HEIMDAL™

Threat Prevention - Endpoint

Busque, prevenga, detecte y responda a las amenazas de sus endpoints.

Trabajando en tándem, DarkLayer Guard™ y Vector^{N} Detection™ son herramientas proactivas autónomas de código perfeccionadas para superponer otras tecnologías protectoras basadas en la detección de códigos.

Mejorado con TTPC (Threat To Process Correlation), su organización obtiene las herramientas esenciales de búsqueda de amenazas para trazar los puntos críticos de seguridad en su entorno.

Ahora mejorado con Predictive DNS, un algoritmo de IA y ML verdaderamente revolucionario que es capaz de predecir que un dominio es malicioso antes de albergar contenido malicioso. Las redes neuronales avanzadas y el análisis lingüístico de IA son capaces de lograr un nivel sin precedentes de prevención verdaderamente inteligente.

DARKLAYER GUARD™

El sistema esencial de prevención de intrusiones basado en host (HIPS)

DarkLayer Guard™ es un motor de filtrado de tráfico bidireccional exclusivo que admite listas blancas / negras totalmente personalizables.

Con él, su organización puede bloquear la comunicación de red para mitigar las vulnerabilidades de Zero Hour, Ransomware C&C, ataques de próxima generación y fugas de datos.

Al utilizar nuestra innovadora tecnología de correlación de amenazas a procesos, podemos identificar los procesos de ataque y proporcionar capacidades de HIPS para los endpoints.

VECTOR^{N} DETECTION™

Detección autónoma de código para encontrar amenazas no detectadas por NGAV y escáneres de código

Al rastrear la comunicación entre el dispositivo y la infraestructura, **Vector^{N} Detection™** detectará las cepas de malware de segunda generación que ningún otro producto puede ver, entregando efectivamente un HIDS en la capa de tráfico de la máquina.

Utilizando el aprendizaje automático para establecer patrones de compromiso y ofreciendo indicadores de compromiso / ataque (IOA / IOC), este es un complemento único que impulsará cualquier otro tipo de seguridad de endpoint.

Las técnicas de ofuscación de malware se están volviendo más avanzadas y capaces de evadir la detección tradicional.

Con **DarkLayer Guard™** y **Vector^{N} Detection™**, el malware se bloquea a nivel de tráfico, deteniendo sus comunicaciones con la infraestructura delictiva.

Aprovechando la inteligencia única obtenida mediante el bloqueo de amenazas a nivel de DNS, HTTP y HTTPS, **DarkLayer Guard™** y **Vector^{N} Detection™** no solo le dan el poder de detener ataques activos, sino que también aceleran su proceso de investigación. De esta manera, los endpoints vulnerables se pueden identificar y reforzar contra futuras amenazas, lo que garantiza un enfoque proactivo de la seguridad.

El costo de implementar una nueva solución, incluida una de seguridad, ha sido durante mucho tiempo una propuesta intimidante para las empresas, especialmente las más pequeñas y con más recursos limitados. Ese no es el caso aquí.

100% compatible con sus soluciones existentes y otros módulos de seguridad de Heimdal, DarkLayer Guard™ y Vector^{N} Detection™ son la solución autónoma de código para combatir el malware de próxima generación, el ransomware y otras amenazas empresariales.

"En términos de prevención de ataques, ya hemos visto un valor claro en los primeros meses que usamos Heimdal™ Security, incluso con un par de ataques de ransomware bloqueados. La forma en que detecta malware que el antivirus no detecta es muy especial. Heimdal es una forma sencilla y rápida de mejorar nuestra seguridad central y nos ayuda a prevenir ataques incluso antes de que sucedan."

- Kifaf General Trading, distribuidor clave de Sony Entertainment en la región de los Emiratos Árabes Unidos

"Aunque nuestra red está muy bien protegida, sabíamos que teníamos que agregar una capa adicional de seguridad a nuestros clientes. Simplemente porque la mayor parte son portátiles. Cuando estos clientes abandonaron el edificio, quedó claro que el antivirus no era suficiente según el panorama moderno de las ciberamenazas."

- Schultz Information

Los delincuentes pueden eludir fácilmente los escáneres de códigos y comportamientos como el antivirus, así como los firewalls, desencadenando devastadores ataques de ransomware o creando violaciones de datos que dañarán su organización.

10,975 DOMINIOS MALICIOSOS

La cantidad de dominios maliciosos eliminados mensualmente en el Reino Unido, solo por una agencia.

– NCSC.gov.uk

1,783 QUEJAS SOBRE RANSOMWARE

El número de quejas presentadas al Centro de Quejas de Delitos en Internet (IC3), con un promedio de 5 víctimas diarias.

– FBI

3,785 FUGAS DE DATOS CORPORATIVOS

En 2017, según consta en The Internet Crime Complaint Center (IC3). En promedio, se producen diariamente 10 violaciones de datos.

- FBI

79% ATAQUES DNS EN 2020

Casi 4 de cada 5 organizaciones (79%) han experimentado un ataque de DNS en 2020.

– IDC 2020 Global DNS Threat Report

9.5 ATAQUES POR AÑO

Organizaciones de todas las industrias sufrieron un promedio de 9,5 ataques por año en 2020.

– IDC 2020 Global DNS Threat Report

$924 MIL EN COSTOS

El costo promedio de un ataque de DNS en 2020 en las organizaciones es de $ 924,000 a nivel mundial

– IDC 2020 Global DNS Threat Report

$1 MILLION EN COSTOS DE DAÑOS

El costo promedio de un ataque de DNS en 2020 en las organizaciones es de $ 1. 082.710 en los EE. UU.

– IDC 2020 Global DNS Threat Report

Póngase en contacto hoy mismo para descubrir cómo mejoran su entorno.

www.thorlatam.com

Disponible para