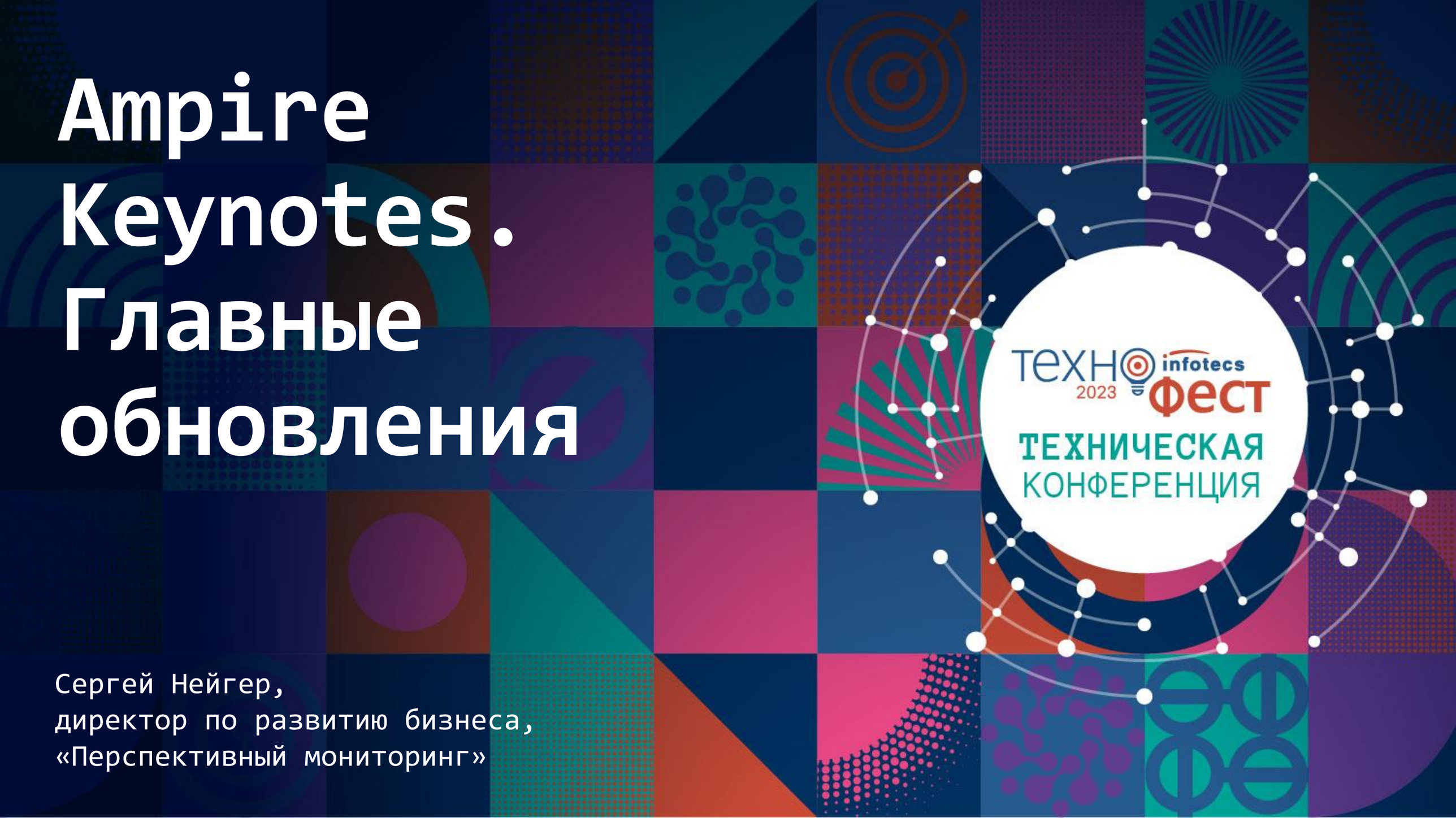
Ampire Keynotes. Главные обновления

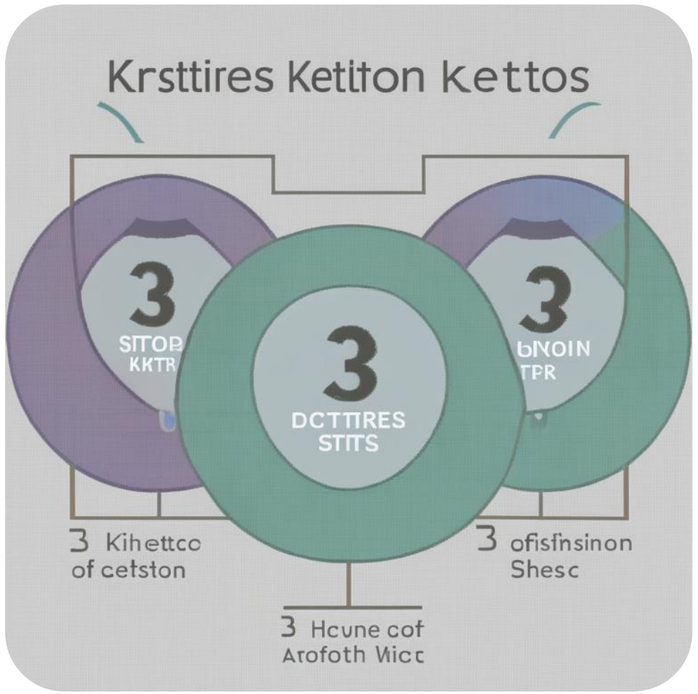


Сергей Нейгер,
директор по развитию бизнеса,
«Перспективный мониторинг»

Три кита ИБ ©ruDALL-E Kandinsky 2.1

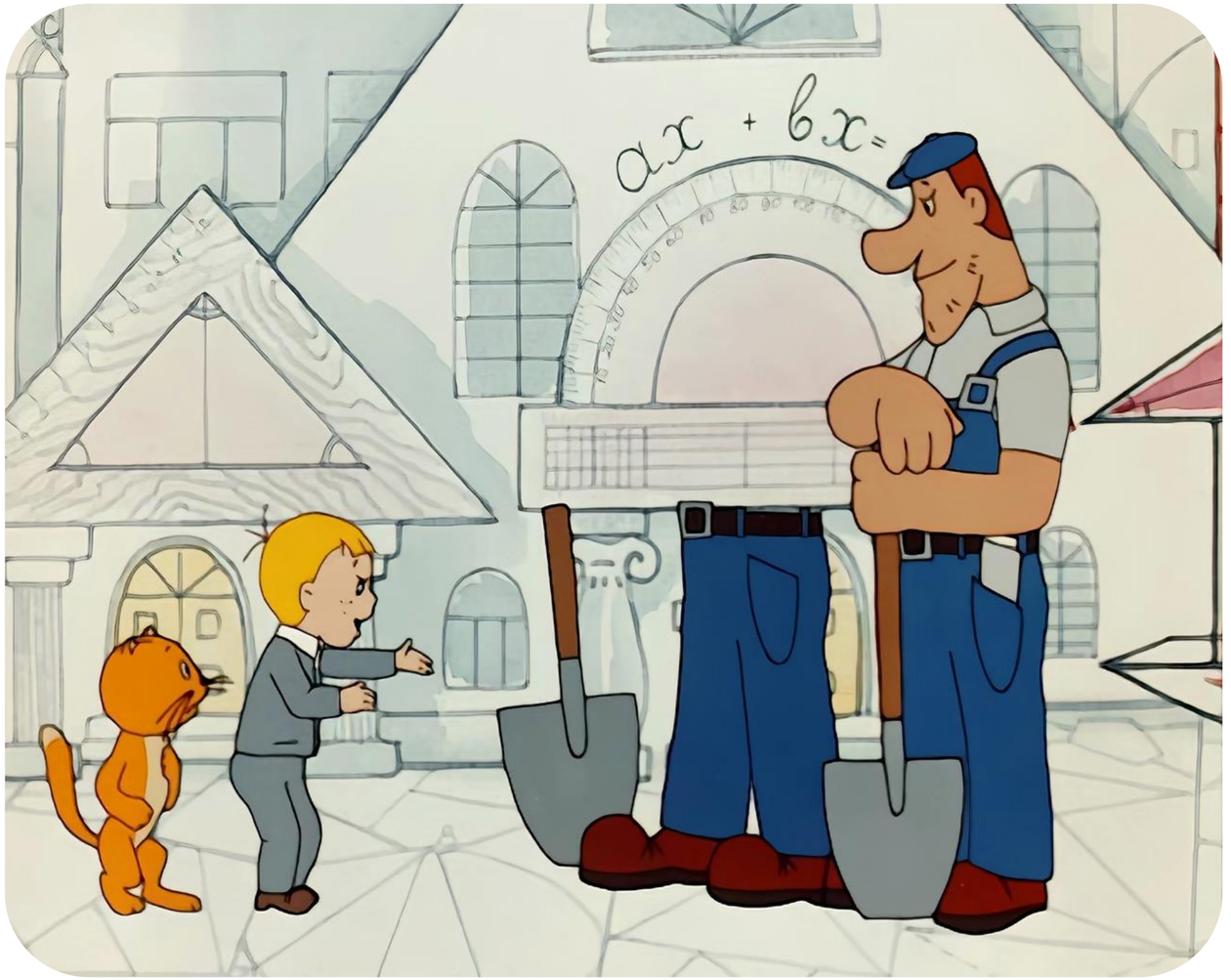
Техника

Люди



Процессы

Проблема «пол-админа»



Проактивная позиция

Не можем повлиять

1) Сам факт атаки
2) Квалификация атакующего
3) Инструментарий
4) Объём ресурсов

Можем повлиять

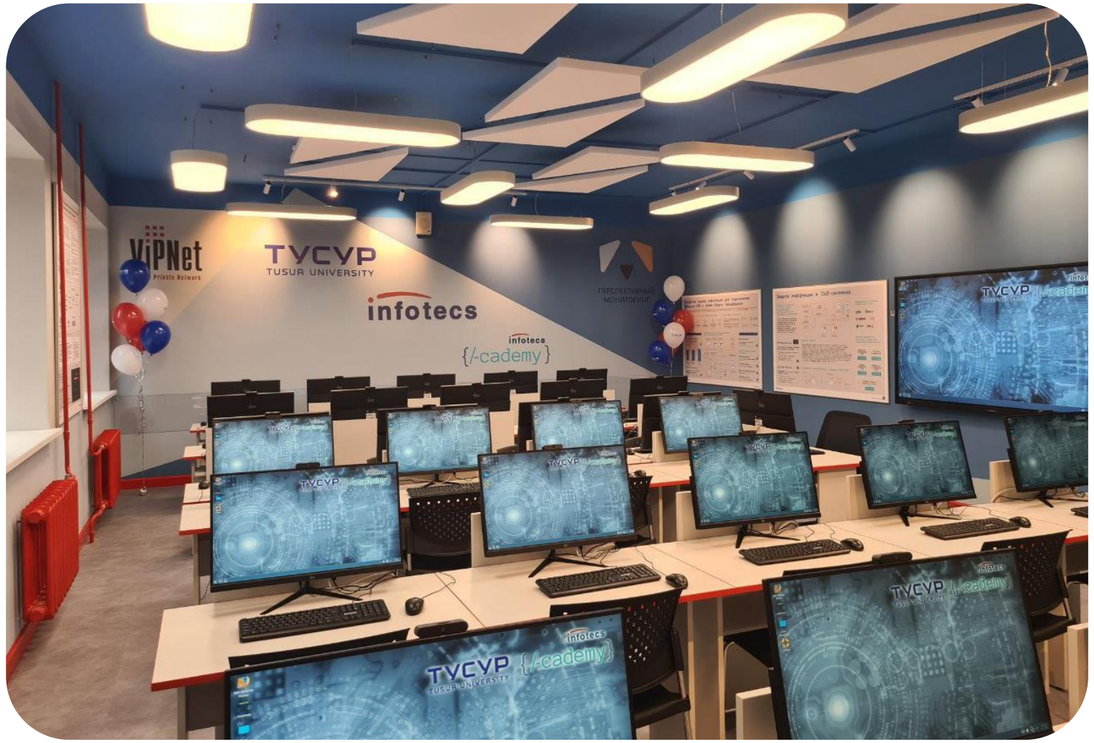
1) Стоимость атаки
2) Скорость реакции
3) Содержание реакции
4) Собственный опыт
5) Планы и изменения

13

киберполигонов

AMPIRE

«Лаборатория КИИ» в ТУСУР



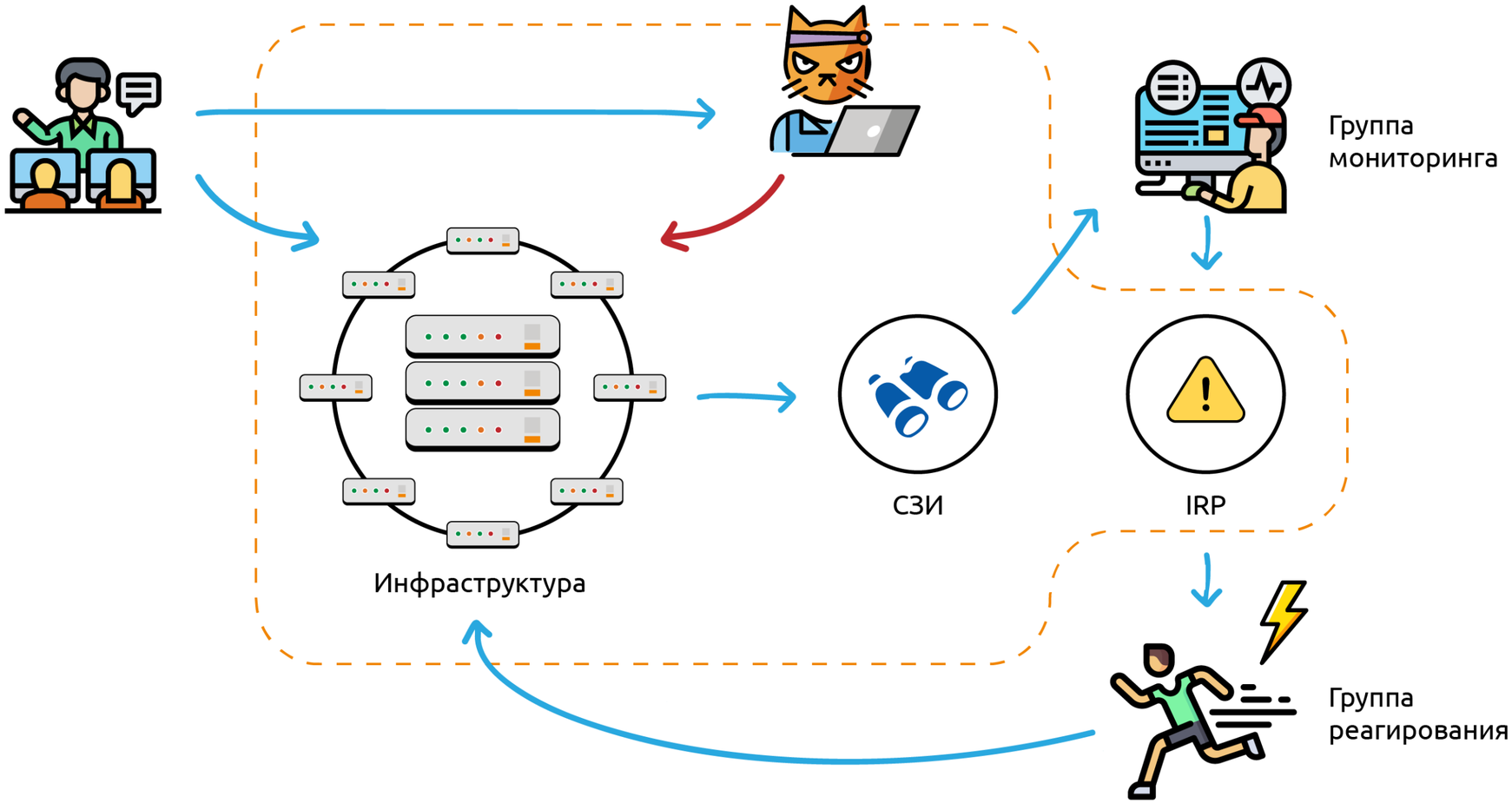
Киберполигон МТУСИ

300

киберучений

AMPIRE

Киберучения Blue Team



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Что же новенького в 1.2

Рефакторинг

Что согласовала PR-служба

Применили лучшие архитектурные паттерны

Повышена стабильность и безопасность

Тыдуракштоле?!!! У нас всегда идеальный код! Удали!

Разработали программный интерфейс для маркетплейса контента

Что хотел сказать я

Убрали кучу костылей, проще добавлять фичи

Вебсокеты почти не отваливаются!
F5 не нужна!

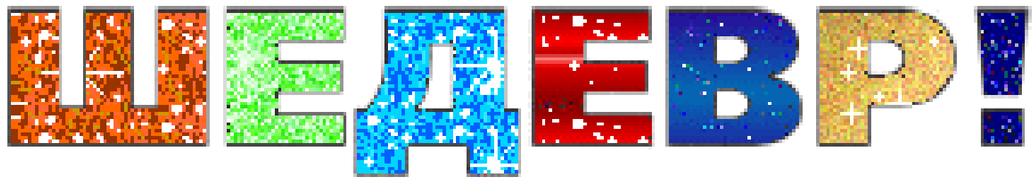
Исправили 600 багов

Новая админка, можно самим загружать шаблоны и сценарии

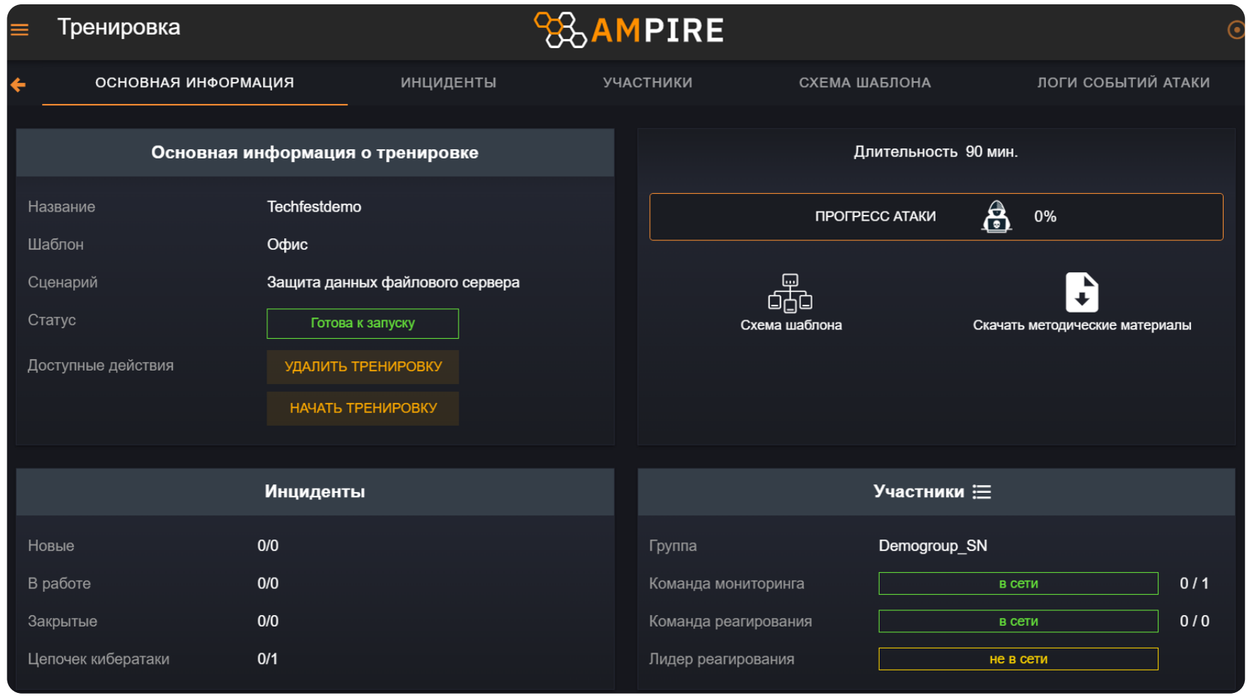
+ 1 гипервизор

- Open-source
- KVM-подобный
- Существует 15 лет
- Активно обновляется

Мгновение шок-контента ☺

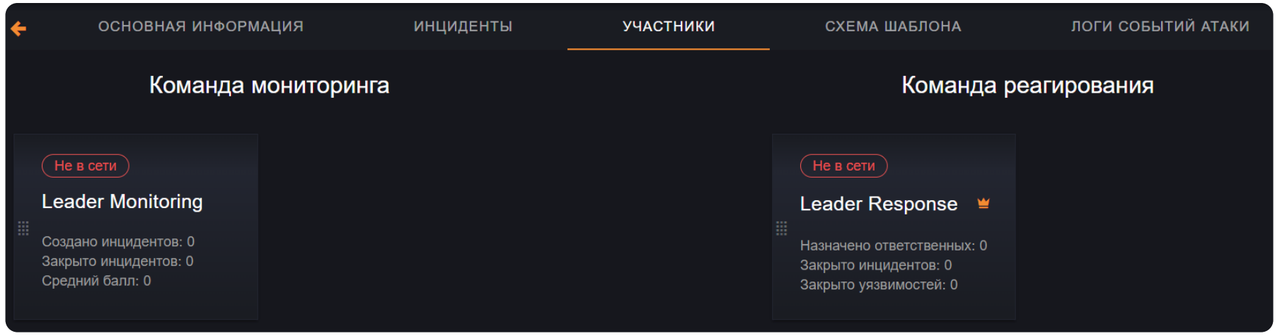


Новый дизайн



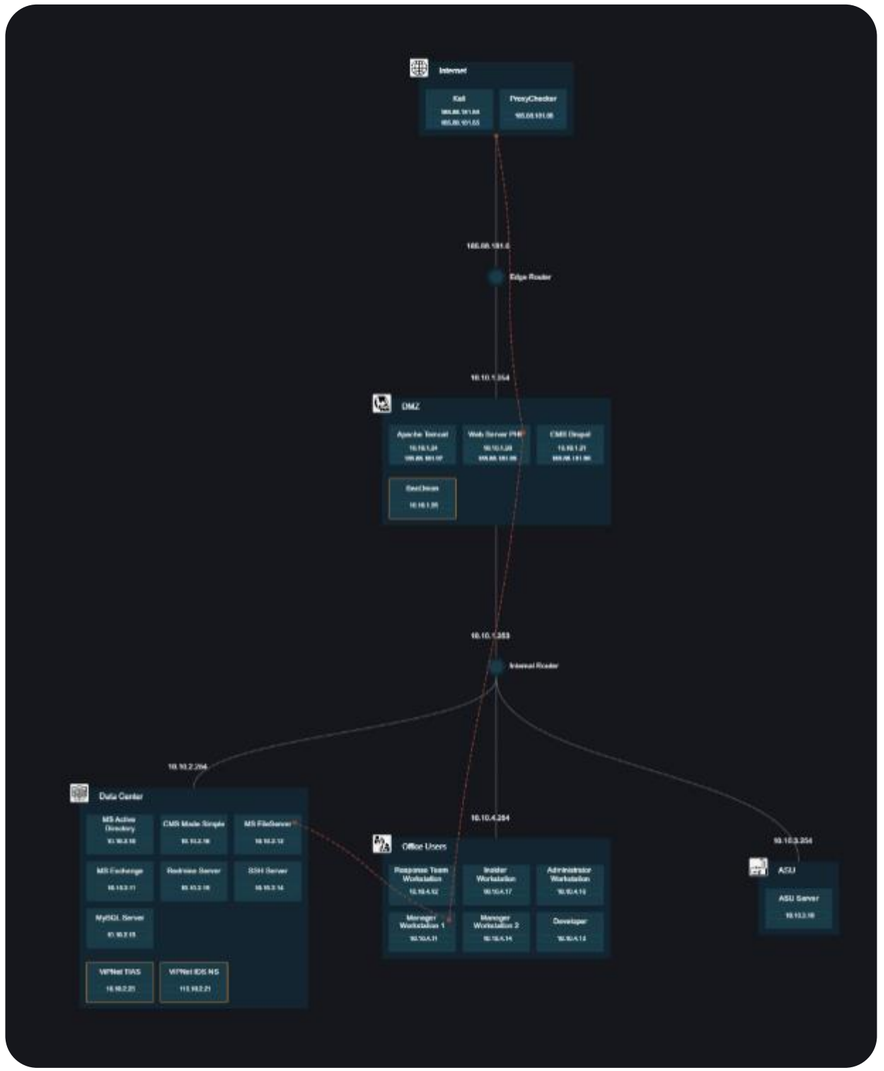
- Единый стиль внешнего вида платформы
- Стандартизированные палитры, шрифты, стили

Новая страница участников



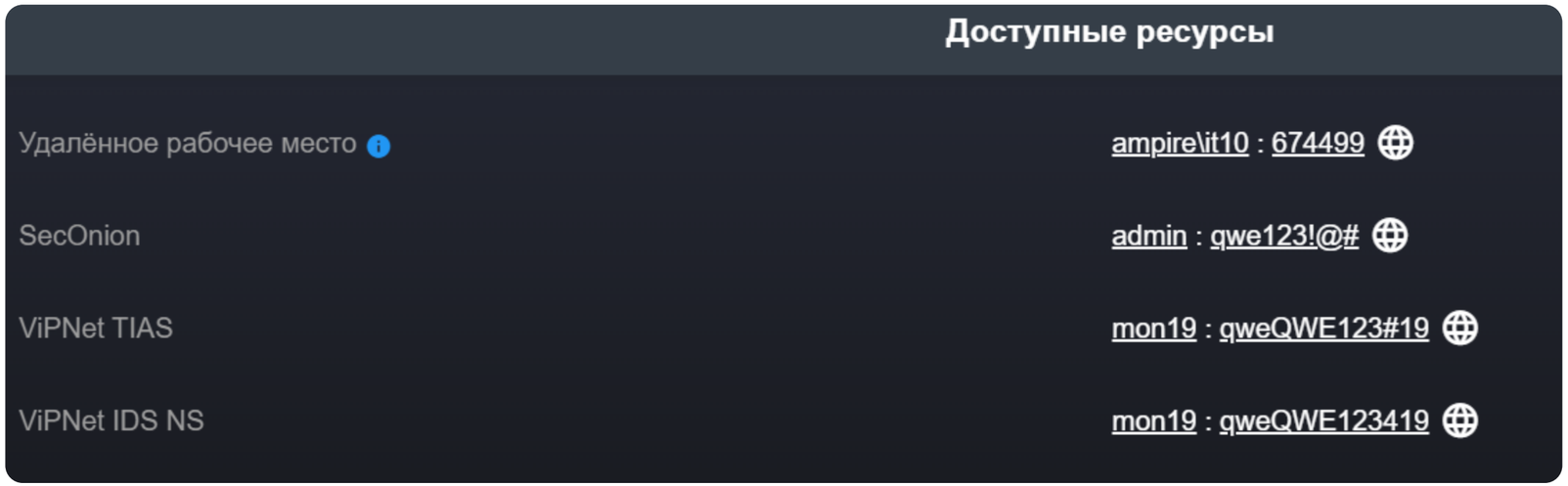
Улучшен опыт создания и редактирования новых пользователей, стандартизированы названия полей в профиле и в карточке пользователя.

Новая схема сети



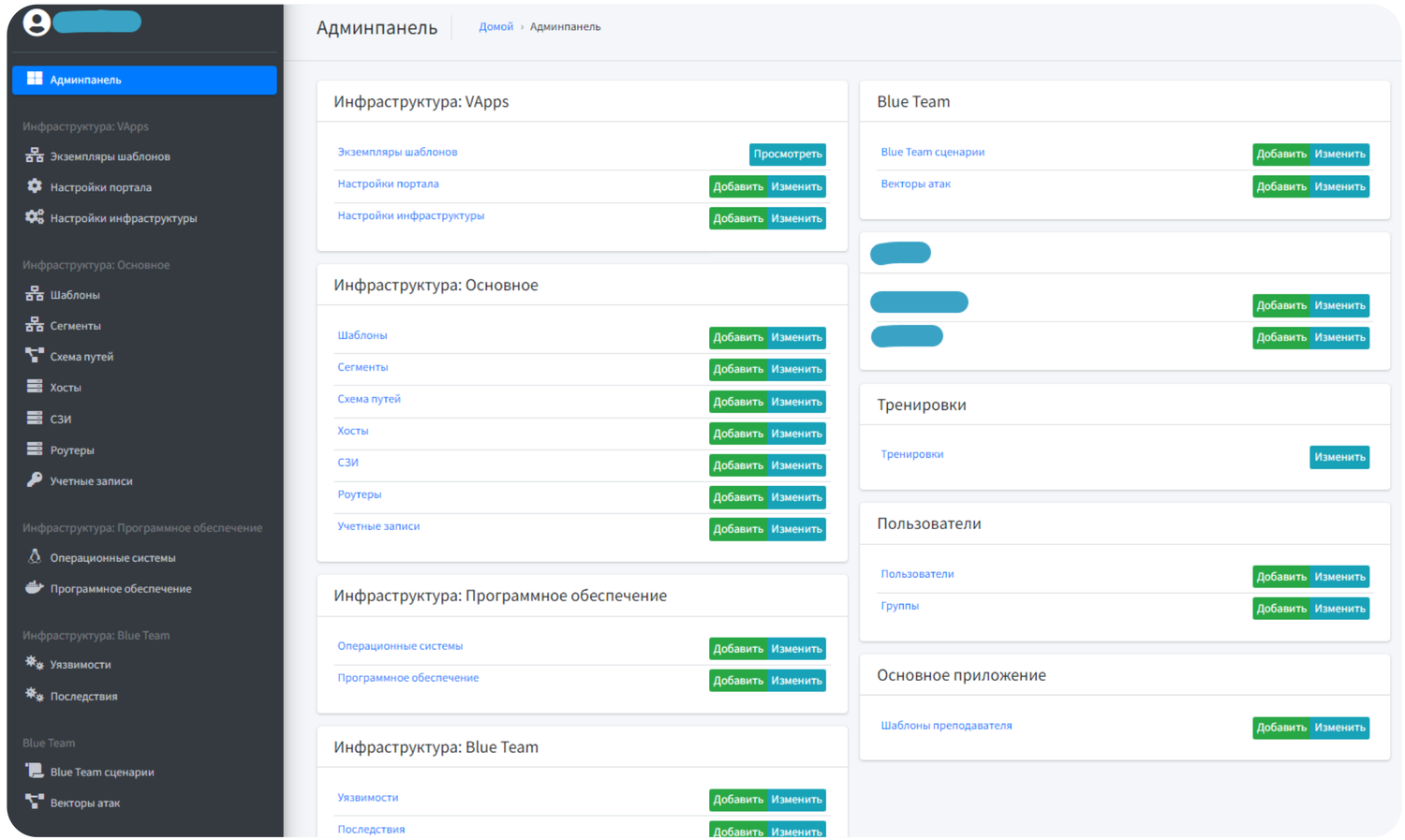
- Интерактивная схема
- Анимированный вектор атаки
- Дополнительная информация по узлам

Удобство для участников



- Креды выдаются в интерфейс
- Креды копируются в буфер
- Все доступные ресурсы — кликабельны

Административная панель



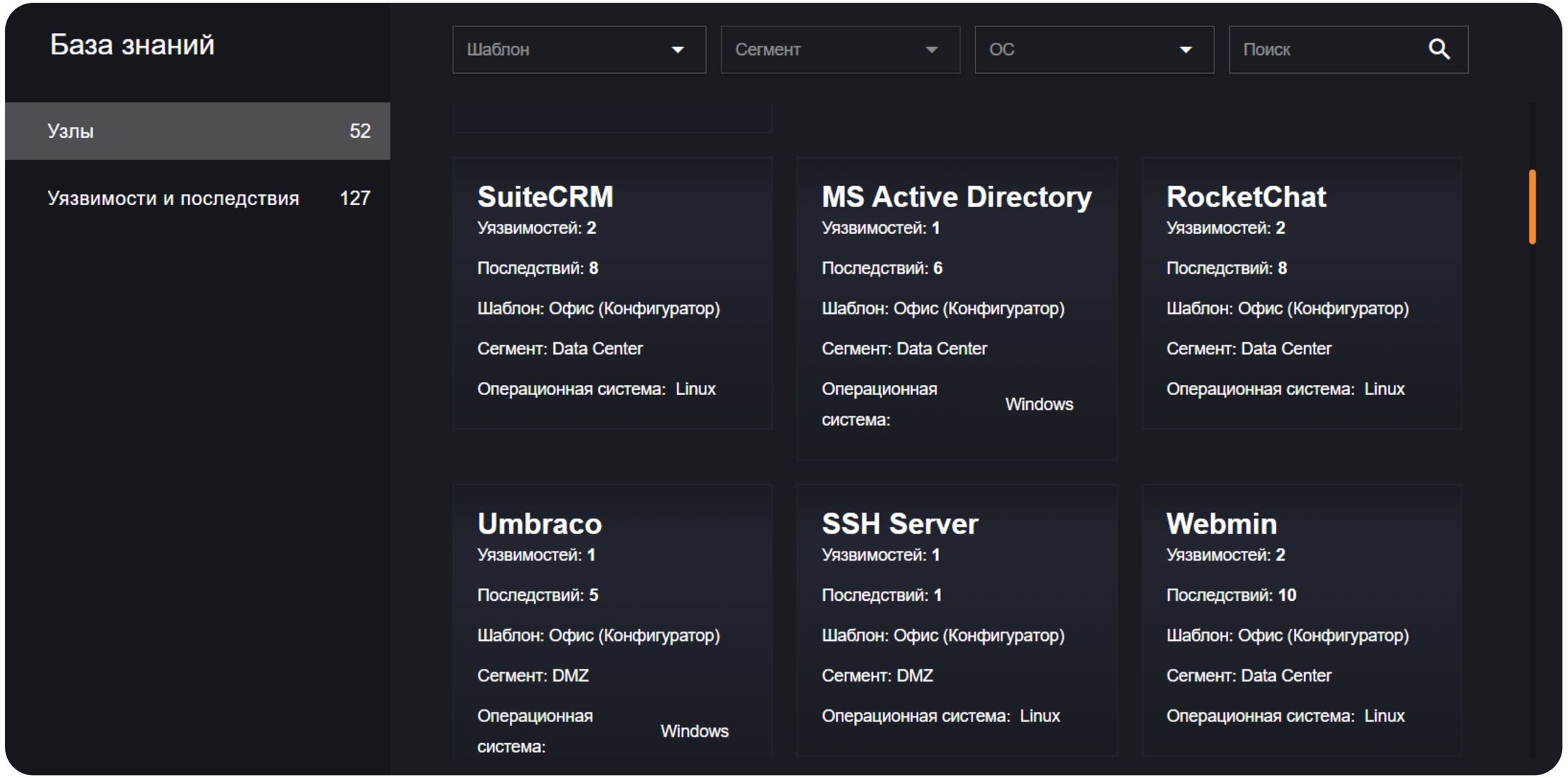
- Теперь две роли — разработчик и администратор
- Разработчик имеет неограниченный доступ по всем панелям для работы и отладки
- Администратор может только развернуть и запустить комплекс

Новые типы нарушителя

Внутренний

Заражённый хост

База знаний


База знаний
Шаблон
Сегмент
ОС
Поиск
Узлы 52
Уязвимости и последствия 127
SuiteCRM
Уязвимостей: 2
Последствий: 8
Шаблон: Офис (Конфигуратор)
Сегмент: Data Center
Операционная система: Linux
MS Active Directory
Уязвимостей: 1
Последствий: 6
Шаблон: Офис (Конфигуратор)
Сегмент: Data Center
Операционная система: Windows
RocketChat
Уязвимостей: 2
Последствий: 8
Шаблон: Офис (Конфигуратор)
Сегмент: Data Center
Операционная система: Linux
Umbraco
Уязвимостей: 1
Последствий: 5
Шаблон: Офис (Конфигуратор)
Сегмент: DMZ
Операционная система: Windows
SSH Server
Уязвимостей: 1
Последствий: 1
Шаблон: Офис (Конфигуратор)
Сегмент: DMZ
Операционная система: Linux
Webmin
Уязвимостей: 2
Последствий: 10
Шаблон: Офис (Конфигуратор)
Сегмент: Data Center
Операционная система: Linux

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Через 2 месяца
в версии 1.3

Red Team

Первая RedTeam тренировка

Время

00:38:56

Прогресс атаки

10%

Статус

Активна

Доступные действия

Остановить

Конфигурация

Шаблон	РедТим шаблон
Сценарий	РедТим сценарий с длинным названием
Группа	РедТим группа

Методические материалы

ОБЩАЯ ИНФОРМАЦИЯ | ОТЧЕТЫ | СХЕМА ШАБЛОНА

Задания

Статус | Искать

Подмена файла обновления на сервере WSUS
Выполнено
Выполнил
Петров Петр
Открыть

Подмена файла обновления на сервере WSUS
Выполняется
Время выполнения
00:15:37
Участники | Открыть

Подмена файла обновления на сервере WSUS
Нет участников
Участники | Открыть

Подмена файла обновления на сервере WSUS
Выполняется
Время выполнения
00:15:37
Участники | Открыть

Статистика

Заданий выполнено	2 / 5
Отчетов сформировано	0 / 2

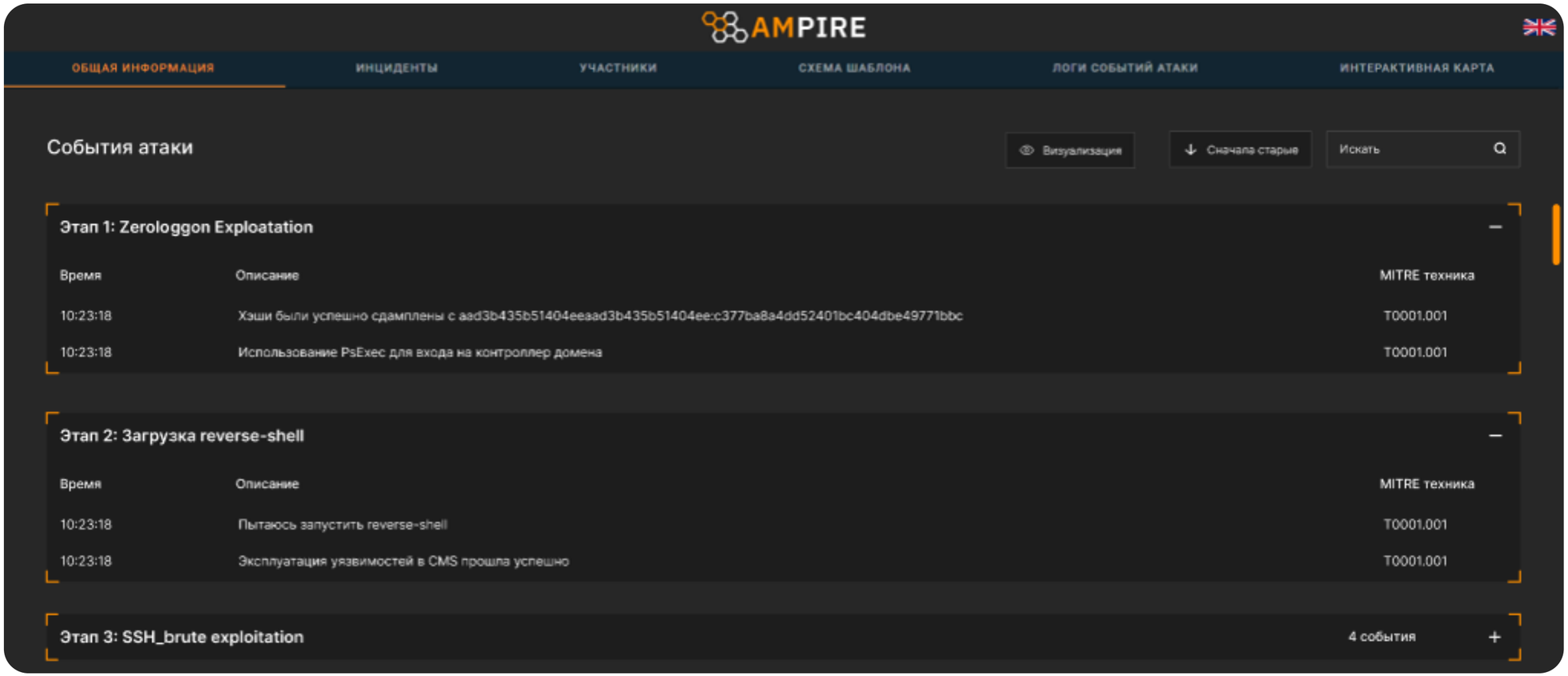
Доступные ресурсы

VipNet IDS NS	127.0.0.1
VipNet IDS NS	127.0.0.1
VipNet IDS NS	127.0.0.1

Топ участников

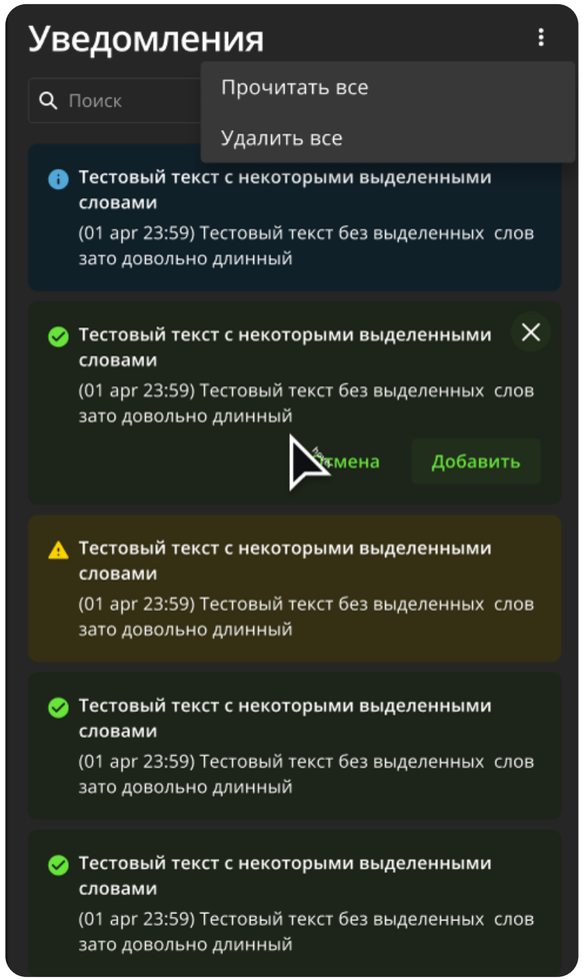
Участник	Выполнил	Участвовал
Петров Петр	1	4
Петров Петр	1	4
Петров Петр	1	4
Петров Петр	1	4
Петров Петр	1	4

MITRE ATT&CK



- Оттегированы действия нарушителя.
- Переработана карточка Cyber Kill Chain (если указанные техники совпадают с эталонными, то считаем, что обучаемый молодец)

Новый Центр уведомлений



- Все уведомления в одном месте, без ограничения времени показа
- Существующие пуши сохранятся

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

t.me/pm_public

amonitoring.ru

Сергей Нейгер

Директор по развитию бизнеса,
«Перспективный мониторинг»

+7 (495) 737-61-97

Sergey.Neyger@amonitoring.ru