Advanced Reporting Tool

Transformación de Datos en Insights Prácticos de TI y Seguridad

panda a WatchGuard brand

EL AUMENTO EN EL VOLUMEN DE LOS DATOS DE SEGURIDAD QUE MANEJAN LAS ORGANIZACIONES EVITA QUE LOS DEPARTAMENTOS DE TI SE CONCENTREN DE MANERA ADECUADA EN LOS DETALLES IMPORTANTES

Esta información puede utilizarse para detectar problemas de seguridad y pérdidas de datos ocasionados tanto por factores externos como por internos de la organización.

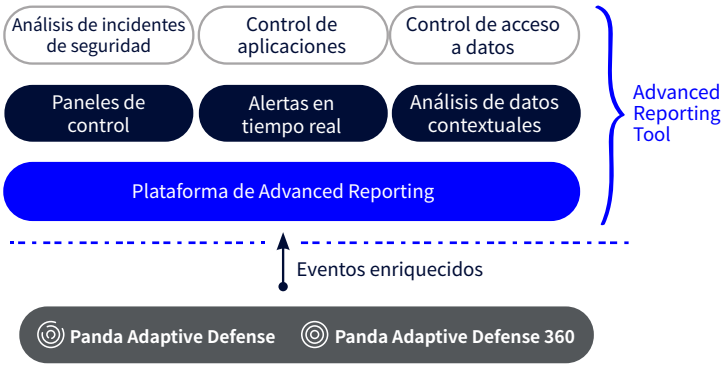
Los departamentos de TI están sobrecargados. Los grandes volúmenes de información manipulada y el surgimiento de malware de última generación hacen que muchos detalles se pasen por alto o no se registren en absoluto, lo que compromete la seguridad de todo el sistema.

LA SOLUCIÓN: PANDA ADAPTIVE DEFENSE 360 Y ADVANCED REPORTING TOOL

La plataforma de Advanced Reporting automatiza el almacenamiento y la correlación de la información generada a través de la ejecución de procesos y su contexto, extraída de endpoints mediante el uso de Panda Adaptive Defense 360.

Esta información permite que Advanced Reporting Tool genere de manera automática inteligencia de seguridad y que provea herramientas que permiten a las organizaciones detectar ataques y comportamientos inusuales, sin importar su origen, así como detectar el uso indebido interno de la red y los sistemas corporativos.

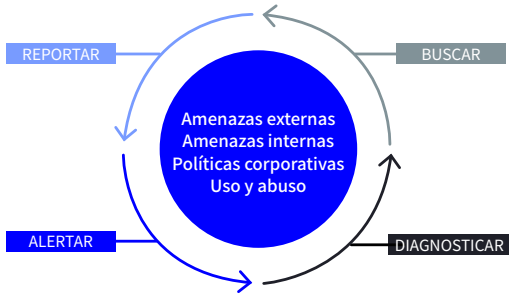
Advanced Reporting Tool brinda a las organizaciones la capacidad de buscar, explorar y analizar grandes volúmenes de datos, lo cual permite insights de TI y de seguridad en la infraestructura, las instalaciones o el mantenimiento.



Advanced Reporting Tool ofrece los datos necesarios para sacar conclusiones fundamentadas sobre la administración corporativa de TI y de seguridad. Estas conclusiones pueden utilizarse luego para definir la base de un plan de acción con los siguientes objetivos:

- **Determinar el origen de las amenazas de seguridad** e implementar medidas de seguridad para impedir futuros ataques.
- Implementar **políticas restrictivas para acceder a información crítica del negocio.**
- Supervisar y controlar **el uso indebido de recursos corporativos** que pueden tener un impacto en el rendimiento de la empresa y los empleados.
- **Corregir el comportamiento de aquellos empleados** que no estén en línea con las políticas de uso de la empresa.

BENEFICIOS CLAVE



1. Encuentre Información Relevante

Maximice la visibilidad de todos los eventos que se producen en los dispositivos y aumente la eficiencia y la productividad del Departamento de TI.

Acceda a los datos históricos para analizar los indicadores corporativos de seguridad y uso de recursos.

Obtenga información detallada para identificar los riesgos de seguridad y el uso indebido interno de la infraestructura de TI.

2. Diagnostique Problemas de Red

Reduzca la cantidad de herramientas y orígenes de datos requeridos para comprender plenamente lo que sucede en los dispositivos y cómo se relaciona esto con la seguridad y el uso de activos corporativos.

Extraiga patrones del uso de recursos y del comportamiento de los usuarios para demostrar su potencial impacto en la empresa. Utilice esta información para implementar políticas de ahorro de costos.

3. Alerte y Esté Alerta

Transforme la detección de anomalías en alertas y reportes en tiempo real.

Genere confianza empresarial marcando las anomalías de seguridad y el uso indebido por parte de los empleados de los recursos de TI en tiempo real.

4. Cree Insights Horizontales y Verticales

Genere reportes detallados configurables para realizar análisis metódicos de la posición de seguridad de su empresa. Identifique el uso indebido de los activos corporativos y descubra anomalías de comportamiento.

Muestre el estado de los indicadores clave de seguridad y realice un seguimiento de su evolución en el tiempo como consecuencia de las medidas correctivas tomadas.

panda
a WatchGuard brand

ANÁLISIS FLEXIBLE ADAPTADO A SUS NECESIDADES

Advanced Reporting Tool (ART) incluye paneles de control con indicadores clave, opciones de búsqueda y alertas predeterminadas para tres áreas específicas:

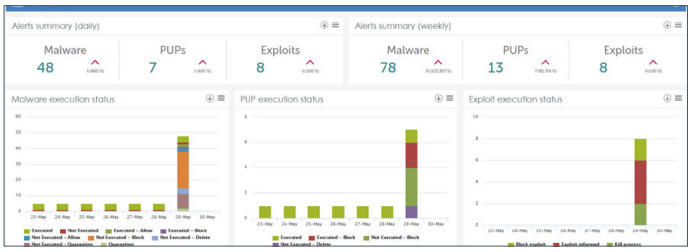
- **Incidentes de seguridad**
- **Acceso a información crítica**
- **Uso de recursos de aplicaciones y de red**

Adapte búsquedas y alertas de información clave a las necesidades de su negocio.

INFORMACIÓN DE INCIDENTES DE SEGURIDAD

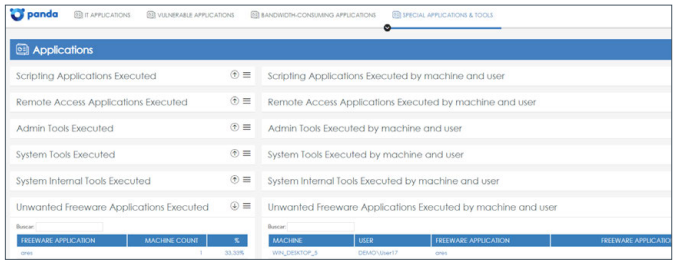
Genere inteligencia de seguridad mediante el proceso y la correlación de eventos generados durante los intentos de intrusión:

- Gráficos de calendario que muestran el malware, el PUP y las vulnerabilidades detectadas en el último año
- Computadoras con más intentos de infección y ejemplares de malware detectados
- Identificación de computadoras con aplicaciones vulnerables
- Estado de ejecución de malware, PUP y vulneraciones



ART incluye widgets para Shadow IT, lo cual ofrece visibilidad de aplicaciones ejecutadas que pueden estar más allá del control del Departamento de TI:

- Las aplicaciones ejecutadas con mayor y menor frecuencia
- Aplicaciones de scripts ejecutadas (PowerShell, Linux shell, Windows cmd, etc.)
- Aplicaciones de acceso remoto ejecutadas (TeamViewer, VNC, etc.)
- Aplicaciones de freeware no deseado ejecutadas (Emule, torrent, etc.)



PATRONES DE USO DE RECURSOS DE LA RED

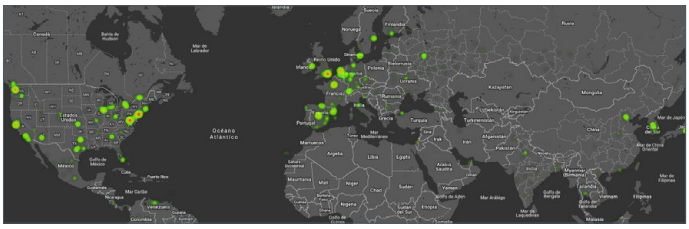
Realice un seguimiento de los patrones de uso de **recursos de TI para definir e implementar políticas de seguridad**:

- Descubra las aplicaciones corporativas y no corporativas que se ejecutan en su red
- Aplicaciones vulnerables que se ejecutan o están instaladas en la red y que pueden provocar infecciones o producir un impacto en el rendimiento de su empresa
- Control de licencias de MS Office usadas o compradas
- Aplicaciones con el más alto consumo de ancho de banda

CONTROL DE ACCESO A DATOS EMPRESARIALES

Muestra **el acceso a archivos de datos confidenciales de la red**:

- Archivos a los que los usuarios de la red acceden y que ejecutan con más frecuencia
- Gráficos de calendario y mapas que muestran los datos enviados en el último año
- Descubra qué usuarios han accedido a computadoras específicas de la red
- Países que reciben el número más alto de conexiones desde su red



ALERTAS EN TIEMPO REAL

Configure alertas basadas en eventos que pueden revelar una vulnerabilidad de seguridad o el incumplimiento de una política corporativa de administración de datos:

- Alertas predeterminadas que indican situaciones de riesgo
- Defina alertas personalizadas basadas en consultas creadas por usuarios
- Siete métodos de entrega (en pantalla y a través de correo electrónico, JSON, Consola de Servicio, Jira, Pushovery y PagerDuty)

Aplicación especial y tablas de herramientas en Advanced Reporting Tool:
http://go.pandasecurity.com/reporting-tool/requirements

Aplicaciones especiales y tablas de herramientas en Advanced Reporting Tool (TI en la Sombra):
http://go.pandasecurity.com/reporting-tool/tools

VENTAS DE EE. UU. +1.800.734.9905 VENTAS INTERNACIONALES +1.206.613.0895 www.watchguard.com/es | pandasecurity.com