SANS

Analyst Program

Descripción del producto

Implementación efectiva del marco de ciberseguridad NIST con Fortinet

Artículo original escrito por **Don C. Weber**
Actualizado por **Jason Dely**

Febrero de 2020
Actualizado en marzo de 2023

FORTINET

Introducción: Desafíos de las redes ICS y TI conectadas

Implementar ciberseguridad nunca es sencillo, y este es particularmente el caso de empresas que ejecutan sistemas de control industrial (ICS) y otras tecnologías operativas (OT).

OT brinda funcionalidad especializada para tareas específicas y esa funcionalidad especializada no se ajusta a las prácticas de seguridad comunes para proteger una red de TI corporativa. Los equipos de seguridad no pueden imponer políticas, estándares y procedimientos de red de TI en los procesos y la tecnología de la red OT. En cambio, deben abordar los sistemas, dispositivos y protocolos únicos configurados en la OT (o las dependencias operativas relacionadas con los requisitos funcionales de un ICS). De no hacerlo, los requisitos de seguridad de TI se diluirán, se rechazarán formalmente o simplemente se ignorarán, lo que pondrá en peligro las operaciones de la empresa. Las redes OT suelen estar conectadas a la red de TI y, cada vez más, están vinculadas a recursos conectados a Internet, como sistemas basados en la nube, todos ellos posibles vectores de entrada de malware que podrían interrumpir operaciones críticas.

Este artículo revisa el enfoque basado en NIST para implementar la seguridad en un entorno de control industrial (ICS/OT), haciendo referencia al Marco de Ciberseguridad NIST[1] (CSF), a los cinco controles críticos de ciberseguridad del SANS Institute que son más relevantes para los ICS, y a las tecnologías del Fortinet Security Fabric[2]. También examinamos cómo respaldar e implementar eficazmente el NIST CSF y exploramos cómo algunas de las ofertas de ciberseguridad de Fortinet pueden ayudar a una organización a cumplir con su hoja de ruta de seguridad ICS/OT.

Origen del marco de ciberseguridad del NIST

Desde la implementación de la Ley de Seguridad e Independencia Energética de 2007 (EISA)[3], NIST ha estado ayudando directamente a la industria de servicios públicos con el desarrollo de estándares para la interoperabilidad y seguridad de la red eléctrica inteligente de EE. UU. Si bien este esfuerzo proporcionó una base de seguridad sólida para el sector energético, los estándares no pudieron aplicarse fácilmente a otras infraestructuras críticas y sectores no regulados de la economía.

De alguna manera, los sectores que deben trabajar bajo regulaciones que dictan los objetivos que debe alcanzar el programa de seguridad de una organización mediante la implementación de controles de ciberseguridad tienen una ventaja. Estos sectores han experimentado, a veces durante décadas, el proceso de traducir estándares, marcos y directrices a programas centrados en los profesionales. Algunos organismos de normalización maduros permiten mejoras en las normas y capacidad de aplicación para medir el cumplimiento.

Sin embargo, las organizaciones no reguladas deben formular su propio enfoque en materia de ciberseguridad. Sin embargo, a menudo se topan con algunas dificultades que no siempre comparten sus contrapartes reguladas. La primera es la ausencia de objetivos claramente definidos que serán respaldados por el programa de seguridad. Las otras son la falta de experiencia y la falta de financiación, que pueden impedir la ejecución y el mantenimiento efectivos del programa de seguridad.

Las deficiencias de EISA se abordaron en 2013, cuando el presidente Obama firmó la Orden Ejecutiva 13636, "Mejora de la ciberseguridad de las infraestructuras críticas".[4] Encargó al NIST que brindara orientación para mejorar la postura de seguridad de todos los sectores de infraestructura crítica. El resultado fue el NIST CSF, que demostró ser lo suficientemente flexible como para mejorar los programas de seguridad en el sector de infraestructura crítica y también en los sectores no regulados. Para obtener antecedentes y orientación más específicos sobre la implementación del NIST CSF, consulte el documento SANS "Security by Design: A Systems Road Map Approach."[5]

[1] Cybersecurity Framework, NIST, www.nist.gov/cyberframework

[2] Fortinet Security Fabric, www.fortinet.com/solutions/enterprise-midsize-business/enterprise-security.html

[3] Energy Independence and Security Act of 2007, www.epa.gov/greeningepa/energy-independence-and-security-act-2007

[4] Executive Order—Improving Critical Infrastructure Cybersecurity, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[5] "Security by Design: A Systems Road Map Approach," SANS Institute, 16 de enero de 2020, www.sans.org/reading-room/whitepapers/analyst/security-design-systems-road-map-approach-39370. (Es necesario registrarse para acceder).

Identificación de esfuerzos operativos y tácticos

El marco de ciberseguridad NIST (NIST CSF) ha sido utilizado con éxito por muchas organizaciones para moldear sus programas de seguridad específicos para OT, y ha demostrado ser adaptable para sus propósitos. El personal de TI y OT encargado de implementar los pasos tácticos a corto y mediano plazo necesarios para alcanzar los objetivos estratégicos de seguridad establecidos para el ICS también debe mantener los requisitos operativos fundamentales de la organización. En cuanto a las organizaciones, prefieren modificar su ICS existente porque es menos costoso que empezar desde cero. También prefieren minimizar las modificaciones realizadas a su arquitectura y operaciones de ICS, favoreciendo las excepciones y alternativas. Un objetivo común es implementar los controles de seguridad necesarios de manera que sea rentable y sin efectos negativos en los procesos dentro de las redes OT.

Es importante que estos objetivos de implementación orientados al negocio se ajusten a un programa que un informe técnico de SANS identificó como "Los cinco controles críticos de ciberseguridad para ICS".[6] (Ver Figura 1.)

ICS INCIDENT RESPONSE

Operations-informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment

DEFENSIBLE ARCHITECTURE

Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement

ICS NETWORK VISIBILITY MONITORING

Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control

SECURE REMOTE ACCESS

Identification and inventory of all remote access points and allowed destination environments, on-demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment

RISK-BASED VULNERABILITY MANAGEMENT

Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation

Figura 1: Cinco controles críticos para la ciberseguridad ICS/OT

Como indica el informe técnico, "Las organizaciones deben tener en cuenta, especialmente si forman parte de la infraestructura crítica, que tienen la obligación de garantizar un entorno de operación seguro para su personal y la responsabilidad de proteger a las comunidades en las que operan mediante inversiones adecuadas en ciberseguridad de ICS".

Muchos de los controles del NIST CSF se centran en el aspecto preventivo de la ciberseguridad, pero sus aspectos influenciados por la TI son difíciles de implementar y pueden dar lugar a excepciones o evasiones de seguridad. Existe un valor intrínseco (y aceptación por parte de los pares) en utilizar un marco como el NIST CSF para dirigir recursos y ciberseguridad hacia los entornos de ICS/OT. Algunas organizaciones pasan años de esfuerzo enfocado en la prevención y detección, destinando un esfuerzo mínimo a las actividades de respuesta y recuperación. A pesar de que la preparación y la disponibilidad de un ICS influyen directamente en una

[6] "The Five ICS Cybersecurity Critical Controls," SANS Institute, 7 de noviembre de 2022, www.sans.org/white-papers/five-ics-cybersecurity-critical-controls (Es necesario registrarse para acceder).

operación segura y confiable, los recursos y esfuerzos deben, como mínimo, aplicarse de manera equitativa a las actividades de respuesta y recuperación del programa de ciberseguridad de ICS/OT. "Los cinco controles críticos de ciberseguridad para ICS" complementan el NIST CSF al ayudar a equilibrar el enfoque del marco, altamente orientado a la prevención.

Para obtener más información sobre NIST CSF y cómo su organización puede usarlo de la mejor manera, consulte la Guía de inicio rápido de NIST CSF.[7]

Cobertura de NIST CSF con Fortinet Security Fabric

Esta sección explora cómo las tecnologías incluidas en el Fortinet Security Fabric podrían ayudar a impulsar una implementación equilibrada del programa de seguridad ICS en las cinco funciones clave (identificar, proteger, detectar, responder y recuperar) descritas en el NIST CSF. La práctica habitual del Programa de Analistas SANS es probar manualmente en un entorno de laboratorio configurado para operaciones normales cada una de las tecnologías analizadas en nuestros artículos para comprender su solidez y sus deficiencias. Sin embargo, las redes de laboratorios de ICS son demasiado restrictivas en comparación con un entorno operativo y no pueden darnos una imagen realista.

Tecnologías del Fortinet Security Fabric

El Fortinet Security Fabric es una integración de productos de red y ciberseguridad de Fortinet (ver Tabla 1) y sus socios proveedores. Dentro de la integración, FortiManager unifica la administración y orquestación de los productos Fortinet, casi proporcionando el proverbial panel único. Otro producto de Fortinet, FortiNAC, brinda visibilidad, control y respuesta automatizada para todo lo que se conecta a la red porque puede integrarse con dispositivos de terceros. Dado que la integración es inherente al Fortinet Security Fabric, los entornos de control se benefician porque la implementación tiene un impacto mínimo en las operaciones actuales.

Tabla 1. Productos de Fortinet y sus descripciones

Producto Fortinet	Descripción del producto
FortiEDR	Ofrece protección en tiempo real y automatizada para endpoints con una respuesta de incidentes orquestada en todos los endpoints de TI y OT. La plataforma integrada ofrece opciones de implementación flexibles y un costo operativo predecible. FortiEDR ofrece mitigación de riesgos en tiempo real, seguridad de endpoints, protección previa a la infección a través de un motor antivirus de próxima generación a nivel de kernel, protección posterior a la infección y análisis forense.
FortiClient FortiClient EMS	FortiClient es un agente de endpoint que brinda visibilidad y control del inventario de software y hardware en todo el Fortinet Security Fabric, lo que permite a las organizaciones descubrir, monitorear y evaluar los riesgos de los endpoints en tiempo real. También proporciona acceso remoto seguro (cliente VPN). FortiClient, junto con FortiClient Enterprise Management Server (EMS), es una parte integral de la oferta de acceso a la red de confianza cero (ZTNA) de Fortinet e incluye funciones ZTNA como borde de servicio de acceso seguro (SASE) y funcioens de protección de endpoints (EPP): • Con ZTNA, los usuarios remotos pueden acceder a sus aplicaciones corporativas, con una autenticación estricta y una postura de seguridad del endpoint verificable antes de conceder el acceso. • Con SASE, los usuarios remotos pueden conectarse de forma segura a la red corporativa siguiendo las mismas políticas de seguridad corporativas independientemente de su ubicación. SASE se integra perfectamente con ZTNA para brindar una experiencia de usuario perfecta y al mismo tiempo ofrecer protección de seguridad contra amenazas avanzadas para todos los endpoints • Con EPP, todos los endpoints obtienen detección y protección de vulnerabilidades, parches automáticos para software antivirus, un firewall de aplicaciones, protección contra ransomware y administración de endpoints.

[7] "Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide," NIST, https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide

Producto Fortinet	Descripción del producto
FortiSwitch	FortiSwitch es una familia de switches de acceso seguro que ofrece rendimiento, escalabilidad y capacidad de administración excepcionales, a la vez que permite a los usuarios con entornos OT ampliar las redes y la seguridad en toda su infraestructura de red. FortiSwitch se integra perfectamente con el Fortinet Security Fabric a través de FortiLink y puede ser administrado por FortiCloud o FortiGate. La gestión unificada de FortiSwitch a través de FortiGate ofrece visibilidad y control completo de los usuarios y dispositivos en la red.
FortiAP	FortiAP es una serie de puntos de acceso Wi-Fi que pueden ser administrados por FortiCloud o FortiGate. Estos puntos de acceso ofrecen alto rendimiento, cobertura óptima y servicios 802.11ax de clase empresarial, además de aplicación de políticas de control de acceso y seguridad.
FortiExtender	Proporciona un enlace (bridge) entre las LAN Ethernet locales y las conexiones WAN inalámbricas LTE/5G. FortiExtender puede soportar diversas aplicaciones inalámbricas con un alto nivel de redundancia de backhaul (red de respaldo para conexión principal) utilizando una única plataforma de módem LTE/5G con tarjetas SIM redundantes conectadas a diferentes redes móviles. FortiExtender se puede utilizar como backhaul LTE/5G de un FortiGate local con la máxima intensidad de señal inalámbrica LTE/5G. Puede ser administrado de manera central por FortiGate.
FortiGate	FortiGate es la familia de productos insignia de firewall y sistemas de prevención de intrusiones (NGFW/NGIPS) de próxima generación de Fortinet, que ofrece la mejor seguridad de su clase, redes de alta velocidad y funciones de rendimiento acelerado por hardware utilizando procesadores de seguridad especialmente diseñados para NGFW/NGIPS, así como SD-WAN integrada y líder en el mercado. FortiGate viene en diferentes factores de forma y tamaños, incluidos dispositivos resistentes para soportar las duras condiciones ambientales que a menudo enfrentan las aplicaciones industriales
FortiToken	Permite autenticación de dos factores a través de una aplicación de contraseña de un solo uso (OTP) con notificaciones push o un token OTP basado en hardware. FortiToken Mobile (FTM) y los tokens OTP de hardware están completamente integrados con FortiClient, protegidos por FortiGuard y aprovechan la administración directa y el uso dentro de los productos de seguridad FortiGate y FortiAuthenticator. La solución integrada FortiGate, FortiToken y FortiAuthenticator es fácil de implementar, usar y administrar para contar con autenticación multifactor.
FortiAuthenticator	FortiAuthenticator ofrece inicio de sesión único y autorización de usuario para la red empresarial segura de Fortinet. Identifica usuarios, consulta permisos de acceso de sistemas de terceros y reenvía las solicitudes de acceso a FortiGate para implementar políticas de seguridad basadas en identidad. FortiAuthenticator soporta varios métodos y herramientas para autenticación y autorización, como Active Directory, RADIUS, LDAP, SAML SP/IdP, PKI y autenticación multifactor.
FortiNAC	Este producto de control de acceso a la red mejora el Fortinet Security Fabric con visibilidad, control y respuesta automatizada para todo lo que se conecta a la red. FortiNAC proporciona protección contra accesos maliciosos, extiende el control de acceso a dispositivos de terceros, ofrece una mayor visibilidad de los dispositivos, admite un control de acceso a la red dinámico y orquesta respuestas automáticas a una amplia gama de eventos de red
FortiAnalyzer	FortiAnalyzer es una plataforma centralizada de gestión de registros, análisis e informes que proporciona a los clientes una única interfaz para la orquestación, automatización y respuesta simplificada en operaciones de seguridad, identificación proactiva y mitigación de riesgos, así como una visibilidad completa de toda la superficie de ataque. FortiAnalyzer puede recopilar diferentes tipos de registros y eventos de los productos Fortinet a través de la integración del Fortinet Security Fabric.
FortiManager	FortiManager ofrece administración centralizada basada en automatización. Permite a los usuarios finales administrar los dispositivos FortiGate, FortiSwitch y FortiAP en su red de manera central con una plataforma de administración centralizada.
FortiSIEM	FortiSIEM brinda correlación de eventos unificada y administración de riesgos para implementaciones de múltiples proveedores. Permite el análisis de diversas fuentes de información, incluidos registros, métricas de rendimiento, trampas SNMP, alertas de seguridad y cambios de configuración. Todos los datos se alimentan en un motor de análisis basado en eventos y admite búsquedas en tiempo real, reglas, paneles y consultas ad hoc. FortiSIEM ofrece el Modelo Purdue para la clasificación de nivel de seguridad de sistemas de control industrial (ICS) para activos, registros y correlación de eventos, y también admite el marco MITRE ATT&CK® para ICS en el análisis de registros. Soporta integración con herramientas de seguridad OT de terceros de forma nativa.
FortiSOAR	FortiSOAR es un banco de trabajo integral de orquestación, automatización y respuesta de seguridad que permite a los equipos de centros de operaciones de seguridad (SOC) responder de manera eficiente al creciente flujo de alertas, automatizar procesos manuales repetitivos y hacer frente a la crónica falta de recursos. Esta plataforma de operaciones de seguridad patentada y personalizable ofrece libros de estrategias automatizados clasificación de incidentes y remediación en tiempo real para que las empresas identifiquen defiendan y contraataquen. FortiSOAR optimiza la productividad del equipo SOC al ofrecer más de 3000 acciones y al integrarse perfectamente con más de 300 plataformas de seguridad. Esto da como resultado respuestas más rápidas, contención optimizada y tiempos de mitigación reducidos, de horas a segundos. FortiSOAR incluye funciones específicas de ICS, como MITRE ATT&CK® para el marco ICS para correlación de activos y eventos, paneles de control de inventario de activos de TI/OT, paneles de cumplimiento para regulaciones y marcos de ciberseguridad específicos de OT, y más.

Producto Fortinet	Descripción del producto
FortiProxy	Este proxy web seguro protege a los empleados contra ataques transmitidos por Internet incorporando múltiples técnicas de detección, como filtrado web, filtrado DNS, prevención de pérdida de datos, protección antivirus, prevención de intrusiones y protección avanzada contra amenazas.
FortiWeb	Un firewall de aplicaciones web (WAF) que asegura recursos basados en la nube y entornos de DevOps al proteger contra amenazas conocidas y desconocidas, incluyendo las sofisticadas como la inyección SQL, el cross-site scripting, desbordamientos de búfer y ataques DDoS.
FortiDeceptor	FortiDeceptor proporciona tecnología de señuelos y decepción para engañar, exponer y eliminar amenazas externas e internas temprano en la cadena de ataque, bloqueando de manera proactiva las amenazas antes de que causen un daño significativo. Integrado con FortiEDR y FortiGate, FortiDeceptor automatiza el bloqueo de atacantes que apuntan a sistemas y dispositivos de TI y OT mediante el diseño de una capa de señuelos e incentivos diseñados para redirigir el enfoque de los atacantes mientras revelan su presencia en la red.
FortiSandbox	FortiSandbox brinda protección de alto nivel contra infracciones basada en inteligencia artificial que se integra con la plataforma Fortinet Security Fabric para abordar tanto amenazas en constante evolución como amenazas dirigidas, incluyendo ransomware y crypto-malware, en una amplia superficie de ataque digital. Diseñado específicamente para OT, FortiSandbox automatiza la detección y respuesta de malware avanzado de día cero para detectar amenazas dirigidas a sistemas y protocolos de OT en tiempo real.
FortiNDR	Tecnología de protección de próxima generación contra infracciones basada en IA para defender contra varias ciberamenazas, incluidas amenazas persistentes avanzadas, a través de un Virtual Security Analyst™ capacitado. El analista virtual ayuda a identificar, clasificar y responder a las amenazas, incluso las bien camufladas. Usando redes neuronales profundas basadas en inteligencia artificial avanzada y redes neuronales artificiales, FortiNDR ofrece una investigación de seguridad rápida (menos de un segundo) al aprovechar tecnologías de aprendizaje profundo que ayudan en una respuesta automatizada para remediar diferentes tipos de ataques.
FortiSASE	FortiSASE, un servicio entregado en la nube, es una arquitectura que combina funciones de red, seguridad y WAN para dar a los endpoints (usuarios remotos, dispositivos y sucursales) acceso seguro a Internet, recursos de la nube y la red del centro de datos. Utiliza tecnologías de seguridad de red que incluyen firewall como servicio (FWaaS), gateway de web seguro (SWG), acceso a la red de confianza cero (ZTNA) y agente de seguridad de acceso a la nube (CASB). Se basa en tecnologías WAN, incluida SD-WAN.
Servicios de seguridad FortiGuard	Los servicios de seguridad FortiGuard son ofrecidos por FortiGuard Labs, un equipo global de investigación y respuesta a amenazas que utiliza sistemas de aprendizaje automático (ML) e inteligencia artificial (IA) en todo el mundo para recopilar inteligencia de amenazas en tiempo real. Los servicios de seguridad FortiGuard se ofrecen a través de paquetes de suscripción e incluyen varios servicios avanzados de protección contra amenazas para redes empresariales, web, nube, OT, etc. El servicio de seguridad industrial y el servicio de detección de IoT se encuentran entre las ofertas de suscripción de FortiGuard. El servicio de seguridad industrial ofrece más de 2,000 firmas IPS para aplicaciones de ICS/OT, así como protocolos que admiten la inspección profunda de paquetes (DPI) y más de 500 firmas IPS para protección específica de amenazas y vulnerabilidades de ICS.
FortiCamera FortiRecorder	Una suite de cámaras de vigilancia de video basadas en red y grabadoras seguras que refuerzan la protección contra ataques ciberfísicos.

Segmentación y aislamiento de redes

El NIST CSF asigna referencias informativas a muchos estándares conocidos, incluido el IEC 62443 (también conocido como ISA 62443). La mayoría de las organizaciones han implementado sus redes ICS siguiendo las pautas descritas por el conjunto de estándares IEC 62443. Una de las publicaciones dentro del IEC 62443 brinda orientación sobre cómo segmentar un ICS en zonas de seguridad y asignar niveles de seguridad (es decir, cantidades específicas de seguridad) basándose en una comprensión clara del riesgo. Se puede encontrar más información sobre el IEC 62443 en el documento técnico de SANS Effective ICS Cybersecurity Using the IEC 62443 Standard".[8]

[8] "Effective ICS Cybersecurity Using the IEC 62443 Standard," SANS Institute, 17 de noviembre de 2020, www.sans.org/white-papers/39960

Administración de redes Fortinet

En nuestras pruebas, FortiManager nos permitió interactuar con productos Fortinet diseñados para realizar la segmentación y el aislamiento de la red detallados en la Arquitectura de Referencia ICS410. (Consulte la pantalla de incorporación de FortiManager en la Figura 2).

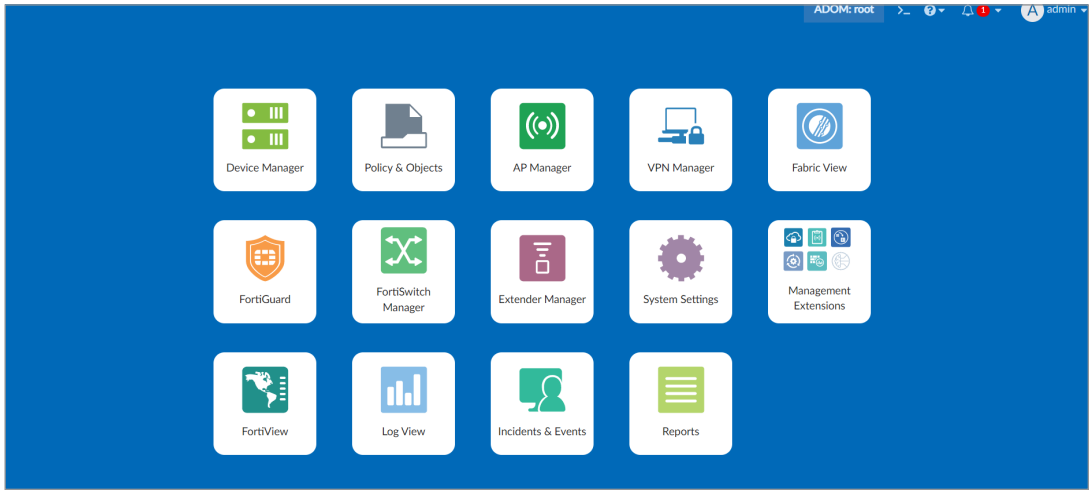

Figura 2. Pantalla de incorporación de FortiManager

Inicialmente, nuestra atención se centró en los íconos de administración de FortiGate para revisar cómo la solución ayuda con la segmentación y el aislamiento de la red. ***Policy & Objects*** y ***VPN Manager*** son necesarios para controlar la segmentación y el aislamiento de la red. Asumimos que la administración de la configuración de la red funcionaría de manera similar a cualquier firewall y, por lo tanto, nos centramos en localizar objetos de política específicos relacionados con los protocolos de control industrial.

La selección del ícono ***Policy & Objects*** nos llevó al portal de administración de FortiGate. Desde allí, ubicamos la gestión de protocolos industriales al profundizar en los elementos del menú ***Security Profiles*** y ***Application Control*** en la barra lateral izquierda, como se muestra en la Figura 3.

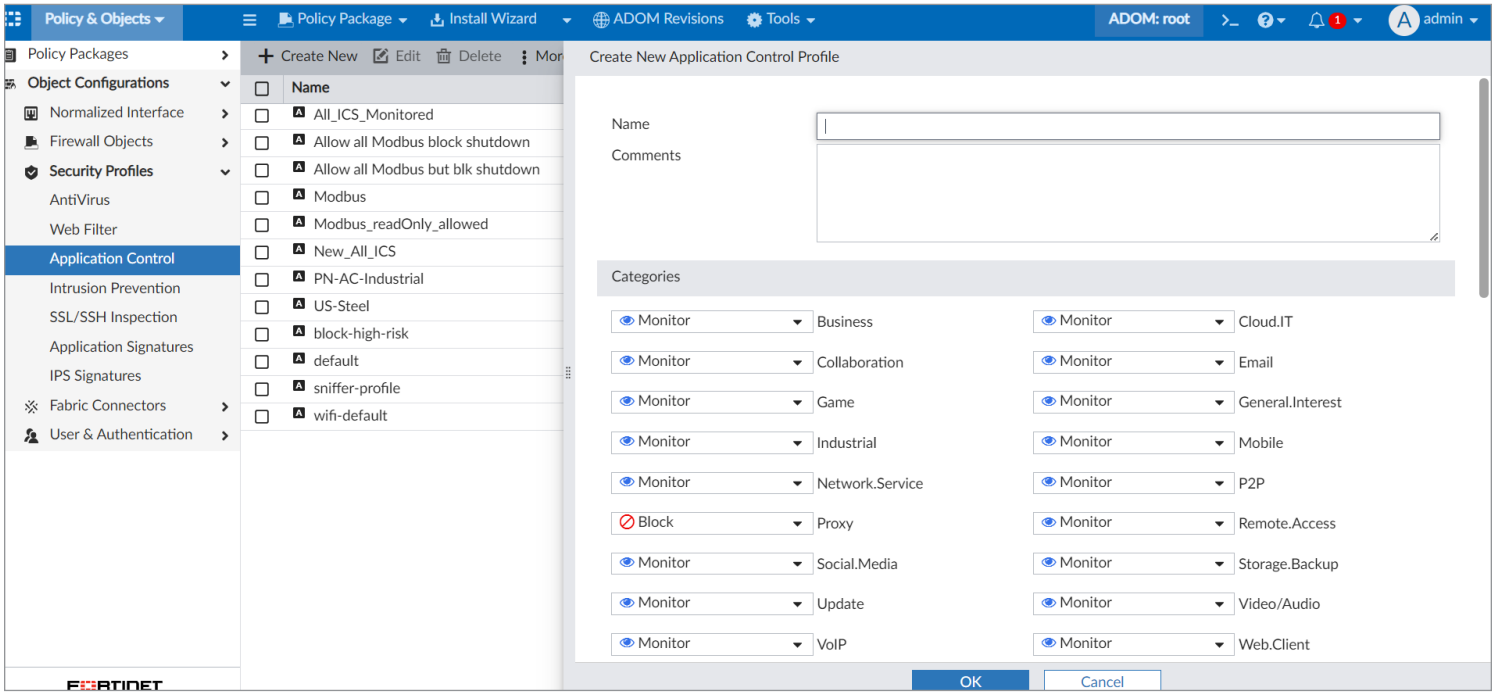

Figura 3. Acceso al perfil de control de aplicaciones

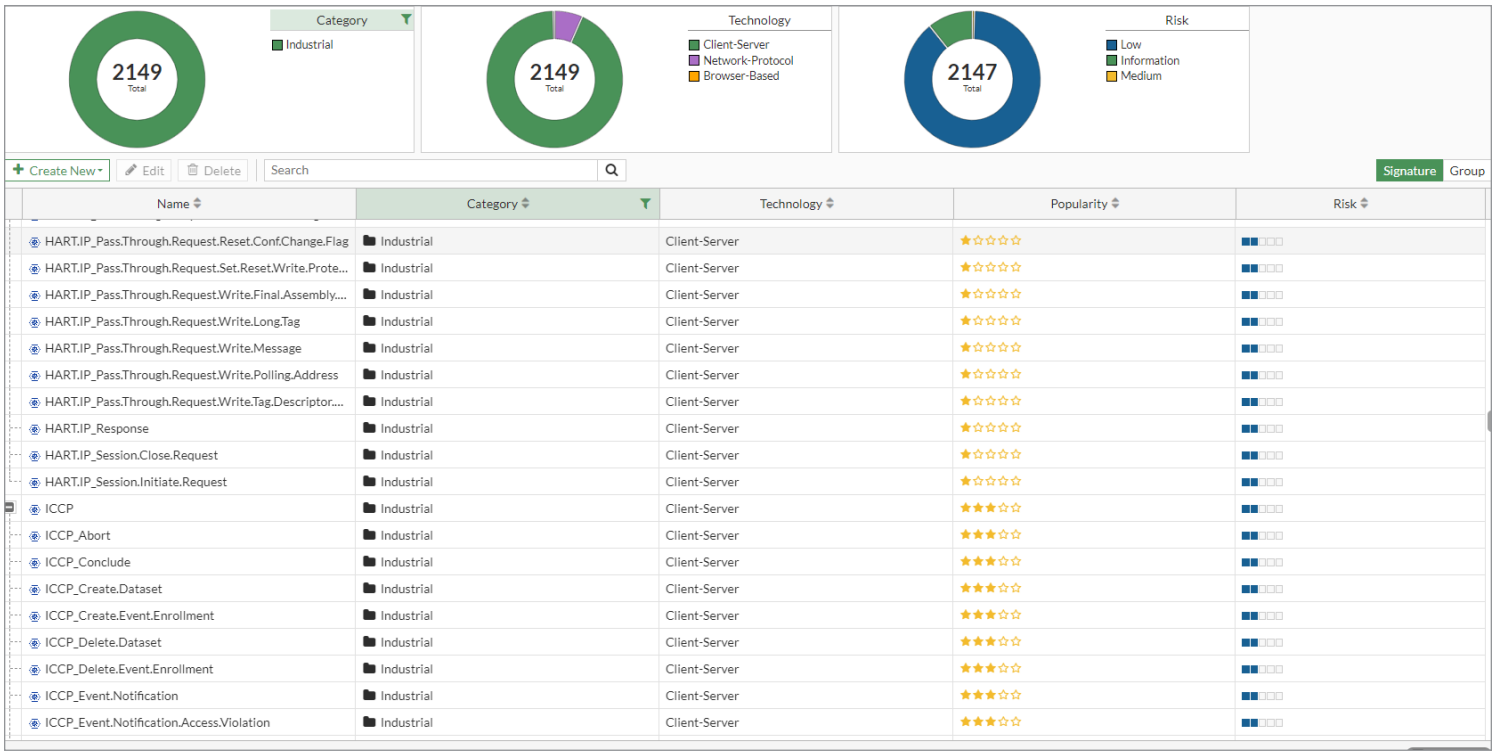

Figura 4. Firmas de control industrial en FortiGate

La revisión de los protocolos industriales muestra que FortiGate cuenta con funciones para monitorear y controlar muchos protocolos que se implementarán dentro de una red de control. Estos incluyen, pero no se limitan a, Modbus, Ethernet/IP, Protocolo Industrial Común (CIP), BACnet, Profinet, Comunicaciones de Plataforma Abierta (OPC), protocolos Siemens, Protocolo de Comunicaciones entre Centros de Control (ICCP) y HART. (Ver Figura 4.)

Para ver algunas de las funciones, ver la Figura 5.

Las funciones ofrecidas permiten administrar comandos de protocolos específicos, como las actividades de lectura y escritura de HART y Modbus, sin embargo, este control se limita a las comunicaciones entre destinos y no a lo que sucede a través del protocolo. En las implementaciones iniciales en entornos operativos, es probable que la restricción se base principalmente en el protocolo utilizado. Conforme las organizaciones maduran, se hace necesaria la capacidad de aplicar restricciones adicionales basadas en funciones y comandos.

Los datos de registro proporcionados por la

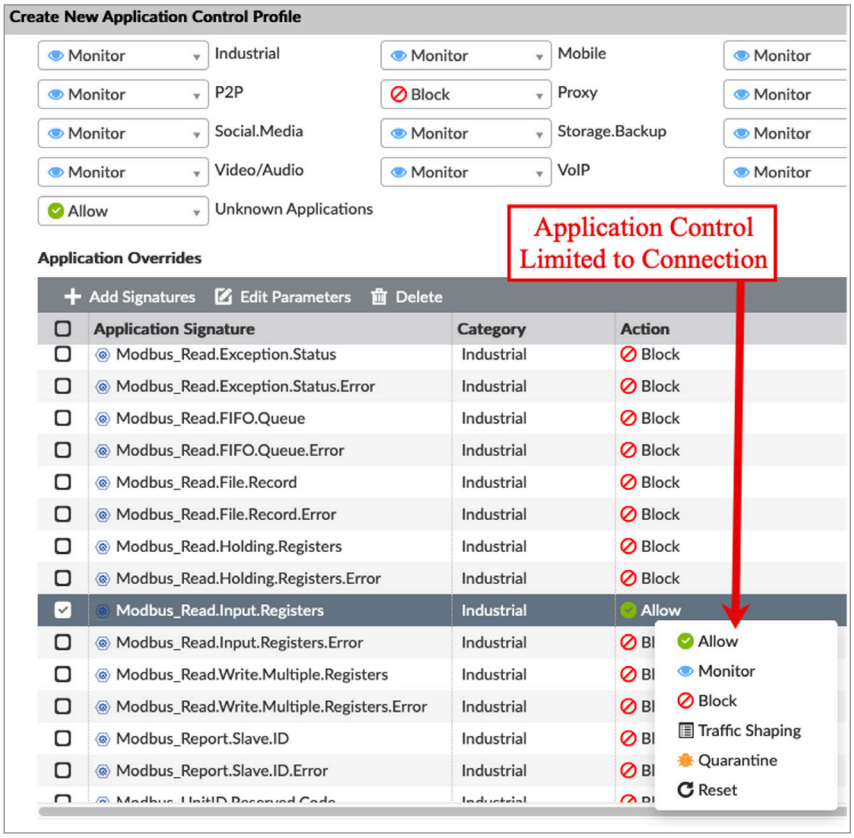

Figura 5. Control de aplicaciones industriales limitado a la conexión

funcionalidad del protocolo industrial de FortiManager deberían brindar visibilidad a una organización en varias áreas clave que preocupan al personal de ICS. Una vez implementados, los registros de comunicación de red se pueden utilizar para revisar las configuraciones de redundancia de los dispositivos, comprender y validar la funcionalidad de conmutación por error y garantizar que no se produzcan problemas de sincronización operativa durante las fallas del dispositivo. Por lo tanto, estos registros de comunicación de red específicos de protocolos industriales podrían mejorar la seguridad y, al mismo tiempo, agregar valor al proceso que se está protegiendo.

Analizamos la funcionalidad del VPN Manager que está integrada con FortiManager. Una herramienta de este tipo es de suma importancia para defender entornos que han aumentado la cantidad de acceso remoto que permiten, especialmente debido al aumento paralelo de grupos de amenazas que utilizan vías de acceso remoto para ingresar a entornos de ICS. La aplicación VPN Manager integrada permite configurar estrategias y tecnologías VPN avanzadas, como las que se encuentran con SD-WAN, acceso de confianza cero y administración de acceso privilegiado. Las funciones de configuración de VPN, que se muestran en la Figura 6, brindan opciones de configuración para limitar la conectividad a activos específicos dentro de la red de control.

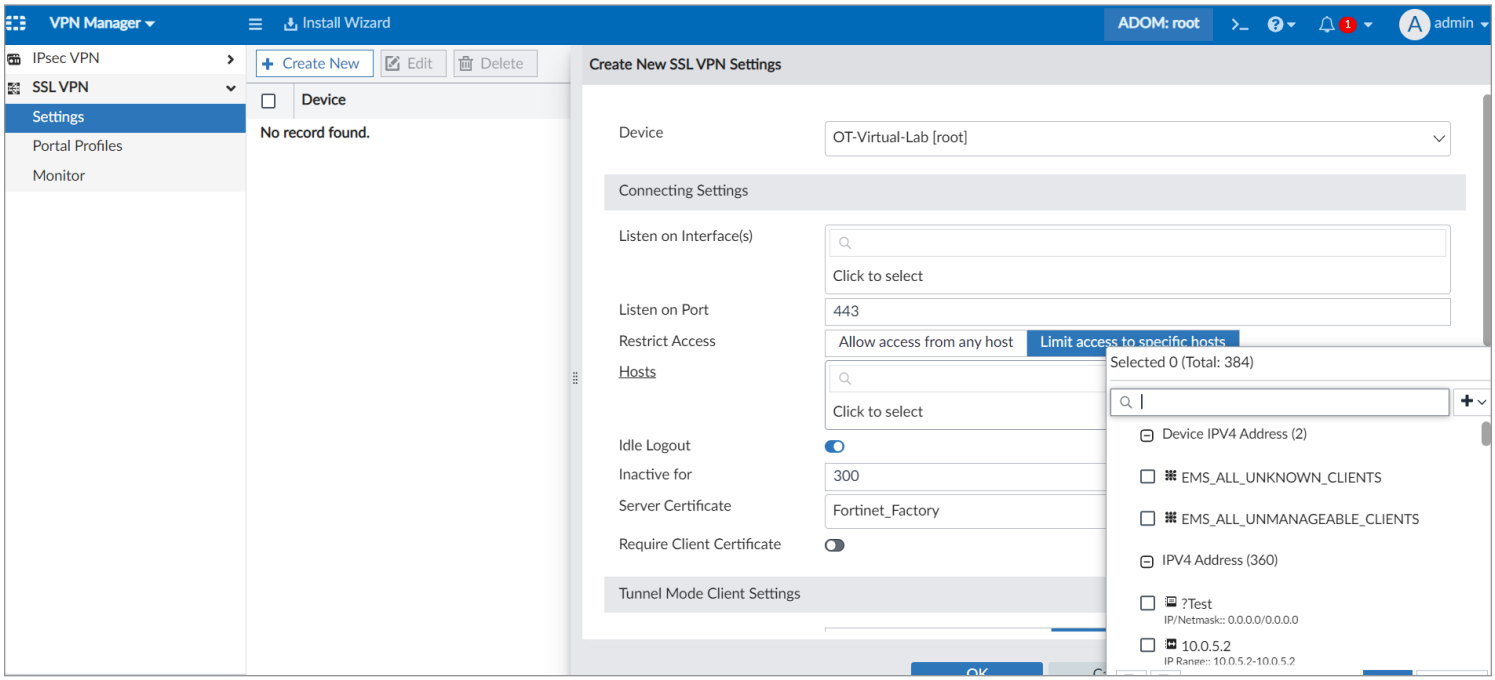

Figura 6. Configuración de VPN SSL para activos internos

Esta función es extremadamente útil al considerar restricciones para el acceso remoto de proveedores e integradores a la red de control. Aunque existen muchas funciones avanzadas de defensa de acceso remoto, no se configuraron en nuestro entorno de prueba y, por lo tanto, no se analizaron más allá de estos pasos.

Control de acceso

El control de acceso, la segunda consideración, es un esfuerzo desafiante para muchas organizaciones. Las redes de control maduras tendrán servidores de autenticación y autorización separados, como servidores Microsoft Active Directory, para su red corporativa y la red de control. Esta situación es común para redes de control asociadas a infraestructura crítica. Sin embargo, las empresas que no están relacionadas con infraestructuras críticas pueden enfrentar dificultades al justificar el costo adicional y la experiencia necesaria para implementar servidores de control de acceso separados dentro de la red de control. Las empresas que han implementado su control de acceso a la red con una relación de confianza con la red corporativa deben reconsiderar inmediatamente esta configuración y separar estos activos.

Los dispositivos FortiAuthenticator y FortiToken son dos tecnologías de Fortinet que podrían ayudar a mejorar la gestión de identidad de la red de control. FortiAuthenticator se integra con FortiManager y podría resultar beneficioso ya que ofrece control más detallado de los usuarios y activos dentro de la red de control y mejorar el registro de actividades. Varios de los productos de Fortinet aprovechan las políticas basadas en identidades y roles para limitar y monitorear las actividades de los usuarios y los activos dentro de la red de control.

El dispositivo FortiToken, que brinda un mecanismo de autenticación de dos factores, es otro dispositivo útil para la red de control. Muchas organizaciones han implementado productos de autenticación de dos factores en su entorno corporativo que, debido a la segmentación y aislamiento de la red, no pueden utilizarse en la red de control. Los requisitos de acceso remoto y acceso administrativo para proveedores e integradores dejan a muchas organizaciones con el dilema de cómo implementar la autenticación de dos factores para los usuarios de la red de control. El dispositivo FortiToken se integra con FortiAuthenticator, aunque no se integra directamente con FortiManager, y puede ofrecer fácilmente una solución a una organización al mismo tiempo que se integra con el resto del Fortinet Security Fabric para brindar funciones de autenticación de dos factores para la administración de seguridad de la plataforma.

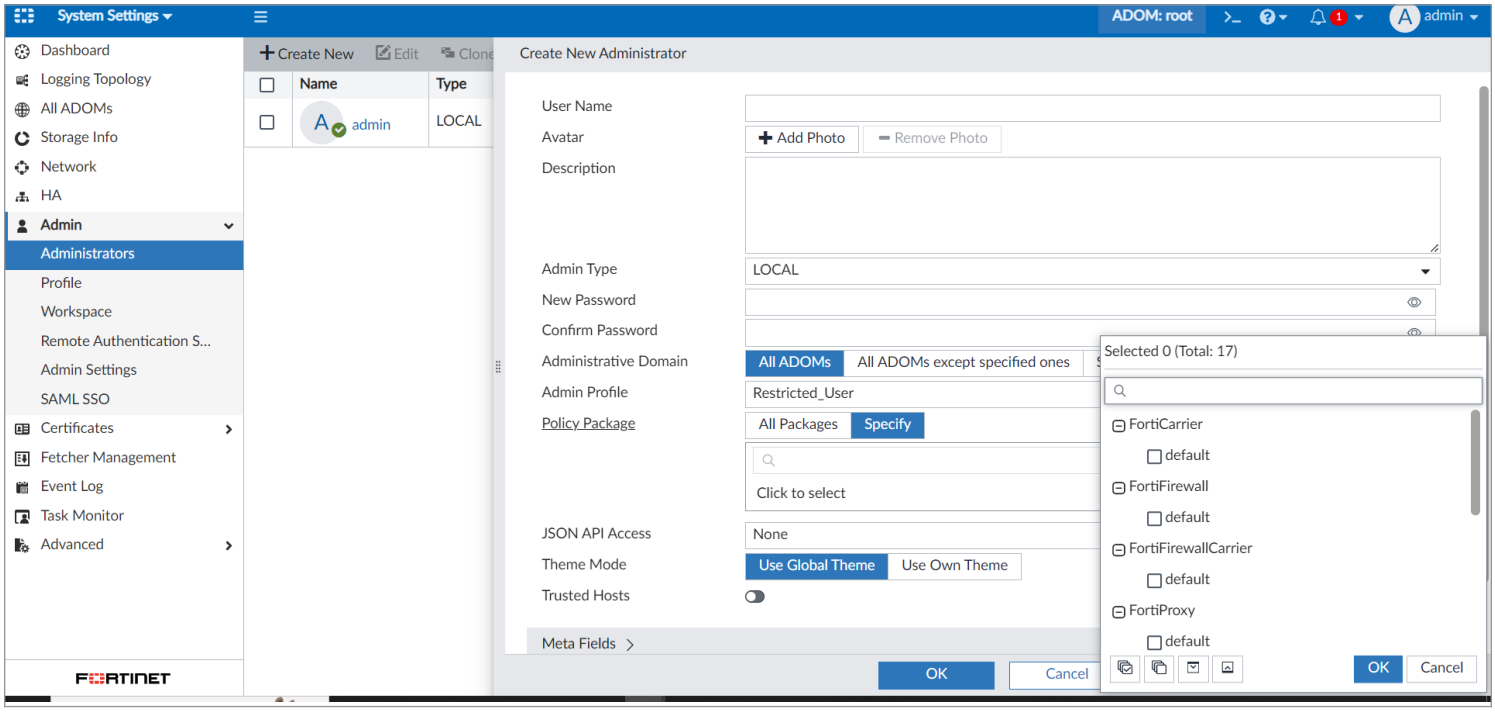

Figura 7. Administración detallada de usuarios de FortiManager

Aunque estas tecnologías no estaban disponibles en la red de prueba, examinamos el control de acceso proporcionado por FortiManager. La implementación de varios controles de seguridad en una red puede resultar en una gestión de usuarios compleja y que consume mucho tiempo. FortiManager brinda la capacidad de gestionar de manera granular los roles y responsabilidades (ver Figura 7) para los usuarios que acceden a la mayoría de los productos de Fortinet.

Junto con la autenticación de dos factores, un punto central de administración para el control de acceso y la administración de roles de los controles de seguridad es una característica importante, y la reducción de los gastos y esfuerzos generales de administración podría resultar útil.

Registro y monitoreo

A continuación, centramos nuestra atención en cómo el Fortinet Security Fabric puede ayudar con la tercera consideración: registro y monitoreo. Cada dispositivo y sistema ICS produce y ofrece una visión de los eventos locales de la tecnología. Conocer y entender estos eventos requiere la generación de alertas sobre actividades inusuales conocidas, correlacionar eventos e informar sobre actividades específicas para clases de activos.

FortiAnalyzer brinda visibilidad de los eventos que ocurren en el Fortinet Security Fabric. Este dispositivo se integra con FortiManager y se puede acceder a sus funciones seleccionando los íconos ***FortiManager SOC/ Log View***, luego ***Incidents & Events*** y ***Reports*** (ver Figura 7). El dispositivo puede importar eventos de syslog de otros dispositivos, pero su capacidad de análisis y generación de informes se limita específicamente a los productos de Fortinet.

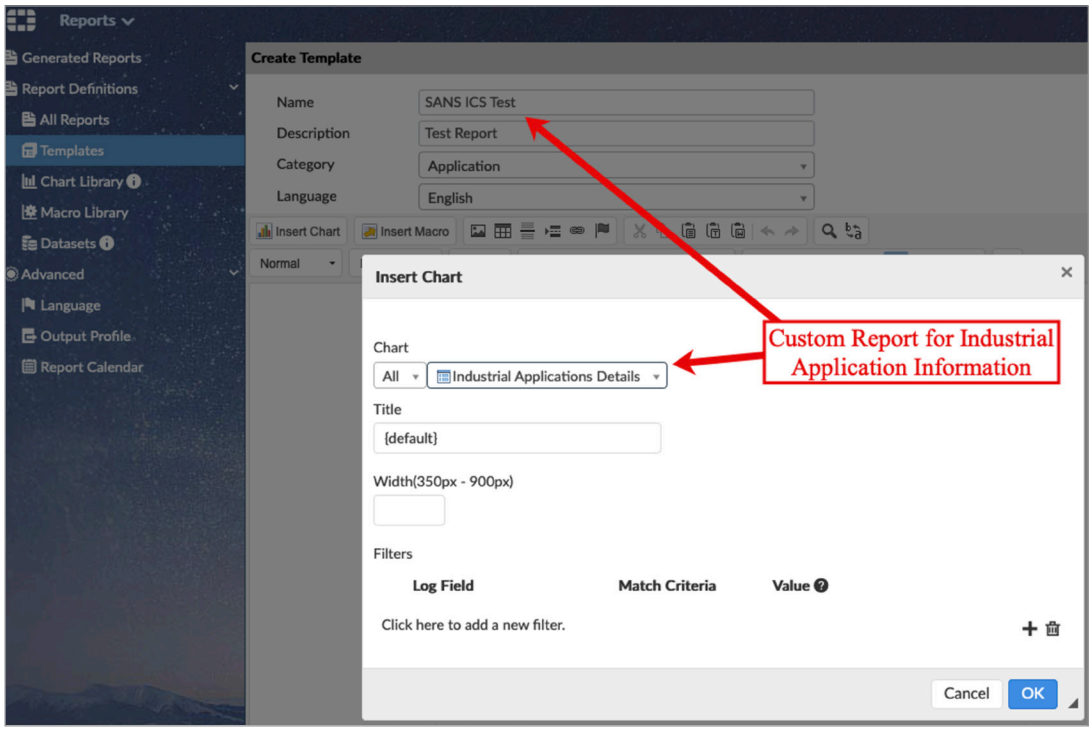

Figura 8. Generando informes personalizados en FortiAnalyzer

El laboratorio de Fortinet al que accedimos no estaba configurado para proporcionar detalles que pudieran informarse. Sin embargo, no se puede subestimar el poder de combinar información de FortiGuard, FortiVPN, FortiNAC y FortiAuthenticator. La integración de protocolos industriales en el dispositivo FortiGuard cuenta con la capacidad de generar informes relacionados con estos protocolos (ver Figura 8).

Entender la línea de base común de las comunicaciones e interacciones de los dispositivos lleva a una organización a generar una línea de base de comportamiento común. Estos datos son invaluables durante la evaluación de eventos y la respuesta a incidentes.

FortiSIEM es el portal principal de registro, correlación y análisis central del Fortinet Security Fabric. Este dispositivo recibe registros de todos los dispositivos OT configurados, genera alertas sobre la actividad configurada y proporciona un portal para los analistas del centro de operaciones de seguridad. Los datos agregados se correlacionan con MITRE ATT&CK® para ICS, así como con fuentes de amenazas de terceros como Dragos y Nozomi. La Figura 9 muestra la interfaz del portal FortiSIEM.

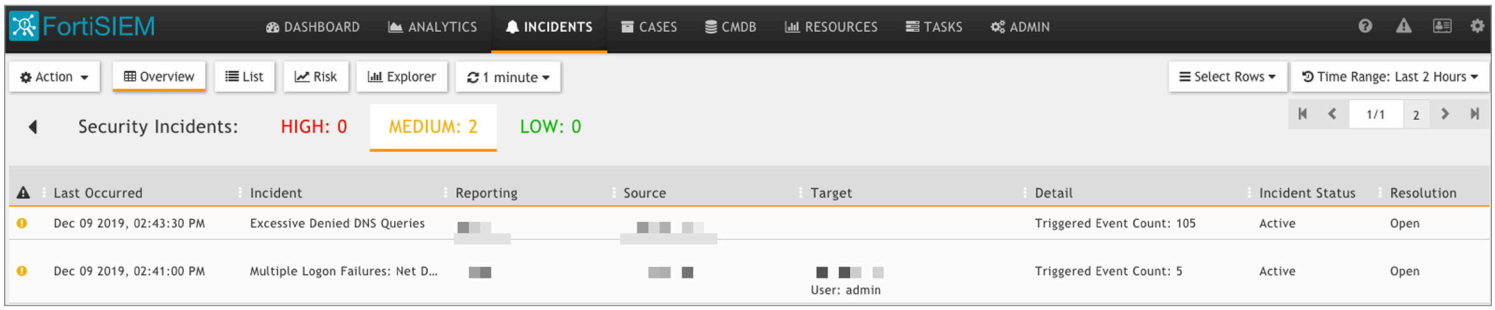

Figura 9. Panel de control FortiSIEM

La eficacia de esta interfaz para identificar eventos y gestionar el flujo de trabajo no se podría determinar sin implementarla en un entorno operativo. El laboratorio tenía activos implementados limitados, por lo tanto, los eventos almacenados en FortiSIEM no se pudieron analizar. Esta situación limitó la revisión de eventos, incidentes, análisis de tickets y generación de informes. Intentamos crear un nuevo informe relacionado con protocolos industriales como Modbus y Profinet, pero el informe no se pudo generar sin datos de una red ICS activa. En este FortiSIEM no se habían configurado reglas para puertos predeterminados relacionados con protocolos industriales.

Inventario de activos

El inventario de activos puede ser difícil para muchas organizaciones. Recopilar y mantener esta información supone una enorme pérdida de personal. Para ayudar con el inventario de hardware, el Fortinet Security Fabric cuenta con dos funciones que parecen facilitar parte de este esfuerzo. El inventario de hardware se puede lograr mediante la integración de FortiNAC y FortiSIEM en el Fortinet Security Fabric. FortiNAC permite integración con dispositivos de red de una organización, como switches y ruteadores Cisco. Ver Figura 10.

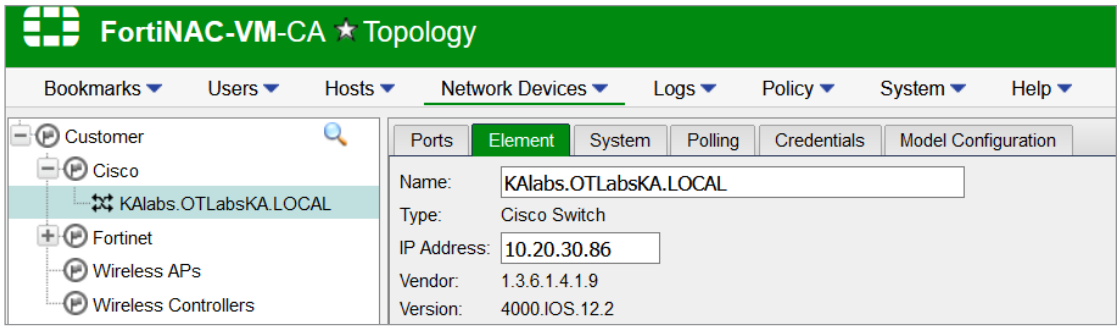

Figura 10. FortiNAC integrado con el switch Cisco

Esta integración permite a FortiNAC observar y dar detalles sobre los dispositivos que se comunican a través de la red ICS. La Figura 11 es un ejemplo de esta información, que se puede extraer en varios formatos, incluidos valores separados por comas y Microsoft Excel. Se pueden generar informes periódicos para saber cuáles son los activos que se comunican dentro de la red de control.

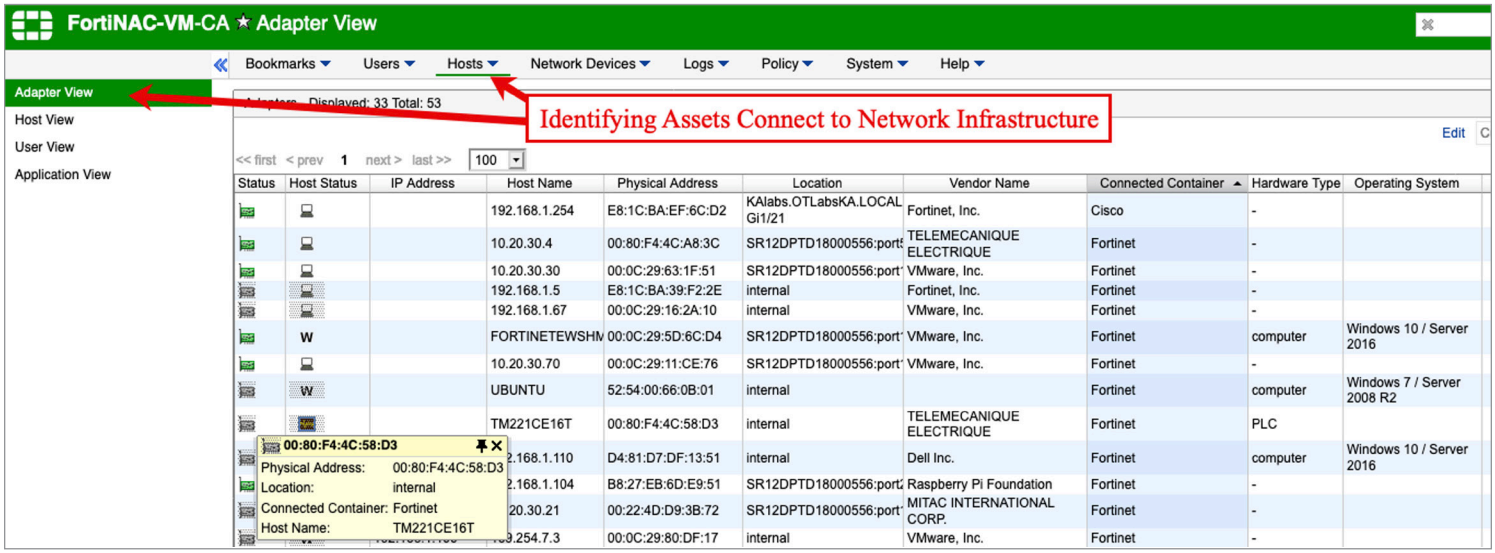

Figura 11. Inventario de activos utilizando FortiNAC

FortiSIEM incluye una función de inventario de activos de OT que también hace una asociación con los niveles de Purdue para informes y alertas, así como una base de datos de administración de configuración, que se muestra en la Figura 12, que rastrea todos los activos que inician sesión en el dispositivo.

La base de datos se actualiza y mantiene automáticamente con información de eventos entrantes, lo que permite a los administradores conocer rápidamente estos activos y dónde están ubicados y generar informes para establecer una base de referencia de la actividad normal. Esta información es extremadamente valiosa para las operaciones normales y crítica durante la investigación de eventos de seguridad y la respuesta a incidentes.

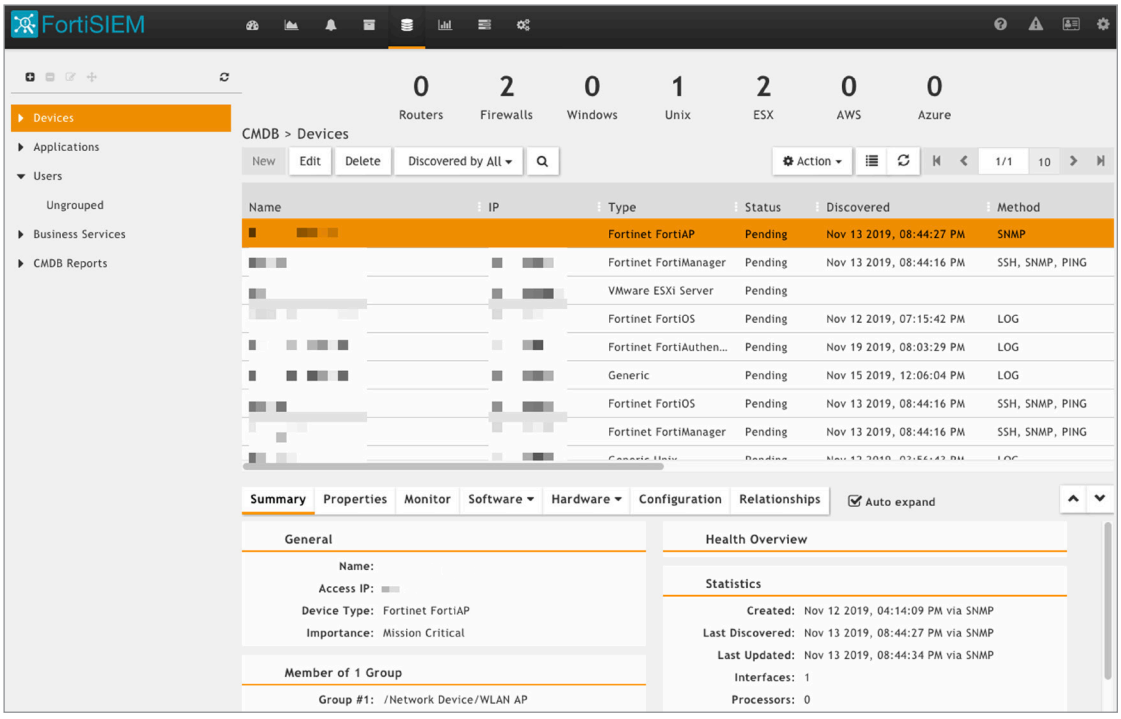

Figura 12. Base de datos de administración de la configuración de FortiSIEM

Además del inventario de hardware, las organizaciones necesitan hacer un inventario de software. Como parte del Fortinet Security Fabric, el inventario de software se puede obtener mediante la implementación de FortiClients en servidores y estaciones de trabajo con la red de control. Durante esta revisión, no pudimos revisar los efectos que FortiClient tiene en los recursos del servidor y de la estación de trabajo, como la memoria, CPU y uso de la red. Por lo tanto, las organizaciones querrán revisar los efectos de FortiClients con sus proveedores o integradores antes de implementarlos en un entorno. Como alternativa, puede ser más fácil implementar FortiClient en estaciones de trabajo de ingenieros, operadores y programadores. El costo de la potencia de procesamiento en el sistema puede justificarse por la información de activos proporcionada a través de FortiClient. Esta información incluye información de software y hardware de la estación de trabajo. Además, brinda valiosa información sobre vulnerabilidades y conectividad con el dispositivo FortiNAC para obtener beneficios administrativos y de seguridad adicionales.

Respuesta a incidentes y recuperación

La respuesta a incidentes y la recuperación puede ser una operación confusa y estresante para cualquier organización. La información precisa sobre los eventos del sistema, la red y la autenticación es fundamental durante estos períodos. Correlacionar estos eventos a través de la red de control es igualmente importante. Tener una única consola de administración que permita a los administradores recopilar y analizar esta información puede resultar especialmente beneficioso al reducir los pasos para acceder a la información.

El laboratorio de Fortinet Security Fabric con el que contamos para este análisis no se configuró de manera tal que nos diera datos reales para conocer su verdadero valor durante un esfuerzo de respuesta a incidentes. Sin embargo, la integración de controles de seguridad, a través de FortiManager, y los datos que correlaciona es prometedora y sería útil para analistas, personal de respuesta a incidentes y gerentes. Una vez configurada e integrada correctamente, la información proporcionada por las tecnologías del Fortinet Security Fabric tiene el potencial de reducir significativamente las brechas entre el compromiso y la identificación. Estos controles de seguridad también ofrecen valiosa información correlacionada que ayudará a contener un incidente de seguridad y a la eventual recuperación del entorno ICS.

El mejor camino a seguir para que cualquier equipo aborde los eventos de seguridad dentro de la red ICS es llevar a cabo escenarios prácticos de respuesta a incidentes. Los activos de Fortinet Security Fabric entregarán al equipo detalles sobre la red de control para ayudar en la generación de escenarios, la recopilación de datos y el análisis de impacto. Con este tipo de datos, los equipos están más preparados que aquellos que deben adquirir y correlacionar manualmente los registros de los dispositivos.

Resumen

El NIST CSF está diseñado para ayudar a los operadores de infraestructura crítica en el desarrollo e implementación de un programa de seguridad específico para entornos ICS. No hay razón alguna por la cual los equipos que administran infraestructuras no críticas no puedan utilizar el NIST CSF de la misma manera. Este enfoque asegura que los procesos en el centro de la red de ICS estén impulsando los requisitos, al mismo tiempo que los miembros de los equipos de TI e ICS aprenden sobre estos requisitos. Esta comunicación y acuerdo sobre las prioridades son las claves del éxito.

Las nuevas políticas de seguridad implicarán un cambio de procedimientos y, potencialmente, de tecnologías. Dado que los procesos no cambian con frecuencia, el uso de un entorno de control de seguridad homogéneo y altamente integrado tiene mucho sentido. Una herramienta como FortiManager, que se asemeja tanto a un panel único para administrar y monitorear muchos controles de seguridad, puede ser de gran ayuda para reducir el tiempo y el esfuerzo. La sobrecarga en la administración de cuentas proporcionada por FortiAuthenticator también debería reducir la confusión y los errores, en comparación con la administración del acceso administrativo y de usuario a cada recurso de forma individual.

Sin datos reales, es difícil juzgar cómo funcionará cada producto Fortinet por separado dentro de una red ICS. Sin embargo, la demostración que tuvo el equipo de revisión del SANS sobre las funciones básicas del Fortinet Security Fabric nos ayudó a comprender el potencial de la integración. Las funciones de FortiGate para monitorear y administrar, incluso a un alto nivel, protocolos industriales específicos ayudarán a los equipos de ICS a implementar límites de cumplimiento efectivos entre cada nivel de Purdue. La integración de FortiGate con FortiAuthenticator y el Active Directory de la red de control proporcionará los beneficios del control de acceso a Fortinet Security Fabric y otras tecnologías de ICS. Los productos FortiAnalyzer y FortiSIEM entregarán a los equipos de ICS eventos de red y sistemas correlacionados generados dentro del entorno de ICS, lo que a su vez, les ayudará a identificar y abordar eventos de seguridad y mejorar la respuesta a incidentes de seguridad. FortiNAC y FortiClient ayudarán a mejorar la gestión de activos de hardware y software, un tema con el que luchan la mayoría de las organizaciones.

Las funciones que aporta el Fortinet Security Fabric a las redes ICS y sus equipos de soporte son impresionantes. Financiar e implementar todas estas tecnologías al mismo tiempo es poco realista para la mayoría de las organizaciones. Pero con un programa de seguridad planificado, basado en los requisitos de seguridad directamente asociados con los procesos de la organización, la migración a una infraestructura ICS administrada por Fortinet Security Fabric podría ser posible y ayudaría a las organizaciones a proteger estas redes y tecnologías críticas. Para procesos nuevos, determine los requerimientos de seguridad de la información e incorpórelos a las fases de pruebas de aceptación en fábrica y en sitio (FAT y SAT) del ciclo de vida del proceso. Esta acción ayudará a identificar y justificar la implementación de estos controles de seguridad y garantizar que tengan un impacto positivo en el proceso. Las organizaciones que aseguran procesos activos deberán utilizar pruebas y tiempos de transición para implementar estos productos; esto dará a los equipos de ICS el tiempo necesario para probar y validar cómo se afectan la fiabilidad y disponibilidad del proceso por la implementación de las nuevas tecnologías. Si se planifican adecuadamente, estas tecnologías deberían mejorar la seguridad y la funcionalidad de los procesos en los que se implementan.

Patrocinador

SANS desea agradecer al patrocinador de este artículo:

FORTINET®