ИНФ ЗАЩИТА
ITPROTECT.RU

# Электронные каналы как основной источник угроз информационной безопасности

# О важности регулярной оценки защищенности

# Анализ защищенности

Процесс проверки инфраструктуры организации на наличие возможных уязвимостей и оценке общего уровня безопасности

Инструментарий: - сканеры защищенности,

- тестирование на проникновение

Регламент: - в лучшем случае 1 раз в квартал

# Breach and Attack Simulation

# BAS - платформа симуляции взломов и кибер атак

**позволяет симулировать атаки и автоматизировать процесс оценки защищенности инфраструктуры**

***предназначено для автоматического тестирования СЗИ, сотрудников и процессы ИБ, на кибер-устойчивость и способность противостоять реальным атакам***

# Принцип действия

BAS - оценивает уровень защищённости , запуская атаки близкие к реальным, но гарантировано без риска реального взлома

Имитирует действия «виртуального хакера», используя машинное обучение

Решения используют вендорские «Hacker’s Playbook» содержащие методы взломов и сценарии атак. Их перечень постоянно обновляется и пополняется.

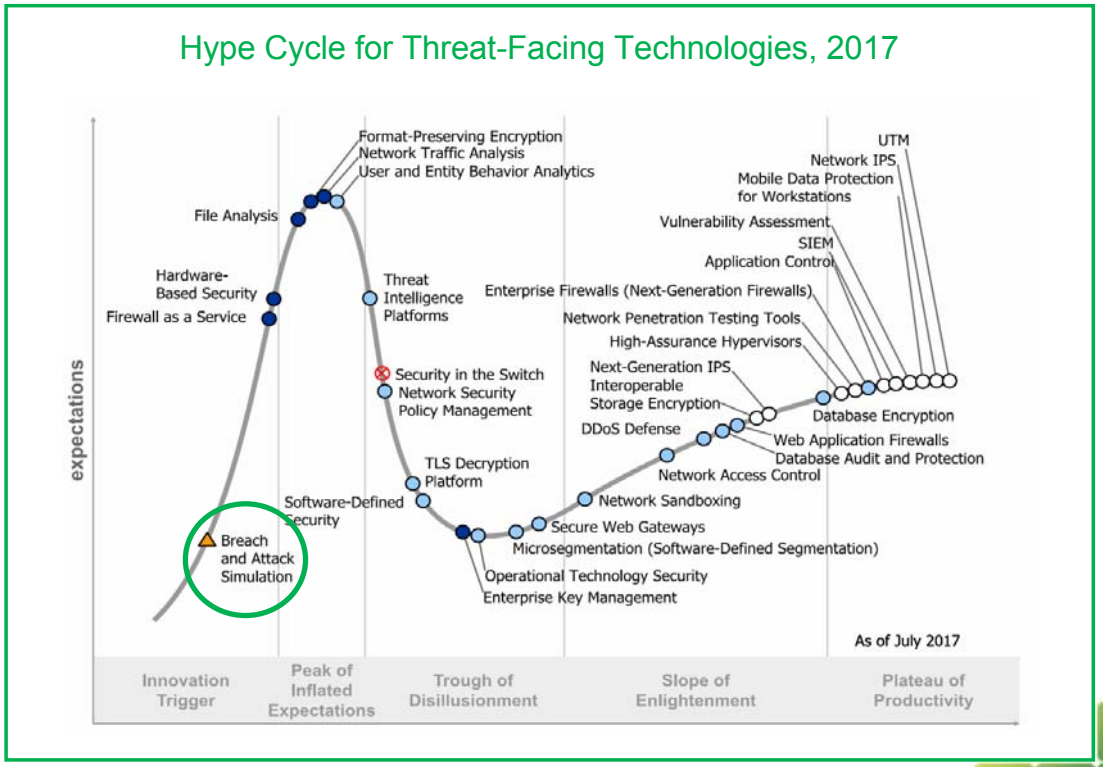
# Новый тип решений

Исследовательская компания **Gartner** в середине 2017 года выделяет новый класс решений: **Breach and Attack Simulation**

«Если у Вас есть возможность выполнить задачу нажатием кнопки, зачем вам для этого человек?»

***BAS и Red Team убьют пен-тесты***

*Августо Баррос, Gartner,*
*14 февраля 2018 г.*



# Возможности

- Анализ защищенности по всем известным уязвимостям
- Запускает реальные атаки на реальные активы, но без риска реального взлома
- Оценка эффективности функционирования средств защиты и процессов
- Оценка динамики уровня защищенности
- Проведение кибер учений и оценки осведомленности сотрудников
- Отчеты с рекомендациями по устранению

# Вектора атак


**Внешний периметр:** доступ по e-mail, через Интернет, защищенность web ресурсов

**Внутренняя сеть:** доступ на endpoint, движение внутри сети, утечки данных

**Процессы и люди:** осведомленность сотрудников, оценка процессов

# Ценность

- Комбинация методов и векторов, от периметра до внутренних ресурсов
- Результат – реально эмулированый сценарий атаки, а не вероятностное предположение
- Возможность получать непрерывную информацию об уровне безопасности
- Эффективное тестирование новых СЗИ и/или изменённых конфигураций

# Преимущества

- Непрерывный и независимый анализ уровня защищенности
- Полностью автоматизированный процесс
- Анализ в режиме 24/7
- Демонстрирует моментальную пользу
- Кибер-устойчивость. Готовность к будущим атакам
- Не влияет на бизнес-процессы
- Не требует пентестеров для эксплуатации

# Спасибо за внимание

**Сергей Смирнов**

s.smirnov@itprotect.ru