positive technologies

PT Threat Intelligence Feeds

Уникальные потоки данных о киберугрозах

PT Threat Intelligence Feeds (PT Feeds) — потоки данных (фиды) об индикаторах компрометации для информирования команд ИБ об актуальных киберугрозах. Они обогащают средства мониторинга и защиты информации и повышают эффективность их работы

> 2 МЛН
новых анализируемых объектов ежемесячно

2000+
семейств ВПО

200+
хакерских группировок

Преимущества

Проверенные данные
Индикаторы компрометации, полученные в ходе расследований и изучения APT-группировок, а также обезличенная телеметрия с инсталляций продуктов Positive Technologies

Расширенный контекст
Позволяет лучше понять потенциальную угрозу, разработать план реагирования и повысить скорость реагирования на инциденты

Готовые наборы
Данные собраны в группы в зависимости от потребностей в выявлении различных видов угроз

Интеграция с продуктами Positive Technologies
Подключение фидов к MaxPatrol SIEM и PT NAD

Интеграция с продуктами других вендоров
PT Feeds поддерживает разные форматы и средства защиты информации, число которых постоянно растет

Онлайн-портал PT IoC Portal
Позволяет проводить бесплатную проверку файлов и индикаторов компрометации

Ключевые характеристики PT Threat Intelligence Feeds

Состав фидов

- Индикаторы компрометации
- Легитимные объекты и сервисы, которые могут быть использованы для атак
- Списки доверенных объектов, которые уменьшают количество ложноположительных срабатываний

Типы индикаторов

- IP-адреса
- URL
- Домены
- Хеш-суммы файлов

Интеграция с другими СЗИ

- SIEM
- TI-платформы
- IRP (SOAR)
- EDR
- ESG
- NTA
- NGFW
- WAF

Основные источники данных

- Обезличенная телеметрия с инсталляций PT NAD
- Результаты анализа хакерских группировок и их инструментов экспертами PT ESC
- Результаты расследований инцидентов ИБ PT ESC
- Данные из открытых источников (OSINT)
- Данные «ФинЦЕРТ»

Комплексное решение для обеспечения полной видимости актуальных киберугроз и защиты от них

PT Threat Intelligence — решение, которое объединяет в себе уникальные сведения об актуальных киберугрозах и платформу для накопления знаний о них и управления ими. Это решение позволит использовать данные о злоумышленниках:

- для раннего выявления угроз и их превентивной блокировки;
- принятия обоснованных решений по реагированию на атаки;
- усиления средств защиты.

«Пилот» PT Threat Analyzer

«Пилот» PT Threat Intelligence Feeds

Получите доступ к PT IoC Portal