**Historias de Usuario (HU)**

A continuación, se presenta las HU del proyecto, tanto las incluidas como las descartadas.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID HU** | **Rol ¿Quien?** | **Característica Funcionalidad Objetivo ¿Quiero?** | **Razón Resultado ¿Para qué?** | **Prioridad** | **Pts Hist HU** | **# Sprint** |
|  | - |  |  |  |  |  |
| HU-PA01 | Como operador | Quiero visualizar alertas en caso de que ocurra una anomalía en la red. | Para tener una visualización rápida de las anomalías. | M | 8 | 1 |
|  | - |  |  |  |  |  |
| HU-PA02 | Como operador | Quiero recibir un correo electrónico en el cual se indique el incidente informático. | Para en caso de no estar en las dependencias, saber que incidente esta ocurriendo. | S | 13 | 2 |
|  | - |  |  |  |  |  |
| HU-PA03 | Como Mantenedor | Quiero generar y visualizar ataques en la sistema de correlación de eventos. | Para poder discriminar entre un incidente y un falso positivo. | M | 13 | 3 |
|  | - |  |  |  |  |  |
| HU-PA04 | Como operador | Quiero poder visualizar el estado de los dispositivos conectados a la red. | Para poder determinar que dispositivo se encuentra con problemas.  **HU Descartada del proyecto.** | M | 13 | 9 |
|  | - |  |  |  |  |  |
| HU-PA05 | Como administrador | Quiero poder integrar de forma correcta el modulo de detección de patrones de comportamiento con el actual sistema de correlación de eventos. | Para poder detectar y mostrar lo desconocido en la red a los encargados. | M | 13 | 5 |
|  | - |  |  |  |  |  |
| HU-PA06 | Como administrador | Quiero poder implementar dicho sistema y que sea escalable, en el sentido de que se puedan agregar mas dispositivos. | Para poder tener una mejor visualización del estado de la red. | M | 13 | 1 |
|  | - |  |  |  |  |  |
| HU-PA07 | Como administrador | Quiero implementar un modulo que logre detectar patrones anómalos de comportamiento dentro de una red corporativa. | Para entregar una mejor visualización a los encargados de Seguridad TI. | M | 26 | 5 |
|  | - |  |  |  |  |  |
| HU-PA08 | Como administrador | Quiero crear reglas de detección de patrones anómalos de comportamiento. | Para poder detectar comportamientos anómalos en la red.  **HU Descartada del proyecto.** | M | 13 | 6 |
| HU-PA09 | Como administrador | Quiero implementar un sitio web en donde se de a conocer el trabajo en Ciberdefensa y tenga la capacidad de generar una autoevaluación a las Pymes. | Para poder detectar el estado actual de la red de una Pyme. | M | 20 | 4 |
| HU-PA10 | Como Mantenedor | Quiero poder extraer todos los Dataset de los ataques ejecutados sobre el sistema a prueba. | Para tener una visualización certera de que efectivamente es lo que se esta realizando sobre la red. | M | 13 | 6 |
| HU-PA11 | Como Mantenedor | Quiero poder categorizar de forma correcta los ataques ejecutados sobre la red a través del módulo Snort de pfSense en conjunto con el correlacionador de eventos. | Para no tener falsos positivos, ni errores de interpretación en gestión y ejecución de medidas de mitigación adoptadas. | M | 13 | 7 |

**Tabla 1: Historias de usuario**

**Criterios de Aceptación (CA)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Número de escenario** | **Criterio de aceptación (Título)** | **Contexto** | **Evento** | **Resultado / Comportamiento esperado** | **Estado** |
| E1 | HU-PA01.T3.E1 - Visualización correcta. | Estando dentro del sistema debo poder visualizar distintos eventos. | Al seleccionar el menú "Search". | Visualizar diferentes eventos de red. | 100 % |
| E2 | HU-PA01.T3.E2 - Evento parseado correctamente. | Al seleccionar un evento, se debe corroborar que ese log sea del origen de datos que dice ser. | Al desplegarse un evento, luego de hacer clic sobre este. | Que el log parseado efectivamente sea del origen de datos que dice ser. | 100 % |
| E3 | HU-PA01.T3.E3 - Evento erróneo. | Al seleccionar un evento, este no muestre nada, solo basura. | Al intentar desplegar un evento, este no muestre nada. | Que efectivamente no se despliegue el menú hacia abajo. | 100 % |
| E1 | HU-PA02.T3.E1 - Evento gatillado correctamente en el panel de alertas. | Dentro del sistema debo poder visualizar el evento gatillado. | Al seleccionar y hacer clic en "Test" dentro de alarmas. | Visualizar alerta gatillada en pantalla. | 100 % |
| E2 | HU-PA02.T3.E2 - Plantilla de correo creada correctamente (JMTE). | Al seleccionar en "Notification" debo visualizar la plantilla JMTE y las configuraciones de envío. | Al seleccionar y hacer clic en "More actions / Edit" dentro de Notifications. | Visualizar configuración de envío y plantilla JMTE. | 100 % |
| E3 | HU-PA02.T3.E3 - Alerta enviada por correo electrónico. | Al seleccionar en el menú superior "Alerts" / "Notifications". | Al seleccionar y hacer clic en "Test" dentro del menú "Alerts" / "Notifications". | Visualizar correo electrónico con alerta enviada desde correlacionador de eventos. | 100 % |
| E1 | HU-PA03.T2.E1 - Parseo generado correctamente desde FW pfSense. | Dentro del sistema debo poder visualizar el evento detectado por Snort. | Al seleccionar y hacer clic en Event, dentro de pfSense. | Visualizar evento gatillado en pantalla. | 100 % |
| E2 | HU-PA03.T2.E2 - Ataque generado desde plataforma Mutillidae | Al seleccionar ingresar a plataforma Mutillidae y seleccionar tipo de ataque. | Al seleccionar y hacer clic en Menú izquierdo Owasp 2017. | Visualizar el envío del ataque. | 100 % |
| E3 | HU-PA03.T2.E3 - Dashboard con detalle de anomalías en la red. | Al seleccionar en el menú superior "Search", filtrar por message o clasificación. | Al seleccionar y hacer clic en message y luego quick value. | Visualizar Dashboard tipo torta y tabla con detalle de incidente. | 100 % |
| E1 | HU-PA05.T3.E1 - Integración exitosa entre modulo y correlacionador. | Cuando el modulo de detección de patrones envíe datos hacia el sistema. | Posterior al ingreso del modulo como "input" al sistema. | Que el sistema muestre como input valido al modulo de detección. | 100 % |
| E2 | HU-PA05.T3.E2 - Datos del modulo visualizados en forma correcta en correlacionador de eventos. | Cuando lo logs lleguen al correlacionador de eventos y este permita el ingreso y visualización de los datos. | Al seleccionar el modulo (input) y hacer clic en "View message". | Logs del modulo sean visualizados con su respectiva categorización. | 100 % |
| E3 | HU-PA05.T3.E3 - Datos del modulo de detección no visualizados en sistema. | Cuando los logs sean enviados desde el modulo, pero no sean visualizados en el sistema. | Al seleccionar el modulo (input) y hacer clic en "View message". | Logs del modulo no sean visualizados con su respectiva categorización. | 100 % |
| E1 | HU-PA06.T3.E1 - Ingreso exitoso. | Cuando usuario y contraseña coincidan con las registradas en sistema. | Posterior al ingresar usuario y contraseña y dar enter. | El usuario hará ingreso al sistema. | 100 % |
| E2 | HU-PA06.T3.E2 - Origen de datos ingresado correctamente. | Cuando el mantenedor ingrese un origen da datos nuevo al sistema. | Al hacer clic en guardar los cambios. | El origen de datos debiera mostrar el estado en "running". | 100 % |
| E3 | HU-PA06.T3.E3 - Origen de datos erróneamente ingresado. | Cuando el mantenedor ingrese un origen da datos nuevo al sistema. | Al hacer clic en guardar los cambios. | El sistema debe mostrar un ventana con la alerta y motivo, del porque no se ingreso el origen de datos. | 100 % |
| E1 | HU-PA07.T3.E1 - Detección exitosa | Cuando el log y el código coincidan con los parámetros programados. | Al ejecutar o hacer correr el modulo. | El modulo debe mostrar detección de comportamiento anómalo. | 100 % |
| E2 | HU-PA07.T3.E2 - Logs sin categorización | Cuando el log y el código no coincidan con los parámetros programados. | Al ejecutar o hacer correr el modulo. | El log no será categorizado como un tipo de anomalía. | 100 % |
| E3 | HU-PA07.T3.E3 - Erróneamente categorizado | Cuando el log y el código coincidan con los parámetros programados, pero esta detección no sea la correcta. | Al ejecutar o hacer correr el modulo. | El log quedara erróneamente categorizado. | 100 % |
| E1 | HU-PA09.T5.E1 - Sitio web generado correctamente en servidores de Universidad. | Dentro del sitio web, debo poder visualizar los distintos módulos que componen este sitio. | Al ingresar a url http://ciberdefensa.informatica-unab-vm.cl. | Visualizar sitio web. | 100 % |
| E2 | HU-PA09.T5.E2 - Formulario de preguntas generado en forma correcta. | Dentro del sitio web en "Autoevaluación" debo visualizar la plantilla en donde se realicen las distintas preguntas. | Al seleccionar y hacer clic en "Autoevaluación" dentro del menú superior del sitio web. | Visualizar configuración de envío y plantilla JMTE. | 100 % |
| E3 | HU-PA09.T5.E3 - Resultados de autoevaluación deben ser enviados vía correo electrónico. | Terminando de responder todas las preguntas del formulario. | Al seleccionar y hacer clic en "Submit". | Visualizar correo electrónico con detalles de preguntas y respuestas en direcciones de email especificadas. | 100 % |
| E1 | HU-PA10.T3.E1 - Generación de Dataset creado y guardado de manera correcta en Modulo | Dentro del sistema debo poder efectuar un ataque hacia una maquina victima y el Modulo debe detectar este ataque. | Al seleccionar y hacer clic en "Run" de la herramienta atacante. | Visualizar Dataset carpeta del Modulo. | 100 % |
| E2 | HU-PA10.T3.E2 - Dataset debe contener los parámetros del Ataque efectuado. | Al abrir el Dataset este debe contener los datos del ataque efectuado. | Al seleccionar y hacer doble clic sobre Dataset. | Visualizar datos el interior del Dataset. | 100 % |
| E3 | HU-PA10.T3.E3 - Dataset debe poder ser rescatado desde ubicación en donde fue creado. | Al traspasar estos Dataset de un lugar a otro, estos debe poder transferirse. | Al seleccionar y copiar Dataset desde ubicación original a otra. | Visualizar Dataset en otro lugar que no sea la ubicación original. | 100 % |

**Tabla 2: Criterios de aceptación**