Sistema para la adquisición y gestión automatizada de amenazas y vulnerabilidades

Duvan Loaiza, Manuel Cárdenas
Maestría en Seguridad de la Información
Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes. Bogotá, Colombia
Diciembre 2020

1. Introducción

El continuo y rápido avance de la tecnología ha permitido desarrollar gran cantidad de soluciones para incrementar la presencia digital en las compañías a nivel global. Este crecimiento también ha impulsado el aumento del número de amenazas producidas por ciberdelincuentes. Debido a esto, las empresas deben invertir parte de sus esfuerzos en crear una postura de seguridad lo suficientemente robusta para detectar y contener estas amenazas, así como cubrir las vulnerabilidades en sus sistemas. Sin embargo, teniendo en cuenta la dificultad que representa lidiar con amenazas avanzadas y de día cero, y la gran cantidad de vulnerabilidades que reportan diferentes fuentes, la capacidad de anticiparse a las acciones de los ciberdelincuentes genera valor para la estrategia de seguridad de las empresas.

Las amenazas avanzadas están en constante aumento con el fin de evadir controles de seguridad basados en firmas. Según el fabricante de seguridad CrowdStrike, los ataques más sofisticados o "sin malware", incrementaron en el año 2019 con respecto a 2018. De acuerdo con lo anterior, año tras año la cantidad de amenazas de seguridad crece sustancialmente, haciendo cada vez más complejas las labores de análisis y contención de amenazas y vulnerabilidades en las entidades, las cuales a su vez requieren asignar herramientas suficientes para dar el correcto manejo a estas alertas.

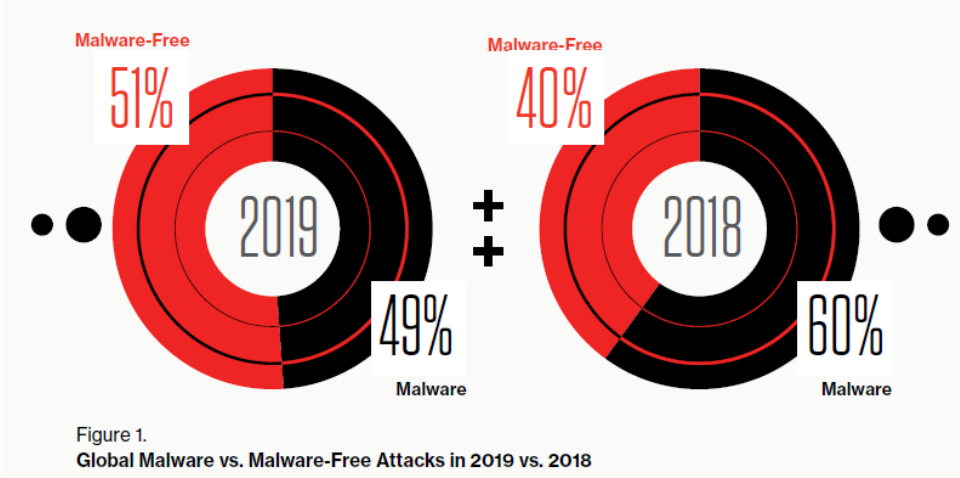

Figura 1. Tomado de Informe Global de Amenazas 2020 de CrowdStrike

Las cifras por pérdidas económicas a nivel global originadas por ciberataques incrementan continuamente. La firma de seguridad Accenture, en su reporte anual, señala que en el 2018

los ciberataques generaron pérdidas por más de 13 millones de dólares. Estas cifras indican que a pesar de que las compañías establezcan diferentes estrategias de seguridad, también es necesario abordar nuevos conceptos y metodologías de vanguardia entre los que se encuentran los servicios de ciber inteligencia y, por ello, cobra una vital importancia la gestión oportuna de estos servicios, de tal forma que se puedan anticipar a los ciberataques.

Consequences of different types of cyberattacks
(average annual cost; figures in US$ million; 2018 total = US$13.0 million)

	Business disruption	Information loss	Revenue loss	Equipment damage	Total cost by attack type
Malware (+11%)	$ 0.5	$ 1.4	$ 0.6	$ 0.1	$ 2.6
Web-based attacks (+17%)	$ 0.3	$ 1.4	$ 0.6	$ –	$ 2.3
Denial-of-service (+10%)	$ 1.1	$ 0.2	$ 0.4	$ 0.1	$ 1.7
Malicious insiders (+15%)	$ 0.6	$ 0.6	$ 0.3	$ 0.1	$ 1.6
Phishing and social engineering (+8%)	$ 0.4	$ 0.7	$ 0.3	$ –	$ 1.4
Malicious code (+9%)	$ 0.2	$ 0.9	$ 0.2	$ –	$ 1.4
Stolen devices (+12%)	$ 0.4	$ 0.4	$ 0.1	$ 0.1	$ 1.0
Ransomware (+21%)	$ 0.2	$ 0.3	$ 0.1	$ 0.1	$ 0.7
Botnets (+12%)	$ 0.1	$ 0.2	$ 0.1	$ –	$ 0.4
Total cost by consequence	$ 4.0	$ 5.9	$ 2.6	$ 0.5	**$ 13.0**

Figura 2. Tomado de "El Costo del Cibercrimen", Accenture (2019)

Algunas soluciones comerciales ofrecen funcionalidades para llevar a cabo ciertas acciones de las actividades que ayudarían a abordar esta problemática. A continuación, definimos los tipos de soluciones que existen:

- TIP (Plataforma de Inteligencia de amenazas): Centraliza información de ciberinteligencia, y permite integración con diferentes dispositivos de seguridad.
- SOAR (Security Orchestration, Automation, and Response): Este tipo de soluciones se concentran en automatizar procesos de productos de seguridad, con el fin de priorizar y estandarizar las funciones de respuesta a incidentes.
- Vulnerability Management: Estas soluciones se centran en identificar vulnerabilidades en equipos o sistemas de un determinado entorno. Por lo general cuentan con algún tipo de sistema de clasificación (débil a crítico) de las vulnerabilidades encontradas.

Los precios de lista de este tipo de soluciones en promedio son:

- TIP: USD 5000/año [3] [4]
- SOAR: USD 21000/año [5] [6]
- Vulnerability Management: USD 8000/año [7] [8]

2. Propuesta de solución

Este proyecto propone el diseño y la construcción de un sistema que automatice las actividades del proceso de gestión de amenazas y vulnerabilidades en una entidad del sector financiero, por medio de la adquisición automática de información, su correspondiente clasificación, priorización y gestión según la criticidad del reporte, y la ejecución inmediata de acciones de protección basadas en los hallazgos, con el fin de mitigar los riesgos de seguridad asociados. A continuación, se listan las funciones que debe cumplir la solución:

- Adquisición de información de amenazas y vulnerabilidades desde diferentes fuentes.
- Clasificación de la información adquirida según tipo y sistema al cual aplica, y extracción de datos relevantes.
- Redirigir información de vulnerabilidades al área encargada (desarrollo, infraestructura, core bancario, telemática).
- Registro y seguimiento de las vulnerabilidades gestionadas (estado, equipo, versión, etc.).
- Ejecutar acciones de protección en equipos y plataformas de seguridad: IPS, firewall, antivirus, antispam, filtro de contenido y sandbox.
- Realizar labores de descubrimiento de amenazas en el sistema correlacionador de eventos con base en la información adquirida revisando el comportamiento procesado por éste.
- Generar alertas para dar inicio al proceso de gestión de incidentes con base en el comportamiento detectado.
- Generar reportes de métricas relacionadas con la gestión de amenazas y vulnerabilidades.

El proceso en el cual se enmarca el presente proyecto se encuentra alineado con el BIA de la entidad, toda vez que la información relacionada con software, versiones y la criticidad de los diferentes tipos de activos son tomados de éste.

3. Diseño

A continuación, se presentan los requerimientos funcionales y no funcionales que harán parte de la versión definitiva del producto, seguido de una descripción de alto nivel de la arquitectura del sistema y la infraestructura del ambiente productivo en el cual será desplegado.

Requerimientos

Requerimientos Funcionales

- Adquisición de información de amenazas y vulnerabilidades:

  La compañía recibe información de amenazas y vulnerabilidades por medio de correo electrónico y peticiones HTTP procedente de diferentes fuentes gratuitas y de pago a

las que se encuentra suscrita. El sistema debe tener acceso a una cuenta de correo empresarial a través de la cual pueda consultar automáticamente la información tan pronto como sea recibida, para poder realizar el tratamiento correspondiente. Así mismo, una tarea programada debe consultar las APIs de aquellas fuentes que ofrezcan la información por medio de peticiones HTTP.

- Clasificación y procesamiento de la información adquirida:

  A partir de la información recibida desde las fuentes externas, se debe clasificar cada alerta según su tipo: Vulnerabilidad o Amenaza. Esta clasificación se realiza según la fuente que la reporta o extrayendo palabras claves del contenido; las alertas que no puedan ser clasificadas se deben registrar por separado para ser analizadas manualmente.

- Registro y seguimiento de información de Vulnerabilidades:

  La información de vulnerabilidades recibida se debe registrar en el sistema siempre que el producto y la versión correspondiente coincida con alguno que posea la compañía. Se debe relacionar esta información junto con la herramienta o equipo afectado y el puntaje de criticidad otorgado por la fuente. El sistema debe notificar por correo electrónico a los usuarios encargados de la evaluación y gestión de la vulnerabilidad. De igual forma, cada vez que se cambie el estado se debe poder asignar un usuario acorde a la fase del proceso en la que se encuentra y notificar al usuario correspondiente.

- Registro y procesamiento de información de Amenazas para envío a equipos de seguridad:

  De la información de amenazas recolectada se deben extraer indicadores de compromiso tales como direcciones IP, URLs, hashes, nombres y extensiones de archivos, e indicadores de correos maliciosos, mediante la integración del sistema con los diferentes equipos de Seguridad Informática de la entidad (IPS, firewall, antivirus, antispam, filtro de contenido y sandbox) para que se ejecuten de forma automática solicitudes de bloqueo. En el sistema debe registrarse cada acción ejecutada junto con el equipo notificado. Los usuarios podrán agregar información de acciones ejecutadas manualmente para complementar el conocimiento de la amenaza.

- Descubrimiento de amenazas en el correlacionador de eventos:

  Realizar labores de descubrimiento de amenazas en el dispositivo correlacionador de eventos con base en la información adquirida y revisando el comportamiento procesado por éste. Se debe enviar la acción de búsqueda de indicadores de compromiso tres meses atrás para fortalecer el proceso de cacería de amenaza en los cuales se realiza la búsqueda de actividades maliciosas en la red para reducir los tiempos de detección en la entidad.

- Generación de alertas en el correlacionador de eventos:

  El sistema debe generar alertas para dar inicio al proceso de gestión de incidentes con base en el comportamiento detectado mediante la integración con el correlacionador de eventos. Se deben enviar alertas que permitan realizar todas las actividades

necesarias del proceso de gestión de incidentes e investigación digital forense que tengan lugar en la compañía.

- Generación de reportes:

  Se deben generar reportes que permitan identificar el estado de los equipos y de aplicación de parches correctivos. De esta forma, se pueden obtener métricas de tiempos de atención de vulnerabilidades, cantidad de vulnerabilidades y amenazas gestionadas, y estado de actualizaciones en los equipos.

- Creación de roles y perfiles de usuarios:

  El sistema debe permitir la creación de diferentes roles tales como operador, analista, auditor y reportes, con el fin de que se permita segregar usuarios de acuerdo a las funciones propias del cargo y para permanecer alineados con las buenas prácticas de seguridad.

- Generación de logs de auditoría:

  El sistema debe crear logs que permitan evidenciar la trazabilidad de las acciones realizadas por los usuarios (inicios de sesión, cambio de estado de vulnerabilidades, modificación o eliminación de registros).

Requerimientos no Funcionales

- Usabilidad: Los tiempos de respuesta del sistema para los usuarios no deben ser mayor a 5 segundos para mantener una buena experiencia de usuario. Aquellas tareas que puedan implicar un tiempo mayor de procesamiento (integración con servicios externos, generación de reportes) deben optimizar su tiempo de respuesta utilizando cachés en las consultas que lo requieran, o de lo contrario informar al usuario de la demora y ejecutar la tarea en segundo plano.
- Concurrencia: El sistema debe soportar al menos 20 sesiones de usuarios concurrentes. Esto se basa en la cantidad de personas que intervienen en el proceso y que pueden requerir acceder al sistema simultáneamente.
- Disponibilidad: Debe ser de al menos 96.7% mensual (máximo 1 día fuera de línea). Se tolera este tiempo de indisponibilidad debido a que no se trata de una aplicación de misión crítica. Previo a la implementación de este proyecto, las tareas de ciberinteligencia son realizadas de forma manual en días hábiles; la mayor parte de las actividades son realizadas el último día de cada mes. La cifra propuesta mejora la disponibilidad actual del proceso.
- Seguridad: El sistema debe permitir la creación de listas de acceso basado en direcciones IP. De esta forma se restringe el acceso a la aplicación desde estaciones no autorizadas.

Requerimientos Técnicos

- El sistema requiere un framework para la construcción de aplicaciones web y el uso de librerías de aprendizaje de máquina para clasificación de información recibida y extracción de indicadores de compromiso.
- Se requiere una base de datos relacional para registrar toda la información del sistema; se escoge utilizar una instancia de base de datos MySQL.
- La aplicación debe ser compatible con navegador Internet Explorer 11 o superior y Google Chrome 85 o superior.
- La aplicación debe utilizar protocolo https con SSL versión 2 y 3 para comunicación con el cliente web.
- La aplicación debe de utilizar protocolos de comunicación segura para la integración con los diferentes equipos de seguridad.

Arquitectura y componentes de del sistema

En la Figura 3, se presenta el diagrama que ilustra la arquitectura del sistema, que incluye los componentes internos y externos que intervienen en el sistema y el flujo de la información, y se relacionan con los requerimientos previamente definidos.

Como puede observarse, el sistema se alimenta de las fuentes externas de amenazas y vulnerabilidades, las cuales son adquiridas mediante consultas HTTP y por correo electrónico. Las alertas son entonces clasificadas, registradas y gestionadas según su tipo.

El componente de Gestión de Vulnerabilidades se encarga de registrar la información de cada vulnerabilidad, asignar un usuario y calcular la criticidad y prioridad de la alerta. Mientras tanto, el componente de Gestión de Amenazas realiza la extracción de los indicadores de compromiso y entrega esta información al componente encargado de ejecutar acciones de protección mediante la integración con los equipos de seguridad. Las amenazas adquiridas también alimentarán el sistema correlacionador de eventos.

Los componentes encargados de la gestión de amenazas servirán como base para la generación de reportes, registros de auditoría y envío de notificaciones por medio de correo electrónico.

Teniendo en cuenta que se trata de una aplicación web, el usuario debe poder acceder al sistema a través de un equipo cliente utilizando un navegador web. Otros sistemas externos que deben ser considerados son los diferentes equipos de seguridad y el servidor de correo.

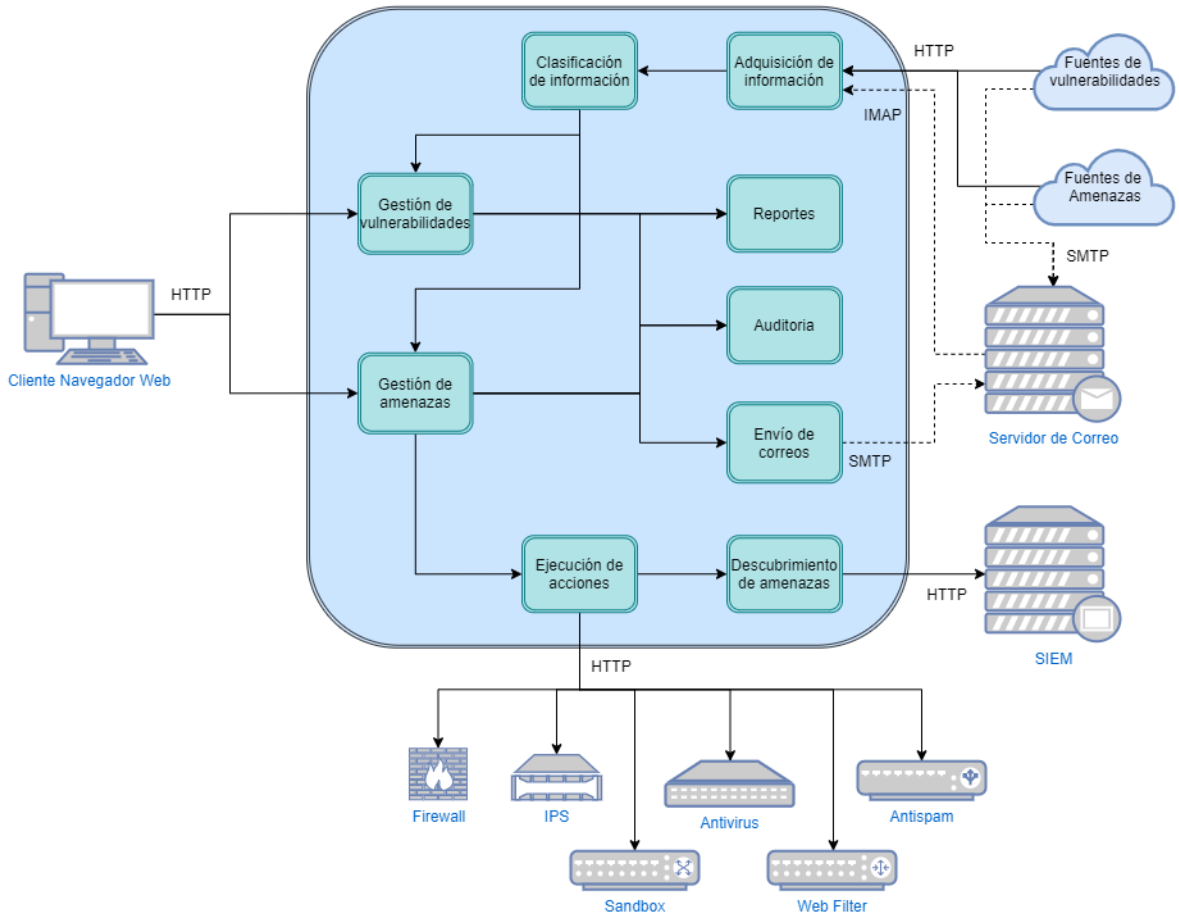

Figura 3. Arquitectura del sistema

Diagrama de infraestructura

La infraestructura sobre la cual se desplegará el sistema consta de dos servidores principales (Servidor Web y Servidor Base de Datos), los cuales poseen especificaciones estándar de la compañía. El diagrama muestra también los segmentos de red y la descripción de ancho de banda del canal de comunicación, para ilustrar a grandes rasgos la infraestructura que soporta la comunicación entre los diferentes componentes del sistema. La figura 4 presenta esta infraestructura.

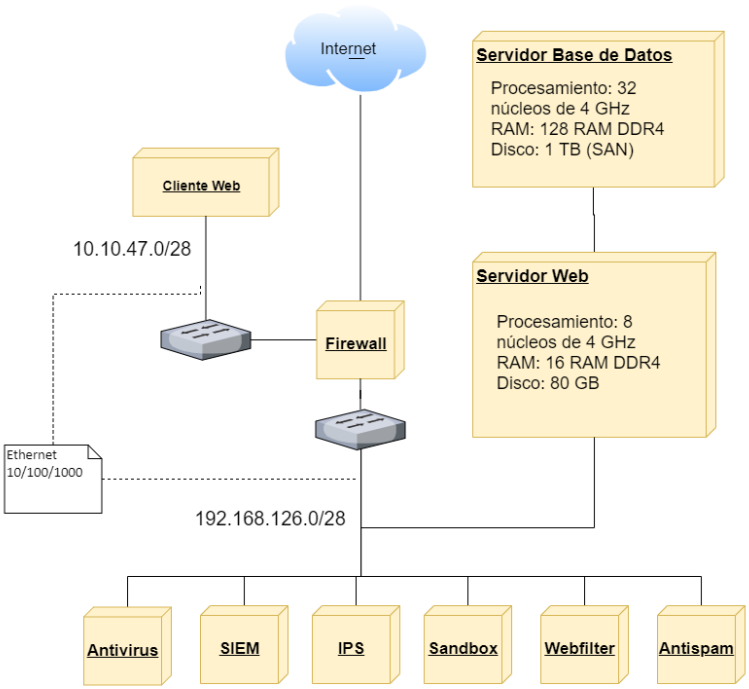

Figura 4. Diagrama de Infraestructura

4. Implementación del Prototipo

Para el desarrollo del prototipo, se utilizaron datos reales de algunos equipos de una compañía con su respectiva criticidad y se realizó un levantamiento del listado de activos, software y versiones necesarios para iniciar el proceso de gestión de vulnerabilidades que se encuentran actualmente implementados en la entidad.

Se escogió el framework Django (Python) puesto que ofrece compatibilidad con aplicaciones de aprendizaje de máquina y módulos para facilitar la comunicación con bases de datos relacionales y autenticación de usuarios, agilizando los tiempos de construcción y el aprendizaje de los desarrolladores.

Las características principales del prototipo son:

- Adquisición y procesamiento de amenazas:
  La aplicación obtiene los mensajes de correo electrónico recibidos de una fuente de amenazas seleccionada, la cual provee la información en formato XML por medio de un archivo en lenguaje STIX (Structured Threat Information eXpression). Los correos adquiridos se procesan para obtener este archivo estándar con la información de las amenazas, en busca de hashes, IPs y dominios. Las amenazas son guardadas en la base de datos e inmediatamente se envían los indicadores de compromiso a los equipos de seguridad correspondientes.

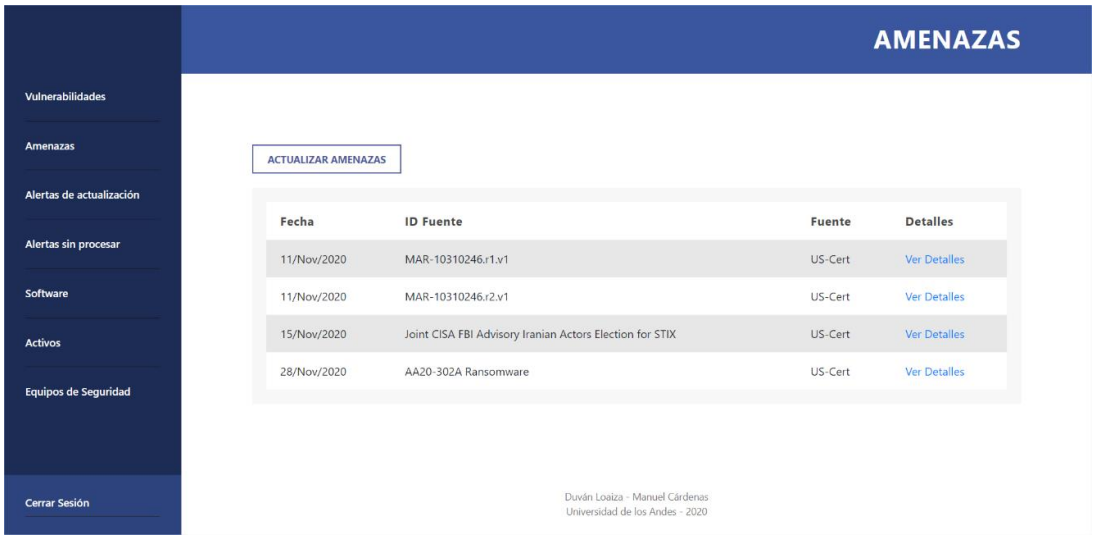

Figura 5. Módulo de Amenazas

- Integración con equipos de seguridad:

    - Envío de dominios a Antispam: Los nombres de dominio son enviados a la herramienta open-source MailCleaner por medio del protocolo HTTP. Una vez ejecutada la solicitud, el listado de dominios puede visualizarse en la interfaz gráfica de la herramienta.
    - Registro de hashes: El sistema almacena los hashes como una cadena estándar en un archivo de texto plano que será leído por el antivirus open-source ClamAV para detectar los archivos maliciosos.
    - Creación de reglas en Firewall: Las direcciones IP maliciosas adquiridas de las alertas de ciberinteligencia son enviadas al Firewall OPNsense para crear reglas de bloqueo de tráfico tanto de entrada como de salida; es decir, por cada IP se generan dos reglas.

- Adquisición de vulnerabilidades:
  Para la adquisición de vulnerabilidades se utiliza una de las fuentes que ofrece la información en formato JSON. A partir de este reporte, la aplicación busca aquellas vulnerabilidades relacionadas con el listado de software y activos cargados en la base de datos. La fuente ofrece un estándar de nombramiento de proveedores, herramientas y versiones, los cuales son cruzados con los registros de la base de datos. Con base en lo anterior, se diseñó un algoritmo para identificar qué software se encuentra afectado por cada vulnerabilidad, y así determinar una priorización. Adicionalmente, permite cambiar el estado de la vulnerabilidad y el usuario asignado.

- Consultas sobre registros del sistema:
  Existen diferentes módulos del sistema que permiten consultar los activos físicos, herramientas de software y equipos de seguridad (y los indicadores de compromiso que estos aceptan) registrados en la base de datos.

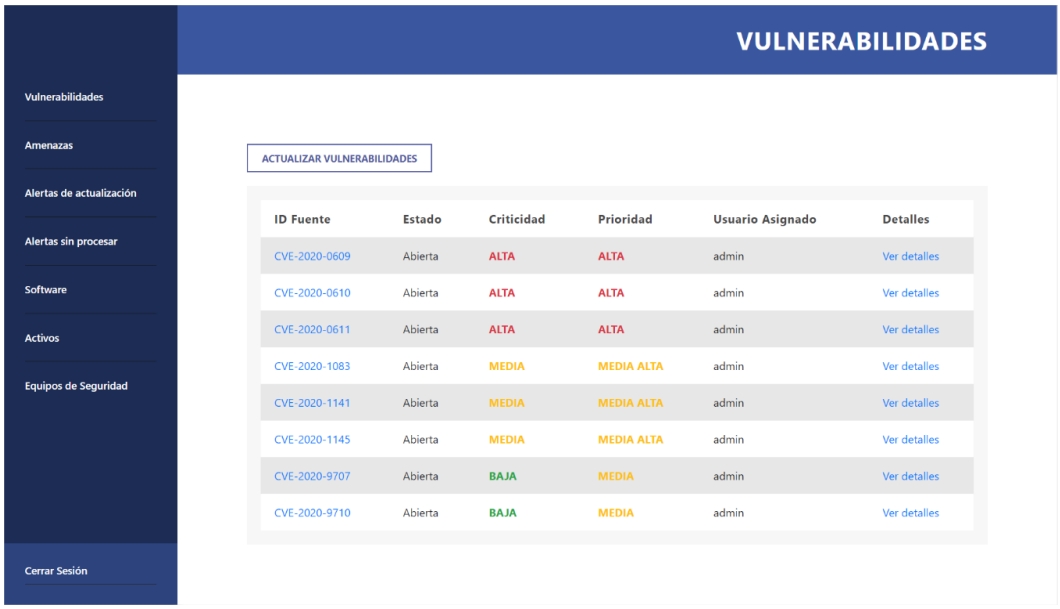

Figura 5. Módulo de Vulnerabilidades

5. Análisis de Resultados

En un primer escenario de análisis, se adquirieron 188 reportes recibidos por la compañía en los últimos meses por medio de correo electrónico para simular la cantidad de alertas recibidas durante un mes y evaluar el tiempo promedio de atención de una alerta y la efectividad de la clasificación. La tabla 1 muestra cómo está conformada la muestra usada para evaluar los resultados.

Tipo de alerta	Cantidad	Porcentaje con respecto a la muestra
Alertas de amenazas procesadas	35	18.62%
Alertas de amenaza no procesadas	13	6.91%
Reportes de actualización de seguridad y alertas de vulnerabilidad	100	53.19%
Recomendaciones de seguridad y otras alertas	40	21.28%

Tabla 1. Muestra para evaluación de resultados – Escenario 1

El procesamiento de esta muestra completa tiene una duración total de 2:28:52. Del total de 48 alertas de amenazas, 35 alertas son correctamente procesadas (72%). 13 de las alertas de amenazas requieren análisis y ejecución de acciones manual (o la implementación de algoritmos más sofisticados para la extracción de indicadores de compromiso).

En promedio, las alertas que realizan bloqueos de IPs tardan 7 minutos en ser procesadas (existe una pequeña demora en los tiempos de respuesta del Firewall); mientras que las alertas de las que se extraen únicamente hashes y dominios tardan en promedio 2 segundos en ser procesadas. Este tiempo ya incluye la integración con los equipos de seguridad; es dependiente de la muestra y de los equipos de seguridad con los cuales está integrado el sistema.

Las demás alertas pueden ser adquiridas directamente de fuentes especializadas por medio de peticiones HTTP, por lo cual su procesamiento se analiza por medio de un segundo escenario: se utiliza como base el reporte de CVE-2019 ofrecido por NIST, el cual contiene todas las vulnerabilidades reportadas durante este año:

Cantidad de vulnerabilidades del reporte	16153
Cantidad de vulnerabilidades identificadas y procesadas por el sistema	1161
Tiempo de procesamiento	0:08:11

Tabla 2. Muestra para evaluación de resultados – Escenario 2

Estos tiempos de procesamiento, si bien no cubren la automatización de todo el proceso de gestión de la vulnerabilidad, permiten la identificación automática de las vulnerabilidades de interés para la compañía, su priorización y la notificación a los encargados. De esta forma, es posible dar inicio al proceso de gestión de la vulnerabilidad.

En estos experimentos, el procesamiento de las vulnerabilidades es menor a 10 minutos. Teniendo en cuenta las dificultades para procesar las alertas de vulnerabilidades recibidas por correo electrónico y los cortos tiempos de procesamiento del segundo escenario, se recomienda realizar la adquisición de este tipo de alertas únicamente a través fuentes especializadas con información estructurada y estandarizada, lo cual conlleva a una mejora en las tasas de clasificación.

6. Conclusiones

El prototipo implementado, teniendo en cuenta el alcance establecido y de acuerdo con los resultados de las pruebas realizadas, permite evidenciar una mejora sustancial de los tiempos de gestión: la extracción de indicadores de compromiso y su correspondiente bloqueo en los equipos de seguridad se realiza en menos de 10 minutos, de forma automática e inmediata. Es decir, el sistema es capaz de gestionar al menos 18 amenazas en el mismo tiempo que un analista se encargaría de gestionar una sola (3 horas).

En el experimento, el 28% de las alertas de amenazas no fueron correctamente procesadas. Con la implementación de algoritmos más sofisticados para la extracción de indicadores sería posible aumentar esta efectividad. Sin embargo, esta cifra señala que el analista podrá dedicar mucho menos tiempo a la gestión manual de amenazas, en comparación con la actividad que realiza actualmente y de esta forma dedicar más tiempo a las tareas que no pueden ser automatizadas y que requieren mayor capacidad de análisis.

La selección de fuentes de vulnerabilidades especializadas, que ofrecen información estructurada y estandarizada, también permite optimizar el procesamiento de las alertas. En el experimento, gracias a los estándares de la fuente, se pudo detectar todas las vulnerabilidades publicadas en el último año, asociadas a las herramientas de software que posee la compañía en un tiempo inferior a 20 minutos. El sistema automáticamente evalúa la criticidad de las vulnerabilidades y asigna una prioridad, lo cual permite dar inicio al proceso de gestión de vulnerabilidades.

El producto de software desarrollado en su totalidad tendría un costo de menos del 50% con respecto al costo que tendría la integración de las tres soluciones de tipo TIP, SOAR y Vulnerability Management, generando aún más valor al abordar el problema directo de la compañía, permitiendo así el desarrollo de características únicas y a la medida de la entidad, como lo es el contexto de la criticidad de activos. Adicionalmente, la implementación de este proyecto evitaría incurrir en los costos de integración entre las diferentes soluciones, y no se requeriría recurso humano adicional para administrar esta solución.

7. Referencias

[1] Crowdstrike, 'GLOBAL THREAT REPORT 2020', 2020 < https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf/>.

[2] Accenture, 'THE COST OF CYBERCRIME', 2019 <https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 />.

[3] Scmagazine, 'Anomali Threat Platform', 2018 < https://www.scmagazine.com/review/anomali-threat-platform-2/>

[4] Trustradius, 'Threat Intelligence Platforms', < https://www.trustradius.com/threat-intelligence-platforms>

[5] Insight, 'Demisto Enterprise - license - 1 full user', <https://www.insight.com/en_US/shop/product/PANDEMISTOFULLUSER/Palo%20Alto%20Networks/PAN-DEMISTO-FULL-USER-ENT/DemistoEnterprise-license-/>

[6] Businesswire, 'Demisto Optimizes Incident Response with Industry's First Threat Intelligence Integrated Comprehensive Incident Management Platform', <https://www.businesswire.com/news/home/20170209005446/en/Demisto-Optimizes-Incident-Response-with-Industry%E2%80%99s-First-Threat-Intelligence-Integrated-Comprehensive-Incident-Management-Platform>

[7] Rapid7, 'Pricing', 2020 < https://www.rapid7.com/pricing//>.

[8] Itcentralstation, 'Tenable SC Reviews', 2019 < https://www.itcentralstation.com/products/tenable-sc-reviews#pricing/>.