitigación en los informes generados.

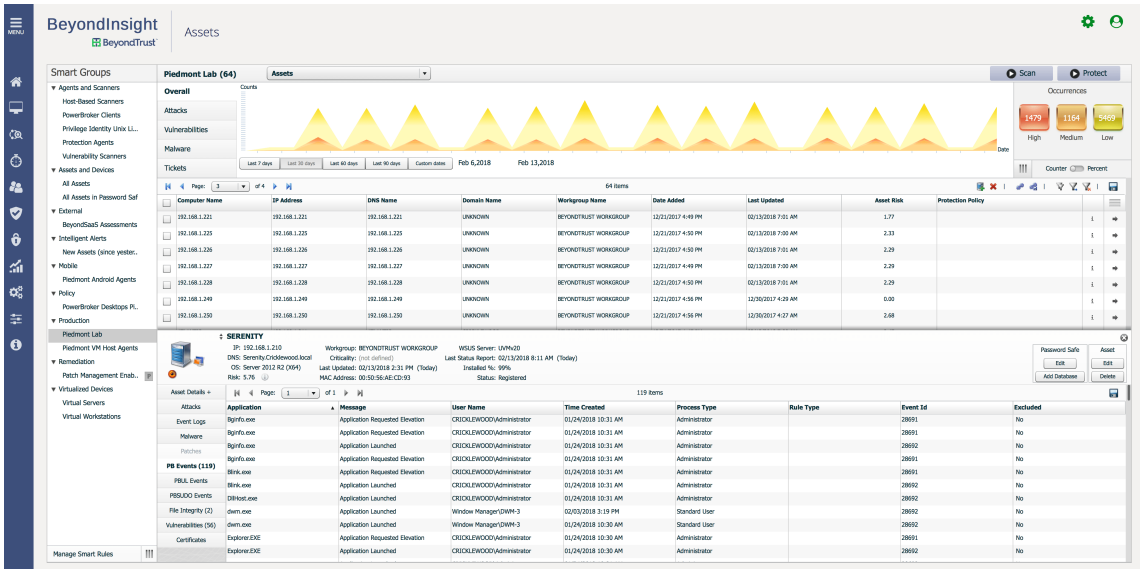

Figura 5.6: BeyondInsight mostrando el informe de un activo

Las soluciones de la plataforma de BeyondTrust no se limitan a la inteligencia de amenazas propia, sino que para mejorar los resultados ofrece integraciones con los conectores de las empresas líderes en cada sector de la ciberseguridad, como podría ser PaloAlto con los *firewalls* de siguiente generación, Qualys y Rapid7 para escáneres de vulnerabilidades y un largo etcétera.
Podemos observar todas estas integraciones con terceros en la figura 5.7.

Figura 5.7: Integraciones de Retina CS

Es por todas estas cualidades que no sorprende que BeyondTrust sea considerado un líder de mercado, ofreciendo seguridad a instituciones de la talla de la NASA, grandes empresas de comunicación como Verizon o grandes empresas internacionales muy dependientes de su ciberseguridad como Blizzard Entertainment, Intel, NBC, Oracle, Paypal y Ubisoft.
Tener clientes de esta talla no hace más que confirmar la profesionalidad y la calidad de las soluciones ofrecidas por BeyondTrust.

Características destacables:

- Control centralizado y muy escalable, puede cubrir una red de clase A con un solo motor de escaneo Retina
- Gran cobertura en informes de conformidad con estándares
- Presenta el mayor ecosistema de soluciones de seguridad integradas del mercado
- El despliegue se puede realizar tanto por software, dispositivo y/o máquina virtual

Áreas de mejora:

- Para realizar los escaneos con autenticación variante también hay que adquirir PowerBroker
- Interfaz muy poco visual e intuitiva

5.1.3. NopSec

La empresa NopSec[28] es sin ningún lugar a dudas la menos conocida y la más pequeña de las cuatro empresas consideradas líderes del sector.
Esta empresa con sede en Nueva York fue fundada en 2009 con la misión de ayudar a la gente a tomar mejores decisiones para reducir los riesgos de seguridad a través de su software como servicio o Software-as-a-Service.
Para ello en 2012 lanzan su hasta día de hoy único producto de gestión de riesgos de vulnerabilidad, Unified VRM.

Unified VRM es una solución que concentra en una sola plataforma todas las etapas necesarias para una correcta evaluación y gestión de vulnerabilidades, además de una plataforma de tickets para organizar la remediación de estas.

Comenzando por el descubrimiento de activos y vulnerabilidades, la versión estándar cuenta con herramientas propias de NopSec para realizar estas etapas a nivel interno y unos módulos extra, entre los que se incluyen Unified VRM Web Application para escaneo de aplicaciones Web expuestas a internet, Unified VRM Network para escaneo de perímetro y activos expuestos a internet, y Unified VRM Security Configuration para evaluar la fortaleza de las configuraciones de seguridad en el *host*, pudiendo también evaluar la conformidad con diversos estándares y regulaciones del nivel de NIST, HIPAA y PCI entre otras.

Una vez completado el escaneo, Unified VRM crea una lista de amenazas prioritaria y genera una serie de gráficos e informes para hacer un seguimiento del progreso mientras los parches son aplicados y se realizan los cambios pertinentes. Uno de los puntos fuertes de esta solución son estos gráficos destinados al personal no técnico y el fácil análisis y filtrado de los riesgos encontrados.

A la hora de recibir los datos del escáner de vulnerabilidades esta herramienta ofrece una integración con soluciones de otras empresas como podrían ser Nessus, HP WebInspect, w3af, IBM AppScan o skipfish entre otras, destacando el potente escáner de Rapid7.
Unified VRM realiza el análisis de estas vulnerabilidades, las cuales han sido evaluadas previamente por el equipo de Ingenieros de Seguridad de NopSec conforme a la funcionalidad, criticidad y sensitividad de los datos para cada activo posible, para posteriormente realizar una clasificación de estas según la importancia del activo, dividiendo en última instancia entre riesgos aceptables y riesgos que tienen que ser mitigados.
Este análisis es de gran calidad, como prueba el hecho de que proporcione este mismo servicio para las soluciones de Qualys y que sean partners de Alien Vault OTX.

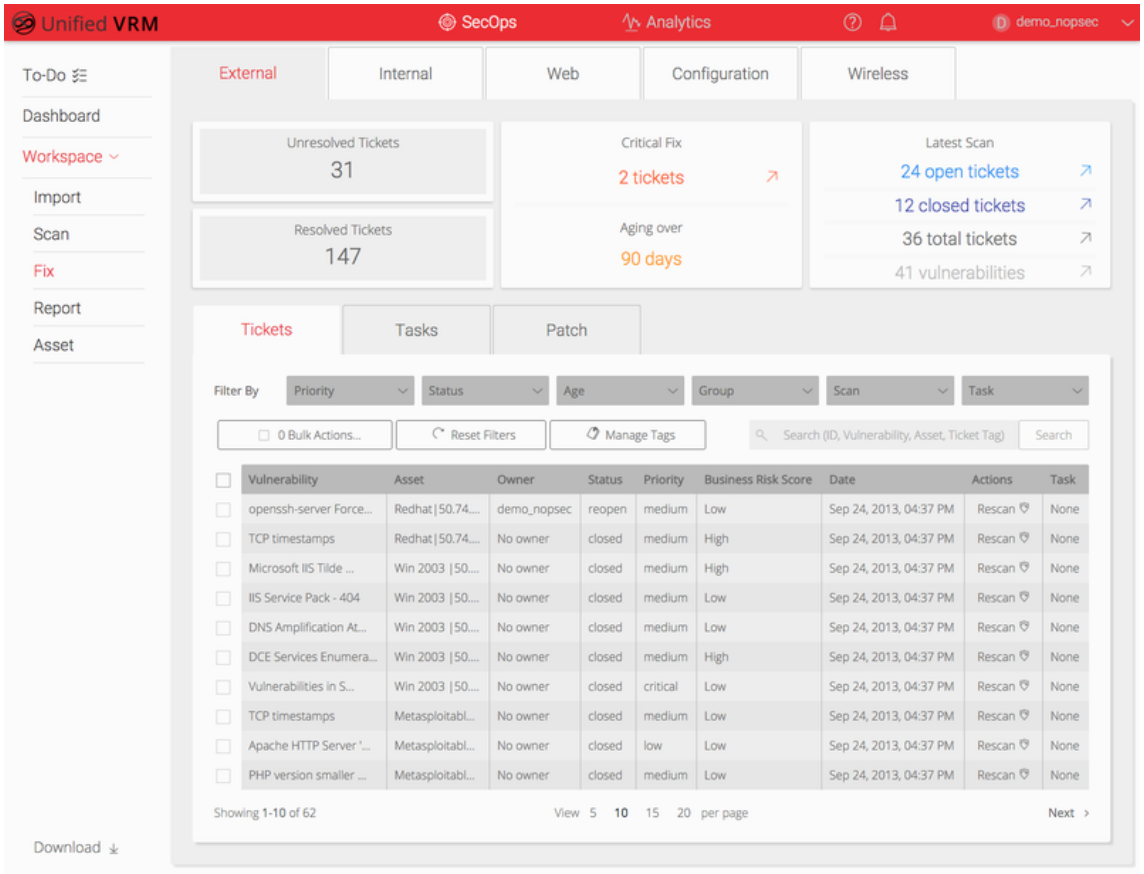

Figura 5.8: UnifiedVRM pestaña Fix para Escáner Interno

Una vez realizado el trabajo análisis desde el apartado Analytics se tiene acceso a un buscador para filtrar las vulnerabilidades encontradas en los activos escaneados. En él se puede hacer búsquedas teniendo en cuenta las tendencias a nivel mundial en cuanto a vulnerabilidades o las características deseadas por el usuario tan variadas como el factor de riesgo, el número de ocurrencias, el nombre de la vulnerabilidad, etc.
Estas búsquedas, de las cuales también se pueden sacar gráficos, se pueden guardar directamente en forma de informe, siendo esta una característica de la que carece la competencia.

Características destacables:

- Interfaz visual agradable a la vista y con una gran usabilidad
- Generador de informes personalizados sencillo a la par que potente
- Se explica detalladamente cada vulnerabilidad encontrada y se proporciona indicaciones para la mitigación de esta
- Sistema de *ticketing* integrado para la remediación de vulnerabilidades

Áreas de mejora:

- Obtener la solución completa requiere de comprar todos los módulos disponibles

- Precio relativamente alto incluso para la versión más básica

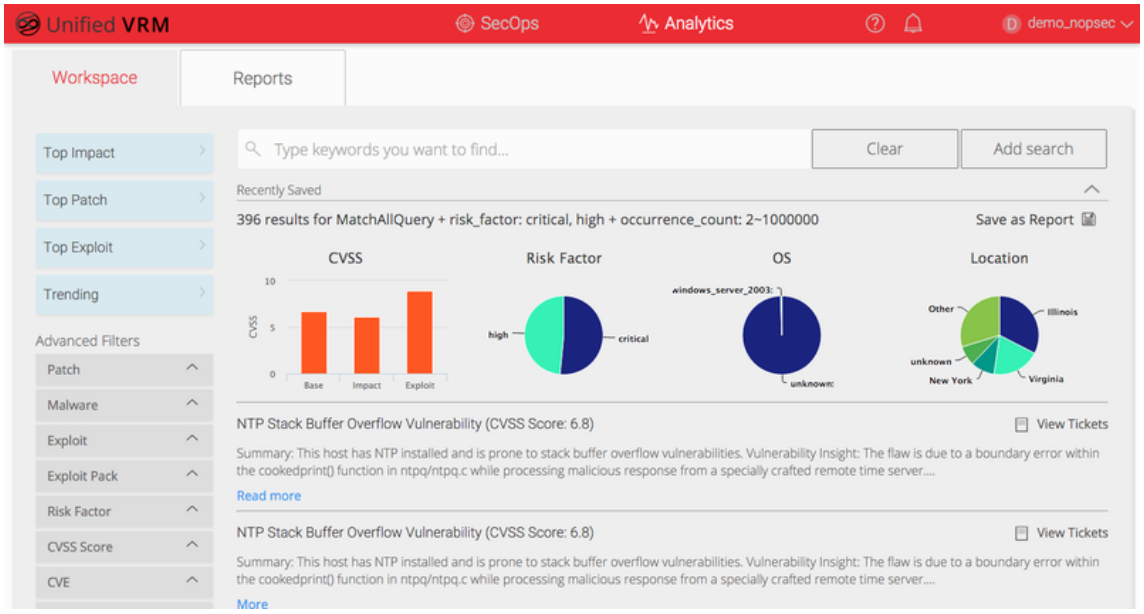

Figura 5.9: UnifiedVRM apartado Analytics

5.1.4. Qualys

Qualys, Inc.[29] es una empresa dedicada a la ciberseguridad con productos para seguridad en la nube, servicios de conformidad, evaluación y gestión de vulnerabilidades y diversos servicios relacionados con la seguridad.
Fundada en 1999 y con sede en Foster City, California, fue la primera empresa en ofrecer la gestión de vulnerabilidades como aplicación web con un modelo de SaaS o software como servicio.
Esto unido a la calidad de sus soluciones le ha llevado a liderar continuadamente prácticamente todos los estudios de mercado realizados sobre soluciones de gestión de vulnerabilidades.

Desde el lanzamiento de QualysGuard en Diciembre del 2000 esta solución no ha parado de mejorar y mutar conforme a las exigencias del mercado, convirtiéndose en la gran plataforma que es hoy, aglutinando todas sus soluciones ofrecidas al público bajo el nombre de Qualys Cloud Platform.

Qualys Cloud Platform recibe toda la información que necesita de cuatro posibles fuentes propias:

- Cloud Agents, agente para cualquier tipo de dispositivo que proporciona visibilidad y recolección continua de datos
- Virtual Scanners, para escaneo interno de software en dispositivo o en nube
- Scanner Appliances, dispositivos hardware de escaneo para redes internas
- Internet Scanners, para escaneo externo en dispositivo o en nube

Esta plataforma única permite gestionar todos los productos ofrecidos por Qualys, que al tener soluciones para todos los campos permite al comprador evitar tener que acudir a diferentes vendedores para confeccionar toda la ciberseguridad de la empresa a defender.
Los datos se recolectan y analizan de manera automática y escalable, que sumado a la tecnología de Cloud Agent permite conocer en tiempo real el estado de todos los activos y posibles nuevas vulnerabilidades, pudiendo configurar notificaciones automáticas para cuando se detecten.
Qualys también ofrece una integración nativa con las plataformas de nube de terceros más importantes, como son Google Cloud Platform, Microsoft Azure y Amazon Web Services, con el fin de proporcionar una visibilidad completa.

En este caso de estudio la aplicación que más interesa analizar es Qualys Vulnerability Management, la cual, según la propia empresa, se trata de la solución de gestión de vulnerabilidades más avanzada, escalable y extensible de la industria.

Qualys VM, además de los escaneos realizados por los dispositivos de Qualys, hace uso de Cloud Agent para realizar escaneos autenticados en cada dispositivo, minimizando a su vez el impacto en la red de la empresa.
Los escaneos e identificación de vulnerabilidades son continuos y realizados con una precisión de Six Sigma[6], reduciendo al mínimo los falsos positivos.
Siendo como las empresas van adoptando el procesamiento en la nube y adquiriendo una mayor movilidad Qualys ofrece soporte para este tipo de ambientes informáticos híbridos.

Un aspecto diferenciador de Qualys VM es la separación del escaneo respecto del informe. En otras soluciones se pueden encontrar escaneos orientados al informe a realizar, mientras que Qualys primero realiza un escaneo profundo y detallado para luego mostrar la información pertinente según el informe deseado. A la hora de realizar el escaneo se puede hacer por direcciones IP, grupos de activos o etiquetas de activos, que han tenido que ser configuradas previamente a mano. A la hora de realizar el escaneo basta con indicar si se quiere que sea externo, interno o ambos.

Para la identificación y priorización de las vulnerabilidades Qualys utiliza KnowledgeBase, una potente base de datos de vulnerabilidades propia que permite contextualizar cada riesgo para el sistema. En esta fase otra ventaja de Qualys VM sobre la competencia es el seguimiento de las vulnerabilidades a lo largo del tiempo, desde que aparecen hasta que son remediadas, o si se da el caso de que vuelven a aparecer. Gracias al uso de Cloud Agent esta solución es capaz de realizar observaciones de los activos tan concretas como ver cuáles usan certificados de la red a punto de caducar o si necesita actualizarse tras el Martes de Parches mensual[7].

[6]Six Sigma: Seis Sigma es una metodología de mejora de procesos, centrada en la reducción de la variabilidad de los mismos, consiguiendo reducir o eliminar los defectos o fallos en la entrega de un producto o servicio al cliente

[7]Martes de Parches: Referente a la tendencia de Microsoft a lanzar los parches de seguridad el segundo martes de cada mes

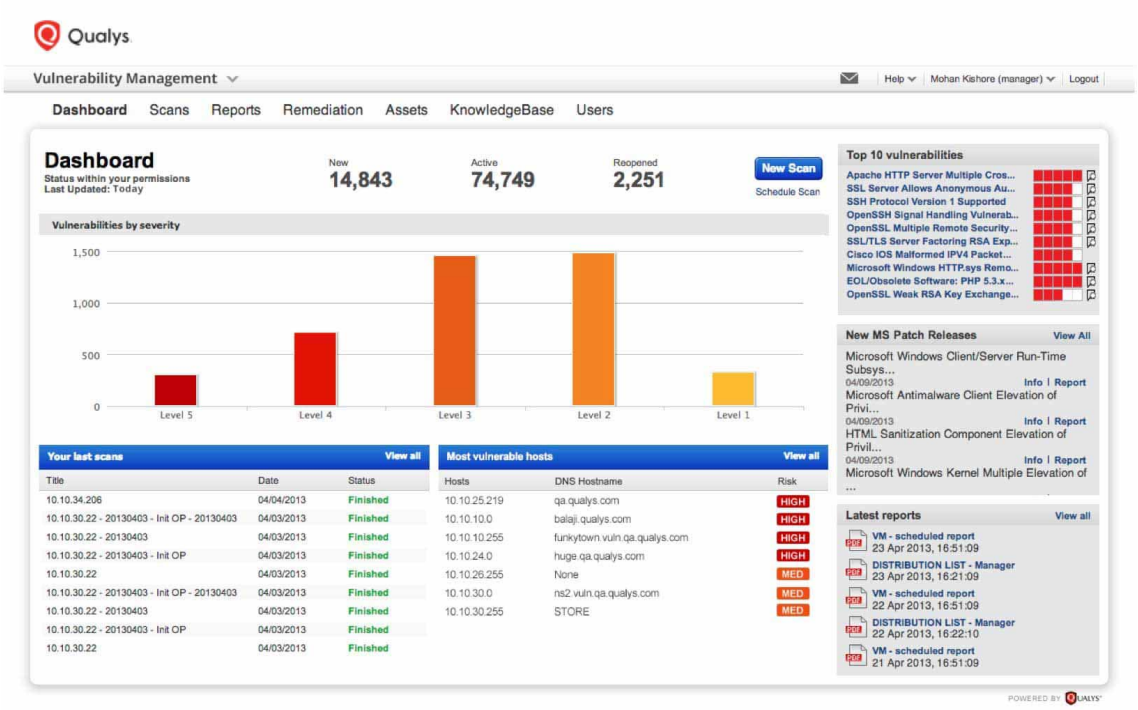

Figura 5.10: Qualys VM pestaña de Dashboard principal

En lo que respecta al informe Qualys VM cuenta con una amplia librería de informes ya incluidos que son susceptibles de personalización por parte del usuario, todo ello sin tener que volver a realizar el escaneo. Estos informes se pueden generar bajo demanda o ser planificados y automatizados, pudiendo generarse para visualización en web, PDF o CSV.
Cuando se encuentran vulnerabilidades, se generan y asignan automáticamente tickets de remediación y existe la posibilidad de integrar estos resultados con sistemas de tickets de terceros.

Por lo visto hasta ahora se podría considerar Qualys VM una buena herramienta de evaluación y gestión de vulnerabilidades aunque no completa. Estas carencias se suplen con el uso de dos de las Qualys Cloud Apps integradas: Asset Inventory y Security Configuration Assessment.

Asset Inventory se encarga de realizar el descubrimiento de activos y mantener un inventario continuamente actualizado de estos independientemente de su localización. Las características inventariadas para cada activo son enriquecidas gracias a los Cloud Agents y se pueden complementar con etiquetas establecidas manualmente por el administrador, que podrán usarse como criterio para la realización de escaneos.
Esta App dispone de un potente buscador para realizar consultas complejas que pueden ayudar a identificar dispositivos muy concretos. Entre la información que se proporciona de los componentes de cada activo se encuentran las especificaciones hardware, el software instalado, aplicaciones instaladas, *drivers*, *plugins*, conexiones de red, parches instalados, usuarios aprobados, servicios, claves de registro, ubicación geográfica y un largo etcétera.

Si lo que se quiere es una visión más generalista del sistema también se dispone de una serie de gráficos que muestran el estado de los activos y las vulnerabilidades con porcentajes y gráficos sectoriales representativos.

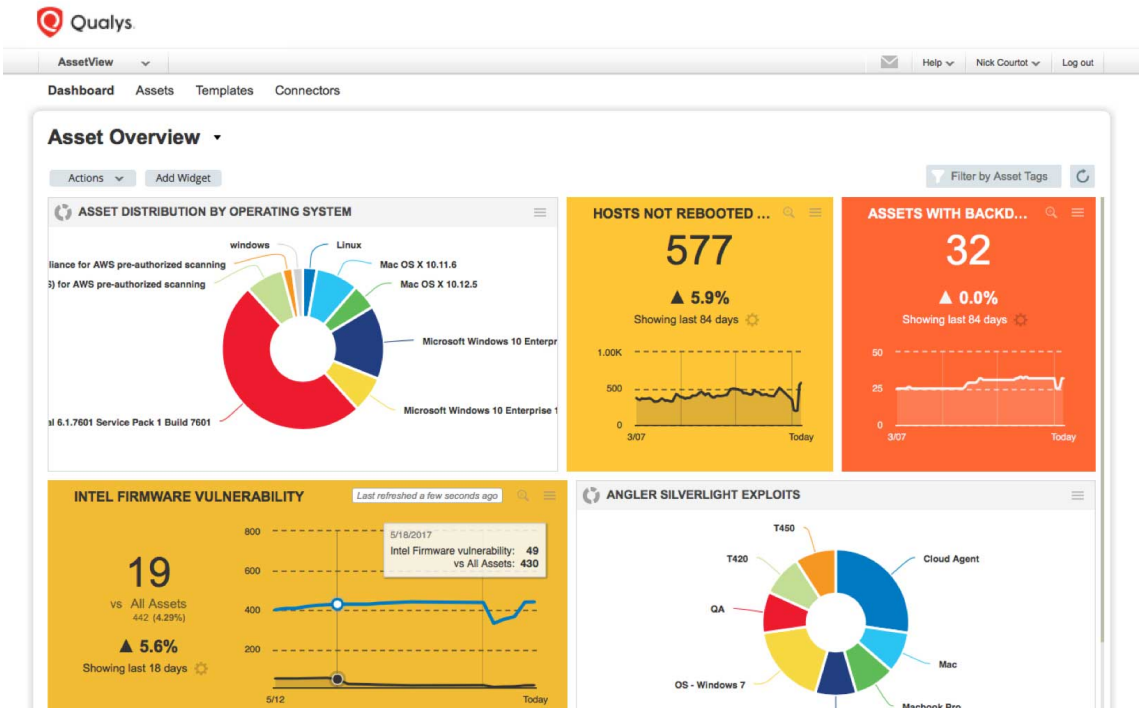

Figura 5.11: Qualys AI pestaña de resumen para un activo

Security Configuration Assessment se encarga de automatizar la evaluación de configuraciones.
Qualys SCA proporciona evaluación, monitorización, informe y remediación para los aspectos de la configuración relacionados con la seguridad. Este proceso asegura la consistencia, integridad y fortaleza de las configuraciones de los activos del sistema.
Todo esto bajo la plataforma Qualys Cloud Platform, pudiendo también generar informes y gráficas similares a las de Qualys VM.

Características destacables:

- Todos los servicios unificados en una sola plataforma en la nube
- Altamente escalable, debido en parte a la ausencia de hardware
- Protección de los datos generados gracias a los servidores cifrados de Qualys, muy bien protegidos tanto a nivel lógico como físico
- Integración con los proveedores de nube pública más potentes

Áreas de mejora:

- Oferta de servicios limitada por el número de IPs a escanear, excluyendo la gestión de tickets y la integración con nubes públicas para pequeñas empresas

- Necesidad de tres aplicaciones para obtener una evaluación y gestión de las vulnerabilidades completa

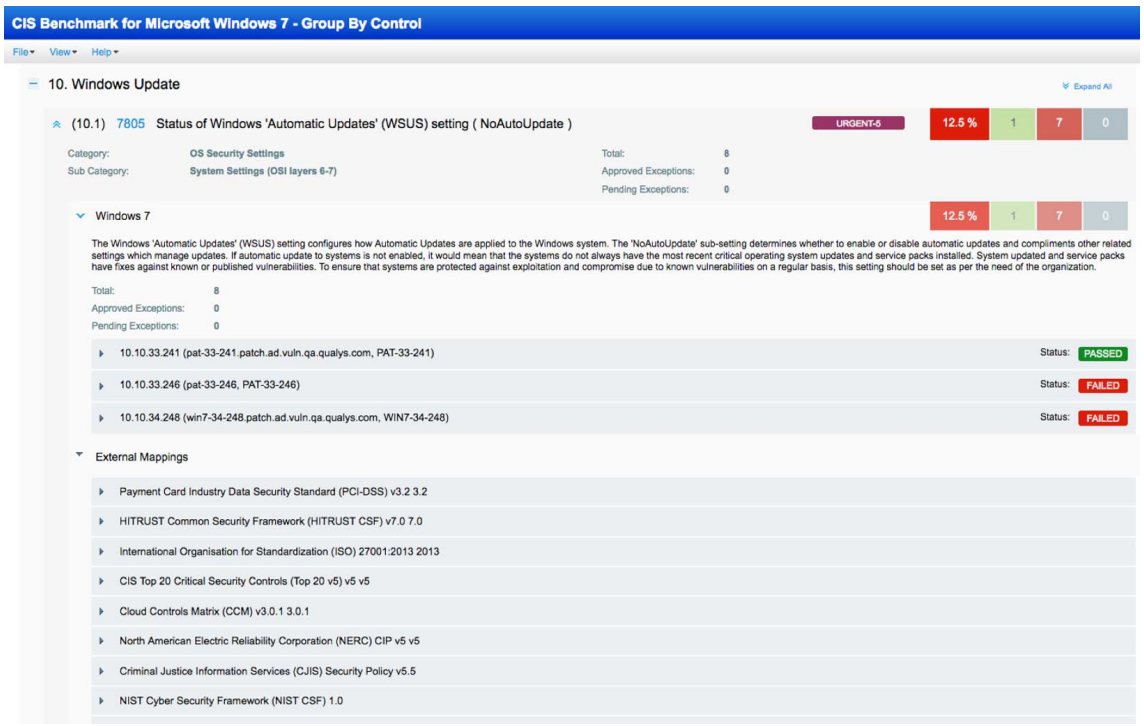

Figura 5.12: Qualys SCA resultado de un benchmark para Windows 7

5.2 Actores Fuertes

5.2.1. Tenable

Tenable Network Security, Inc.[30] se fundó en 2002 con el objetivo de ofrecer una solución que permitiera una visión comprensible e integrada de la salud de una red de empresa.
Con ese objetivo lanzó su primer y exitoso producto, el escáner de vulnerabilidades Nessus, que actualmente se vende para empresas bajo el producto Nessus Professional.
Con el paso del tiempo ha ido aumentando su catálogo ofreciendo detección de vulnerabilidades para sistemas industriales con Industrial Security, la priorización de vulnerabilidades con informes, gráficas y alertas con Security Center, y la plataforma para la gestión de vulnerabilidades Tenable.io . Es esta última en la que se va a centrar el análisis.

La plataforma Tenable.io consiste de tres diferentes aplicaciones (Vulnerability Management, Web Application Scanning y Container Security) y una cuarta que se espera para 2018 (Lumin), como se puede observar en la figura 5.13 .

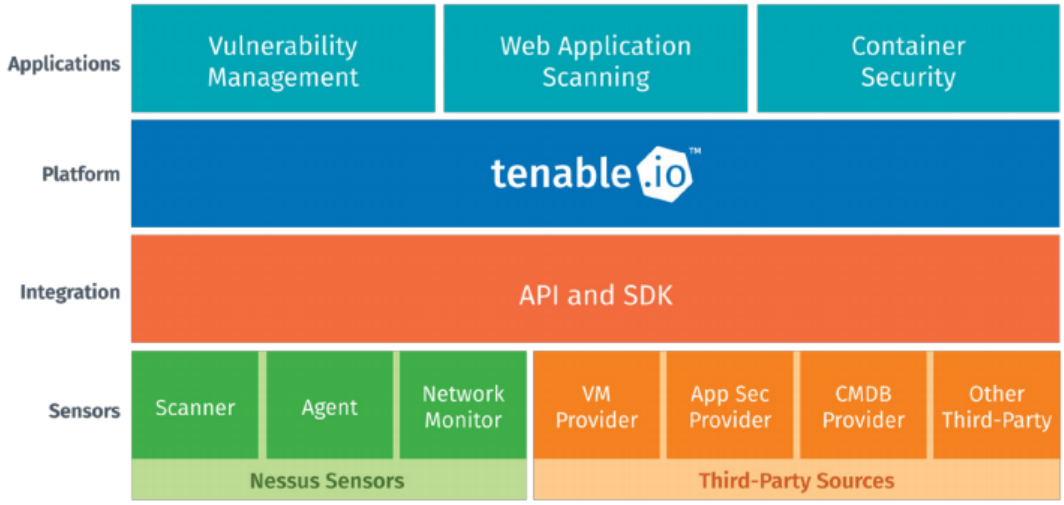

Figura 5.13: Plataforma Tenable.io

La aplicación Web Application Scanning permite identificar con certeza problemas de seguridad en aplicaciones web. Esta solución permite conocer las aplicaciones web y obtener información detallada de las partes de la aplicación que el escáner no ve. Para evitar los problemas de latencia o la caída de la web el administrador puede establecer que partes se deberían escanear normalmente y cuales evitar.
Es capaz de auditar desde aplicaciones web HTML tradicionales hasta aplicaciones modernas construidas sobre HTML5 y con *frameworks* AJAX. Estos escaneos pueden ser automatizados e integrados con Vulnerability Management, ampliando la visión de vulnerabilidades de la plataforma sobre el conjunto del sistema.

Como ya se ha expuesto anteriormente, en 2016 Tenable adquirió FlawCheck, y desde entonces está disponible la aplicación Container Security en la plataforma. Container Security permite supervisar el desarrollo de contenedores en busca de vulnerabilidades.
Es tan sencillo como integrar el producto con el registro privado de contenedores de la empresa (o directamente crearlo en la aplicación) para que se realicen los primeros escaneos y se automaticen los nuevos escaneos conforme se vaya actualizando la base de datos de vulnerabilidades de Container Security. Estos registros también se pueden sincronizar con registros de terceros como Docker Registry, Docker Trusted Registry, JFrog Artifactory y Amazon EC2 Container Registry.
Estos análisis detectan posible *malware* en el código fuente y también vulnerabilidades, que son luego sincronizadas con toda la plataforma Tenable.io mejorando la visión general de la red. Todos estos datos obtenidos por la aplicación se pueden exportar para uso de terceros con la API integrada.
Esta funcionalidad es muy poco común en el mercado de evaluación y gestión de vulnerabilidades, lo cual representa una gran baza para esta plataforma si se tiene en cuenta el incremento del uso de contenedores con la tecnología Docker.
En la imagen 5.14 se puede observar el resultado que proporciona Container Security tras uno de estos escaneos.

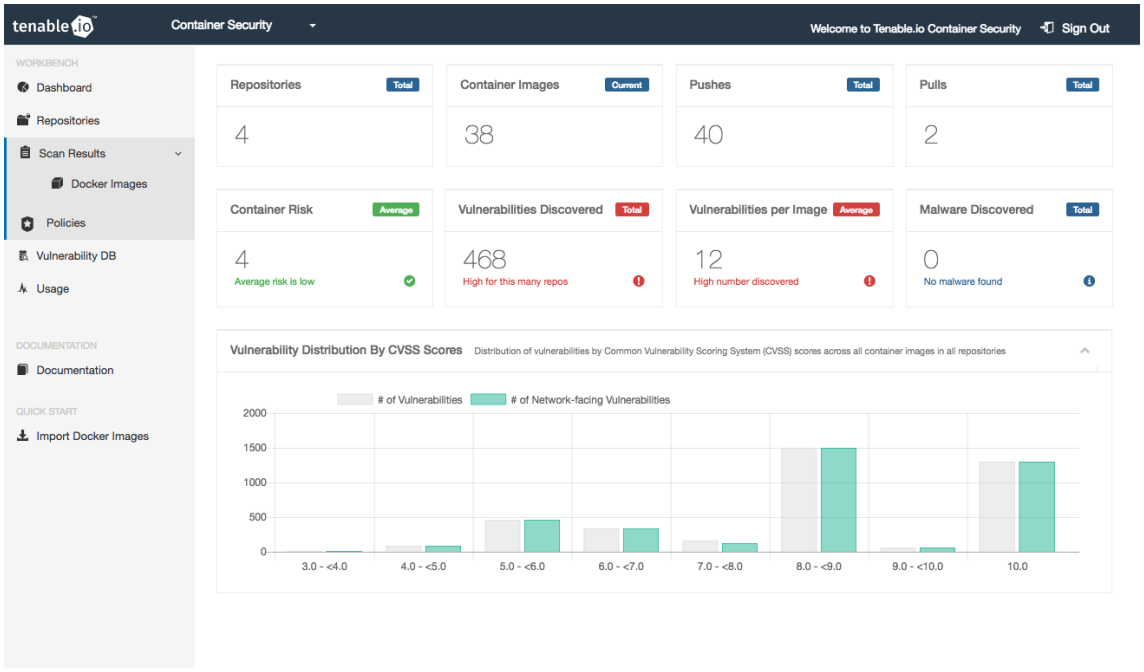

Figura 5.14: Resultado de escaneo con Container Security

La aplicación de principal interés para la evaluación y gestión de vulnerabilidades es Vulnerability Management. Esta se encarga de identificar y escanear todos los activos de la red para que luego el cliente pueda priorizar las vulnerabilidades de una manera eficiente.
Vulnerability Management hace uso del famoso Nessus como escáner de vulnerabilidades, pero se pretende alejar de escaneos planificados y aboga por hacer plataformas inclusivas. Por ello existe la posibilidad de integrar datos de terceros.
Estos escaneos de vulnerabilidades se realizan a través de los Nessus Sensors, sensores que pueden ser una mezcla de escáneres activos, agentes y sensores de escucha pasiva. Todos ellos con capacidades de escaneo y que son seleccionados en función del sistema a analizar para minimizar los puntos ciegos de la aplicación.
Las vulnerabilidades encontradas por estos sensores son seguidas basándose en su activo y estos datos pueden ser compartidos fácilmente con soluciones de terceros a través de la API y SDK oficial proporcionada por Tenable.

Debido al aumento en el número de activos transitorios en las empresas, como podrían ser portátiles, dispositivos móviles, instancias de la nube o contenedores, Tenable ha dibujado una nueva identidad para los activos, en vez de el simple uso de la dirección IP que viene siendo utilizada en el sector.
Como consecuencia de este cambio en la enumeración de activos, también se ha dado este cambio en las licencias, pudiendo darse que una licencia sirva para más de una IP o que las licencias se vayan asignando y revocando a estos activos transitorios, suponiendo un gran ahorro para el cliente en términos económicos.

Con la incursión en las redes de este tipo de activos dinámicos también se fuerza

un cambio en el descubrimiento de estos. Ya no sirve realizar escaneos periódicos para observar grandes cambios en el sistema sino que es necesario tener escaneada la red de una manera continuada y sin pausa. Es esto precisamente lo que logra Tenable.io VM con la escucha pasiva de tráfico, siendo capaz de tener un conocimiento de la estructura de la red en todo momento y de los cambios que suceden en los activos mediante un avanzado algoritmo de identificación.

Todos los activos son seguidos con el sistema de Pinpoint Asset Tracking, mediante el cual se sigue cada activo y sus respectivas vulnerabilidades con una gran precisión, maximizando la visibilidad y el conocimiento sobre la red para poder priorizar efectivamente las vulnerabilidades del sistema.
Este algoritmo consigue identificar hasta los activos dinámicos gracias a que establece la identidad del activo a través de una extensa lista de atributos que permite realizar un seguimiento independientemente de donde se encuentren o de cuanto duren en la red. Entre otros atributos podemos encontrar el Tenable ID, el nombre de NetBIOS o la dirección MAC.

Se puede encontrar un ejemplo de este seguimiento en la figura 5.15 .

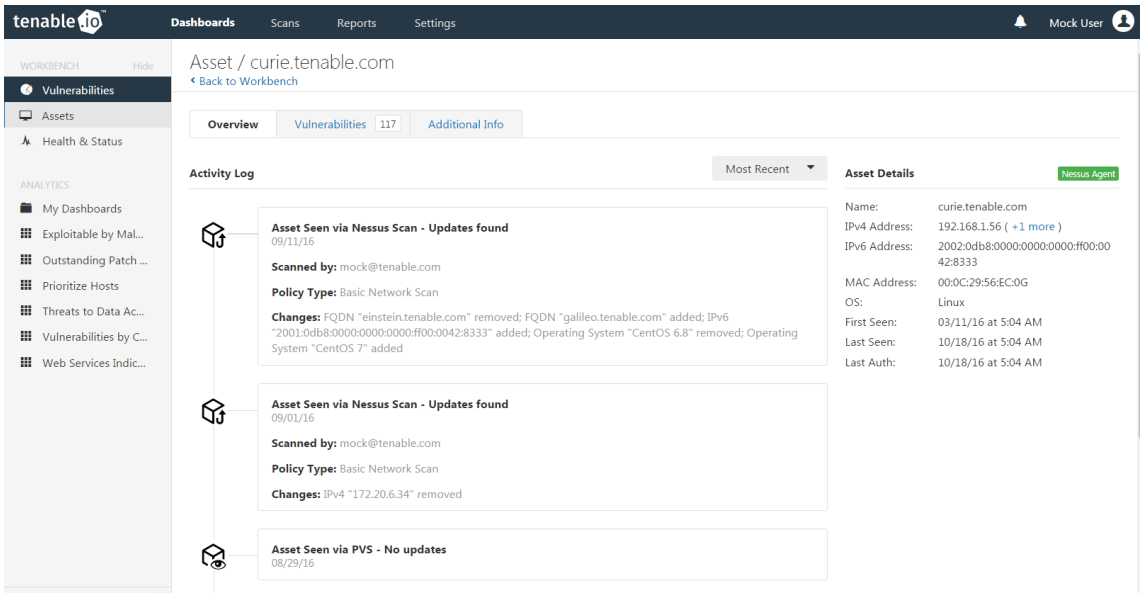

Figura 5.15: Seguimiento de un activo en Tenable.io

Tenable.io Vulnerability Management viene con otras soluciones ya pre-integradas, como gestión de parches, gestión de credenciales o gestión de dispositivos móviles, listas para usar de inmediato desde la misma plataforma en caso de ser adquiridas.
La interfaz que presenta la plataforma es intuitiva y está continuamente guiada por mensajes, además te ofrece un Service Level Agreement (SLA)[8], que garantiza para el gestor de vulnerabilidades un tiempo mínimo de servicio útil, ofreciendo compensaciones económicas en caso de no cumplir con la robustez acordada.

[8]Service Level Agreement: Acuerdo de Nivel de Servicio

Por último se encuentra la futura aplicación Lumin, de la cual se prevee el lanzamiento en 2018.
Lumin será una solución para la visualización, análisis y medida de vulnerabilidades que transforma datos recolectados de vulnerabilidades en valiosos conocimientos para la organización de la gestión del riesgo informático en la organización.
Esta aplicación supondrá desde la plataforma de Tenable.io la capacidad de realizar una priorización más correcta de las vulnerabilidades del sistema, una mejora significativa en las capacidades de visualización del estado de la red y una mayor calidad en los informes generados de todo el proceso.
Si Lumin da en un futuro todo lo que se promete Tenable será un serio candidato al grupo de líderes de mercado en evaluación y gestión de vulnerabilidades.

Características destacables:

- Soporte para la seguridad de contenedores
- Uso de Nessus como escáner de vulnerabilidades, herramienta líder en su sector
- Modelo de licenciado por activo en vez de por IP, pudiendo tener una licencia para un activo con diversas direcciones IP
- Garantía de un tiempo mínimo de servicio útil

Áreas de mejora:

- Priorización de vulnerabilidades y generación de informes avanzados no disponible actualmente (Lumin)
- Informes demasiado extensos y poco útiles

5.2.2. Skybox Security

Skybox Security, Inc.[31] es una empresa que se dedica a proveer soluciones de gestión de vulnerabilidades para empresas. Esta compañía fundada en 2002 creó su primer producto Skybox en 2004 y desde entonces ha ido aumentando su abanico de productos con soluciones para la visibilidad de la red, el control de *firewalls*, gestor de cambios, etc.
Pero para realizar una evaluación y gestión de vulnerabilidades el producto a analizar es Skybox Threat-Centered Vulnerability Control.

Este producto aplica la gestión de vulnerabilidades centrada en la amenaza (TCVM), priorizando las amenazas inminentes y ayudando a gestionar las amenazas potenciales a lo largo del tiempo.
Se encarga de buscar amenazas que están expuestas debido a la infraestructura de la red y sus configuraciones de seguridad teniendo en cuenta para ello las vulnerabilidades que ya son usadas por los cibercriminales, las que tienen un código de *exploit* conocido y hecho público, y las que existen en la red pese a no tener un exploit conocido. Teniendo en cuenta estos parámetros y la exposición se le

asignará una prioridad a la vulnerabilidad.
Si a este método de priorización le unes el conocimiento de la superficie de ataque, inteligencia en vulnerabilidades y amenazas, y análisis de vectores de ataque, TCVM cuenta con las herramientas y el contexto óptimo para detectar las vulnerabilidades que suponen un riesgo real y remediarlas de inmediato.

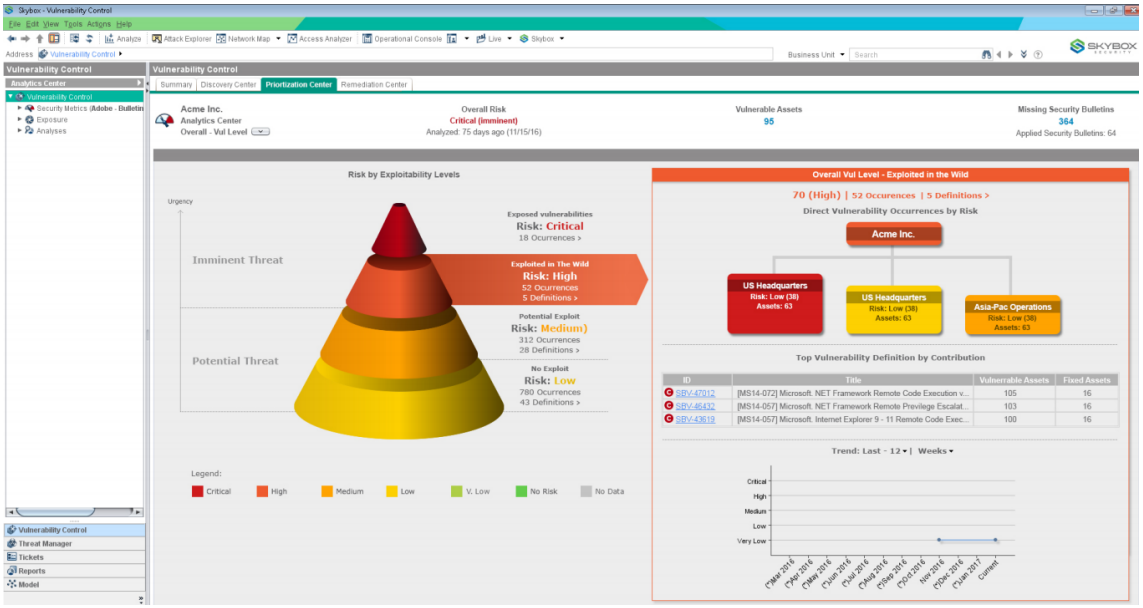

Figura 5.16: Skybox Vulnerability Control panel de priorización de riesgos

Este tipo de gestión utiliza una gran cantidad de datos de diferentes fuentes y analizando los datos desde perspectivas múltiples. Es por ello que este proceso debe de ser automatizado. Entre las diferentes tareas automatizadas se encuentran:

- Importación de datos desde escáneres de vulnerabilidades de terceros
- Importación de datos desde los sistemas de gestión de activos y parches, además de otra información del sistema analizado para completar la evaluación de vulnerabilidades pasiva sin escaneo, el cual se explicará más adelante.
- Importación de fuentes de inteligencia en amenazas.
- Conversión de datos de activos y configuración en un modelo de red. Este modelo se actualizará constantemente con las fuentes de inteligencia de Skybox.
- Simulación de ataques con origen en el atacante mediante diferentes técnicas contra activos vulnerables y simulación de ataques de pivotaje desde activos expuestos directamente, para averiguar exposiciones indirectas.
- Análisis de los datos para identificar qué vulnerabilidades están expuestas directamente a atacantes, son usadas por cibercriminales o tienen una muestra funcional del *exploit* disponible públicamente.

Todas estas tareas pueden ser secuenciadas y programadas para crear procesos que se realicen de manera regular. El proceso completo de Skybox VM divide su trabajo en cinco fases diferenciadas.

En primer lugar se realiza el descubrimiento de activos y escaneo de vulnerabilidades, con la particularidad de que este escaneo se realiza de forma pasiva y sin hacer uso de una herramienta del tipo escáner de vulnerabilidades activo.
El descubrimiento de activos ya viene dado por Skybox Horizon, pero para descubrir las vulnerabilidades sin un escáner es necesario recolectar y evaluar la mayor información posible de los activos, la topología de la red y los controles de seguridad, incluyendo los dispositivos físicos, de nube y tecnologías de red. Toda esta información se une en forma de un modelo de la red para ser usada en la siguiente fase.

En segundo lugar se procede a priorizar las amenazas, correlando los datos de los activos con inteligencia de amenazas e información de explotabilidad para hallar las vulnerabilidades. Usando el modelo de la red creado en el paso anterior se analizan los diferentes ataques potenciales para priorizar la remediación de estos en función del nivel de amenaza que supongan para los activos críticos del sistema.

A continuación, para la remediación se procede a aplicar los parches o si es necesario aplicar medidas para bloquear todos los ataques posibles. Entre las posibles medidas de remediación se pueden encontrar firmas IPS, reglas de acceso o segmentación de red entre otras. Primero se tratan las amenazas consideradas inminentes mientras que las consideradas como potenciales se subsanan con más tiempo.

Finalmente solo queda la supervisión, siguiendo todo el proceso y analizando los resultados obtenidos para encontrar áreas que requieren más atención o recursos. También hay que monitorizar las vulnerabilidades pendientes de remediar por si se producen cambios en cuanto a su exposición o uso por parte de cibercriminales, cambiando por tanto su prioridad de remediación.

En resumen, se trata de una plataforma desde la que se puede observar por completo la superficie de ataque, incluyendo vulnerabilidades y vectores de ataque potenciales de un modo visual e interactivo.
Se pueden automatizar los procesos de gestión de vulnerabilidades, desde la evaluación a la remediación y supervisión, ofreciendo alternativas eficientes a algunos parches y por tanto mejorando la consecución de los acuerdos de nivel de servicio (SLAs) en la red.
Esta reducción de riesgos se puede medir y seguir de una forma fácil para identificar dónde pueden faltar más recursos y demostrar el progreso mediante los paneles que se muestran.

Para mejorar la inteligencia de amenazas de la plataforma se puede adquirir el producto Skybox Threat Manager, el cual se encarga de proporcionar un conocimiento más extenso de los riesgos en el contexto de la red a analizar.
Skybox TM recoge sus datos de docenas de fuentes de inteligencia de amenazas,

entre las que se incluye la Base de Datos de Vulnerabilidades Nacional (NVD), y de la fuente de inteligencia Skybox, generada y validada por el equipo de investigación de la empresa Skybox Research Lab, una fuente de información de amenazas actualizada diariamente. También cabe la posibilidad de integrar inteligencia de terceros entre los que se encuentran Symantec DeepSight o VeriSign iDefense.
Tras la enumeración de vulnerabilidades y con una gran cantidad de datos sobre el estado actual de la ciberseguridad se encarga de revisar la prioridad de las amenazas basándose en la relevancia de estas para la propia red y la relevancia que tienen actualmente entre los cibercriminales.

Gracias a una mejor detección y priorización se reduce el tiempo y recursos necesarios para la protección contra ciberataques, alineando el análisis de vulnerabilidades e impacto con la red analizada y las tendencias entre los ciberatacantes. Con esto se logra centrar los esfuerzos del equipo de remediación en las amenazas inminentes para la organización y mantener a raya las amenazas potenciales. Estas prioridades son establecidas tras un primer análisis pero cambian constantemente de acuerdo a los nuevos datos que se reciben de las fuentes de inteligencia, obteniendo siempre la seguridad más eficiente posible en cuanto a riesgo.

Características destacables:

- Solución enfocada a la correcta priorización de las amenazas
- Capacidad de importar muchos datos de terceros
- Proporciona mucha información de cara a la remediación

Áreas de mejora:

- Ausencia de informes generados
- Ausencia de escáner de vulnerabilidades propio
- Un mejor análisis de amenazas requiere de la compra de Skybox Threat Manager

5.2.3. Digital Defense

Digital Defense, Inc.[32] es una empresa con sede en San Antonio (USA) fundada en 1999 que se dedica a proveer soluciones de evaluación de riesgos de seguridad. En concreto se especializa en evaluaciones regulares, reacción rápida a amenazas, concienciación en seguridad y propiedades intelectuales.

Es la primera de sus especializaciones la que interesa para la evaluación y gestión de vulnerabilidades, haciendo posible la realización de todas las fases en una misma plataforma bajo el nombre de Frontline Vulnerability Manager.
Esta plataforma está construida pensando en la movilidad desde un inicio, con una interfaz en HTML5 y Angular para poder ser accesible desde cualquier tipo de dispositivo.

Además, esta solución es ofrecida como SaaS, sin la necesidad de mantener una infraestructura adicional por parte del cliente, quitando del Frontline RNA, el cual se explicará posteriormente.
A estas facilidades se les une un muy buen servicio de soporte al cliente con disponibilidad 24/7 en todos los packs que se ofrecen.

Para realizar la detección de activos y el escaneo de vulnerabilidades, Frontline VM se basa principalmente en los datos recolectados por el dispositivo de reconocimiento de redes Frontline RNA.
Este dispositivo es propiedad de Digital Defense y viene ya preconfigurado para realizar la evaluación de seguridad de la red, incluyendo escaneo de aplicaciones web y la detección automática de aplicaciones. Si unimos este dispositivo a los escáneres externos propios de Digital Defense nos encontramos con que se pueden realizar escaneos internos y externos, los cuales a su vez pueden ser autenticados o no autenticados.

Frontline RNA cuenta con un sistema operativo también propiedad de Digital Defense basado en Linux, utilizado para escanear las vulnerabilidades y debilidades de todas las IPs accesibles desde el dispositivo, incluyendo servidores, impresoras, teléfonos IP, *routers*, *switches* y *firewalls* entre otros. Los datos recogidos de estos escaneos son enviados mediante conexiones cifradas al Centro de Operaciones de Red Segura (SNOC) de Digital Defense, donde se procederá a analizarlos. Tanto el escaneo como la evaluación y la gestión de vulnerabilidades son ejecutadas bajo demanda del cliente.

Este dispositivo hace uso del motor de escaneo NIRV, también propiedad de Digital Defense, el cual propone una metodología de escaneo diferente a la de la competencia. Mientras que las tecnologías de otras empresas ofrecen una auditoria de cada servicio en aislamiento de una manera repetitiva, NIRV es capaz de auditar redes enteras como una serie de entidades contiguas, donde la información recolectada de un activo, servicio o aplicación es tenida en cuenta en el escaneo del resto de la red.

Siguiendo este procedimiento NIRV es capaz de emular mejor que el resto de escáneres el comportamiento de un atacante real, haciendo uso de estos datos de otros activos para encontrar vulnerabilidades más graves haciendo uso de otras que podrían parecer menos importantes a priori. Gracias a esta tecnología de análisis de contexto cruzado ya se han reportado decenas de vulnerabilidades a grandes empresas de software, resultando en otros tantos CVEs.

La otra tecnología esencial para Frontline VM es la Atribución Digital de Nodo (DNA), la cual se encarga de realizar una correcta catalogación de activos. DNA es capaz de realizar una correcta identificación del activo a lo largo del tiempo independientemente de identificadores dinámicos como pueden ser la dirección IP, el nombre de DNS y el de NetBIOS. Como resultado de esta mejor identificación de activos también se obtiene un mejor escaneo general.
Tras establecer los diferentes activos se usa un etiquetado inteligente. Este se divide en las etiquetas automáticas, establecidas previamente por el usuario, y etiquetas dinámicas, que permiten la creación de grupos al momento basándose en

las necesidades del usuario en ese preciso instante.

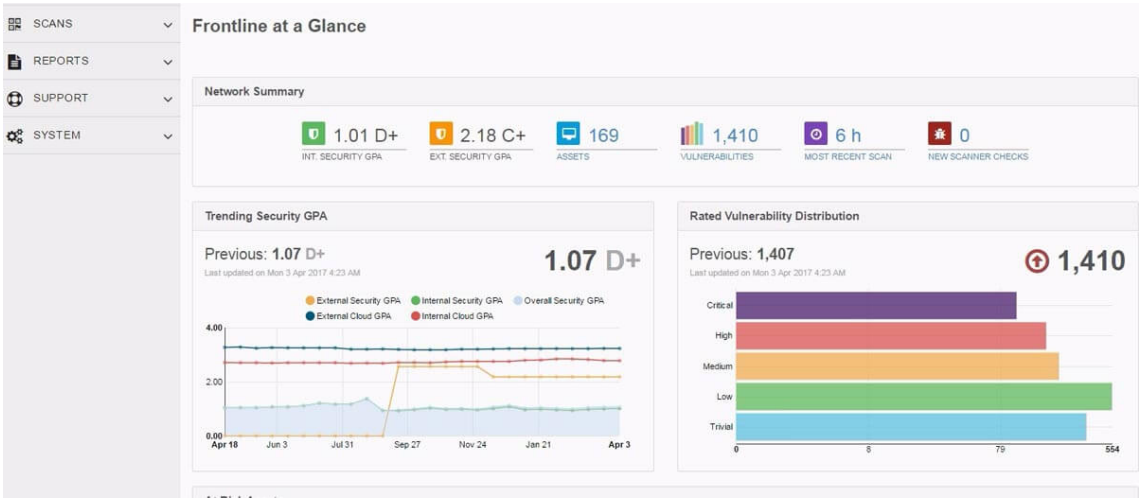

Figura 5.17: Frontline VM panel general

A la hora de puntuar el riesgo de cada vulnerabilidad se hace uso de Frontline Security GPA, unas métricas capaces de reflejar las mejoras que se dan entre las continuas evaluaciones de la red.
Adicionalmente, se cuenta con una inteligencia de amenazas propia que se obtiene del equipo de investigación Vulnerability Research Team (VRT) propio de la compañía, que se encuentra en búsqueda de nuevos riesgos de forma continua.
Para la puntuación de cada activo se tiene en cuenta qué tipo de dispositivo es este y se prioriza de acuerdo a su importancia en la red y la puntuación que corresponde a la vulnerabilidad en solitario.

Digital Defense también es un vendedor certificado CIS y vendedor de escáneres aprobado PCI ASV, estando cualificado para mostrar el estado de conformidad de estándares gracias a una metodología de pruebas explícitas. Se pueden crear tanto informes personalizados como usar los informes de conformidad predeterminados. Entre estos últimos se encuentran informes predeterminados para CIS, PCI, HIPAA/HITECH, SOX, GLBA, FISMA, FFIEC, OWASP y NERC.
En el ámbito general de la plataforma también destaca la capacidad de crear informes específicos para cada activo, así como generar bajo demanda informes ejecutivos, informes para administradores e informes de conformidad, estos últimos pudiendo diferenciarse según el activo, el escaneo o la vulnerabilidad. Todos los informes realizados se pueden generar en los formatos PDF, HTML, CSV, y XML.
Con el fin de proporcionar una visión general del estado de la seguridad también se pueden generar paneles ejecutivos para ver los indicadores clave de la infraestructura de un solo vistazo.

Todos estos datos recolectados en cualquier fase de la evaluación y gestión de vulnerabilidades de esta plataforma pueden ser exportados o importados con terceros a través de las Frontline Connect RESTful APIs, para realizar intercambio de información con plataformas de gestión y SIEM de terceros como pueden ser IBM QRadar, ServiceNow y ZenDesk.

Características destacables:

- Buen soporte para el producto y para la creación de una estrategia de seguridad en la empresa
- Facilidad a la hora de ver el progreso en los informes, destacando nuevas vulnerabilidades o activos
- Informes generados altamente personalizables

Áreas de mejora:

- No cuenta con capacidades de escaneo continuo
- Necesidad de comprar dispositivos Frontline RNA en función de la segmentación de la red y número de activos que hay que securizar
- No se explica el funcionamiento de la priorización de vulnerabilidades por parte de Frontline Security GPA

5.3 Competidores

5.3.1. Kenna Security

Kenna Security[33] es una joven empresa fundada en 2009 con sede en San Francisco, California, que se dedica exclusivamente a proveer soluciones de gestión de vulnerabilidades e inteligencia de riesgo.
El hecho de que no preste las herramientas de escaneo de vulnerabilidades no impide a esta herramienta ser considerada una competidora debido a la excelente gestión que realiza en el resto de etapas de la evaluación y gestión de vulnerabilidades.
La solución estándar también se vende bajo el nombre de Kenna Security aunque se puede expandir con Application Risk Module, el módulo destinado a asistir en el desarrollo seguro de aplicaciones.

Para hacer uso de esta solución primero es imprescindible importar un escaneo de vulnerabilidades para poblar la lista de activos de la empresa. Luego se podrá dividir manualmente esta lista en grupos, a los que se asignará una prioridad que Kenna Security tendrá en cuenta.
Y es aquí donde se llega a uno de los puntos fuertes de este producto: la inteligencia de riesgos. Combina los recursos de más de 8 fuentes de inteligencia de primera línea, como son Qualys, Rapid7, Nessus, Exploit Database o Metasploit entre otras fuentes, para así establecer una puntuación general y evaluar el riesgo de todo el sistema.

Usando esta calificación para las vulnerabilidades y teniendo en cuenta la importancia de cada grupo de activos se llevará a cabo una priorización automática de vulnerabilidades que gracias a la puntuación de vulnerabilidades basada en

amenazas de Kenna se dividirán en las categorías Máxima Prioridad, Brechas de Internet Activas, Fácilmente Explotables, Explotables por Malware, Objetivos Populares y Vulnerabilidades de día 0, como se puede observar en la figura 5.18 .

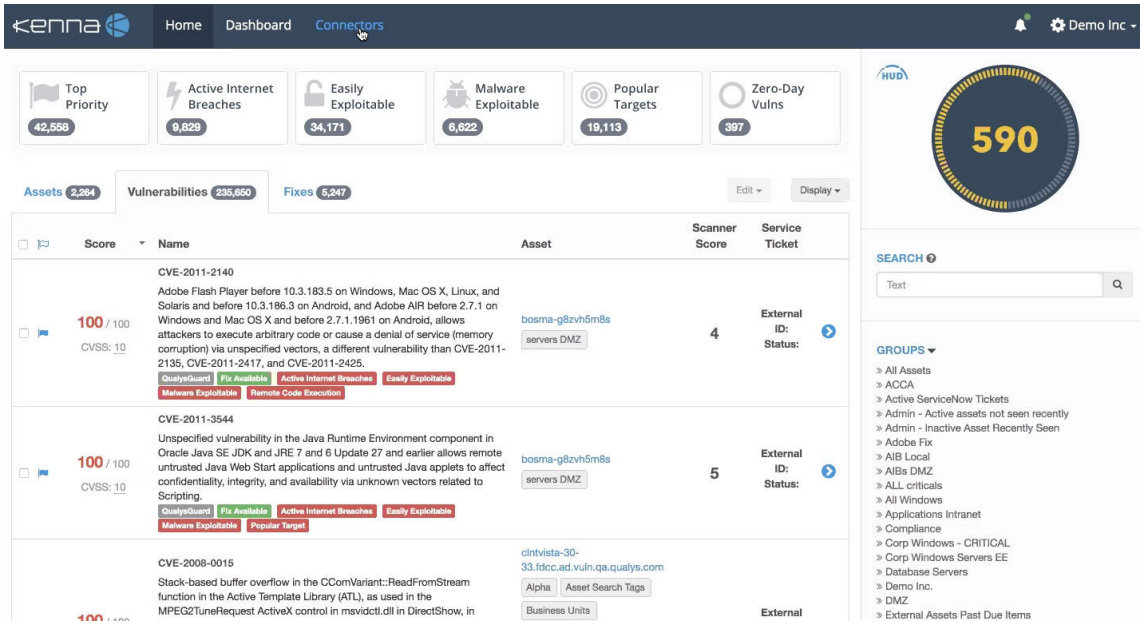

Figura 5.18: Kenna Security pestaña Home

Esta solución no proporciona simplemente diferentes listas priorizadas en función de los tipos de ataques, sino que también cuenta en cada una de estas listas los arreglos que hay que realizar para corregir estas vulnerabilidades. La información de dichas vulnerabilidades y su solución pueden ser enviadas automáticamente al equipo de remediación, gestionando de una manera centralizada todo el proceso de remediación.

Por último también cuenta con informes generalistas a base de gráficos para poder mostrar los resultados del trabajo realizado a personal no técnico. Los informes se pueden hacer desde generales hasta de grupos en concreto y se pueden exportar desde la misma pestaña de Dashboards, como se puede observar en la figura 5.19 .

Características destacables:

- Priorización de vulnerabilidades muy potente
- Generador de informes sencillo y completo
- Aplicación visual e intuitiva

Áreas de mejora:

- Carece de escáner de vulnerabilidades propio
- Coste alto y con problemas de escalabilidad
- Falta de transparencia a la hora de justificar la priorización de riesgos

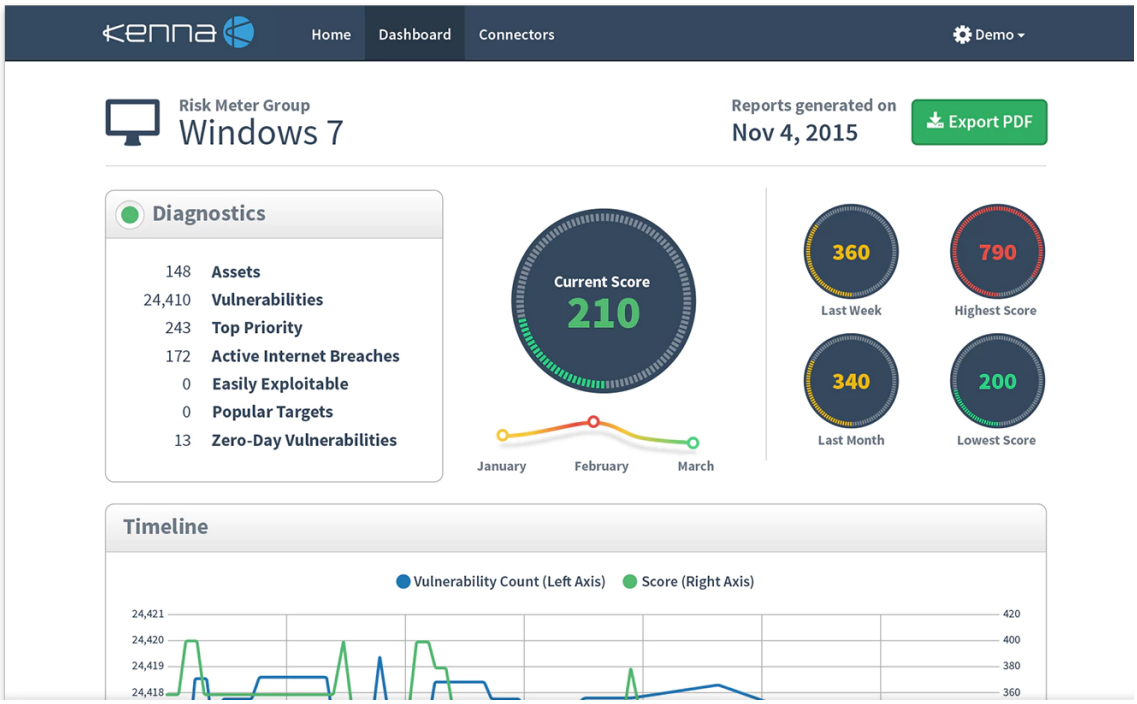

Figura 5.19: Kenna Security pestaña Dashboard

5.3.2. Tripwire

En 1992 y como reacción al escándalo del Gusano Morris, incidente que ya se ha explicado con anterioridad, el estudiante de la Purdue University, Gene Kim junto con su profesor Gene Spafford crearon la versión inicial del software Tripwire[34]. Aunque se creó por aquél entonces, no sería hasta 1997 que se fundó la empresa que lleva por nombre el de este pionero software de detección de intrusiones.

La empresa basada en Portland inicialmente abrió el código de la versión universitaria con Open Source Tripwire, pero no sería hasta 2005 que lanzarían Tripwire Enterprise, el buque insignia de la empresa para el control de cambios en configuraciones y archivos.
Posteriormente en 2010 llegaría Tripwire Log Center, una solución dedicada a la seguridad de la información y logs y gestión de eventos (SIEM), para finalmente alcanzar el lanzamiento de Tripwire IP360 en 2013 tras la adquisición de nCircle.

Este último producto es el que más interesa para el estudio, al tratarse de un gestor de vulnerabilidades y evaluador de riesgo.
Aunque se puede usar de manera independiente uno de los puntos fuertes de la oferta de esta empresa es una integración de estas dos soluciones comentadas con anterioridad, cubriendo muchos ángulos de la seguridad de la empresa desde un solo sistema que mejora cada una de sus soluciones gracias a la retroalimentación con los resultados de las otras soluciones Tripwire.

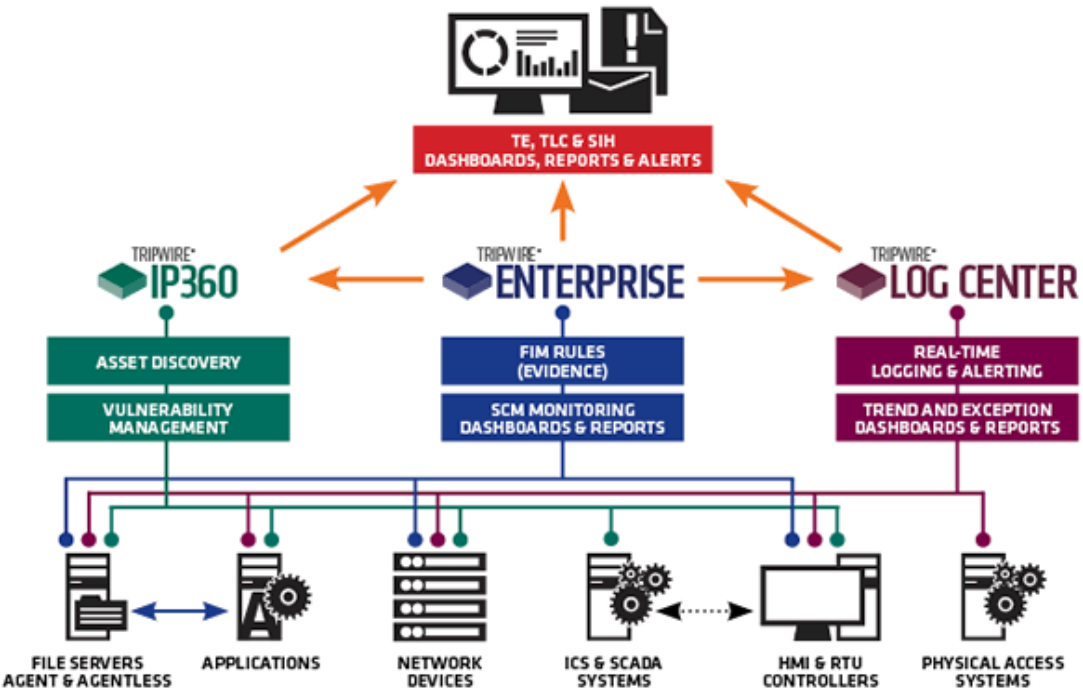

Figura 5.20: Componentes de la solución completa Tripwire

Tripwire IP360 dispone de herramientas de descubrimiento de activos en propiedad, así como de escáneres de vulnerabilidades. Estos últimos se basan en inteligencia de riesgos propia de Tripwire, la cual se obtiene y mejora continuamente gracias a un extenso equipo de investigadores, el Vulnerability and Exposure Research Team (VERT).
El escaneo de vulnerabilidades es tanto autenticado como sin autenticar. En el escaneo autenticado primero se identifica el activo que se está analizando para solo buscar vulnerabilidades que pueden afectar a ese tipo de activos, mejorando la calidad del escaneo y reduciendo considerablemente el tiempo necesario para hacer este tipo de análisis.

Pero si hay algo que destaca de esta solución es el sistema de puntuación de vulnerabilidades, el cual, al contrario de lo que sucede en Kenna Security, se encargan de explicar al detalle en la misma página del vendedor.
Esta puntuación se rige principalmente por la fórmula mostrada en la figura 5.21.

$$V_n = \sqrt{t_n} \times \frac{r_n!}{{s_n}^2}$$

Figura 5.21: Tripwire Vulnerability Scoring System

t: Es el número de días transcurridos desde que la vulnerabilidad n fue hecha pública en fuentes importantes de ciberseguridad, ya sea el propio vendedor o prensa especializada.

r!: Es el factor 'clase de riesgo', representa la amenaza que supone tener la vulnerabilidad n en un sistema s.
Este es establecido por el VERT con valores desde 0 para vulnerabilidades de revelaciones de información hasta 720 para vulnerabilidades remotas con las que se puede obtener privilegios administrativos completos.

s: Es una medida de la 'habilidad' necesaria por parte del atacante para llevar a cabo un ataque que explote la vulnerabilidad n.
Esta es establecida por el VERT con valores desde 6 para vulnerabilidades sin exploits disponibles hasta 1 para vulnerabilidades con *exploits* ya automatizados disponibles.

V: Representa la puntuación de la vulnerabilidad, suponiendo un mayor valor una mayor prioridad de reparación.

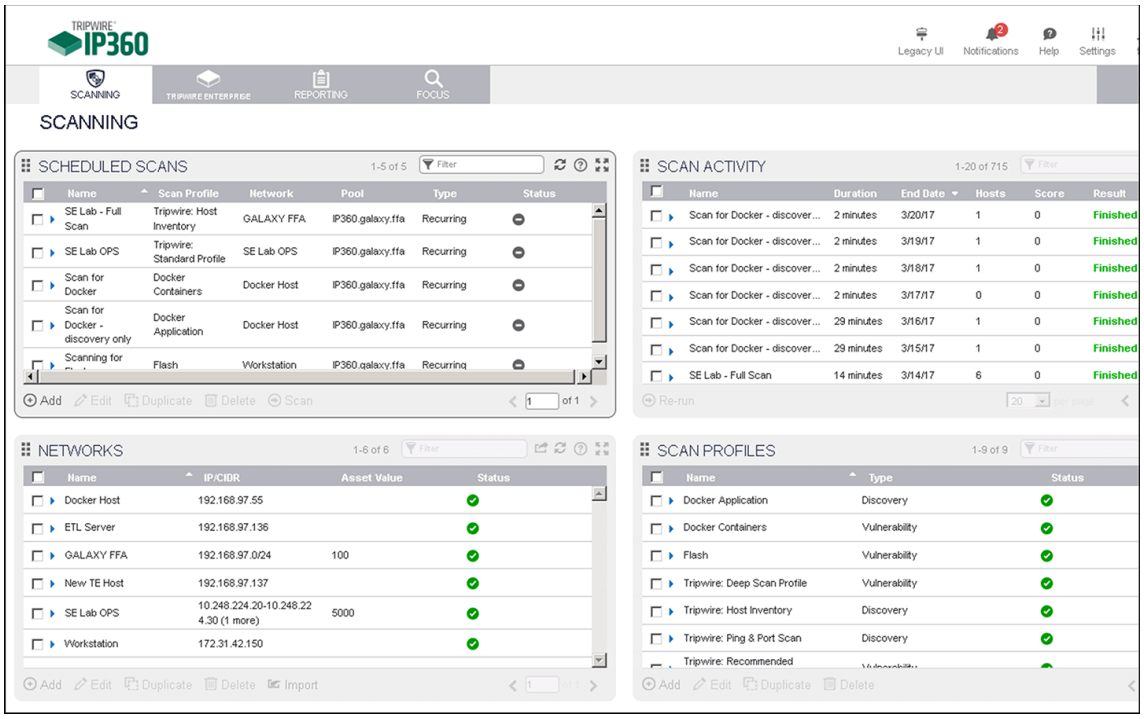

Figura 5.22: Tripwire IP360 pestaña de Escaneo

Esta puntuación obtenida no es la definitiva para una vulnerabilidad, ya que en cada implementación de Tripwire la puntuación final dependerá del valor que se le haya otorgado al activo tras ser descubierto. Esta puntuación se llama Asset Value y debe ser introducida manualmente por el encargado de gestionar Tripwire IP360 para asignar una importancia al activo en el contexto del sistema entero. La puntuación final de la vulnerabilidad dependerá directamente del Asset Value del activo en el que se encuentre.

Características destacables:

- Sistema de puntuación único y eficaz
- Excelente sinergia con el resto de productos Tripwire
- Arquitectura muy resilente, gracias a dispositivos físicos o virtuales basados en Linux y mejorados en términos de seguridad

Áreas de mejora:

- Carece de funcionalidad para comprobar conformidad
- Carece de evaluación de vulnerabilidades para nube y contenedores
- Interfaz poco amigable y usable

5.4 Desafiadores

5.4.1. Beyond Security

La empresa Beyond Security Ltd.[35] fue fundada en 1999 con el objetivo de proveer a los clientes herramientas para gestionar las debilidades de las redes.

Para realizar la evaluación y gestión de vulnerabilidades, esta empresa israelí ofrece la solución Automated Vulnerability Detection System bajo el producto beSECURE.
beSECURE es una herramienta que detectará vulnerabilidades en los activos de la red en la que se encuentre. Una vez encontradas estas vulnerabilidades serán reportadas con la información necesaria para la remediación de las mismas.

Esto se logra gracias a una visión en tiempo real de los activos y de la red en general, priorizando los activos vulnerables para mejorar la seguridad de la red de manera eficiente. beSECURE lo consigue mediante escaneos automáticos de todos los nodos con direcciones IP y una base de datos de vulnerabilidades actualizada cada hora.
Para lograr un resultado satisfactorio para el cliente el equipo de Beyond Security ha decidido centrarse en tres diferentes aspectos: La precisión del análisis, la felxibilidad del producto y la simplicidad.

Los evaluadores de vulnerabilidades actuales dependen demasiado de la comprobación de versiones, aunque existe la posibilidad de que el activo esté seguro pese a tener una versión antigua y uno con la versión actualizada no lo sea. Por ello Automated Vulnerability Detection System utiliza pruebas basadas en comportamiento, considerando la interacción de ajustes de configuración, disponibilidad de servicios, parches implementados mediante *backporting*[9] y otros factores

[9]Backporting: La acción de tomar partes de una versión más reciente de un sistema o componente software y adaptarlo a una versión más antigua de ese mismo software

que pueden securizar por completo un activo no actualizado. Este tipo de escaneo de los activos resulta en:

- Reducción de falsos positivos, poniendo en relevancia las vulnerabilidades encontradas
- Priorización más precisa, permitiendo a beSECURE tratar la vulnerabilidades más críticas con certeza
- Resultados más utilizables, dado que se crean informes más sucintos y precisos se incluyen más recomendaciones de mitigación que aportan un mayor valor

En cuanto a la flexibilidad y para poder adaptar la solución de Automated Vulnerability Detection System a cualquier escenario se proporcionan tres diferentes versiones del producto:

- beSECURE I, esta versión es ofrecida como Software as a Service, basada en la nube y haciendo uso de agentes para cada activo.Tiene la capacidad de crecer desde 100 hasta 50,000 IPs. Es la mejor versión para escanear entornos basados en la nube
- beSECURE II, hace uso de un sensor hardware ADVS, el cual tiene todos los datos almacenados en el interior y cuenta con una gran seguridad, excediendo los estándares internacionales. Esta versión es ideal para entornos SMB y puede llegar hasta las 2,500 IPs
- beSECURE III, esta es la versión más potente y segura, haciendo uso de sensores con una seguridad reforzada. Puede llegar a cubrir grandes redes distribuidas desde las 1,000 hasta 1,000,000 de IPs

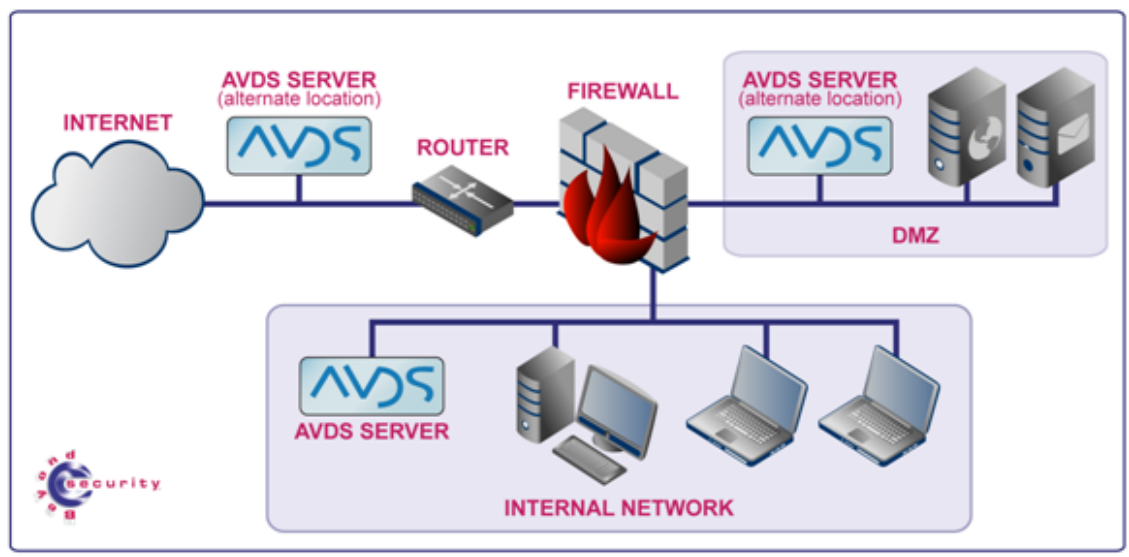

Figura 5.23: Posible esquema de red con Sensores ADVS

La simplicidad la logra a través de un producto con una interfaz sencilla e intuitiva. También se ha reducido al mínimo la complejidad de la configuración y el

mantenimiento, incluyendo hasta la instalación, que no requiere ni de personal cualificado para hacerla.
Más allá de la misma plataforma también se ha implementado un sistema de licencias optimizado para rangos de red muy grandes.

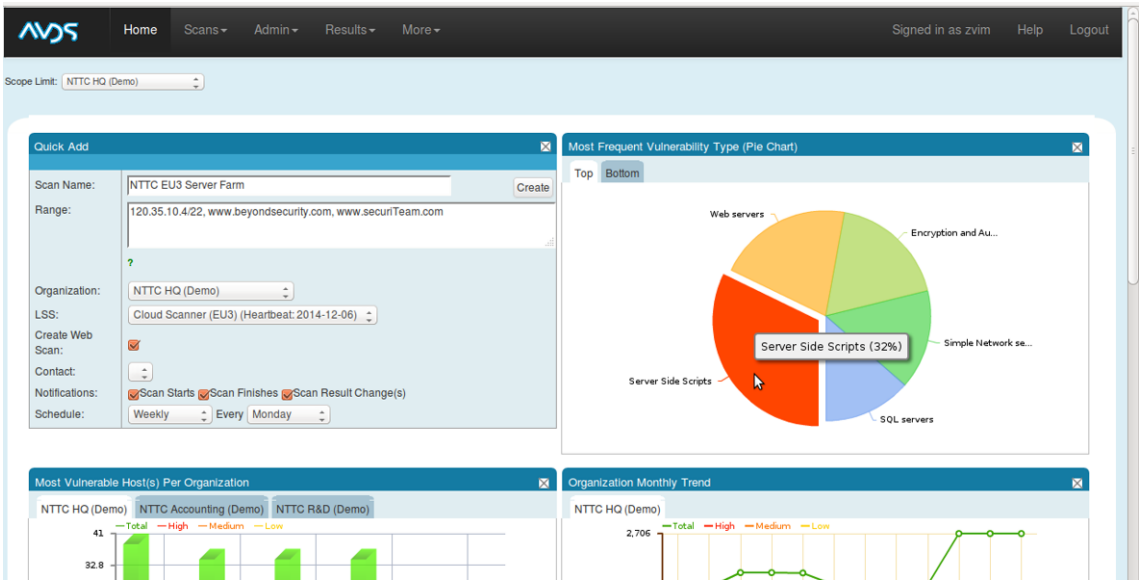

Figura 5.24: Beyond Security ADVS pestaña Home

Adicionalmente esta solución también ofrece escaneo de vulnerabilidades para aplicaciones web y bases de datos.
Las vulnerabilidades de estos activos también se tendrán en cuenta para los informes de conformidad. Estos informes cubren un gran número de estándares como PCI, HIPAA, ISO, SOX o NERC-CIP.

Los informes están construidos según el lector para el que vayan dedicado, los hay para ejecutivos, gerentes y administradores entre otros. Un informe destacado es el de conformidad con la GDPR, que supone un punto a favor dadas las fechas que corren.

Por último beSECURE incluye APIs flexibles y bi-direccionales para la integración con sistemas de *ticketing*, generación de informes y SIEM.

Características destacables:

- Gran precisión a la hora de verificar vulnerabilidades
- Instalación y mantenimiento de la solución al alcance de personal no técnico
- Generación de informe de conformidad con la EU GDPR

Áreas de mejora:

- No se especifica apenas nada del funcionamiento interno de la solución
- Generación de informes limitado a tipos establecidos
- No han habido apenas mejoras para la aplicación en los últimos años

5.5 Conclusiones del análisis de mercado

Una vez vistas en detalle las distintas soluciones que componen el grueso de la oferta a nivel mundial en cuanto a evaluación y gestión de vulnerabilidades, se procederá a hacer una comparativa en forma de tabla de todas ellas y a explicar la elección más apropiada en dos casos de uso representativos para un número elevado de empresas.

A la hora de realizar la tabla comparativa de todas las soluciones analizadas en el documento se seguirán los criterios ya expuestos y definidos al comienzo de este capítulo:

1. Gestión de los activos de la empresa
2. Calidad de la enumeración de vulnerabilidades, uso de escaneo activo/pasivo, autenticado/no autenticado y si tiene agente de sistema
3. Rapidez y calidad de las actualizaciones de la base de datos de vulnerabilidades y/o amenazas usada
4. Soporte para la evaluación de servicios en la nube y contenedores
5. Compatibilidad con diferentes sistemas operativos e integración con terceros
6. Algoritmo de priorización de amenazas
7. Evaluación de conformidad respecto de estándares y normativas
8. Calidad de los informes generados
9. Usabilidad ofrecida por la solución
10. Soporte proporcionado por el vendedor

Finalmente, para calificar cada una de estas características de las soluciones se usará el siguiente sistema de puntuación numérico:

0: Inexistente

1: Deficiente

2: Regular

3: Bien

4: Muy Bien

5: Excelente

Tabla 5.1: Tabla de calificación nº1.

	Rapid7	BeyondTrust	NopSec	Qualys	Tenable
Gestión de activos	5	4	4	5	5
Enumeración Vulnerabilidades	5	5	4	5	5
Calidad de la base de datos	5	4	4	5	4
Nube y contenedores	5	3	3	5	5
Compatibilidad e integración	5	5	5	5	5
Algoritmo de priorización	5	4	5	5	3
Evaluación de la conformidad	0	5	4	0	0
Generación de informes	2	5	5	4	3
Usabilidad de la solución	5	2	5	4	4
Soporte del vendedor	3	4	3	3	3

Tabla 5.2: Tabla de calificación nº2.

	Skybox S.	Digital D.	Kenna S.	Tripwire	Beyond S.
Gestión de activos	3	4	0	3	3
Enumeración vulnerabilidades	2	2	0	4	4
Calidad de la base de datos	4	4	5	4	4
Nube y contenedores	4	3	0	2	2
Compatibilidad e integración	4	3	3	3	4
Algoritmo de priorización	5	4	4	5	3
Evaluación de la conformidad	0	4	0	0	4
Generación de informes	0	4	4	3	2
Usabilidad de la solución	2	4	4	2	2
Soporte del vendedor	3	5	4	3	2

Pero como ya se ha visto a lo largo del análisis cada solución tiene características únicas en el mercado, como único es el entorno y las necesidades de cada empresa. Es por ello que a continuación se mostrará el proceso de la elección de herramienta para la evaluación y gestión de vulnerabilidades por parte de dos empresas ficticias pero con entornos muy reales y usuales en una gran cantidad de empresas.

En primer lugar se procederá a explicar la situación de la empresa para posteriormente justificar la decisión tomada en cuanto a la solución a utilizar. Se llamará a estas empresas Alpha y Beta respectivamente.

5.5.1. Empresa Alpha

Alpha es una empresa tecnológica internacional cuyo negocio consiste en ofrecer juegos móviles gratuitos con micropagos. Ya que para llevar a cabo estos pagos se necesita almacenar los datos de las tarjetas de crédito de los usuarios tienen que cumplir con el PCI Data Security Standar, un estándar para mejorar la seguridad del tratamiento, procesado o almacenamiento de información de tarjetas de crédito.

Los usuarios pueden hacer uso de los juegos localmente pero para realizar los pagos necesitan conectarse directamente a uno de los múltiples servidores públicos propiedad de Alpha. La infraestructura interna es una red de unas 500 IPs donde coexisten desarrolladores y personal no técnico.
La dirección de la empresa tiene un especial interés en controlar la evaluación y gestión de vulnerabilidades a la par que la conformidad con el PCI, por ello se busca una solución con una generación de informes potente y también orientado a personal no cualificado.

Para encontrar la solución óptima primero siempre hay que buscar los aspectos que sean importantes para la empresa y sean más difíciles de encontrar en el mercado. En este caso ese aspecto es la evaluación de la conformidad con el PCI. De todas las soluciones analizadas solo dos proporcionan informes de conformidad con PCI, y estas son las soluciones de NopSec y Digital Defense. Aunque a priori NopSec se encuentra un escalón por encima de Digital Defense al ser considerados líderes de sector y los segundos solo actores fuertes, hay que analizar las necesidades de la empresa para ver cual se adecua mejor a los requerimientos.

Ambas soluciones tienen un desempeño y servicios muy similar en casi todos los aspectos de su evaluación y gestión de las vulnerabilidades, por lo la comparación se centrará en los dos aspectos más importantes para esta empresa: La evaluación de la conformidad y la calidad de los informes generados.

Respecto de la conformidad ambas ofertan la evaluación de conformidad de PCI entre otros estándares, con el resultado de la generación de un informe al respecto. Además Digital Defense es un vendedor de escáneres aprobado PCI ASV, por lo cual el resultado de sus informes ya están aprobados para el cumplimiento del

estándar.

En lo relativo a la generación de informes la solución de NopSec crea una lista de amenazas prioritarias una vez finalizado el escaneo y genera una serie de gráficos e informes personalizables y muy visuales para personal no técnico. Por parte de Digital Defense ofrece una serie de informes bajo demanda para ejecutivos y administradores, ambos se pueden realizar a nivel de escaneo general, activo o vulnerabilidad específica, además de la capacidad de configurar paneles para la visualización de los resultados.

Pese a que a priori la solución de NopSec parecía partir con ventaja, tras analizar las características buscadas por el cliente se puede comprobar como la solución de Digital Defense mejora con creces a su adversario.
Si a esto se le une que esta solución se ofrece por un precio menor a la de NopSec queda en evidencia que la solución óptima para la evaluación y gestión de vulnerabilidades en la empresa Alpha es Frontline Vulnerability Manager, de Digital Defense.

5.5.2. Empresa Beta

La empresa Beta se dedica a la publicación de artículos y tutoriales relacionados con la ciberseguridad.
A nivel de infraestructura posee solamente una pequeña red centralizada en la sede de la empresa, donde trabajan los desarrolladores y personal de la empresa, ya que el servicio de cara al público se ofrece a través de Amazon Web Services (AWS). Por último, una singularidad de la empresa es que hacen uso a nivel interno de aplicaciones para la creación de los tutoriales desarrolladas por ellos mismos en contenedores bajo la tecnología Docker.

En este caso el hecho de que todos los servicios al público sean hechos a través de Amazon AWS, unido al uso de contenedores internamente facilita mucho el primer filtrado de soluciones.
Estos dos aspectos son críticos para la empresa, y el hecho de tratarse de una empresa que se dedica al sector de la seguridad no hace sino acentuar la importancia de una buena ciberseguridad de cara a posibles atacantes externos.
Es por ello que se decidirá la solución entre las empresas que oferten un mejor control sobre la nube y los contenedores, o lo que es lo mismo, entre las soluciones de Rapid7, Qualys y Tenable.

No hay más que echar un vistazo a la tabla de calificaciones sacada como conclusión del estudio de mercado para observar la igualdad de estas tres soluciones en todos los puntos, con Qualys destacando un poco en la generación de informes y Tenable con unos resultados ligeramente inferiores en general al de las dos empresas líderes en el sector.

La solución de Rapid7 destaca por su escaneo continuo mediante el agente Insight Agent, el cual se puede integrar de manera nativa con Amazon Web Services y repositorios de contenedores Docker.

Esto otorga a insightVM una visibilidad continua de servicios *cloud* y contenedores gracias al agente que permite mantener una visión unificada de todos estos activos. También es una ventaja con esta solución el tamaño reducido de la red de Beta, ya que se necesitaría un paquete de compra pequeño y por ende más económico.

La propuesta de Qualys es Qualys Vulnerability Management, que ofrece servicios de escaneo de nube con Virtual Scanner y también cuenta con integración nativa de Amazon Web Services.
Sin embargo la oferta de esta solución viene limitada en cuanto a número de IPs a escanear y para obtener todo el sistema de evaluación y gestión de vulnerabilidades son necesarias dos aplicaciones más: Qualys Asset Inventory y Qualys Security Configuration Assessment.
Para la evaluación de repositorios de contenedores hace falta adquirir Qualys Container Security, aunque carece de ninguna integración nativa con productos de terceros.

Finalmente se encuentra la opción de Tenable, la plataforma Tenable.io que incluye las aplicaciones Vulnerability Management, Web Application Scanning y Container Security.
La última de estas es la que se encarga concretamente de la evaluación de repositorios de contenedores y disfruta de una integración nativa con productos de terceros como Docker Registry y Docker Trusted Registry.
La integración con Amazon Web Services está garantizada ya que Tenable pertenece a la red de asociación AWS Partner Network (APN).
Adicionalmente esta solución sí que presenta un generador de informes con un desempeño aceptable.

Una vez analizadas todas las opciones claramente la mejor opción en casi todos los aspectos es inisghtVM de Rapid7, sin embargo la calidad de sus informes generados podría suponer un problema para la empresa si se les da una gran importancia a estos en detrimento de la gestión de la remediación.
Si el caso fuera tal, la mejor opción sería Tenable.io, que ofrece una generación de informes de calidad aceptable penalizado solo con una ligera bajada de nivel respecto de insightVM en el resto de funcionalidades.

CAPÍTULO 6
Conclusiones

Basados en lo visto a lo largo de todo este documento, se ha podido demostrar el impacto que puede tener en la seguridad de una empresa el uso de soluciones de evaluación y gestión de vulnerabilidades.

El mercado de los ciberatacantes y de las amenazas continuas ha llegado para quedarse. Como se ha podido observar, pese a una sostenida mejora de la ciberseguridad en las empresas a lo largo de la historia, los ataques exitosos hacia estas mismas se siguen sucediendo hasta en empresas a las que se les supone grandes defensas por los datos que atesoran.
Lo más alarmante de la mayoría de estos ataques es que se dan por vulnerabilidades conocidas, ya sea en el software o servicios de los que hacen uso estas empresas, estando estas incluso tipificadas en diversos estudios de riesgos en aplicaciones.

Y estas empresas no solo deben de preocuparse por su propia integridad, sino de la integridad de todos los datos de usuarios que almacenan, dado que si no lo hacen existen normativas como la LOPD y la GDPR que podrían imponer importantes sanciones incluso económicas en el caso de que la empresa no gestione correctamente la seguridad de esta información personal de los usuarios.

El cibercrimen actualmente se focaliza en la explotación de vulnerabilidades conocidas que pueden reportar resultados rápidos en vez buscar nuevas vulnerabilidades como sí que hacía en un pasado.
Es por todo esto que la evaluación y gestión de vulnerabilidades cobra una gran importancia en el ecosistema actual de la ciberseguridad. Estos procesos se encargan de detectar y eliminar precisamente este tipo de amenazas conocidas que a menudo se pueden solucionar con parches o actualizaciones, estas vulnerabilidades que aunque a priori resulten incomprensibles siempre se pueden encontrar en la red de cualquier empresa.

Hoy en día casi todas las organizaciones hacen uso de pruebas de pentesting, un proceso que busca vulnerabilidades en el sistema pero priorizando la profundidad, no siendo de mucha utilidad para empresas sin una ciberseguridad notable previa. Sin embargo la evaluación y gestión de vulnerabilidades es un proceso que se centra en la amplitud, abarcando las vulnerabilidades en toda la red de la empresa frente a la profundización que puede hacer un *pentest* haciendo uso de

una sola vulnerabilidad.

En el estudio de las diferentes soluciones se ha demostrado la utilidad de la evaluación y gestión de vulnerabilidades, no solo en lo referente a detectar y remediar riesgos existentes para la seguridad de la red de la empresa, sino para tener un conocimiento de los activos que conforman esta red y de cómo afecta la seguridad de cada uno de estos a la red completa.

Las soluciones ofrecidas actualmente en el mercado son de una calidad ostensiblemente superior a las que se podrían encontrar hace escasos años, contando actualmente con capacidades para la evaluación de nuevas tecnologías como podrían ser entornos virtuales, dispositivos móviles, entornos de nube o incluso contenedores. A estas nuevas capacidades también hay que sumarles una mejor inteligencia para la priorización de estos riesgos y la integración con productos de terceros para mejorar la visión y capacidades de estas soluciones.

Si bien es cierto que no se ha podido probar ninguna de estas soluciones en un entorno personal debido a la dificultad de crear un entorno de pruebas aceptable, ya que requeriría de una simulación de una red de empresa completa, con su correspondiente tráfico real y una simulación de ataques tanto externa como interna, y a la imposibilidad de obtener una *demo* por parte del vendedor si no se trata de un posible comprador; sin embargo para compensar esta condición se ha hecho uso de análisis de estas soluciones por parte de terceros en diferentes estudios y se ha realizado una investigación extensiva de las funcionalidades que ofrecen cada uno de estos productos.

Con todo esto se espera haber realizado un documento que explique el procedimiento de la evaluación y gestión de vulnerabilidades y a su vez ser legible para personal no técnico sin renunciar a una gran cantidad de información técnica de las distintas soluciones.
Resulta sorprendente la cantidad de empresas que no cuentan con una correcta evaluación y gestión de vulnerabilidades, más aún tras ver todas las bondades de este procedimiento continuo, y es por ello que se ha pretendido darlo a conocer en profundidad.

A modo de conclusión se puede decir que la evaluación y gestión de vulnerabilidades es un proceso estrictamente necesario para la consecución de una ciberseguridad óptima de la empresa, lo cual es fácil de conseguir actualmente gracias al gran abanico de soluciones ofrecidas por múltiples vendedores y que cubren todas las posibles singularidades de cada organización.

Bibliografía

[1] Definición ciberseguridad por Oxford. Consultado el 18 de Abril de 2018. https://en.oxforddictionaries.com/definition/cybersecurity.

[2] Definición ciberseguridad por The Economic Times. Consultado el 18 de abril de 2018. https://economictimes.indiatimes.com/definition/cyber-security.

[3] Onceava encuesta anual de Riesgos Emergentes. Consultado el 18 de Abril de 2018. https://www.soa.org/research-reports/2018/11th-emerging-risk-survey/.

[4] Impacto Económico del Cibercrimen-Sin Deceleración, McAfee. Consultado el 18 de Abril de 2018. https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf.

[5] Artículo de Expansión sobre la ciberseguridad en España. Consultado el 18 de Abril de 2018. http://www.expansion.com/economia-digital/companias/2017/12/08/5a27d24e268e3ed9598b45f7.html.

[6] Artículo de The Washington Post sobre injerencias rusas en elecciones estadounidenses. Consultado el 19 de Abril de 2018. https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?noredirect=on&utm_term=.7d11e8a3d249.

[7] La gran mentira de Cambridge Analytica: ningún efecto en los resultados de Facebook. Consultado el 19 de Abril de 2018. http://www.abc.es/tecnologia/redes/abci-gran-mentira-cambridge-analytica-ningun-efecto-resultados-facebook-201804noticia.html.

[8] Estudio CSIRT-CV: Cryptomining Malware. Consultado el 19 de Abril de 2018. https://www.csirtcv.gva.es/sites/all/files/downloads/Cryptomining_Malware.pdf.

[9] Declaraciones de Dave Hogue en la conferencia CyberUK 2018. Consultado el 20 de Abril de 2018. https://www.infosecurity-magazine.com/news/cyberuk18-nsa-attack-tactics-change/.

[10] Proyecto OWASP Top 10 - 2017. Consultado el 20 de Abril de 2018. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

[11] Informe Winning the Game, McAfee. Consultado el 23 de Abril de 2018. https://www.infosecurity-magazine.com/news/cyberuk18-nsa-attack-tactics-change/.

[12] Cyber Security Breaches Survey 2018, Department for Digital, Culture, Media and Sport. Consultado el 23 de Abril de 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf.

[13] Declaraciones del evento IDC Ciberseguridad 2018. Consultado el 23 de Abril de 2018. http://www.blog-idcspain.com/datos-personales-comprometidos/.

[14] Artículo de Forbes sobre la detención de los operarios de la página webstresser.org . Consultado el 23 de Abril de 2018. https://www.forbes.com/sites/nvidia/2018/04/25/how-ai-is-changing-the-multi-billion-dollar-hair-care-industry/#7fe88a5b579f.

[15] To Kill a Centrifuge, Ralph Langner. Consultado el 25 de Abril de 2018. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

[16] Informe de FireEye sobre el ciberataque a Saudi Aramco. Consultado el 25 de Abril de 2018. https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

[17] Artículo de Business Insider sobre el ciberataque a Yahoo. Consultado el 26 de Abril de 2018. http://www.businessinsider.com/fbi-yahoo-hackers-used-spear-phishing-email-gain-access-500-million-accounts-2

[18] Artículo de The Telegraph sobre el ciberataque a Ashley Madison. Consultado el 26 de Abril de 2018. https://www.telegraph.co.uk/technology/internet-security/11750432/Adultery-website-Ashley-Madison-hack-threatens-to-expose-37.5m-cheaters.html.

[19] Guía paso a paso de Phineas Fisher para ownear a Hacking Team. Consultado el 27 de Abril de 2018. http://pastebin.com/raw/0SNSvyjJ.

[20] Artículo de Bank Info Security sobre el ciberataque al Banco Central de Bangladesh. Consultado el 27 de Abril de 2018. https://www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061.

[21] Explicación de Beyond Trust sobre el funcionamiento de WannaCry. Consultado el 20 de Abril de 2018. https://www.beyondtrust.com/blog/wannacry-ransomware-attack-explained-makes-me-wanna-cry/.

[22] Boletín de Seguridad de Microsoft MS17-010. Consultado el 20 de Abril de 2018. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.

[23] Vulnerability Risk Management Q1 2018 Forrester Wave, Forrester. Consultado el 17 de Abril de 2018. https://reprints.forrester.com/#/assets/2/1336/RES141053/reports.

[24] Market Guide for Vulnerability Assessment 2017, Gartner. Consultado el 18 de Abril de 2018. https://www.gartner.com/technology/media-products/newsletters/tenable/gartner.html.

[25] Vendor Landscape: Vulnerability Management 2017, Forrester. Consultado el 18 de Abril de 2018. http://emspartner.pl/wp-content/uploads/2017/09/Report-Forrester-Vendor-Landscape-Vulnerability-Management-2017.pdf.

[26] Página oficial de Rapid7. Consultado el 5 de Mayo de 2018. https://www.rapid7.com/.

[27] Página oficial de BeyondTrust. Consultado el 8 de Mayo de 2018. https://www.beyondtrust.com/.

[28] Página oficial de NopSec. Consultado el 11 de Mayo de 2018. https://www.nopsec.com/.

[29] Página oficial de Qualys. Consultado el 15 de Mayo de 2018. https://www.qualys.com/.

[30] Página oficial de Tenable. Consultado el 18 de Mayo de 2018. https://www.tenable.com/.

[31] Página oficial de Skybox Security. Consultado el 22 de Mayo de 2018. https://www.skyboxsecurity.com/.

[32] Página oficial de Digital Defense. Consultado el 26 de Mayo de 2018. https://www.digitaldefense.com/.

[33] Página oficial de Kenna Security. Consultado el 30 de Mayo de 2018. https://www.kennasecurity.com/.

[34] Página oficial de Tripwire. Consultado el 5 de Junio de 2018. https://www.tripwire.com/.

[35] Página oficial de Beyond Security. Consultado el 8 de Junio de 2018. https://www.beyondsecurity.com/.