AMPIRE

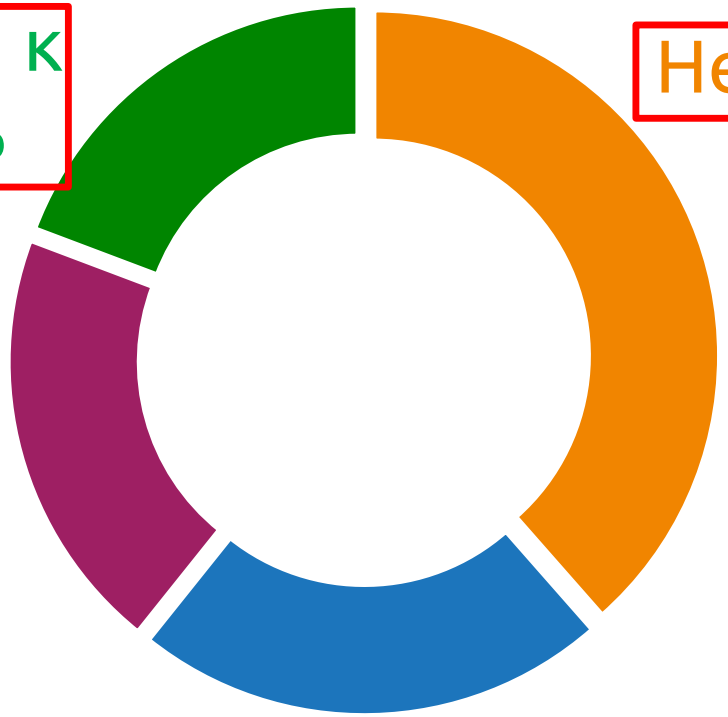
ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ученье – свет, а киберучения – практика. Как готовить специалистов так, чтобы мы их потом не переучивали

Пушкин Александр

технический директор ЗАО ПМ

Ключевой угрозой кибербезопасности предприятий становится дефицит профессиональных навыков ИБ-департаментов*



* По результатам опроса, проведённого в социальных сетях накануне Infosecurity Europe 2019.

http://safe.cnews.ru/news/top/2019-04-29_kiberbezopasnost_evropejskih_predpriyatij_pod

Почему так?

Поступили на профильные кафедры ИБ

Выбрали работу в ИТ/ИБ

Ушли в разработчики ПО

Ушли в пентест

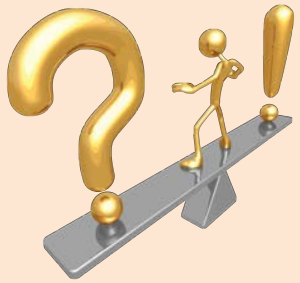
Специалист SOC

Печальный результат

1. Долгие поиски сотрудников SOC
2. За 2019 год **68** «подвисших» инцидентов у заказчиков
3. Целые федеральные субъекты испытывают кадровый голод в специалистах ИБ

Необходимое и достаточное условие

Hard Skills



Soft Skills

1. Знание технологий атаки и защиты
2. Знание и умение применять необходимые СЗИ и другие инструменты

1. Навыки командной работы
2. Умение взаимодействовать с другими членами группы реагирования
3. Навыки тайм-менеджмента

Текущая ситуация в отрасли ИБ

1. Теоретические курсы
2. Соревнования CTF
3. Курсы производителей ПО/оборудования

Дают сильно теоретизированные или практические навыки, оторванные от реальной ситуации

Может стажировка в действующем SOC?

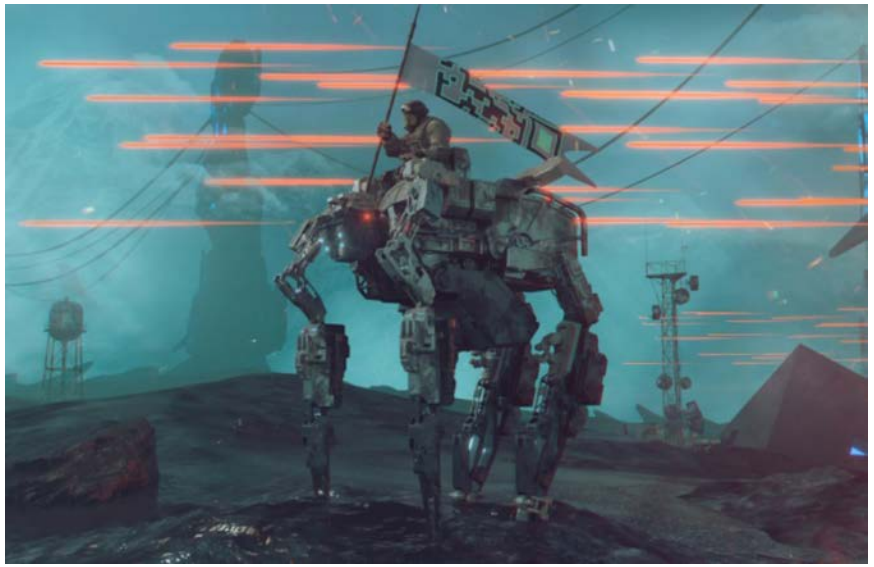
1. Работа на актуальных СЗИ
2. Опыт действующих сотрудников SOC
3. Анализ реальных инцидентов

1. Отвлечение действующих сотрудников
2. Риски для реальных заказчиков
3. Работа впустую

Киберучения?!

Процесс **моделирования целевых компьютерных атак** на некую ИТ-инфраструктуру с акцентом в сторону отработки навыков **защиты**:

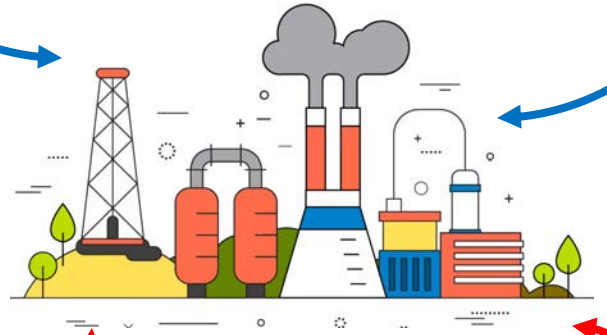
- анализ событий ИБ
- регистрация и расследование инцидентов
- устранение причин успешного выполнения КА
- командное взаимодействие

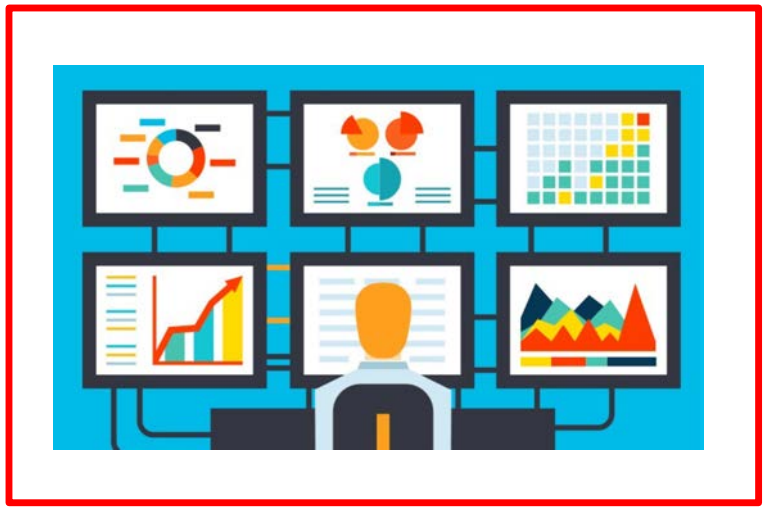


Ограничения для киберучений

1. Необходимость привлечения специалистов в «атакующей сфере»
2. Нельзя проводить в «боевой» инфраструктуре

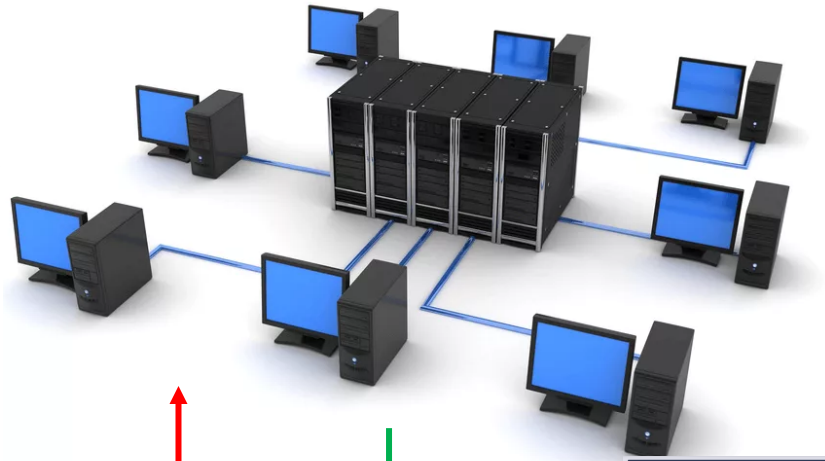
Необходимо создавать **киберполигоны** с максимальным уровнем автоматизации

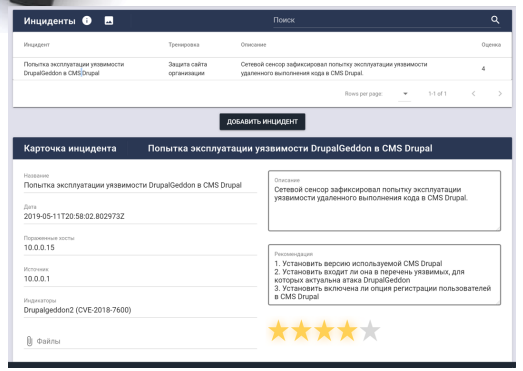




Киберучения. Киберполигон. Особенности

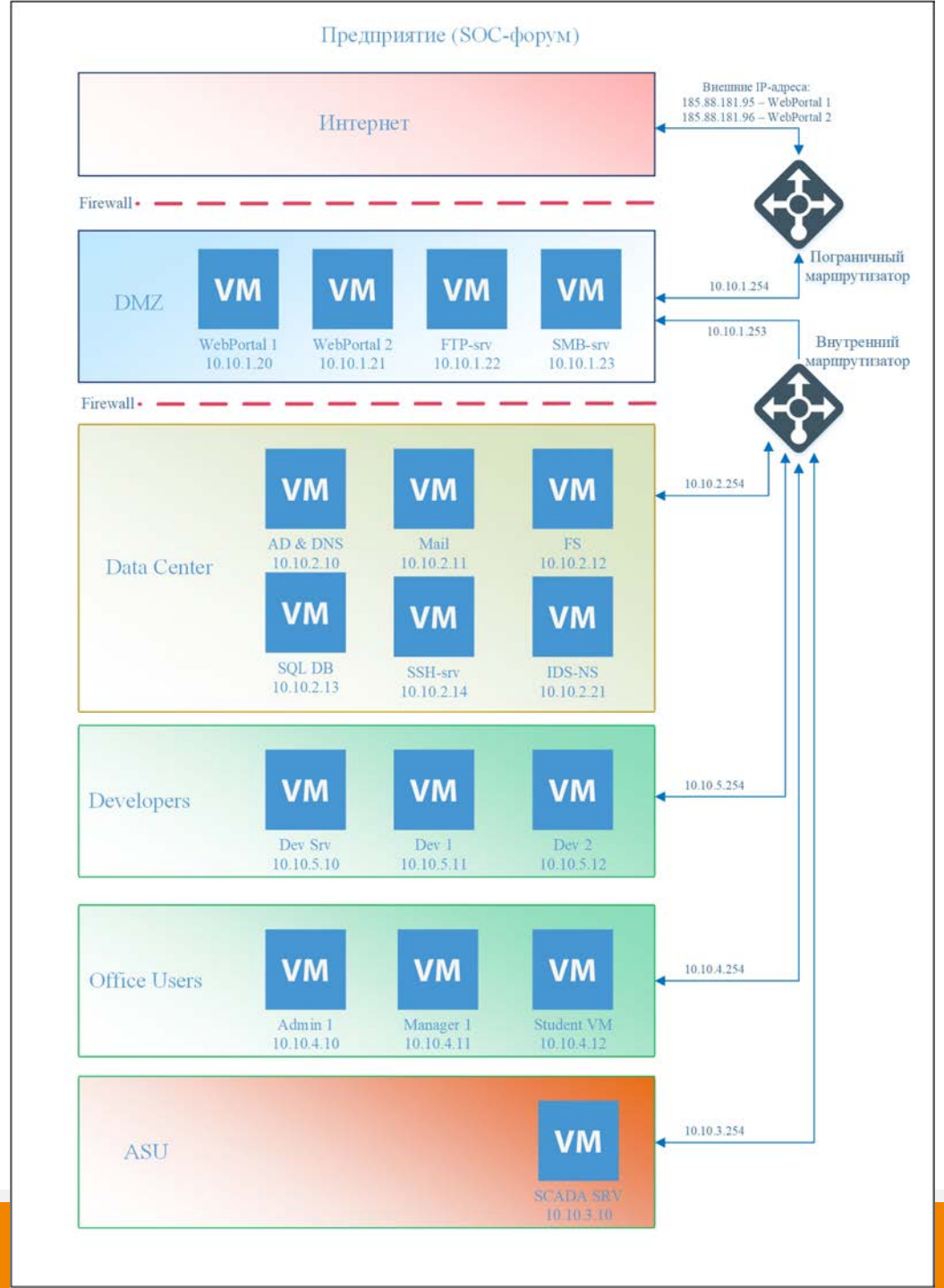
- Это **учебный** процесс, не шоу
- Они должны **восполнять пробелы** в технических и организационных знаниях
- Дать возможность посмотреть на атаки со всех сторон
- **Поэкспериментировать** с система обнаружения и защиты
- Дать обоснованные **метрики оценки**



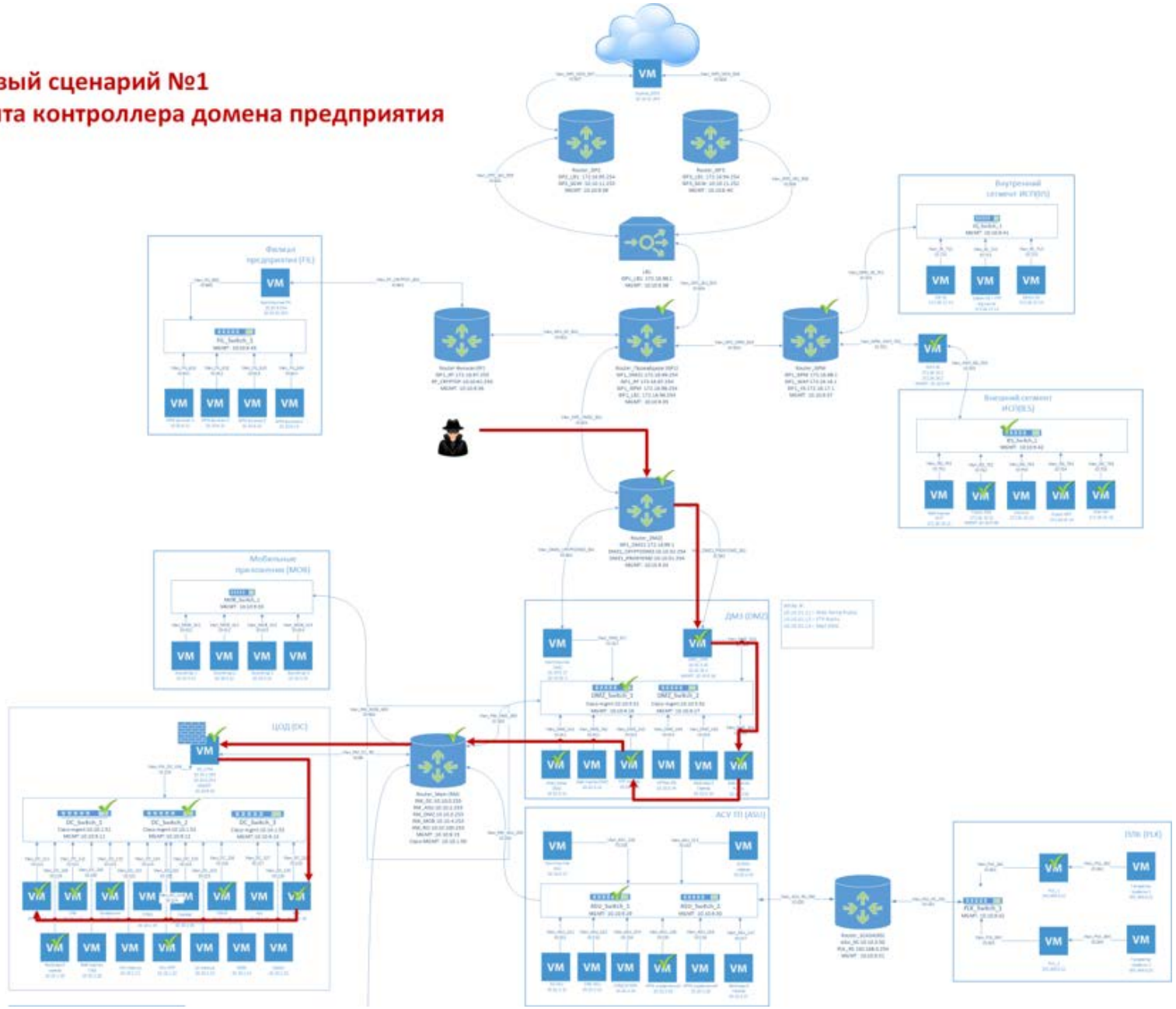


Группа мониторинга

Группа реагирования


Предприятие (SOC-форум)
Интернет
Внешние IP-адреса:
185.88.181.95 – WebPortal 1
185.88.181.96 – WebPortal 2
Firewall
Пограничный маршрутизатор
10.10.1.254
DMZ
VM
WebPortal 1
10.10.1.20
VM
WebPortal 2
10.10.1.21
VM
FTP-srv
10.10.1.22
VM
SMB-srv
10.10.1.23
10.10.1.253
Внутренний маршрутизатор
Firewall
10.10.2.254
Data Center
VM
AD & DNS
10.10.2.10
VM
Mail
10.10.2.11
VM
FS
10.10.2.12
VM
SQL DB
10.10.2.13
VM
SSH-srv
10.10.2.14
VM
IDS-NS
10.10.2.21
10.10.5.254
Developers
VM
Dev Srv
10.10.5.10
VM
Dev 1
10.10.5.11
VM
Dev 2
10.10.5.12
10.10.4.254
Office Users
VM
Admin 1
10.10.4.10
VM
Manager 1
10.10.4.11
VM
Student VM
10.10.4.12
10.10.3.254
ASU
VM
SCADA SRV
10.10.3.10

Базовый сценарий №1
Защита контроллера домена предприятия




КИБЕРУЧЕНИЯ
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ
AMPIRE
infotecs
КИБЕРУЧЕНИЯ
SOC ФОРУМ
ШТАБ
ANGARA

Киберполигон

1. Работа на актуальных СЗИ
2. Опыт действующих сотрудников SOC
3. Анализ реальных инцидентов
4. Не надо отвлекать действующих сотрудников
5. Рисков для заказчиков нет
6. Большая пропускная способность

1. Разработать или приобрести

Спасибо за внимание!

Пушкин Александр Несергеевич

Технический директор

ЗАО «Перспективный мониторинг»