ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Киберполигон Ampire

Российская платформа для тренировки специалистов по обеспечению информационной безопасности

Максим Кувшинов
Руководитель обособленного подразделения
Перспективного мониторинга

Атакуют, обязательно атакуют

Хулиганы

Криминал

Наёмники

Кибервойска

Проактивная позиция

Не можем повлиять

- Сам факт атаки
- Квалификация атакующего
- Инструментарий
- Объём ресурсов

Можем повлиять

- Стоимость атаки
- Скорость реакции
- Содержание реакции
- Собственный опыт
- Планы и изменения

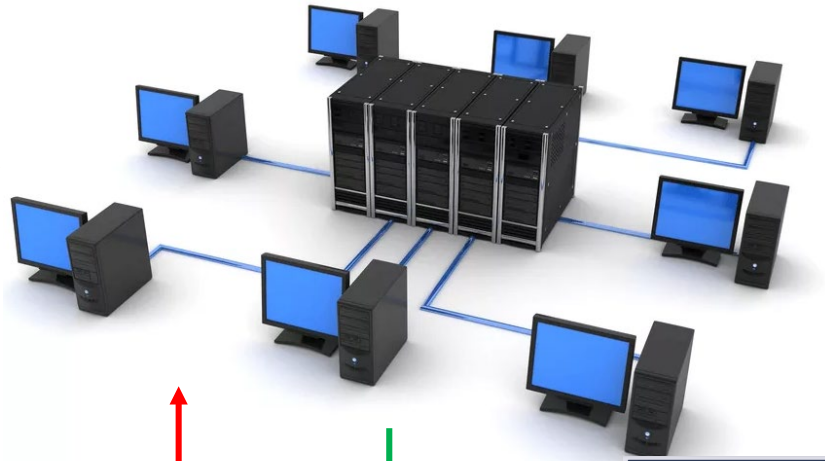
Способность действовать в экстренной ситуации зависит не от уровня знаний, а от уровня подготовки

Целевая аудитория

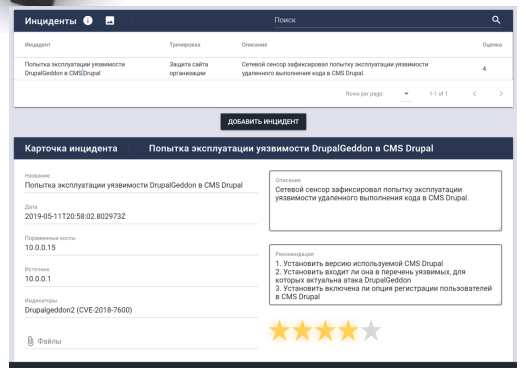
- Школьники и студенты с базовым знанием TCP/IP сетей, которые планируют работать в сфере защиты информации.
- ИБ-специалисты, которые хотели бы выделиться среди других кандидатов глубокими знаниями в определённых областях.
- ИТ-специалисты: новички и те, кто хотел бы увеличить перечень навыков в резюме.

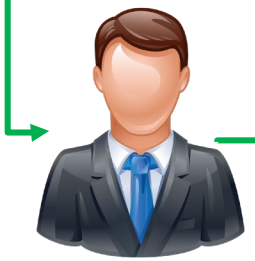
AMPIRE

Наша учебно-тренировочная платформа содержит сценарии различной сложности для проведения киберучений, сертификационных тестов и отработки необходимых навыков.



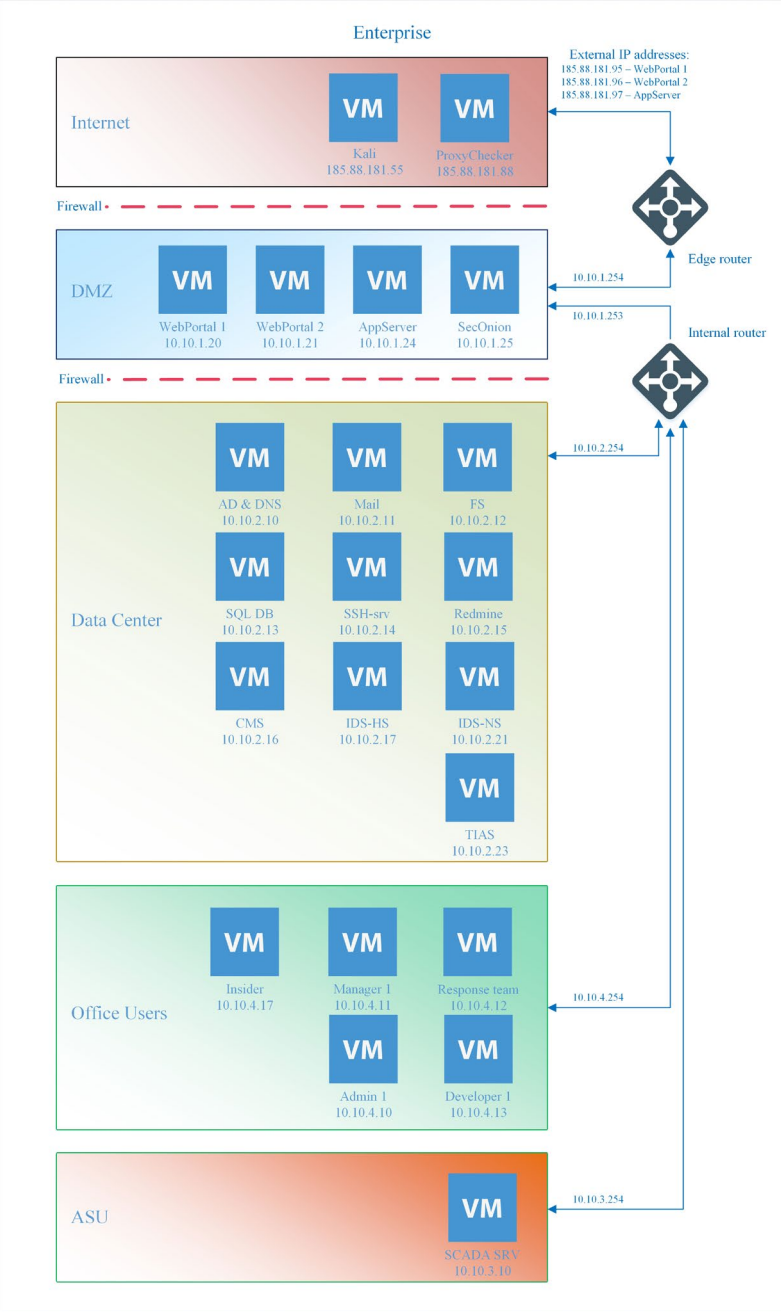
AMPIRE





Группа мониторинга

Группа реагирования



← Этот по умолчанию.

Можем сделать кастом.

Базовые сценарии киберучений

Защита базы данных предприятия

Защита контроллера домена предприятия

Защита файлового сервера предприятия (MS17-010)

Защита данных сегмента АСУ ТП

Защита научно-технической информации предприятия

Защита корпоративного портала от внутреннего нарушителя

СЗИ

ТехноФест 2022 infotecs

ViPNet IDS NS

ViPNet IDS HS

ViPNet TIAS

IDS/IPS Snort

IDS/IPS Suricata

ELK

Security Onion

И почти любые другие

Типы проводимых занятий

- Киберучения
- Анализ защищённости и аудит ИТ-инфраструктуры виртуальной организации
- Противодействие группе реальных нарушителей (концепция Red Team и Blue Team)
- Лабораторные работы по настройке средств безопасности и прикладных сервисов
- Киберквесты

Минимум для участия

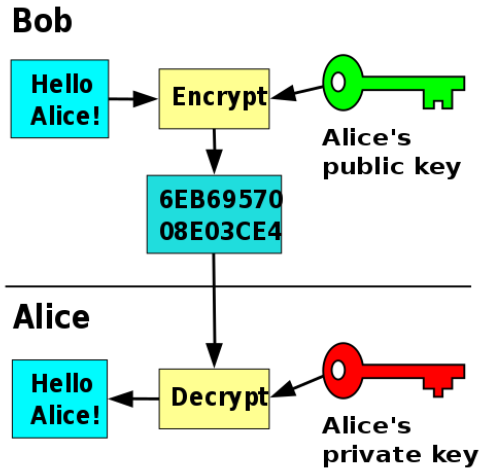
- Начальное знание сетевых технологий и TCP/IP стека.
- HTTP и основы построения веба.
- Основные типы компьютерных атак и уязвимостей ПО.
- Базовые знания по работе операционных систем.
- Принципы криптографической защиты информации, концепции симметричного и ассиметричного шифрования.

Навыки после прохождения курса

- Основные меры защиты сети, их преимущества и недостатки.
- Практика работы со средствами обнаружения вторжений (просмотр и фильтрация событий, правила выявления и реагирования на критичные события).
- Основные уязвимости веб-приложений и способы эксплуатации.

Навыки после прохождения курса

- Практика защиты веб-ресурсов при помощи WAF и исправления уязвимостей.
- Основные типы угроз для ОС и навыки защиты ОС.
- Средства защиты конечных точек.
- Криптографическая защита конфиденциальных данных при передаче и хранении.
- Навыки защиты технологический сетей.



Ключевые преимущества Ampire

- Полная независимость пользователя в проведении киберучений.
- Практические занятия для ИБ- и ИТ-специалистов любого уровня подготовки на «**двойнике**» реальной инфраструктуры.
- Полностью **автоматические сценарии атак**, разработанные экспертами по пентестам и базирующиеся на реальных инцидентах.
- Возможность создавать собственные сценарии по различным видам атак для ИТ-, ИБ-служб, операторов АСУТП, офиса, руководства.
- Подтверждение компетенций и развитие навыков группы реагирования на компьютерные атаки.
- ИТ-инфраструктура, СЗИ — всё вместе на одной платформе!

ТЕХНО 2022 infotecs Фест

Спасибо за внимание!

И давайте посмотрим Ampire

Максим Кувшинов

Руководитель обособленного подразделения г. Новосибирск
«Перспективный мониторинг»

Maksim.Kuvshinov@amonitoring.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363