TXDXSECURE

2025

NET HARDENING

NUESTRA SOLUCIÓN

Net Hardening está diseñado para fortalecer la seguridad de tus dispositivos de red (IOS) a través de un enfoque integral. Implementamos las mejores prácticas de gobernanza, identificación de activos, protección de redes y respuesta ante incidentes. Este servicio optimiza la seguridad en cada capa de la infraestructura, garantizando un entorno de red robusto y confiable.

ACCIONES CLAVE

FASE 1: GOBERNANZA

El servicio comienza con el establecimiento de un marco de gobernanza sólido, alineando las políticas de seguridad con las mejores prácticas y regulaciones.

Funciones Clave:

- **Marco de Gobernanza:** Definición de políticas y procedimientos alineados con las mejores prácticas de seguridad.
- **Evaluación de Riesgos:** Identificación de vulnerabilidades en los planos de gestión, control y datos.
- **Evaluación de Políticas de Seguridad:** Revisión de controles de acceso, segmentación y uso de criptografía.
- **Monitoreo de Cumplimiento:** Revisión del cumplimiento regulatorio aplicado a los dispositivos IOS.

FASE 2: IDENTIFICACIÓN

Realizamos un inventario detallado de los dispositivos IOS y evaluamos las principales amenazas, ofreciendo una visión clara del panorama de seguridad de la red.

Funciones Clave:

- **Inventario de Activos:** Registro detallado de todos los dispositivos IOS y su rol dentro de la red.
- **Threat Landscape:** Identificación y clasificación de las principales amenazas que pueden comprometer los dispositivos.
- **Línea Base de Configuración:** Desarrollo de configuraciones seguras para todos los planos, incluyendo ACL, protocolos seguros y RBAC, estableciendo un estándar de seguridad.

FASE 3: PROTECCIÓN

Fortalecemos la seguridad en los planos de gestión, control y datos, aplicando controles avanzados para proteger los dispositivos y evitar accesos no autorizados.

Funciones Clave:

- **Hardening del Plano de Gestión:** Fortalecimiento de accesos, optimización de recursos y protección avanzada de servicios críticos.
- **Hardening del Plano de Control:** Filtrado de tráfico, protección de protocolos y monitoreo de tráfico de control.
- **Hardening del Plano de Datos:** Configuración de ACLs, protección anti-spoofing y filtrado de tráfico ICMP/IP.

FASE 4: DETECCIÓN

Implementamos mecanismos para detectar anomalías en el tráfico y registros, ofreciendo recomendaciones que mejoran la capacidad de respuesta ante incidentes.

Funciones Clave:

- **Detección de Anomalías:** Análisis de comportamientos inusuales en los planos de la red. Este análisis identificará posibles cambios no autorizados en el enrutamiento o patrones de tráfico inesperados, y se recomendarán acciones para mitigar estos riesgos de manera proactiva.
- **Registros de Auditoría:** Recomendaciones para mejorar la visibilidad y seguridad a través de mejores prácticas de auditoría.

FASE 5: RESPUESTA

Desarrollamos un plan de respuesta ante incidentes que permite contener amenazas de forma rápida, junto con alertas automatizadas y análisis forense.

Funciones Clave:

- **Plan de Respuesta a Incidentes:** Evaluación y optimización de los procesos de respuesta ante incidentes de seguridad.
- **Mecanismos de Alerta:** Implementación de sistemas automatizados para notificación de brechas de seguridad.
- **Análisis Forense:** Propuestas para la implementación de análisis detallados en caso de incidentes, lo que permitirá facilitar investigaciones posteriores a incidentes y optimizar las defensas contra futuros ataques.

FASE 6: RECUPERACIÓN

Implementamos mecanismos para detectar anomalías en el tráfico y registros, ofreciendo recomendaciones que mejoran la capacidad de respuesta ante incidentes.

Funciones Clave:

- **Recomendación de Procedimientos de Recuperación:** Análisis y recomendaciones de recuperación post-incidente, se documentarán recomendaciones claras para restaurar configuraciones endurecidas y políticas de control de acceso seguras después de una brecha, asegurando una recuperación eficiente.
- **Recomendación de Copias de Seguridad de Configuraciones:** Evaluación de las prácticas de respaldo para garantizar que las configuraciones de cada plano (gestión, control y datos) se respalden adecuadamente, facilitando la restauración en caso de incidentes.

ENTREGABLES

- Presentación Kick Off "Análisis de Gobernanza" (PAG)
- Documento de Pruebas Operacionales Simplificadas (TestPlan)
- Documento de Plan de Implementación (NIP)
- Presentación de Transferencia Operacional (PTO)
- Documento de Informe final (DIF)

TXDXSECURE S.A.C.
RUC: 20607043427
Contáctanos: +51 942 325 448; +51 999 379 845
Correo: administracion@txdxsecure.com

Calle las Gorsellas No 167 Naranjal
San Martín de Porres
Lima, Perú

www.txdxsecure.com

2025