Especialización en Ciberseguridad

Análisis de Logs en Sistemas SCADA para prevención y mitigación de Ciberataques en Sistemas eléctricos de Potencia

Sebastián Maldonado Posada

Universidad® Católica de Manizales
VIGILADA MINEDUCACIÓN
Obra de Iglesia de la Congregación
Hermanas de la Caridad Dominicas de La Presentación de la Santísima Virgen

Análisis de Logs en Sistemas SCADA para prevención y mitigación de Ciberataques en Sistemas eléctricos de Potencia

Trabajo de grado presentado como requisito para optar al título de *Especialización en Ciberseguridad*

Modalidad de grado: Monografía

Héctor Gordon [1]

Sebastián Maldonado Posada

UNIVERSIDAD CATÓLICA DE MANIZALES

FACULTAD INGENIERÍA Y ARQUITECTURA

ESPECIALIZACIÓN EN CIBERSEGURIDAD

Manizales, Caldas

2023

[1] 0000-0002-3453-8226

Tabla de contenido

Listado de figuras

Listado de tablas

Resumen

Este proyecto se enfoca en el análisis de logs de sistemas SCADA para sistemas eléctricos de potencia (transmisión y distribución de energía), se buscará la implementación de mejoras en la seguridad y protección de los sistemas de control de procesos y activos críticos. El análisis de logs permite examinar y analizar los registros de eventos generados por el sistema, identificar posibles amenazas o vulnerabilidades y prevenir futuros incidentes de seguridad. Se buscarán herramientas y técnicas para el análisis de logs y que posiblemente puedan ser aplicadas en sistemas de tiempo real entornos industriales, para lograr evaluar los sistemas de control y automatización. El objetivo principal es buscar mejoras en el uso de estas herramientas de análisis, implementar buenas prácticas en Ciberseguridad y la protección de los sistemas de control de activos críticos, para garantizar su funcionamiento óptimo y la continuidad del negocio, la cual es fundamental para empresas que prestan servicios públicos. Se dará contexto de la arquitectura de un sistema SCADA para operación eléctrica y se brindará objetividad en los elementos a analizar dentro de estos sistemas.

Palabras clave: logs, eventos, SCADA, RTU, protocolos industriales, analítica básica, análisis de vulnerabilidades.

Abstract

This project focuses on the analysis of logs of SCADA systems for electrical power systems (energy transmission and distribution), the implementation of improvements in the safety and protection of process control systems and critical assets will be sought. Log analysis allows you to examine and analyze the event logs generated by the system, identify possible threats or vulnerabilities and prevent future security incidents. Tools and techniques will be sought for log analysis that can possibly be applied in real-time systems in industrial environments, to evaluate control and automation systems. The main objective is to seek improvements in the use of these analysis tools, implement good practices in Cybersecurity and the protection of critical asset control systems, to guarantee their optimal functioning and business continuity, which is essential for companies that They provide public services. Context of the architecture of a SCADA system for electrical operation will be given and objectivity will be provided in the elements to be analyzed within these systems.

Keywords: logs, events, SCADA, RTU, industrial protocols, basic analytics, vulnerability analysis.

El contenido deberá ajustarse a los requerimientos de la modalidad elegida. De acuerdo con el formato de evaluación que corresponde:

1. Introducción

Los sistemas SCADA están categorizados como un componente crítico para la Operación, restablecimiento de energía, calidad y confiabilidad de los sistemas eléctricos, en todos los mercados de energía, tanto generación, transmisión y distribución de la energía eléctrica, por lo que la seguridad de la información y protección de datos de estos sistemas es de suma importancia. Muchas de las arquitecturas e infraestructuras de los sistemas SCADA, son soportadas en máquinas físicas propensas a ser vulnerables y con Sistemas operativos que resultan tener algunos aspectos a corregir en el ámbito de la Ciberseguridad. En este sentido, el análisis de logs se presenta como una herramienta clave para identificar posibles riesgos, amenazas y vulnerabilidades, así como para tratar de prevenir futuros incidentes de seguridad. Con este proyecto, se espera mejorar el conocimiento frente a la seguridad y protección de los sistemas de control de activos críticos, para garantizar su funcionamiento óptimo y la continuidad del negocio en las empresas que prestan servicios públicos de energía eléctrica. Los beneficios de implementar un análisis de logs en sistemas SCADA incluyen una mayor visibilidad de la seguridad del sistema, la detección temprana de amenazas y la reducción del tiempo de inactividad. Además, la implementación de un análisis de logs puede ayudar a las organizaciones a cumplir con los requisitos de regulaciones y estándares de seguridad, como NERC-CIP o ISA/IEC 62443, NIST, Acuerdos del CNO, ISO/IEC27001 entre otras. Se espera brindar aspectos básicos de seguridad relacionados con los activos de operación eléctrica al personal encargado del proceso de Automatización y control, incentivando las buenas prácticas de Ciberseguridad en estos sistemas y fomentar su uso e implementación cuando se tenga el aval por parte de la organización establecida, en este caso la CHEC S.A. E.S.P BIC.

2. Localización

La Central Hidroeléctrica de Caldas (CHEC S.A E.S.P BIC) con ubicación principal en el departamento de Caldas en la ciudad de Manizales, es una empresa prestadora del Servicio Público de Energía Eléctrica para las regiones de Caldas y Risaralda. Se caracteriza por ser una empresa consolidada en el sector eléctrico desde hace 78 años donde su principal negocio es la distribución de energía, contando actualmente con alrededor de 560 mil usuarios a través de todo el territorio mencionado. También cuenta con los negocios de Generación y Transmisión, haciendo parte vital del Sistema Interconectado Nacional o STN (Sistema de Transmisión Nacional) el cual está regulado por el XM o CND (Centro Nacional de Despacho) y es donde todos los operadores de la red eléctrica en Colombia reportan las actividades de sus activos críticos con Niveles de Alta Tensión (redes eléctricas de 110 kV a 500 kV).

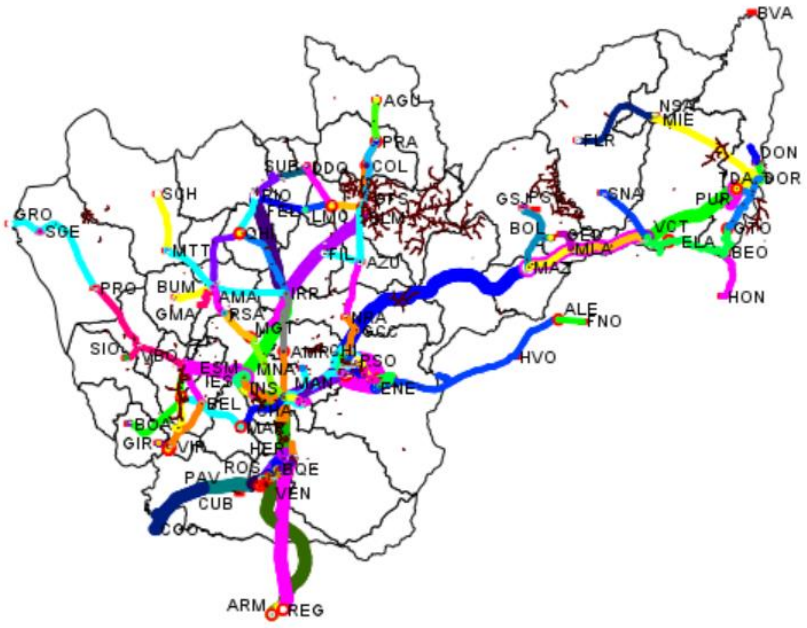


***Figura 1. Región de cobertura eléctrica CHEC**. (Ver: Referencia 1)*

La empresa también se ha caracterizado por su cuidado al cliente al cliente la cobertura y disposición al momento de presentar fallas en la red eléctrica. Sus objetivos estratégicos apuntan directamente al desarrollo organizacional, la planeación y las comunicaciones.

Dentro de los objetivos misionales que tiene, son precisamente los negocios de Distribución, Generación, Comercio y atención al cliente. Brindando acá un enfoque esencial a la prestación del servicio de energía eléctrica.

Los usuarios de la región Caldense y Risaraldense están cobijados por 63 subestaciones de Transmisión y Distribución interconectadas según las necesidades del sector y la topología nacional del STN. Estas subestaciones son supervisadas a través de sistemas SCADA que monitorean el comportamiento eléctrico de los activos de la subestación en tiempo real, llevando información clara y precisa de manera inmediata al Centro de Control principal ubicado de manera remota a dichas subestaciones. Uno de los procesos operativos más importantes es el restablecimiento y las maniobras remotas que se puedan realizar a todos los equipos de corte implicados en la Transmisión y Distribución de energía, para la operación del sistema este es un punto crítico para el cuidado del cliente y las posibles sanciones que implique el desabastecimiento de energía; la calidad del servicio se ve afectada y para Colombia existen regulaciones que castigan severamente este indicador. Este proceso de Operación es de vital importancia y depende netamente del funcionamiento y configuración correcta de los sistemas SCADA.

3. Objetivos

Objetivo General

Plantear mecanismos, estrategias, buenas prácticas y el uso de herramientas que ayuden a mejorar la seguridad de los sistemas SCADA en el proceso de transmisión y distribución de energía, mediante la identificación y respuesta oportuna a posibles amenazas de ciberseguridad y aumentar la visibilidad y el conocimiento de la infraestructura de dichos sistemas, a través de la recopilación y análisis de los logs que brindan los diferentes dispositivos que conforman el sistema SCADA.

Objetivos Específicos

- Identificar patrones y comportamientos anómalos en los logs generados en los sistemas SCADA, para algunos dispositivos específicos, con el fin de utilizar herramientas y crear alertas para notificar a los responsables de estos sistemas sobre posibles amenazas.

- Proponer y documentar mejoras en los procesos y sistemas de automatización y control para aumentar la eficiencia y efectividad de la seguridad y protección de los ciber activos críticos que se encuentran definidos en los acuerdos regulatorios (CNO) y marcos normativos nacionales e internacionales.

- Capacitar al personal encargado de la gestión de los sistemas SCADA en buenas prácticas de ciberseguridad en ambientes TO, utilizando el análisis de logs como herramienta para respuesta y prevención a posibles incidentes.

4. Antecedentes (si es del caso)

Para revisar todo lo relacionado con incidentes de Ciberseguridad en infraestructura Eléctrica Crítica vamos a citar varias noticias relevantes en el mundo, tanto de la operación eléctrica y como en el mundo de la Ciberseguridad.

Se citarán varios escenarios donde fueron atacadas algunas Centrales Eléctricas, entre ellas subestaciones eléctricas y que implicaron alguna maniobra de un equipo de campo por algún externo y analizar el peligro que puede llegar a traer un ataque de estos y que implicaciones puede tener para la vida humana, para el sector eléctrico, para el sector comercial y que lecciones aprendidas se pueden aprender por el personal de TO:

Lo menciona BBC noticias en una de sus páginas oficiales (1), donde cita los ataques que tuvieron las centrales eléctricas en Ucrania en 2015 y 2016:

"En 2015, la red eléctrica de Ucrania se vio interrumpida por un ataque cibernético llamado BlackEnergy, que causó un apagón a corto plazo para 80.000 clientes de una empresa de servicios públicos en el oeste de Ucrania".

Casi exactamente un año después, otro ataque cibernético conocido como Industroyer dejó sin energía durante aproximadamente una hora a casi una quinta parte de Kiev, la capital de Ucrania, EE.UU. y la UE nombraron y responsabilizaron de los ataques a hackers militares rusos.

"Rusia podría absolutamente intentar ejecutar un ataque como este contra Occidente como una ilustración de sus capacidades y para enviar una señal", afirma Marina Krotofil, responsable de seguridad cibernética ucraniana, quien ayudó a investigar los cortes de energía.

Este tipo de noticias nos brinda una alerta real a las empresas de energía en Latinoamérica donde nos lleva a preguntarnos si en realidad tenemos la capacidad de reaccionar o de tener alguna reacción inmediata frente a estos ataques y a esta contingencia.

Y no se está exento de este tipo de ataques en cualquier empresa que maneje redes de TI y TO para sus procesos diarios, BBC menciona en el mismo artículo:

"En mayo de 2021 se declaró el estado de emergencia en varios estados de EE.UU. después de que un grupo de hackers causara el cierre de un gasoducto vital." (ver: Referencia 3)

Otra noticia que se conoce demasiado dentro de los titulares importantes de los que nos gusta el mundo de la Ciberseguridad es el siguiente:

"El gusano Stuxnet que afecta a sistemas SCADA causa revuelo internacional" (ver: referencia 3); se menciona en la página del Centro Criptológico Nacional de España. Un encabezado que lleva a reflexionar sobre los posibles ataques que se puedan dar en los sistemas SCADA.

Por este tipo de noticias es que se deberá emplear una estrategia para proteger los diferentes sistemas operativos de las empresas, tanto de la infraestructura de TI como de la de TO, la cual viene siendo crítica para las empresas de producción.

Se conoce relativamente poco de los logs que se deberán analizar en los sistemas SCADA, pero se realizará la tarea investigativa con el fin de ejecutar y proporcionar herramientas que sirvan para los administradores de dicho sistema.

Esta tarea se vuelve relevante tanto para el proceso de soporte dentro de la empresa, sino también para la línea final de atención al cliente, que es la que realmente apuntan los objetivos estratégicos y misionales de la empresa.

5. Marco teórico (si es del caso)

Este proyecto se basará directamente en el análisis de los servidores que utilizan aplicaciones SCADA en la empresa CHEC. Donde veremos que protocolos, equipos, servidores, sistemas operativos y redes se utilizan para llevar a cabo la operación remota de activos eléctricos en distintos niveles de tensión.

Para verificar el desarrollo del estudio relacionado con los sistemas propios de la empresa, se analizarán principalmente algunas aplicaciones de proveedores conocidos internacionalmente; en los cuales se dará a conocer brevemente que arquitectura de datos utilizan para transmitir la información en tiempo real y de esta manera verificar los distintos protocolos y que resultados pueden llegar a tener con la extracción de logs de dichos protocolos.

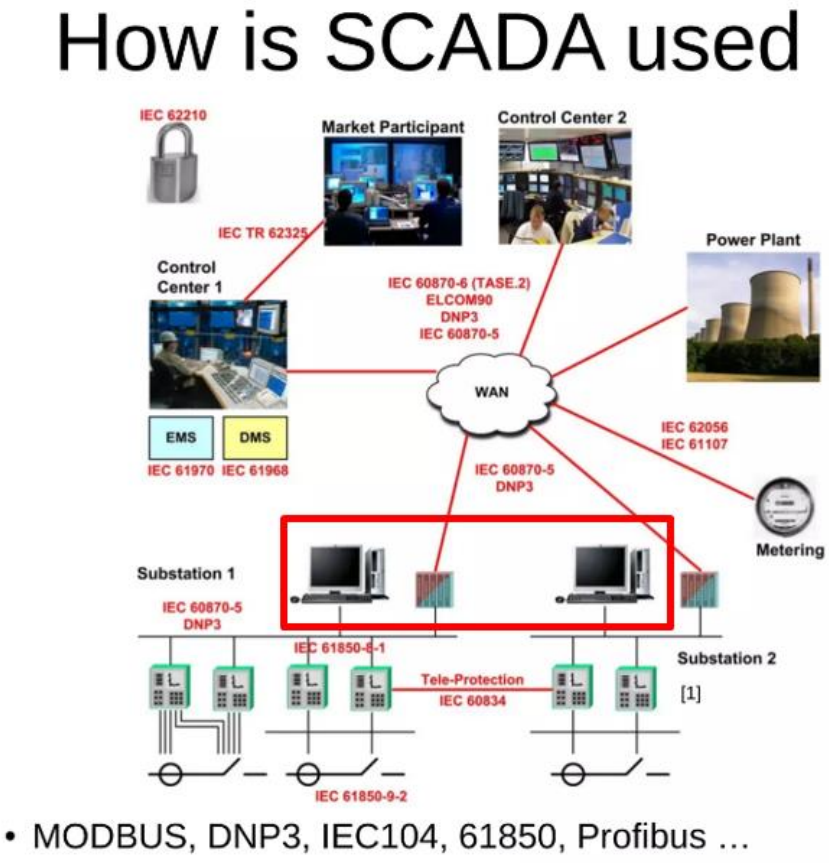


Figura 3. Arquitectura y protocolos de un sistema SCADA *(ver: Referencia 4)*

Dicho intercambio de información implica directamente personal de distintas aréas con conocimientos específicos diferentes, en los que se puede llevar a analizar la política de protección de datos, desde una mirada más profunda, los cuales implica temas de ingeniería social y coordinación de comunicación asertiva entre los distintos actores de la operación eléctrica dentro de una empresa que trabaja con personal externo.

En este orden de ideas, se puede empezar por argumentar y dar a conocer de manera muy general los protocolos y configuraciones de arquitecturas de red que se utilizan en dichas subestaciones; los protocolos utilizados son de vital importancia para dar conclusiones y mostrar resultados frente a la aplicación de conceptos de seguridad aplicados en los mismos.

Apuntar directamente a las buenas prácticas desde este nivel de SCADA es importante, y realizarlo requiere un análisis profundo de los malos hábitos que se tienen en estos equipos e instalaciones. Es decir, que, para desarrollar este proyecto, se piensa en analizar equipos remotos que tengan acceso por personal tanto propio de la empresa como contratista, donde se reflejen en los logs seleccionados, dichas actividades que impliquen un riesgo para la ciberseguridad; ya sea por malas prácticas o por acciones que no estén dentro del conocimiento del personal en sitio.

La hipótesis que se conserva para llevar a cabo esta actividad tiene que ver con todo lo relacionado al seguimiento que se le pueda realizar a los usuarios del sistema, tanto externos como propios de la empresa, al comportamiento eléctrico de los equipos, identificar anomalías según eventos presentados en el sistema y verificar posibles amenazas que se pueden presentar en tiempo real, estar preparado para ellas y gestionar de manera inmediata dichos incidentes.

6. Metodología

Para tratar de brindar un enfoque estructurado y sistemático con el fin de llevar un buen planteamiento desde la misma planeación para lograr las metas propuestas con este proyecto. Se definen algunos parámetros clave para implementar la metodología más adecuada:

Para esto podemos empezar por definir la estructura de implementación del proyecto, donde se proyectan varios procesos:

1. Planeación

2. Requerimientos y evaluación de Riesgos

3. Monitoreo y Análisis Continuo

Para llevar a cabo esta metodología se debe tener claro que actividades se deben realizar por cada uno de los planteamientos, veremos a detalle cada una:

1. Planeación:

- Definición de objetivos (Objetivo General, Específicos)
- Identificación de los sistemas SCADA a analizar: Es importante verificar que tipos de aplicaciones se utilizan para el sistema SCADA, tipos de infraestructura y sistemas Operativos utilizado, esto determinará los tipos de logs a recopilar y analizar.
- Infraestructura requerida para el análisis: Identificar los activos críticos, categorizarlos y analizar los datos según el personal responsable.

2. Requerimientos y evaluación de Riesgos:

Identificar los principales riesgos para el sector de la Operación de activos eléctricos, verificar su cumplimiento según regulación, normas establecidas de Ciberseguridad, estándares y creación de procedimientos y equipos de trabajo para evaluar y dar soporte. Se pueden tomar como riesgos, todos los activos críticos de las subestaciones eléctricas, esto desprende los requerimientos, en la siguiente tabla se plantean algunos escenarios según el activo de cada subestación, enfatizando en los equipos propios del Sistema SCADA:

Activo	Confidencialidad		Integridad		Disponibilidad	
	Valoración	Justificación	Valoración	Justificación	Valoración	Justificación
IED	Moderado	Información operativa convencional que no merece ser confidencial	Catastrófico	Por ser la unidad básica de recepción/envió de información, su integridad es de muy alta valoración.	Moderado	Indisponible la supervisión sobre el elemento o la función que realice el elemento indisponible
HMI S/E	Moderado	Información operativa convencional que no merece ser confidencial	Moderado	Si su funcionamiento no es adecuado se realiza manejo del IED directamente	Mayor	La supervisión y control de la S/E se hace muy dispendiosa y la información no estaría disponible
HMI Principal	Moderado	Información operativa convencional que no merece ser confidencial	Mayor	Si su funcionamiento no es adecuado se realiza manejo del HMI de todas las S/E o IED directamente	Catastrófica	La supervisión y control del Sistema eléctrico no podría realizarse.
Front End	Moderado	Información operativa convencional que no merece ser confidencial	Mayor	Si su funcionamiento no es adecuado se realiza manejo del HMI de todas las S/E o IED directamente	Catastrófica	La supervisión y control del Sistema eléctrico no podría realizarse.
Protocolos	Insignificante	Protocolos utilizados son estándares	Menor	Los protocolos utilizados son confiables	Insignificante	No aplica el concepto de disponibilidad

Figura 4. Matriz de riesgos para activos críticos de una subestación eléctrica *(ver: referencia 5)*

Es notorio lo crítico que puede llegar a ser la pérdida de la Disponibilidad de un HMI del Sistema SCADA, el cual corresponde a una gran responsabilidad tanto para las vidas humanas como para las sanciones y penalizaciones que un operador de red puede tener por prestación y Calidad del Servicio de Energía Eléctrica.

De todas formas, también se plantean como en cualquier sistema la posibilidad de errores humanos, malas configuraciones, malas intenciones, y demás posibilidades que se pueden ver frente a un ataque Cibernético:

Disponibilidad del Activo

VALORACION RIESGO - PERDIDA DE **DISPONIBILIDAD** DEL ACTIVO						
VULNERABILIDAD	**AMENAZA**	**IED**	**HMI S/E**	**HMI P/L**	**FE**	**PT**
Controles inadecuados de acceso físico/lógico	Abuso de privilegios	IA	IA	IA		
	Acceso no autorizado	ID	ID	ID		
	Denegación de Servicios	ID	ID	ID		
	Ataque dirigido		ID	ID	ID	
Configuración incorrecta o Inadecuada	Acceso no autorizado	ID	ID	ID		
	Ataque dirigido		ID	ID	ID	
	Caída del sistema por agotamiento de recursos		ID	IA	ID	
	Denegación de servicios	ID	ID	ID	ID	
Insuficiente protección contra virus y código malicioso	Fallas de sw		ID	ID		
	Vulnerabilidad de los programas		ID	ID		
	Denegación de servicios		ID	ID		
Punto único de fallo	Fallas de hardware				ID	
	Caídas del sistema por agotamiento de recursos				ID	
	Ataque dirigido				ID	
Insuficientes o inadecuados mantenimientos predictivos, preventivos y/o correctivos	Fallas de hardware				ID	
	Degradación de los soportes de almacenamiento				ID	
	Avería de origen físico/lógico				ID	

Figura 5. Valoración de riesgos para activos críticos de una subestación eléctrica *(ver: referencia 6)*

3. <u>Monitoreo y Análisis Continuo</u>:

Consolidar herramientas para realizar seguimiento continuo y alertar por posibles factores definidos dentro de la construcción del proyecto. De esta manera se garantiza el análisis de los datos en tiempo real y la detección temprana de posibles amenazas, se debe definir un proceso que lo respalde.

7. Cuerpo del trabajo

Para realizar las actividades iniciales de análisis de logs, referentes a algún equipo en específico dentro de la red SCADA, nos remitimos a la Figura 3. la cual nos da un amplio margen de protocolos industriales, utilizados en los sistemas SCADA. Al pertenecer estos protocolos a una "red aislada", se debe validar como realizan los diferentes envíos de datos a través de alguna red corporativa que esté conectada directamente a internet.

Uno de los principales errores de administradores de Sistemas SCADA es mencionar las frases: "*las redes SCADA están aisladas de internet y no pueden ser hackeadas*", "*si funciona, no lo toques*", y algunas otras frases que pueden estar muy fuera de la realidad si nos ponemos a analizar a detalle y revisar a fondo como se puede vulnerar un sistema de estos por un externo. Algunos protocolos utilizados, incluso no presentan ninguna medida de seguridad y representan una vulnerabilidad latente donde se encuentren:

Protocolo IEC104: Es un protocolo con medio de transmisión guiado con estándar EIA568-B lo cual utiliza como medio físico cables ethernet, los cuales representan una conexión común y sencilla para equipos críticos de operación:

Algunos aspectos identificados para este protocolo son:

- Captura sencilla de paquetes con Span Port, DNS Poisoning
- Wireshark
- ARP Spoofing
- Captura y réplica de paquetes (Comandos, Lecturas, Alarmas…)
- Generación de logs

MODBUS: Protocolo serial de comunicación abierto, con configuración maestro-esclavo el cual permite comunicar dispositivos electrónicos a través de los estándares RS232/RS485/RS422, algunos aspectos encontrados para este protocolo son:

- Acceso de datos: Read/Write, modificar estructura de archivos
- Registro de archivos: Logs
- Ningún aspecto de seguridad: No autenticación, no encriptación, sin seguridad
- Identificación sencilla de los dispositivos

IEC61850: Estándar de redundancia utilizado en subestaciones eléctricas, para suplir la necesidad de alta disponibilidad de los equipos, utiliza como medio físico por lo general la fibra óptica, aunque dependiendo de los recursos algunas empresas utilizan medios de cobre como el cable Ethernet, algunas aspectos encontrados para este protocolo son:

- TLS
- Medios guiados gestionados por conexiones remotas a través de aplicaciones web sin seguridad
- Generación de logs

Ahora, obtenemos una gráfica de cuantas subestaciones utilizan dichos protocolos, para verificar por cantidad donde podemos presentar mayores riesgos según el protocolo que se utilice, es de anotar que de las 63 subestaciones del área de cobertura de la organización algunas cuentan con configuraciones especiales de arquitectura del sistema SCADA, es decir cuentan con distintos equipos, distintos niveles de tensión, distintos software SCADA, lo que las vuelve aún más particular a la hora de relacionar los datos y encontrar los posibles riesgos. No se va a realizar análisis por cada una, la idea es verificar que tipos de logs se obtienen según el protocolo y configuración del sistema dentro de la subestación:

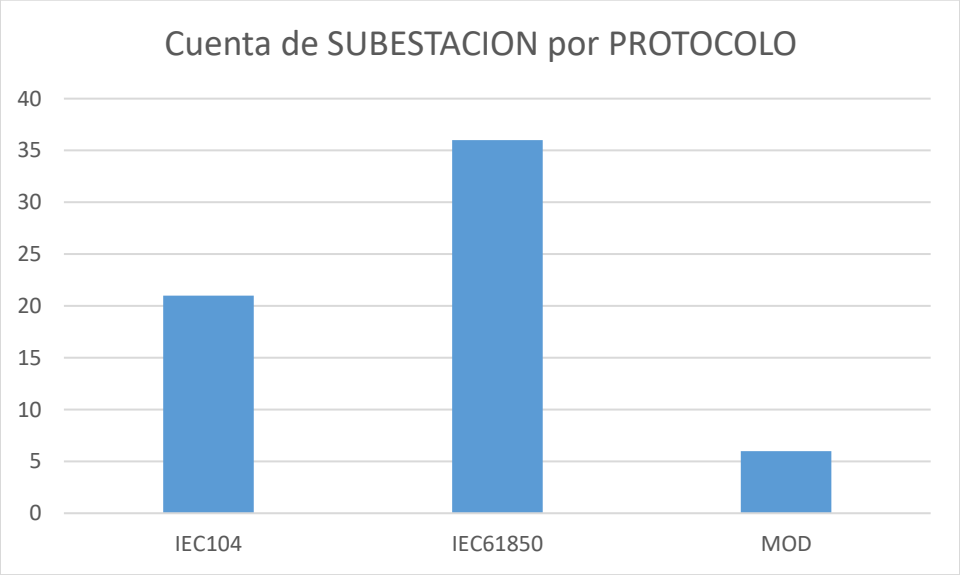


Tabla 1. Cuenta de Subestación por protocolo

Dentro de las diferentes configuraciones al sistema SCADA, se tienen como ya se dijo, diferentes equipos que sirven como totalizador o concentrador de la información, estos equipos suelen ser los Servidores utilizados para correr la aplicación SCADA necesaria para obtener las variables eléctricas de la subestación. Estos servidores están en la mitad de la red y funcionan en cierta medida como Gateways que convierten los diferentes protocolos y ejecutan el envío de información dependiendo de la funcionalidad. Para este caso la mayoría de equipos están soportados en algún tipo de Windows Server, ya sea 2008 o superior. Se plantea ejecutar el inventario de activos Críticos a analizar los logs, su respectivo sistema operativo y la aplicación ejecutada en dichas máquinas; esto con el fin de identificar a que dispositivos se le va a aplicar el análisis de logs respectivo:

SUB	SERVIDOR	MARCA	S.O.	MicroSCADA
1	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
2	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
3	SYS600C	ABB	Windows Server2008R2	MicroSCADA Base System 9.3 FP2 HF3
4	ADVANTECH	ADVANTECH	Windows Server2008R2	MicroSCADA Base System 9.4 FP1 HF2
5	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
6	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
7	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
8	SYS600C	ABB	Windows Server2008R2	MicroSCADA Base System 9.3 FP2 HF3
9	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
10	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
11	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
12	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
13	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
14	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
15	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
16	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
17	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
18	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2
19	SYS600C	ABB	Windows Server2012 R2	MicroSCADA Base System 9.4 FP1 HF2

Tabla 2. Sistemas operativos según la subestación y aplicación SCADA utilizada

- Se toma como muestra 19 subestaciones las cuales son llamadas como suebstaciones Críticas o Mayores, por su nivel de complejidad frente al nivel de tensión que manejan los activos (115kV o 230kV) y por su influencia en el sistema de interconectado nacional.
- Adicional a eso, por la configuración del sistema SCADA en estas subestaciones (Protocolos), estos ciber activos tienen la manera de entregar logs tanto del sistema operativo en el que se soporta como en la aplicación que se utiliza.

Software afectado

Sistema operativo	Impacto máximo en la seguridad	Clasificación de gravedad agregada	Boletines reemplazados por esta actualización
Windows Server 2008 para sistemas de 32 bits Service Pack 2 **	Ejecución remota de código	Importante	Ninguno
Windows Server 2008 para sistemas basados en x64 Service Pack 2 **	Ejecución remota de código	Importante	Ninguno
Windows Server 2008 para sistemas basados en Itanium Service Pack 2	Ejecución remota de código	Importante	Ninguno
Windows Server 2008 R2 para sistemas basados en x64 y Windows Server 2008 R2 para sistemas basados en x64 Service Pack 1 **	Ejecución remota de código	Importante	Ninguno
Windows Server 2008 R2 para sistemas basados en Itanium y Windows Server 2008 R2 para sistemas basados en Itanium Service Pack 1	Ejecución remota de código	Importante	Ninguno

Figura 6. Vulnerabilidades del Windows Server 2008. *(ver: Referencia 7)*

Vulnerabilities By Weakness Types

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2013	17	5			1						5
2014	4	4				1					7
2015	14	22			1	1					21
2016	19	9				3					16
2017	21	4		1				2			30
2018	6	4		1				2			15
2019	1	24			1			10			21
2020	2	18									9
2021	1	6			1						2
2022		3									
2023		1									
Total	85	100		2	4	5		14			126

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2013	18		2	13	1
2014	11	1	8	9	3
2015	46	2	45	17	25
2016	42	15	91	8	28
2017	51	2	51	24	110
2018	33	1	47	12	65
2019	117	1	79	25	86
2020	84		241	13	85
2021	101		115	22	61
2022	131		174	38	50
2023	162		118	67	62
Total	796	22	971	248	576

Figura 7. Vulnerabilidades del Windows Server 2012. *(ver: Referencia 8)*

- Para realizar un análisis rápido de vulnerabilidades para la aplicación SCADA utilizada, debemos incurrir en ambientes virtualizados controlados, con permisos de la organización y con supervisión del personal de Seguridad. Se plantea esta opción al equipos de Soporte a Tecnologías de la Operación para intentar verificar que vulnerabilidades posee la aplicación, se pueden brindar herramientas como Nessus para dicho análisis, la cual nos brindará un panorama inicial y minucioso de que tipo de vulnerabilidades puede presentar la aplicación MicroScada de ABB.
- Frente al sistema Operativo, se realizan consultas iniciales en algunas páginas referenciadas para tal fin, como se puede observar a través de los años se han presentado ciertos tipos de amenazas que podrían incluso ejecutar código en las máquinas de control de subestaciones, para verificar el estado actual de dichas máquinas también se requiere

coordinación previa con el personal de Seguridad y TO para llevar a cabo esta actividad.

Para este caso se utilizan datos actualizados y referenciados de la red donde vemos los posibles riesgos que se pueden presentar utilizando estos sistemas operativos.

Logs que se requieren analizar

Los sistemas SCADA presentados nos brindan la oportunidad de almacenar y analizar los logs para los servidores mencionados, la aplicación SCADA utilizada para la supervisión de los activos eléctricos críticos de la subestación y también nos debe mostrar un registro de logs de acceso a dicha máquina. Para este proyecto, se realizará un análisis a detalle como cuota inicial de estas 3 posibles fuentes de información que van a mostrar los accesos indebidos o no a los servidores SCADA, el registro de configuración de la aplicación, el registro de eventos anómalos en el sistema eléctrico, y con ello se buscará dar respuesta a los objetivos inicialmente planteados.

Logs de Windows Server:

Windows nos brinda gran variedad de herramientas según la versión de sistema operativo que se tenga para servidores. En este caso, observamos que desde la administración del equipo nos brinda distintas categorías de Logs generados por el sistema; entre ellos logs de: Aplicación, Seguridad, Configuración, Sistema, etc. Con esta variedad se fundamenta y se proyecta la actividad de revisión de logs en el sistema operativo de los servidores SCADA. Para plantear que tipo de logs de estos se deben analizar y gestionar en alguna herramienta para tener respuesta oportuna frente a algún incidente de ciberseguridad, se debe tener claro que información suministra cada uno de estos logs y automatizar el análisis.

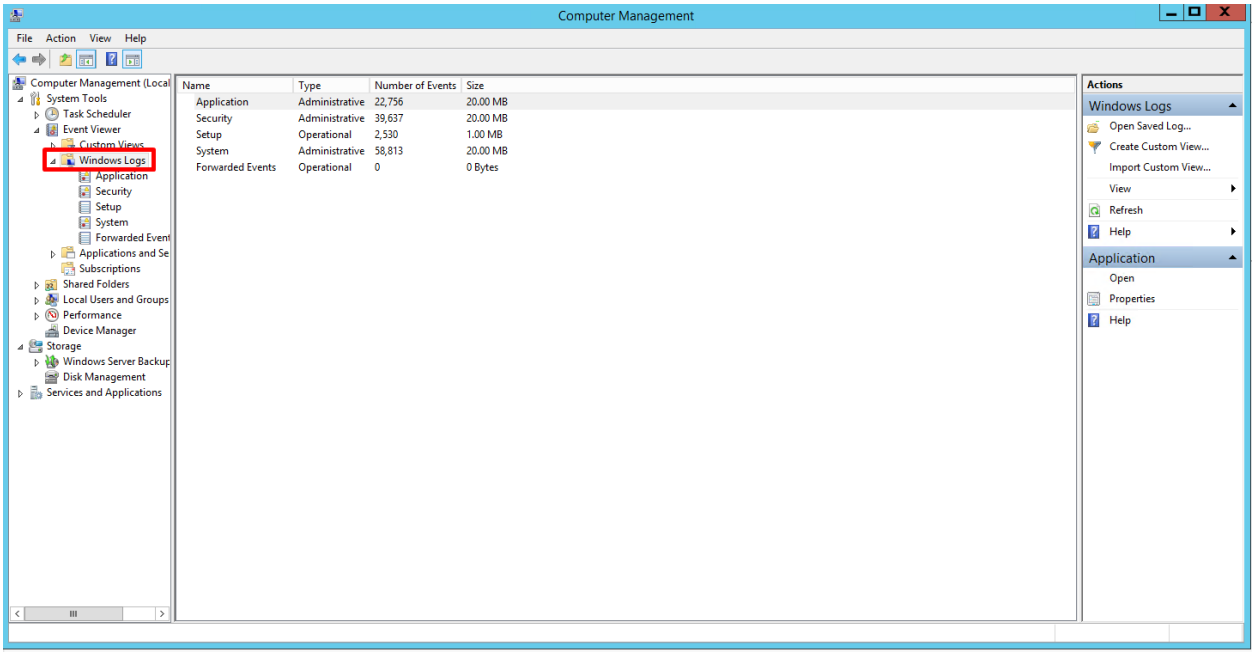


Figura 8. Administrador del equipo Servidor SCADA, imagen de equipo propio

- Frente a las. clasificaciones de Logs, el proceso de Soporte a Tecnologías de Operación debería enfocarse en analizar e interpretar de mejor manera los logs referentes a la seguridad de Windows. identificar patrones y utilizar herramientas de análisis para llegar a tener conclusiones que brinden soluciones para la prevención de riesgos en los ciber activos críticos de la operación

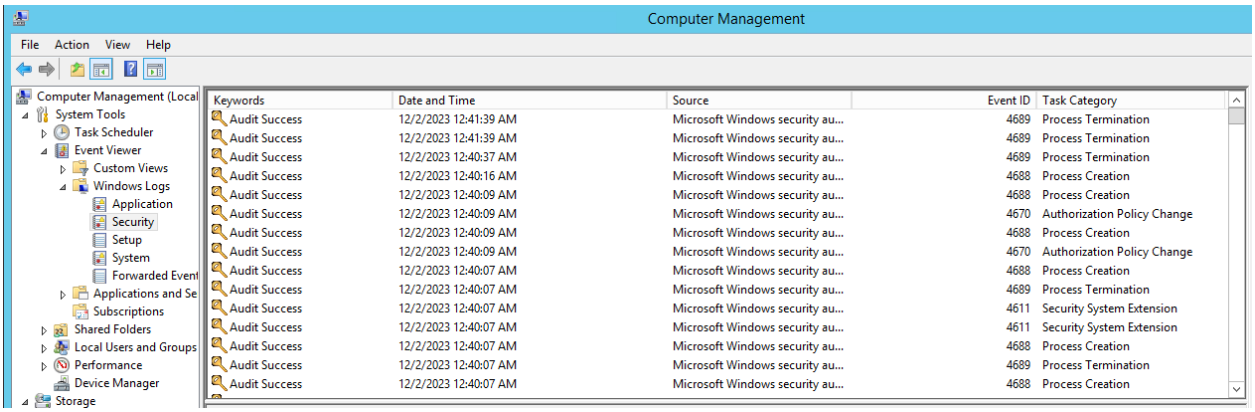
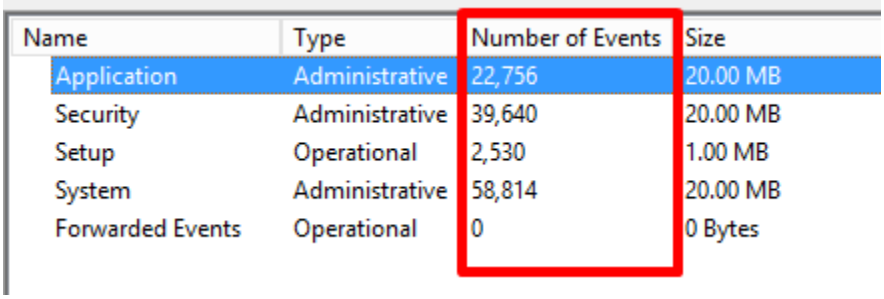


Figura 9. Logs de Seguridad de Windows Server 2012, imagen de equipo propio

- También se debe contemplar la cantidad de registros generados por el Sistema operativo analizado (WS2012), el cual se vuelve parte importante en dicho análisis, ya que requerirá un gran esfuerzo saber que logs se deben contemplar para el análisis y cuales no. Para eso se debe plantear algún mecanismo que nos lleve a mejorar en eficacia y respuesta a este análisis:

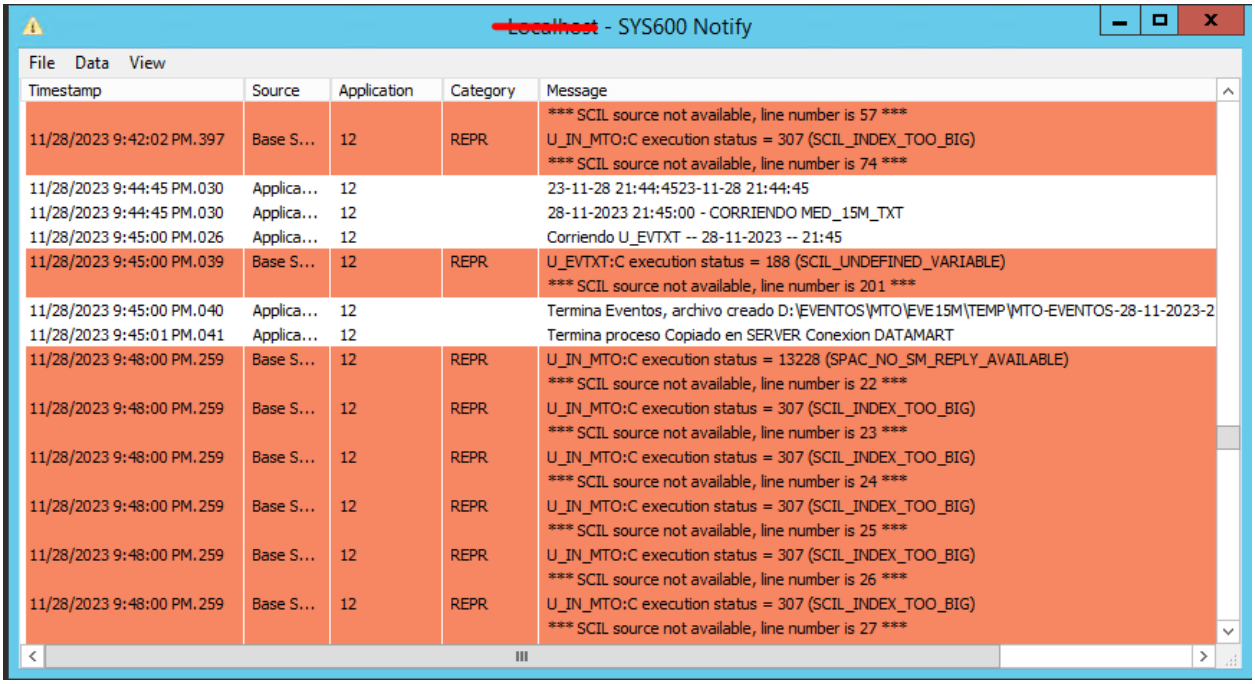


Name	Type	Number of Events	Size
Application	Administrative	22,756	20.00 MB
Security	Administrative	39,640	20.00 MB
Setup	Operational	2,530	1.00 MB
System	Administrative	58,814	20.00 MB
Forwarded Events	Operational	0	0 Bytes

Figura 10. Número de eventos generados por los diferentes logs, imagen de equipo propio

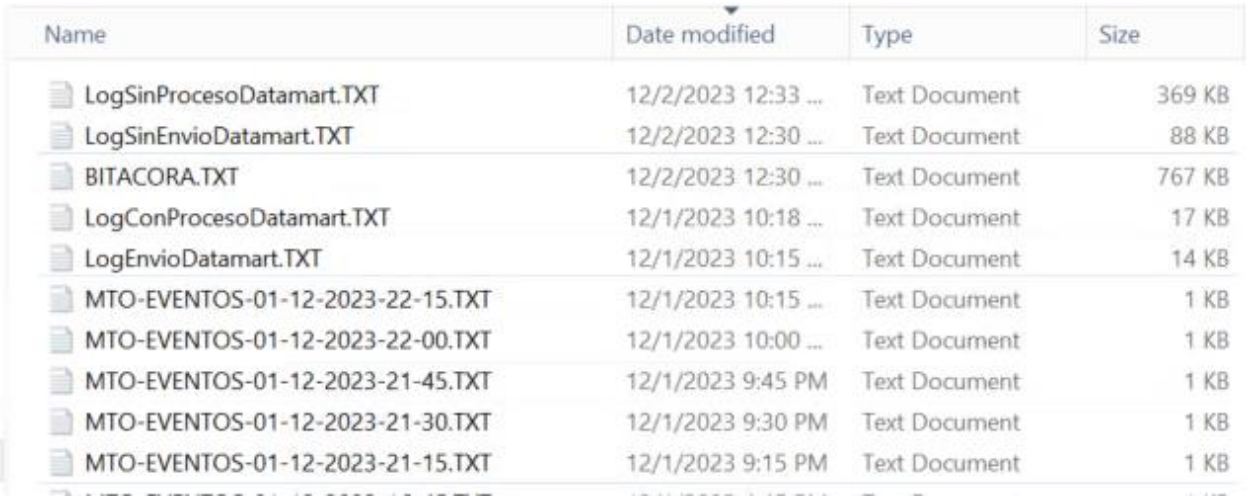
Logs de Aplicación SCADA (MicroScada ABB)

La aplicación MicroScada del proveedor ABB, es la herramienta utilizada para adquirir datos de las variables eléctricas y supervisarlos, los muestra en una interfaz Hombre-Máquina (HMI), la cual entrega información detallada y gráficamente de los equipos de campo, este software maneja información de los diferentes protocolos con los que es capaz de interactuar el sistema. Hay algunos logs, relacionados directamente con el funcionamiento de la aplicación y otros logs que sirven para verificar accesos, configuraciones, enlaces con otras aplicaciones y automatismos:



Timestamp	Source	Application	Category	Message
11/28/2023 9:42:02 PM.397	Base S...	12	REPR	*** SCIL source not available, line number is 57 *** U_IN_MTO:C execution status = 307 (SCIL_INDEX_TOO_BIG) *** SCIL source not available, line number is 74 ***
11/28/2023 9:44:45 PM.030	Applica...	12		23-11-28 21:44:4523-11-28 21:44:45
11/28/2023 9:44:45 PM.030	Applica...	12		28-11-2023 21:45:00 - CORRIENDO MED_15M_TXT
11/28/2023 9:45:00 PM.026	Applica...	12		Corriendo U_EVTXT -- 28-11-2023 -- 21:45
11/28/2023 9:45:00 PM.039	Base S...	12	REPR	U_EVTXT:C execution status = 188 (SCIL_UNDEFINED_VARIABLE) *** SCIL source not available, line number is 201 ***
11/28/2023 9:45:00 PM.040	Applica...	12		Termina Eventos, archivo creado D:\EVENTOS\MTO\EVE15M\TEMP\MTO-EVENTOS-28-11-2023-2
11/28/2023 9:45:01 PM.041	Applica...	12		Termina proceso Copiado en SERVER Conexion DATAMART
11/28/2023 9:48:00 PM.259	Base S...	12	REPR	U_IN_MTO:C execution status = 13228 (SPAC_NO_SM_REPLY_AVAILABLE) *** SCIL source not available, line number is 22 ***
11/28/2023 9:48:00 PM.259	Base S...	12	REPR	U_IN_MTO:C execution status = 307 (SCIL_INDEX_TOO_BIG) *** SCIL source not available, line number is 23 ***
11/28/2023 9:48:00 PM.259	Base S...	12	REPR	U_IN_MTO:C execution status = 307 (SCIL_INDEX_TOO_BIG) *** SCIL source not available, line number is 24 ***
11/28/2023 9:48:00 PM.259	Base S...	12	REPR	U_IN_MTO:C execution status = 307 (SCIL_INDEX_TOO_BIG) *** SCIL source not available, line number is 25 ***
11/28/2023 9:48:00 PM.259	Base S...	12	REPR	U_IN_MTO:C execution status = 307 (SCIL_INDEX_TOO_BIG) *** SCIL source not available, line number is 26 ***
11/28/2023 9:48:00 PM.259	Base S...	12	REPR	U_IN_MTO:C execution status = 307 (SCIL_INDEX_TOO_BIG) *** SCIL source not available, line number is 27 ***

Figura 11. Log del Notify, aplicación SCADA, imagen de equipo propio



Name	Date modified	Type	Size
LogSinProcesoDatamart.TXT	12/2/2023 12:33 ...	Text Document	369 KB
LogSinEnvioDatamart.TXT	12/2/2023 12:30 ...	Text Document	88 KB
BITACORA.TXT	12/2/2023 12:30 ...	Text Document	767 KB
LogConProcesoDatamart.TXT	12/1/2023 10:18 ...	Text Document	17 KB
LogEnvioDatamart.TXT	12/1/2023 10:15 ...	Text Document	14 KB
MTO-EVENTOS-01-12-2023-22-15.TXT	12/1/2023 10:15 ...	Text Document	1 KB
MTO-EVENTOS-01-12-2023-22-00.TXT	12/1/2023 10:00 ...	Text Document	1 KB
MTO-EVENTOS-01-12-2023-21-45.TXT	12/1/2023 9:45 PM	Text Document	1 KB
MTO-EVENTOS-01-12-2023-21-30.TXT	12/1/2023 9:30 PM	Text Document	1 KB
MTO-EVENTOS-01-12-2023-21-15.TXT	12/1/2023 9:15 PM	Text Document	1 KB

Figura 12. Logs de automatización de tareas de eventos, imagen de equipo propio

Logs de Accesos Remotos

Los registros del sistema Windows nos brinda información general de accesos remotos por RDP o VNC, para este caso hay otro tipo de herramientas que facilitan el control de acceso a los diferentes equipos de SCADA. Dicha herramienta brinda información importante que puede ayudar a interpretar de mejor

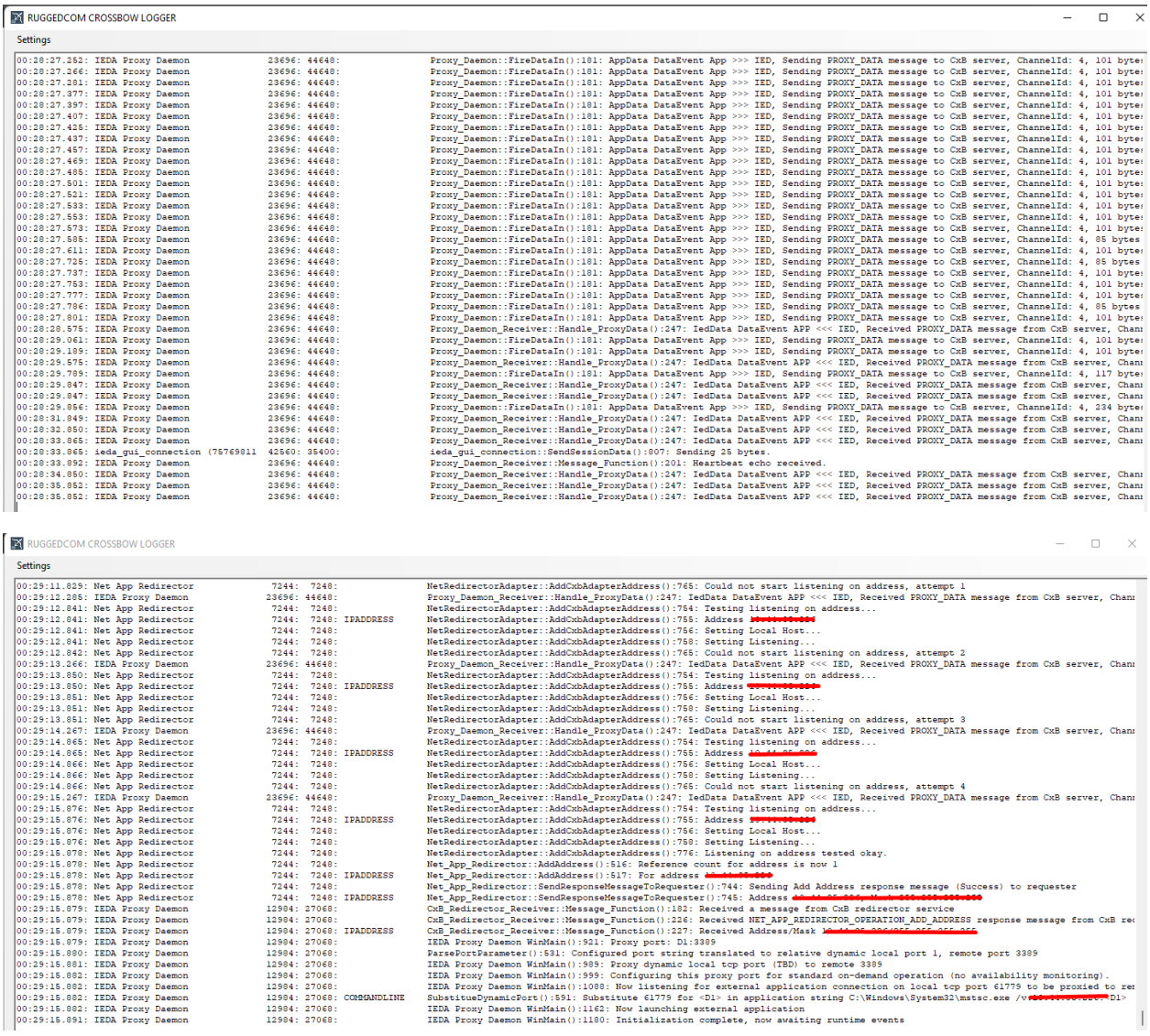


Figura 13. Logs de Crossbow, herramienta para control de accesos, imagen de equipo propio

HERRAMIENTAS PARA UTILIZAR EN EL ANÁLISIS DE LOGS

Se investigan algunas herramientas que pueden ayudar en esta tarea, hay cantidad innumerable de software que puede servir como base para empezar con este trabajo. Algunos ejemplos son:

Loggly:

Es una herramienta en la nube para la administración de registros (logs), llama la atención esta herramienta por su disponibilidad en un sistema protegido por datos en la nube y que brinda información en tiempo real al usuario final. Puede utilizar estándares HTTP y SysLog y se evita instalar algún software complicado o riesgoso para el sistema SCADA.

Algunas de sus funciones principales son:

- Recopilar e interpretar registros (logs) de texto de cualquier fuente, sea cliente o servidor
- Utiliza un algoritmo de búsqueda para realizar tipos de búsqueda según valores establecidos
- Contiene un panel de análisis de datos para otorgar visibilidad estratégica con los logs a analizar.

Esta aplicación tiene una versión "lite", la cual no tiene costo y permite realizar hasta cierto número de análisis con determinada cantidad de eventos. Después, ofrece unas versiones Standard, Pro y Enterprise que según su membresía puede utilizar y realizar un seguimiento de mayor cantidad de datos, o automatizar algún tipo de tarea.

Esta solución, es un poco distinguida en la organización aunque sin ninguna implementación por falta de investigación en esta área; sin embargo presenta características importantes que llaman la atención para brindar una solución.

Figura 14. Interfaz y panel de control aplicación Loggly. *(Ver: referencia 9)*

SPLUNK:

Es una herramienta en la gestión de registros (logs) y eventos que busca diagnosticar e informar dichos eventos relacionados con datos mediante indexación y análisis de logs de cualquier tipo, esto incluye aplicaciones estructuradas (Software SCADA), no estructuradas o de cualquier sistema operativo.

Algunas de sus funciones principales son:

- Entender datos de las máquinas de cualquier tipo (Servers, IEDs, Mainframes, protocolos de red).
- Interfaz de usuario para buscar y analizar datos en tiempo real
- Capaz de generar informes utilizando automatismos según criterios dados.

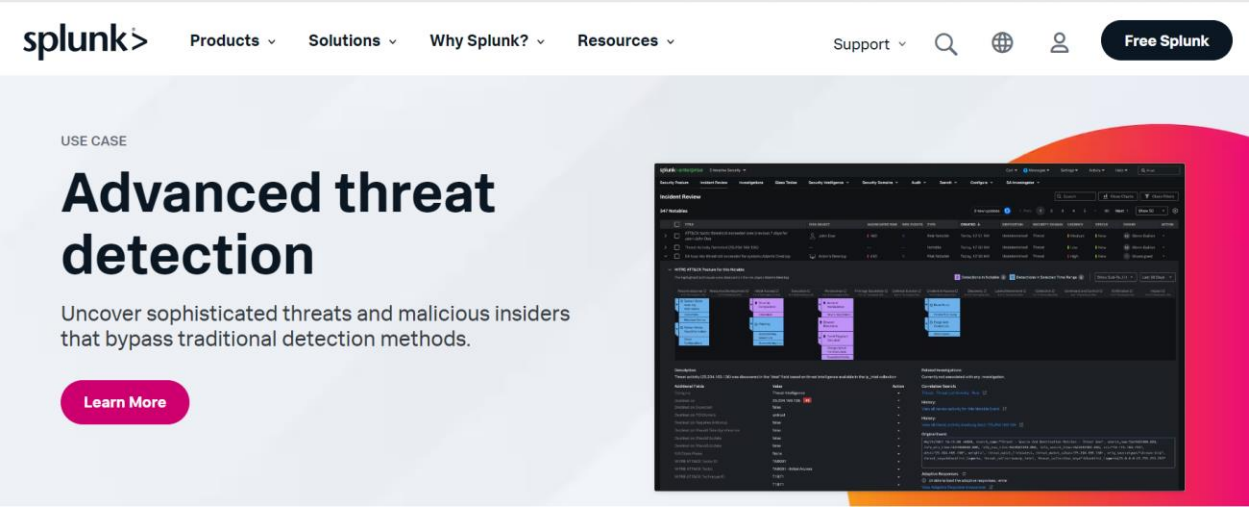


Figura 15. Link de descarga de SPLUNK. *(Ver: referencia 10)*

Este software tiene una parte de la distribución de uso "*Free*", sin embargo en su documentación de licenciamiento, indica que es "a pedido"; lo que quiere decir que es según la necesidad de la organización. Este tema es debatible dentro de algunas empresas porque se requiere tener claro el alcance del sistema y sus requerimientos para llegar a un acuerdo que brinde un soporte global a la herramienta después de su implementación. Sin embargo, llama la atención algunas bondades que tiene SPLUNK como la interfaz de usuario que presenta, su facilidad a la hora de parametrizar reportes y las entregas visuales de dichos informes.

Hay otra cantidad de herramientas que como se menciona al inicio, son incontables y según las necesidades de la organización se deben seguir investigando y poder definir cual es la más útil para realizar el análisis en sistemas SCADA.

De las herramientas expuestas, se tiene conocimiento básico y empírico del funcionamiento, se tomaron como ejemplo porque fueron las primeras fuentes de análisis de este proyecto y de esta manera se intenta consultar, analizar e interpretar que tipos de herramientas son las más adecuadas, sin embargo se encuentran otras herramientas que según su licenciamiento, la empresa que lo desarrolla y el enfoque y metodología que utilizan son más costosas y especializadas en Identificación Temprana de Amenazas, tanto para sistemas en tiempo real como cualquier tipo de sistema que deba proteger datos.

Algunos ejemplos son:

- McAffe Enerprise: Gestión de registros (logs) de cualquier tipo de sistema; Bases de datos, Redes, Servidores, Aplicaciones, sistemas operativos
- SolarWinds Log & Event Manager: Gestor de eventos y registros, especializado en inteligencia de amenazas, remediación en tiempo real, monitoreo de integridad de archivos.
- ManageEngine EventLog Analyzer: Herramienta de IT para gestión de logs basado en un SIEM (Security Information and Event Management), esta opción suele brindar grandes oportunidadades de automatización del análisis y respuesta temprana incidentes.

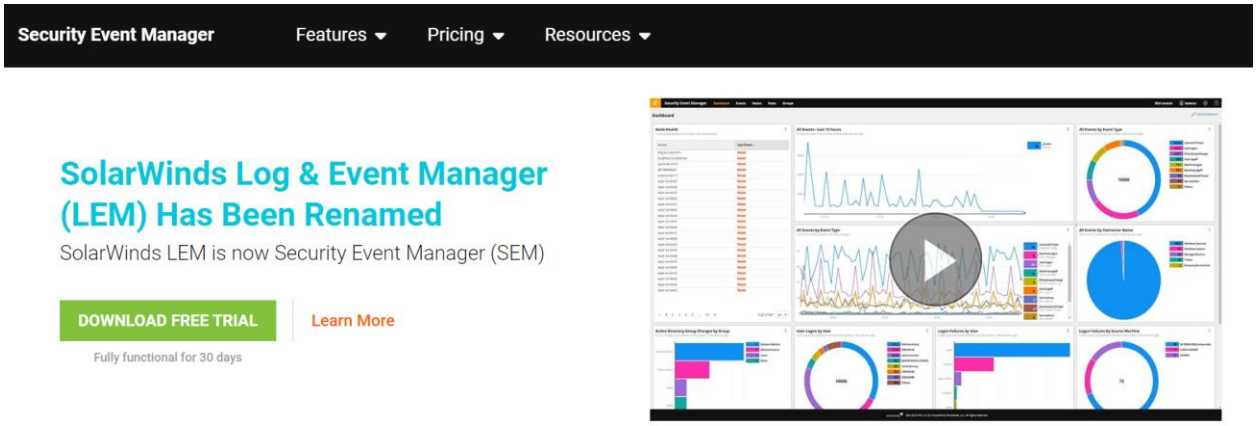


Figura 16. Imagen de referencia SolarWinds Log and Event Manager. *(Ver: referencia 11)*

DATOS DE AUDITORÍA Y REGISTRO DE BACKUPS

La idea de implementar esta actividad es tener el personal capacitado para la atención temprana de incidentes de ciberseguridad en ambientes de operación y sistemas SCADA, brindar alternativas para el análisis y cuidad de la información fundamental para los ciber

activos críticos del sistema eléctrico y adicional a eso fundamentar y aplicar los principios de la seguridad de la información a ambiente de Tecnologías de la Operación, apuntando principalmente a la disponibilidad del sistema.

Con base en esto, se da una investigación inicial a los datos analizados, con el fin de no realizar pruebas en sistemas que se encuentran activos y funcionando en tiempo real, adicional a eso no se tiene licencias ni conocimiento suficiente para implementar algún tipo de software mencionado sobre alguno de los equipos relacionados en este documento. Todos los datos de la disponibilidad de los activos que están reportados a entes regulatorios como el XM o Centro Nacional de Despacho, son de vital importancia para el principio de la calidad de la energía eléctrica. Por esta razón se conservan los datos intactos, solo se utilizan accesos de consulta y verificación con fines investigativos.

También, se conservan los backups de las máquinas consultadas previamente en el repositorio indicado por personal de TO de la organización, con el fin de garantizar el restablecimiento por algún tipo de paso indebido o mala configuración por parte de esta actividad de análisis de logs.

8. Análisis de resultados

Como se menciona anteriormente algunas soluciones también se basan en otra metodología como implementar un SIEM (Security Information and Event Management), la implementación de dichos procesos suele convertirse en una ardúa tarea de directivos, personal de TO/TI, personal de seguridad y algunas partes interesadas para esta labor. Aunque se convierte en una buena práctica de seguridad y quizás el cumplimiento de alguna política definida por la empresa, se deben contemplar otras alternativas que puedan brindar la solución y que estén al alcance de los recursos existente.

Una metodología encontrada dentro de la bibliografía citada, es la llamada MELISSA (Mining Event Logs for Intrusion in SCADA Systems), es una metodología que en un tipo de dagrama de flujo parece ser sencilla y evidencia algunas posibilidades de empezar a realizar un laboratorio real con los equipos disponibles. El proceso se centra en identificar los logs de los sistemas a analizar, realizar un barrido de información y detectar cambios y registros anómalos, prepara la información en un concentrador y utilizar una especia de motor de patrones que identifique estos comportamientos extraños, los liste, los depure y los entregue en un informe de eventos de Patrones de SCADA, todo esto se resume en el siguiente diagrama:

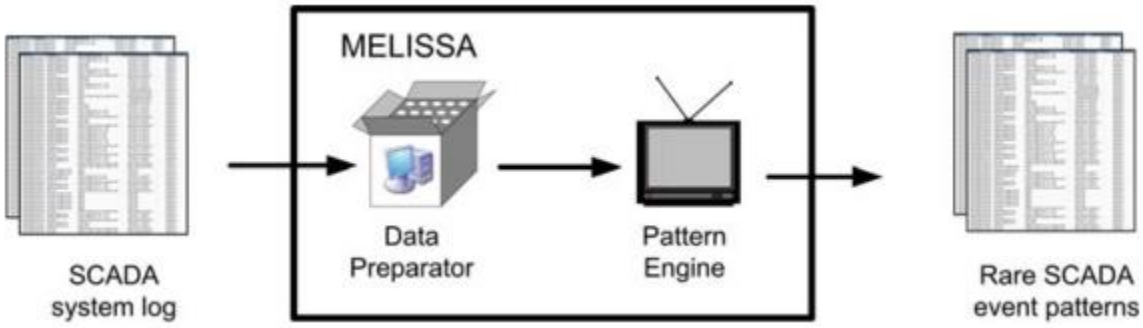


Figura 17. Imagen sacada del artículo: A log mining approach for process monitoring in SCADA ver referencia. (*Ver: referencia 12)*

El siguiente diagrama de flujo muestra el paso a paso de otra alternativa de análisis de logs. Empezando con la recolección de los logs a analizar, procesamiento de dicha data, después existen dos técnicas de minería de patrones, A priori y FP, las cuales ejecutan algoritmos que entregan los resultados de dicho análisis. En esta metodología surgen términos nuevos, sin embargo al parecer el tema tiene gran profundidad y en el artículo del cual se extrae este diagrama se detalla como se debe realizar cada actividad que implica y como se debe realizar:

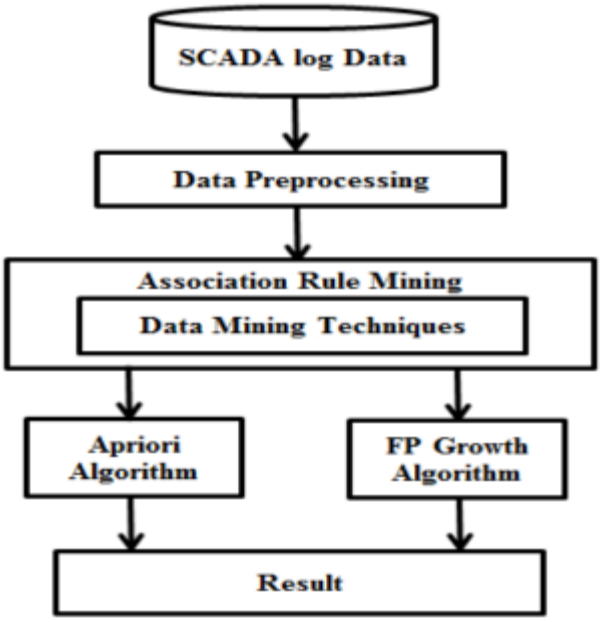


Figura 18. Diagrama de flujo extraído del artículo: Detection of Undesired Events on Real-World SCADA Power System through Process Monitoring. *(Ver: referencia 13)*

9. Conclusiones

- Se identifican y se caracterizan los dispositivos y los logs a identificar dentro de un sistema SCADA, y se precisan algunas herramientas que se pueden utilizar durante la implementación, se debe seguir profundizando en el uso seguro de dichas herramientas para no afectar procesos que demandan el principio de disponibilidad.

- Se obtiene información de ciertos procesos que se deben mejorar respecto a buenas prácticas de ciberseguridad y que apunten directamente a los acuerdos y políticas de la empresa respecto a la seguridad de la información, con el fin de implementar una herramienta o un procedimiento para el análisis de logs, inicialmente se debe tener claro que requisitos y recursos se disponen para implementar dichos procesos y procedimientos.

- No fue posible capacitar al personal de TO en este lapso, se concluye que se deben tener claros los lineamientos normativos, tanto internos como externos y los que cubren el sector eléctrico, con el fin de proteger la información Operativa del sistema de supervisión y control.

10. Referencias bibliográficas

Macaulay, Tyson (2011) "Cybersecurity for Industrial Control Systems: Scada, DCS, PLC, HMI, and SIS"

1. Imagen extraída de las aplicaciones corporativas de CHEC: SIG. Sistema de Información Geográfico. Área de Cobertura CHEC.

2. Imagen de Niveles de Control de un Sistema SCADA: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.facebook.com%2Finelinc%2Fphotos%2Fniveles-de-control-en-subestaciones-el%25C3%25A9ctricas%25EF%25B8%258F-desde-el-punto-de-vista-del-cont%2F704818106780285%2F&psig=AOvVaw1-Xn8-QhV6F7GfgrO6bLmt&ust=1695763445291000&source=images&cd=vfe&opi=89978449&ved=0CBIQjhxqFwoTCPC8qajZxoEDFQAAAAAdAAAAABAO

3. Noticias Citadas: Ataques a sistemas SCADA, consulta en Google

Link 1

https://www.bbc.com/mundo/noticias-60850173#:~:text=En%202015%2C%20la%20red%20el%C3%A9ctrica,en%20el%20oeste%20de%20Ucrania.&text=Pie%20de%20foto%2C,visto%20afectada%20anteriormente%20por%20ciberataques.

Link 2

https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/1222-el-gusano-stuxnet-que-afecta-a-sistemas-scada-causa-revuelo-internacional.html

4. Arquitectura y protocolos de un sistema SCADA: Imagen extraída del documento: S. Mohagheghi, J. Stoupis and Z.Wang. Communication Protocols and networks for power systems-current status and future trends. In power Systems conference an exposition, 2009. PSCE '09. IEEE/PES, March 2009

5. Imagen extraída de documentos internos en CHEC, Matriz de riesgos de activos críticos de una subestación eléctrica

6. Imagen extraída de documentos internos en CHEC, Valoración de riesgos de activos críticos de una subestación eléctrica

7. Imagen Vulnerabilidades identificadas para SO Windows Server 2008: Extraído desde https://learn.microsoft.com/es-es/security-updates/securitybulletins/2012/ms12-012

8. Imagen Vulnerabilidades identificadas para SO Windows Server 2012: Extraído desde

https://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26

9. Link de acceso a Loggly: Herramienta para automatización de Logs https://betterstack.com/logs?utm_medium=c&utm_campaign=adwords19703922957&utm_so

urce=adwords&utm_content=648793502879&utm_term=loggly&gad_source=1&gclid=EAIaIQobChMI1pS1nJr3ggMV5KRaBR1D_QulEAAYASAAEgL-BfD_BwE

10. Link de acceso a SPLUNK: Herramienta para detección de amenazas https://www.splunk.com/en_us/solutions/advanced-threat-detection.html

11. Link de acceso a Solarwinds:

https://www.solarwinds.com/security-event-manager/use-cases/log-event-manager-software

12. Artículo encontrado llamado: A log mining approach for process monitoring in SCADA.

13. Diagrama de flujo extraído del artículo: Detection of Undesired Events on Real-World SCADA Power System through Process Monitoring: Link:

https://hsnarman.github.io/CONF/20-UEMCON-Scada.pdf

Universidad®
Católica
de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia
de la Congregación

Hermanas de la Caridad
Dominicas de La Presentación
de la Santísima Virgen

Universidad Católica de Manizales
Carrera 23 # 60-63 Av. Santander / Manizales - Colombia
PBX (6)8 93 30 50 - www.ucm.edu.co