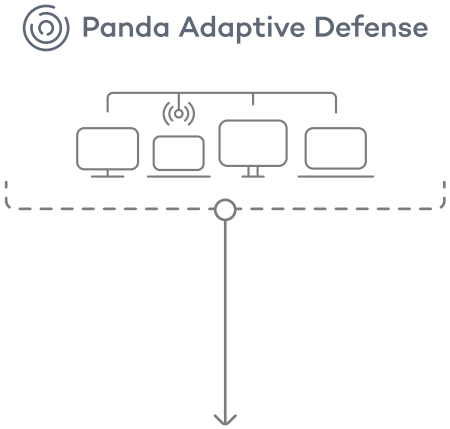
SIEM Feeder

Интеграция с корпоративными SIEM-системами для добавления данных и контекста всего, что запущено в Вашей ИТ- сети

Новый источник информации: Программы пользователя.

SIEM-решения (System Information and Event Management) стали необходимостью для управления безопасностью крупных и средних IT-инфраструктур. Их возможности собирать и учитывать статус IT-систем позволяют предприятиям превратить огромные объемы данных в полезную информацию для принятия решений.

Интегрируйте новый источник важной информации в Вашу SIEM-систему по сбору и анализу информации о безопасности: все процессы и программы, запущенные на Ваших устройствах, непрерывно контролируются Adaptive Defense.



Новый статус безопасности

IT-отделы требуют высокого уровня видимости и контроля, чтобы иметь возможность предвидеть проблемы безопасности со стороны вредоносных программ нового поколения.

Panda Adaptive Defense помогает фильтровать огромные объемы данных, обрабатываемых SIEM-системами, и фокусироваться на том, что реально беспокоит:

- Какие новые программы запущены и еще не классифицированы как вредоносные или невредоносные?
- Как эти программы попали в сеть?
- Какие подозрительные действия они выполнили на устройствах пользователя (редактирование реестра, установка драйверов и т.д.)?
- Какое используется легальное ПО с известными и используемыми уязвимостями?
- Какие процессы обращаются к документам пользователей и отправляют информацию во вне?
- Как используется сеть каждым процессом, запущенным в IT-сети?

Простая интеграция и эксплуатация

Adaptive Defense идеально интегрируется с существующими корпоративными SIEM-решениями без дополнительных внедрений на устройствах пользователей. Контролируемые события безопасно отправляются с использованием форматов LEEF/CEF, совместимых с большинством SIEM-систем на рынке, прямо в эти системы или через плагины.

Поддерживаемые платформы и системные требования для SIEM Feeder:
http://go.pandasecurity.com/siem-feeder/requirements

Модуль доступен для:

- Panda Adaptive Defense
- Panda Adaptive Defense 360

Совместим с:

ALIEN VAULT · ArcSight An HP Company · QRadar · bitacora · lookwise

Также совместим с форматами LEEF и CEF