MARCUS

MARCUS

Seguridad completa para entornos físicos, virtuales, híbridos y en la nube

MARCUS tiene el propósito de garantizar la seguridad, detectar, analizar, y responder a amenazas especializadas y de prevenir proactivamente una administración en tiempo real.

MARCUS es un dispositivo de propósito específico de protección frente a amenazas avanzadas que proporciona visibilidad e inteligencia de toda la red. Es la mejor solución de detección y respuesta de red (NDR) de su clase diseñada para ayudar a las organizaciones con incidentes.

FUNCIONES PRINCIPALES

DETECCIÓN, MITIGACIÓN Y PREVENCIÓN DE VULNERABILIDADES

- Capacidad para realizar inspección profunda de paquetes (DPI) bidireccionalmente, detectando, analizando y previniendo ataques a vulnerabilidades nuevas (zero-day) y existentes en sistemas operativos y aplicaciones instaladas en cada servidor.
- Operación en dos modos: modo de prevención, que permite monitorear el tráfico para registrar ataques sin tomar acciones de bloqueo; y modo de detección, que permite monitorear el tráfico para registrar y bloquear ataques sin afectar el tráfico normal no relacionado con el ataque.
- Capacidad para realizar escaneos en los servidores y determinar automáticamente los parches virtuales necesarios para proteger las vulnerabilidades del sistema operativo y las aplicaciones.
- Capacidad para bloquear el tráfico entre las interfaces de red de los servidores.

MONITOREO DE INTEGRIDAD

- Identificación de cambios en archivos críticos, configuraciones, carpetas, servicios y claves del registro tanto del sistema operativo como de las aplicaciones, a través de reglas de monitoreo de integridad automatizadas.
- Capacidad de alertar en tiempo real cuando se detecte una modificación en carpetas, archivos o claves del registro del sistema operativo y aplicaciones. Las alertas pueden ser enviadas por correo electrónico o syslog.
- Creación de reglas personalizadas para el monitoreo de modificaciones en archivos críticos, carpetas y claves del registro.
- Capacidad para ejecutar tareas programadas y asignar automáticamente las reglas de monitoreo de integridad recomendadas por la solución.

MONITOREO DE BITÁCORAS

- Inspección de bitácoras del sistema operativo y aplicaciones para identificar eventos de seguridad relevantes o críticos.
- Permite la inspección de eventos generados en el visor de eventos para servidores Windows y en syslog messages para servidores con sistema operativo Linux.
- Permite la inspección de eventos generados por aplicaciones, almacenados en archivos de bitácoras.
- Capacidad de alertar en tiempo real cuando se genera un evento crítico o relevante, con envío de alertas por correo electrónico o syslog.
- Creación de reglas personalizadas para el monitoreo de bitácoras.
- Ejecución de tareas programadas y asignación automatizada de reglas de monitoreo de bitácoras recomendadas por la solución.

MONITOREO DE AMENAZAS INTERNAS & EXTERNAS

- Administración de eventos de red, alarmas, logs y tickets enviados desde diversas fuentes y sondas a la consola central.
- Visibilidad de los eventos de seguridad en un dashboard intuitivo.
- Acceso a la información y acciones de configuración con roles múltiples, al menos dos, que correspondan a diferentes niveles de acceso requeridos, como monitoreo y auditoría.
- Capacidad para generar informes automatizados programables en formatos PDF, JPG y CSV.
- Administración delegada basada en roles, permitiendo la delegación según la estructura de seguridad corporativa.
- Soporte para la agrupación de administradores para dispositivos específicos.
- Software de administración y monitoreo a través de una sola consola gráfica basada en web HTML5 para administración local y remota.

MONITOREO DE APLICACIONES MULTIPLATAFORMA

- Capacidad para detectar y bloquear software no autorizado de forma automática, sin limitaciones del sistema operativo, en base a una lista de sistemas operativos.
- Escaneo del servidor para determinar qué aplicaciones están actualmente en ejecución.
- Bloqueo del sistema una vez creado el inventario, evitando la ejecución de nuevas aplicaciones que no estén en la lista blanca definida por el administrador.
- Integración en un entorno DevOps para permitir cambios continuos en las listas de aplicaciones, manteniendo al mismo tiempo la protección mediante APIs.
- Capacidad para capturar amenazas que aún no tienen firma, incluidas las amenazas zero-day.
- Configuración sencilla e intuitiva, permitiendo una rápida puesta en marcha.

MONITOREO DE TRÁFICO

- Monitoreo y visualización del desempeño de la red.
- Interfaz web totalmente funcional que facilita la implementación de políticas de monitoreo de throughput, disponibilidad y alarmas de caída de enlaces.
- Selección de interfaces específicas para monitoreo.
- Notificación automática de alarmas ante fallas o cortes de servicio, con envío por correo electrónico al área usuaria designada.
- Configuración de ancho de banda para transmisor y receptor.
- Análisis de tipo y calidad de servicio (QoS).
- Generación de reportes personalizados mensuales y bajo demanda.

ALMACENAMIENTO

- Capacidad de almacenamiento histórico de datos con granularidad de visualización adaptable.

MONITOREO DE COMPORTAMIENTOS

- Motores de detección especializados con reglas de correlación y aislamiento personalizado para detectar todos los aspectos de un ataque dirigido, no solo del malware.
- Lista de vigilancia para proteger dispositivos de mayor riesgo en la red.
- Capacidad de análisis de más de 80 protocolos de red (HTTP, SMTP, POP3, FTP, IRC, etc) para detectar posibles medios de infección.
- Consola de información en tiempo real para visibilidad constante.
- Detección de tráfico C&C y actividad backdoor sin discriminar entre diferentes sistemas operativos.
- Monitoreo de aplicaciones no autorizadas por las políticas internas del usuario (P2P, chat en IRC, multimedia, etc.).
- Detección de movimientos laterales, malware avanzado (zero-day o desconocido), comportamientos de ataques humanos y otras amenazas mediante motores de detección propietarios.

SANDBOXING

- Capacidad de utilizar imágenes virtuales configuradas para que coincidan exactamente con la configuración del sistema, drivers, aplicaciones instaladas y versiones de idioma de la organización.
- Soporte de sandboxing local para replicar entornos específicos del usuario.
- Soporte mínimo de 2 sistemas operativos en entorno controlado.
- Sandboxing personalizable según requerimientos del usuario.

ESPECIFICACIONES TÉCNICAS

INTERFACES DE RED

- Soporte para interfaces de cobre y varios tipos de fibra.
- Soporte para velocidades mínimas de 1G y 10G.

CARACTERÍSTICAS DE SEGURIDAD

- Inspección profunda de paquetes (DPI).
- Monitoreo bidireccional del tráfico.
- Detección y prevención de vulnerabilidades zero-day.
- Aplicación de parches virtuales.
- Bloqueo de tráfico entre interfaces de red de servidores.

CONTROL DE APLICACIONES

- Detección y bloqueo de software no autorizado.
- Inventario y control de aplicaciones del servidor.
- Integración con entornos DevOps.
- Detección de amenazas zero-day.

INTEGRACIONES

- Capacidad de mantener una gestión centralizada
- Compatible con ONESECURITY, SIEM FLAMMAS, ONE SOAR
- Integración nativa con soluciones SIEM como HP ArcSight, IBM QRadar y Splunk.
- Integraciones eficaz con soluciones NGFW (Fortinet, pfSense, Palo Alto, Hillstone,etc)

SOPORTE DE DISPOSITIVOS

- Capacidad para soportar un mínimo de 100 dispositivos concurrentes con todas las funcionalidades activas.
- Capacidad de integrar en modo transparente

MONITOREO

- Monitoreo de integridad de archivos, configuraciones, servicios y claves del registro.
- Alertas en tiempo real vía correo electrónico o syslog.
- Ejecución de tareas programadas.
- Reportes gráficos a través de herramienta web sobre el tráfico diario, semanal y mensual en línea de tiempo (tiempo real), con almacenamiento de bitácoras para fines comparativos.
- Reportes mensuales de calidad del servicio, disponibilidad, fallas, relación de tráfico de entrada/salida, prevención de vulnerabilidades, monitoreo de integridad y aplicaciones multiplataforma.

MARCUS - PHYSICAL APPLIANCE

Model		CC-1000	CC-2000	CC-3000
Based on STA	STA	5STA-100	8STA-100	12STA-100
	Throughput (Gbps)	1	3	5
Based on Logs	Daily access log number (Million/Day)	200	250	350
	Average EPS (Per log/Sec)	3,130	4,380	6,255
	Peak EPS (Per log/Sec)	12,000	15,000	18,000
	Disk consumption (GB/Day)	112	140	196
Sandboxing Support		2/4	2/4	4/8

TECHNICAL SPECIFICATIONS

CPU (Cores)	12	24	48
Data Hard Drive Capacity	SATA 4TB (Hasta: SATA 32TB)	SATA 4TB (Hasta: SATA 40TB)	SATA 4TB (Hasta: SATA 48TB)
Rack Height	2U	2U	2U
Gross Weight (kg)	28	28	37.5
Power Supply	Redundant	Redundant	Redundant
Copper Ports	10/100 /1000BASE-T*4	10/100 /1000BASE-T*4	10/100 /1000BASE-T*4
SFP/SFP + Ports	N/A	10GbE SFP+*2	10GbE SFP+*2
USB	4**USB2.0 or above	4**USB2.0 or above	4**USB2.0 or above

Las capacidades y requerimientos detallados son referentes a la versión 4.0 FlammasOS y posteriores.

Model	STA-50	STA-100	STA-300	STA-500
PERFORMANCE				
Peak Sustained Throughput	Up to 500Mb	Up to 1Gb	Up to 3Gb	Up to 10Gb
Maximum Unique Internal Devices Analyzed	1,000	3,000	10,000	35,000
TECHNICAL SPECIFICATIONS				
Memory (GB)	4	8	8	48
Hard Drive	128GB SSD	128GB SSD	480GB SSD (2TB SATA HDD - Optional)	960GB SSD
Rack Height	1U	1U	2U	2U
Power Supply	Single	Single	Dual	Dual
Copper Ports	10/100 /1000BASE-T*4	10/100 /1000BASE-T*6	10/100 /1000BASE-T*6	10/100 /1000BASE-T*4
SFP/SFP + Ports	N/A	10GbE SFP*2	10GbE SFP+*2	1GbE SFP*4 10GbE SFP+*8
Serial Ports	RJ45*1	RJ45*1	RJ45*1	RJ45*1
USB	USB2.0*2	USB2.0*2	USB2.0*2	USB2.0*2

Las capacidades y requerimientos detallados son referentes a la versión 4.0 FlammasOS y posteriores.

MARCUS - VIRTUAL

Model	vCC-10	vCC-50	vCC-100	vCC-500	vCC-1000	vCC-2000	vCC-3000
PERFORMANCE							
Traffic Handling Capacity (Gbps)	0.5	1	2	3	5	8	12
Blog Handing Capacity (EPS/s, Peak)	5,000	5,000	5,000	5,000	10,000	12,000	15,000
TECHNICAL SPECIFICATIONS							
CPU (Main Frequency, Number of Cores)	2.10Hz*8	3.60GHz*8	3.60GHz*8	3.60GHz*8	2.10GHz*16	2.10GHz*32	2.60GHz*40
Memory (GB)	8	16	64	64	128	128	256
Sandboxing Support	2/4			20		30	
Minimum Hard Disk Requirement	1TB	1TB	2TB	2TB	4TB	8TB	8TB
Recommended Hard Disk Requirement	6TB	6TB	12TB	12TB	24TB	48TB	48TB

Las capacidades y requerimientos detallados son referentes a la versión 4.0 FlammasOS y posteriores.

MARCUS (STA) SENSOR - VIRTUAL

Model	vSTA-10	vSTA-30	vSTA-50	vSTA-100	vSTA-200	vSTA-500	vSTA-1000
PERFORMANCE							
Traffic Handling Capacity (Gbps)	100Mb	300Mb	500Mb	1Gb	2Gb	5Gb	10Gb
Sandboxing Support	2/4			20		30	
CPU (Main Frequency, Number of Cores)	2.4GHz*4	2.4GHz*4	2.4GHz*4	2.4GHz*4	2.4GHz*8	2.4GHz*16	2.4GHz*28
Memory (GB)	4	4	4	8	16	32	48
System Disk	> 64GB	> 64GB	> 64GB	> 64GB	> 64GB	> 64GB	> 64GB
Recommended Minimum Data Disk	> 128GB	> 128GB	> 128GB	> 128GB	> 480GB	> 480GB	> 480GB

Las capacidades y requerimientos detallados son referentes a la versión 4.0 FlammasOS y posteriores.

© 2025 Flammas, Inc. All rights reserved. Flammas®, ONESECURITY®, SIEM FLAMMAS®, ONE SOAR® and other trademarks are the registered property of Flammas Inc. Performance results and other metrics mentioned herein are derived from internal testing under controlled conditions, so actual results may vary. This document does not constitute a contractual obligation on the part of Flammas. Unless otherwise provided in a written contract signed by a senior legal representative of Flammas, the company makes no warranties, express or implied, regarding the performance of its products. Flammas reserves the right to modify, update or adjust this content at any time without notice, with the most recent published version always applying.