Services & Training Portfolio

EXCLUSIVE NETWORKS

Servicios Profesionales

Experiencia técnica, allí donde la necesite

Nuestros Servicios Profesionales aportan experiencia técnica especializada a cualquier solución de nuestro portfolio, ayudando a partners y clientes a desplegar, migrar, optimizar y adoptar tecnología con confianza.



Modelo de servicio

Asistencia técnica

- Soporte bajo demanda prestado por ingenieros certificados o expertos.
- Servicio por tareas, con precio según el perfil y el número de días.
- Refuerce su equipo con especialistas siempre que los necesite.

Oferta personalizada

- Adaptada al contexto y los objetivos específicos del cliente.
- Desarrollada a partir de una sesión de descubrimiento con el cliente o partner.
- Adaptada a los requisitos de la RFP, con condiciones específicas de la oferta.



Por qué es importante

- Experiencia flexible que se adapta a cada proyecto.
- Ingenieros certificados en todo nuestro portfolio tecnológico.
- Despliegue y adopción de tecnología fluidos.
- Alcance y precios claros para agilizar la toma de decisiones.
- Aumente el negocio en las tecnologías que no conoce.

Nos enorgullece nuestra experiencia multivendor, con un equipo técnico capacitado en las principales tecnologías del sector y la capacidad de prestar servicios en varios idiomas (inglés, francés, italiano o español).

Trabajamos con fabricantes líderes como:

Vendor	Technologies
Fortinet	Fortigate, FAZ,FMG, SD-WAN, Wi-Fi, NAC, EMS, Mail, Web, FAC, SASE, ZTNA
F5	BIG-IP application delivery & security (LTM, Advanced WAF, APM, DNS).
Palo Alto	Next-gen firewalls (Strata), cloud & SASE (Prisma Access), SOC analytics & XDR (Cortex).
Infoblox	DDI core network services (NIOS, BloxOne) y seguridad DNS.
SentinelOne	Detección y respuesta en endpoints para clientes y dispositivos móviles.
One Identity	Gestión de identidades y accesos privilegiados (OneLogin, PAM).
Extreme Networks	Redes cableadas e inalámbricas gestionadas desde la nube (XIQ, NAC).
Tenable	Escaneo de vulnerabilidades y gestión del riesgo cibernético.
Nozomi	Redes: monitorización de redes OT e ICS y detección de anomalías.
Netskope	Plataforma cloud-native Secure Access Service Edge (SASE).
Zyxel	Seguridad y conectividad de red (firewalls, Wi-Fi, switching).
Forescout	Control de acceso a la red, incluida la seguridad de dispositivos IoT/OT.
Proofpoint	Seguridad avanzada del correo electrónico y formación en concienciación sobre seguridad.
TXOne	Protección especializada de endpoints OT para sistemas industriales.
Zero networks	Microsegmentación de red y aplicación de Zero Trust.
IMPERVA	Cloud Web Application Firewall y soluciones de seguridad de datos.

Catálogo completo de servicios

Descubra nuestro portfolio completo de Servicios Profesionales, diseñado para ayudar a partners y clientes a evaluar riesgos, reforzar la seguridad, simplificar despliegues y migraciones y mantener la continuidad operativa en entornos modernos de IT y OT.



01 Services around the box

02 Vulnerability Assessment

03 Pentest

04 Fortinet Trade-Up

05 Tech bundle

06 SASE

07 OT

08 RMA management

09 Wi-Fi survey

10 Fortinet Conversion as a Service

11 Awareness

01

Services around the box

Del almacén a producción: totalmente preparado

Service Around the Box es nuestro compromiso para simplificar y acelerar los despliegues sin comprometer la calidad. Podemos ayudar desde el staging hasta la entrega local.



Qué incluye

- Preparación y preconfiguración en nuestros almacenes
- Configuración totalmente personalizable
- Envío a cualquier ubicación, incluida la entrega directa al cliente final
- Rack & stack, instalación y pruebas in situ en todo el mundo



Por qué es importante

- Ahorro de tiempo significativo durante el despliegue
- Experiencia de alto nivel en la fase más crítica
- Precios claros y fijos, sin sorpresas
- Sin costes de desplazamiento innecesarios

02

Vulnerability Assessment

Nuestra Evaluación de Vulnerabilidades ofrece a sus clientes una visión clara de su exposición al riesgo cibernético, al descubrir vulnerabilidades ocultas y configuraciones incorrectas en su entorno de IT.

Valor para nuestros partners

Abre oportunidades para proyectos posteriores destinados a corregir los problemas identificados; orienta las conversaciones con los clientes hacia riesgos y soluciones reales; y refuerza su credibilidad como asesor de seguridad de confianza.

Alcance

Escaneo integral de vulnerabilidades del entorno de IT del cliente (on-premise, cloud e híbrido); análisis en profundidad y priorización de los hallazgos; entrega de un informe técnico detallado y un resumen ejecutivo orientado a la dirección; propuesta de un plan de remediación priorizado.

03 Pentest

Escenarios de ataque reales, información de seguridad real.
Nuestros servicios de Pentest simulan cómo atacarían realmente los atacantes a una organización.
Nuestros enfoques de evaluación:

Web Applications Pentest

- Pruebas black-box y grey-box.
- Enfoque en plataformas orientadas al cliente.
- Identificación de fallos de aplicación y de lógica.

External Pentest

- Pruebas black-box de activos expuestos a Internet.
- Simula amenazas procedentes del exterior de la organización.

Internal Pentest

- Simula usuarios comprometidos o amenazas internas.
- Evalúa el movimiento lateral y la escalada de privilegios.

El resultado

- Visibilidad clara de las vulnerabilidades explotables.
- Recomendaciones prácticas para reforzar las defensas.

04

Fortinet Trade-Up

Actualizar un firewall o dispositivo de seguridad ya no tiene por qué interrumpir las operaciones de su cliente.

Con nuestro servicio Fortinet Trade-Up, migramos la configuración existente de un dispositivo Fortinet antiguo a un nuevo modelo y entregamos la nueva unidad preconfigurada y lista para desplegar.

Un ingeniero experimentado de Fortinet se encarga de la conversión para garantizar la precisión.

Incluso podemos enviar el nuevo dispositivo directamente a las instalaciones del cliente final, donde puede instalarse inmediatamente con un tiempo de inactividad mínimo.

Todo el proceso es ágil y transparente, con una lista clara de precios fijos para que usted y su cliente conozcan el coste de antemano y se beneficien de una actualización rápida dirigida por expertos.



05

Tech bundle

Nuestros Tech Bundles son ofertas de servicios preconfiguradas que añaden valor a la venta de productos, ideales para nuevas oportunidades, renovaciones tecnológicas o migraciones de productos al final de su vida útil. Con cada nueva venta de tecnología, podemos incluir:



Nuevas oportunidades y renovaciones tecnológicas

Incluya una sesión de actualización tecnológica con cada nueva venta de una solución, para garantizar que los clientes aprovechen al máximo las últimas funcionalidades desde el primer día.

Transiciones de fin de vida útil

Ofrezca un taller técnico al sustituir productos al final de su vida útil, con el fin de planificar una migración fluida a plataformas más modernas.

Servicios preconfigurados

Cada Tech Bundle está predefinido con un precio fijo, basado en el número de dispositivos o en el alcance, lo que proporciona un ámbito claro y un coste predecible para facilitar el upselling..

06

SASE

Experiencia de fabricantes y tecnologías cubiertas:

Netskope

Seguridad basada en la nube para el acceso web y SaaS, que permite una conectividad segura y de alto rendimiento para usuarios remotos.
Tecnologías cubiertas: SASE, ZTNA.

Palo Alto Networks

Prisma Access y Zero Trust Network Access, que extienden políticas de seguridad coherentes a los usuarios estén donde estén.
Strata, Cortex, Prisma Access.

Fortinet

Secure SD-WAN, seguridad entregada desde la nube y ZTNA integrados en el framework SASE de Fortinet.
FortiGate, SD-WAN, SASE, ZTNA, firewalling y seguridad avanzada.

Qué ofrecemos

- Diseño y despliegue de arquitecturas SASE
- Convergencia de redes y seguridad en un único modelo habilitado para la nube
- Despliegue adaptado a los usuarios, las ubicaciones y los requisitos de seguridad de cada organización

Resultados clave

- Acceso seguro a aplicaciones y recursos desde cualquier lugar.
- Arquitectura unificada de redes y seguridad.
- Aplicación coherente de políticas en todos los usuarios y ubicaciones.
- Soporte para entornos remotos, híbridos y distribuidos.

07

OT Security Services

Protección de entornos industriales sin interrumpir las operaciones

Experiencia de fabricantes y tecnologías cubiertas:

Nozomi Networks

Evaluación, despliegue y ajuste de plataformas de monitorización para entornos OT/ICS, que proporcionan visibilidad avanzada y detección de anomalías. Tecnologías cubiertas: OT Security, monitorización OT/ICS, visibilidad de activos y detección de anomalías.

Fortinet

Segmentación y protección de activos industriales mediante soluciones robustas e integración IT/OT dentro de Security Fabric. Tecnologías cubiertas: soluciones de seguridad robustas, Security Fabric, integración IT/OT, segmentación y firewalling.

TXOne Networks

Protección de endpoints industriales, sistemas legacy y dispositivos sin parches en entornos de producción. Tecnologías cubiertas: OT Security, protección de endpoints industriales, protección de sistemas legacy y aislamiento de red.

Qué ofrecemos

- Servicios de seguridad especializados para entornos OT e ICS
- Un enfoque que equilibra la protección cibernética con la continuidad operativa
- Servicios prestados sobre tecnologías de fabricantes líderes.

Resultados clave

- Mayor visibilidad de los sistemas de control industrial
- Menor exposición a amenazas cibernéticas en entornos OT
- Segmentación de activos industriales críticos
- Protección de sistemas legacy y difíciles de parchear

08

RMA Management

Sustitución rápida, interrupción mínima

Qué gestionamos

- Diagnóstico inicial del equipo defectuoso.
- Apertura del ticket de soporte y solicitud de sustitución al fabricante.
- Coordinación con fabricantes y partners logísticos.
- Seguimiento del envío de la unidad de sustitución.
- Puesta en marcha in situ cuando sea necesario.

Ventajas del servicio

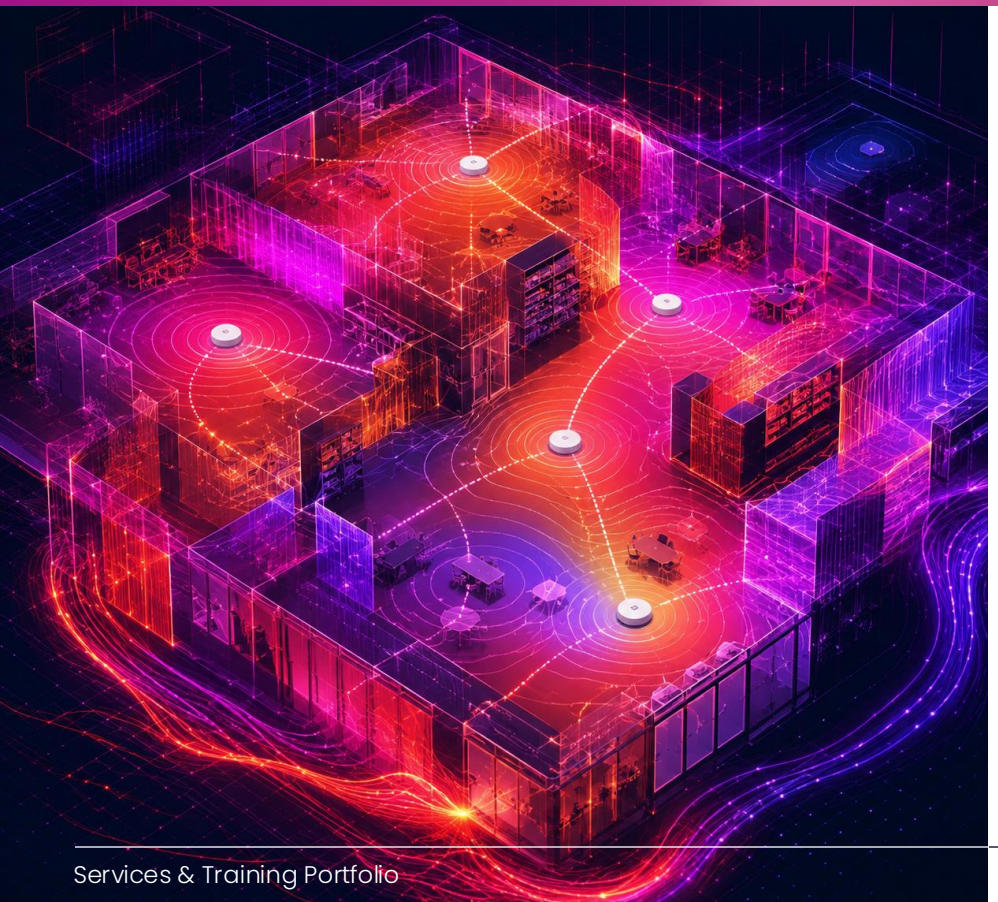
- Gestión integral de la sustitución de hardware defectuoso.
- SLA fijo para una mayor previsibilidad.
- Cobertura local en más de 150 países.
- Reducción del tiempo de inactividad operativo.



09

Wi-Fi Survey

Cobertura inalámbrica fiable,
diseñada desde el principio



Qué analizamos

- Propagación de la señal de radio en todo el emplazamiento mediante simulación RF
- Impacto de paredes, cristal, estanterías y otros materiales estructurales
- Número y ubicación óptimos de los puntos de acceso
- Informe posterior al estudio que detalla los resultados del análisis y los requisitos para una instalación óptima.

Resultados clave

- Cobertura Wi-Fi sólida y uniforme, sin zonas muertas
- Menos rediseños y cambios de cableado
- Despliegue más rápido y preciso
- Menor tiempo y coste de instalación

10

Fortinet Conversion as a Service

Migraciones seguras y optimizadas, sin interrupciones. Simplificamos las migraciones complejas de firewalls con un enfoque sin riesgos dirigido por expertos

Capacidades de migración

- Conversión rápida y precisa de la configuración
- Migración desde plataformas legacy de Fortinet
- Migraciones cross-vendor desde soluciones de terceros
- Tiempo de inactividad mínimo y continuidad del servicio
- Premigración completada en nuestro almacén antes de la entrega in situ

Revisión experta de la configuración

- Sin errores de transcripción manual
- Revisión por expertos certificados de Fortinet

Optimización y hardening

- Eliminación de reglas obsoletas o redundantes
- Consolidación de políticas
- Aplicación de las mejores prácticas de Fortinet
- Mejora de la postura de seguridad y del rendimiento

11

Awareness

Construir la capa humana de la seguridad

Nuestros Awareness Managed Services ayudan a las organizaciones a reducir el riesgo humano mediante formación y pruebas continuas



Qué ofrecemos

Formación adaptada a los usuarios y las amenazas

- Contenido basado en roles y orientado por las amenazas
- Evaluaciones y encuestas periódicas a los usuarios
- Aprendizaje multiformato: vídeos, cuestionarios y artículos



Pruebas reales

Simulaciones basadas en escenarios de ataque reales

- Simulaciones de ingeniería social
- Campañas de phishing
- Pruebas alineadas con las amenazas actuales



Impacto en el negocio

Concienciación que puede medirse a lo largo del tiempo

- Mayor concienciación sobre seguridad
- Reducción de comportamientos de riesgo
- Mejora medible a lo largo del tiempo

Formación

En Exclusive Networks aspiramos a ser

Su partner de referencia para formación tecnológica

capacitando a su equipo con los conocimientos necesarios para aprovechar las soluciones más innovadoras.



Lo que ofrecemos es un portfolio completo de cursos certificados por los fabricantes, impartidos en un entorno de aprendizaje **estimulante e interactivo.**

Cómo lo hacemos: mediante formadores experimentados y certificados que ofrecen orientación personal a cada alumno, asegurándose de que nadie se quede atrás.

Nuestra misión es ofrecer formación de **alta calidad** que no solo ayude a los participantes a superar los exámenes de certificación, sino que les permita aplicar eficazmente sus nuevas competencias en situaciones reales. En resumen, combinamos contenidos de primer nivel con un enfoque dinámico para convertir el aprendizaje en éxito empresarial.

Descripción general del portfolio

Como partner de formación autorizado, ofrecemos distintos formatos de formación impartidos por formadores autorizados y en varios idiomas, para adaptarnos a diferentes necesidades y horarios.

Disponibles en italiano, inglés, español y francés.

Formación oficial:

Cursos completos y en profundidad, impartidos por instructores certificados, que combinan teoría y práctica. Son clases interactivas que preparan exhaustivamente a los participantes para los exámenes oficiales de certificación, al tiempo que desarrollan competencias prácticas.

Bootcamps:

Sesiones intensivas centradas en tecnologías o casos de uso específicos. Los Bootcamps están dirigidos por formadores expertos e incluyen talleres o laboratorios para profundizar en temas avanzados en poco tiempo.

Sesiones de formación rápida:

Talleres rápidos y específicos de entre 1 y 3 horas, diseñados para proporcionar conocimientos o competencias clave sobre un tema concreto. Los Fast Track ayudan a los equipos a actualizar rápidamente sus competencias sobre nuevas funcionalidades o conceptos, sin comprometerse con un curso de varios días.

Soluciones de formación personalizadas:

Si nuestra oferta estándar no responde exactamente a sus necesidades, podemos diseñar un programa de formación específico para su organización, desde el desarrollo de un temario personalizado hasta una planificación flexible, para garantizar que reciba exactamente lo que necesita.

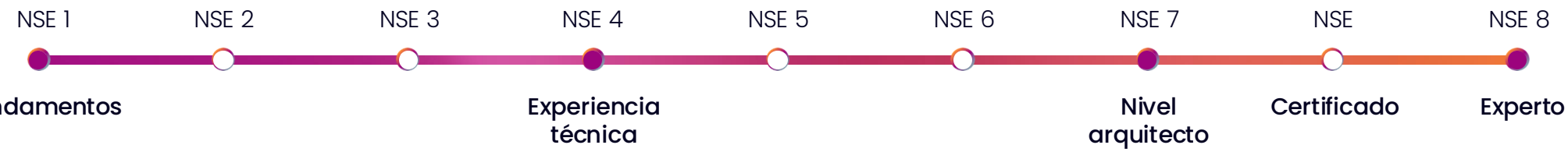
Ofrecemos formación para múltiples fabricantes líderes



Rutas de certificación de Fortinet

Ayudamos a su equipo a recorrer el completo itinerario de certificación NSE de Fortinet, desde NSE 1 (conceptos fundamentales) hasta NSE 7 (nivel arquitecto).

El programa de Fortinet está estructurado de forma que cada nivel se basa en las certificaciones activas de los niveles anteriores y cubre especializaciones en Secure Networking, SASE (Secure Access Service Edge), Cloud Security y Security Operations. Siguiendo este itinerario, los ingenieros pueden avanzar desde la administración básica de FortiGate hasta el diseño y la gestión integral del Security Fabric de Fortinet, y nosotros ofrecemos la formación necesaria en cada etapa para ayudarles a conseguirlo.

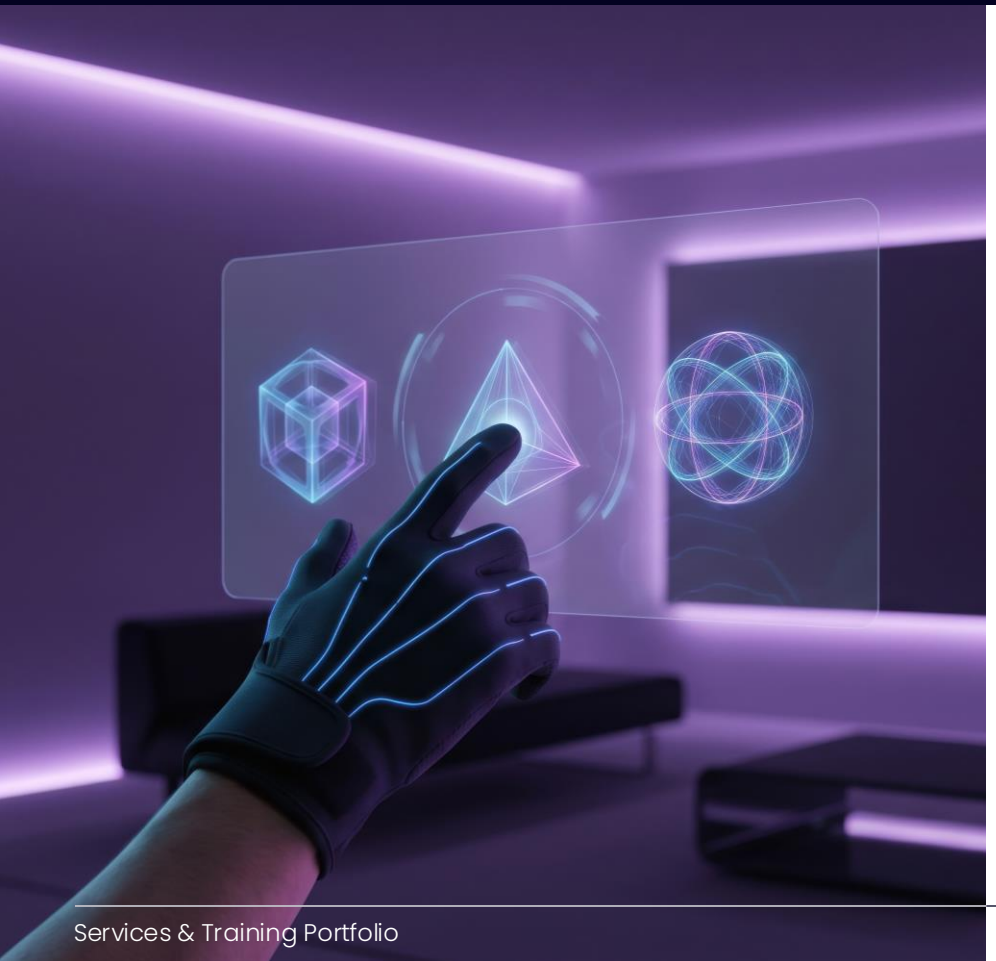


Rutas de certificación de Fortinet

Niveles	Secure networking	SASE	Cloud	Security operations
NSE4	FORTIOS ADMINISTRATOR			
NSE5	FortiSwitch / Secure Wireless LAN / SD-WAN Core	SASE and Sd-wan Core / Administrator	FortiWeb / FortiADC / FortiAppSec	FortiAnalyzer Analyst
NSE6	FortiManager / FortiAnalyzer Admin / FortiNAC / FortiVoice	FortiClient EMS FortiEDR / FortiDLP	FortiMail / FortiMail / Workspace / FortiDDoS / FortiCNAPP Analyst	FortiSOAR Analyst / FortiSIEM Analyst / FortiRecon Analyst / FortiNDR Analyst / FortiDeceptor
NSE7	Secure Networking Architect	SASE Architect	Public Cloud Security Architect	Security Operations Architect
NSE CERTIFIED	MSSP Security			
	OT Security			
NSE8	EXPERT			

Fortinet Bootcamps

Como complemento a la formación oficial, organizamos Fortinet Bootcamps específicos que profundizan en temas de alta demanda.



Estas sesiones intensivas están diseñadas para elevar rápidamente las competencias en áreas de solución concretas. Por ejemplo, nuestro Bootcamp **Zero Trust Network Access (ZTNA)** aborda la implementación integral mediante FortiGate, FortiAuthenticator y FortiClient. También ofrecemos un **FortiSASE Bootcamp**, centrado en la oferta SASE de Fortinet, y un **FortiPAM Bootcamp** para Privileged Access Management.

Cada Bootcamp es una experiencia práctica y de profundización dirigida por expertos en la materia, que garantiza que los participantes adquieran un dominio práctico de estas soluciones avanzadas de Fortinet.

Fortinet Bootcamps

Como complemento a la formación oficial, organizamos Fortinet Bootcamps específicos que profundizan en temas de alta demanda.

Bootcamp	Productos				
	FortiGATE	Forti Authenticator	FortiPAM	FortiCLIENT	FortiSASE
Forti Authenticator					
ZTNA					
Bootcamp FortiSASE					
FortiPAM					

Rutas de certificación de Palo Alto

Palo Alto Networks:

Cursos oficiales como Firewall Configuration & Management (EDU-210), gestión de Panorama, Firewall Troubleshooting, diseño y operación de Prisma Access SASE y formaciones de Cortex XDR/XSIAM, entre otros. Estas propuestas ayudan a los ingenieros a dominar las plataformas de seguridad de Palo Alto y a obtener la certificación Network Security Professional y otras certificaciones.



Rutas de certificación de Palo Alto

Formación	Certificación							
	Network Security Professional	Next-Generation Firewall Engineer	Security Service Edge Engineer	SD-WAN Engineer (Pro)	SD-WAN Engineer (Specialist)	XSIAM Analyst	XDR Analyst	XDR Analyst/ Engineer
Firewall: Configuration & Management (EDU-210)	✓							
Panorama: NGFW Management (EDU-220)	✓	✓						
Firewall: Troubleshooting (EDU-330)		✓						
Prisma Access SSE Configuration and Deployment (EDU-318)			✓					
Prisma SD-WAN Advanced Ops						✓		
Prisma SD-WAN 6.0: Design and Operation (EDU-238)					✓			
Cortex XSIAM: Investigation and Analysis (EDU-272)				✓				
Cortex XDR: Prevention and Deployment (EDU-260)							✓	
Cortex XDR (EDU-160)								✓

Infoblox

Formación sobre productos, laboratorios prácticos y certificaciones reconocidas por el sector.

INE Training

Objetivos del curso y competencias adquiridas. Al finalizar la formación, los participantes podrán:

- Comprender y seguir los procedimientos de soporte de Infoblox.
- Abrir y gestionar tickets de soporte con Infoblox Technical Support.
- Resolver problemas relacionados con la interfaz gráfica de Infoblox.
- Diagnosticar y resolver problemas relacionados con DHCP.
- Diagnosticar y resolver problemas relacionados con DNS.
- Prepararse para el correspondiente examen de certificación de Infoblox.

INO / INA Training

Objetivos del curso y competencias adquiridas
Al finalizar la formación, los participantes podrán:

- Comprender el concepto y el funcionamiento de Infoblox GRID.
- Identificar y definir las funciones de los diferentes dispositivos y componentes de la infraestructura.
- Utilizar eficazmente la interfaz gráfica de Infoblox.
- Configurar y gestionar servicios DNS.
- Configurar y gestionar servicios DHCP.
- Configurar y utilizar funciones de reporting.
- Configurar y utilizar funcionalidades de IP Address Management (IPAM).

BloxOne™ Threat Defense (B1TD) 8.4 V1

Al finalizar la formación, los participantes podrán:

- Comprender y gestionar un entorno Infoblox GRID.
- Utilizar eficazmente la interfaz gráfica de Infoblox.
- Configurar y administrar servicios DNS, incluidos DNSSEC y DNS Firewall.
- Utilizar TIDE, Dossier y Threat Insight para el análisis y la protección frente a amenazas.
- Configurar capacidades de reporting e integrar Active Directory Protection (ADP).

F5

AUTHORIZED TRAINING CENTER

Cursos impartidos por instructores, diseñados para ayudarle a desarrollar los conocimientos y la experiencia práctica necesarios para desplegar, configurar y gestionar productos F5.

F5 Networks:

- F5: Configuration Local Traffic Manager (LTM)
- Configuring BIG-IP DNS
- Configuring BIG-IP AFM: Advanced Firewall Manager
- Configuring BIG-IP DNS
- Configuring BIG-IP AFM: Advanced Firewall Manager
- Administration Big-IP
- F5 : Advanced WAF (AWAF)
- Developing iRules for BIG-IP
- F5 : Access Policy Manager (APM)



Formación de Microsoft Azure

Además de nuestro programa centrado en la seguridad, ofrecemos formación oficial de Microsoft Azure para ayudar a los partners a responder a la demanda de cloud.



Nuestros cursos de Azure son programas completos de cuatro días impartidos por Microsoft Certified Trainers e incluyen:

Azure Administrator (AZ-104) – cubre todos los aspectos de la gestión de recursos e infraestructuras de Azure, desde computación y almacenamiento hasta identidad y gobierno, para que los administradores puedan gestionar eficazmente los entornos Azure.

Azure Security Technologies (AZ-500) – enseña a los profesionales de seguridad de IT a implementar controles de seguridad sólidos en Azure, gestionar la postura de seguridad de una organización y detectar y corregir vulnerabilidades en cargas de trabajo cloud.

Azure AI Engineer (AI-102) – prepara a los profesionales para diseñar, desarrollar y desplegar soluciones de inteligencia artificial mediante Azure Cognitive Services, bots y otras herramientas de IA, permitiéndoles integrar capacidades de IA en aplicaciones empresariales.

Exclusive Training Centre

Nuestro centro de formación también abarca otros fabricantes y tecnologías clave:

Netskope

Netskope Security Cloud Operation and Administration

El curso comienza con una introducción a la plataforma Netskope y a la interfaz de usuario. A continuación, aborda aspectos clave de la plataforma como la creación de políticas, DLP, Threat Protection, Netskope NG-SWG, la protección de datos en la nube pública con Netskope, la generación de informes y análisis y otras funciones esenciales. El curso incluye ejemplos y práctica guiada para aplicar políticas basadas en uno o varios factores granulares, como servicio, categoría, usuario, grupo, dispositivo, contenido, perfil de data loss prevention (DLP) y otros.

Netskope Security Cloud Implementation and Integration

El curso Netskope Security Cloud Implementation and Integration (NSCI&I) es una formación en profundidad sobre Netskope Security Cloud Platform, dirigida por un experto de Netskope. Este curso de tres días cubre SAML, Netskope Private Access (NPA), Advanced DLP, Web Security, Netskope Advanced Analytics, Netskope REST API, Security Posture Management, Netskope Remote Browser Isolation (RBI) y Netskope Cloud Exchange. El curso incluye ejemplos y práctica guiada sobre cómo implementar e integrar la plataforma Netskope en un entorno empresarial.

Extreme Networks:

Formación en switching y gestión de redes, desde la instalación y configuración de Extreme Switching hasta redes fabric avanzadas y resolución de incidencias. Estos cursos ayudan a los partners a ofrecer soluciones expertas de redes cableadas e inalámbricas.

Formación rápida

Nuestra serie de formación rápida ofrece laboratorios breves sobre numerosas tecnologías, ideales para profesionales con poco tiempo que necesitan conocimientos aplicables en menos de dos horas.

Estas sesiones permiten a partners y clientes explorar funcionalidades o casos de uso específicos en un entorno guiado.

Por ejemplo, pueden ponerse al día sobre la plataforma de gestión cloud Nebula de Zyxel, incluida la gestión multi-tenant de Wi-Fi y switches; convertirse en un «héroe» de Fortinet en menos de una hora con sesiones como “From Zero to IPS Hero” o “SD-WAN in 60 Minutes”; conocer el control cloud de Extreme Networks; o profundizar en las mejores prácticas de protección frente a amenazas de WatchGuard. Estas sesiones condensan lo esencial en un formato dinámico y práctico, para que su equipo pueda aprender y aplicar nuevas competencias rápidamente.

Otra oferta formativa

Completamos nuestra oferta formativa con programas especializados de ciberseguridad que desarrollan competencias avanzadas basadas en perfiles profesionales:

Certified Ethical Hacker (CPEH): forma a los profesionales en técnicas avanzadas de penetration testing y explotación de vulnerabilidades para que puedan evaluar y reforzar las defensas de las organizaciones.

SOC Analyst Path: itinerario completo que lleva a los participantes desde los fundamentos de la monitorización de un SOC (Security Operations Centre) hasta el análisis avanzado de incidentes y la respuesta, ideal para quienes desean desarrollar una carrera en operaciones de seguridad.

Forensic Analyst Path: se centra en la informática forense y enseña a recopilar, analizar y presentar evidencias digitales, competencias esenciales para investigaciones y procedimientos legales posteriores a incidentes de seguridad.

Malware Analyst Path: desarrolla experiencia en el análisis de malware mediante técnicas de análisis estático y dinámico, sin requerir conocimientos avanzados de programación o ingeniería inversa. Los participantes aprenden a diseccionar código malicioso y comprender su comportamiento para mejorar las estrategias de defensa.

CISO Programme: diseñado para actuales o futuros Chief Information Security Officers, este curso desarrolla competencias de liderazgo estratégico en ciberseguridad y gestión del riesgo de la información, ayudando a profesionales experimentados a avanzar hacia puestos ejecutivos de seguridad.



EXCLUSIVE NETWORKS

We Are Exclusive.

Somos un especialista global de confianza en ciberseguridad, que combina experiencia local con alcance internacional. Gracias por consultar nuestro Catálogo Sur de Servicios Profesionales y Formación.

Para obtener más información, visite www.exclusive-networks.com.

Casos de éxito

SD-WAN GLOBALE con Fortinet en Italia.

De despliegues de red complejos y distribuidos a una arquitectura estandarizada, escalable y gestionada de forma centralizada.

El reto

Implementación de una red SD-WAN segura y de alto rendimiento para sedes distribuidas globalmente, con necesidad de despliegue rápido y gestión centralizada.

Qué hicimos

- Modelo de staging centralizado: firewall Fortinet preconfigurado en nuestro almacén
- Despliegue global a escala: instalación mediante ingenieros de campo locales en todo el mundo (EXN PARTNERS)
- Activación remota: configuración y optimización completas realizadas por nuestros expertos

---

Impacto conseguido

- Tiempo de despliegue ↓ (modelo de rollout rápido y repetible)
- Coste operativo ↓ (menor intervención de ingeniería in situ)
- Rendimiento de las aplicaciones ↑ (gestión del tráfico optimizada)
- Visibilidad y control ↑ (monitorización y gobierno centralizados)



SD-WAN-SSE en España

Servicios de despliegue para Palo Alto Networks SD-WAN y SSE.

Servicio basado en una transformación nacional de la infraestructura de red y seguridad mediante el despliegue de soluciones Palo Alto Networks SD-WAN y Secure Service Edge (SSE) en 72 sedes repartidas por toda España. Para garantizar un rollout fluido, eficiente y sin riesgos, se propone un servicio integral de despliegue end-to-end. Este servicio está diseñado para simplificar las operaciones al cubrir logística, instalación in situ, configuración remota y soporte posterior al despliegue, proporcionando una implementación coherente y de alta calidad en todas las ubicaciones.



SDWAN-SSE en España – Descripción general del alcance del servicio

1 - Almacenamiento centralizado de equipos y gestión logística

Todos los dispositivos de Palo Alto Networks se recibirán, almacenarán de forma segura y gestionarán en una instalación centralizada antes del despliegue. Esta fase garantiza: Custodia segura y almacenamiento controlado de los equipos / Gestión completa del inventario y trazabilidad por sede / Preparación del despliegue alineada con el calendario de rollout.

2 - Distribución nacional de equipos

El servicio incluye el envío coordinado de los equipos a cada una de las 72 sedes de España, garantizando:
Entrega puntual conforme al plan de despliegue acordado / Coordinación logística específica por sede / Menor impacto operativo en los equipos locales.

3 - Instalación y conectividad in situ

Una vez entregados, profesionales cualificados realizarán:
Instalación física de los dispositivos en los armarios o racks existentes / Encendido y conexión a los enlaces WAN y a la infraestructura de red local / Validación inicial de la disponibilidad y conectividad del hardware.

4 - Configuración remota y habilitación del servicio

Todos los dispositivos se parametrizarán y configurarán completamente de forma remota, siguiendo las mejores prácticas de Palo Alto Networks y los estándares de seguridad y red del cliente. Esto incluye:
Configuración de SD-WAN y activación del servicio / Integración con servicios SSE / Aplicación de políticas de seguridad, segmentación y priorización del tráfico / Validación funcional end-to-end por sede.

5 - Soporte posterior al despliegue y RMA Management

Para garantizar la continuidad operativa a largo plazo, el servicio incluye soporte posventa centrado en la gestión del ciclo de vida del hardware, que incluye: Gestión end-to-end de RMA (Return Material Authorization) / Coordinación con el fabricante para la sustitución del hardware / Seguimiento y resolución de incidencias hasta la restauración completa del servicio.



Caso de éxito de formación en Francia

¿Qué dicen nuestros partners sobre nosotros?

«En OBS, el desarrollo de las competencias de nuestros equipos técnicos es una prioridad estratégica clave, especialmente en el ámbito de la ciberseguridad. Gracias a Exclusive Networks France, nos beneficiamos de una formación de máxima calidad, impartida por expertos reconocidos y perfectamente alineada con la realidad operativa del mercado. La calidad de la enseñanza, la experiencia técnica y el acompañamiento proporcionado convierten a Exclusive Networks France en un partner esencial para acelerar el desarrollo de las competencias de nuestros empleados».

Bruno Charrieras
Learning Development Manager

