RED DINÁMICA

Con el objetivo de asegurar la protección, detectar, analizar y responder a amenazas especializadas, así como prevenir de manera proactiva mediante una administración en tiempo real, este dispositivo de defensa contra amenazas avanzadas ofrece visibilidad e inteligencia a lo largo de toda la red. Es la mejor solución en su clase para la detección y respuesta de red (NDR), diseñada para asistir a las organizaciones en la gestión de incidentes.

FUNCIONES PRINCIPALES

DETECCIÓN, MITIGACIÓN Y PREVENCIÓN DE VULNERABILIDADES

Capacidad para realizar inspección profunda de paquetes (DPI) en ambas direcciones, detectando, analizando y previniendo ataques tanto a vulnerabilidades nuevas (zero-day) como a las existentes en sistemas operativos y aplicaciones instaladas en cada servidor. Funciona en dos modos:

- **Modo de prevención:** Permite monitorear el tráfico para registrar ataques sin realizar acciones de bloqueo.
- **Modo de detección:** Permite monitorear el tráfico para registrar y bloquear ataques sin interferir con el tráfico normal no relacionado con el ataque.

Capacidad para escanear servidores y determinar automáticamente los parches virtuales necesarios para proteger las vulnerabilidades en el sistema operativo y las aplicaciones, así como 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 de registro tanto del sistema operativo como de las aplicaciones, mediante reglas automatizadas de monitoreo de integridad.

- Capacidad de alertar en tiempo real cuando se detecten modificaciones en carpetas, archivos o claves de 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 de registro.

- Capacidad para ejecutar tareas programadas y asignar automáticamente las reglas de monitoreo de integridad recomendadas por la solución.

MONITOREO DE BITÁCORAS

- Monitoreo de bitácoras del sistema operativo y de las aplicaciones para identificar eventos de seguridad importantes o críticos.
- Permite revisar eventos generados en el visor de eventos de servidores Windows y en los mensajes de syslog para servidores con sistema operativo Linux.
- Facilita la revisión de eventos generados por aplicaciones y almacenados en archivos de bitácoras.
- Ofrece la capacidad de enviar alertas en tiempo real cuando se detecta un evento crítico o relevante, con notificaciones por correo electrónico o syslog.
- Permite crear reglas personalizadas para el monitoreo de bitácoras.
- Capacidad de ejecutar tareas programadas y asignar automáticamente las reglas de monitoreo de bitácoras recomendadas por la solución.

MONITOREO DE APLICACIONES MULTIPLATAFORMA

- Capacidad para detectar y bloquear software no autorizado de forma automática, sin limitaciones del sistema operativo, de acuerdo con la lista de sistemas operativos indicados en las características principales.
- 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 AMENAZAS INTERNAS & EXTERNAS

- Gestión de eventos de red, alarmas, registros y tickets enviados desde diversas fuentes y sondas hacia una consola central.
- Visualización de eventos de seguridad en un panel de control intuitivo.
- Acceso a la información y acciones de configuración con múltiples roles, al menos dos, que correspondan a diferentes niveles de acceso requeridos, como monitoreo y auditoría.
- Capacidad para generar informes automatizados y 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 según dispositivos específicos.
- Software de administración y monitoreo accesible a través de una única consola gráfica basada en web HTML5, tanto para administración local como remota.

ESPECIFICACIONES TÉCNICAS

- Compatibilidad con interfaces de cobre y diversos tipos de fibra.
- Soporte para velocidades mínimas de 1G/10G.
- Capacidad para manejar al menos 100 dispositivos concurrentes con todas las funcionalidades activas.
- Capacidad de almacenamiento histórico de datos con una granularidad de visualización adaptable.

ESPECIFICACIONES TÉCNICAS

INTERFACES DE RED

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

ALMACENAMIENTO

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

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.

SOPORTE DE DISPOSITIVOS

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

MONITOREO

- Monitoreo de integridad de archivos, configuraciones, servicios y claves del registro.
- Alertas en tiempo real vía correo electrónico o syslog.
- Creación de reglas personalizadas para integridad y bitácoras.
- Ejecución de tareas programadas.

GESTIÓN

- Administración centralizada de eventos, alarmas, logs y tickets.
- Dashboard intuitivo para eventos de seguridad.
- Control de acceso basado en roles.
- Generación automatizada de informes.
- Consola gráfica basada en HTML5 para administración local y remota.

SANGFOR CYBER COMMAND – PHYSICAL APPLIANCE

Model		CC-1000	CC-2000	CC-3000
Based on STA	STA	5STA-100	8STA-100	12STA-100
	Throughput (Gbps)	1	8	12
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
TECHNICAL SPECIFICATIONS				
Memory (GB)		128	128	256
CPU (Cores)		12	16	48
System Disk		240GB SSD	240GB SSD	240GB SSD
Data Hard Drive Capacity		SATA 4TB*8 (Total: SATA 32TB)	SATA 4TB*10 (Total: SATA 40TB)	SATA 4TB*12 (Total: 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

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

SANGFOR CYBER COMMAND - 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	2.10Hz*8	3.60GHz*8	3.60GHz*8	2.10GHz*16	2.10GHz*32	2.60GHz*40
Memory (GB)	32	32	64	64	128	128	256
System Disk	128GB SSD	128GB SSD	128GB SSD	128GB SSD	128GB SSD	128GB SSD	128GB SSD
Minimum Hard Disk Requirement	1TB	1TB	2TB	2TB	4TB	8TB	8TB
Recommended Hard Disk Requirement	6TB	6TB	12TB	12TB	24TB	48TB	48TB

STEALTH THREAT ANALYSIS (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
TECHNICAL SPECIFICATIONS							
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	>	>	>	>	>	>	>
Recommended Minimum Data	64GB	64GB	64GB	64GB	64GB	64GB	64GB
Disk	128GB	128GB	128GB	128GB	480GB	480GB	480GB