# Advanced Reporting Tool

## Автоматизированная расширенная безопасность
## Положите конец кибер-угрозам

## РОСТ ОБЪЕМА ОБРАБАТЫВАЕМЫХ ДАННЫХ О БЕЗОПАСНОСТИ НЕ ДАЕТ ИТ-ОТДЕЛАМ СФОКУСИРОВАТЬСЯ НА ВАЖНОЙ ИНФОРМАЦИИ

Эта информация может использоваться для выявления проблем безопасности, вызванных внешними факторами и/или инсайдерами внутри компании.

**ИТ-отделы не справляются**: большие объемы обрабатываемых данных и появление угроз нового поколения приводит к тому, что многие моменты **упускаются из виду или вообще не фиксируются** - это снижает безопасность всей системы.

## РЕШЕНИЕ: PANDA ADAPTIVE DEFENSE 360 И ADVANCED REPORTING TOOL

Платформа **Advanced Reporting Tool** автоматизирует хранение и корреляцию информации, связанной с выполнением процессов и их содержимым, которая собирается с компьютеров решениями Panda Adaptive Defense [360].

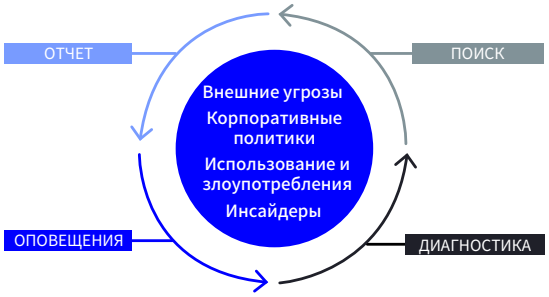
Эта информация позволяет модулю **Advanced Reporting Tool** автоматически осуществлять глубокий анализ данных по безопасности и предоставлять предприятиям инструменты, позволяющие **выявлять атаки и подозрительное поведение** процессов вне зависимости от их происхождения и обнаруживать внутренние злоупотребления корпоративными системами и сетью.

Решение **Advanced Reporting Tool** предлагает компаниям возможности поиска, исследования и анализа, предоставляя полное понимание ИТ и безопасности без дополнительных инвестиций в инфраструктуру, внедрение или обслуживание.


**Advanced Reporting Tool** предоставляет необходимые данные для составления обоснованных экспертных заключений по вопросам управления корпоративной ИТ-безопасностью. Такие заключения могут использоваться для составления плана действий с целью:

- **Обнаружения источника угроз безопасности** и применения мер безопасности для предотвращения будущих атак.
- Внедрения **более ограничительных политик доступа** к конфиденциальной корпоративной информации.
- Мониторинга и контроля **злоупотребления корпоративными ресурсами**, которые могут негативно сказаться на работе предприятия и производительности сотрудников.
- **Корректировки поведения сотрудников**, которые не соблюдают установленные политики безопасности.

## КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА




### 1. Поиск требуемой информации

Максимальная видимость всего, что происходит на каждом устройстве, рост производительности и эффективности работы ИТ-отдела.

Доступ к журналам событий для анализа безопасности корпоративных ресурсов и индикаторов их использования.

Подробная информацию для выявления рисков безопасности и инсайдерского злоупотребления ИТ-инфраструктурой.

### 2. Диагностика сетевых инцидентов

Сокращение количества требуемых инструментов и источников данных для полного понимания всего происходящего на устройствах и их связью с безопасностью и использованием корпоративных ресурсов.

Получение моделей использования ресурсов и поведения пользователей для демонстрации их возможного ущерба для предприятия. Использование этой информации для внедрения ресурсосберегающих политик.

### 3. Предупреждения и оповещения

Переход от обнаружения аномалий к оповещениям и отчетам в реальном времени.

Укрепление конфиденциальности в компании за счет выявлений в реальном времени аномалий безопасности и злоупотребления при использовании ИТ-ресурсов.

### 4. Анализ ситуации с разных сторон

Настраиваемые подробные отчеты для методического анализа статуса безопасности компании, выявления злоупотреблений ИТ-активами предприятия и поиска аномального поведения.

Показ статуса ключевых индикаторов безопасности и мониторинг их изменения после применения корректирующих действий.

panda
a WatchGuard brand

## ГИБКИЙ АНАЛИЗ, АДАПТИРОВАННЫЙ К ПОТРЕБНОСТЯМ ВАШЕЙ КОМПАНИИ

**Advanced Reporting Tool** содержит панели управления с ключевыми индикаторами, опциями поиска и оповещениями по трем направлениям:

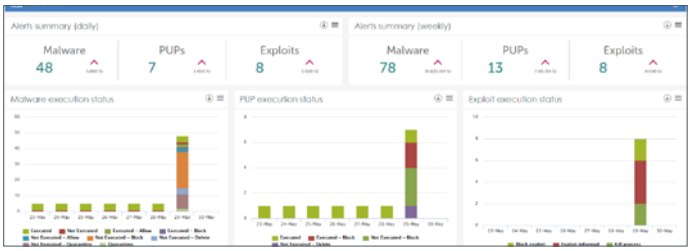
- **Инциденты безопасности**
- **Доступ к критически важной информации**
- **Использование приложений и сетевых ресурсов**

Адаптируйте фильтры и оповещения по ключевым индикаторам под потребности Вашей компании

## ДАННЫЕ ОБ ИНЦИДЕНТАХ БЕЗОПАСНОСТИ

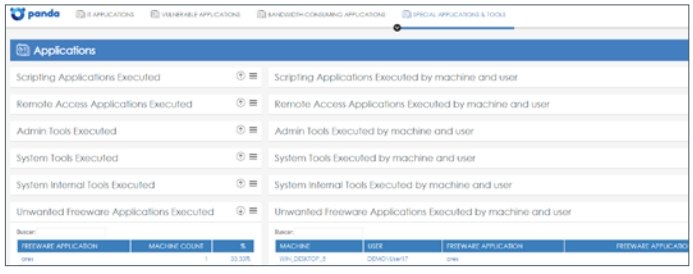
**Получайте полную информацию о безопасности**, обрабатывая и сопоставляя события, происходящие при попытках вторжения:

- Графики обнаруженных вредоносных программ, ПНП и эксплойтов за последний год
- Компьютеры с максимальным числом попыток вторжений и обнаруженных образцов угроз
- Выявление ПК с уязвимыми приложениями
- Статус выполнения вредоносного ПО, ПНП и эксплойтов




Advanced Reporting Tool содержит виджеты для **теневого ИТ**, позволяя видеть запущенные приложения, которые находятся вне контроля со стороны ИТ-отдела:

- Часто и редко запускаемые приложения
- Запуск скриптов (powershell, linux shell, windows cmd и т.д.)
- Запуск приложений удаленного доступа (teamviewer, vnc и пр.)
- Запуск нежелательных бесплатных приложений (emule, torrent...)




## МОДЕЛИ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ СЕТИ

Узнайте **модели использования ИТ-ресурсов в Вашей компании для внедрения политики снижения затрат**:

- Корпоративные и личные приложения, запущенные в сети
- Уязвимые приложения, запущенные или установленные в сети, которые могут привести к инфекции, иметь негативное влияние на работу предприятия и т.д.
- Используемые лицензии MS Office из числа приобретенных
- Приложения, больше всего потребляющие пропускную способность канала связи

## КОНТРОЛЬ ДОСТУПА К КОРПОРАТИВНЫМ ДАННЫМ

Показывает **доступ к файлам в сети с конфиденциальными данными:**

- Файлы с наибольшим доступом и запуском пользователями сети
- Графики и карты, показывающие данные, отправленные за последний год
- Какие пользователи подключались к каким ПК в сети
- Страны, к которым было максимальное число подключений из Вашей сети

## ОПОВЕЩЕНИЯ В РЕАЛЬНОМ ВРЕМЕНИ

**Настройте оповещения о событиях**, которые помогут выявить нарушения безопасности или политики управления корпоративными данными:

- Оповещения по умолчанию о рискованных ситуациях
- Настройте оповещения на основе запросов пользователей
- Семь способов доставки (на экране, по электроннной почте, JSON, Service Desk, Jira, Pushovery и PagerDuty)

**Поддеживаемые платформы и системные требования для ADVANCED REPORTING TOOL:**
http://go.pandasecurity.com/reporting-tool/requirements

**Таблицы специальных приложений и утилит в ADVANCED REPORTING TOOL - SHADOW IT:**
http://go.pandasecurity.com/reporting-tool/tools

WatchGuard

В МИРЕ +1 (206) 613-08-95 В РОССИИ И СНГ +7 (495) 105-94-51 watchguard.com | pandasecurity.com | cloudav.ru