Prueba de valor de Darktrace

Darktrace le ofrece la oportunidad de evaluar el poder y los beneficios de la galardonada tecnología de inteligencia artificial cibernética de Darktrace sin costo para su empresa.

Una Prueba de Valor de Darktrace (POV) es una prueba de 30 días diseñada para demostrar el Enterprise Immune System en acción, dentro del contexto de su entorno digital. El punto de vista también le brinda la oportunidad de ver su red visualizada a través del Threat Visualizer, la visibilidad en 3D de Darktrace y la interfaz de usuario de investigación.
Un ejecutivo de cuentas y un ciber tecnólogo lo guiarán a través de la experiencia POV.

Beneficios de la POV

Detecta amenazas no antes vistas

Darktrace forma rápidamente una comprensión evolutiva del "patrón de vida" de su red. Detectará automáticamente amenazas y comportamientos anómalos que de otra manera no serían detectados por herramientas tradicionales.

100% de visibilidad

Como parte de la POV, Darktrace le proporciona una visibilidad completa de la red en la que se implementa, lo que le permite comprender mejor su patrimonio digital. Con acceso al Threat Visualizer, también puede visualizar, investigar y reproducir amenazas cibernéticas o incidentes.

Informes de Inteligencia de Amenazas (TIRs)

Además del acceso al Threat Visualizer, recibirá tres Informes de Inteligencia de Amenazas (TIR) durante una POV de Darktrace. Producidos por el reconocido equipo de Cber Analista de Darktrace, los TIRs resumen y evalúan los descubrimientos realizados cada semana de la POV, y ayudan a sus equipos y ejecutivos a comprender y evaluar el nivel de amenaza actual de su organización y ayudan en la toma de decisiones.

Cronología de la POV

Agenda	Pasos	Recursos de Darktrace	Recurso de su empresa
Pre POV	• Programar fecha de instalación • Asignación de un ciber tecnólogo (CT)	Ejecutivo de cuentas (AE), CT	Representante Técnico
Día 1	• CT llega al sitio para instalar Darktrace (1-2 horas) • La recopilación y validación pasiva de datos comienza utilizando el puerto (SPAN) a través de su equipo de red existente	CT	Representante Técnico
Semana 1	• Activación de Machine Learning • Darktrace inicia proceso de análisis de datos de la red, estudiando patrones de normalidad para cada usuario y dispositivo	CT	Representante Técnico
Semana 2	• Reunión de Revisión de TIR 1 • Proceso de adaptación detallado con la interfaz de usuario	CT, AE	Representante Técnico
	• Acceso a la interfaz del Threat Visualizer 3D • Observe lo que está sucediendo en tiempo real	CT	Representante Técnico
Semana 3	• Reunión de Revisión de TIR 2 • Presentación de propuesta comercial para instalación completa en la red	CT, AE	Representante Ejecutivo, Representante Técnico
	• Igual que semana 2 • Continúa familiarizándote con el Visualizador de amenazas • Observe y responda a alertas en tiempo real	CT	Representante Técnico
Semana 4	• Reunión de Revisión de TIR 3 • Presentación de la hoja de Términos y Condiciones de Darktrace	CT, AE	Representante Ejecutivo, Representante Técnico
	• La POV se termina • Agende una reunión de resumen sobre los TIRs (Opcional) • Pasos comerciales de seguimiento son acordados	CT, AE	Representante Ejecutivo, Representante Técnico

Recursos técnicos necesarios para una prueba exitosa

Conexión segura

Los dispositivos Darktrace se conectan al Darktrace Central Management ("Call Home") a través de un canal de autenticación de dos factores seguro y encriptado para recibir nuevos modelos matemáticos y actualizaciones de software. Para implementaciones administradas y POV, esto también le permite aprovechar la experiencia de los analistas cibernéticos de Darktrace. Los clientes mantienen el control total de la conexión, la cual es iniciada y mantenida desde el dispositivo y se puede iniciar, terminar o auditar en cualquier momento. A los efectos de llevar a cabo controles de mantenimiento continuos, solicitamos que se mantenga una conexión durante el horario laboral normal.

Mapeo de datos

Para aprovechar al máximo el machine learning sin supervisión en hosts con direccionamiento IP dinámico, la señal DHCP del servidor al cliente debe estar contenido en el feed de datos. Esto ayuda a construir la comprensión más granular de la máquina particular y el comportamiento del usuario. Para implementaciones más allá de la Prueba de Valor, se pueden usar otras formas de mapeo de datos para permitir la integración con múltiples sistemas de registro estándar de la industria. Si los datos DHCP de la red no están disponibles, consulte a su contacto de Darktrace para obtener opciones secundarias.

Un compromiso conjunto: Revisiones TIR

Darktrace se compromete a proporcionar un punto de vista sin costo y sin compromiso, desde la instalación hasta los servicios posteriores y la consulta con nuestros especialistas en ciberseguridad. Además, cada informe de inteligencia de amenazas se produce exclusivamente para su organización, detallando las anomalías específicas que se descubren durante la POV.

Por cada informe inteligente de amenazas entregado, se lleva a cabo una reunión de revisión de TIR o una convocatoria con su equipo de cuentas, lo que lo ayuda a comprender los resultados de la POV y evaluar esos resultados. Para obtener el valor total de este compromiso, Darktrace requiere que el personal apropiado está involucrado en cada paso del proceso.

Privacidad y consideraciones legales

- La recolección de datos es pasiva.
- El procesamiento de datos de tráfico de red de Darktrace se realiza localmente en los dispositivos y no se carga en la nube o en un centro de datos de Darktrace.
- Los datos solo son accesibles a través de la conexión segura a menos que se acuerde lo contrario.
- Si el cliente aprovecha los servicios de análisis de paquetes profundos de Darktrace, los analistas de Darktrace aprovecharán el servicio 'Call Home' desde y hacia los dispositivos para inspeccionar de forma remota la interfaz de usuario local principal de Darktrace (Threat Visualizer) para el informe de inteligencia de amenazas (TIR) y, cuando sea necesario, extraer de manera forense, datos de captura de paquetes de muestra para ayudar a la identificación de amenazas. Además, el equipo de Operaciones de Darktrace utiliza "Call Home" para el monitoreo de la revisión de la salud y las actualizaciones del software del sistema.
- Los datos se eliminan de forma segura si no desea continuar más allá de la POV.
- El dispositivo no afecta a la red ni a las operaciones comerciales.
- Se requiere un contrato legal de retractilado para activar el dispositivo.