INFORME MENSUAL SOCaaS **ID de Documento: 20240902-000000**

CORTE DE SUPREMA DE JUSTICIA

MOTIVO	**INFORME MENSUAL DE SERVICIO SOCaaS CORRESPONDIENTE AL MES DE AGOSTO DE 2024**

CONTACTO	FECHA DE EMISION	ANALISTA RESPONSABLE
Luis Ruiz Diaz SOCaaS@pj.gov.py CORTE SUPREMA DE JUSTICIA	02/sep/2024	Eduardo Lagrave eduardo-lagrave@sekiura.com.py SEKIURA

RESUMEN EJECUTIVO

El propósito del presente documento es presentar un resumen de las actividades realizadas en el marco de la provisión del Servicio SOCaaS para CORTE SUPREMA DE JUSTICIA.

Para el funcionamiento del presente Servicio SOCaaS se ha instalado e implementado una Infraestructura Tecnológica que da soporte a los componentes tecnológicos necesarios.

Este informe incluye un descriptivo y visual del compendio de detecciones relevantes y no-relevantes, que han ocurrido durante el periodo Agosto de 2024 del presente servicio.

Es importante mencionar que es la primera vez que CORTE SUPREMA DE JUSTICIA utiliza este tipo de servicios y también es la primera vez que recibe este tipo de informe, por lo que está previsto ampliar aún más el contenido del presente informe en la medida que se avance con la adopción e incorporación del Servicio SOCaaS en la totalidad del parque de equipos a monitorear de CORTE SUPREMA DE JUSTICIA.

Adicionalmente se acompaña recomendaciones de acción que con el acompañamiento de SEKIURA, CORTE SUPREMA DE JUSTICIA deberá planificar y concretar para elevar y fortalecer su Postura de Ciberseguridad de su parque de equipos.

CONFIDE

Luis Ruiz Diaz
Recibido 02/sep/2024

CORPORATION SEKIURA S.A.C.E.I. RUC: 80070880-0

INDICE

1. Infraestructura Tecnológica Desplegada 3
2. Parque de Equipos Registrados en el SIEM Wazuh 4
3. Informe Técnico 5
4. Actividad realizada en conjunto 9
5. Evolución Mensual del Servicio 10
6. Recomendaciones 11

CONFIDENCIAL

CORPORATION SEKIURA S.A.C.E.I. RUC N°80070889-0

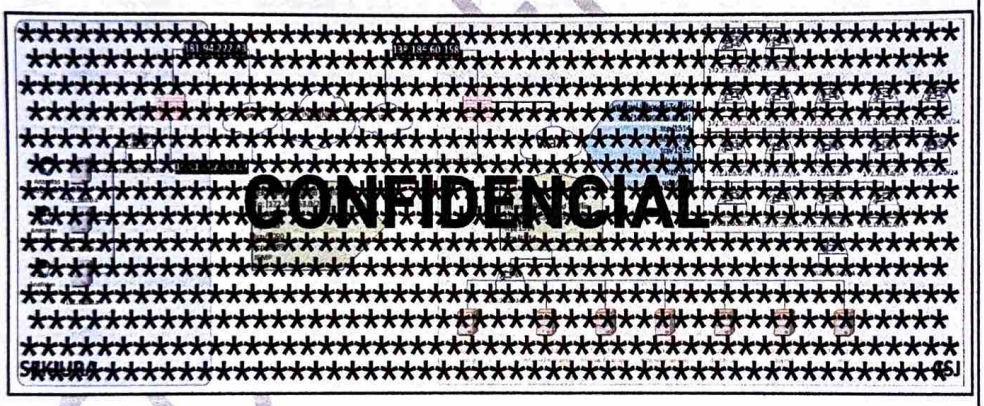
1. Infraestructura Tecnológica Desplegada

SEKIURA ha proporciona un equipo de tipo Servidor, identificado con las siguientgs características:

- Marca Modelo: [redacted]
- Número de Serie: [redacted]
- Características principales: [redacted]

El cual proporciona soporte tecnológico para albergar el ecosistema de Servidores Virtuales que posibilita la puesta en servicio de los componentes para capturar, analizar, correlacionar y categorizar (entre otras actividades) el volumen de registros que son originados desde el parque de equipos que se encuentran registrados en la plataforma SIEM Wazuh.

La siguiente ilustración demuestra lo mencionado:



CONFIDENCIAL

CORPORATION SEKIURA S.A.C.E.I. RUC N°80070880-0

2. Parque de Equipos Registrados en el SIEM Wazuh

Actualmente, en el Sistema SIEM Wazuh se encuentran registrados la cantidad de 72 (setenta y dos) equipos, los cuales se encuentran enviando sus eventos para que sean analizados por el SIEM Wazuh.

Es importante proseguir con las actividades de despliegue (de agente y configuraciones según correspondan) en los equipos que son de interés de CORTE SUPREMA DE JUSTICA.

La siguiente ilustración es una visualización que primeramente muestra de manera completa la cantidad de equipos registrados y de forma parcial el detalle de éstos:

CORPORATION SEKIURA S.A.C.E.I. RUC N°80070880-0

3. Informe Técnico

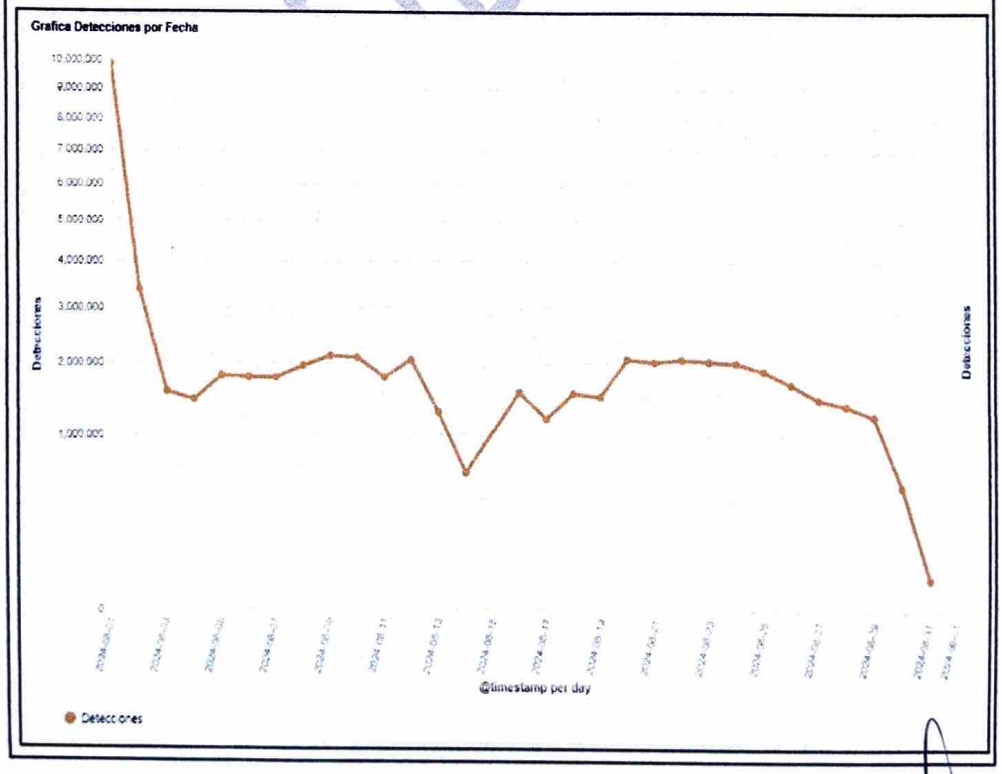
Fundamentado en el inmenso volumen de detecciones que son originados desde los equipos que son monitoreados por el SIEM Wazuh, parta este primer informe SEKIURA ha considerado como mejor estrategia para atender las diversas detecciones registradas, es exponer de manera descriptiva la información que fue generada gracias a los datos que a su vez fueron son proporcionados desde los equipos que se encuentran registrados en el SIEM Wazuh.

La información compilada se presenta a continuación:

A. Grafica Detecciones por Fecha

La cantidad de diversas detecciones que han sucedido en cada día del mes. Se observa un comportamiento mayormente homogéneo sin variaciones visibles.

El promedio de detección diaria se encuentra en el orden de 3.000.000 (tres millones) de detecciones.



CORPORATION SEKIURA S.A.C.E.I. RUC N°80070889-0

B. Distribución de Detecciones por Severidad

Cada una de las detecciones son analizadas, correlacionadas y valorizadas por la herramienta SIEM Wazuh, como resultado asigna un Nivel de Severidad, cuyos posibles valores van del número 0 (menor nivel de severidad) hasta el numero 16 (mayor nivel de severidad).

La gráfica muestra las siguientes columnas:

Rango: determina el Nivel de Severidad cuya interpretación es la siguiente:

- De 00 a 06: Severidad Baja
- De 07 a 11: Severidad Media
- De 12 a 14: Severidad Alta
- De 15 a 16: Severidad Critica

Severidad: el valor propiamente de la detección.

Descripción: la etiqueta descriptiva de la detección.

Cantidad: la cuenta de las detecciones.

CONFIDENCIAL

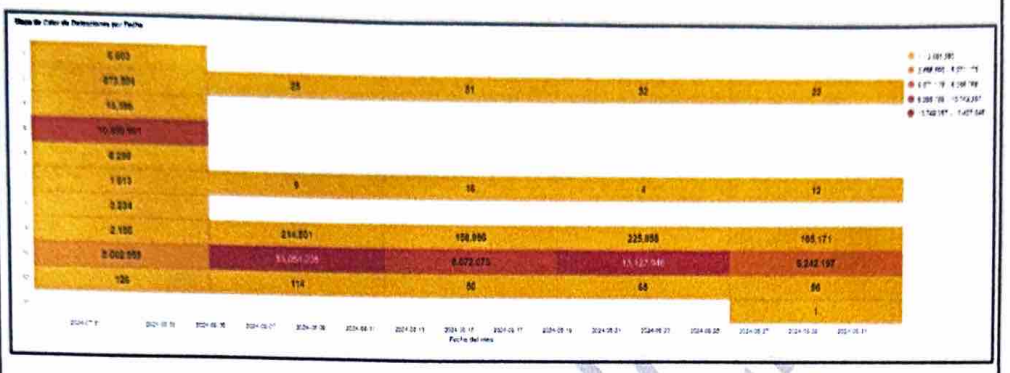
Rango	Severidad	Descripción de la Detección	Cantidad
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

‹ 1 ›

CORPORATION SEKIURA S.A.C.E.I. RUC 80070580-0

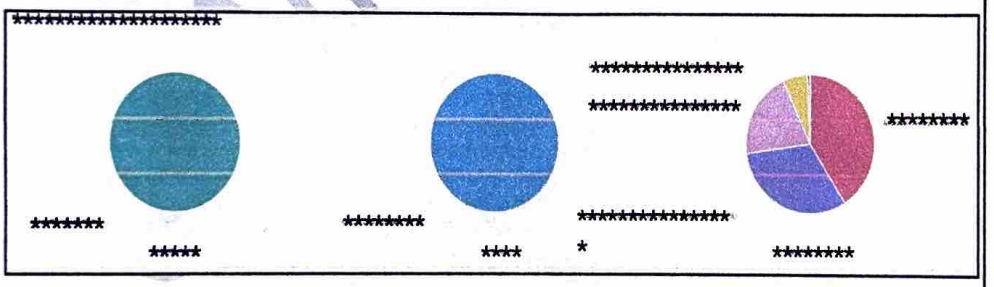
C. Mapa de Calor de Detecciones por Fecha

Permite conocer la cantidad y distribución de las detecciones en el transcurso diario del mes, lo cual permite entender el comportamiento y evolución de las detecciones en el parque de equipos.



D. Parque de Equipos Monitoreados: Sistemas Operativos Presentes

Permite conocer la composición y diversidad de Sistemas Operativos presentes en el parque de equipos que se encuentran en monitoreo del SIEM.



E. Parque de Equipos Monitoreados: Sistemas Operativos Detallado

Amplia el grafica anterior, indicando las cantidades exactas de Sistemas Operativos presentes en el parque de equipos que se encuentran en monitoreo del SIEM.

CORPORATION SEKIURA S.A.C.E.I. RUC N°80070880-0

[redacted]

CONFIDENCIAL

F. **Parque de Equipos Monitoreados: Sistemas Operativos y sus Vulnerabilidades Detectadas**

Es una agrupación de alto nivel el cual informa acerca de los tipos de vulnerabilidades detectadas en el Software (sean de: Sistema Operativo, Aplicaciones o Paquetes instalados) presentes en el parque de equipos que se encuentran en monitoreo del SIEM, sean estos de

[redacted]

Tipo de Sistema Operativo	Tipo de Vulnerabilidad Detectada	Cantidad
centos	Critical	1
centos	Low	313
[redacted]	[redacted]	[redacted]
[redacted]	Medium	9
[redacted]	Critical	184
[redacted]	[redacted]	[redacted]
windows	Low	178
[redacted]	[redacted]	[redacted]
[redacted]	Critical	1

CONFIDENCIAL

CORPORATION SEKIURA S.A.C.E.I. RUC N°80070880-0

4. Actividad realizada en conjunto

En atención a un inusual y extraordinario volumen de una misma detección, que consistía en la identificación de intentos fallidos de autenticación, que conforme a la nomenclatura del SIEM Wazuh se denomina **[Multiple Windows logon failures]**, se ha registrado la cantidad de 45.705.543 (cuarenta y cinco millones setecientos cinco mil quinientos cuarenta y tres) detecciones.

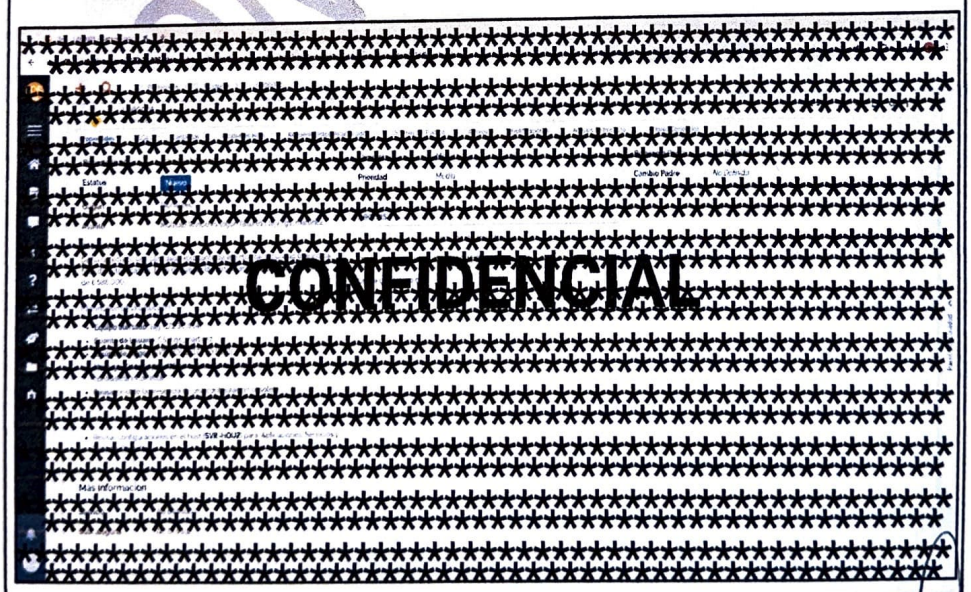
Si bien el volumen es inmenso, el 99% estas detecciones ocurrieron en un único equipo y correspondía a una específica e identificada cuenta de usuario, que por la experiencia de SEKIURA indica que se trata de una falla de configuración o de usuario (lo cual ha sido posteriormente confirmado); y no de un Ataque de Ciberseguridad que involucrada una credencial comprometida.

El 1% restante correspondía a fallos de contraseñas que fueron causadas accidentalmente por los usuarios, lo cual es típico en organízanos que poseen miles Usuarios, tal como lo es CORTE SUPREMA DE JUSTICIA.

Para atender esta situación, se ha llevado a cabo una tarea mancomunada que involucró a las áreas de: Seguridad Informatica [CORTE SUPREMA DE JUSTICIA], Infraestructura Tecnología [CORTE SUPREMA DE JUSTICIA] y SOC Analyst L2 [SEKIURA]

El registro de las actividades concernientes al presente caso se encuentra debidamente registrado en el ticket registrado para el efecto, al cual se puede acceder mediante el siguiente vinculo (URL):

[redacted]



CONFIDENCIAL

CORPORACION SEKIURA S.A.C.E.I. RUC N°80050880-0

5. Evolución Mensual del Servicio

El siguiente cuadro se muestra la evolución del servicio considerando diferentes indicadores:

Periodos	Equipos monitoreados	EPS	Tickets procesados	Incidentes reportados
08/2024	56	22,329 (*)	1 (**)	57.876.417

(*) El valor representa que en promedio ocurre 22,329 (veintidós y fracción) de detecciones por segundo, en todo el lapso que comprende el periodo indicado.

(**) Tener en cuenta que esta detección se ha representado poco más del 78% de todo el mes (lo que representa 45.589.120 detecciones) y por ese motivo se ha decidido abordar primera y únicamente este caso.

CONFIDENCIAL

CORPORATION SEKIURA S.A.C.E.I. RUC 80070809-0

6. Recomendaciones

El presente informe corresponde a los datos que han sido procesados por la plataforma SIEM Wazuh durante el mes Agosto de 2024, la cual se encuentra instalada en CORTE SUPREMA DE JUSTICIA. Esta plataforma colecta, categoriza e identificar los eventos de seguridad que ocurren en los equipos que se encuentran monitoreados por el SIEM.

A efectos de incrementar y mejorar la postura de Ciberseguridad de CORTE SUPREMA DE JUSTICIA se mencionan los siguientes:

1) Proseguir con el despliegue de las configuraciones para que los equipos y servicios que sean de interés de CORTE SUPREMA DE JUSTICIA estén registrado en la plataforma SIEM Wazuh y consecuentemente debidamente monitoreados por el Servicio SOCaaS.
2) Establecer una ventana de trabajo preestablecidas con las áreas operativas que poseen privilegios de administración, sobre los equipos monitoreados a efectos que puedan recibir acompañamiento de SOC/CSIRT de SEKIURA en pos de atender las incidencias y vulnerabilidades detectadas.
3) Procurar normalizar las versiones de Sistemas Operativos desplegados en su parque de equipos.
4) Abordar la remediación de las vulnerabilidades detectadas que atañen a [**Aplicaciones**] y a [**Sistemas Operativos**], aplicar lo más pronto posible las remediaciones de las vulnerabilidades de tipo [**Baja**] y [**Media**], como también planificar la remediación de tipo [**Alta**] y [**Criticas**].

El Servicio SOC/CSIRT se encuentra a vuestra disposición para acompañar las actividades mencionadas, como también para colaborar en su planificación.

CONFIDENCIAL

CORPORATIVA SEKIURA S.A.C.E.I. RUC N°80070880-0

Marcelo Oviedo