ESPE ESPE-CERT

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

"INSTALACIÓN DEL SERVICIO DE MONITOREO DE AMENAZAS MEDIANTE UN CORRELACIONADOR DE EVENTOS (SIEM) EN EL ESPE CERT UTILIZANDO ITIL V4"

AUTOR: MEZA NAVARRETE BRYAN ESTEBAN

CRUZ GUACHILEMA EDUARDO ANTONIO

DIRECTOR: ING. RON EGAS MARIO BERNABÉ MSC.

SANGOLQUÍ

2023

CONTENIDOS

01	INTRODUCCIÓN	• Problemática • Objetivos
02	FUNDAMENTACIÓN TEÓRICA	• SIEM • ITIL V4
03	FASE I	• Plan • Diseño y Transición
04	FASE II	• Entrega y Soporte • Mejora
05	FINALIZACIÓN	• Conclusiones • Recomendaciones

INTRODUCCIÓN

PROBLEMÁTICA

En la actualidad y con los avances tecnológicos, las amenazas de seguridad aumentan constantemente.

Dispositivos de control parcial o semiautomático para el monitoreo de amenazas, ya que estas dificultan las tareas de reacción oportuna y eficaz respuesta ante incidentes informáticos de SGSI.

Se identificó que en el área del ESPE-CERT, hace falta una herramienta que realice la recolección de eventos y permita brindar una respuesta eficaz a los incidentes de seguridad.

OBJETIVOS

Objetivo General

- Implantar el Servicio de monitoreo de amenazas mediante un correlacionador de eventos (SIEM) en el ESPE CERT utilizando ITIL V4, para la Universidad de las Fuerzas Armadas ESPE, para estar en capacidad de ampliar el servicio a otras universidades.

Objetivos Específicos

Fundamentación teórica	 Establecer el estado del arte

Fase 1

Establecer el Plan

Realizar el Diseño y la Transición

Fase 2

Realizar la Entrega y el Soporte

Plantear la Mejora

FUNDAMENTACIÓN TEÓRICA

SIEM

Plataforma central de los centros de operaciones de seguridad modernos, recopila eventos de múltiples sensores.

Correlacionan eventos y brindan vistas sintéticas de las alertas para el manejo de amenazas.

Agrega, normaliza y correlaciona varios eventos de seguridad generados por una infraestructura.

Surgen de la unión de tecnologías SIM y SEM.

Componentes de un SIEM

- **Capa de recolección:**
  - Recolecta los eventos generados
- **Capa de normalización:**
  - Estandariza los eventos que son recolectados
- **Capa de correlación**:
  - Identifica patrones en común
- **Capa de reporte:**
  - Analiza los resultados generados y genera distintos informes sobre los eventos que ocurren en los dispositivos de red.

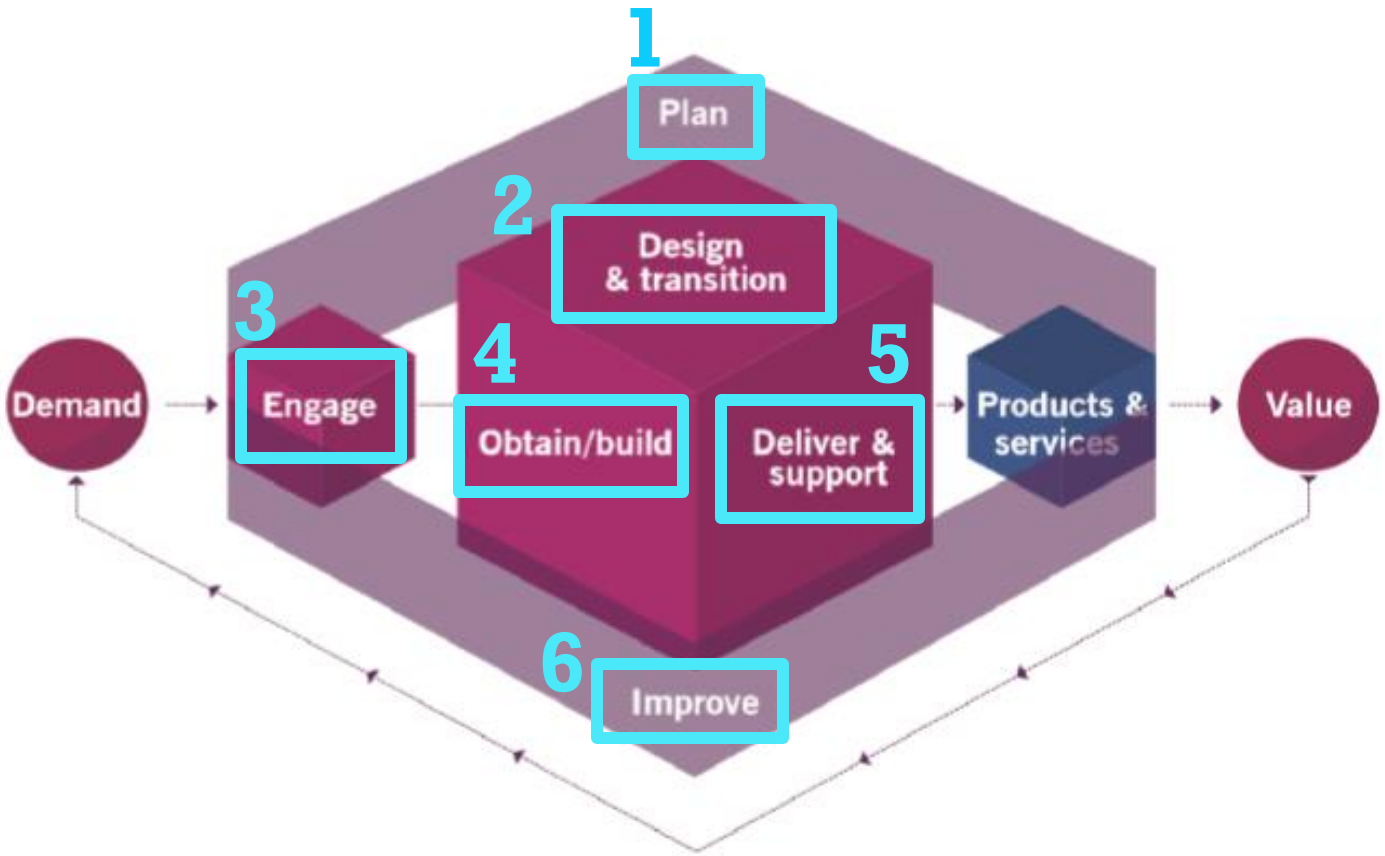
Selección del SIEM

Característica	Wazuh	OSSIM	OSSEC	Elastik stack
Open Source	Si	Si	Si	Si
Almacenamiento y procesamiento de logs	Si	No	Si	Si
Se puede instalar en un SO	Si	No	Si	Si
Transferencia segura de datos	Si	Si	Si	Si
Monitoreo de amenazas	Si	Si	Si	Si
Visualización en base a criterios como días, semanas, meses, etc.	Si	Si	No	Si
Gestión de incidentes	Si	Si	Si	Si
Análisis de vulnerabilidades	Si	Si	Si	Si
Alertas de intrusión	Si	Si	Si	Si
Soporte y documentación	Si	Si	Si	Si
Sitio web de comunidad activa	Si	Si	Si	No
Puntaje	**11**	**9**	**10**	**10**

SIEM seleccionado

ITIL V4

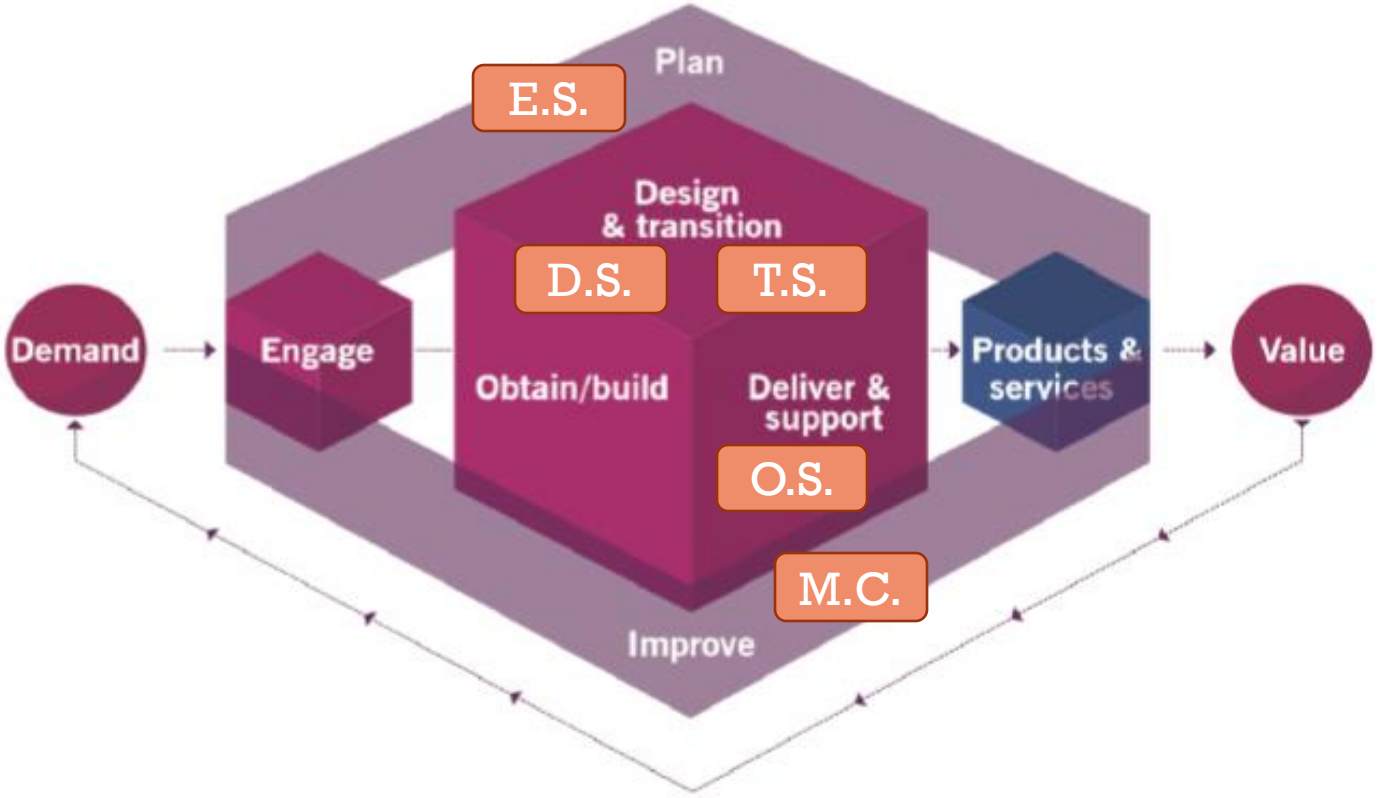
Cadena de Valor de Servicio



1	Asegurar un entendimiento
2	Cumplir: calidad, costos, tiempos
3	Comprender las necesidades
4	Disponibilidad
5	Garantizar entrega y soporte
6	Mejora continua

ITIL V3 en comparación a ITIL V4

ITIL V3 (Ciclo de Vida)	ITIL V4 (Cadena de Valor de Servicio)
Estrategia del Servicio (E.S.)	Plan
Diseño del Servicio (D.S.)	Diseño y Transición
Transición del Servicio (T.S.)	
Operación del Servicio (O.S.)	Entrega y Soporte
Mejora Continua (M.C.)	Mejora



FASE I

ACTIVIDAD: PLAN

Gestión del portafolio de servicios

Ord.	Servicio	Estado Actual	Definición
1	Gestión de incidentes	En implementación	Restablecer los servicios lo más pronto posible para minimizar el daño que pueda tener la institución.
2	Análisis de vulnerabilidades	Implementado	Se generan informes donde se identifican, clasifican y priorizan las debilidades o fallos de seguridad.
3	Monitoreo y alerta de primer nivel	Implementado	Servicio de monitoreo que indica cuando un evento puede producirse y afectar al equipo.
4	Asesoramiento técnico y consultoría	En implementación	Ayuda a resolver procesos relacionados con los aspectos técnicos de las TIC.
5	Firma electrónica	Implementado	Garantizar la autenticidad, integridad y confidencialidad de los documentos en Internet.
6	Hacking ético	En implementación	Servicio para realizar intrusiones de manera controlada sobre un sistema informático.

ACTIVIDAD: DISEÑO

Gestión de la continuidad del servicio

Recuperar los servicios críticos en un plazo de entre 24 y 72 horas.

Se cuenta con un UPS activo.

Se debe reiniciar el servicio por medio de comandos o en el peor de los casos, reinstalarlo mediante la guía de instalación.

Gestión del catálogo de servicios

1. Monitoreo de amenazas
2. Gestión de incidentes
3. Alertas de intrusión
4. Análisis de vulnerabilidades
5. Recopilación de Logs

Gestión de los niveles de servicio

El servicio tendrá un SLA del 95%.

Fuera de servicio:

- Diariamente: 1 hora 12 minutos
- Semanalmente: 8 horas 24 minutos
- Mensualmente: 1 día 12 horas
- Anualmente: 18 días 6 horas

Gestión de la capacidad y rendimiento

Recursos tecnológicos:

Servidor CentOS

Disco utilizado 45 Gb

RAM 80%

Procesador 15 – 25%.

ACTIVIDAD: TRANSICIÓN

Gestión de lanzamiento

Objetivos

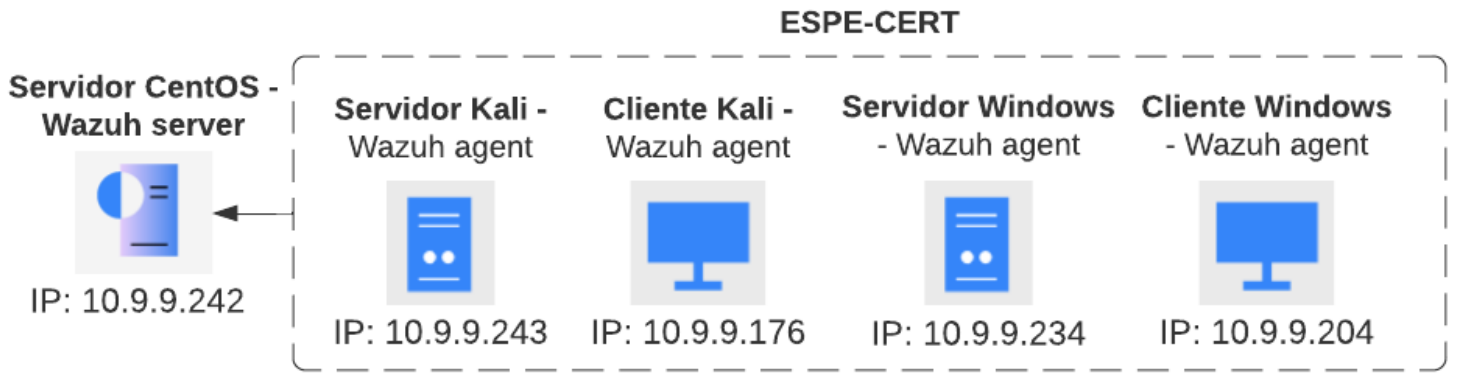
- Preparar el servidor para la implantación del nuevo servicio
- Implantación del nuevo servicio
- Enrolar los sensores al SIEM.
- Monitorear los eventos de seguridad

Tareas a realizar

- Preparación del servidor para la instalación
- Instalación del SIEM en el servidor del ESPE-CERT
- Instalación de software necesario en los sensores del ESPE-CERT
- Evaluación del nuevo servicio

Alcance

Plazo aproximado de 2 semanas desde el comienzo de la transición para encontrarse en operación y poder brindar servicio al ESPE-CERT.



INSTALACIÓN DE WAZUH (SERVIDOR)

Ejecución del lanzamiento

1

```
root@espe-cert-server1:/home/espe-cert/SIEM
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@espe-cert-server1 SIEM]# ls -l
total 0
[root@espe-cert-server1 SIEM]# curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh
[root@espe-cert-server1 SIEM]# ls -l
total 148
-rw-r--r--. 1 root root 148555 ene 10 21:25 wazuh-install.sh
[root@espe-cert-server1 SIEM]# curl -sO https://packages.wazuh.com/4.3/config.yml
[root@espe-cert-server1 SIEM]# ls -l
total 152
-rw-r--r--. 1 root root    622 ene 10 21:27 config.yml
-rw-r--r--. 1 root root 148555 ene 10 21:25 wazuh-install.sh
```

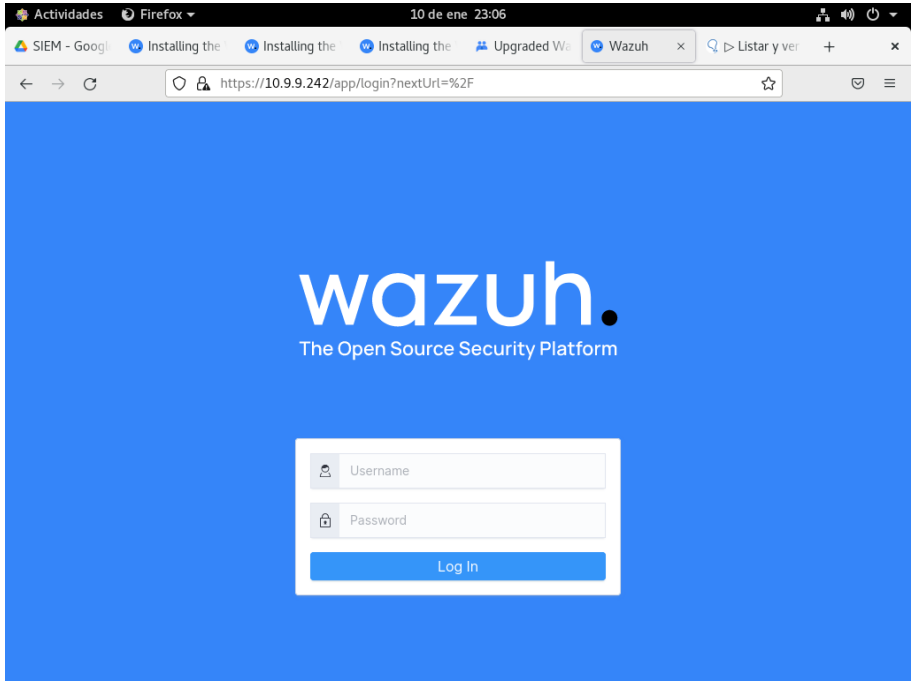
2

```
root@espe-cert-server1:/home/espe-cert/SIEM
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: cert-node-1
      ip: 10.9.9.242
    #- name: node-2
    #  ip: <indexer-node-ip>
    #- name: node-3
    #  ip: <indexer-node-ip>

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: cert-wazuh-1
      ip: 10.9.9.242
    #  node_type: master
    #- name: wazuh-2
    #  ip: <wazuh-manager-ip>
    #  node_type: worker
    #- name: wazuh-3
    #  ip: <wazuh-manager-ip>
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: cert-dashboard
      ip: 10.9.9.242
~
```

3

```
root@espe-cert-server1:/home/espe-cert/SIEM
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@espe-cert-server1 SIEM]# bash wazuh-install.sh --generate-config-files
10/01/2023 21:34:54 INFO: Starting Wazuh installation assistant. Wazuh version: 4.3.10
10/01/2023 21:34:54 INFO: Verbose logging redirected to /var/log/wazuh-install.log
10/01/2023 21:35:08 INFO: --- Configuration files ---
10/01/2023 21:35:08 INFO: Generating configuration files.
10/01/2023 21:35:09 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certifi
cates, and passwords necessary for installation.
[root@espe-cert-server1 SIEM]# ls -l
total 160
-rw-------. 1 root root  10570 ene 10 21:35 wazuh-install-files.tar
```

4



INSTALACIÓN DE WAZUH (AGENTE)

Ejecución del lanzamiento

1

Administrador: Windows PowerShell

```
PS C:\Users\ESPE\Documents> cd .\SIEM\
PS C:\Users\ESPE\Documents\SIEM> dir


    Directorio: C:\Users\ESPE\Documents\SIEM


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         13/1/2023     11:01                Windows
-a----         13/1/2023     10:58        5885952 wazuh-agent-4.3.10-1.msi


PS C:\Users\ESPE\Documents\SIEM> .\wazuh-agent-4.3.10-1.msi /q WAZUH_MANAGER="10.9.9.242"
```

2

```
PS C:\Users\ESPE\Documents\SIEM> NET START WazuhSvc
El servicio de Wazuh está iniciándose.
El servicio de Wazuh se ha iniciado correctamente.
```

3

Administrador: Windows PowerShell

```
PS C:\Users\ESPE\Documents\SIEM> function Ignore-SelfSignedCerts {
>>     add-type @"
>>         using System.Net;
>>         using System.Security.Cryptography.X509Certificates;
>>         public class PolicyCert : ICertificatePolicy {
>>             public PolicyCert() {}
>>             public bool CheckValidationResult(
>>                 ServicePoint sPoint, X509Certificate cert,
>>                 WebRequest wRequest, int certProb) {
>>                 return true;
>>             }
>>         }
>> "@
>>     [System.Net.ServicePointManager]::CertificatePolicy = new-object PolicyCert
>>     [System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12;
>> }
PS C:\Users\ESPE\Documents\SIEM>
PS C:\Users\ESPE\Documents\SIEM> Ignore-SelfSignedCerts
```

4

Administrador: Windows PowerShell

```
PS C:\Users\ESPE\Documents\SIEM> $base64AuthInfo=[Convert]::ToBase64String([Text.Encoding]::ASCII.GetBytes(("{0}:{1}" -f
 "wazuh-wui", "w0w[redacted]")))
PS C:\Users\ESPE\Documents\SIEM>
```

5

Administrador: Windows PowerShell

```
PS C:\Users\ESPE\Documents\SIEM> Invoke-WebRequest -UseBasicParsing -Headers @{Authorization=("Basic {0}" -f $base64Auth
Info)} -Method GET -Uri https://10.9.9.242:55000/security/user/authenticate | Select-Object -Expand Content
{"data": {"token": "eyJhbGciOiJFUzUxMiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJ3YXp1aCIsImF1ZCI6IldhenVoIEFQSSBSRVNUIiwibmJmIjoxNjc
zNjQ2MDIwLCJleHAiOjE2NzM2NDY5MjAsInN1YiI6IndhenVoLXd1aSIsInJ1b19hcyI6ZmFsc2UsInJiYWNfcm9sZXMiOlsxXSwicmJhY19tb2RlIjoid2h
pdGUifQ.AU1OT5Bo8GoFx2WA8O-jTFrCp7ZD_oE-VipYa2ZwqH2uJCFtgbapbM2VZkXq3C_frK8zKXIafWF7zZhorD99H3knACKWv46gQyxT0DiIhCcnnQ_b
xsmFrApIBZBJgnVK6KIupN8FgDKeeh9yZo8kJ86XCxro6259V9cV8YBlUCKFCLqB"}, "error": 0}
PS C:\Users\ESPE\Documents\SIEM>
```

6

Administrador: Windows PowerShell

```
PS C:\Users\ESPE\Documents\SIEM> Invoke-WebRequest -UseBasicParsing -Headers @{Authorization=("Bearer {0}" -f $TOKEN)} -
Method POST -ContentType "application/json" -Uri https://10.9.9.242:55000/agents -Body $AgentName


StatusCode        : 200
StatusDescription : OK
Content           : {"data": {"id": "004", "key": "MDA0IGN1cnQtd2luLWNsaWVudC0wMSBhbnkgMmQ5Y2Y1ODI0YzZiMjNkZjc1YmNlNTA0M
jg5MTc0Mzc4ZmE1NTdkYWNkNGEyZDU2N2I3Y2UyMzF1NTZkOTFkOQ=="}, "error": 0}
RawContent        : HTTP/1.1 200 OK
                    Strict-Transport-Security: max-age=63072000; includeSubdomains
                    X-Frame-Options: DENY
                    X-XSS-Protection: 1; mode=block
                    X-Content-Type-Options: nosniff
                    Content-Security-Policy: none...
Forms             :
Headers           : {[Strict-Transport-Security, max-age=63072000; includeSubdomains], [X-Frame-Options, DENY], [X-XSS-P
rotection, 1; mode=block], [X-Content-Type-Options, nosniff]...}
Images            : {}
InputFields       : {}
Links             : {}
ParsedHtml        :
RawContentLength  : 170
```

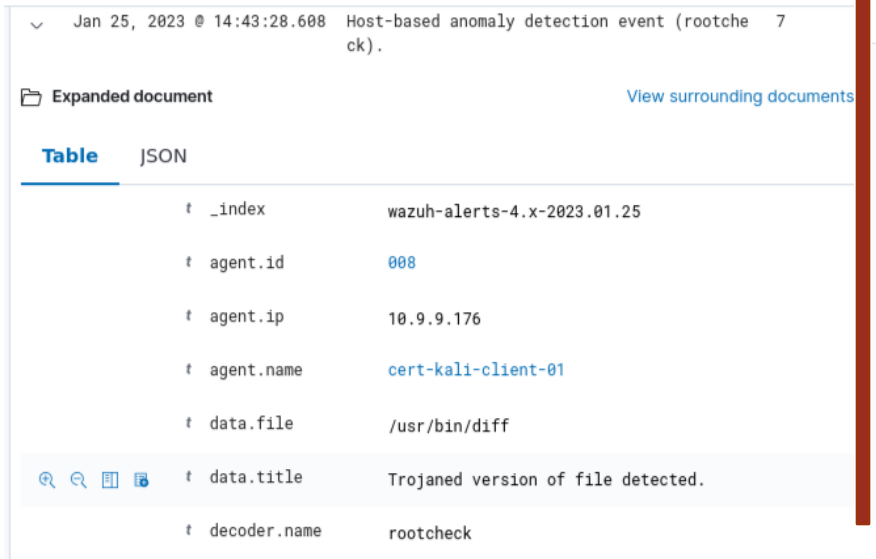
FASE II

ACTIVIDAD: ENTREGA Y SOPORTE

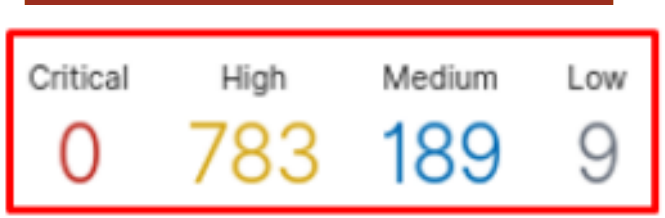
Registro de incidentes

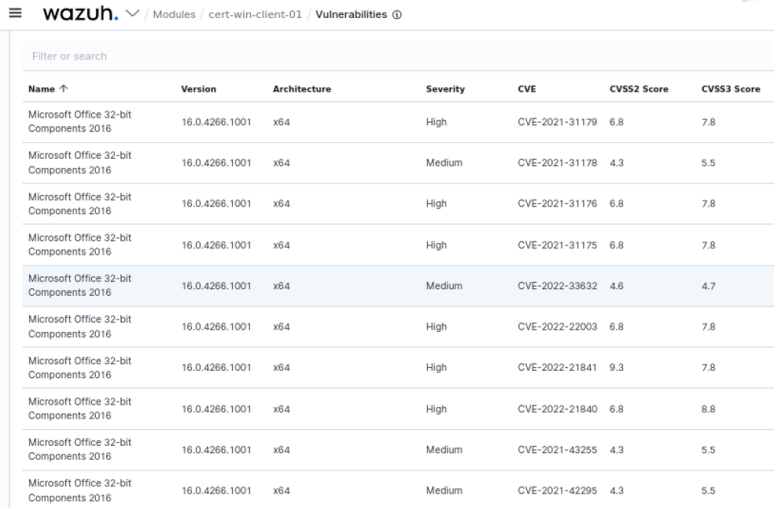
Host-based anomaly detection event (rootcheck)

Detección de una versión troyana del archivo, lo cual nos indica que el archivo especificado, podría ser un virus troyano.

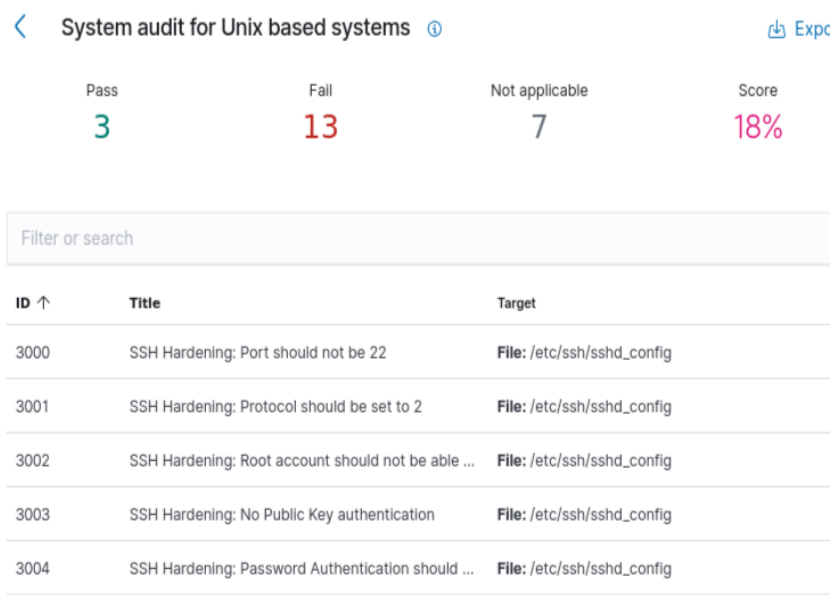


Detección de vulnerabilidades





Evaluación de configuración de seguridad



ACTIVIDAD: ENTREGA Y SOPORTE

Servicio de Validación y Pruebas

Plan de investigación de campo

Instrumento de investigación de campo:

Guía de Observación

Elaboración de guía de observación en base a preguntas planteadas.

Evaluación técnica del servicio

Resultado de responder las preguntas básicas planteadas en la guía de observación:

¿Se están mostrando correctamente cada uno de los incidentes registrados?

¿Se logró recopilar las distintas alertas y encontrar una solución?

Informe de auditoría

Observaciones y Recomendaciones referentes a:

Funcionalidad de servicio

Procedimiento de instalación

- Mejora y creación de reglas

MEJORA

ACTIVIDAD: MEJORA

Objetivo General

Tomar las acciones necesarias en base a las recomendaciones emitidas en el informe de auditoría mediante una capacitación más profunda sobre Wazuh y la instalación de agentes adicionales para mejorar el funcionamiento del servicio y hacer uso de todas sus capacidades.

Al momento de realizar la instalación

wazuh.

Un uso más a profundidad de la herramienta SIEM Wazuh

Mejora y creación de reglas en Wazuh

Acciones a realizar

Ord.	Criterio	Descripción
1	Uso de funcionalidades adicionales	Realizar una capacitación sobre el uso de las funcionalidades que no están siendo usadas de Wazuh.
2	Uso de funcionalidades adicionales	Replicar lo aprendido en los agentes que se encuentran actualmente siendo monitoreados por Wazuh.
3	Mejora o agregación de reglas	Realizar una capacitación sobre el funcionamiento de las reglas de correlación en Wazuh.
4	Mejora o agregación de reglas	Realizar un análisis de las reglas de correlación actuales y verificar si es necesario modificarlas.

Acciones a realizar

Ord.	Criterio	Descripción
5	Mejora o agregación de reglas	Considerar si es necesario plantear y agregar nuevas reglas para obtener reportes más específicos.
6	Agregación de nuevos agentes	Realizar una planificación sobre en qué áreas se podrían localizar nuevos agentes para ser monitoreados.
7	Agregación de nuevos agentes	Verificar que exista conectividad entre el servidor Wazuh y los nuevos sensores.
8	Agregación de nuevos agentes	Verificar en el dashboard que los agentes se hayan enrolado correctamente y realizar las configuraciones necesarias.

FINALIZACIÓN

CONCLUSIONES

- El servicio de monitoreo de amenazas mediante un SIEM se implementó satisfactoriamente en el ESPE-CERT, utilizando el marco de trabajo de ITIL V4 para una gestión eficiente del servicio. Se analizó la situación actual de los servicios y la infraestructura tecnológica disponible, y se siguieron las actividades de plan, diseño y transición, entrega y soporte y mejora para agregar el nuevo servicio al portafolio del ESPE-CERT.

- Se realizaron búsquedas de estudios primarios relacionados con la problemática del trabajo de titulación para comprender mejor el funcionamiento del correlacionador de eventos (SIEM) y los beneficios que puede traer a la institución. Estos estudios fueron útiles para las actividades de plan y diseño del servicio de monitoreo de amenazas.

CONCLUSIONES

- La actividad de diseño y transición permitió una implementación exitosa del SIEM en el servidor designado gracias una clara definición de objetivos, alcance y fechas para realizar cada tarea. La implantación no tuvo inconvenientes debido a la buena conectividad entre equipos y el acceso a Internet.

- Durante la entrega y soporte del servicio, se llevaron a cabo varias pruebas utilizando las herramientas del SIEM Wazuh, las cuales son: evaluación de la configuración de seguridad; eventos de seguridad; alertas y alarmas y la generación de informes y comunicados. Para procesar toda esta información, se utilizó una guía de observación como instrumento de investigación.

RECOMENDACIONES

Se recomienda extender el servicio de monitoreo a otras áreas de la universidad que cuenten con una serie de equipos que ejecuten procesos críticos de la institución y solo en el área del ESPE-CERT.

Wazuh cuenta con varias funcionalidades, de las cuales no pudieron ser explotadas en su totalidad debido a la falta de experiencia y conocimientos en algunos apartados. Por lo que, se recomienda coordinar cursos de capacitación, estos pueden realizarse de manera individual por el área del ESPE-CERT o en cooperación junto con las UTIC.

¡MUCHAS GRACIAS POR SU ATENCIÓN!

Bryan Esteban Meza Navarrete
bemeza@espe.edu.ec

Eduardo Antonio Cruz Guachilema
eacruz8@espe.edu.ec