ПОЛИГОН. ПЕРВЫЙ. НАШ

На конференции IT-Security Международный центр образования «ROZUM» Национального центра обмена трафиком презентовал киберполигон CyberRing, разработанный в нашей стране. О новинке – разговор с руководителем центра образования Юлией СОКОЛОВОЙ.

ВС *– Что такое киберполигон? И чем вызвана необходимость отечественной разработки?*

– Киберполигон – это виртуальный тренажер, который применяют для отработки практических навыков специалистов в области кибербезопасности. Например, для отражения и расследования киберинцидентов.

В Международном центре образования «ROZUM» такой элемент, как полигон для подготовки специалистов, внедрили около двух лет назад. Правда, сразу на базе решений российских вендоров. Чтобы не зависеть от иностранных вендоров и сократить затраты на обучение, принято решение создать свою отечественную виртуальную площадку.

Разработчиком выступил Национальный центр обмена трафиком. Перед разработкой его специалисты, а также Оперативно-аналитического центра при Президенте Республики Беларусь протестировали доступные киберполигоны компаний «Инностейдж», «Солар» («Ростелеком»), «Университет Иннополис» и других. У каждого выделили сильные стороны. Например, где-то – расширенную виртуальную инфраструктуру, где-то – более удобную «админку», где-то – большой выбор доступных сценариев киберинцидентов. И, как результат, в НЦОТ создали свой киберполигон CyberRing, учитывающий сильные стороны конкурентов. Уже в апреле этого года полигон стал доступен пользователям.

ВС *– И в чем же уникальность белорусского полигона?*

– На отечественном тренажере воссоздана среда с учетом опыта работы белорусских компаний в сфере обеспечения информационной безопасности. При построении инфраструктуры учитывались не только требования законодательства, но и наличие оборудования

и соответствующего программного обеспечения в нашей стране. Сценарии проникновения в инфраструктуру нашего киберполигона прописываются на основе реальных случаев, с которыми сталкивалась наша Национальная команда реагирования на киберинциденты.

Кроме того, в эту разработку максимально интегрированы произведенные в нашей стране программные продукты: они дешевле, доступнее и поддерживаются в актуальном состоянии. В их числе – созданная НЦОТ система NTechnology SIEM, с помощью которой осуществляются сбор, хранение и анализ событий, исходящих от устройств компьютерной сети, формируются инциденты информационной безопасности для повышения уровня защищенности предприятий.

> На отечественном тренажере воссоздана среда с учетом опыта работы белорусских компаний в сфере обеспечения информационной безопасности. При построении инфраструктуры учитывались не только требования законодательства, но и наличие оборудования и соответствующего программного обеспечения в нашей стране.

ВС *– Из чего же состоит полигон и какой у него функционал?*

– За полгода коллектив разработчиков создал киберполигон CyberRing, который включает 3 системы для построения инфраструктуры, веб-портал и чат. На полигоне могут отрабатываться сценарии, когда либо команда «Синие» отражает проникновение в свою инфраструктуру, либо команда «Красные» нападает.

ВС *– Можно ли на киберполигоне задавать уровень сложности заданий?*

– Поскольку с помощью полигона мы повышаем квалификацию не отдельных специалистов, а целой команды, в этом нет необходимости. То есть нам надо научить взаимодействию людей с разным уровнем подготовки: условно, одного опытного специалиста в области кибербезопасности с десятком менее квалифицированных. Надо понимать, что, так как область кибербезопасности сейчас одно из самых востребованных ИТ-направлений, остро стоит вопрос подготовки опытных, сильных специалистов в этой области.

> С помощью полигона мы повышаем квалификацию не только отдельных специалистов, но и целой команды. То есть нам надо научить взаимодействию людей с разным уровнем подготовки: условно, одного опытного специалиста в области кибербезопасности с десятком менее квалифицированных.

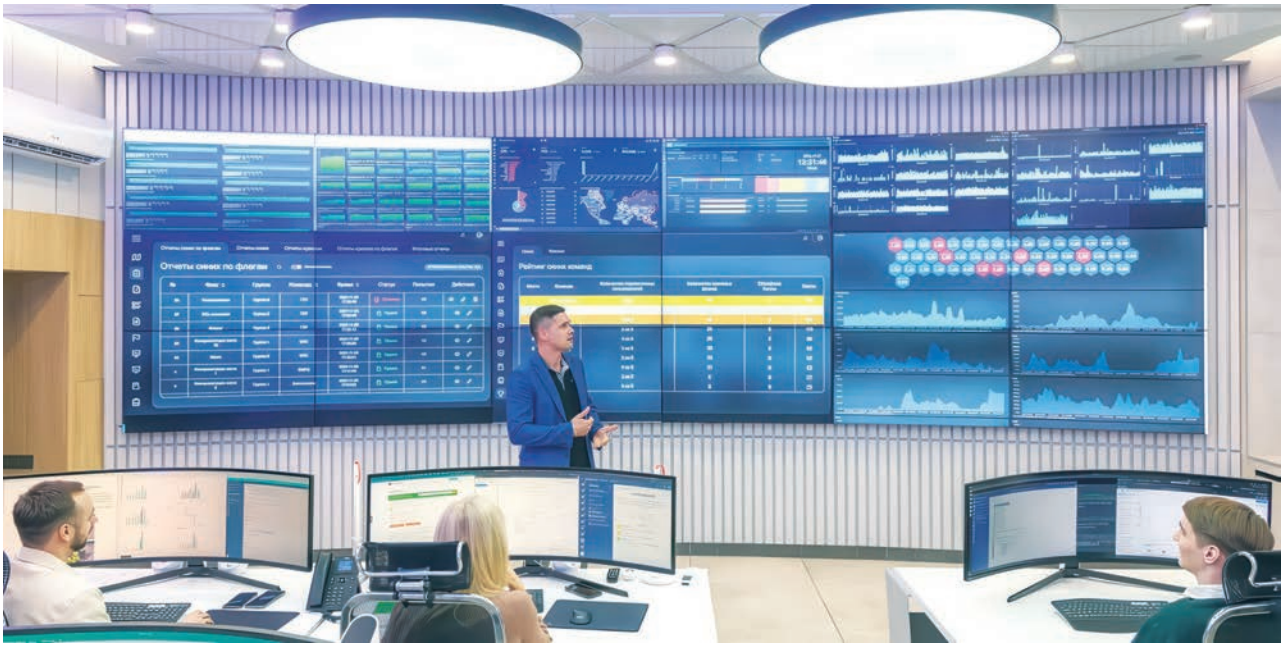
ВС *– Какие варианты использования предусмотрены для полигона?*

– Киберполигон базируется на современном мощном оборудовании, которое более сотни человек могут использовать одномоментно. Причем с большим количеством доступных инструментов для проведения расследования атаки.

То, что киберплощадка может выдерживать значительную нагрузку, дает нам возможность проводить на ней республиканские соревнования одновременно для 10–20 команд. К слову, первые уже прошли в декабре 2024 года. В ходе киберучений участники расследовали инциденты, связанные с компрометацией инфраструктуры вымышленной компании. По сценарию хакеры получили доступ к ее технологическому сегменту, содержащему критически важные объекты информатизации. В результате злоумышленники вызвали взрыв промышленной установки, а проблема не была решена внутренними силами компании. Киберучения прошли в несколько этапов и были максимально приближены к реальным условиям. Они позволили участникам не только проверить свои навыки, но и выработать эффективные стратегии противодействия кибератакам.

> То, что киберплощадка может выдерживать значительную нагрузку, дает нам возможность проводить на ней республиканские соревнования одновременно для 10–20 команд.

Второй вариант использования полигона – это, естественно, интеграция полигона в образовательные программы нашего центра образования. Планируется, что практические занятия на этой виртуальной площадке будут проходить слушатели, уже обладающие определенными знаниями в области кибербезопасности. Например, на курсе «Этичный хакинг».



Киберполигон позволяет анализировать ход проведения учений. На панели модератора – рейтинг и анализ действий команды

Третий вариант – корпоративное обучение. В таком случае компаниям предлагается в течение трех дней расследовать киберинцидент, а потом еще день посвятить работе над ошибками совместно с командой менторов из числа специалистов в области кибербезопасности НЦОТ, которые, к слову, в 2024 году заняли призовые места в международном чемпионате по кибербезопасности в рамках Петербургского международного экономического форума.

Еще один вариант – это продажа продукта компаниям, которые пожелают самостоятельно «прокачивать» навыки специалистов.

В принципе занятия на киберполигоне можно рассматривать как тимбилдинг. Цель, по сути, та же: сформировать эффективную команду. С бонусом в виде новых знаний и опыта.

ВС *– Планируется ли внедрение киберполигона в учебный процесс наших вузов?*

– Уже есть договоренности, что полигон будут использовать студенты факультета информационной безопасности БГУИР. В их учебной программе предусмотрено выполнение около 20 лабораторных работ, и с нового учебного года как минимум 4 из них будут проводиться на базе полигона в нашем образовательном центре.

ВС *– Обучая команды на киберполигоне, вы видите все их слабые места, формируете отчеты. Можете ли вы гарантировать пользователям, что эти сведения не попадут в руки хакеров?*

– Добыть сведения из тренажера невозможно. Полигон доступен только из закрытого контура: доступа к нему извне нет. Провести выгрузку данных в момент тренировки тоже не получится: эти действия строго контролируются модераторами и администратором.

Сохранность всей конфиденциальной информации гарантируется компаниям условиями договора.

ВС *– Каким вы видите развитие полигона?*

– Так как актуальность одного сценария атаки – 3–6 месяцев, для нас важно регулярно обновлять наш полигон. Например, в данный момент у наших специалистов в разработке находятся 2 новых сценария: один – для проведения осенью республиканских киберучений и второй – специфичный, для одной из важнейших отраслей экономики.

Сейчас мы готовим в основном специалистов-универсалов. И обучаем их базовым вещам, которые будут важны в любой компании и сфере. Но в перспективе хотелось бы в полигон внедрять больше дополнительных элементов-модулей, которые можно было бы, как конструктор, составлять под конкретные сферы и, соответственно, усложнять задачи. ВС

Анастасия МАНУИЛОВА

НЦОТ rozum

ПЕРВЫЙ КИБЕРПОЛИГОН