TXDXSECURE

2025

RANSOMSAFE PROACTIVE DEFENSE

NUESTRA SOLUCIÓN

Nuestro servicio de **Ransom Safe Proactive Defense** ofrece una solución integral para **detener ataques, recuperar datos y proteger tu infraestructura crítica.** Utilizando tecnologías de respuesta autónoma y análisis en tiempo real, identificamos, contenemos y neutralizamos el ransomware, garantizando la continuidad de tus operaciones con la mínima interrupción. Además, **reforzamos tus sistemas** con medidas de seguridad avanzadas para prevenir futuros ataques.

OBJETIVO: DETENER, RECUPERAR, PROTECCIÓN Y DEFENSA

FASE 1: IDENTIFICACIÓN

Realizamos un análisis forense inicial para entender el ransomware, identificar los sistemas comprometidos, y clasificamos los activos críticos para priorizar su protección.

Funciones Clave:

- **Evaluación de riesgo y alcance:** Determinamos qué tan expuesto está tu sistema y qué ha sido comprometido.
- **Clasificación de activos:** Priorizamos la protección de tus sistemas y datos más críticos.
- **Análisis forense inicial:** Estudiamos el ransomware y cómo ingresó a tu red.
- **Documentación del incidente:** Registramos cada detalle para análisis y aprendizaje.

FASE 2: PROTECCIÓN

Revisamos los controles de acceso, eliminamos usuarios comprometidos y reforzamos las defensas perimetrales con firewalls y autenticación multifactorial para asegurar que no haya vulnerabilidades adicionales.

Funciones Clave:

- **Aislamiento de sistemas:** Desconectamos las redes afectadas para evitar una mayor propagación.
- **Segmentación de la red:** Aplicamos microsegmentación para confinar el ataque.
- **Control de acceso:** Reajustamos permisos y eliminamos cuentas comprometidas.
- **Fortalecimiento de perímetro:** Implementamos firewalls y autenticación multifactor para proteger tus sistemas.

FASE 3: DETECCIÓN

Usamos herramientas avanzadas como SIEM y EDR para identificar patrones sospechosos y analizamos logs en busca de indicadores de compromiso (IoC), asegurando la detección temprana de amenazas.

Funciones Clave:

- **Monitoreo continuo:** Observamos el comportamiento de tus sistemas en tiempo real.
- **Detección de actividad anómala:** Utilizamos SIEM y EDR para identificar cualquier actividad sospechosa.
- **Análisis de logs:** Revisamos los registros para detectar posibles indicadores de compromiso (IoC).
- **Inspección profunda de tráfico (DPI):** Analizamos todo el tráfico de la red en busca de comportamientos anormales.

FASE 4: RESPUESTA

Contenemos el ataque rápidamente, deteniendo la propagación del ransomware y desactivando accesos comprometidos. Aseguramos la coordinación de la respuesta mediante comunicaciones seguras, eliminando cualquier amenaza adicional de forma eficiente.

Funciones Clave:

- **Contención del ataque:** Detenemos la propagación del ransomware y realizamos el bloqueo de cualquier acción adicional.
- **Desactivación de accesos comprometidos:** Eliminamos accesos de usuarios no autorizados.
- **Comunicaciones seguras:** Coordinamos la respuesta mediante canales seguros.
- **Negociación supervisada:** Evaluamos todas las opciones, incluyendo el rescate, si es la última alternativa.

FASE 5: RECUPERACIÓN

Implementamos una reintegración segura y controlada de todos los sistemas, y mejoramos la infraestructura con nuevas medidas de protección para prevenir futuros incidentes.

Funciones Clave:

- **Restauración de sistemas:** Recuperamos tus datos y sistemas desde backups seguros.
- **Validación de integridad:** Aseguramos que los sistemas están limpios antes de restablecer la conexión.
- **Reintegración segura:** Progresivamente reintroducimos los sistemas de forma controlada.
- **Mejoramiento de capacidades:** Fortalecemos las defensas para prevenir futuros ataques.

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