**Tecnologías de Seguridad**

**Trabajo en clase**

**Integrantes:**

* Luis Enrique Pérez Señalin.
* Jossué Rivadeneira
* Marlon Paul Zurita Chimbolema

**Tema:** Análisis de Características de Dispositivos de Seguridad

**Objetivos:**

1. Buscar un dispositivo firewall Next Generation
2. Analizar las características del dispositivo firewall
3. Analizar el tipo de dispositivo que es (IPS – IDS)
4. **Dispositivo Firewall Next generation**

Los dispositivos firewall next generation son los firewalls actuales que tienen distintas funcionalidades para proteger a la red.

El dispositivo seleccionado es el MAESTRO HYPERSCALE ORCHESTRATOR 140 | 175, con el datasheet <https://www.checkpoint.com/downloads/products/maestro-hyperscale-orchestrator-datasheet.pdf>.

1. **Características**

El firewall tiene las siguientes características.

**Tipo:** First Time Prevention Capabilities **Correspondiente:** IPS, al ser prevención de primera vez corresponde a un IPS, todas las características analizan las amenazas en la red.

|  |  |
| --- | --- |
| **Característica** | **Comentario** |
| CPU-level, OS-level and static file analysis | Analiza amenazas de forma avanzada |
| File disarm and reconstruction via Threat Extraction | Analiza el archivo en búsqueda de amenazas, identificando partes del archivo que representen un riesgo para luego eliminarlo y reconstruir el archivo sin la parte maliciosa. |
| Average emulation time for unknown files that require full sandbox evaluation is under 100 seconds | Analiza los archivos desconocidos usando un Sandbox (entorno virtual aislado) para que no afecte a los equipos reales, realizando un análisis exhaustivo en 100 segundos. |
| Maximal file size for Emulation is 100 MB | Tiene un tamaño suficiente para programas pequeños. |
| Emulation OS Support: Windows XP, 7, 8.1, 10 | Utiliza emuladores para sistemas operativos específicos para ejecutar y analizar el comportamiento de archivos posiblemente maliciosos. |

**Tipo:** Applications **Correspondiente:** NGFW ,Next generation Firewall, tiene la capacidad de administrar y controlar el tráfico de forma avanzada.

|  |  |
| --- | --- |
| **Característica** | **Comentario** |
| Use 10,000+ pre-defined or customize your own applications | Tiene la capacidad de reconocer más de 10.000 aplicaciones por defecto y personalizar aplicaciones para el uso de la empresa. |
| Accept, prevent, schedule, and apply traffic-shaping | Lo que permite bloquear o permitir ciertas aplicaciones o páginas en la red para ciertos usuarios, incluso ajustándolo por horarios y la cantidad de ancho de banda para cada aplicación. |

**Tipo:** Data Loss Prevention **Correspondiente:** IDS, debido a la relación que comparten la detección e identificación de patrones de ataques basados en firmas conocidas

|  |  |
| --- | --- |
| **Característica** | **Comentario** |
| Classify 700+ pre-defined data types |  |
| End user and data owner incident handling |  |

**Tipo:** Dynamic User-based Policy **Correspondiente:** IDS, Política Dinámica Basada en Usuarios, se utiliza para aplicar reglas y políticas de seguridad específicas en función de la identidad del usuario y evitar que existan intrusos.

|  |  |
| --- | --- |
| **Característica** | **Comentario** |
| Integrates with Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers and with 3rd parties via a Web API | El enfoque en servicios de autenticación y perfiles de usuario es manejado por un IDS |
| Enforce consistent policy for local and remote users on Windows, macOS, Linux, Android and Apple iOS platforms | El manejo de perfiles de usuarios para garantizar la seguridad de la organización con políticas consistentes es administrado por un IDS |