ТИХООКЕАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Создание экосистемы кибербезопасности в университете: с нуля до студенческого SOC

Автор:
Москвичева Ксения Сергеевна,
заместитель заведующего кафедры компьютерной безопасности, руководитель IT-ТОГУ

ФГБОУ ВО «Тихоокеанский государственный университет»

Актуальность проблемы и цель

- Кибербезопасность требует постоянного обновления знаний и навыков.
- Традиционные программы фокусируются на теории, игнорируя практику.
- Пробел между учебным процессом и требованиями индустрии.

Цель исследования:

Разработка и оценка эффективности модели создания экосистемы кибербезопасности для подготовки востребованных специалистов.

Методология создания экосистемы

5 ключевых компонентов экосистемы:

1. CTF как точка входа. Развитие практических навыков через соревнования. Формирование сообщества энтузиастов.

2. Интеграция CTF в учебные дисциплины. Практико-ориентированные задачи в рамках курсов.

3. Геймификация образования. Элементы мотивации: внутренняя валюта, мерч, стажировки.

4. Разработка университетского киберполигона. Моделирование реальных атак и защита инфраструктуры.

5. Студенческий SOC. Мониторинг событий безопасности, анализ логов, работа с реальными кейсами.

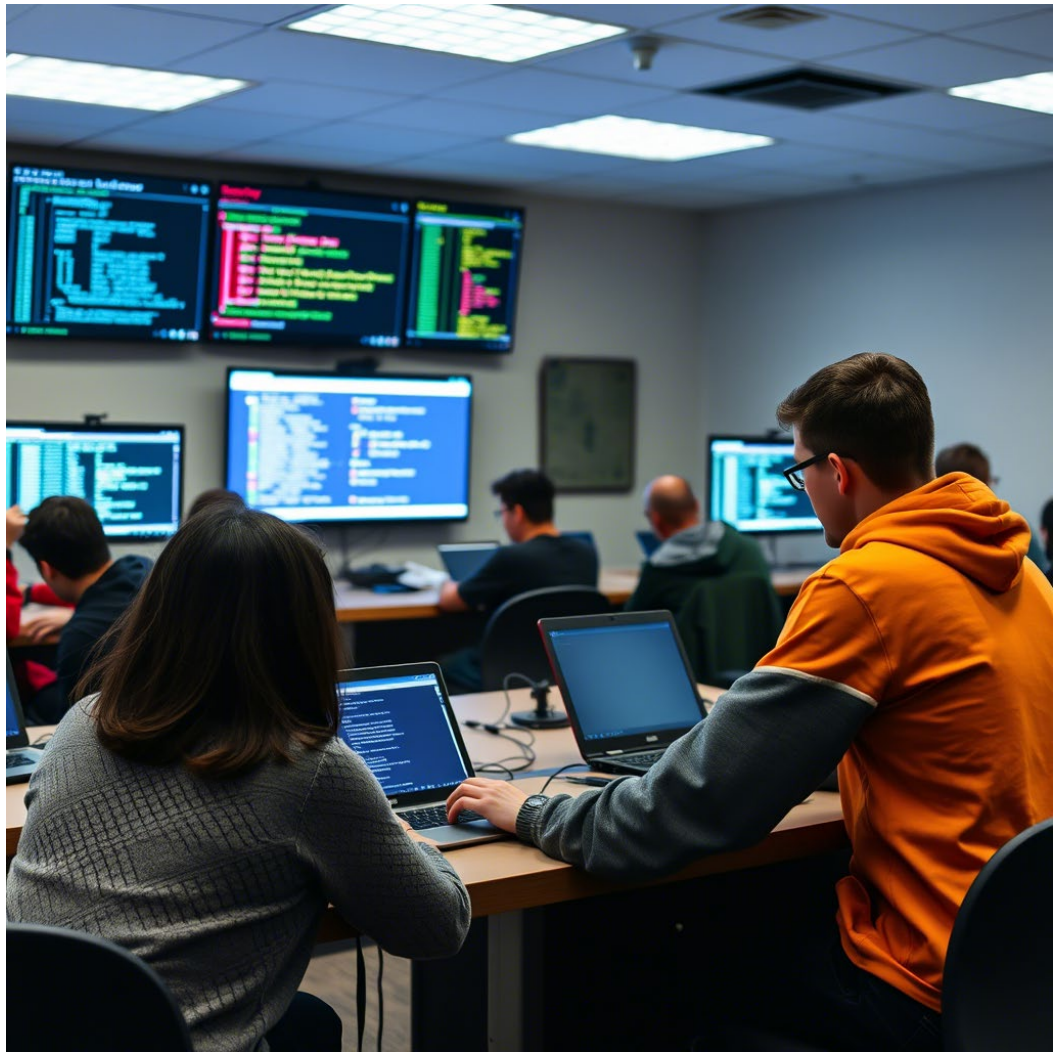
CTF как точка входа

- Регулярные соревнования для студентов всех курсов.
- Участие в международных и всероссийских конкурсах (VolgaCTF, BRICS+ CTF).
- Ежегодные соревнования "FarEastCTF" для школьников и студентов.

Результат:

Формирование сообществ энтузиастов. Выявление талантов и их дальнейшее развитие.

Интеграция CTF в учебные дисциплины



Задачи CTF адаптированы под учебные курсы:

- "Теория вероятностей": анализ False Positive-срабатываний.
- "Математическая статистика": выявление аномалий в трафике.
- "Криптографические протоколы": шифрование данных.
- Использование реальных логов и событий безопасности.

Пример:

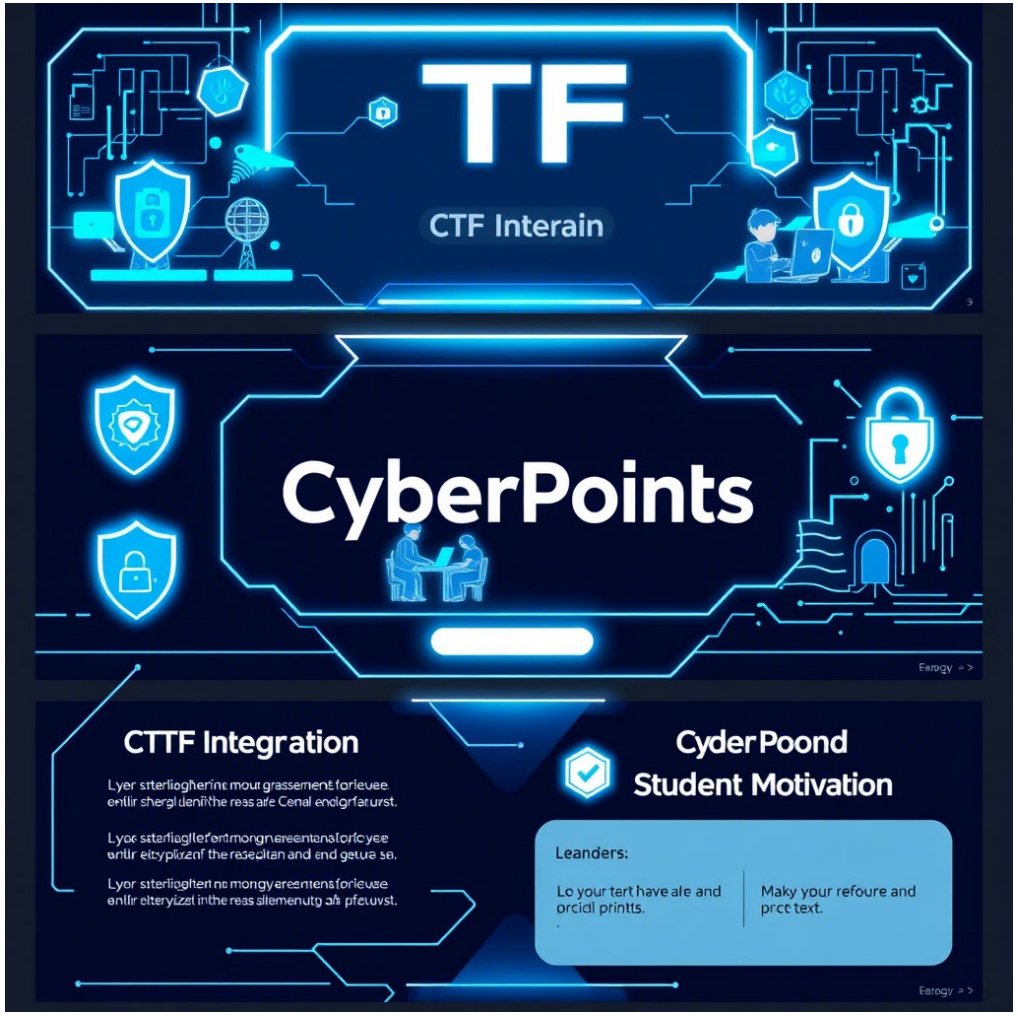
Анализ логов сервера университета для предотвращения Brute Force-атак.

Геймификация образования

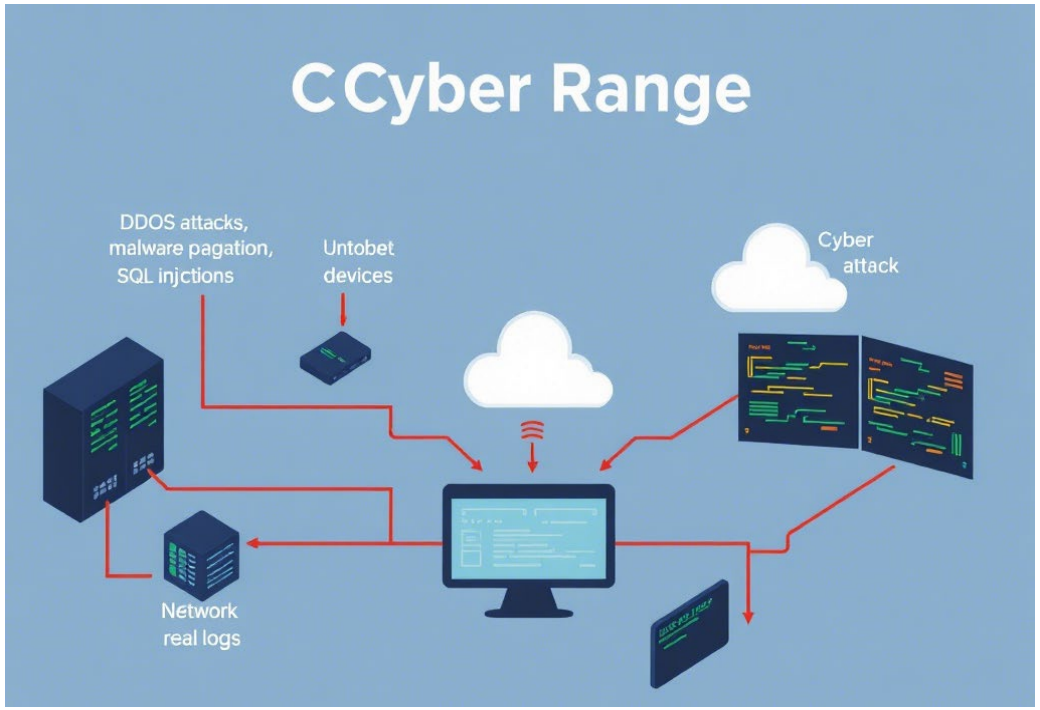
Система "CyberPoints":

- Баллы за участие в CTF, выполнение заданий, прохождение курсов.
- Возможность обмена баллов на мерч или стажировки.
- Повышение вовлеченности и здоровой конкуренции.

Студенты мотивированы развивать навыки. Формирование устойчивого интереса к кибербезопасности.



Киберполигон: площадка для реальных тренировок



Инфраструктура: серверы, сетевые устройства, SIEM-система.

Реальные сценарии атак:

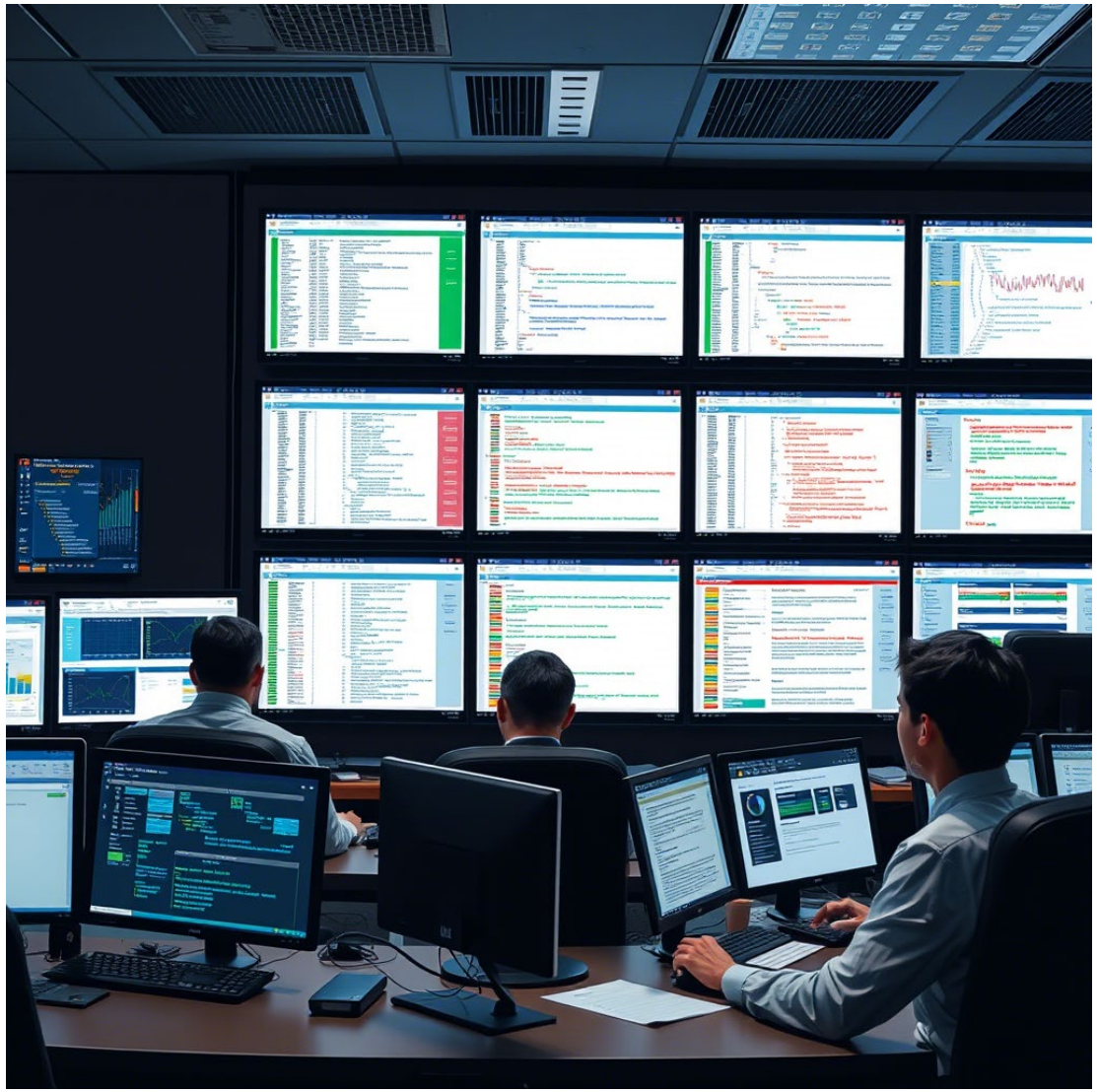
- DDoS-атаки.
- Распространение вредоносного ПО.
- SQL-инъекции и XSS-атаки.
- Подключение к SIEM университета для анализа реальных логов.

Студенты предотвращают DDoS-атаку, анализируя трафик и настраивая защитные механизмы.

Студенческий SOC

- Центр мониторинга событий безопасности на базе Тихоокеанского центра противодействия киберугрозам.
- Анализ логов и реагирование на инциденты.
- Сотрудничество с бизнесом, университетами и государственными структурами.
- Автоматизация первой линии SOC через IRP и скрипты.

Студенты получают уникальный опыт работы в условиях, приближенных к реальным.



Эффективность внедрения экосистемы

- Переход от теоретической базы к практико-ориентированному обучению.
- Повышение вовлеченности и мотивации студентов.
- 80% студентов трудоустраиваются по профилю уже на 4-м курсе.
- Высокая оценка уровня подготовки выпускников со стороны работодателей.

Комплексный подход объединяет образовательные нововведения и практическую подготовку, обеспечивая университету положительную обратную связь от студентов и индустрии.

Спасибо за внимание!

Сообщество FarEastCTF

Кафедра компьютерной безопасности

Школа кибербезопасности IT-ТОГУ