PR-OPE-006

Gestión de actividad sospechosa

Responsables

Elaboró:	Líder SOC
Revisó:	Control de Documentos
Aprobó:	Gerente de Operaciones

Control de versiones

Versión	Fecha	Descripción del cambio
1	26/02/2020	Emisión inicial
2	05/04/2022	Revisión anual
3	12/10/2022	Actualización de formato y revisión general del documento.

Clave del formato de procedimiento: F-SGI-002 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Objetivo del procedimiento

Definir los lineamientos para detectar, atender y corregir los eventos de actividad sospechosa derivado o identificados en el monitoreo preventivo de los servicios, con la finalidad de minimizar el impacto que estas tengan sobre las operaciones.

2. Alcance

El presente proceso cubre la detección, categorización, atención y seguimiento de las actividades sospechosas sobre los componentes y/o servicios monitoreados.

3. Definiciones

Actividad Sospechosa: Evento anómalo detectado en las herramientas de seguridad

Incidente: Afectación y/o degradación en el servicio.

SOC: Centro de operaciones de seguridad.

Ticket: Consulta de cualquier índole que puede usted realizar desde su área de clientes o si no es cliente aún, desde la opción "Contacto" desde nuestro sitio.

Materialización: Vulnerabilidad dentro de un activo informático que ha sido explotada

4. Responsabilidades

Rol	Responsabilidades y/o funciones
Dueño del Proceso	▪ Proporcionar el respaldo y recursos necesarios para garantizar el buen desempeño y cumplimiento del proceso.
Administrador del Proceso	▪ Generar información de la gestión del proceso. ▪ Monitorear la efectividad del proceso y hacer recomendaciones de mejora. ▪ Apoyar a los diferentes niveles, en caso de solicitar ayuda.
Herramienta de Monitoreo	▪ Detectar de manera automática los eventos atípicos o sospechosos a nivel global sobre redes externas ▪ Dar visibilidad del comportamiento de los índices de seguridad informática a nivel mundial, ejecutando análisis de los eventos detectados para sobre guardar la integridad, disponibilidad y confidencialidad de la información.
1er Nivel – SOC	▪ Monitorear alertas de herramienta de amenazas globales

	▪ Realizar un análisis, para determinación de amenaza conocida ▪ Realizar el registro de ticket, asignar a grupo resolutor de Ciberinteligencia y enviar notificación a cliente, indicando el hallazgo detectado. ▪ Revisar que el ticket este documentado y contenga el informe del análisis realizado por el equipo de Ciberinteligencia ▪ Enviar informe y solicitar contención sobre los IOC identificados
2do Nivel – Ciberinteligencia	▪ Documentar el ticket que les fue asignado y notificar a SOC que se está atendiendo ▪ Realizar investigación relacionada a la amenaza ▪ Emitir informe de Alerta Temprana, documentar ticket y adjuntar informe al mismo
Cliente	Recibir información de Alerta Temprana, autorizar contención de IOC

5. Descripción de actividades

No.	Actividad	Responsable	Descripción de la actividad	Registro
Inicio del procedimiento				
1.	Monitorear alertas de herramienta de amenazas globales	1er Nivel – SOC	Revisión 7x24x365 de la herramienta de gestión de amenazas globales	Herramienta de monitoreo
2.	Realizar un análisis, para determinación de una nueva amenaza de recién descubrimiento global	1er Nivel – SOC	Realizar un análisis, para determinación de amenaza ¿Se determina que es amenaza? SI pasar al paso 3 NO regresar al paso 1	Herramienta de monitoreo
3.	Realizar el registro de ticket, asignar a grupo resolutor de Ciberinteligencia y enviar notificación a cliente, indicando el hallazgo detectado.	1er Nivel – SOC	El equipo SOC después de realizar un análisis inicial, determina que dicha identificación debe analizarse de manera profunda por el equipo de Ciberinteligencia para identificar IOC	Herramienta de tickets
4.	Documentar el ticket que les fue asignado y notificar a SOC que se está atendiendo	2do Nivel – Ciberinteligencia	Dar seguimiento a nivel documental del ticket asignado, cambio estado del mismo a en curso	Herramienta de tickets

5.	Realizar investigación relacionada a la amenaza	2do Nivel – Ciberinteligencia	Analizar de manera minuciosa la amenaza detectada, identificando los IOC asociados a la misma	Herramientas de Ciberinteligencia
6.	Emitir informe de Alerta Temprana, documentar ticket y adjuntar informe al mismo	2do Nivel – Ciberinteligencia	Generación de análisis conocido como Alerta Temprana, indicado los hallazgos asociados a dicha amenaza	
7.	Revisar que el ticket este documentado y contenga el informe de actividad sospechosa	1er Nivel – SOC	Revisar que el ticket este documentado y contenga el informe de actividad sospechosa SI ir al paso 8 NO ir al paso 6	
8.	Enviar informe y solicitar contención sobre IOC identificados	1er Nivel – SOC	Dar seguimiento a la actividad proactiva ante el cliente, solicitando su apoyo para contener los IOC dentro de las herramientas de seguridad en las que aplique.	
9.	Recibir información de Alerta Temprana, autorizar contención de IOC	Cliente	Retroalimentar de manera oportuna las solicitudes emitidas por el SOC para aplicar las contenciones pertinentes.	P-SGI-019_Gestion_solicitudes_servicio
Fin del procedimiento				

6. Documentos relacionados

- P-SGI-019_Gestion_solicitudes_servicio

7. Anexos

N\A