CYBERBIT
PROTECTING A NEW DIMENSION

Cyberbit Range

Для Государственного и Корпоративного Сектора

Первая Гипер-Реалистичная Имитационная Платформа Для Специалистов По Кибер Безопасности

Проблема

Институт SANS отмечает, что лидеры в области обеспечения кибербезопасности указывают на дефицит квалифицированного персонала, как на основное свое препятствие для эффективного реагирования на такого рода инциденты. При этом дефицит квалифицированного персонала в кибербезопасности будет продолжать существовать и дальше на фоне более чем 200 тысяч трудовых вакансий в одних только США, ожидается, что к 2019 г. эта цифра достигнет 1,5 миллиона незанятых рабочих мест (Forbes Magazine, октябрь 2015 г.). Отсутствие спонсирования обучения и повышения квалификации является общей причиной ухода способных сотрудников, увеличивая текучесть кадров. Поэтому обучение и сертификация персонала является наивысшим инвестиционным приоритетом для лидеров в области обеспечения безопасности на 2017 г. (SANS).

Cyberbit Range

Cyberbit Range представляет собой гипер-реалистичную имитационную платформу, позволяющую корпорациям создавать и эксплуатировать свои собственные центры подготовки специалистов по кибербезопасности. Эта платформа дает возможность работающим в организации профессионалам в области кибербезопасности участвовать в практическом обучении в условиях приближенных к реальным. Cyberbit Range служит также испытательным стендом для оценки инструментов и архитектур обеспечения безопасности в безопасной и контролируемой среде. В качестве ведущей в мире учебной платформы, Cyberbit Range позволяет как специалистам по кибербезопасности, так и руководящему составу компании отрабатывать реалистичные сценарии устранения инцидентов и существенно повышать показатели своей работы в случае действительного возникновения инцидентов в части кибербезопасности. Cyberbit Range ускоряет переподготовку, уменьшает время, затрачиваемое на сертификацию, и обеспечивает подготовку более компетентных сотрудников, обладающих самыми современными знаниями.

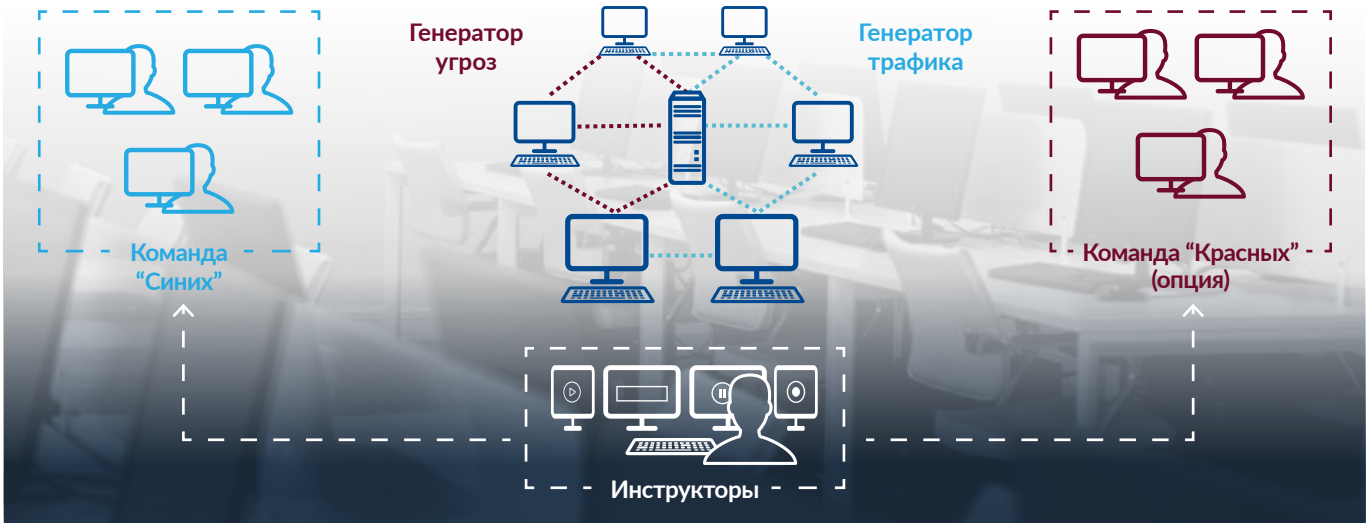
Преимущества Cyberbit Range

- **Повышает эффективность Вашего реагирования на инциденты** – вместо того, чтобы отрабатывать вопросы взаимодействия и реагирования во время действительного нарушения кибербезопасности, группы реагирования на инциденты репетируют свои рабочие процессы заблаговременно, благодаря чему они в состоянии значительно быстрее реагировать на действительно случающиеся инциденты и более эффективно устранять их.
- **Позволяет создать Ваш специализированный учебный центр -** Cyberbit Range является полностью динамичной и настраиваемой системой. Какими бы ни были Ваши сеть, инструменты и проблемы, Cyberbit Range позволяет Вам приспособить Вашу сетевую среду, применяемые инструменты и учебные сценарии к Вашим конкретным потребностям.
- **Независимое обучение –** благодаря разработке Ваших собственных учебных сценариев, курсов и процессов сертификации, Вы можете самостоятельно эксплуатировать Ваш учебный центр.
- **Поддерживает и обновляет навыки Вашего персонала –** за счет тренировки с использованием самых последних сценариев атак и новейшего инструментария кибербезопасности, Ваш персонал всегда хорошо информирован и находится в курсе дела.
- **Ускоряет повышение квалификации –** имитационное обучение позволяет Вам быстрее осуществлять повышение квалификации и сертификацию Вашего персонала, так что вновь принятые сотрудники в течение минимального времени становятся готовыми к работе.
- **Улучшает навыки групповой и индивидуальной работы –** улучшает навыки сотрудничества и взаимодействия Вашего персонала и их общие показатели успешности как в составе группы, так и по отдельности.
- **Обучение Вашего руководящего состава –** менеджмент часто является частью процесса реагирования на инциденты. Cyberbit Range обеспечивает такие учебные сценарии, как борьба с программами – вымогателями (ransomware), в которых задействован руководящий состав.
- **Обеспечивает безопасное тестирование Вашего инструментария кибербезопасности –** дает возможность тестировать Ваши системы и выполнять проверку концепций в реалистичной, но при этом безопасной среде, без воздействия на находящуюся в эксплуатации сеть.
- **Определение уязвимостей сети и тестирование архитектуры кибербезопасности –** позволяет безопасным образом оценивать Вашу ситуацию в части кибербезопасности без риска для находящейся в эксплуатации сети.

Как это работает?

Cyberbit Range симулирует работу сети, корпоративный и интернет трафик в виртуальной среде. Допускает подключение приложений и оборудования Заказчика, чтобы сделать симулятор максимально соответствующим реальной сети компании. Используя предустановленные Cyberbit сценарии атак, демонстрируются различные типы атак и методы противодействия им. Обучающиеся оцениваются по умению отслеживать, расследовать, реагировать и устранять угрозы и достигать целей предопределённых заданием на сессию. Сессия записывается и привязывается к временной шкале, чтобы позже, при подведении итогов сессии, иметь возможность ее воспроизвести и проанализировать. Каждый сеанс может быть запущен с любой временной отметки и повторен. Cyberbit Range обеспечивает моделирование сети ИТ и SCADA с возможностью подключения дополнительного физического оборудованием SCADA, а также поддерживает как индивидуальные, так и командные тренировки.

Настраиваемая сеть, трафик и угрозы



Возможности конфигурирования сети, типов трафика и угроз

Cyberbit Range Основные возможности

Сложная распределенная сеть, сценарии атак и трафик.

Реалистичные настройки

Cyberbit Range первая гипер-реалистичная платформа моделирования для обучения специалистов по кибербезопасности. Предоставляя тренерский опыт в окружении близком к реальной жизни, она позволяет слушателям подготовиться к фактическим проблемам, с которыми они столкнутся во время реальных атак, и эффективно противостоять им. Это достигается за счет точного копирования настроек сети, реалистичнго трафика и возникающих угроз, также как они будут появляться в процессе реальных атак, используя при этом фактические инструменты безопасности, которые стажеры будут использовать на работе.

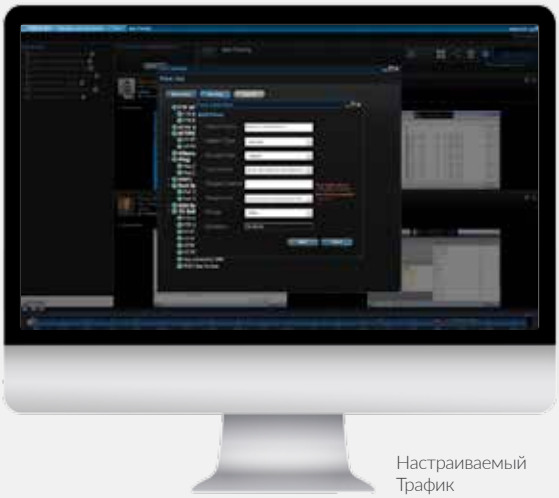
Гибкая и настраиваемая

Cyberbit Range полностью настраиваемая платформа, вы можете использовать предустановленные производителем настройки и сценарии, или создать собственные типы сетей, варианты сетевого трафика и сценарии атак. Добавление инструментов безопасности производится очень просто, преподаватель может использовать те же инструменты безопасности, которые используются, обучаемыми, в реальной жизни. В результате, конкретные клиенты получат кастомизированную персонально под них среду обучения, что значительно повышает эффективность процесса.

Полностью автоматизированная

Учебные занятия и сценарии моделирования выполняются автоматически, с автоматическим наполнением сети доброкачественным трафиком и запуском сценариев угроз, устраняя необходимость в наличии «красной команды» – команды атакующих. Это позволяет обеспечить полную независимость при проведении курсов и отработке тестовых сценариев, обеспечивая при этом последовательное обучение, которое не зависит от опыта и квалификации команды атакующих.

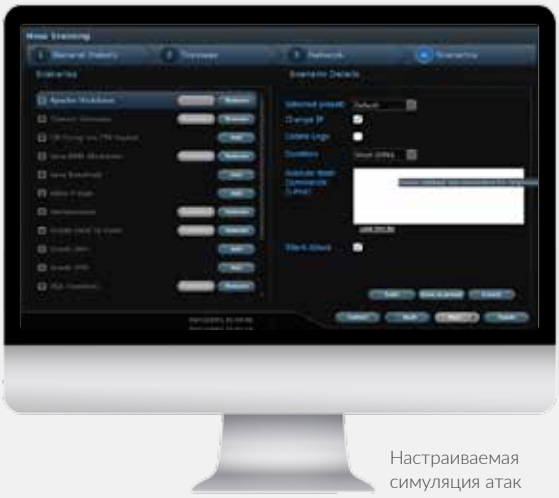
Cyberbit Range Основные возможности



Настраиваемый Трафик

Генератор реального трафика

Cyberbit Range создает реалистичный трафик и запускает его в смоделированную сеть, трафик реплицирует действия пользователей и обычных сетевых коммуникаций. Трафик может быть изменен до или в течение всей сессии, используя различные протоколы связи и каналов, включая HTTP, HTTPS, FTP, SMTP, POP3, SCADA и многое другое.



Настраиваемая симуляция атак

Симуляция комплексных атак

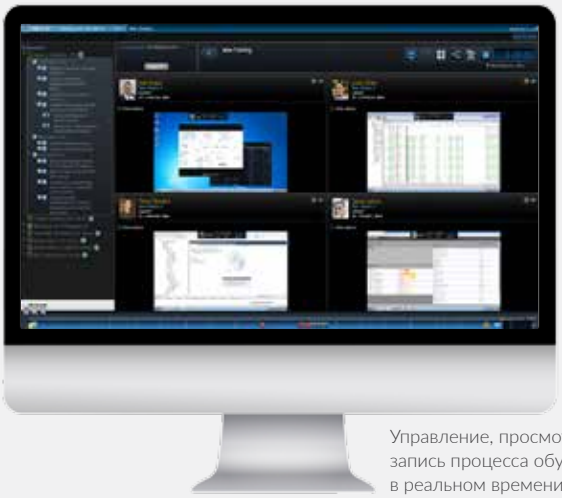
Генератор атаки позволяет легко создать любой сценарий атаки, основанный на наборе инструментов, который включает в себя сотни компонент. Атаки могут осуществляться из любого источника в сети и быть направлены на любой сетевой компонент. Операторы учебного центра вооружены большим набором инструментов для создания новых сценариев атак независимо друг от друга, или они могут настроить библиотеку предопределенных сценариев атак, которые предоставляются по умолчанию.

Симуляция информационных и промышленных сегментов сети

Cyberbit Range обеспечивает симуляцию как информационных, так и промышленных сегментов сети, с подключением физического оборудования для промышленного сегмента, который интегрируется с информационным и SCADA сегментами, а также готовые сценарии атак, включая атаки, которые начинаются в информационном сегменте сети и продолжаются в промышленном сегменте, аналогичные тем, которые происходили в реальной жизни в недавнем прошлом.

Передовая методика обучения

Cyberbit Range обеспечивает представление и мониторинг всей тренировки на рабочем месте инструктора в реальном времени, что позволяет преподавателям писать замечания, контролировать рабочие места обучаемых, отслеживать цели и скорость реакции. Каждое действие привязано ко времени в журнале аудита. Сессии записываются и могут быть воспроизведены с пояснениями для обучаемого, для оптимальной обратной связи. Расширенные инструменты оценки позволяют инструкторам проводить оценку обучаемого и эффективность группы на постоянной основе.



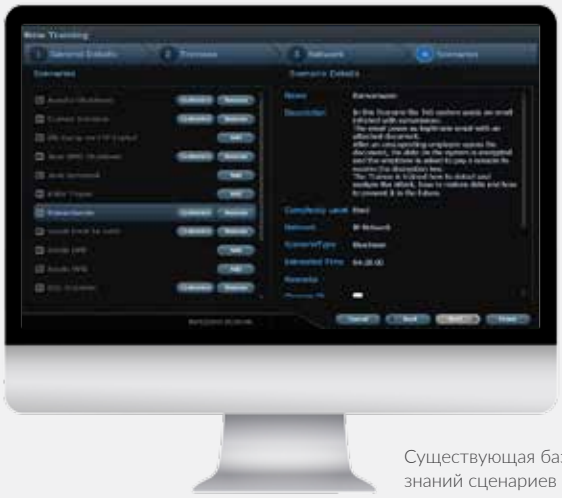
Управление, просмотр и запись процесса обучения в реальном времени

Контролируемое тестовое окружение

Cyberbit Range используется для оценки безопасности сетевой архитектуры, поиску и оценки ее уязвимостей, служит инструментом для тестирования и пилотирования в настроенном сетевом окружении технологий кибербезопасности третьих производителей, используя трафик аналогичный существующему и различные сценарии атак.

Cyberbit Range Основные возможности

Оценка результатов обучаемых и команд



Существующая база знаний сценариев атак

Персональное и командное обучение

Cyberbit Range поддерживает обучение как отдельных специалистов, так и целых команд по кибербезопасности. Персональное обучение построено на теоретической и практической подготовке обучаемых по различного уровня сложности сценариям угроз, выполнении заданий и принятии ответственных решений. Подготовка команд на развитии сотрудничества и общения, выстраивании правильных процессов и процедур.

База знаний Cyberbit

Cyberbit предлагает готовые настройки сетей (как информационных, так и технологических), наполнение трафика и сценарии угроз различных уровней сложности. Cyberbit обеспечивает периодические обновления существующей в системе базы знаний новыми сценариями атак, разработанными нашей группой экспертов по кибербезопасности, чтобы обеспечить наших Заказчиков самыми актуальными сценариями, на сегодняшний день.

О КОМПАНИИ CYBERBIT™

Cyberbit предлагает передовые решения в области кибербезопасности для финансовых организаций, предприятий критической инфраструктуры, военных и правительственных организаций. Портфолио компании предоставляет полный набор продуктов для обнаружения и митигации кибератак, а также помогает нашим Заказчикам решать оперативные задачи управления кибербезопасностью. Портфолио Cyberbit включает в себя решения по обнаружению и реагированию для конечных устройств (EDR), по кибербезопасности и контроля бесперебойной работы SCADA (SCADAShield), по автоматизации процессов управления SOC (SOC 3D), а также по подготовке персонала для обеспечения кибербезопасности на базе полнофункционального симулятора (Range). Продукты компании Cyberbit были выбраны крупными международными корпорациями по всему миру для обеспечения кибербезопасности своих сетей.

Cyberbit является стопроцентной дочерней компанией Elbit Systems Ltd. (NASDAQ и TASE: ESLT)

sales@cyberbit.net | www.cyberbit.net

Офис в Израиле:

CYBERBIT Commercial Solutions Ltd.
22 Zarhin St. Ra'anana
Israel 4310602
Тел.: +972-9-7799800 | E-mail: sales@cyberbit.net

CYBERBIT
PROTECTING A NEW DIMENSION