Deep Discovery Inspector

PLAN DE EVALUACIÓN DE SEGURIDAD

Contenido

1.- Introducción

Actualmente los ataques a los sistemas de información han demostrado su capacidad para evadir las defensas de seguridad convencionales y permanecer sin ser detectados durante prolongados períodos de tiempo, llevando a cabo de esta manera el robo y la fuga de datos corporativos. Los analistas y expertos de seguridad reconocen esta problemática, y recomiendan que las empresas redefinan la estrategia de seguridad para adoptar tecnología que permita entregar mayor visibilidad para la detección de amenazas y establecer un proceso proactivo de gestión de amenazas en tiempo real.

La solución de Trend Micro **Deep Discovery Inspector**, proporciona visibilidad de toda la red y el control que se necesita para combatir los ataques dirigidos y las amenazas persistentes avanzadas. Su capacidad de descubrimiento y análisis detecta de forma única amenazas evasivas en tiempo real, proporcionando la inteligencia que permite detectar, analizar, adaptar y responder a los ataques dirigidos contra su organización.

2.- Objetivos

El objetivo principal de este documento es entregar las directrices y un plan para implementar la solución Deep Discovery Inspector en modelo "Proof-of-Concept". A través de esta implementación se podrá realiza una evaluación profunda del estado de seguridad de las redes y sistemas de la organización para luego poder definir los controles adecuados que permitan minimizar los riesgo a la seguridad de la información y de la continuidad operacional.

2.1 Objetivo Específico

- Implementar la solución Deep Discovery Inspector para el monitoreo del tráfico de la red que permita el análisis de ataques y amenazas en tiempo real en modelo "Proof-of-Concept / Evaluación".

2.2 Alcance

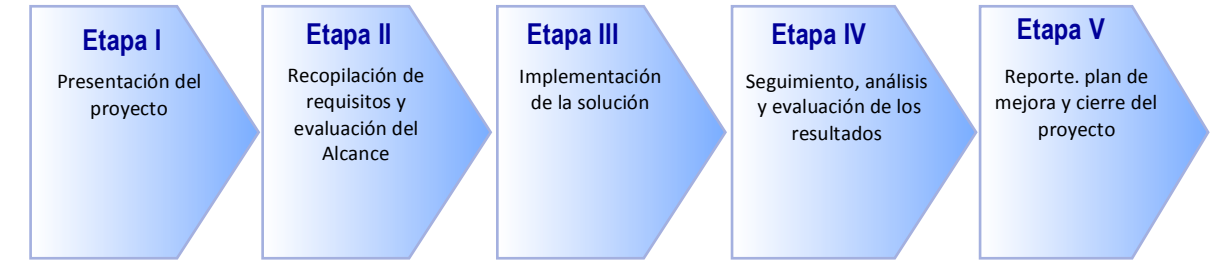
- Realizar la implementación de la solución en un entorno real para demostrar sus capacidades
- Evaluar y medir el nivel de seguridad de la compañía mediante el análisis de los resultados.

3.- Metodología

La metodología propuesta comprende la ejecución de distintas etapas como se explica a continuación:

- 1.- Presentación del proyecto.
- 2.- Recopilación de requisitos y evaluación del alcance.
- 3.- Implementación de la solución.
- 4.- Seguimiento, análisis y evaluación de los resultados.
- 5.- Reporte, plan de mejoras y cierre del proyecto.

El proyecto considera un periodo de evaluación de 15 días.



- Presentación del proyecto y tecnología (Kick-off)
- Establecimiento del plan de comunicación y coordinación con el cliente.
- Solicitud de requerimientos iniciales.

- Recopilación de información de la infraestructura tecnológica.
- Análisis del diseño de red y definición del alcance para el análisis.
- Definición de la estrategia de implementación.
- Coordinación interna y requerimientos específicos para la implementación de la solución.

- Validación de los requerimientos técnicos y de coordinación entre las áreas.
- Implementación de la solución.
- Configuración del producto.
- Test de evaluación del funcionamiento.

- Seguimiento semanal para el análisis de los datos recopilados.
- Ajustes a la configuración
- Periodo de recopilación y análisis de datos
- Evaluación de los resultados

- Desarrollo de reporte de resultados y plan de mejoras.
- Reunión para la presentación de los resultados.
- Entrega de informes y cierre del proyecto.

4.- Arquitectura Conceptual de la Solución

DETECCIÓN DE AMENAZAS

- Amenazas avanzadas persistentes y ataques dirigidos.
- Ataques de tipo “zero-day”.
- Actividad de maliciosas en la red.
- Amenazas Web (pirateo, descargas).
- Amenazas en el correo electrónico y la mensajería instantánea.
- Fuga de datos.
- Bots, Troyanos y gusanos.
- Keyloggers y crimewares.
- Aplicaciones disruptivas.

PRINCIPALES VENTAJAS

- Detección de amenazas avanzadas
- Reduce los riesgos de daño y pérdida de datos.
- Visibilidad en toda la red
- Visibilidad del estado de seguridad
- Análisis en profundidad
- Proporciona una evaluación de las
- amenazas en tiempo real.
- Gestión centralizada de información y eventos de seguridad

Deep Discovery Inspector no interviene la continuidad de las operaciones, ya que analiza el tráfico fuera de línea a través de un port mirror en el segmento de red que sea definido para el análisis.

	DETECCIÓN DE ATAQUES	MÉTODOS DE DETECCIÓN
Contenidos maliciosos	• Emails que contienen programas maliciosos (en archivo adjunto o enlace a una URL) • Descargas furtivas • Programas maliciosos conocidos o de tipo “zero-day”	• Desciframiento y descompresión de ficheros adjuntos • Ejecución de ficheros sospechosos en sandbox • Detección de las vulnerabilidades de los navegadores • Escaneo antimalware (firmas y heurística)
Comunicaciones sospechosas	• Comunicaciones C&C en todos los programas maliciosos: bots, programas de descarga, robo de datos, gusanos y amenazas de tipo mixto. • Establecimiento de backdoor por parte de un cibercriminal	• Análisis de destino (URL, IP. Dominio, email, canal de IRC,...) mediante listas negras y listas blancas dinámicas. • Evaluación de la reputación de las URL mediante Smart Protection Network • Fingerprinting de flujos de comunicación
Comportamiento de los ataques	• Actividad de programas maliciosos: propagación, descarga, envío de spam,... • Actividad de cibercriminales: escaneos, ataque de fuerza bruta, robo de servicios,... • Extracción de datos	• Análisis heurístico basado en normas • Identificación y análisis de utilización de cientos de protocolos y aplicaciones, especialmente de aplicaciones basadas en HTTP

5.- Requerimientos

Deep Discovery Inspector puede ser instalado en un ambiente virtual como físico, sin embargo se debe considerar las siguientes especificaciones:

Requerimientos Hardware Virtual Appliance	
▪ Deep Discovery Inspector Virtual Appliance: ○ **CPU:** Two Intel™ Core™2 Quad processors recommended ○ **RAM:** 8GB ○ **Hard disk space:** 100GB ○ **Network interface card (NIC):** 2 NICs ○ **ESX Host:** Version 4.x or 5.x ○ **Port Mirror**	
Requerimientos para Deep Discovery Inspector Appliance (Físico)	
• 1 U of Rack Space	
• 2 Power Outlets	
• Hardware Compatible: Dell PowerEdge R420 / Dell PowerEdge R720	
Internet Access	
• Deep Discovery Inspector requiere acceso a internet para realizar actualizaciones y tener información detallada de amenzas.	

7.- Checklist Pre Instalación

7.1 Información General

Registro de Información	
Nombre de la Organización	
Dirección	
Contacto Principal Nombre/Teléfono/Email	
Contacto Secundario Nombre/Teléfono/Email	
Fecha de Inicio del Proyecto	
Motivo de Evaluación	

7.2 Requerimientos Configuración Redes

- Listado de los segmentos de red a monitorear
- Lista de direcciones ip y hostname de los servicios de red (dns, active directory, file server, Gateway, DNS, proxy, etc...)
- Lista de todos los dominios públicos e internos.

7.3 Trend Micro Contactos

Rol	Nombre	Email	Teléfono
Trend Micro Cordinador del Proyecto			
Trend Micro Consultor			