Advanced Reporting Tool

Convierte los datos en conclusiones de Seguridad y Gestión IT

EL AUMENTO DEL VOLUMEN DE INFORMACIÓN DE SEGURIDAD MANEJADO IMPIDE A LOS DEPARTAMENTOS DE IT FIJARSE EN LOS DETALLES IMPORTANTES

Esta información es utilizada para detectar problemas e infracciones de seguridad provocados tanto por elementos externos como por los Insiders de la compañía.

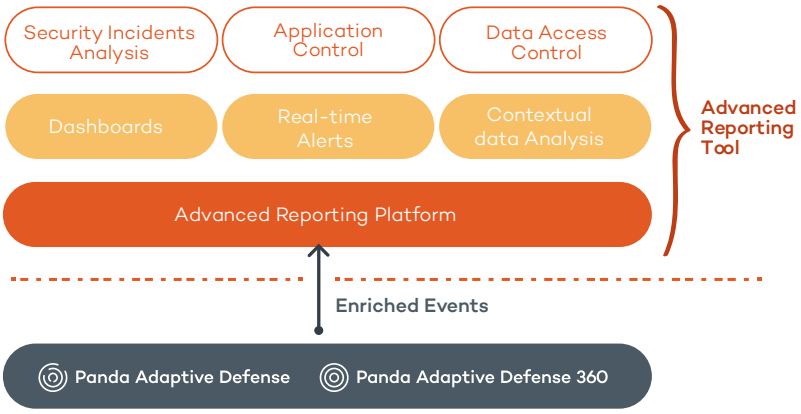
Los departamentos de IT se encuentran desbordados: el alto volumen de información gestionada y la entrada en escena del malware de nueva generación, hacen que **muchos detalles pasen inadvertidos o no sean registrados en absoluto**, comprometiendo la seguridad de todo el sistema.

LA SOLUCIÓN: PANDA ADAPTIVE DEFENSE 360 Y ADVANCED REPORTING TOOL

Advanced Reporting Platform automatiza el almacenamiento y correlación de la información generada por la ejecución de procesos y su contexto, extraída por **Panda Adaptive Defense 360** en el endpoint.

Gracias a esta información, **Advanced Reporting Tool** es capaz de generar inteligencia de seguridad de forma automática, y ofrecer herramientas que permitan tanto **localizar ataques y comportamientos extraños**, sea cual sea su origen, como **revelar el mal uso interno que se hace de los equipos y de la red corporativa.**

Advanced Reporting Tool permite encontrar, explorar y analizar conclusiones operativas de IT & Seguridad sin necesitar infraestructura, instalaciones, mantenimientos o procesamiento de logs.



Advanced Reporting Tool proporciona las herramientas necesarias para obtener conclusiones fiables sobre la seguridad y la gestión IT de la empresa. Estas conclusiones son el inicio de un plan de actuación IT orientado a:

- **Determinar el origen de las amenazas de seguridad** y aplicar mecanismos de resolución y políticas de seguridad que eviten futuros ataques.
- **Implantar políticas más restrictivas de acceso a la información** crítica de la empresa.
- **Controlar el mal uso de los recursos** que pueden afectar al negocio o al desempeño de los empleados.
- **Corregir el comportamiento de los empleados** que no se ajustan a las políticas de uso establecidas por la empresa.

PRINCIPALES BENEFICIOS

1. Encontrar la información relevante

Maximizando la visibilidad de lo que sucede en todos los dispositivos e incrementando la eficiencia del departamento de IT.

Visualizando datos históricos para analizar los indicadores de seguridad y de utilización de los recursos de la empresa.

Profundizando en detalle para localizar fácilmente dónde están los riesgos de seguridad o abusos en el uso de la infraestructura IT.

2. Diagnosticar el problema

Reduciendo el número de herramientas y conocimientos para comprender lo que sucede en los dispositivos y su relación con la seguridad y el uso de activos corporativos.

Extrayendo patrones de uso de los recursos y el comportamiento de los usuarios identificando su impacto en el negocio. Esto puede llevar a la aplicación de políticas que produzcan un ahorro o reducción de costes.

3. Ser alertado y alertar

Transformando las búsquedas de anomalías en alertas en tiempo real e informes.

Generando confianza en la empresa, detectando en el momento las anomalías de seguridad o de mal uso de los recursos corporativos.

4. Informar horizontal y verticalmente

Generando informes de detalle configurable que permiten un análisis metódico del nivel de seguridad de la empresa, del mal uso de los activos y de actividades anómalas de los usuarios.

Mostrando, el estado de indicadores clave de seguridad y su evolución en el tiempo, como consecuencia de las acciones correctivas realizadas.

Advanced Reporting Tool

ANÁLISIS PREDEFINIDOS ADAPTABLES A LAS NECESIDADES DE LAS EMPRESAS

Advanced Reporting Tool (ART) incorpora paneles de control con indicadores clave, búsquedas y alertas predeterminadas en 3 áreas específicas de actuación:

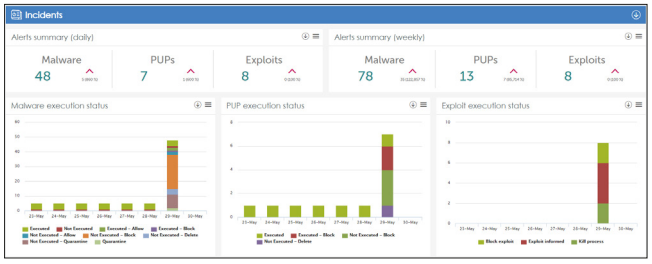
- **Incidencias de seguridad.**
- **Acceso a la información crítica.**
- **Aplicaciones y recursos de red utilizados.**

Las búsquedas y alertas de información clave pueden ser adaptadas a las necesidades específicas de cada empresa.

INFORMACIÓN DE INCIDENCIAS DE SEGURIDAD

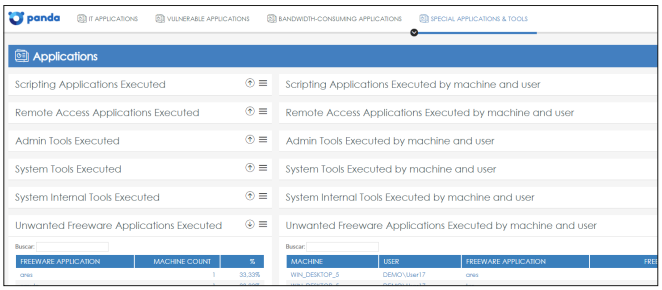
Generación de **inteligencia de seguridad**, procesando y relacionando los eventos generados con intentos de intrusión:

- Calendario anual de Malware, PUP's y Exploits detectados.
- Equipos con más intentos de infección y tipo de malware detectado.
- Equipos que usan aplicaciones con vulnerabilidades conocidas.
- Estado de la ejecución de Malware, PUP's y Exploits.



Las gráficas de **Shadow IT** de Advanced Reporting Tool dan visibilidad sobre aplicaciones ejecutadas que pueden estar fuera del control del departamento de IT:

- Aplicaciones ejecutadas con menos frecuencia.
- Aplicaciones ejecutadas de scripting (powershell, linuxshell, cmd, etc).
- Aplicaciones ejecutadas de acceso remoto (teamviewer, vnc, etc).
- Aplicaciones ejecutadas de software libre de descarga masiva (emule, torrent, etc).



PATRONES DE USO DE RECURSOS Y APLICACIONES

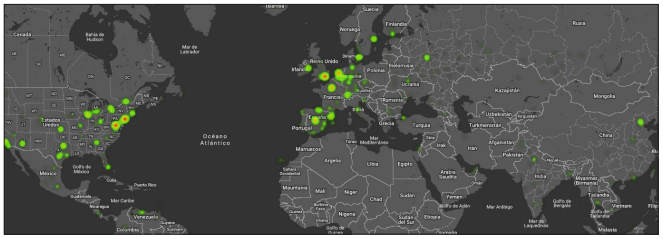
Descubrimiento de **patrones de uso de los recursos informáticos** por parte de los usuarios para el desarrollo y aplicación de políticas de seguridad sobre:

- Software ejecutado, aplicaciones corporativas y no corporativas ejecutadas en el parque informático.
- Control del uso de licencias de MS Office.
- Aplicaciones vulnerables ejecutadas que puedan ser origen de infecciones o impacten en la producción de la empresa.
- Aplicaciones con mayor consumo del ancho de banda.

CONTROL DE ACCESO A LOS DATOS DE LA EMPRESA

Muestra el **acceso a ficheros** con información confidencial y su **circulación en la red**:

- Países de mayor tráfico intercambiado con la red del cliente.
- Ficheros más accedidos por los usuarios y ejecutados con mayor frecuencia.
- Localiza qué usuarios han accedido a determinados equipos de la red.
- Calendario anual y mapa de datos enviados.



ALERTAS EN TIEMPO REAL

Creación de alertas tomando como base **eventos** que pueden identificar una brecha de seguridad o una violación de las políticas de gestión de datos de la empresa:

- Alertas predefinidas que identifican situaciones de peligro como ataques o un uso indebido de recursos de la empresa.
- Creación de alertas personalizadas en base a consultas creadas por el usuario.
- 7 métodos de entrega (en consola, email, JSON, Service Desk, Jira, Pushovery y PagerDuty).

Plataformas Soportadas y Requisitos del Sistema para Advanced Reporting Tool:
http://go.pandasecurity.com/reporting-tool/requisitos

Tablas de aplicaciones especiales y herramientas en Advanced Reporting Tool:
http://go.pandasecurity.com/reporting-tool/herramientas

CERTIFICACIONES Y RECONOCIMIENTOS

Panda Security participa regularmente y obtiene premios en protección y rendimiento de Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs. Panda Adaptive Defense logró la certificación EAL2 + en su evaluación para el estándar Common Criteria.