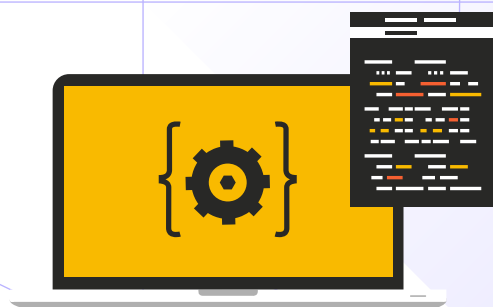


Autopentest iSTEM

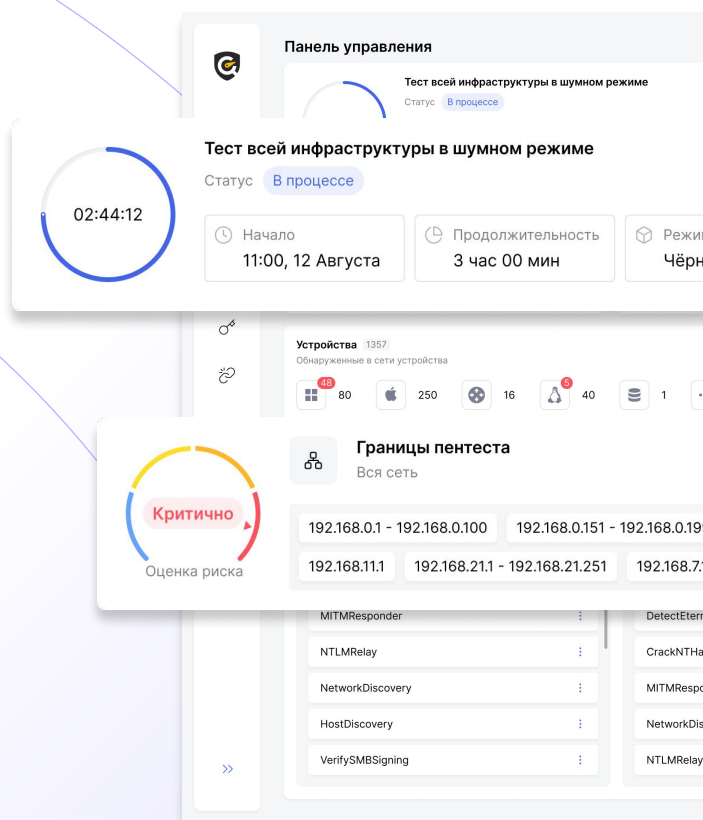
Непрерывный анализ и усиление киберзащиты

Платформа Autopentest iSTEM создана в ответ на актуальные вызовы в сфере кибербезопасности. Система автоматизирует тестирование защиты корпоративной ИТ-инфраструктуры и позволяет заказчикам без привлечения узкопрофильных экспертов или третьих лиц быстро и безопасно выполнять **непрерывный пентест сетей любых размеров и конфигураций**.



Актуальные вызовы

С каждым днём киберугрозы становятся более частыми, агрессивными и сложными, а совокупный ущерб от хакерских атак измеряется миллиардами. В то же время дефицит квалифицированных специалистов по информационной безопасности значительно обостряет проблему. Организациям из любых отраслей нужна уверенность в том, что их **решения в сфере кибербезопасности работают действительно эффективно**.



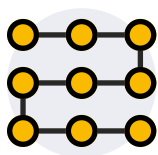
Автоматизация процессов киберзащиты – ключ к предотвращению современных угроз!

[Узнать больше](#)

Offensive Security - Взгляните на свою сеть глазами хакера



Эксперты по информационной безопасности понимают, что для создания эффективной киберзащиты необходимо использовать опыт хакерского сообщества. Для анализа своих сетей важно применять те же инструменты, которые используют злоумышленники в реальных атаках. Подход Offensive Security позволяет выполнять реальную оценку защищённости с учётом всех внедрённых в организации инструментов безопасности. При этом ежегодный пентест отдельных сегментов сети или поверхностное сканирование статических уязвимостей не позволяют справиться с этой задачей.



Платформа Autopentest iSTEM моделирует мышление и действия хакера, играя роль оппонента для команды кибербезопасности. Виртуальный «злоумышленник», безопасно для организации, применяет актуальные хакерские техники и выявляет слабые места в окружении, корпоративных политиках и поведении пользователей. Система визуализирует пошаговые цепочки атак и демонстрирует приоритеты по устранению уязвимостей, опасных для сети в конкретный момент времени. Вместо теоретической оценки рисков, фокус внимания направлен на действительно критичные угрозы, подтверждённые на практике.

Непрерывный анализ киберзащиты

Современные сети динамичны. Они непрерывно меняются из-за появления в них обновлений, новых устройств, пользователей, программ и конфигураций. Вместе с этими изменениями меняется поверхность атаки, поэтому важно постоянно выполнять оценку киберзащиты и своевременно реагировать на новые угрозы, чтобы удерживать киберриски на приемлемом уровне.

Платформа Autopentest позволяет заказчикам непрерывно тестировать и усиливать свою киберзащиту, сильно сократить затраты как на сами тесты, так и на устранение уязвимостей.

[Узнать больше](#)