Advanced Reporting Tool

Transformando Dados em Insights Acionáveis de TI e Segurança

panda
a WatchGuard brand

O AUMENTO DO VOLUME DOS DADOS DE SEGURANÇA PROCESSADOS PELAS ORGANIZAÇÕES IMPEDE QUE OS DEPARTAMENTOS DE TI SE CONCENTREM EM DETALHES IMPORTANTES

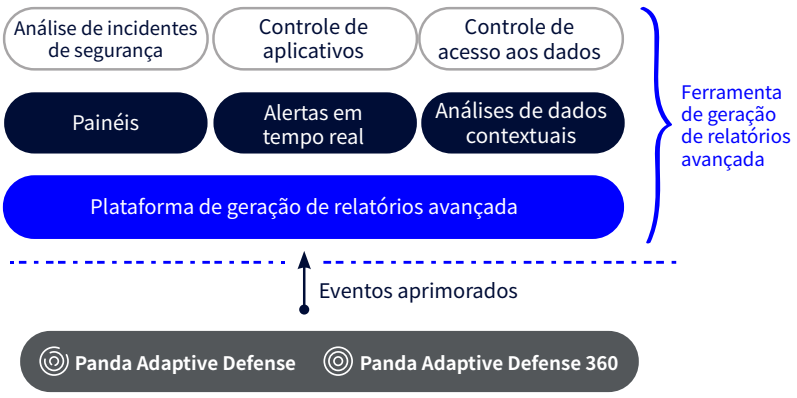
Essas informações podem ser usadas para detectar violações e problemas de segurança provocados por fatores externos e funcionários internos. Os departamentos de TI estão sobrecarregados. Com o grande volume de informações processadas e o surgimento de malwares de última geração, muitos detalhes passem despercebidos ou simplesmente não são registrados, comprometendo a segurança do sistema inteiro.

A SOLUÇÃO: PANDA ADAPTIVE DEFENSE 360 E A FERRAMENTA DE GERAÇÃO DE RELATÓRIOS AVANÇADA

A Plataforma de geração de relatórios avançada automatiza o armazenamento e a correlação de informações geradas pela execução de processos e pelo contexto, que são extraídas dos endpoints pelo Panda Adaptive Defense 360.

Com essas informações, a Ferramenta de geração de relatórios avançada pode gerar automaticamente inteligência de segurança e oferecer recursos que permitem às organizações identificar ataques pontuais e comportamentos incomuns, independentemente da origem, e ainda detectar internamente o uso indevido da rede e dos sistemas corporativos.

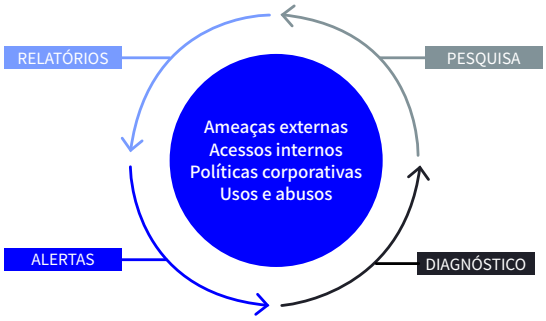
A Ferramenta de geração de relatórios avançada fornece às organizações a capacidade de pesquisar, explorar e analisar grandes volumes de dados, possibilitando insights de TI e segurança em infraestrutura, instalações ou manutenção.



Além disso, a tecnologia disponibiliza os dados necessários para tirar conclusões informadas sobre o gerenciamento corporativo de TI e segurança. Essas conclusões podem ser usadas para definir a base de um plano que inclui estas ações:

- **Determinar a origem das ameaças à segurança** e aplicar medidas de proteção para evitar futuros ataques.
- Implementar **políticas restritivas para o acesso a informações importantes da empresa**.
- Monitorar e controlar o **uso indevido de recursos corporativos** que pode ter impacto no desempenho da empresa e dos funcionários.
- **Corrigir comportamentos de funcionários** que não estejam de acordo com as políticas de uso da empresa.

PRINCIPAIS BENEFÍCIOS



1. Encontre Informações Relevantes

Maximize a visibilidade de todos os eventos que ocorrem nos dispositivos e aumente a eficiência e a produtividade do departamento de TI.

Acesse dados históricos para analisar indicadores corporativos de segurança e o uso de recursos.

Veja informações detalhadas para identificar riscos de segurança e o uso indevido da infraestrutura de TI.

2. Faça Diagnósticos de Problemas da Rede

Reduza o número de ferramentas e fontes de dados necessárias para ter uma visão completa do que acontece nos dispositivos e entender a relação de cada evento com a segurança e o uso de recursos corporativos.

Identifique padrões de uso de recursos e comportamento do usuário para demonstrar o impacto potencial na empresa. Use essas informações para implementar políticas de economia de custos.

3. Receba e Envie Alertas

Transforme a detecção de anomalias em alertas e relatórios em tempo real.

Fortaleça a confiança na empresa sinalizando anomalias de segurança e o uso indevido dos recursos de TI por funcionários em tempo real.

4. Crie Insights Horizontais e Verticais

Gere relatórios detalhados configuráveis para realizar análises metódicas da postura de segurança da sua empresa. Identifique o uso indevido de recursos corporativos e encontre anomalias de comportamento.

Veja o status dos principais indicadores de segurança e acompanhe a evolução desses dados ao longo do tempo para ver os efeitos de ações corretivas.

panda
a WatchGuard brand

ANÁLISE FLEXÍVEL ADAPTADA ÀS SUAS NECESSIDADES

A Ferramenta de geração de relatórios avançada (ART) incorpora painéis com indicadores-chave, opções de pesquisa e alertas padrão para três áreas específicas:

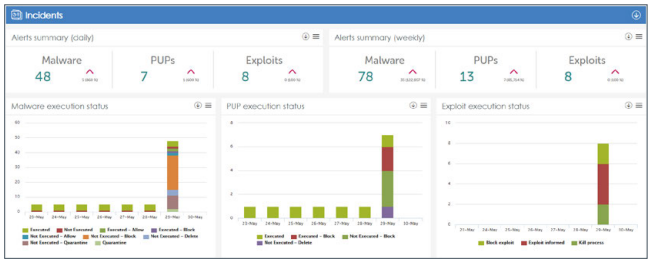
- **Incidentes de segurança**
- **Acesso a informações importantes**
- **Uso de aplicativos e recursos de rede**

Adapte **pesquisas** e **alertas** de informações importantes às necessidades da sua empresa.

INFORMAÇÕES DE INCIDENTES DE SEGURANÇA

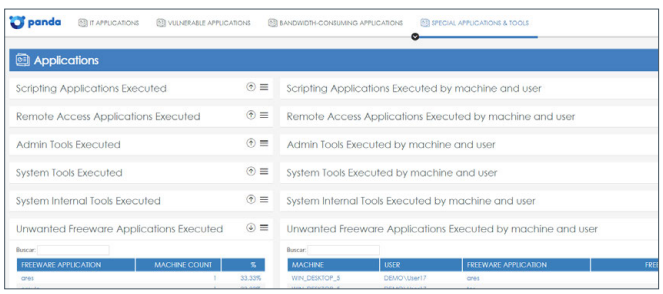
Gere inteligência de segurança processando e correlacionando os eventos ocorridos durante tentativas de invasão:

- Gráficos de calendário que mostram atividades de malware, programas potencialmente indesejados (PUPs) e explorações detectadas no último ano
- Computadores com a maior incidência de tentativas de infecção e amostras de malware detectadas
- Computadores com aplicativos vulneráveis
- Status de execução de malware, programas potencialmente indesejados (PUPs) e explorações



A ART inclui widgets para Shadow IT, oferecendo visibilidade dos aplicativos executados que podem estar além do controle do departamento de TI:

- Aplicativos com maior e menor frequência de execução
- Aplicativos de script executados (PowerShell, shell do Linux, cmd do Windows etc.)
- Aplicativos de acesso remoto executados (TeamViewer, VNC, etc.)
- Aplicativos freeware indesejados executados (Emule, Torrent, etc.)



PADRÕES DE USO DOS RECURSOS DE REDE

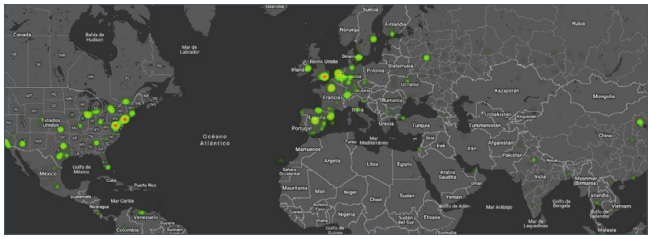
Acompanhe os padrões de **uso dos recursos de TI para definir e aplicar políticas de segurança:**

- Encontre os aplicativos corporativos e não corporativos em execução na sua rede
- Identifique aplicativos vulneráveis em execução ou instalados na rede que podem levar à infecção ou afetar o desempenho da empresa
- Faça o controle de licença do MS Office (uso x compra)
- Verifique os aplicativos com maior consumo de largura de banda

CONTROLE DO ACESSO AOS DADOS DA EMPRESA

Monitore o **acesso a arquivos de dados confidenciais na rede:**

- Identifique os arquivos mais acessados e executados pelos usuários da rede
- Veja gráficos e mapas de calendário com os dados enviados no último ano
- Descubra quais usuários acessaram computadores específicos na rede
- Saiba que países recebem o maior número de conexões da sua rede



ALERTAS EM TEMPO REAL

Configure alertas com base em eventos que podem revelar uma violação de segurança ou o descumprimento de uma política de gerenciamento de dados corporativos:

- Compartilhe alertas padrão indicando situações de risco
- Defina alertas personalizados com base em consultas criadas pelo usuário
- Acesse sete métodos de entrega (na tela e via e-mail, JSON, Service Desk, Jira, Pushovery e PagerDuty)

Aplicativo especial e tabelas de ferramentas da Advanced Reporting Tool:
http://go.pandasecurity.com/reporting-tool/requirements

Aplicativos e tabelas de recursos especiais na Ferramenta de geração de relatórios avançada - Shadow IT:
http://go.pandasecurity.com/reporting-tool/tools

WatchGuard

VENDAS NOS EUA 1.800.734.9905 VENDAS INTERNACIONAIS +1.206.613.0895 www.watchguard.com/br | pandasecurity.com