DARKTRACE

HOJA DE DATOS

Prueba de Valor de Darktrace

¿Qué es una Prueba de Valor?

Una Prueba de Valor (PDV) es una prueba sencilla de cuatro semanas que le permite evaluar el Enterprise Immune System y el Threat Visualizer de Darktrace dentro de su propio entorno. La PDV permite a las organizaciones comprender por qué razón algunas de las compañías más importantes del mundo recurren a Darktrace para adquirir una visibilidad sin precedentes de sus redes y detectar ciber amenazas emergentes dentro de sus sistemas en tiempo real, antes de que se conviertan en incidentes dañinos. Nuestro experimentado equipo instalará un aparato Darktrace dentro de su entorno en apenas un día, y le proporcionará acceso a nuestra innovadora interfaz Threat Visualizer. Durante la PDV, usted también recibirá actualizaciones detalladas acerca de lo que encontramos, producidas por nuestros ciber analistas de talla mundial.

¿Por qué razón hacer una PDV?

Lograr Visibilidad Global

Las redes de hoy son grandes, ajetreadas y complejas, lo que hace muy difícil dilucidar en todo momento qué está pasando, dónde y cómo. Darktrace simula, mapea y visualiza toda su red, hasta el nivel de dispositivo y usuario, proporcionándole un panorama singular e intuitivo de lo que está sucediendo dentro de su organización.

- Vea cómo es realmente su red y sus interacciones
- Tenga la posibilidad de 'adentrarse' en partes de su infraestructura, por red, dispositivo o usuario
- Conozca a su organización mejor de lo que la conocen sus adversarios

Detectar Amenazas cuya Existencia No Conocía

El singular enfoque de sistema inmunológico de Darktrace se vale de matemáticas probabilísticas y aprendizaje de máquina. No recurre a firmas, reglas ni conocimientos a priori de amenazas o de su entorno. La tecnología aprende constantemente qué es actividad 'normal' dentro de su entorno, correlacionando múltiples indicadores sutiles para formar un conocimiento preciso de comportamientos normales y anormales.

- Encuentre anomalías y amenazas cuya existencia ignoraba. El enfoque matemático y de aprendizaje de máquina de Darktrace funciona desde el primer día y está aprendiendo constantemente para detectar comportamientos inusuales, sin ningún conocimiento a priori.
- Sepa cuáles son sus prioridades principales en seguridad. Darktrace le permite ver y actuar en relación con las principales amenazas a las que se enfrenta su organización, sin distraerse con el ruido de la red
- Tome medidas a tiempo para minimizar los riesgos que se plantean para su organización y ponga freno a comportamientos maliciosos o dañinos

Informes de Inteligencia de Amenazas

Una PDV de Darktrace incluye tres Informes de Inteligencia de Amenazas semanales que le explicarán y detallarán las anomalías más destacadas que detecte el Enterprise Immune System, según lo determinen nuestros analistas expertos. Darktrace emplea algunos de los profesionales en inteligencia y seguridad cibernética más importantes del mundo. Nuestros analistas en ciber amenazas en general tienen una sólida trayectoria en inteligencia de gobierno, y proceden de NSA, GCHQ, MI5 y de otras agencias de inteligencia, contando con una experiencia sin precedentes en el mundo real en la identificación y defensa contra algunas de las ciber amenazas y ciber atacantes más persistentes y perniciosos.

- Benefíciese con el análisis especializado de los principales analistas en ciber amenazas del mundo
- Colabore directamente con nuestros analistas para conocer las conclusiones del aparato Darktrace
- Reciba Informes de Inteligencia de Amenazas semanalmente a partir de la segunda semana, que le proporcionarán análisis personalizados de las principales amenazas de su entorno basados en las investigaciones de nuestros excelsos analistas cibernéticos
- Obtenga asesoramiento experto en remediación de amenazas en respuesta a las anomalías detectadas

¿Cómo funciona?

1. Instalación del aparato Darktrace

Un aparato Darktrace se puede instalar en 1-2 horas o menos, y utiliza hasta 2U de espacio de bastidor.

2. Recolección pasiva de datos

Darktrace utiliza el tráfico bruto de la red para obtener la máxima visibilidad de su red y simular su empresa, sus dispositivos y usuarios con un grado alto de precisión. Los datos se recogen de forma pasiva utilizando uno de los siguientes métodos:

- División de puertos vía sus equipos actuales de red
- Inserción o reutilización de un empalme de red en línea
- Acceso a depósitos existentes de datos de red

3. Análisis y simulación de datos

Darktrace comienza inmediatamente a ingerir, analizar y simular datos de la red. Utilizando sus singulares algoritmos probabilísticos y de aprendizaje de máquina, Darktrace establece un 'patrón de vida' para la empresa, al igual que para cada uno de los dispositivos y usuarios, y detecta anomalías reales. Durante el transcurso de la PDV, este conocimiento se pule y revisa de manera constante a medida que el Enterprise Immune System va aprendiendo cada vez más cómo se comporta su organización.

Cronología de la PDV

Nivel	Programa	Pasos	Su Recurso
1	Pre-PDV	Programar la fecha de instalación del aparato Darktrace	Se le asigna un Especialista en Tecnología Cibernética (ETC)
	Día 1	• Instalación (1-2 horas) • Validación del flujo de datos • Se activa el aprendizaje de máquina	Su ETC
	Semana 1	**Conocer su red** • Su red es topológicamente mapeada en 3D vía la interfaz Threat Visualizer • Ver lo que está sucediendo dentro de la organización, a medida que va sucediendo	Su ETC y acceso a su Analista Cibernético exclusivo conforme resulte necesario
2	Semana 2	**Comprender el comportamiento del usuario** • Obtener acceso inicial al Centro de Notificación de Amenazas • Visualizer demuestra comportamientos inusuales de los empleados • Conocer cómo se utilizan las credenciales de usuario • Comienzan los Informes de Inteligencia de Amenazas semanales	Su ETC y acceso a su Analista Cibernético conforme resulte necesario
3	Semana 3	**Investigar amenazas en tiempo real** • Obtener acceso pleno al Centro de Notificación de Amenazas • Formación para familiarización con la interfaz de usuario para aprovechar al máximo el Threat Visualizer • Apreciar cómo el Threat Visualizer proporciona mayor visibilidad y poder de investigación a su entorno. • Ver y responder ante alertas en tiempo real de anomalías reales, que han sorteado otros controles de seguridad • Segundo Informe de Inteligencia de Amenazas semanal	Su ETC y acceso a su Analista Cibernético conforme resulte necesario
4	Semana 4	**Evaluar y revisar** • Se presenta el último Informe de Inteligencia de Amenazas y el Resumen de Amenazas de la PDV en reunión de revisión • Termina la PDV	Patrocinador ejecutivo y Experto Temático sénior
	Post-PDV	• Firmar contrato • Planificar implementación en empresa y sus necesidades de asistencia	Patrocinador ejecutivo

Recursos Necesarios para el Éxito

Conexión Segura

Los aparatos Darktrace se conectan con la Gerencia Central de Darktrace por un canal de autenticación de doble factor, seguro y codificado para recibir nuevos modelos matemáticos y actualizaciones de software. Para implementaciones gestionadas y PDV, esto también permite a los analistas cibernéticos de Darktrace revisar y ajustar la salida del sistema. Los clientes mantienen el control total de la conexión, que es iniciada y mantenida desde el aparato, y puede ser iniciada, terminada o auditada en cualquier momento. A los efectos de realizar controles de salud continuos, solicitamos que se mantenga una conexión durante el horario hábil normal.

Alternativamente, se puede utilizar una VPN para conectar el aparato con la Gerencia Central de Darktrace, de acuerdo con los protocolos de los clientes.

Correlación de Datos

Para sacar máximo provecho de los anfitriones de aprendizaje de máquina no supervisados con direcciones de IP dinámicas, la señal DHCP del servidor al cliente debe estar contenida en la alimentación de datos. Esto ayuda a formar el conocimiento más granular de un determinado comportamiento de máquina y usuario. Para implementaciones más allá de la Prueba de Valor, se pueden utilizar otras formas de correlación de datos para permitir la integración con muchos sistemas de registro estándares en la industria.

Si los datos DHCP de la red no estuvieran disponibles, pregunte acerca de opciones secundarias a su contacto Darktrace.

Privacidad y Consideraciones Legales

- La recolección de datos es pasiva – todos los datos recogidos se mantienen dentro de las instalaciones y no se suben a la nube o a un centro de datos de Darktrace. Los datos son accesibles solo a través de la conexión segura salvo acuerdo en contrario.
- El aparato no afecta las operaciones de la red ni de la empresa.
- Los datos se eliminan de forma segura si usted no deseara proceder más allá de la PDV.
- Para activar el aparato, se requiere un contrato legal de aceptación tácita.

Acerca de Darktrace

Nombrada como 'Pionera Tecnológica' por el Foro Económico Mundial, Darktrace es una de las compañías de defensa contra cíber-amenazas más importantes del mundo. Su tecnología Enterprise Immune System detecta en tiempo real amenazas no identificadas previamente, valiéndose de matemáticas y aprendizaje de máquina desarrollados en la Universidad de Cambridge, que analizan el comportamiento de cada uno de los dispositivos, usuarios y redes que hay dentro de una organización. Algunas de las corporaciones más grandes del mundo confían en el aparato de auto-aprendizaje de Darktrace aplicándolo en sectores como energía y servicios públicos, servicios financieros, telecomunicaciones, atención sanitaria, fabricación, comercio minorista y transporte. La compañía fue fundada en 2013 por excelsos especialistas en aprendizaje de máquina y expertos en inteligencia de gobierno y tiene sedes en Cambridge, Reino Unido y San Francisco, y oficinas en Londres, París, Milán, Varsovia, Mumbai, Bangalore, Singapur, Seúl, Tokio, Nueva York, Chicago, Washington D.C., Boston, Los Ángeles, Dallas, Toronto, Auckland, Sydney and Melbourne.

T: +44 (0) 1223 350 653 E: info@darktrace.com www.darktrace.com