Cymulate
Breach & Attack Simulation

Непрерывная симуляция атак и взломов

Илья Осадчий, Тайгер Оптикс

О компании Cymulate

- 2016 – компания основана в в Израиле
- 2018 – Gartner Cool Vendor
- 2018 – Первые два заказчика в РФ
- 2019, январь – Заказчики из списка Fortune 2000, на всех континентах, в т.ч. Топ-10 банк РФ
- 2019, май – Приватное облаков в РФ
- 2019, июнь – Единственное решение, которое симулирует полную цепочку APT-атаки

Gartner Cool Vendor 2018

Награды

Инвесторы

SGE SUSQUEHANNA GROWTH EQUITY, LLC

DELL Technologies CAPITAL

vertex VENTURES

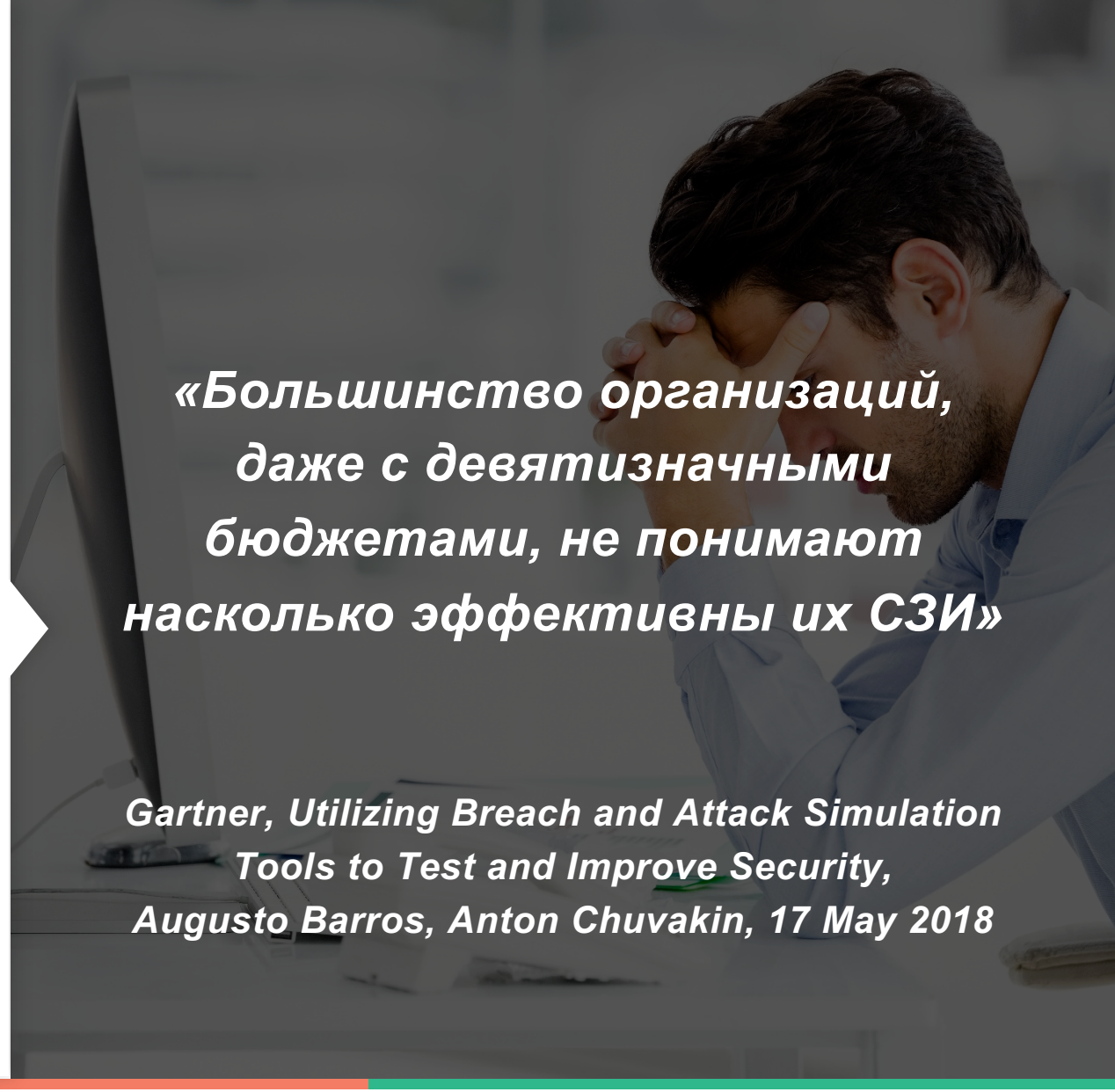
Gartner, Cool Vendors in Application and Data Security, Ayal Tirosh, 4 May 2018. The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Мотивация создания Cymulate

Cymulate
Breach & Attack Simulation

Почему CISO плохо спит ночью?

- Насколько моя компания **реально** защищена?
- Где я больше всего уязвим? Что не работает?
- Защищены ли мы от новой 0-day атаки?
- Справятся ли мои сотрудники при APT-атаке?
- Тратить ли бюджет на новое СЗИ?
- Что реально происходит в новой «дочке»?



«Большинство организаций, даже с девятизначными бюджетами, не понимают насколько эффективны их СЗИ»

Gartner, Utilizing Breach and Attack Simulation Tools to Test and Improve Security, Augusto Barros, Anton Chuvakin, 17 May 2018

Cymulate
Breach & Attack Simulation

Частичные ответы

- Пентест
- Редтим

Разовые проверки конкретных сценариев

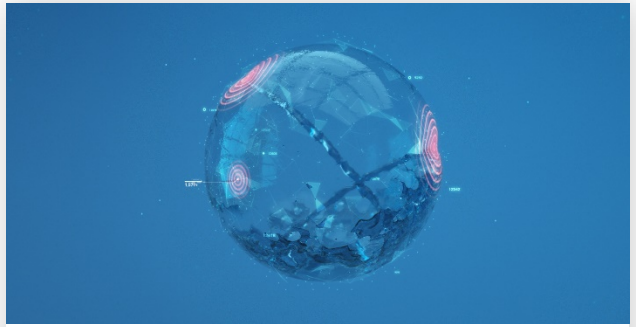
Ручная работа. Стоят немало

К моменту получения отчета все уже изменилось

Все равно что планировать ваш следующий отпуск, проверяя прошлогодний прогноз погоды

Cymulate
Breach & Attack Simulation

Cymulate. Комплексное решение

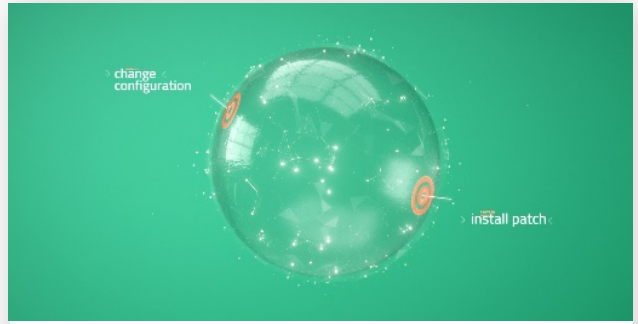


01 **Симулируйте**

атаки по всей длине цепочки Kill Chain

02 **Оценивайте**

результаты и выявленные дыры



03 **Исправляйте**

на основании подробных отчетов

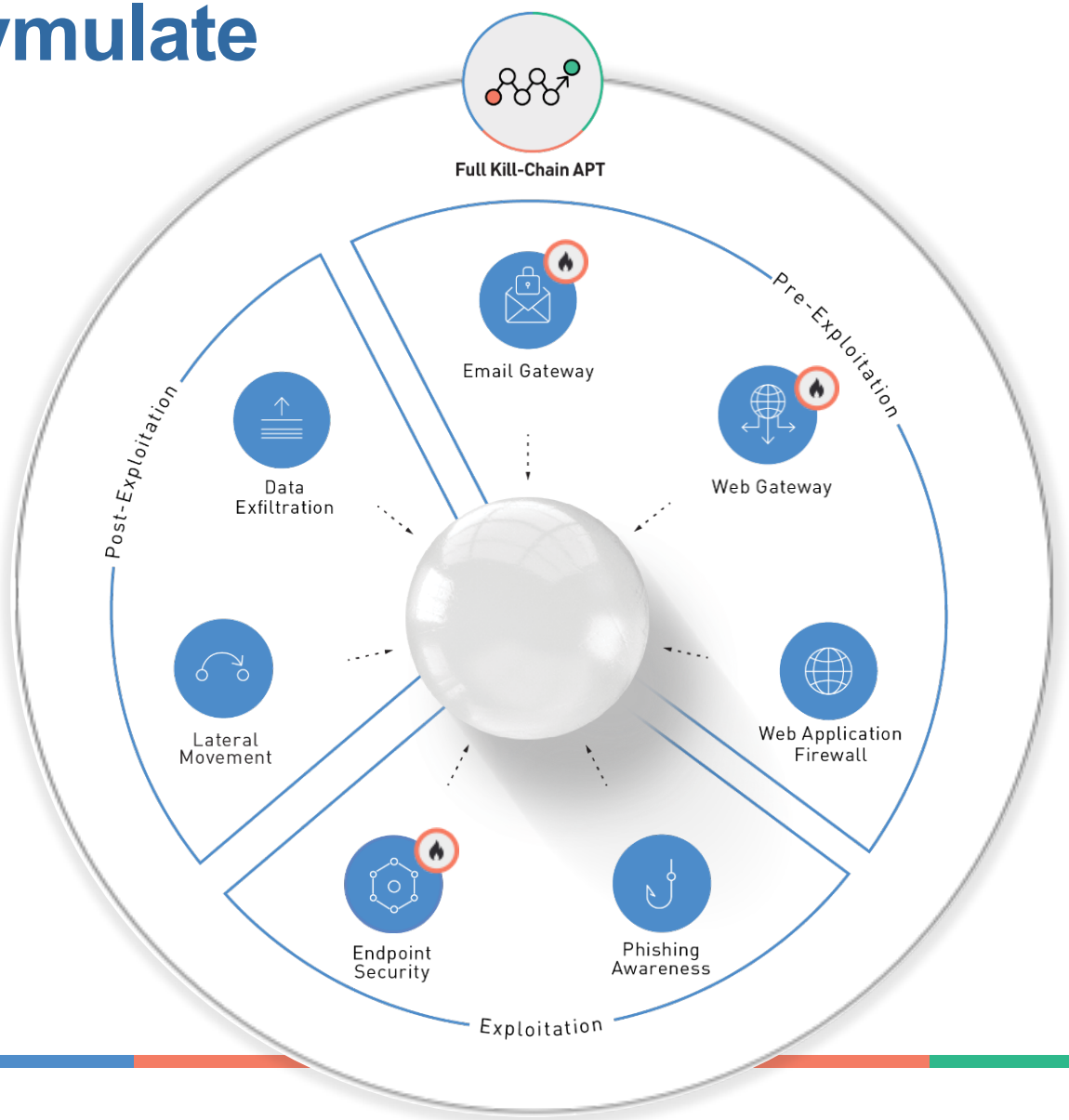
Повторяйте. Еженедельно, ежедневно или в любое время 24x7x365

Cymulate
Breach & Attack Simulation

Как работает Cymulate?

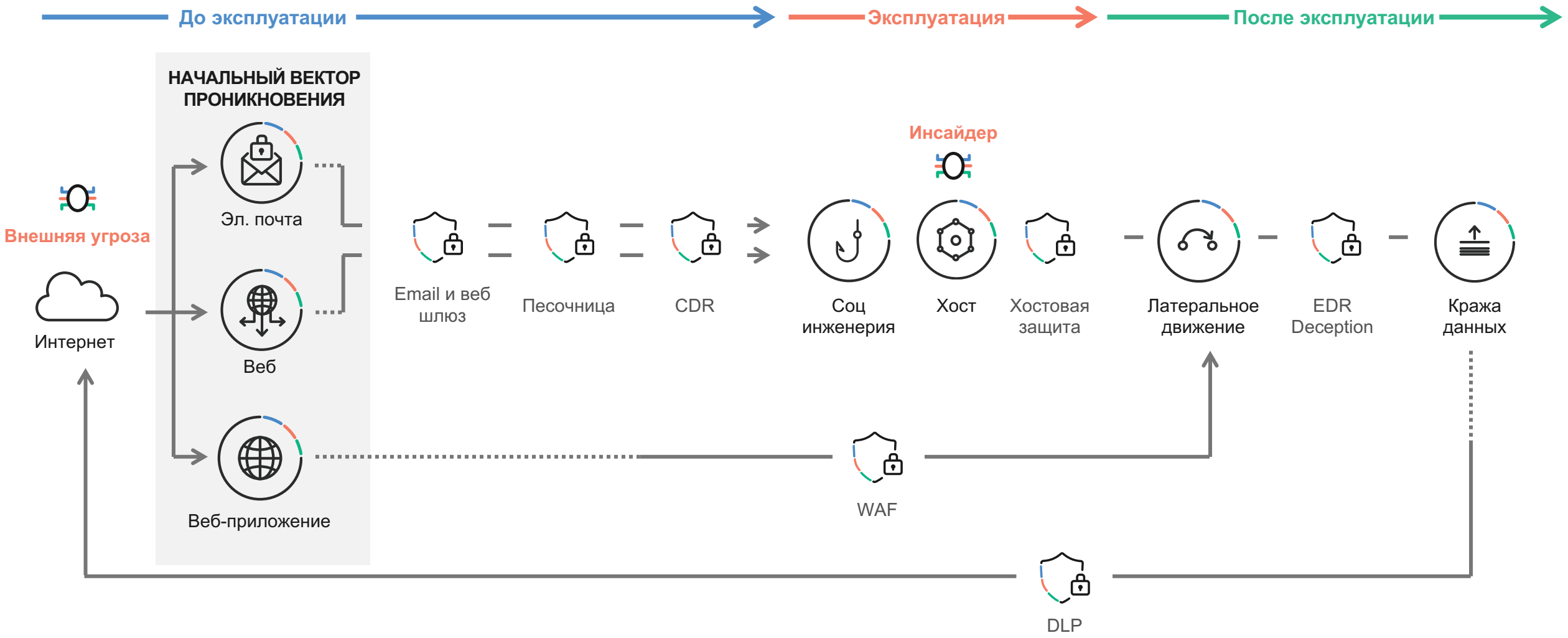
Cymulate
Breach & Attack Simulation

Платформа Cymulate



Cymulate
Breach & Attack Simulation

Принцип работы Cymulate



Симуляция полноценных APT-атак

- Последовательно симулирует все шаги APT-атаки в рамках одной проверки
- Включает предсозданные шаблоны известных APT-атак: Lazarus, APT38, FIN8, Cobalt и пр.
- Позволяет создавать свои атаки в режиме конструктора
- Предоставляет отчетность по все атаке, в т.ч. рекомендации по детектированию и предотвращению

Строим реплику реальной APT-атаки

До эксплуатации → Эксплуатация → После эксплуатации

Электронная почта

Доставка зараженных писем

Веб-шлюз

Зараженные сайты и ссылки

Фишинг

Индивидуальные фишинговые кампании

Хостовая защита

Скачивание и исполнение вредоносных сценариев

Латеральное движение

Разведка и построение карты потенциальных путей атаки и уязвимых хостов в сети

Кража данных

Попытка кражи чувствительных данных с помощью различных техник

Cymulate
Breach & Attack Simulation

Company Confidential & Proprietary

Разбор полетов и повышение защищенности

Cymulate
Breach & Attack Simulation

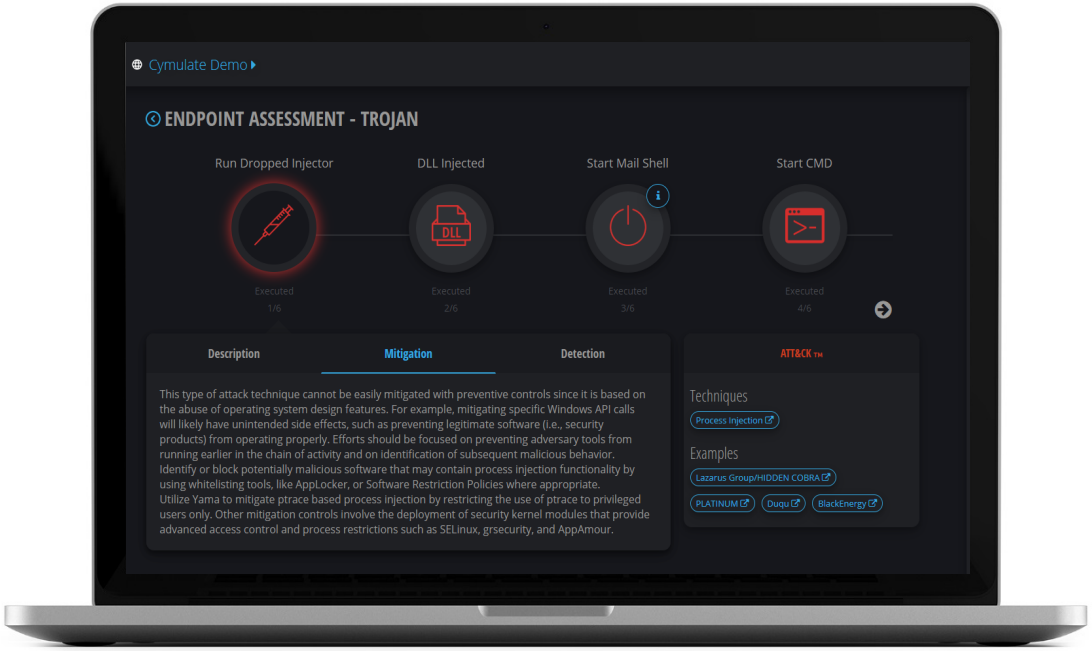
Технические и бизнес-отчеты

Для экспертов ИБ / SOC

- Уязвимые места / слепые пятна / ATT&CK
- Наиболее проблемные области
- Рекомендации по исправлению

Для CISO / руководителя

- Динамика защищенности
- Сферы инвестиций
- Сравнение с индустрией / с собой



Cymulate
Breach & Attack Simulation

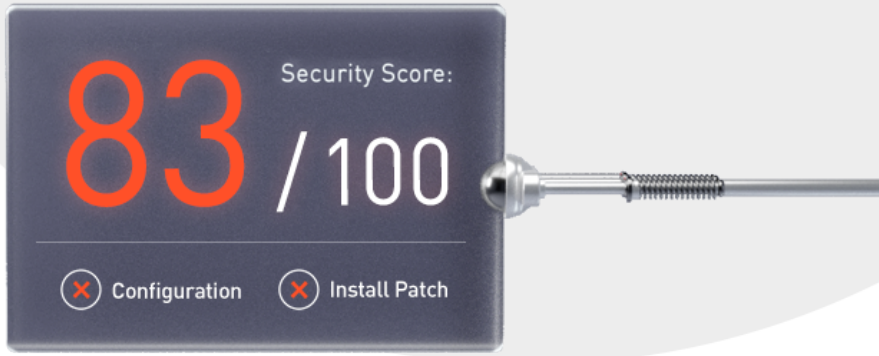
Cymulate Score. Количественная оценка защищенности

NIST Risk Management Framework

MITRE ATT&CK Framework™

CVSS V3.0 Calculator

Microsoft's DREAD



Переменные

- Серьезность атаки
- Вероятность возникновения
- Успешность атаки в прошлом

Следующий шаг: Тестирование

Илья Осадчий, Тайгер Оптикс
io@tiger-optics.ru

Cymulate
Breach & Attack Simulation