SIEM Feeder

Integración con sistemas corporativos SIEM para agregar detalles y contexto de todo lo que se ejecuta en la red de TI

panda a WatchGuard brand

UNA NUEVA FUENTE DE INFORMACIÓN: PROGRAMAS DE USUARIO

Las soluciones de System Information and Event Management (SIEM) se han convertido en una necesidad para administrar la seguridad de infraestructuras grandes y medianas de TI. Sus capacidades para recopilar y correlacionar el estado de sistemas de TI permite a las organizaciones convertir grandes volúmenes de datos en información útil para la toma de decisiones.

Integran una nueva fuente de información crítica con inteligencia de seguridad recopilada y correlacionada por su solución de SIEM: todos los procesos y los programas se ejecutan en sus dispositivos y Panda Adaptive Defense los supervisa de manera continua.

UN NUEVO ESTADO DE SEGURIDAD

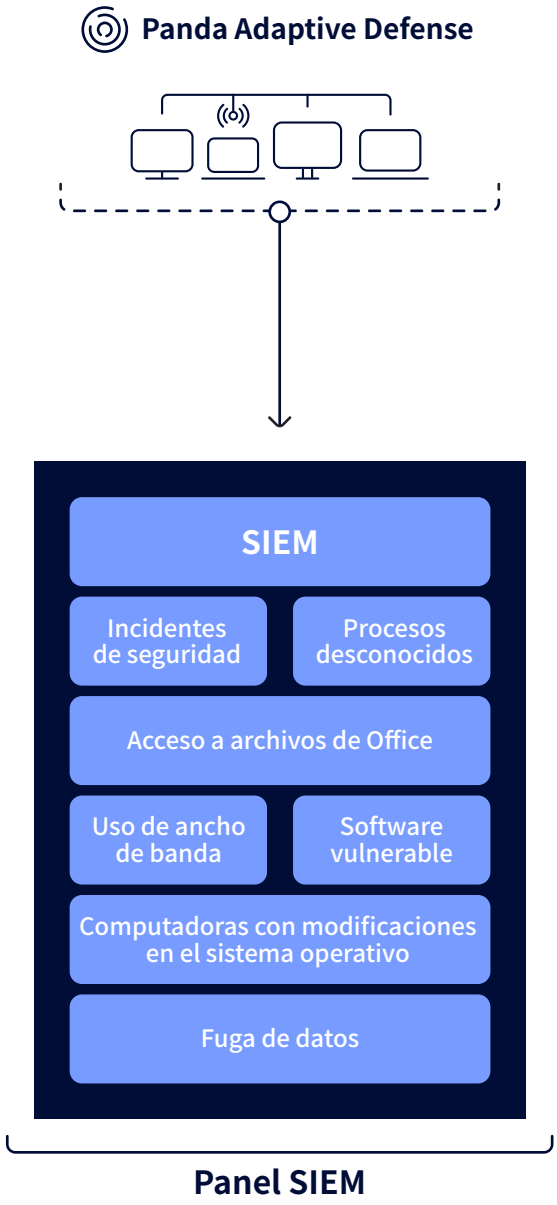
Los departamentos de TI requieren de altos niveles de visibilidad y control para poder anticipar los problemas de seguridad provocados por el malware de próxima generación.

Panda Adaptive Defense ayuda a los administradores a filtrar los grandes volúmenes de datos manejados por los sistemas de SIEM y a concentrarse en lo que realmente importa:

- ¿Cuáles son los nuevos programas que se están ejecutando y que aún deben clasificarse como goodware o malware?
- ¿Cómo llegaron esos programas a la red?
- ¿Qué actividades sospechosas están llevando a cabo en los dispositivos del usuario (edición de registros, anzuelos, instalación de controladores, etc.)?
- ¿Qué software legítimo con vulnerabilidades conocidas y aprovechables está en uso?
- ¿Qué procesos acceden a documentos de usuarios y envían información?
- ¿Cuál es el uso de red de cada proceso que se ejecuta en la red de TI?

INTEGRACIÓN Y OPERACIÓN SIN PROBLEMAS

Panda Adaptive Defense se integra sin problemas con soluciones corporativas de SIEM existentes sin implementaciones adicionales en los dispositivos de los usuarios. Los eventos supervisados se envían de manera segura con los formatos LEEF/CEF compatibles con la mayoría de los sistemas de SIEM del mercado, ya sea en forma directa o indirecta a través de complementos. SIEM Feeder permite una integración nativa de la telemetría en una instancia de plataforma DEVO en segundos, sin la necesidad de un proyecto de integración (SIEM FEEDER a DEVO).



Plataformas compatibles y requisitos del sistema de SIEM Feeder

http://go.pandasecurity.com/siem-feeder/requirements

Este módulo está disponible en:

Panda Adaptive Defense **Panda Adaptive Defense 360**

Compatible con:

ALIEN VAULT · ArcSight An HP Company · Radar · bitacora · lookwise · Formatos LEEF y CEF

WatchGuard

VENTAS DE EE. UU.: 1.800.734.9905 VENTAS INTERNACIONALES: +1-206-613-0895 www.watchguard.com | pandasecurity.com