

Система обнаружения сетевых атак нового поколения Jet Pluton



Jet Pluton – решение для обнаружения скрытых угроз в сетевом трафике, позволяющее выявить большинство признаков атак. Система анализирует сетевые пакеты как сигнатурными методами, так и с помощью технологий машинного обучения, предоставляя глубокую аналитику для расследования подозрительного поведения в сети.



Разработано компанией «Инфосистемы Джет»

Решаемые задачи



Предоставление актуальных данных по инвентаризации оборудования и ПО



Оперативное обнаружение сетевых угроз



Ретроспективный анализ данных



Проверка правил настройки сетевого оборудования

Механизмы обнаружения



Контроль сетевого трафика
Выявление известной вредоносной и аномальной активности в сети



Машинное обучение
Математические алгоритмы для выявления аномалий



Пассивное сканирование сети
Построение карты сети, определение подозрительных устройств



Синхронизация с существующими базами знаний
Определение известных зловредных IP, DNS, кодов вирусов и опасных email

Обработка результатов



Визуализация и отчеты
События безопасности, графики статистики, отчеты



Расширенный набор данных
События, логи, трафик и данные устройств



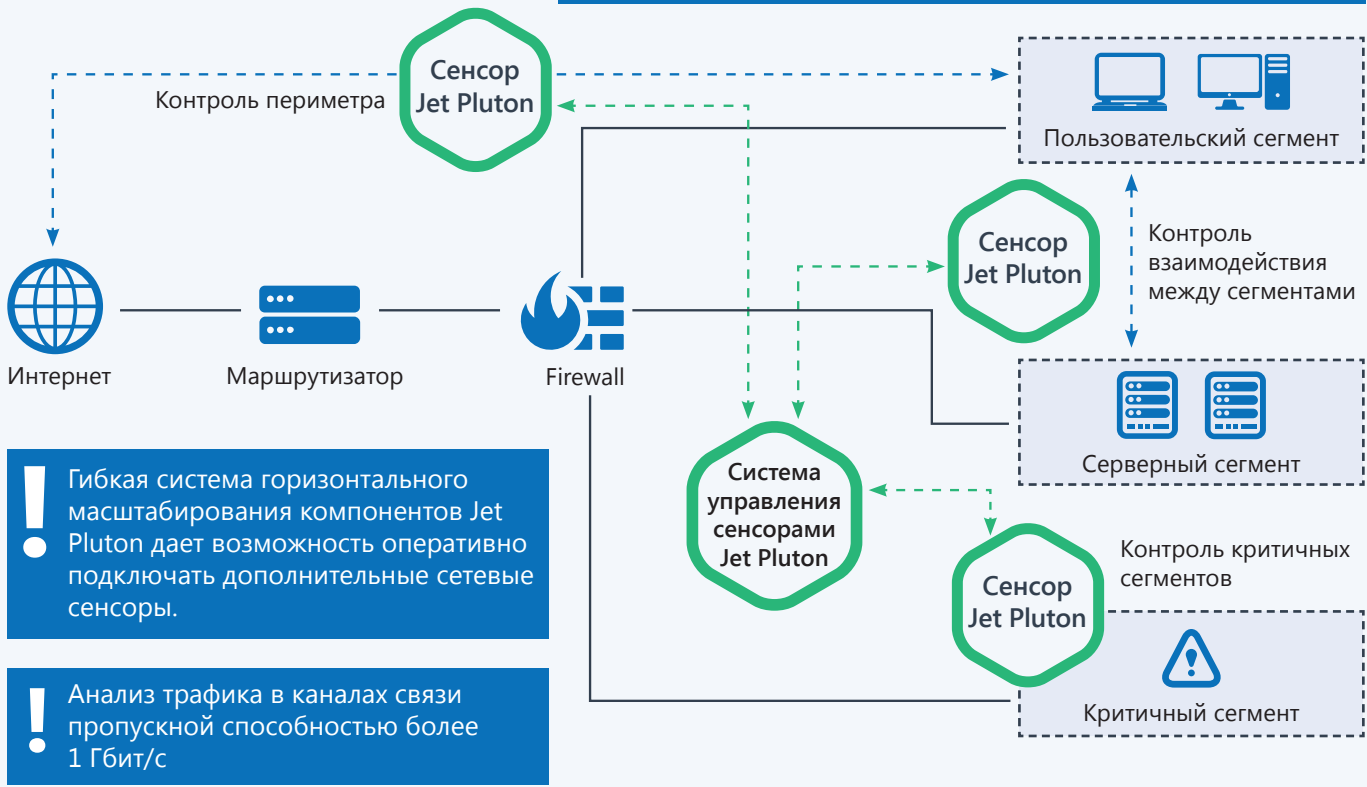
Интеграция
Передача данных для расследования в SIEM, сбор данных со сторонних источников, интеграция с межсетевыми экранами



Ведение собственной базы правил анализа трафика
сигнатурные правила, правила на основе мат моделей, комбинированные

Как работает Jet Pluton

! Отказоустойчивая архитектура Jet Pluton позволяет в случае отказа одного из компонентов автоматически перенаправлять поток событий на резервные компоненты



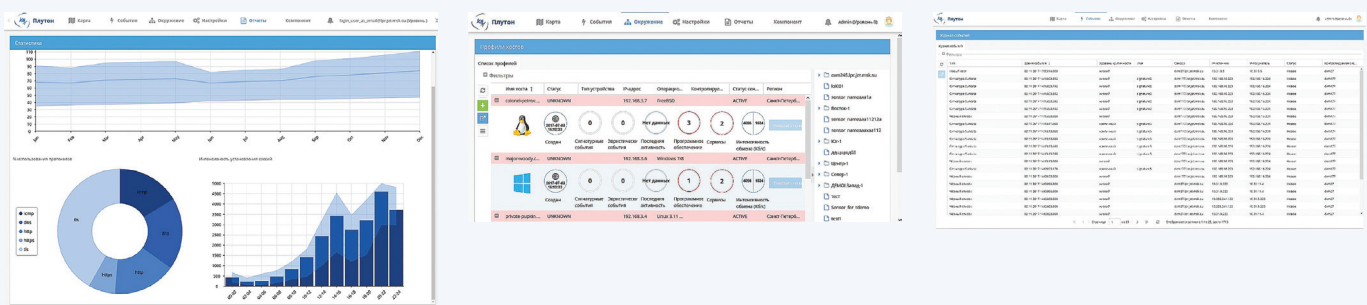
! Гибкая система горизонтального масштабирования компонентов Jet Pluton дает возможность оперативно подключать дополнительные сетевые сенсоры.

! Анализ трафика в каналах связи пропускной способностью более 1 Гбит/с

Свидетельства и сертификаты Jet Pluton

- ✓ Свидетельство о государственной регистрации программы для ЭВМ № 2017610847 от 18 января 2017 года
- ✓ Сертификат Минобороны России № 3861 подтверждающий соответствие требованиям Приказа МО РФ, в том числе:
 - по второму классу защиты систем обнаружения вторжений уровня сети;
 - по второму уровню контроля отсутствия недеklarированных возможностей (НДВ-2);
 - по соответствию реальных и декларируемых в документации функциональных возможностей (РДВ).
- ✓ Jet Pluton включен в единый реестр российских программ для электронных вычислительных машин и баз данных (реестр российского ПО). Приказ Минкомсвязи России от 28.04.2017 № 212

Гибкая настройка и расширенная аналитика



127015, Россия, Москва, ул. Большая Новодмитровская, 14с1
Бизнес-Центр «Новодмитровский»

Для получения дополнительной информации вы можете обращаться к Анне Олейниковой, менеджеру по продвижению продукта Jet Pluton компании «Инфосистемы Джет»

+7 495 411-76-01 | pluton@jet.su | www.jet.su

