

2026

Catálogo de Ciberseguridad

NORMICRO
Soluciones Informáticas





Normicro SL

Con 30 años de experiencia, prestamos servicios de soporte informático y atención a puesto de usuario focalizando esfuerzos en acciones preventivas y evolutivas.

+ Secure Tech Solutions.

Pack integral de servicios informáticos.

- Sistemas
- Ciberseguridad
- Monitorización
- Backup

Ciberseguridad

Soluciones de ciberseguridad a medida: acciones de prevención, protección de dispositivos y sensibilización para personal.

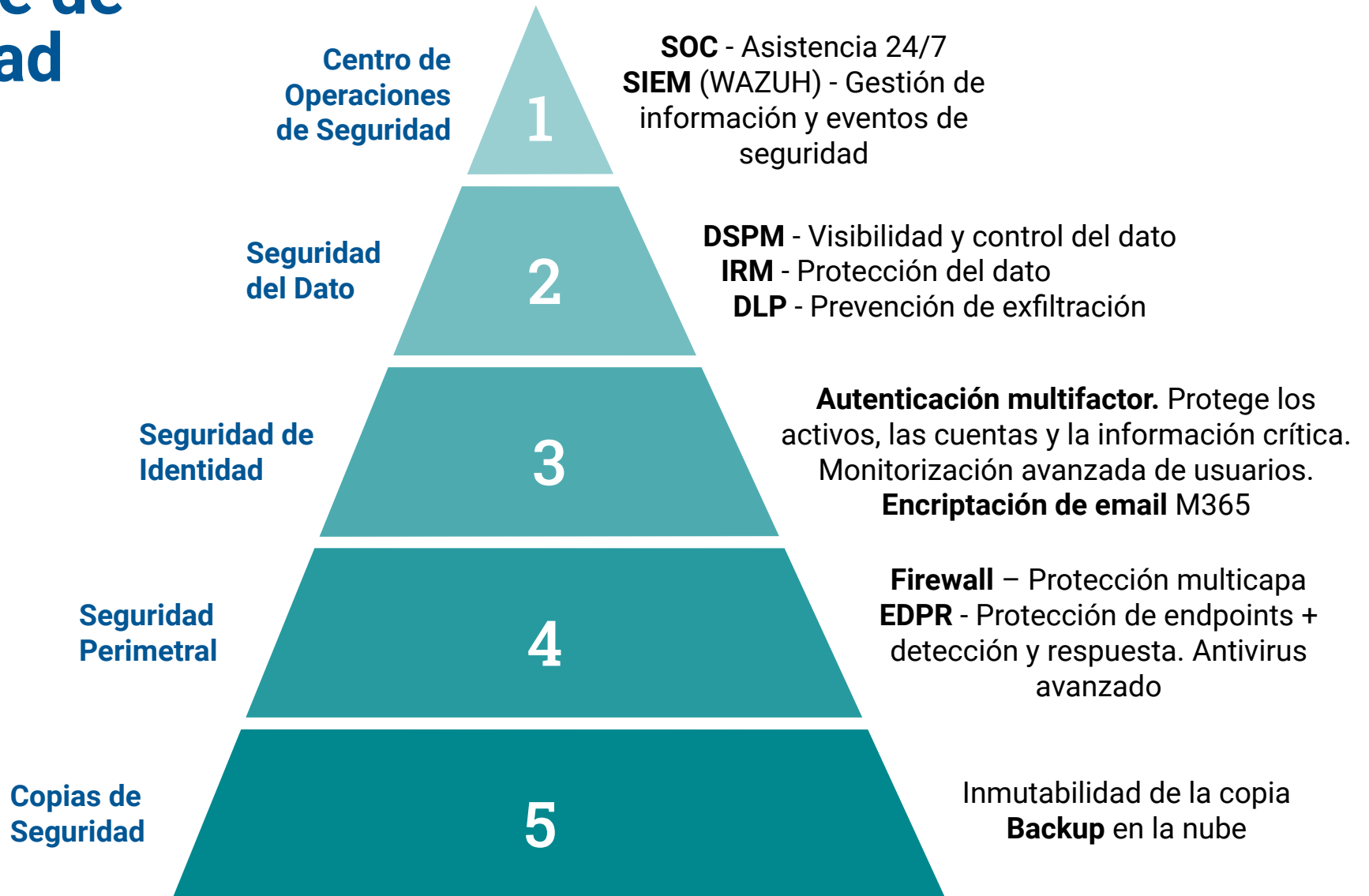


Ciberseguridad

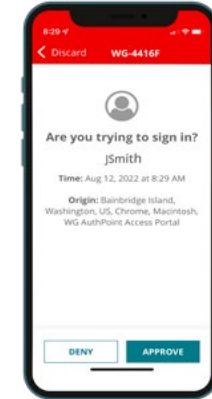
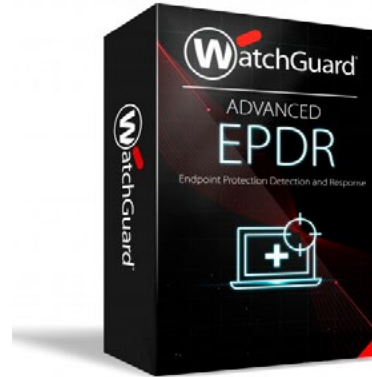
Secure Tech Solutions
Pack integral de servicios informáticos

- + **Protección de dispositivos** y herramientas de securización del puesto de trabajo.
- + Servicios gestionados de dispositivos UTM para **protección perimetral**. Plataforma de seguridad de gestión de recursos.
- + Políticas de seguridad, **formación en concienciación** en ciberseguridad y análisis de riesgos.
- + **Monitorización**, detección de amenazas en tiempo real. Respuesta ante incidentes.

Pirámide de seguridad



Somos
**WatchGuard
Gold Partner**



	WatchGuard EPDR - Seguridad EndPoint	WatchGuard UTM - Seguridad Perimetral	WatchGuard Passport - MFA Authpoint
Nivel de seguridad	Esencial	Medio	Avanzado
	Antivirus avanzado	Cortafuegos	Doble verificación
Protección	Protección de endpoints (EPP) + detección y respuesta (EDR)	Unified Threat Management Protección multicapa	Autenticación multifactor. Proteger los activos, las cuentas y la información crítica.

Consulta precios

Hacemos cotización a la medida de tus necesidades y nº de equipos.

¿Necesitas ayuda? Te asesoramos: comercial@normicro.es

Secure Tech Solutions

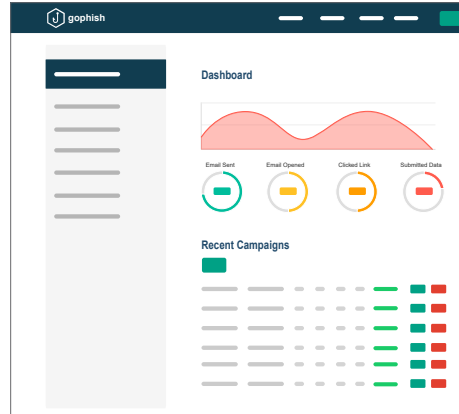
Ciberseguridad

Ofrecemos servicios complementarios para garantizar la correcta instalación y gestión de estas herramientas.



Haz click sobre los productos para ver más

Ofrecemos diferentes capas de ciberseguridad. **Soluciones avanzadas para tu empresa**



	Simulación de ataques - Phising	Auditoría Pentest	Risk Assessment - Análisis de riesgos
Nivel de seguridad	Medio	Medio	Avanzado
	Reducir el riesgo por fallo humano	Identificación de vulnerabilidades	Prevención del ciberriesgo
Protección	Simulación de las tácticas más habituales de Phising y otros vectores de ataque afines.	Recogida en fuentes de acceso abierto de información sobre la empresa.	Evaluación e identificación de los problemas críticos y determinación de plan de intervención.

Consulta precios

Hacemos cotización a la medida de tus necesidades y nº de equipos.

¿Necesitas ayuda? Te asesoramos: comercial@normicro.es

Secure Tech Solutions

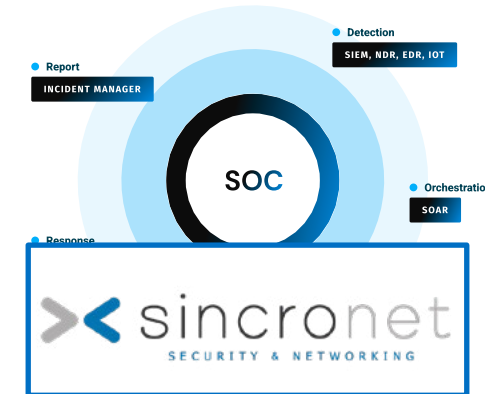
Ciberseguridad

Ofrecemos servicios complementarios para garantizar la correcta instalación y gestión de estas herramientas.



Haz click sobre los productos para ver más

Ofrecemos diferentes capas de ciberseguridad. **Somos Partner Certificado de Arexdata**



	Arexdata DSPM	Sealpath IRM	SOC 24/7
Nivel de seguridad	Avanzado	Avanzado	Avanzado
	Trazabilidad del dato	Prevención de fuga de información	Security Operations Center 24/7
Protección	Seguridad del dato que audita, clasifica y protege el dato	Protección que acompaña al documento tanto en su red como fuera de ella.	Detección, orquestación y automatización de respuesta ante ciberataques.

Consulta precios

Hacemos cotización a la medida de tus necesidades y nº de equipos.

¿Necesitas ayuda? Te asesoramos: comercial@normicro.es

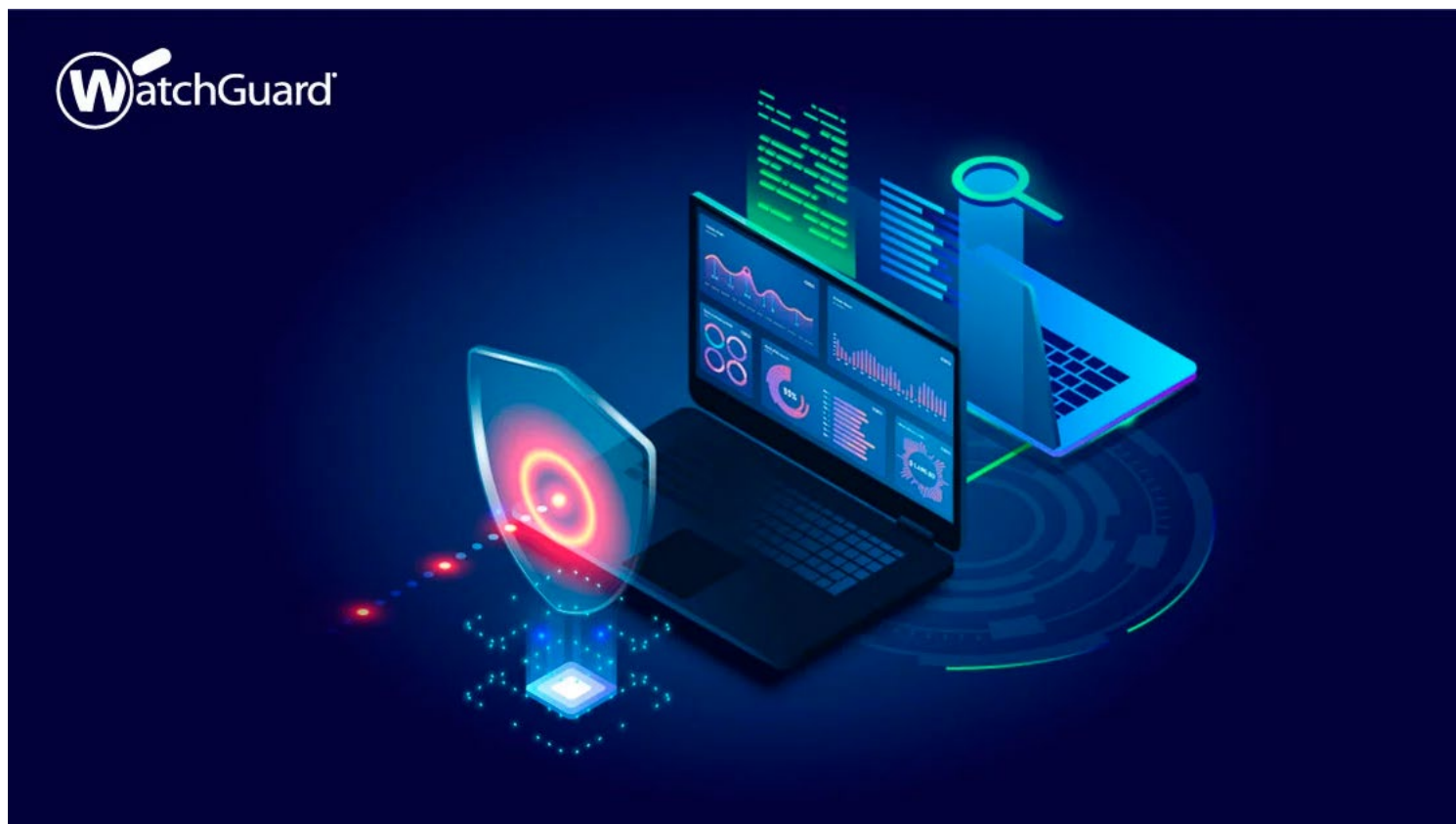
Secure Tech Solutions

Ciberseguridad

Ofrecemos servicios complementarios para garantizar la correcta instalación y gestión de estas herramientas.



Haz click sobre los productos para ver más



Combina las técnicas tradicionales con funciones y servicios avanzados. Al permitir la supervisión continua de los endpoints, la detección y la clasificación de toda la actividad, se puede revelar y bloquear los comportamientos anómalos de usuarios, máquinas y procesos. Al mismo tiempo, descubre proactivamente nuevas técnicas y tácticas de ataques informáticos y evasión para protegerte rápidamente.

**Normicro
somos GOLD
Partner de
WatchGuard**

Antivirus avanzado

WatchGuard EPDR -
Seguridad EndPoint

- + Supervisión continua que impide la ejecución de procesos desconocidos.
- + Análisis de comportamiento y detección de scripts, macros...
- + Detección y respuesta automáticas para ataques dirigidos y vulnerabilidades.
- + Filtrado de direcciones URL, el control de dispositivos y el firewall gestionado.
- + Zero-Trust Application y Threat Hunting se ofrecen como servicios administrados.
- + Un agente ligero y una consola basada en la nube fácil de usar con informes detallados.



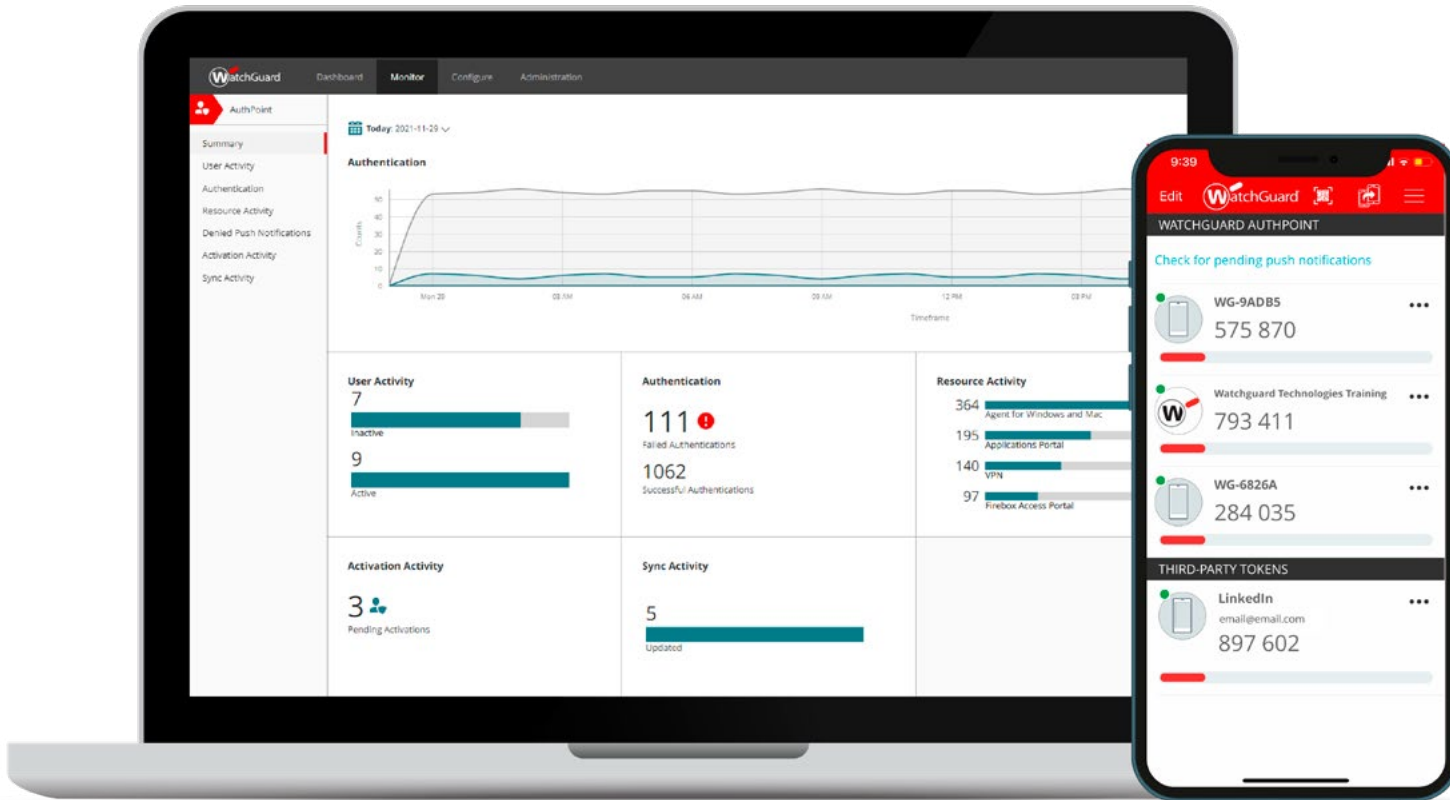
Los dispositivos Unified Threat Management (UTM) están diseñados para facilitar la implementación, el uso y la administración continua, además de proporcionar la mayor seguridad posible. Ofrece la más amplia variedad de servicios de seguridad de red, desde IPS estándar, filtrado de direcciones URL, AV para puerta de enlace (Gateway AV), Application Control y filtro de correo no deseado hasta servicios para combatir las amenazas avanzadas, como sandboxing para archivos, protección contra ransomware y más.

**Normicro
somos GOLD
Partner de
WatchGuard**

Cortafuegos

WatchGuard UTM -
Seguridad Perimetral

- + IPS (Intrusion Prevention Service)
 - + RED (Reputation Enabled Defense Service)
 - + Spamblocker
 - + GAV (Gateway Antivirus)
 - + Webblocker
 - + Application Control
-
- + APT Blocker
 - + Threat Detection & Response
 - + HRP (Host Ransomware Prevention)
 - + DLP (Data Loss Prevention)
 - + Network Discovery
 - + Dimension Command
 - + Access Portal
 - + DNS Watch
 - + IntelligentAV



Doble verificación

WatchGuard
Passport -
MFA Authpoint

+ Autenticación en línea (Push) y sin conexión (código QR y OTP).

+ Servicio en la nube con costo total de propiedad bajo.

+ Control de ADN de dispositivo móvil para una coincidencia de identidad eficaz.

+ Incluye protección de inicio de sesión en PC, VPN y nube.

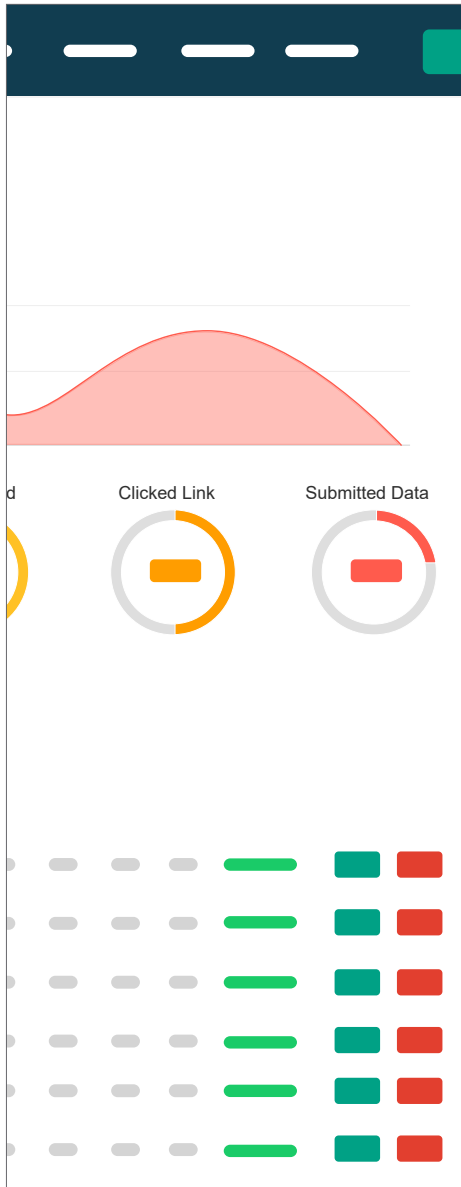
+ Proteja fácilmente las apps en la nube y en la VPN, y los servicios web con las guías de integración.

+ Aplicación móvil liviana y con funcionalidades completas en 13 idiomas.

Es una solución de autenticación multifactor (MFA) totalmente gestionada en la nube eficaz y sencilla que permite: proteger las identidades de los usuarios, asegurar la VPN de acceso remoto, proteger los inicios de sesión, proteger las aplicaciones de nube, etc.

MFA de WatchGuard es tan segura porque se basa en Token virtuales anti-clonación compuestos por tres factores, la suma de ellos hace una llave única que dificulta las capacidades para ser clonada.

**Normicro
somos GOLD
Partner de
WatchGuard**



Simulación de ataques - Phishing

Planes

- + Básico (3 meses)

- + Medio (12 meses)

- + Avanzado (12 meses + Charla de Concienciación en Ciberseguridad)

¿Cuál es el objetivo?

La finalidad es reducir el riesgo de fallo humano, que provoca la mayor parte de las vulnerabilidades en Ciberseguridad dentro de las organizaciones. Esto se vendrá a realizar mediante formación continua, simulaciones de ataques, análisis del comportamiento de los usuarios y el fomento de una cultura de seguridad digital en la empresa.

Te acompañamos en el proceso: comercial@normicro.es

Cómo se desarrolla

Simulación de ataques (Phishing). Envío de correos electrónicos que simulan las tácticas más habituales de Phishing y otros vectores de ataque afines. Estos emails están diseñados de forma realista para que la trampa sea verosímil.

Se plantean 3 niveles de dificultad: desde trampas más evidentes hasta situaciones más sofisticadas que pongan en riesgo información más sensible. Así como adaptadas a departamentos y diferentes roles y responsabilidades dentro de la corporación.

Módulo interactivo + Píldoras formativas. Recursos formativos breves (gráficos, artículos, vídeos...) en los que se recuerdan las cuestiones fundamentales para la prevención de ataques de ciberseguridad.

Evaluación y reporte. Análisis de resultados por usuario y departamento, scoring de riesgo por perfil, Reunión final con presentación de métricas y riesgos detectados.

+ Charla de Concienciación en Ciberseguridad

Se recomienda complementar este servicio con una sensibilización.



Auditoría Pentest

Seguridad superior
Exterior + Interior

Beneficios

- + Identificación de vulnerabilidades.

- + Ciberestatus (postura de seguridad)

- + Ahorro de costes.

- + Continuidad de negocio.

- + Cumplimiento normativo: GDPR, NIS2.

- + Protección de la información.

- + Confianza y reputación.

¿Qué es una Auditoría de Pentest?

Un Pentesting es un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para corregirlas. Estas auditorías comienzan con la recogida en fuentes de acceso abierto de información sobre la empresa, los empleados, usuarios, sistemas y equipamientos.

Te acompañamos en el proceso: comercial@normicro.es

Fases

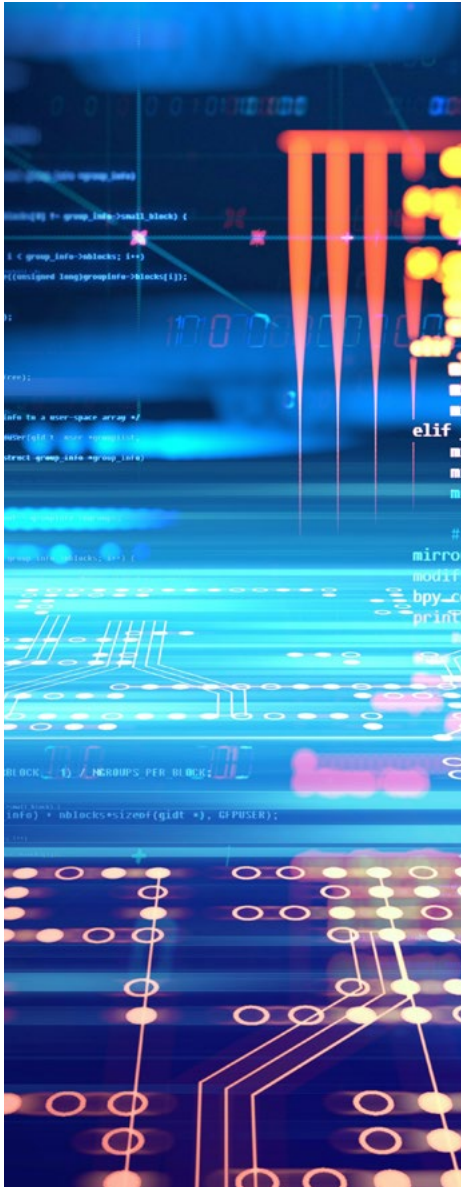
Descubrimiento. Se lleva a cabo un ataque de fuerza bruta DNS para descubrir posibles subdominios a partir del dominio original de su página web.

Enumeración. Un escaneo de puertos y servicios permite identificar servicios expuestos en puertos abiertos y sus posibles versiones.

Análisis de vulnerabilidades. Identificamos los servicios web únicos según los dominios asociados a la máquina con servicio HTTP(s). determinamos los framework, certificados SSL, librerías JS, plugins, WAFs, CMSes y otros softwares.

Explotación. Probamos una serie de inyecciones contra los formularios HTTP y los parámetros de las URLs. Esto permite comprobar la existencia de inyecciones de commando y SQL, LFI y XSS.

Documentación. Presentar, cuantificar y calificar la información obtenida.



Risk Assessment

Análisis de riesgos

Planes

+ Fase 1. Encuestas de campo. **Objetivo:** cuantificación del riesgo cibernético.

+ Fase 2. Evaluación de seguridad. **Objetivo:** identificación de la criticidad.

+ Fase 3. Identificación del plan de intervención. **Objetivo:** definición de las prioridades y del roadmap.

Gestión del riesgo

Proteger la información significa analizar las situaciones y áreas en las que se evalúan los riesgos de seguridad asociados.

+ Personas. Protección de figuras corporativas para procesos estratégicos del negocio.

+ Sistemas. Protección de sistemas que alojan o hacen utilizables datos y servicios.

+ Información. Protección de datos estratégicos para el negocio en cualquier formato.

Estimación de riesgos

Amenaza ¿Qué podría pasar? Por ejemplo, un ciberataque llevado a cabo por una comunidad de hackers.

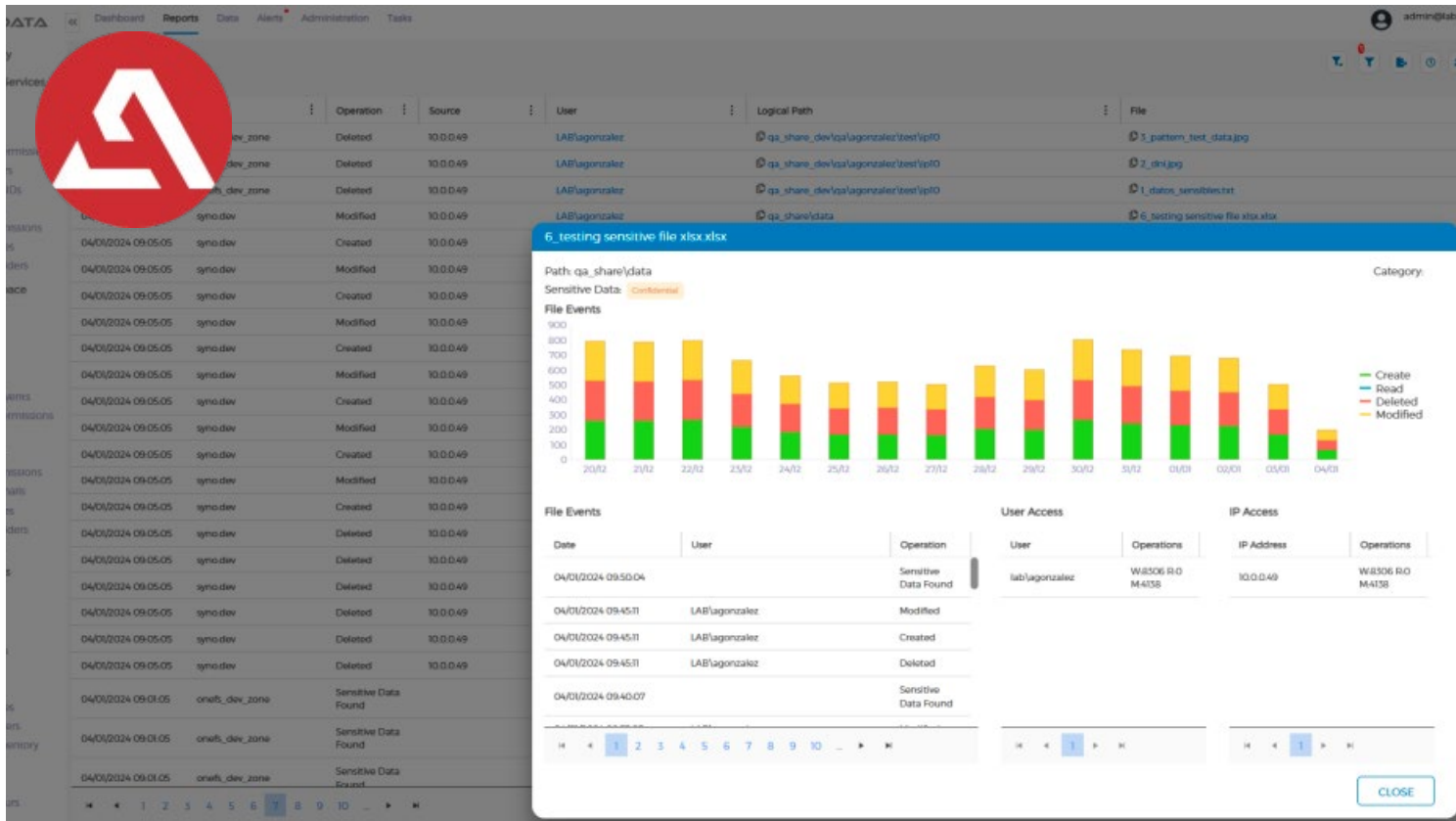
Oportunidad ¿Qué posibilidad hay? La probabilidad coincide con el nivel de exposición al ataque.

Vulnerabilidad ¿Qué grado de exposición tengo? La vulnerabilidad es la implementación parcial o ausencia de medidas de seguridad.

Impacto ¿Qué tipo de daño causaría? El daño resultante del compromiso de la confidencialidad, integridad y disponibilidad de la información.

Contramedida ¿Cómo puedo protegerme de lo que pueda pasar? Con metodologías e iniciativas de prevención y gestión de riesgos.

Te acompañamos en el proceso: comercial@normicro.es



Arexdata DSPM

Trazabilidad del dato

- + Descubrimiento de ubicación de datos.
- + Informes de su postura de seguridad del dato.
- + Mapa de permisos de acceso a los datos.
- + Trazabilidad de datos.
- + Detección de sobre exposición de datos.
- + Asegurar la confidencialidad.
- + Integridad y confianza cero.
- + Análisis de riesgos.
- + Respuesta incidentes.

AREXDATA DSPM es una Tecnología de Ciberseguridad: una Plataforma de Seguridad del Dato (Data Security Platform Management) que audita, normaliza, clasifica y protege al dato en las compañías, además de proporcionar una visibilidad y trazabilidad extremo a extremo de manera centralizada.

**Normicro
somos Partner
Certificado de
Arexdata**



Utilizando un enfoque de seguridad centrada en los datos, SealPath permite a las organizaciones proteger sus datos sensibles de forma persistente en cualquier ubicación a lo largo de todo su ciclo de vida.

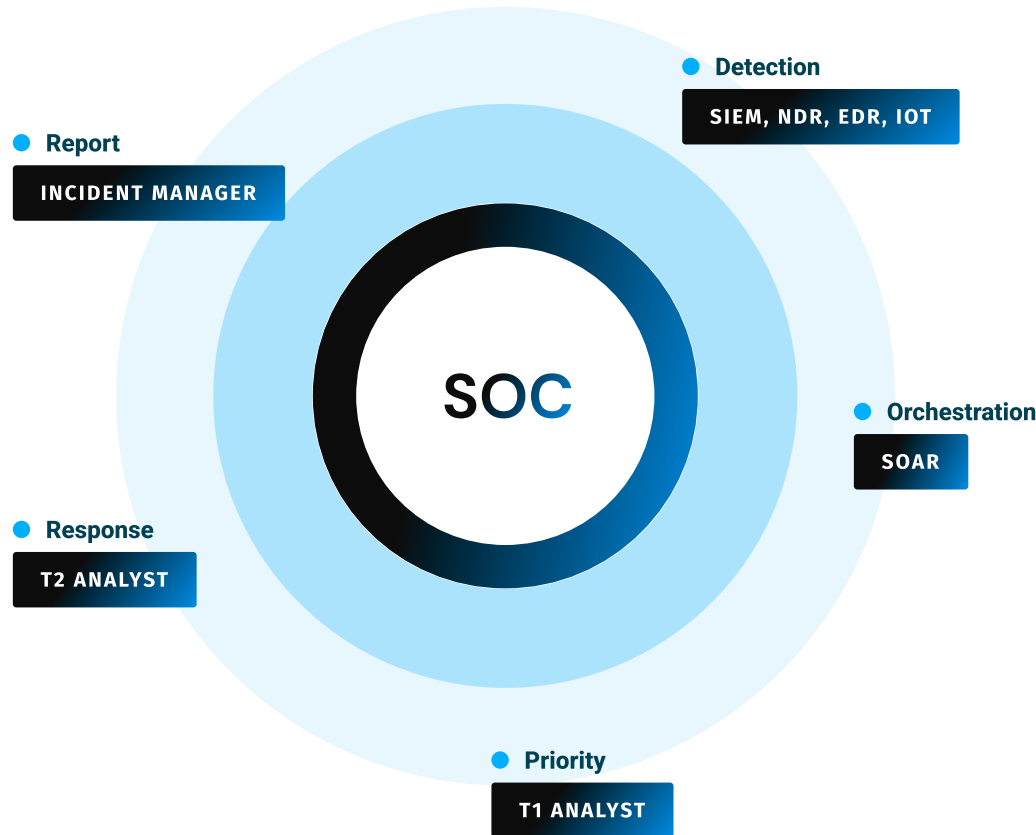
La seguridad viaja con el fichero, permitiendo a la empresa mantenerlo bajo control incluso cuando esté en otras redes o equipos. Ofrece completa visibilidad sobre quién accede, cuándo, o si alguien intenta acceder sin permisos.

Con un click permite restringir en tiempo real el acceso a los datos, aunque estos estén en las manos de otros usuarios.

Sealpath IRM

Prevención de fuga de información

- + Protección dinámica de datos.
- + Máxima sencillez de uso.
- + Colaboración sin agentes ni instalaciones.
- + Exhaustiva auditoría y control de accesos.
- + Automatización de la protección.
- + Integración con sistemas corporativos.
- + Utiliza las herramientas habituales.
- + Opciones de despliegue flexibles.
- + Reducción de riesgos y responsabilidad legal.



Un SOC (Security Operations Center) es un equipo especializado en monitorear, analizar y responder a incidentes de seguridad cibernética en tiempo real. Su objetivo principal es garantizar la protección continua de los sistemas, redes y datos de una organización frente a amenazas internas y externas.

Normicro colabora con Sincronet

SOC 24/7

Security Operations Center

+ **Vigilancia continua 24/7:** garantiza la protección en todo momento, todos los días del año.

+ **Agnóstico:** compatible con cualquier infraestructura o herramienta de seguridad existente. No requiere cambios en las plataformas actuales.

+ **Adaptable:** personalizado para satisfacer las necesidades específicas de cada cliente.

+ **Respuesta automatizada:** basada en análisis avanzado de amenazas mediante SIEM y SOAR.

+ **Zero Trust:** microsegmentación para proteger aplicaciones críticas; aislamiento de hosts para garantizar máxima seguridad.



Sensibilización

Charlas y formaciones en Ciberseguridad

+ Impartimos **Charlas de Concienciación en Ciberseguridad** para todos los trabajadores, desde empleados hasta directivos.

Los servicios de sensibilización son soluciones integrales con envío de materiales complementarios como píldoras de formación y emisión de certificado de aprovechamiento.

+ Organizamos **Encuentros Profesionales** orientados a la ciberseguridad empresarial y en el sector educativo.

+ Participamos en **eventos clave** organizados por proveedores de los que somos Partners.



NORMICRO

Soluciones Informáticas

Somos una empresa con amplia experiencia prestando servicios informáticos, en el sector público y privado. Contamos con una plantilla de profesionales cualificados y el apoyo de colaboradores para solucionar cualquier necesidad que se presente ante nuestros clientes.

Contacto

944 807 337
comercial@normicro.es
www.normicro.es

Nuestras oficinas

Kandela Zubieta Kalea, 35
Leioa, Bizkaia 48940

