DARKTRACE

Características de Producto

Sistema Inmune Empresarial y Visualizador de Amenazas

Descripción General

El Sistema Inmune Empresarial es una solución de red para detectar e investigar ciberamenazas emergentes que han evadido la seguridad perimetral y puntos de defensa. Aplicando matemáticas avanzadas a modelos de comportamiento en su compañía, el sistema monitorea comportamientos y detecta anomalías en las computadoras de su organización y en las actividades de los usuarios. El enfoque matemático del sistema inmune empresarial no requiere de reglas ni características predefinidas y puede detectar ataques emergentes desconocidos que no habían sido vistos antes.

Darktrace se entrega como un dispositivo que se alimenta de manera pasiva de la información del tráfico puro de sus redes. Una vez conectado, la tecnología inmediatamente comienza a utilizar un rango de aproximaciones matemáticas para crear numerosos modelos de comportamiento para cada usuario y máquina de manera individual dentro de la organización. El autoaprendizaje matemático del Sistema Inmune Empresarial comienza a trabajar desde el primer día, detectando comportamientos anómalos de la red. El sistema continúa aprendiendo de forma permanente adaptándose a la evolución de la organización.

Creando poderosos modelos de “patrones de vida” de cada individuo y dispositivo de la red, le permiten a Darktrace detectar incluso sutiles cambios en el comportamiento, como la forma en la que alguien está usando la tecnología, los patrones o tendencias de acceso a datos en las comunicaciones. Esto puede indicar cualquier número de eventos potencialmente peligrosos, como el robo de credenciales de un usuario, un dispositivo comprometido, o las acciones de un empleado descontento o negligente.

Ejemplos como el reconocimiento de la red y de su recorrido, descargas inesperadas desde dominios inusuales de Internet, intranet o clonación de sistemas de archivos, inicios de sesión de datos sensibles desde un nuevo dispositivo y ubicación, aplicaciones y protocolos inusuales, o un cambio en el patrón de la subida de información son detectados a través de modelos matemáticos. Estas actividades pueden ser dignas de investigación si presentan una significativa desviación de la conducta normal.

Visualizador de Amenzas

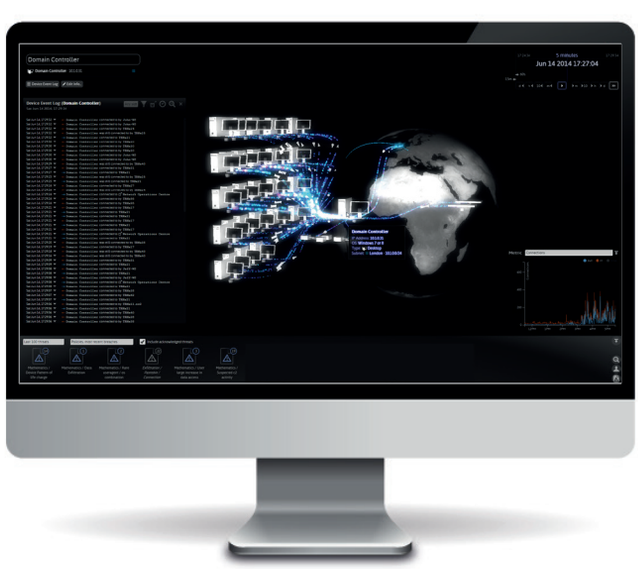
El Sistema Inmune Empresarial se complementa con el Visualizador de Amenazas, una interfaz gráfica 3D e interactiva diseñada específicamente para permitir a los analistas y ejecutivos de negocio visualizar intuitivamentecomportamientos e investigar anomalías, sin necesidad de una comprensión de las matemáticas avanzadas que potencian la plataforma.

Características Principales

- Detección avanzada de amenazas incluyendo nuevos y únicos ciberataques
- Basado en un sofisticado aprendizaje de máquina y modelos matemáticos.
- El algoritmo sin características predefinidas permite la detección de ataques emergentes o ataques específicos que no han sido vistos antes
- Trabaja en tiempo real para proporcionar alertas conforme surgen las amenazas
- Poderosa plataforma de visualización que permite analizar e investigar amenazas intuitivamente
- Dispositivo de red instalado de forma pasiva en la infraestructura en menos de una hora

El visualizador de amenazas provee a los usuarios con conocimientos basados en la información del relacionamiento y flujo de datos a través de la red, en tiempo real y para cualquier punto en su historial de conexiones. Cuando una anomalía emerge, el Visualizador de Amenazas muestra los acontecimientos previos y durante la anomalía, lo que le permite reproducir la secuencia de los acontecimientos cuestionables tal como sucedieron.

El visualizador es una herramienta interactiva, permite a los analistas investigar a fondo las capas a detalle y realizar consultas muy complejas. La plataforma soporta análisis e investigación a nivel detallado y permite la descarga de paquetes relevantes de la red para llevar una auditoria en la herramienta que su organización prefiera (ejemplo Wireshark).



Tecnología Complementaria

El Sistema Inmune Empresarial está diseñado para complementar la infraestructura y esquemas de seguridad existentes. La correcta configuración de las defensas perimetrales y centrales de la red son esenciales, pero solo parcialmente exitosas contra determinados ataques ya sean externos o internos. La integracion del monitoreo y detección sin características predefinidas provee una oportunidad para responder a ataques nuevos o específicos dentro de su organización.

La información del Sistema Inmune Empresarial puede ser direccionada a tableros de control de seguridad comerciales, hechos a la medida o SIEM a través de diferentes mecanismos (Syslog, SNMP, conectores, archivo, base de datos o API).

Fundamentos Matemáticos

La clave para estos nuevos modelos matemáticos no es solamente identificar las relaciones significativas de los datos, sino también cuantificar la incertidumbre asociada a tales inferencias. Mediante la comprensión de esta incertidumbre, es posible reunir muchos resultados dentro de un marco coherente – la base del análisis probabilístico Bayesiano.

El corazón del producto Darktrace son cuatro motores que utilizan múltiples enfoques matemáticos donde se intregra lo último en Estimación Bayesiana Recursiva. Los primeros tres motores producen modelos de comportamiento de manera individual de la gente, los dispositivos que usan y de la compañía entera de la cual son parte.

Cuando un comportamiento inusual es detectado en uno o más de estos tres motores, una alerta candidata es enviada al motor “Paraguas”, el “Clasificador de Amenazas”. Su trabajo consiste en mirar a través de las salidas de todos los modelos de forma continua, para filtrar falsos positivos e informar sobre anomalías auténticas dignas de una investigación, sin embargo sutiles. La combinación única de múltiples enfoques bayesianos correlacionados y moderados por el Clasificador de Amenazas hace a Darktrace altamente preciso en la detección de anomalías a escala empresarial.

Módulo de Políticas y Cumplimiento Darktrace

El Sistema Inmune Empresarial también se beneficia de un módulo integrado para políticas y monitoreo de cumplimiento y aplicación. Este soporta la definición de políticas adicionales de cumplimiento que pueden ser ajustadas para requerimientos específicos de detección de un usuario (ejemplo: no acceso a Dropbox, no viajar con tecnologías de la información sensible a ciertos países, únicamente servicios internos de DNS, etc.).

Sus datos son sus datos.

El Sistema Inmune Empresarial hace todo su procesamiento dentro de sus data centers. No envía datos a la nube y no hay acceso de los empleados por Darktrace, al menos que se acuerde con la organización con antelación. Los datos del cliente y los resultados inteligentes no se comparten con una comunidad amplia de usuarios.

Instalación y Configuración

Captura completa de paquetes.

El Sistema Inmune Empresarial consume tráfico puro de la red, de los siguientes casos:

- Puerto de expansión de su equipo de red existente
- Insertando/re usando una conexión de línea de red (TAP)

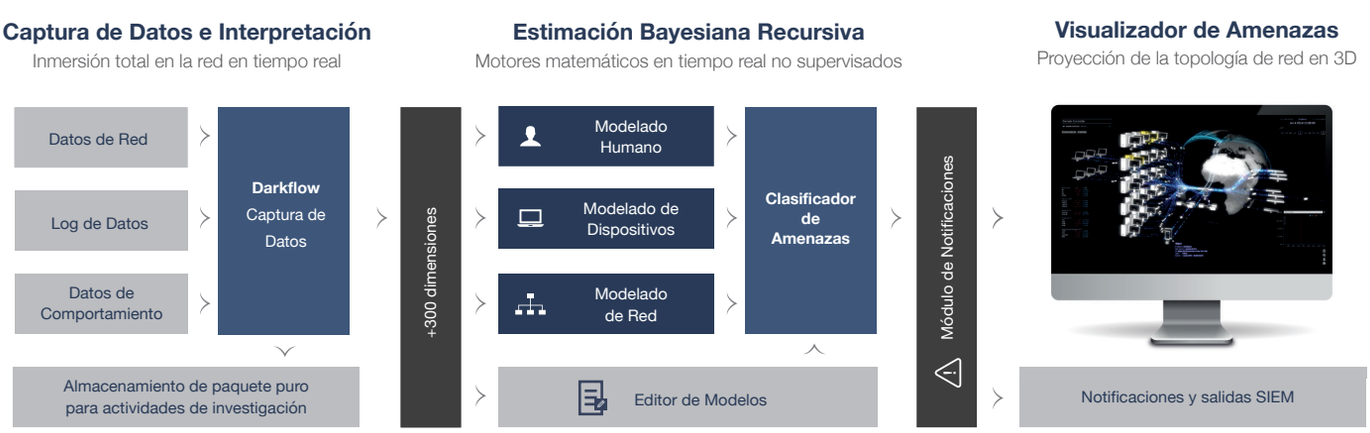
Simple de instalar, configurar y soportar.

- Aparato individual que ocupa 2U de espacio de rack
- Instalación, configuración y pruebas en menos de una hora
- Todas las interfaces de usuario son accedidas a través de un navegador web
- Requiere muy poca asistencia

Fácil de escalar

Un solo dispositivo Darktrace puede tener múltiples entradas de tráfico de red y cubrir hasta decenas de miles de máquinas individuales, en función de los volúmenes de tráfico pico. Varios dispositivos Darktrace pueden agruparse para cubrir las redes distribuidas geográficamente, eliminando la necesidad de mover grandes volúmenes de datos en torno a la red.

SISTEMA INMUNE EMPRESARIAL DARKTRACE



Darktrace Cyber Intelligence Platform (DCIP)

Darktrace appliances are highly tuned, high performance pieces of hardware that host the Darktrace platform. There are multiple types of Darktrace appliance, with different throughput capacities and options for data ingestion.

Darktrace's technical experts will help you decide which type of appliance you need based on the organization's bandwidth and the number of internal devices present.

DCIP-S: Ideal for small deployments with a limited number of devices. It can be configured as a probe to act as a collector in larger deployments. The DCIP-S appliance contains the following ports:

- 1 x out-of-band (OOB) interface
- 1 x 1Gbe admin interface
- 3 x 1Gbe analysis ports

DCIP-M: Small to Medium sized companies typically choose the Medium DCIP as they're 25x more powerful than a small in terms of connection count capacity. The DCIP-M appliance contains the following physical ports:

- 1 x 1Gbe admin interface
- 1 x out of band interface
- 3 x 1Gbe analysis port
- 2 x SFP+ analysis ports

DCIP-X2: The Darktrace DCIP-X2 series appliances are capable of ingesting data from multiple sources over different types of cable media. The X2 series is suitable for deployment in higher capacity environments and can operate as a master or probe as part of a distributed Darktrace deployment, or can function as a standalone device. The X2 series can be further expanded by additional network interface modules to provide further flexibility in deployment configuration. The DCIP-X2 appliance contains the following physical ports:

- 1 x 1Gbe admin interface
- 1 x out of band interface
- 1 x 1Gbe analysis port
- 2 x 1Gbe / 10Gbe analysis ports
- 2 x SFP+ analysis ports

DCIP-Z: The DCIP-Z series combine maximum processing power and high speed disk access. DCIP-Z appliances are suited to be placed as master appliances at the core of a high throughput master/probe distribution. The DCIP-Z appliance contains the following physical ports:

- 1 x 1Gbe admin interface
- 1 x out of band interface
- 1 x 1Gbe analysis port
- 2 x 1Gbe / 10Gbe analysis ports
- 2 x SFP+ analysis ports

Peak sustained throughput, maximum unique internal devices and maximum connections per minute are dependent on the type of traffic analyzed, the behavior of the devices and the application of software features. The values in this table have been derived from real-world corporate networks, and refer to a sustained rate, allowing for traffic peaks. Every network is different and so these metrics should be used as a guide only. In addition, the exact throughput capacity of any metric is dependent on the type and nature of the traffic seen by Darktrace.

Peak sustained throughput is the 95th percentile of bandwidth ingestion.

	DCIP-S	DCIP-M	DCIP-X2-11G	DCIP-Z
Form factor	1U rack mountable (half-depth)	1U rack mountable	2U rack mountable	2U rack mountable
Dimensions (in)	17.32" x 14.57" x 1.73"	17.32" x 29.33" x 1.73"	17.32" x 29.33" x 3.46"	17.32" x 29.33" x 3.46"
Dimensions (cm)	44cm x 37cm x 4.4cm	44cm x 74.5cm x 4.4cm	44cm x 74.5cm x 8.8cm	44cm x 74.5cm x 8.8cm
Weight (lbs / Kg)	13.3 lbs / 6 Kg	33 lbs / 15 kg	51 lbs / 23 Kg	51 lbs / 23 Kg
Racking	Fits 19" Rack	Fits 19" rack	Fits 19" rack	Fits 19" rack
Interface admin ports	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T
Remote management ports	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T
Copper analysis ports	3 x 10/100/1000 BASE-T	3 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T 2 x 10 GBASE-T	1 x 10/100/1000 BASE-T 2 x 10 GBASE-T
SFP+ analysis ports	n/a	2 x 10Gbe/1Gbe SFP+	2 x 10Gbe/1Gbe SFP+	2 x 10Gbe/1Gbe SFP+
Peak sustained throughput	Up to 300 Mbps	Up to 2Gbps	Up to 5Gbps	Up to 5Gbps
Maximum unique internal devices	Up to 1000 devices analyzed	Up to 8,000 devices analyzed	Up to 36,000 devices analyzed	Up to 50,000 devices analyzed
Maximum connections per minute	2,000	50,000	100,000	250,000
Power supply	Single 350W IEC 13C 100/240V	Dual 750W IEC 13C 100/240V	Dual 1100W IEC 13C 100/240V	Dual 1100W IEC 13C 100/240V
Power consumption	Idle 26 W - 89 BTU/hr	Idle 120 W - 409 BTU/hr	Idle: 128 W - 436 BTU/hr	Idle: 128 W - 436 BTU/hr
	85% 89 W - 305 BTU/hr Max 105 W – 358 BTU/hr	85% 359 W - 1224 BTU/hr Max 418 W – 1426 BTU/hr	85%: 365 W - 1245 BTU/hr Maximum: 426 W - 1453 BTU/hr	85%: 365 W - 1245 BTU/hr Maximum: 426 W - 1453 BTU/hr
Supported Expansion Modules	Can support one expansion model: • 2-port 1G/10G SFP+ • 2-port 1G RJ45 1000 BASE-T • 4-port 1G RJ45 1000 BASE-T	Can support one expansion model: • 2-port 1G/10G SFP+ • 2-port 10G RJ45 10000 BASE-T • 2-port 1G RJ45 1000 BASE-T • 4-port 1G RJ45 1000 BASE-T	Can support up to three expansion models: • 2-port 1G/10G SFP+ • 2-port 10G RJ45 10000 BASE-T • 2-port 1G RJ45 1000 BASE-T • 4-port 1G RJ45 1000 BASE-T	Can support up to three expansion models: • 2-port 1G/10G SFP+ • 2-port 10G RJ45 10000 BASE-T • 2-port 1G RJ45 1000 BASE-T • 4-port 1G RJ45 1000 BASE-T
Safety certificate	UL 60950-CSA 60950, EN 60950, IEC 60950 CB Certicate & Report, IEC 60950			
EMI Certification	FCC Part 15, Class A (CFR 47) (USA), ICES-003 Class A			