

	Buena Práctica	Fecha:	29-10-2020
		Versión:	1
		Código:	CI-FO-08

Nombre o Lema de la iniciativa	Monitoreo Prevención de Fuga de información en SILA	
Datos de contacto	Autoridad Nacional de Licencias Ambientales MSI Raúl Trujillo García rtrujillo@anla.gov.co Profesional especializado	
Contexto	En la Autoridad Nacional de Licencias Ambientales, la documentación sensible dentro de los procesos misionales de Evaluación y seguimiento que se realizaban en la aplicación de SILA, sin embargo, se han presentado varios incidentes frente a la fuga de información mientras los conceptos técnicos se encuentran en construcción, por lo que es necesario crear reglas de negocio a través del correlacionador de eventos de alertas, cada vez que la información sensible de SILA sea accedida o descargada.	
Proyecto/ Iniciativa	Configurar reglas de negocio sobre la documentación sensible permite a la entidad conocer la trazabilidad y el acceso a la información sensible dentro de la aplicación de SILA.	
Resultados	El alertamiento proactivo frente a la descarga y el acceso a los documentos en construcción que permiten la prevención de fuga de información. A la fecha ninguna dependencia misional ha solicitado la información; sin embargo, no significa que desde la OTI no se esté realizando el monitoreo.	
Factores clave	El conocimiento del alcance de las herramientas de seguridad informática y el reporte de incidentes de seguridad, por parte de los jefes de las dependencias misionales.	
Actividades	1	Configurar las reglas de negocio para el alertamiento de los documentos sensibles de SILA en el correlacionador de eventos Fortisiem.
	2	Entrega a la dependencia misional el reporte de descargas del documento involucrado (fuga de información), con la información del personal que descargó y modificó el mismo. El anterior reporte se realiza a demanda.
	3	Consulta de los reportes de fuga de información, por medio de un tablero de control de Power BI solicitado por la Dirección General de la entidad.
Insumos: Describa las herramientas, materiales y personal participante en la iniciativa o proyecto	Herramientas: SILA Correlacionador de eventos Fortisiem	
	Materiales: NA	
	Personal: Profesional especializado de libre nombramiento de la dependencia de la Oficina de Tecnologías de la información - Raúl Trujillo Contratista de Seguridad de la información - Jorge Enrique Vega	
Sostenibilidad	Involucrar a las áreas del negocio para levantar las necesidades del negocio y las novedades frente a los incidentes de seguridad y los riesgos mismos de los procesos. Figura 1. Tablero Control Descarga Documentos SILA - Power BI	

NOTA: Al tratarse de un tablero de control en el que se visualiza información sensible este no se publica ni en la intranet ni en el portal web.

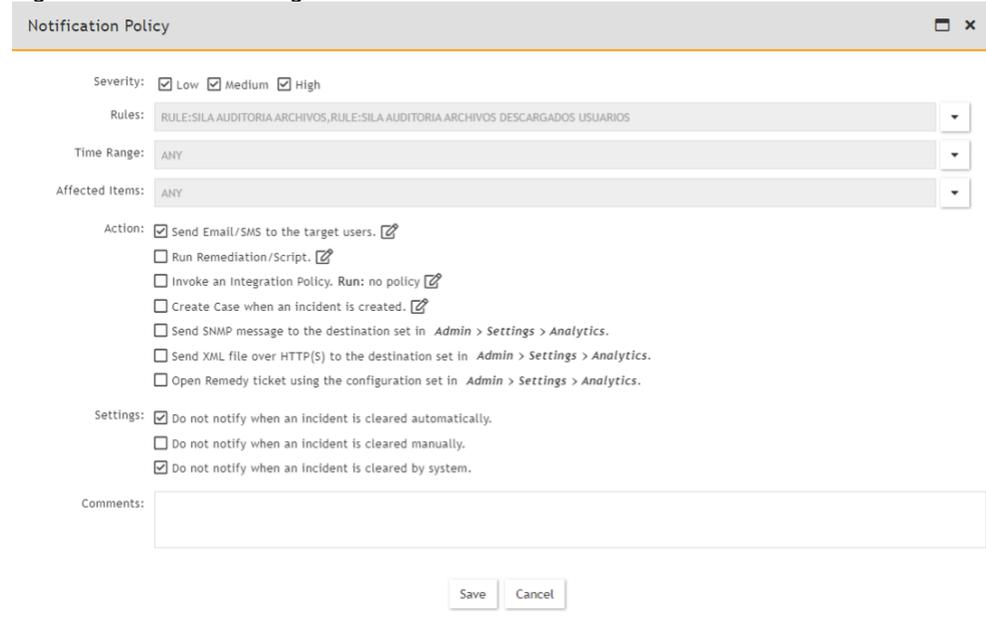
En acción

Figura 1. Front tablero de control



EXPEDIENTE	Usuario	ETAPA ACTIVIDAD	FECHA_DESCARGA	COMENTARIO
SAN0198-00-2020	Juan David Herrera	Sancionatorio	26/09/2022 10:30:37	El usuario jdherreira inicializo la descarga del archivo: 1895967_2022922CT_CARGOS_SAN0198-00-2020_FINAL.docx, el día: 26/09/2022 a la hora:10:30 a. m. del expediente: SAN0198-00-2020 actividad: CONCEPTO TÉCNICO DE FORMULACIÓN DE CARGOS O CESACIÓN DE PROCEDIMIENTO SANCI
SAN0275-00-2020	Juan David Herrera	Sancionatorio	20/09/2022 10:46:10	El usuario jdherreira inicializo la descarga del archivo: 1886618_2022919SAN0275-00-2020_CTCARGOS_VFinal.docx, el día: 20/09/2022 a la hora:10:46 a. m. del expediente: SAN0275-00-2020 actividad: CONCEPTO TÉCNICO DE FORMULACIÓN DE CARGOS O CESACIÓN DE PROCEDIMIENTO SANCI
SAN0275-00-2020	Juan David Herrera	Sancionatorio	20/09/2022 9:35:41	El usuario jdherreira inicializo la descarga del archivo: 1886618_2022919SAN0275-00-2020_CTCARGOS_VFinal.docx, el día: 20/09/2022 a la hora:9:35 a. m. del expediente: SAN0275-00-2020 actividad: CONCEPTO TÉCNICO DE FORMULACIÓN DE CARGOS O CESACIÓN DE PROCEDIMIENTO SANCI
SAN0275-00-2020	Juan David Herrera	Sancionatorio	20/09/2022 9:35:40	El usuario jdherreira inicializo la descarga del archivo: 1886618_2022919SAN0275-00-2020_CTCARGOS_VFinal.docx, el día:

Figura 2. Pantalla de configuración de notificaciones



Notification Policy

Severity: Low Medium High

Rules: RULE:SILA AUDITORIA ARCHIVOS,RULE:SILA AUDITORIA ARCHIVOS DESCARGADOS USUARIOS

Time Range: ANY

Affected Items: ANY

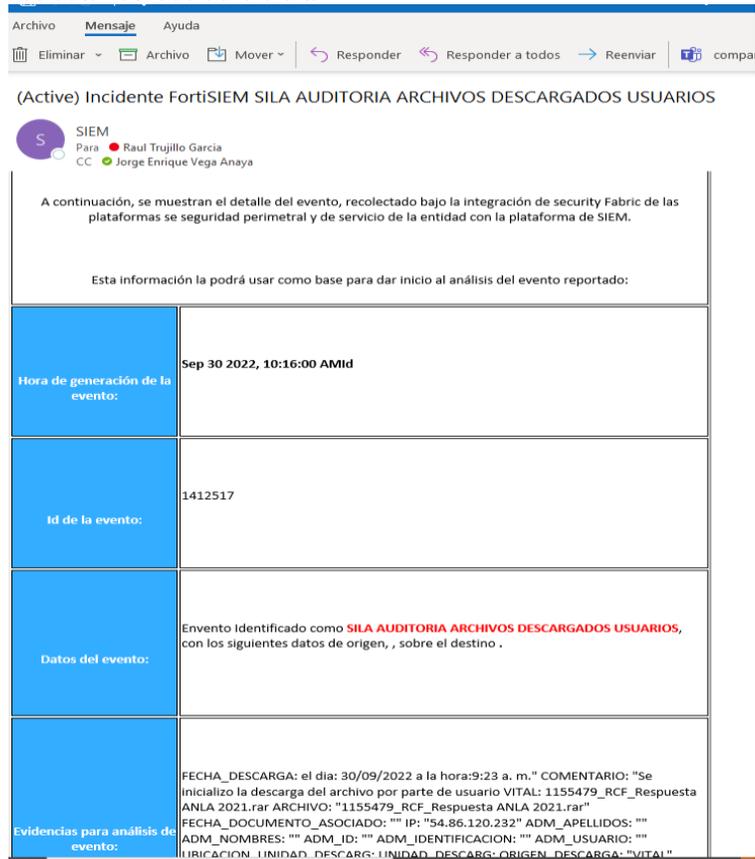
Action: Send Email/SMS to the target users. Run Remediation/Script. Invoke an Integration Policy. Run: no policy Create Case when an incident is created. Send SNMP message to the destination set in Admin > Settings > Analytics. Send XML file over HTTP(S) to the destination set in Admin > Settings > Analytics. Open Remedy ticket using the configuration set in Admin > Settings > Analytics.

Settings: Do not notify when an incident is cleared automatically. Do not notify when an incident is cleared manually. Do not notify when an incident is cleared by system.

Comments:

Save Cancel

Figura 3. Correo automatizado de la alerta



Archivo Mensaje Ayuda

Eliminar Archivar Mover Responder Responder a todos Reenviar

(Active) Incidente Fortisiem SILA AUDITORIA ARCHIVOS DESCARGADOS USUARIOS

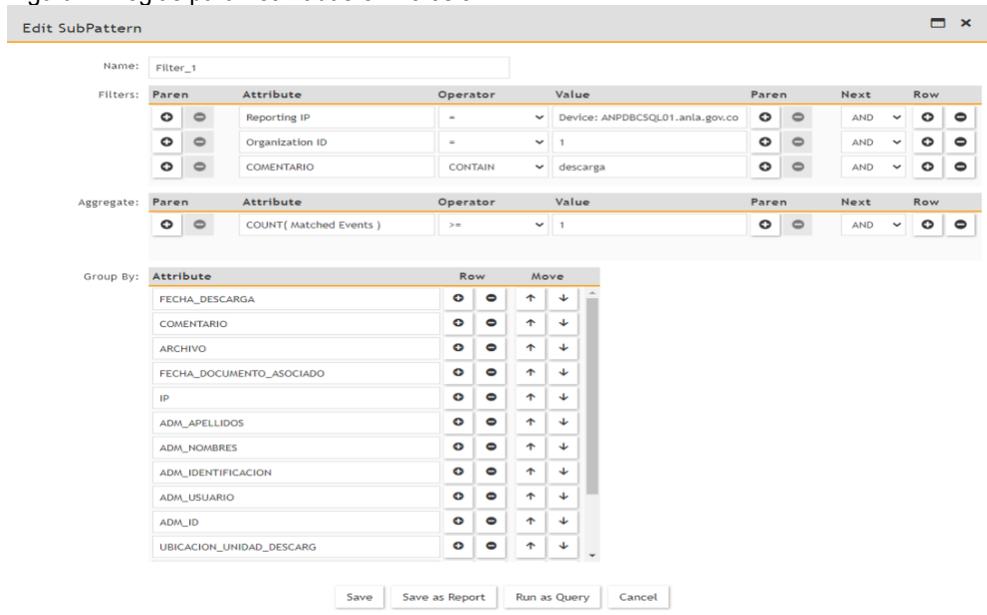
SIEM
Para Raul Trujillo Garcia
CC Jorge Enrique Vega Anaya

A continuación, se muestran el detalle del evento, recolectado bajo la integración de security Fabric de las plataformas de seguridad perimetral y de servicio de la entidad con la plataforma de SIEM.

Esta información la podrá usar como base para dar inicio al análisis del evento reportado:

Hora de generación de la evento:	Sep 30 2022, 10:16:00 AMId
Id de la evento:	1412517
Datos del evento:	Evento Identificado como SILA AUDITORIA ARCHIVOS DESCARGADOS USUARIOS , con los siguientes datos de origen, , sobre el destino .
Evidencias para análisis de evento:	FECHA_DESCARGA: el día: 30/09/2022 a la hora:9:23 a. m." COMENTARIO: "Se inicializo la descarga del archivo por parte de usuario VITAL: 1155479_RCF_Respuesta ANLA 2021.rar ARCHIVO: "1155479_RCF_Respuesta ANLA 2021.rar" FECHA_DOCUMENTO_ASOCIADO: "" IP: "54.86.120.232" ADM_APELLIDOS: "" ADM_NOMBRES: "" ADM_ID: "" ADM_IDENTIFICACION: "" ADM_USUARIO: "" UBICACION_UNIDAD_DESCARG: UNIDAD_DESCARG: ORIGEN_DESCARGA: "VITAL"

Figura 4. Reglas parametrizadas en Fortisiem



Edit SubPattern

Name: Filter_1

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	(Reporting IP	=	Device: ANPDBC5QL01.anla.gov.co)	AND	1
	(Organization ID	=	1)	AND	2
	(COMENTARIO	CONTAIN	descarga)	AND	3

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
	(COUNT(Matched Events)	>=	1)	AND	1

Group By:	Attribute	Row	Move
	FECHA_DESCARGA	1	2
	COMENTARIO	1	2
	ARCHIVO	1	2
	FECHA_DOCUMENTO_ASOCIADO	1	2
	IP	1	2
	ADM_APELLIDOS	1	2
	ADM_NOMBRES	1	2
	ADM_IDENTIFICACION	1	2
	ADM_USUARIO	1	2
	ADM_ID	1	2
	UBICACION_UNIDAD_DESCARG	1	2

Save Save as Report Run as Query Cancel