**Защита от APT-атак**

Для полноценного детектирования и противодействия направленным атакам необходимо использовать одновременно пять основных методов и технологий защиты:

1. Применение технологий анализа сетевого трафика для построения модели сетевого взаимодействия. Дальнейший поиск отклонений и аномальных ситуаций. Данный анализ происходит в реальном времени с блокировкой подозрительного трафика для предотвращения атак.
2. Сбор данных о сетевом трафике без активного противодействия для поиска аномалий и проведения анализа на большом объеме данных. Применяется только для детектирования атак и последующего расследования происшествий.
3. Применение технологии «песочниц» для анализа поведения приложений, которые скачиваются пользователями или проходят в сетевом трафике.
4. Поведенческий анализ пользовательских компьютеров — перехват системных функций и обращений к ресурсам компьютеров и поиск аномалий в функционировании пользовательских приложений и операционной системы. Включает в себя проактивные механизмы защиты — блокирует подозрительные операции и изолирует потенциально вредоносные приложения.
5. Сбор данных об активности приложений и операционной системы на рабочих станциях без активного противодействия для дальнейшей работы с большим объемом данных.

Стоит отметить, что целенаправленные атаки распределены по времени, используют разные векторы атак и точки вторжения, и чем больше используется различных средств и методов защиты, тем выше шанс своевременно обнаружить и предотвратить атаку.

**Примеры защитных средств:**

* системы класса NG FW (Check Point, Stonesoft, HP Tipping Point);
* система обнаружения потенциально опасных файлов (песочница) (Check Point, McAfee, FireEye);
* специализированные средства защиты web-приложений (WAF) (Imperva SecureSphere WAF, Radware AppWall, Fortinet Fortiweb);
* системы обнаружения аномалий в сетевом трафике (StealthWatch, RSA NetWitness, Solera Networks);
* системы анализа и оптимизации настроек МЭ инфраструктуры (Algosec, Tufin, RedSeal, SkyBox);
* аудит безопасности кода (HP Fortify, Digital Security ERPScan CheckCode, IBM AppScan Source);
* защита от мошенничества при доступе к системам интернет-банкинга (Versafe);
* цифровое расследование инцидентов ИБ (Forensic Analysis and Incident Response) (AccessData);
* система защиты от DDoS (железо — Radware DefensePRO, ARBOR PRAVAIL, Check Point DDoS Protector; сервис — Kaspersky DDoS Prevention, QRATOR HLL).