Descripción Técnica de Sucuri

Descripción de Productos y Servicios

ÍNDICE

DESCRIPCIÓN TÉCNICA DE SUCURI

DESCRIPCIÓN DEL PRODUCTO/SERVICIO

EXPOSICIÓN

DESCRIPCIÓN DE SUCURI

DESCRIPCIÓN DE LA EMPRESA

Sucuri es una empresa de seguridad reconocida en todo el mundo, que se especializa en la seguridad integral para los propietarios de sitios web. La empresa establecida en Estados Unidos fue fundada en 2010 y mantiene una presencia global. Sucuri cuenta con personal en más de 23 países a través de los principales continentes para asegurar un soporte accesible 24/7/365. La compañía ofrece servicios de seguridad de sitios web a más de 45.000 clientes en todo el mundo, limpia y repara más de 500 sitios web infectados por día, supervisa más de 400.000 sitios web y maneja más de 16 mil millones de visitas de páginas únicas al mes.

Toda la tecnología que tiene Sucuri es construida por nuestro equipo de ingenieros de seguridad e investigadores. Nuestra tecnología ha sido desarrollada para satisfacer las crecientes amenazas de seguridad en línea a medida que aparecen. Nuestro equipo está dedicado a asegurar la confidencialidad, integridad y disponibilidad de cada sitio web dentro de la red Sucuri.

En Sucuri, nos preocupamos por cada sitio web y tratamos a cada uno de ellos como si fuesen el nuestro. La solución que ofrecemos se basa en tres pilares principales - Protección | Detección | Respuesta. Adoptamos un enfoque de defensa en profundidad para la seguridad de sitios web que emplea varias capas de seguridad para proporcionar la solución más completa disponible. Combinamos personas, procesos y tecnología para el cuidado de los sitios web y mitigamos los ataques de la manera más rápida y eficiente posible.

Estos pilares permiten a Sucuri desplegar una solución defensiva para evitar que los atacantes abusen de sus componentes del sitio web. Esta solución de prevención se agrega a un mecanismo de verificación permanente para identificar cualquier elemento nocivo que pueda ser indicador de un posible compromiso. Por último, Sucuri ofrece un equipo profesional de respuesta a incidentes (IRT) para cuando los ataques tienen éxito, dando a las empresas la tranquilidad que necesitan con nuestra atención obsesiva a las amenazas actuales y emergentes en el dominio de seguridad de sitios web.

PERSONAS, PROCESOS Y TECNOLOGÍA

Hay soluciones turnkey para la seguridad. Es una combinación de personas, procesos y tecnología que ayuda a crear un enfoque flexible y escalable para la seguridad de cualquier organización. Los productos de Sucuri están diseñados para reducir el riesgo de infracción de marca a través de los mecanismos de aplicación tanto preventivos como reactivos, dirigiéndose a cada uno de los elementos descritos anteriormente. La solución Sucuri es una oferta complementaria que se une a los controles de seguridad existentes de una organización, de acuerdo con una serie de requisitos de la gobernanza, mientras permite que los equipos de seguridad sigan a centrarse en sus principales responsabilidades.

DESCRIPCIÓN DEL PRODUCTO/SERVICIO

Sucuri ofrece una solución de seguridad completa para los sitios web, llamada de Paquete de Seguridad de Sitios Web (Website Security Stack - WSS). Se compone de cuatro plataformas centrales diseñadas para proporcionar a las organizaciones una solución de seguridad integral para las propiedades de los sitios web de una organización.

PLATAFORMA DE MONITOREO

La plataforma de monitoreo es un sistema de detección de intrusiones (Intrusion Detection System - IDS) de software como servicio (Software as a Service SaaS) basado en la nube. Esta plataforma se basa en el concepto de un sistema de monitoreo de integridad basado en la red (Network-Based Integrity Monitoring System - NBIMS). Se trata de un mecanismo de escaneo remoto y local (server-side) permanente, proporcionando visibilidad sobre el estado de seguridad de un sitio web casi en tiempo real.

Desarrollado con el objetivo de detectar múltiples indicadores de compromiso (Indicators of Compromise - IoC), que incluyen, pero no se limitan a:

- Distribución de malware
- Incidentes de Notificaciones (Blacklisting)
- Spam de SEO
- Certificados SSL
- Páginas de Phishing Lure
- Cambios en Whois
- Cambios en DNS

La plataforma de monitoreo incluye un sistema de alerta en caso de un IoC. El Grupo de Operaciones de Seguridad (Security Operations Group - SOG) es notificado y toma medidas inmediatamente por el IRT de seguridad.

La plataforma no requiere instalación o cambios en la aplicación. Todos los sitios web se agregan y configuran a través del panel de Sucuri. Para activar el escaneo del lado del servidor, es necesario haber un agente PHP en el root del dominio principal.

Nota: Los eventos de monitoreo pueden ser emitidos por el sistema de gestión de la información y eventos (System Information and Event

Management - SIEM) de la empresa bajo petición.

PLATAFORMA DE PROTECCIÓN

La plataforma de protección ("Sucuri Firewall") es un sistema de prevención de intrusiones (IPS) Website Application Firewall (WAF) SaaS en la nube para sitios web. Funciona como un proxy inverso, interceptando e inspeccionando todas las solicitudes de Hypertext Transfer Protocol/Secure (HTTP/HTTPS) a un sitio web mediante el filtrado de todas las solicitudes maliciosos en la red Sucuri antes que lleguen a su servidor. El Firewall Sucuri incluye los motores de Patching Virtual y Hardening Virtual para permitir la mitigación de amenazas en tiempo real sin afectar al sitio web.

El Firewall Sucuri se basa en una red de distribución de contenidos (Content Distribution Network - CDN), que proporciona funciones de optimización del rendimiento de un sitio web. El CDN utiliza un enfoque de propiedad (proprietary approach) para almacenamiento en caching dinámico y contenido estático en todos los nodos de la red para garantizar el mejor rendimiento en el mundo.

Además, el Firewall Sucuri proporciona servicios integrales para Domain Name Server (DNS).

El Firewall Sucuri se ejecuta en una red Anycast distribuida globalmente (Globally Distributed Anycast Network - GDAN), construida y gestionada por el equipo de Sucuri. La configuración GDAN proporciona alta disponibilidad y redundancia en caso de fallas de la red. Sucuri gestiona seis puntos de presencia (Points of Presence - PoP).

Puntos de Presencia

San Jose, CA
Dallas, Texas
Distrito de Columbia (DC)
Londres, Reino Unido
Frankfurt, Alemania
Tokio, Japón

La plataforma se apoya en el centro de operaciones de seguridad de Sucuri (Sucuri Security Operations Center - SOC), que proporciona monitoreo 24/7/365 y respuesta a todos los ataques. Algunas de las características que la plataforma de protección ofrece a los propietarios de sitios web:

- Mitigación de ataques de denegación de servicio (Distributed Denial of Service - DDoS)
- Prevención de Intentos de Explotación de Vulnerabilidades (SQLi, XSS, RFI / LFI, etc...)
- Protección contra el Top 10 de OWASP (Open Web Application Security Project) y más
- Protección contra ataques al acceso (intentos de fuerza bruta)
- Optimización del rendimiento

La plataforma no requiere instalación o cambios en la aplicación. Todo se hace a través de DNS mediante la adición de un A record o cambiando para name servers de Sucuri.

PLATAFORMA DE RESPUESTA

La plataforma de respuesta ofrece un equipo profesional de respuesta a incidentes de seguridad (Security Incident Response Team - RT). Este equipo está disponible para responder a todos los incidentes de seguridad relacionados con sitios web, incluyendo cuestiones identificadas por Sucuri. El personal es altamente capacitado y capaz de mitigar todas las infecciones de sitios web y problemas relacionados con malware.

Esta plataforma existe debido a la naturaleza compleja de la seguridad de sitios web. Intrusiones ocurren por muchas razones. A pesar de que nuestras diferentes tecnologías se utilizan para ayudar a prevenir este tipo de compromisos, hay cosas que escapan al control de Sucuri. Los ejemplos incluyen la gestión o creación de contraseñas de usuarios débiles, la configuración de seguridad deficiente y otras cuestiones relativas al entorno.

Debido al vector de ataque expandido fuera del control de Sucuri, la plataforma de respuesta está diseñada para proporcionar a las organizaciones un equipo complementario para ayudar en la identificación y erradicación de las invasiones exitosas. La plataforma incluye el análisis de sus causas, ayudando en la aplicación de parches y en la restauración del ambiente al funcionamiento.

La plataforma de respuesta incluye, pero no se limita a:

- Infecciones de malware a nivel del servidor
- Infecciones de malware en sitios web
- Inyecciones de spam de SEO
- Redirecciones de Usuarios Maliciosos
- Desfiguraciones (Defacements) de sitios web
- Eliminación de todas backdoors
- Eliminación de las notificaciones de listas negras de sitios web

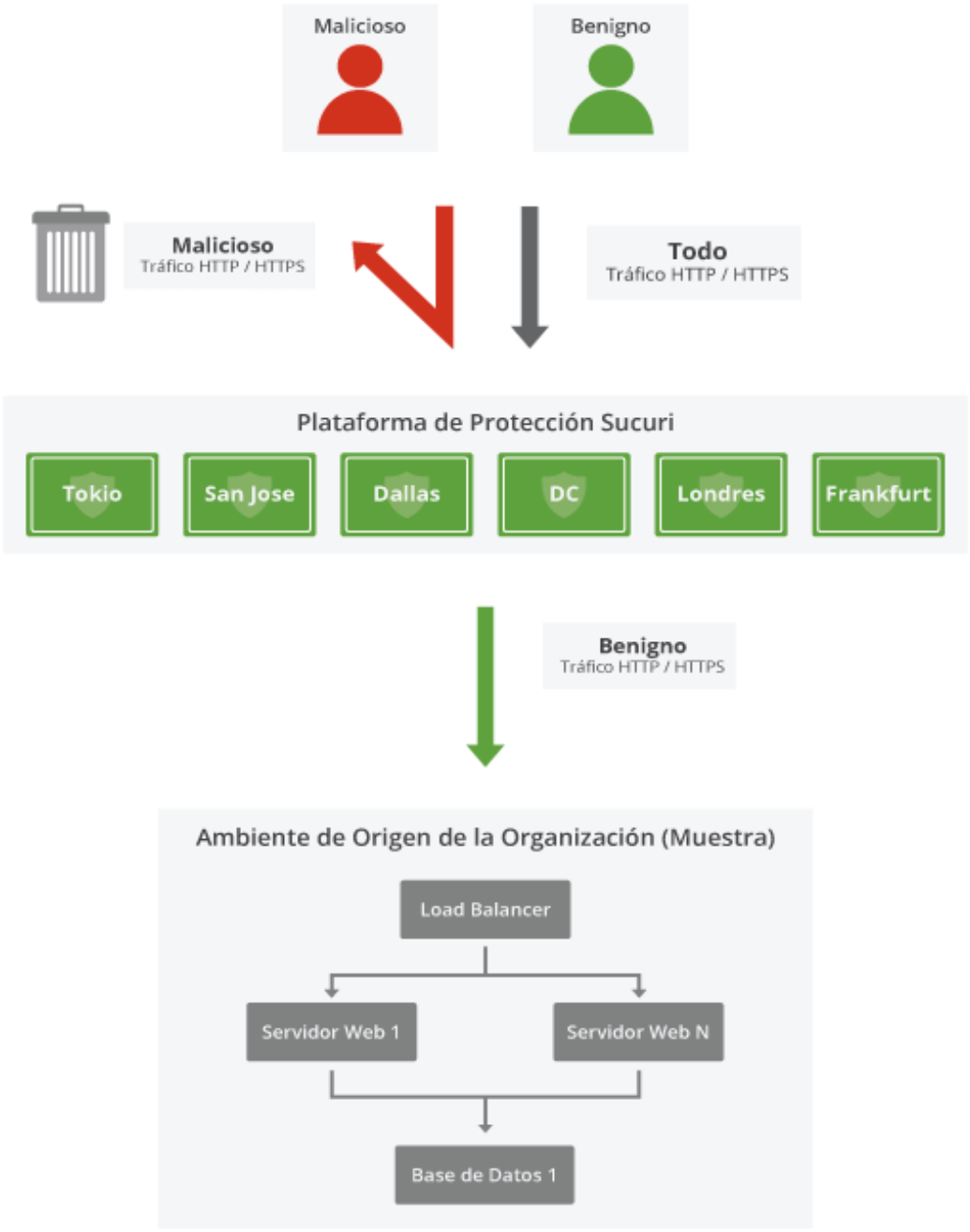
La plataforma no requiere ninguna instalación o cambio en la aplicación, pero requiere acceso directo al web server / application vía FTP / SFTP o SSH.

PLATAFORMA DE COPIAS DE SEGURIDAD

La plataforma de copias de seguridad proporciona a organizaciones una operación permanente en el caso de una emergencia. La plataforma incluye el almacenamiento de todos los archivos de sitios web y bases de datos en una ubicación remota en la red Sucuri. En el caso de un problema, las copias de seguridad estarán disponibles para la organización.

La plataforma no requiere instalación o cambio en la aplicación. Todos los sitios web se añaden y se configuran en el panel de Sucuri.

EXPOSICIÓN A: DIAGRAMA DE RED HOLÍSTICO (PLATAFORMA DE PROTECCIÓN)



EXPOSICIÓN B: MITIGACIÓN DE DDOS

La mitigación de ataques de denegación de servicio (DDoS) es una característica clave que el Firewall Sucuri ofrece a sus clientes.

ATAQUES DDOS BASADOS EN LA RED (ATAQUES VOLUMÉTRICOS)

El enfoque de Sucuri para mitigar los ataques basados en la red incluye inversión en los recursos de todos los lugares del PoP. La mitigación de DDoS se desarrolla en una red de difusión anycast, que permite la distribución de todo el tráfico entrante (inbound traffic) a través de la red y explícitamente bloquea todo el tráfico no HTTP / HTTPS. La capacidad actual de la red es de más de 250 gigabytes por segundo (GPS). Cada PoP tiene varios ports de 10G y 40G de diferentes proveedores, todos diseñados para absorber y escalar cuando hay grandes pedidos para el tráfico entrante y ataques.

ATAQUES DDOS BASADOS EN LA APLICACIÓN (APPLICATION-BASED DDOS)

Estos ataques están diseñados para interrumpir la disponibilidad de un sitio web y atacar directamente los recursos del servidor. Al inundar un servidor de peticiones, un atacante es capaz de consumir recursos del servidor local hasta que el servidor sea incapaz de responder a las peticiones legítimas. En tales casos, el sitio web no responderá. El orden de magnitud es muy diferente: estos ataques se miden en peticiones por segundo (RPS) y pueden comenzar a 100/200 peticiones por segundo para muchos servidores web.

El enfoque de Sucuri para mitigar estos ataques es su tecnología: parte humana y parte inteligencia artificial. La plataforma cuenta con tecnología que permite que el equipo y el motor analicen aplicaciones a través de la red, lo que nos permite separar adecuadamente las peticiones maliciosas de las benignas. Además, en la red Sucuri, los sitios web pueden soportar 300k + RPS por sitio web.

EXPOSICIÓN C: PREVENCIÓN DE EXPLOIT

La prevención de intentos de exploits remotos que intentan abusar las vulnerabilidades de software, tales como las identificadas por el Open Web Application Security Project (OWASP) es una característica crítica de la plataforma de protección.

Estos ataques pueden incluir intentos de exploits contra el sitio web directamente y metas como inyecciones (SLQi, XSS, etc.), la ejecución remota de código (remote code execution- RCE), el error de configuración de seguridad, la inclusión remota de archivos (remote file inclusion - RFI) y muchas otras vulnerabilidades.

La plataforma de protección utiliza un enfoque multinivel de propiedad para identificar y eliminar las solicitudes de aplicaciones maliciosas

Nivel 1	Describiendo la Aplicación	El primer nivel usa un enfoque de rechazar todo y un modelo de permisos (whitelist), en la que todas las peticiones que no encajan en un perfil de aplicación se bloquean de forma explícita desde el principio. Este perfil se construye dinámicamente en la tecnología / plataforma que utiliza un sitio web. No utilizamos servicios de terceros.
Nivel 2	Motor de lista negra	El segundo nivel utiliza un modelo de bloque de firmas de listas negras construido por el equipo Sucuri dar cuenta de los posibles outliers y amenazas en constante evolución. No utilizamos servicios de terceros..
Nivel 3	Motor de Correlación	El tercer nivel analiza todas las peticiones en la red Sucuri para establecer el perfil del comportamiento del atacante a nivel mundial y aplicarlo a todos los sitios web protegidos por Sucuri. Se trata de un mecanismo de aprendizaje que aplica de forma proactiva actualizaciones a la red tan pronto como las amenazas evolucionan.

Por otra parte, la plataforma de protección emplea Parches Virtuales y un enfoque de Hardening Virtual a su estrategia de mitigación:

PARCHE VIRTUAL	Con parches virtuales, el equipo Sucuri es capaz de responder rápidamente a las nuevas amenazas sin afectar a los sitios web. Todos los parches se aplican en Sucuri. Esto es especialmente efectivo para las organizaciones más grandes con la gobernabilidad estricta de seguridad sobre cuándo y cómo los parches pueden ser aplicados a un entorno de producción. Además, las reglas personalizadas también se pueden aplicar.
HARDENING VIRTUAL	Con el hardening virtual, el equipo de Sucuri es capaz de aplicar parches agnósticos a vulnerabilidades de sitios web. El hardening puede ser específico para la plataforma (es decir, WordPress, Joomla, Drupal, etc.) o más genérico, para un servidor web (por ejemplo Apache / IIS).

La eficacia de la plataforma de protección se limita a su capacidad de ver todo el tráfico entrante. La técnica más común es evitar el ataque directo al servidor de origen. Todo el tráfico directo al servidor de origen debe limitarse a la red de Sucuri.

EXPOSICIÓN D: PREVENCIÓN DE EXPLOIT

La plataforma de protección es capaz de mitigar interceptando todo el tráfico entrante y realizando el análisis en tiempo real de todas las solicitudes de HTTP / HTTPS (es decir, peticiones de capa 7). El tráfico se cifra (mediante HTTPS) y también se debe inspecionar.

Para lograr este objetivo, el end-point debe terminar en la red Sucuri. La plataforma de protección debe interceptar y analizar todo el tráfico para ser eficaz. Todo el análisis se hace en la memoria, en tiempo real - **no hay almacenamiento de los paquetes de petición**. Los únicos datos almacenados son los meta-datos de peticiones en forma de logs de acceso web.

Las organizaciones tienen muchas opciones de SSL:

OPCIÓN 1	El uso de certificados Comodo DV generados por Sucuri.
OPCIÓN 2	El uso de un certificado LetsEncrypt gratuito generado por Sucuri.
OPCIÓN 3	El uso de un certificado personalizado generado por la organización.
OPCIÓN 4	Sucuri ofrece un CSR para que las organizaciones generen un certificado a través de su propia CA.

EXPOSICIÓN E: INSTALACIÓN Y CONFIGURACIÓN

Cada plataforma tiene sus propios requisitos de configuración y despliegue, pero cada una de ellas está diseñada para ser simple y requiere una baja sobrecarga y compromiso. Los requisitos son los siguientes:

PLATAFORMA DE PROTECCIÓN	No requiere instalación. Un cambio en el A-record vía DNS. También es compatible con la gestión de DNS completa a través del cambio de nameservers. La hora de ir en vivo depende del tiempo del valor Time to Live (TTL).
PLATAFORMA DE MONITOREO	No requiere instalación. Escaneo remoto: Los dominios se cargan en el panel de Sucuri vía API o interfaz del panel. Escaneo del servidor: agentes de dominio PHP se cargan en el root de cada directorio del sitio web en el servidor web. ** Requiere acceso SFTP / FTP / SSH para cargar archivos. La organización puede optar por cargar los archivos por su cuenta.
PLATAFORMA DE RESPUESTA	No requiere instalación. En el caso de un incidente, todos los eventos son manipulados y manejados a través del sistema de tickets de Sucuri. El soporte y acuerdo de nivel de servicio (Service Level Agreement - SLA) están en su contrato. Requiere acceso al servidor vía SFTP/FTP/SSH. Los cambios se pueden negociar en su contrato.
PLATAFORMA DE COPIAS DE SEGURIDAD	No requiere instalación. El soporte y acuerdo de nivel de servicio (Service Level Agreement - SLA) están en su contrato.

Algunos contratos incluyen soporte al cliente y servicios de integración. Algunos acuerdos incluyen soporte personalizado e integración de servicios. Lea su contrato o hable con el administrador de su cuenta para fines específicos relativos a la aplicación de cada plataforma y las responsabilidades asociadas.

EXPOSICIÓN F: OPTIMIZACIÓN DE DESEMPEÑO Y CACHING

Todo el contenido estático se almacena en caching cuando posible. Esto permite una respuesta más rápida a las peticiones (500 ms vs 10 ms) y escalas (50 usuarios simultáneos vs 200k usuarios simultáneos). Las plataformas más conocidas, como Wordpress, Joomla, Drupal y otras aplicaciones CMS similares utilizan cookies, lo sabemos y explicamos cómo nuestra memoria caching funciona.

La función de caching funciona a través de la construcción de una clave de caching. Cada petición que coincide con la clave recibe la misma página. La clave de caching consiste en el protocolo HTTP o HTTPS, dominio, solicitud URI y el agente de usuario estándar (dispositivo móvil, desktop, tablet o RSS bot). Esto significa que los usuarios de diferentes plataformas (desktop vs dispositivo móvil) no verán el mismo contenido.

OPCIONES DE CACHING

La plataforma ofrece cuatro tipos de caching:

OPCIÓN	DESCRIPCIÓN DE LA OPCIÓN	TIEMPO
Activado (Recomendado)	Almacena caching de todo el sitio web y sólo elimina la memoria caching en pocas horas.	All - 3 hrs +
Caching Mínimo	Almacena caching de todo el sitio web y sólo elimina la memoria caching en pocos minutos	200 - 8 m 404 - 2 m 302 - 15 m 301 - 15 m
Caching del Sitio Web (Encabezados de Sitios Web)	Almacena caching del contenido estático y respeta los encabezados del sitio web.	200 - 180 m 404 - 10 m 302 - 180 m 301 - 180 m
Desactivado (Utilizar con precaución)	Sólo almacena caching del contenido estático, como imágenes, .css, .js, .pdf, .txt,.mp3 y algunas otras extensiones.	200 - 1 m 404 - 1 m 302 - 10m 301 - 10m

ELIMINANDO CACHING

La eliminación de la memoria caching es una característica crítica de la plataforma. Permitimos que el caching se elimine a través del Panel Sucuri o API WAF. Una vez iniciado, el caching se propaga a través de la red y limpia todos nodos en segundos.

EXPOSICIÓN G: SEGURIDAD DE LA INFRAESTRUCTURA Y COMPLIANCE

Cada centro de datos funciona a partir de sus necesidades y cumple o excede todos los estándares y regulaciones de compliance:

REGULACIONES DE COMPLIANCE

SSAE16 COMPLIANCE
OHSAS 18001:2007
PCIDSS PAYMENT CARD INDUSTRY STANDARD
ISO CERTIFICATION
ISO 9001:2008
ISO 14001:2004
ISO / IEC 27001:2005 AND 27001:2013
ISO 50001:2011

INFRAESTRUCTURA DE LA RED

La red Sucuri consta de varios proveedores de tránsito en cada punto que se utiliza para el encaminamiento del tráfico primario, enrutamiento interno, y redundancia de tráfico.

El uso de una red compartida con una terminación primaria y secundaria para cada conexión evita que un punto falle.

OPERACIONES

- Dispositivo diario de escaneo de vulnerabilidades realizado internamente
- Escaneo diario de vulnerabilidades y escaneo de compliance realizada por terceros
- Pruebas de penetración internas y pruebas de terceros
- Documentación, prácticas y educación continua del personal
- Procedimientos de gestión y modificación del Firewall
- Clasificación de datos y de propiedad
- Gestión de Incidencias
- BCP (Business Continuity Plan) y DRP (Disaster Recovery Plan)
- Monitoreo de la red y revisión de log continuo

GESTIÓN Y RECURSOS HUMANOS

- Formación de concienciación de seguridad obligatorias y evaluación para cada empleado
- Prácticas de acceso de menor privilegio en todos los equipos
- Acuerdos de no divulgación y confidencialidad
- Comprobación de background y evaluación de competencias
- Gestión activa en todos los aspectos de la comunidad de seguridad
- Mantenerse actualizados en el mundo cibernético que siempre cambia

sucuri.net | 1.888.873.0817 | sales@sucuri.net