TechnologyPartners

Creando huella basados en servicio experiencial

Informe Consolidado de Mejoras Implementadas en la Plataforma

PREPARADO PARA:

Distrito de Medellín

www.techno-partners.com
soporte@techno-partners.com

Tabla de contenido

Resumen Ejecutivo **3**

1. Principales Mejoras Implementadas **4**

1.1 Optimización de ServerProtect for Storage (SPFS) 4

Actividades ejecutadas 4

Resultados obtenidos 4

1.2 Plan de Erradicación del Malware MSIL en NAS 4

Actividades ejecutadas 4

Resultados obtenidos 4

Hallazgo relevante 4

1.3 Cobertura de Dispositivos Legacy 5

Actividades ejecutadas 5

Resultados obtenidos 5

1.4 Incremento de Visibilidad y Gobierno desde Vision One 5

Actividades ejecutadas 5

Resultados obtenidos 5

1.5 Gestión de Riesgo mediante CREM 5

Actividades ejecutadas 5

Resultados obtenidos 5

1.6 Gestión de Vulnerabilidades y Exposición 6

Actividades ejecutadas 6

Beneficios esperados 6

2. Indicadores de Avance **6**

3. Riesgos y Retos Identificados **6**

4. Próximos Pasos **7**

5. Conclusión **7**

Resumen Ejecutivo

Durante el periodo 2025-2026 se ejecutó un plan continuo de fortalecimiento orientado a incrementar la capacidad de detección, mejorar la cobertura de protección, optimizar la operación de escaneo sobre almacenamiento NAS y aumentar la visibilidad de riesgos dentro del ecosistema Trend Micro.

Como resultado del trabajo realizado se obtuvieron avances importantes en cinco frentes estratégicos:

- Fortalecimiento de la protección sobre almacenamiento NAS mediante ServerProtect for Storage.
- Incremento progresivo de cobertura en dispositivos sin agente y dispositivos legacy.
- Habilitación de capacidades avanzadas de visibilidad y telemetría en Vision One.
- Optimización de estabilidad y actualización tecnológica de componentes críticos.
- Consolidación de procesos de gestión de exposición al riesgo (CREM).

1. Principales Mejoras Implementadas

1.1 Optimización de ServerProtect for Storage (SPFS)

Actividades ejecutadas

- Identificación y corrección de conflictos entre políticas de firewall y ServerProtect.
- Escalamiento técnico con fabricante para revisión de comportamiento de logs.
- Actualización progresiva del producto desde versión 6.0.0.1304 hasta versión 6.0.0.1835.
- Reinstalación controlada de servidores con fallas de despliegue.
- Ajustes operativos para administración de caché y continuidad de escaneos.

Resultados obtenidos

- Recuperación de estabilidad operativa.
- Normalización del despliegue de actualizaciones.
- Mejora en consistencia de escaneos.
- Mayor capacidad de seguimiento de eventos.

1.2 Plan de Erradicación del Malware MSIL en NAS

Actividades ejecutadas

- Ejecución de múltiples ciclos de escaneo sobre almacenamiento HNAS.
- Análisis de logs entre ServerProtect y Vision One.
- Investigación de muestras sospechosas en laboratorio controlado.
- Correlación de eventos con telemetría adicional.

Resultados obtenidos

- Incremento progresivo de detecciones durante campañas de limpieza.
- Validación de acciones efectivas de erradicación.
- Identificación de limitaciones estructurales relacionadas con metadata ICAP.

Hallazgo relevante

Se confirmó que la limitación principal de trazabilidad no corresponde a ServerProtect sino a la información entregada por HNAS.

1.3 Cobertura de Dispositivos Legacy

Actividades ejecutadas

- Identificación de dispositivos Windows 7 y Windows 8.
- Creación de política dedicada “Windows Legacy”.
- Diseño de procedimiento de migración desde SEP hacia Workload Security.
- Desarrollo de pilotos controlados.
- Validación de telemetría mediante Activity Monitoring.

Resultados obtenidos

- Cobertura ampliada sobre dispositivos fuera de soporte.
- Habilitación de capacidades de Virtual Patching (IPS).
- Incremento de visibilidad hacia Vision One.

1.4 Incremento de Visibilidad y Gobierno desde Vision One

Actividades ejecutadas

- Identificación de dispositivos sin sensor XDR.
- Consolidación de inventarios mediante integración con Directorio Activo.
- Implementación de consultas avanzadas y búsqueda de amenazas.
- Creación de Smart Folder para administración operativa.

Resultados obtenidos

- Reducción de puntos ciegos.
- Mejor capacidad investigativa.

1.5 Gestión de Riesgo mediante CREM

Actividades ejecutadas

- Implementación del módulo CREM.
- Revisión de más de 7.000 eventos de bajo riesgo.
- Análisis de cuentas comprometidas.
- Investigación de eventos relacionados con exposición en dark web.

Resultados obtenidos

- Identificación de cuentas comprometidas.
- Generación de acciones preventivas.
- Priorización de remediaciones.

1.6 Gestión de Vulnerabilidades y Exposición

Actividades ejecutadas

- Socialización de capacidades de Vulnerability Management.
- Preparación para habilitación de escaneos agentless.
- Envio de solicitud para el despliegue del Service Gateway.

Beneficios esperados

- Descubrimiento de activos.
- Priorización basada en riesgo.
- Reducción de superficie de ataque.

2. Indicadores de Avance

Línea de trabajo	Estado
Actualización ServerProtect	Completado
Escaneos NAS	Completado con restricciones de visibilidad
Cobertura dispositivos legacy	En ejecución
Implementación XDR	En expansión
Gestión CREM	Activa
Vulnerability Management	Preparación

3. Riesgos y Retos Identificados

- Limitaciones de metadata entregada por HNAS.
- Restricciones de soporte en sistemas operativos legacy.
- Necesidad de ampliar cobertura de sensores y agentes.

4. Próximos Pasos

1. Completar despliegue en dispositivos legacy.
2. Continuar actualización de agentes pendientes.
3. Activar capacidades de Vulnerability Management.
4. Análisis de reportes HNAS con Vision One.
5. Mantener sesiones periódicas de seguimiento.

5. Conclusión

Las actividades desarrolladas permitieron fortalecer significativamente las capacidades de prevención, detección y respuesta del entorno. Se logró aumentar la cobertura tecnológica, estabilizar componentes críticos y generar mejores capacidades de investigación y gestión del riesgo.

Para el siguiente ciclo se recomienda priorizar el cierre de brechas en dispositivos legacy, ampliar telemetría y continuar evolucionando el modelo de operación basado en visibilidad y automatización.

.