AMPIRE

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

По следам ТехноФеста: разбираем сценарий атаки на киберполигоне AMPIRE

Вебинар 19 сентября 2019 г.

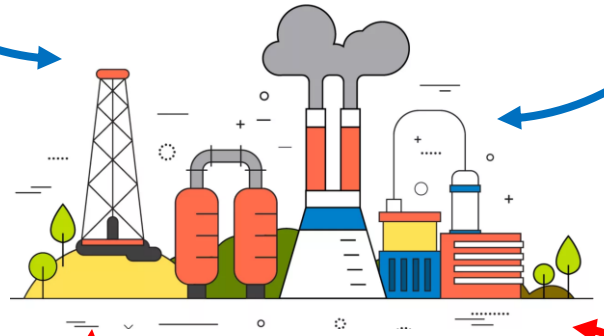
Пушкин Александр, Технический директор ЗАО ПМ

План вебинара

- Организация киберучений
- Рабочие материалы
- Разбор сценария атаки

Часть 1

Первые практические киберучения



AMPIRE

Практика – залог умения, хм

AMPIRE TEAM

Костюлин Илья

Овчинникова Александра

Худой Юрий

Овчинников Сергей

Пушкин Александр

Цели киберучений

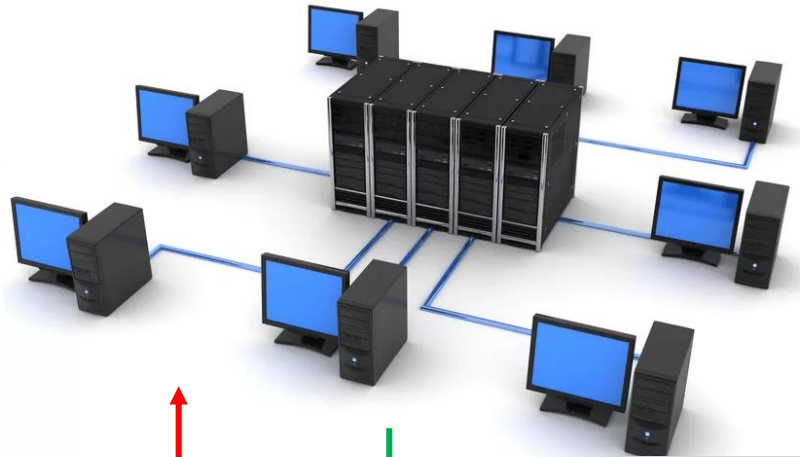
- Создать собственный SOC
- Научиться выявлять компьютерные атаки
- Наладить взаимодействие между подразделениями
- Устранить существующие уязвимости

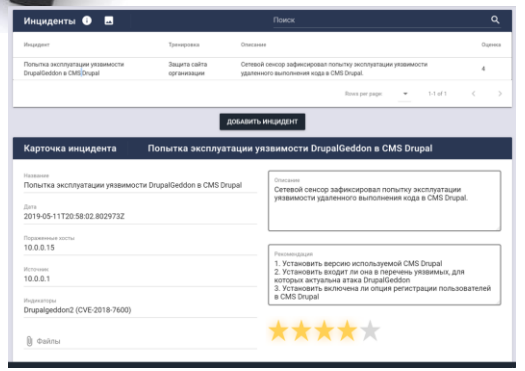
Тайминг

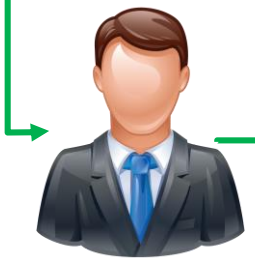
Раунд №1. Защита баз данных предприятия 10:30 - 12:30	10:30 - 10:45	Вводная часть. Назначение, цели и задачи Ampire. Организация киберучений
	10:45 - 12:15	Прохождение сценария
	12:15 - 12:30	Подведение итогов. Награждение участников

Тайминг

Раунд №2. Защита баз данных предприятия 10:30 - 12:30	13:30 - 13:45	Вводная часть. Назначение, цели и задачи Ampire. Организация киберучений
	13:45 - 15:15	Прохождение сценария
	15:15 - 15:30	Подведение итогов. Награждение участников

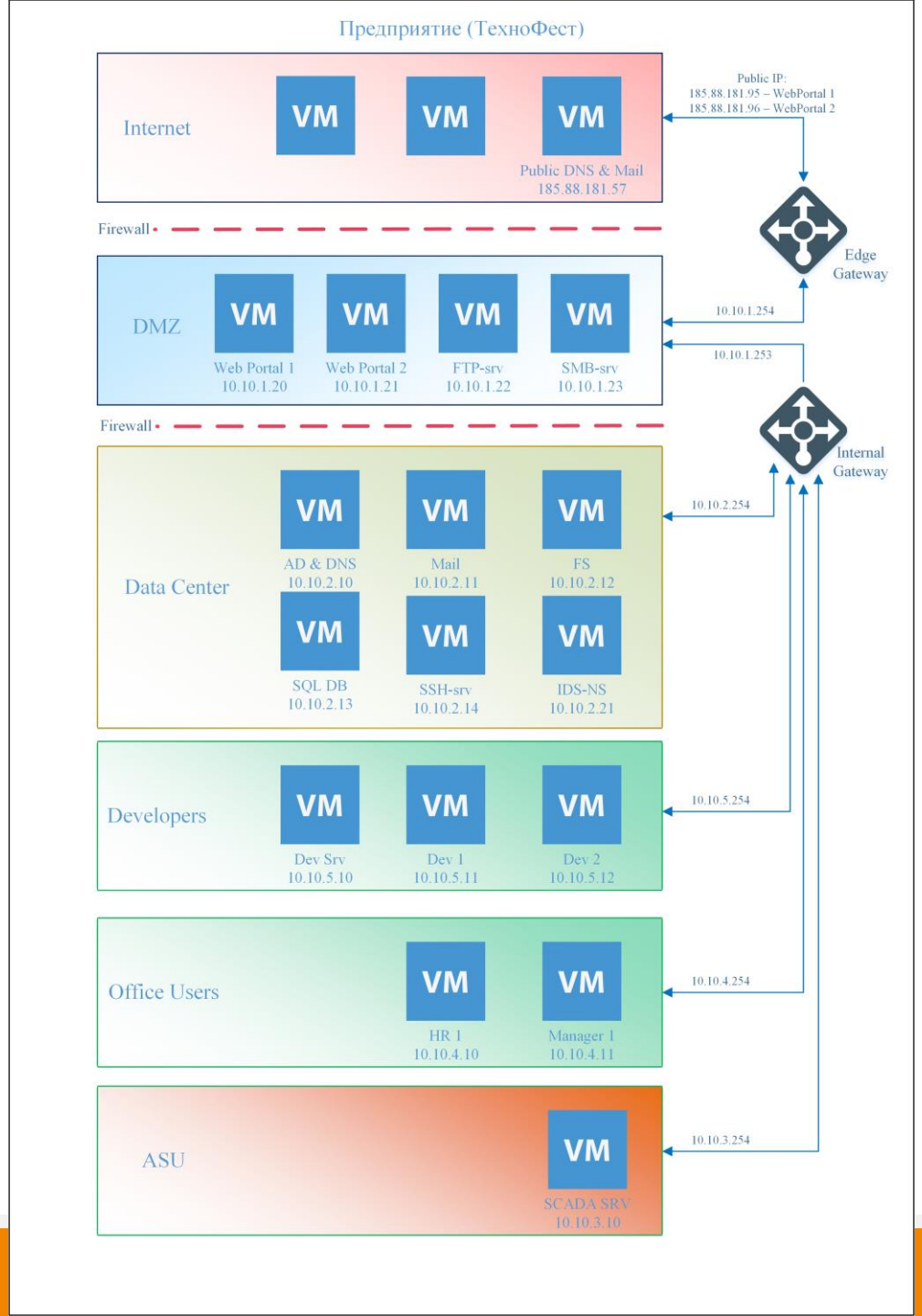






Группа мониторинга

Группа реагирования


Предприятие (ТехноФест)
Internet
VM
VM
VM
Public DNS & Mail
185.88.181.57
Public IP:
185.88.181.95 – WebPortal 1
185.88.181.96 – WebPortal 2
Firewall
Edge
Gateway
DMZ
VM
VM
VM
VM
Web Portal 1
10.10.1.20
Web Portal 2
10.10.1.21
FTP-srv
10.10.1.22
SMB-srv
10.10.1.23
10.10.1.254
10.10.1.253
Firewall
Internal
Gateway
Data Center
VM
VM
VM
AD & DNS
10.10.2.10
Mail
10.10.2.11
FS
10.10.2.12
VM
VM
VM
SQL DB
10.10.2.13
SSH-srv
10.10.2.14
IDS-NS
10.10.2.21
10.10.2.254
Developers
VM
VM
VM
Dev Srv
10.10.5.10
Dev 1
10.10.5.11
Dev 2
10.10.5.12
10.10.5.254
Office Users
VM
VM
HR 1
10.10.4.10
Manager 1
10.10.4.11
10.10.4.254
ASU
VM
SCADA SRV
10.10.3.10
10.10.3.254

Сценарий

Группа мониторинга

1. *Участник 1*
2. *Участник 2*
3. *Участник 3*
4. *Участник 4*

Анализ событий ИБ

Заведение карточек инцидентов

Описание вектора атаки (Cyber Kill Chain)

Группа реагирования

1. ***Участник 1***
2. *Участник 2*
3. *Участник 3*
4. *Участник 4*

Расследование инцидентов

Устранение уязвимостей

Время начала тренировки	30.08.2019, 13:03:07
Время окончания тренировки	30.08.2019, 14:13:07

Шаблон	Шаблон Предприятие
Сценарий	Предприятие. Сценарий 1
Группа	Группа Д1

2 / 2

0 / 3

50 / 100

98%

Vuln

Vuln3

Vuln2

Автор	Инцидент	Оценка
Александр Верзин	Перебор паролей к SSH-серверу	★ ★ ★ ☆ ☆
Михаил Ананьев	Попытка SQL-инъекции	★ ★ ★ ★ ☆

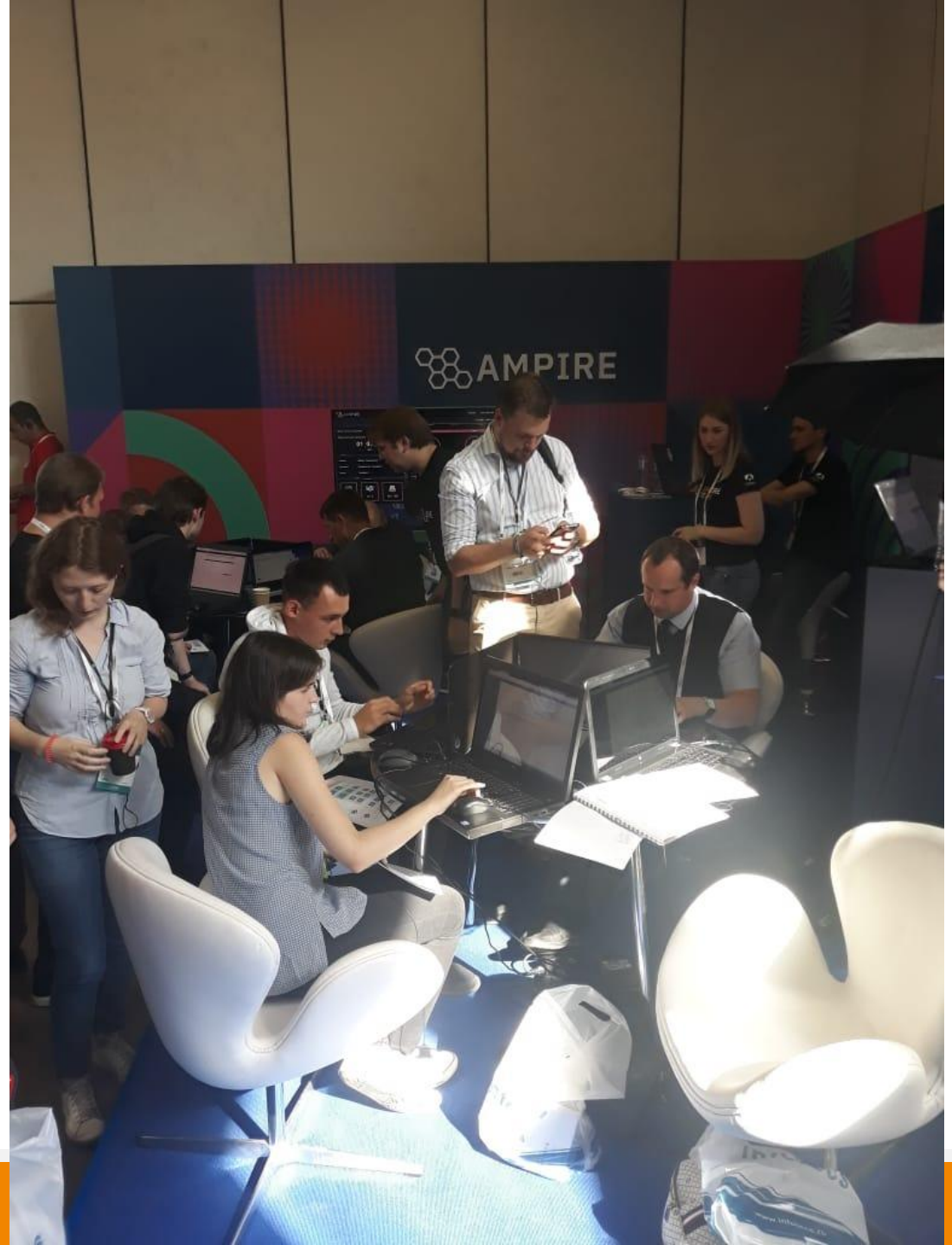
Методические материалы

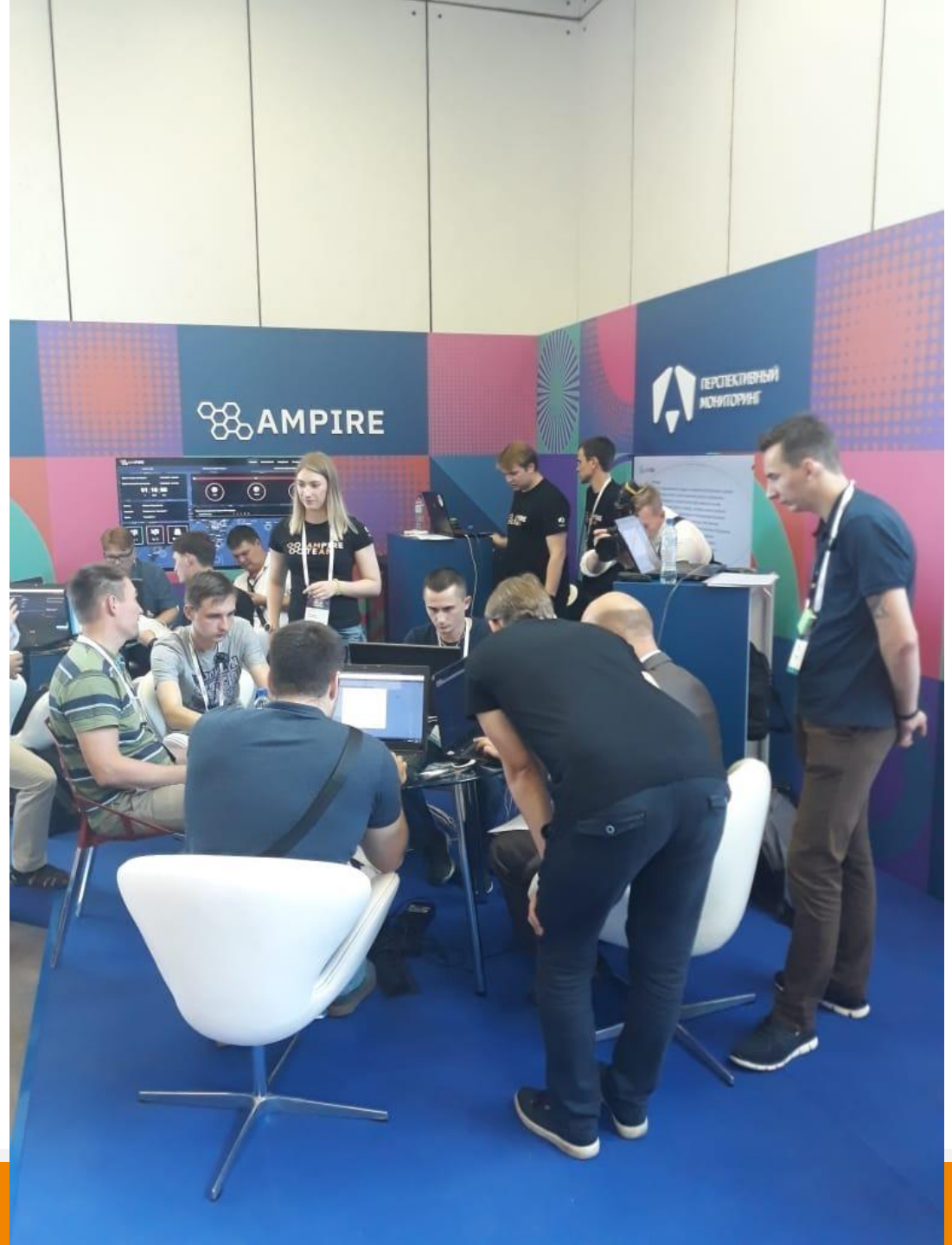
- Руководство пользователя ViPNet IDS NS
- Логическая схема корпоративной сети предприятия
- Параметры доступа к Ampire
- Легенда

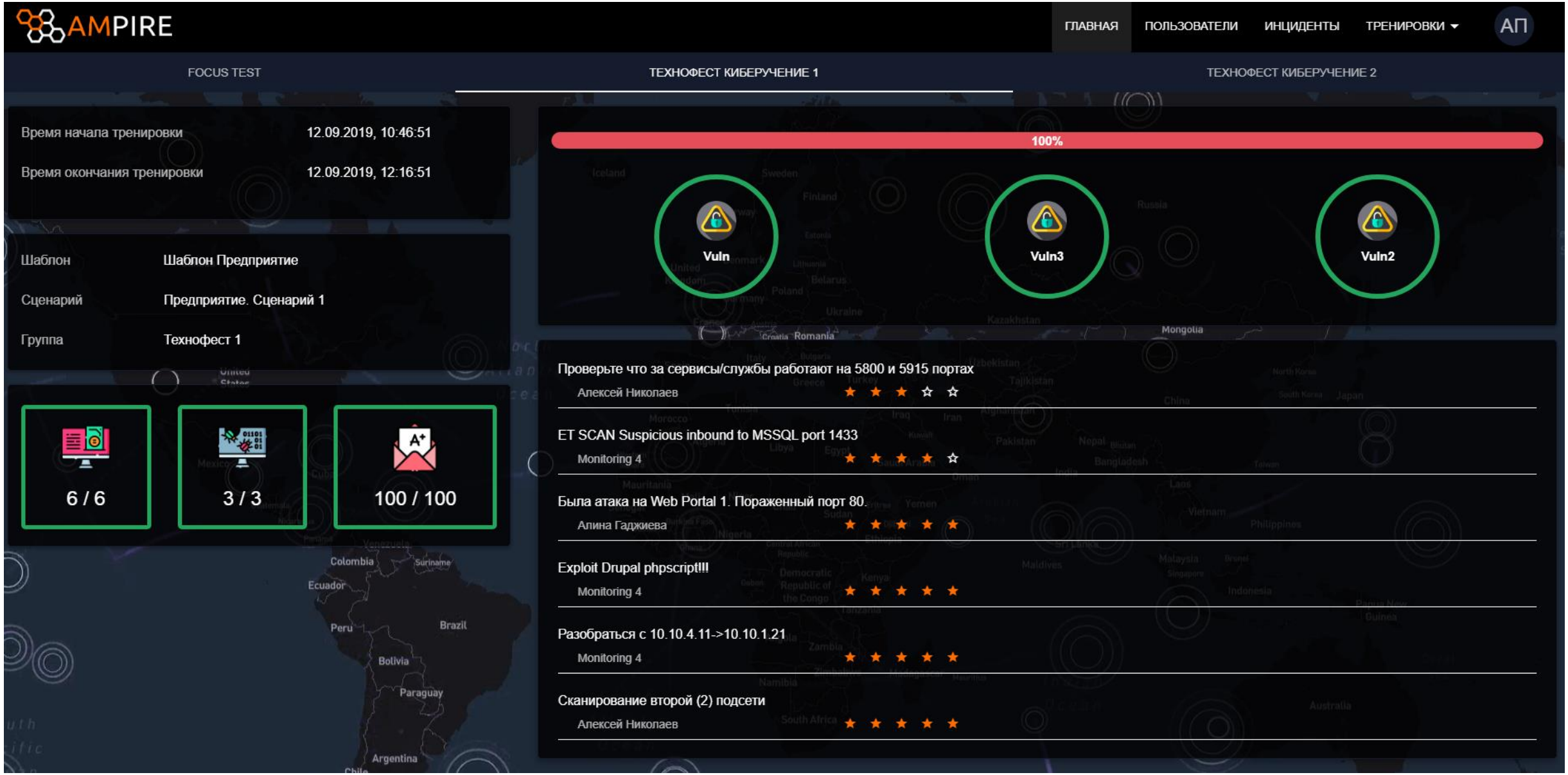
Легенда:
Внешний злоумышленник находит в интернете сайт Компании и решает провести атаку на него с целью получения доступа к внутренним ресурсам. Обнаружив и проэксплуатировав уязвимость на нем, нарушитель получает доступ к серверу, который помимо основной информационной задачи предоставляет пользователям Компании инструмент для генерации отчетов. С помощью этого вектора нарушитель пробует получить доступ на рабочие машины сотрудников. Главная цель – сделать дамп корпоративной базы данных. Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

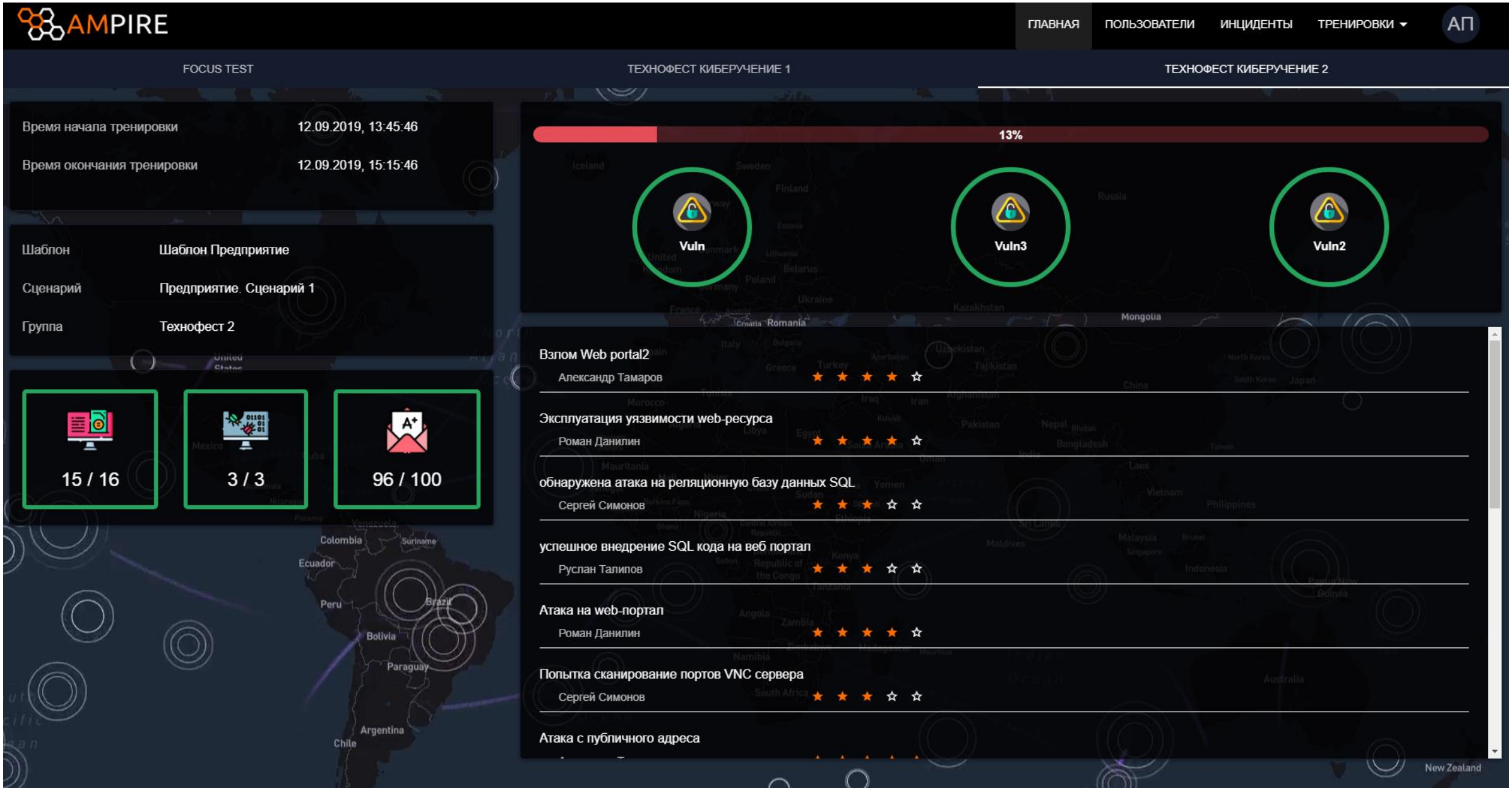
Часть 2

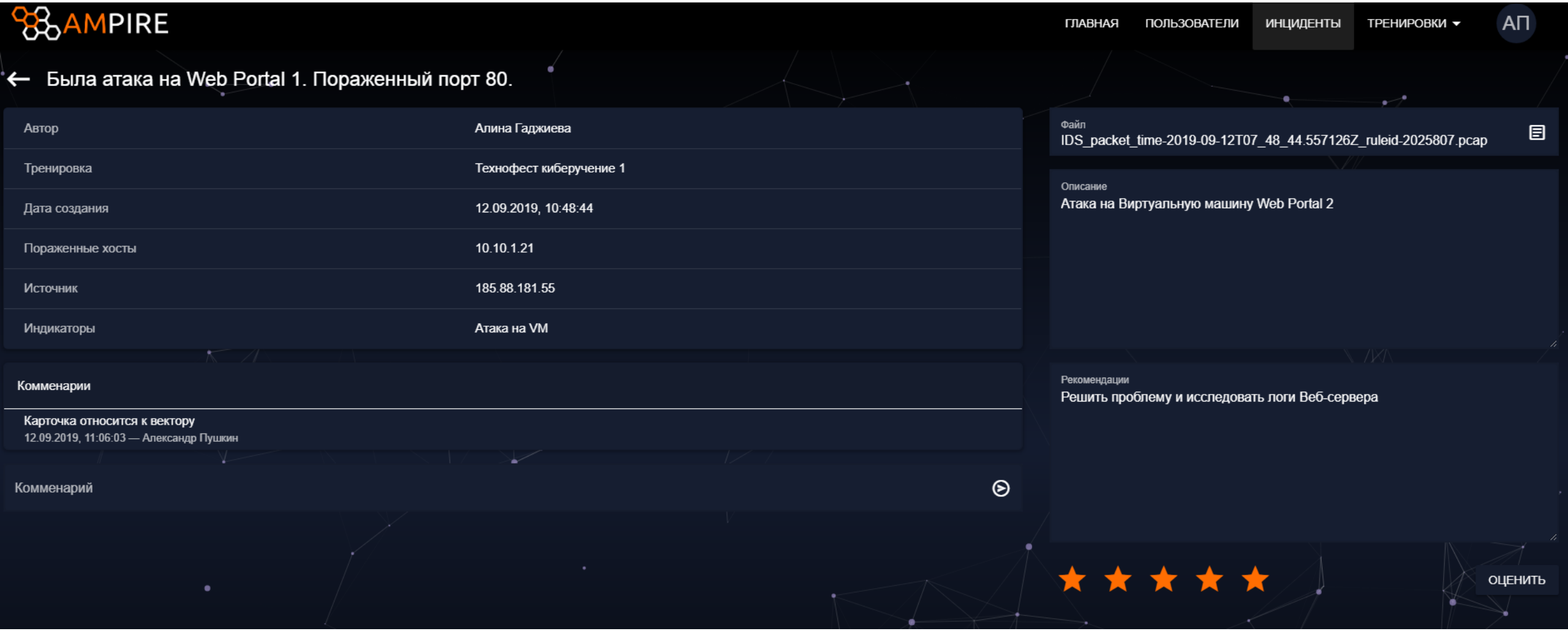

AMPIRE
ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

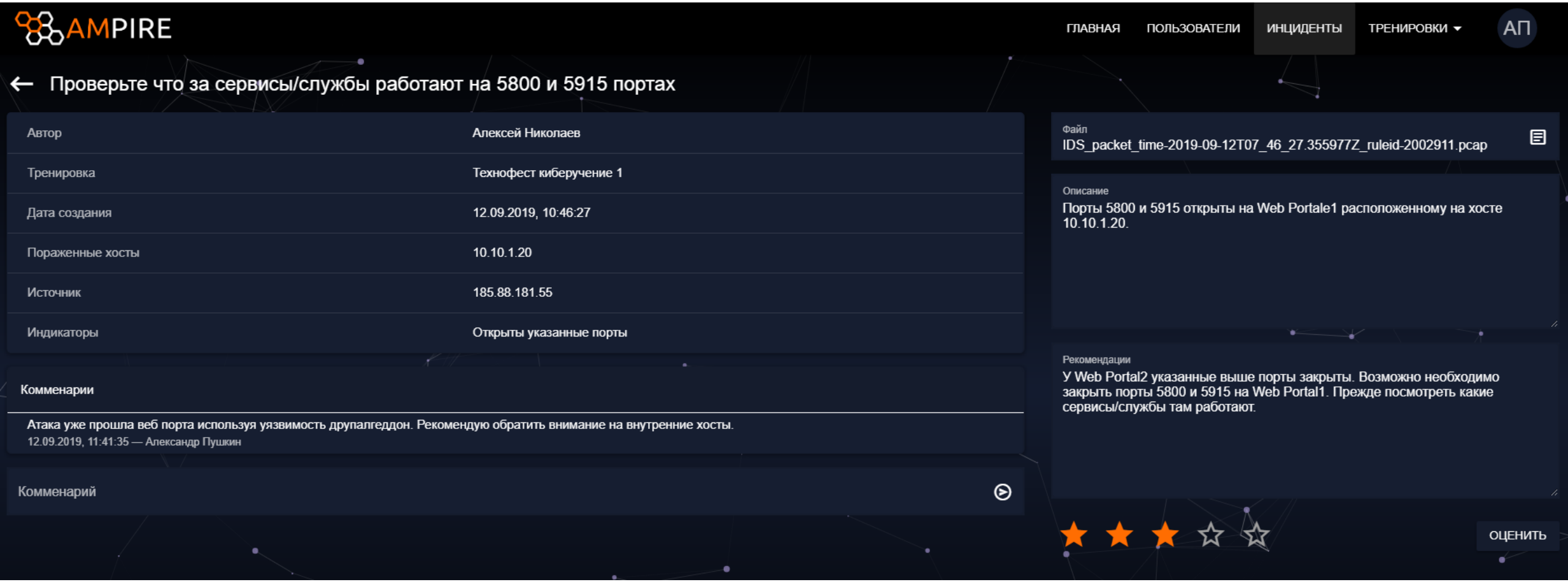

AMPIRE

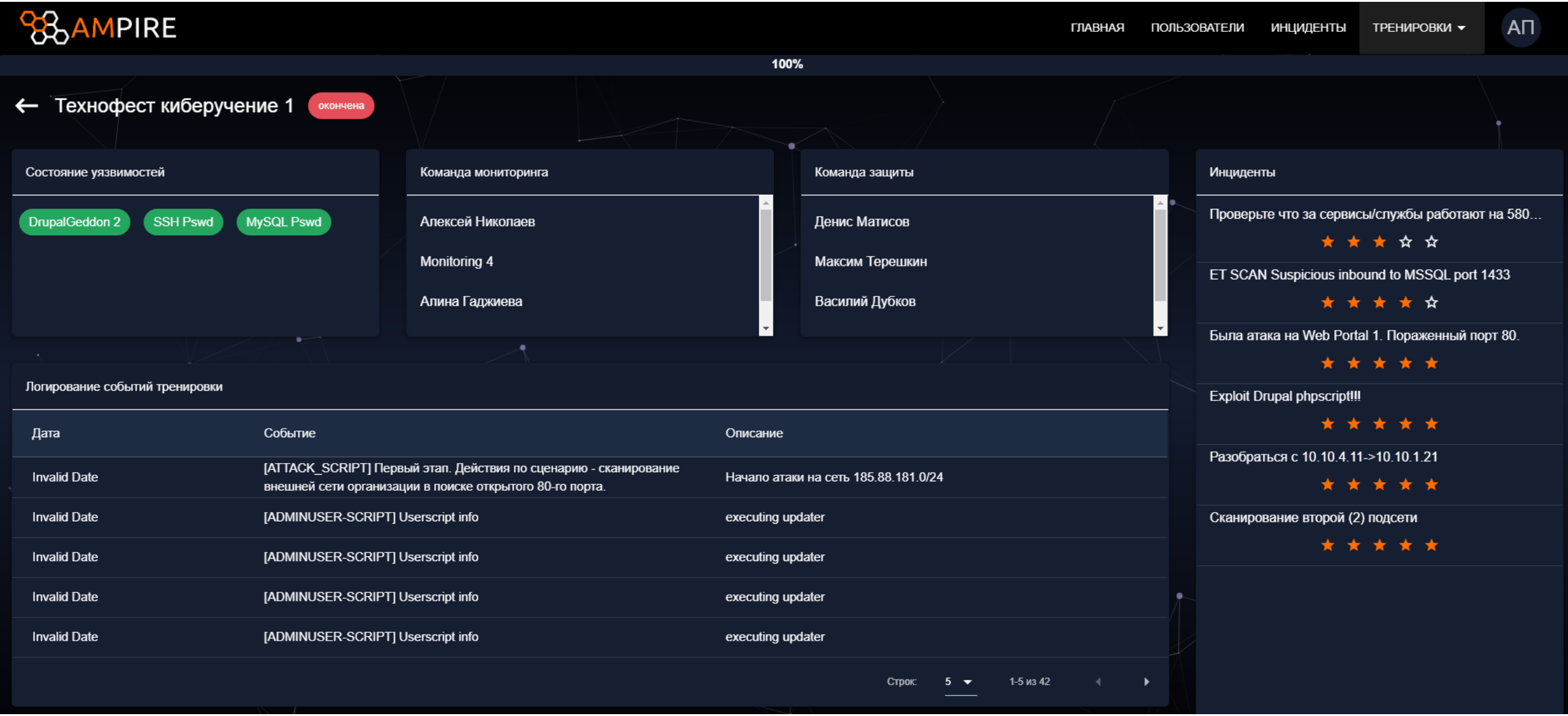

AMPIRE
ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ


AMPIRE
ГЛАВНАЯ
ПОЛЬЗОВАТЕЛИ
ИНЦИДЕНТЫ
ТРЕНИРОВКИ
АП
FOCUS TEST
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 1
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 2
Время начала тренировки 12.09.2019, 10:46:51
Время окончания тренировки 12.09.2019, 12:16:51
Шаблон Шаблон Предприятие
Сценарий Предприятие. Сценарий 1
Группа Технофест 1
6 / 6
3 / 3
100 / 100
100%
Vuln
Vuln3
Vuln2
Проверьте что за сервисы/службы работают на 5800 и 5915 портах
Алексей Николаев
ET SCAN Suspicious inbound to MSSQL port 1433
Monitoring 4
Была атака на Web Portal 1. Пораженный порт 80.
Алина Гаджиева
Exploit Drupal phpscript!!!
Monitoring 4
Разобраться с 10.10.4.11->10.10.1.21
Monitoring 4
Сканирование второй (2) подсети
Алексей Николаев

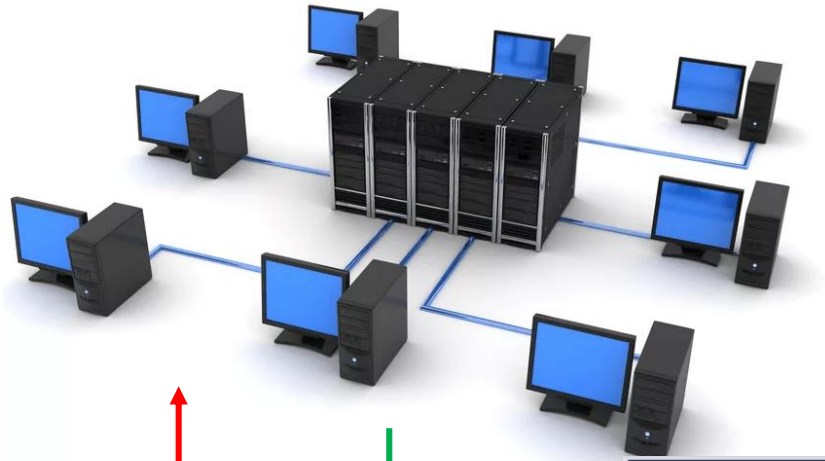

AMPIRE
ГЛАВНАЯ
ПОЛЬЗОВАТЕЛИ
ИНЦИДЕНТЫ
ТРЕНИРОВКИ
АП
FOCUS TEST
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 1
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 2
Время начала тренировки
12.09.2019, 13:45:46
Время окончания тренировки
12.09.2019, 15:15:46
Шаблон
Шаблон Предприятие
Сценарий
Предприятие. Сценарий 1
Группа
Технофест 2
15 / 16
3 / 3
96 / 100
13%
Vuln
Vuln3
Vuln2
Взлом Web portal2
Александр Тамаров
Эксплуатация уязвимости web-ресурса
Роман Данилин
обнаружена атака на реляционную базу данных SQL
Сергей Симонов
успешное внедрение SQL кода на веб портал
Руслан Талипов
Атака на web-портал
Роман Данилин
Попытка сканирование портов VNC сервера
Сергей Симонов
Атака с публичного адреса
Colombia
Suriname
Ecuador
Peru
Brazil
Bolivia
Paraguay
Argentina
Chile
Mongolia
New Zealand

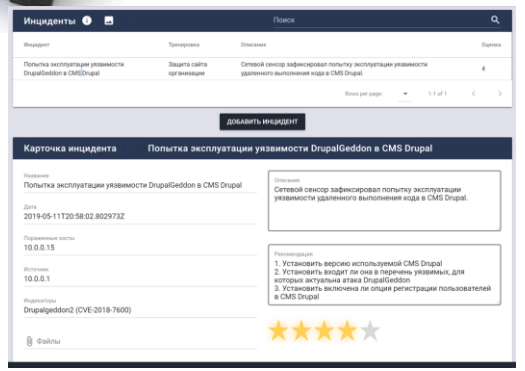

AMPIRE
ГЛАВНАЯ
ПОЛЬЗОВАТЕЛИ
ИНЦИДЕНТЫ
ТРЕНИРОВКИ
АП
Была атака на Web Portal 1. Пораженный порт 80.
Автор
Алина Гаджиева
Тренировка
Технофест киберучение 1
Дата создания
12.09.2019, 10:48:44
Пораженные хосты
10.10.1.21
Источник
185.88.181.55
Индикаторы
Атака на VM
Комменарии
Карточка относится к вектору
12.09.2019, 11:06:03 — Александр Пушкин
Комменарий
Файл
IDS_packet_time-2019-09-12T07_48_44.557126Z_ruleid-2025807.pcap
Описание
Атака на Виртуальную машину Web Portal 2
Рекомендации
Решить проблему и исследовать логи Веб-сервера
ОЦЕНИТЬ


AMPIRE
ГЛАВНАЯ
ПОЛЬЗОВАТЕЛИ
ИНЦИДЕНТЫ
ТРЕНИРОВКИ
АП
Проверьте что за сервисы/службы работают на 5800 и 5915 портах
Автор
Алексей Николаев
Тренировка
Технофест киберучение 1
Дата создания
12.09.2019, 10:46:27
Пораженные хосты
10.10.1.20
Источник
185.88.181.55
Индикаторы
Открыты указанные порты
Комменарии
Атака уже прошла веб порта используя уязвимость друпалгеддон. Рекомендую обратить внимание на внутренние хосты.
12.09.2019, 11:41:35 — Александр Пушкин
Комменарий
Файл
IDS_packet_time-2019-09-12T07_46_27.355977Z_ruleid-2002911.pcap
Описание
Порты 5800 и 5915 открыты на Web Portale1 расположенному на хосте 10.10.1.20.
Рекомендации
У Web Portal2 указанные выше порты закрыты. Возможно необходимо закрыть порты 5800 и 5915 на Web Portal1. Прежде посмотреть какие сервисы/службы там работают.
ОЦЕНИТЬ


AMPIRE
ГЛАВНАЯ
ПОЛЬЗОВАТЕЛИ
ИНЦИДЕНТЫ
ТРЕНИРОВКИ
АП
100%
Технофест киберучение 1
окончена
Состояние уязвимостей
DrupalGeddon 2
SSH Pswd
MySQL Pswd
Команда мониторинга
Алексей Николаев
Monitoring 4
Алина Гаджиева
Команда защиты
Денис Матисов
Максим Терешкин
Василий Дубков
Инциденты
Проверьте что за сервисы/службы работают на 580...
ET SCAN Suspicious inbound to MSSQL port 1433
Была атака на Web Portal 1. Пораженный порт 80.
Exploit Drupal phpscript!!!
Разобраться с 10.10.4.11->10.10.1.21
Сканирование второй (2) подсети
Логирование событий тренировки
Дата
Событие
Описание
Invalid Date
[ATTACK_SCRIPT] Первый этап. Действия по сценарию - сканирование внешней сети организации в поиске открытого 80-го порта.
Начало атаки на сеть 185.88.181.0/24
Invalid Date
[ADMINUSER-SCRIPT] Userscript info
executing updater
Invalid Date
[ADMINUSER-SCRIPT] Userscript info
executing updater
Invalid Date
[ADMINUSER-SCRIPT] Userscript info
executing updater
Invalid Date
[ADMINUSER-SCRIPT] Userscript info
executing updater
Строк:
5
1-5 из 42

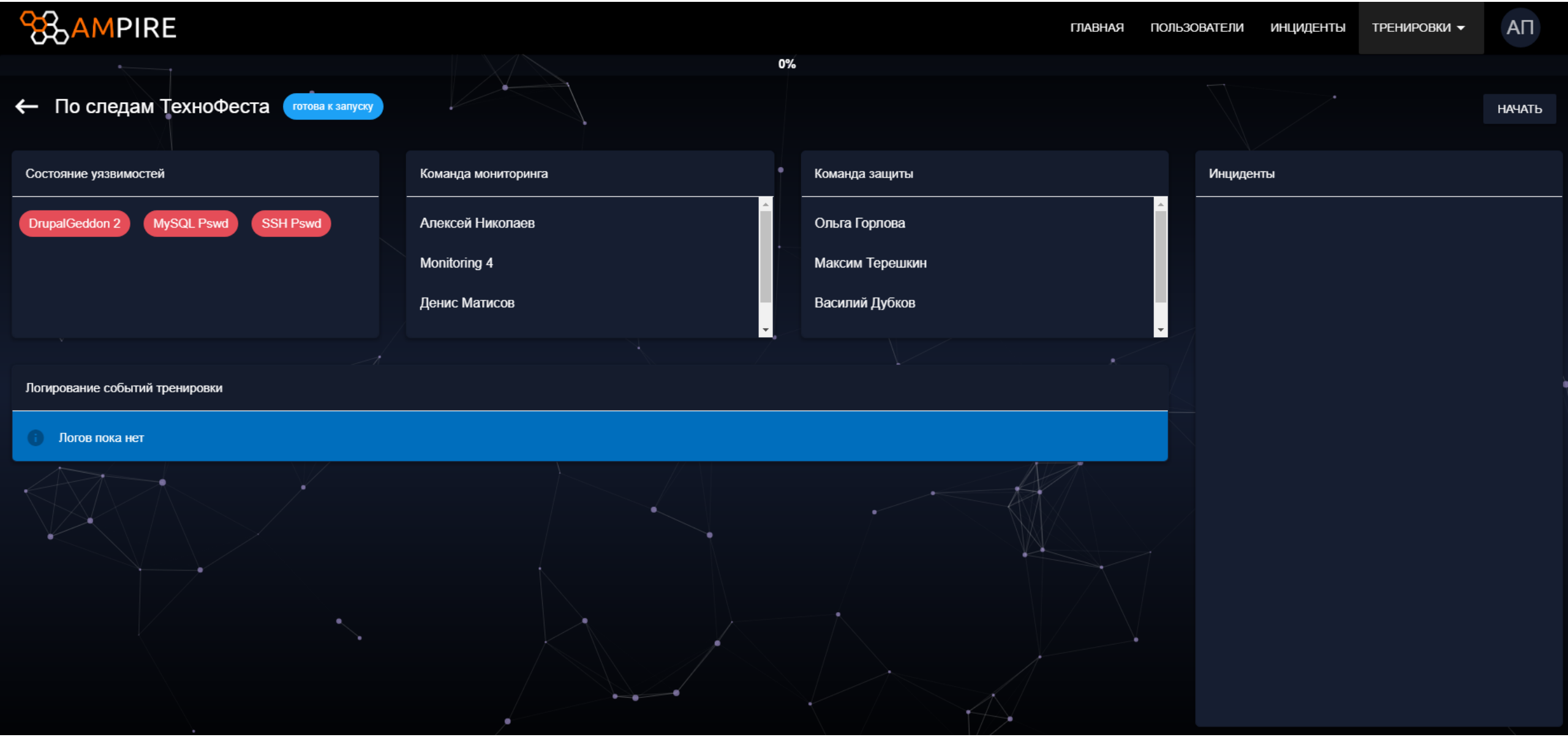
Часть 3

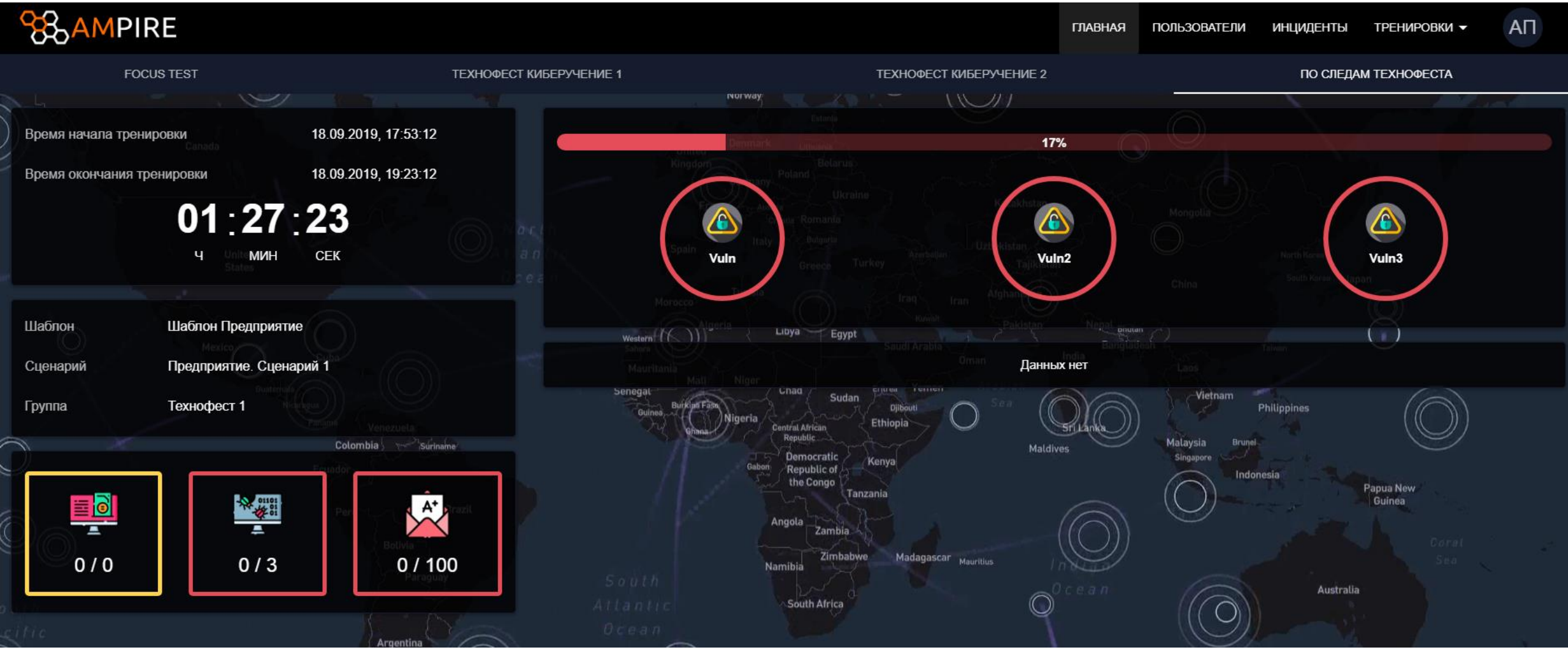


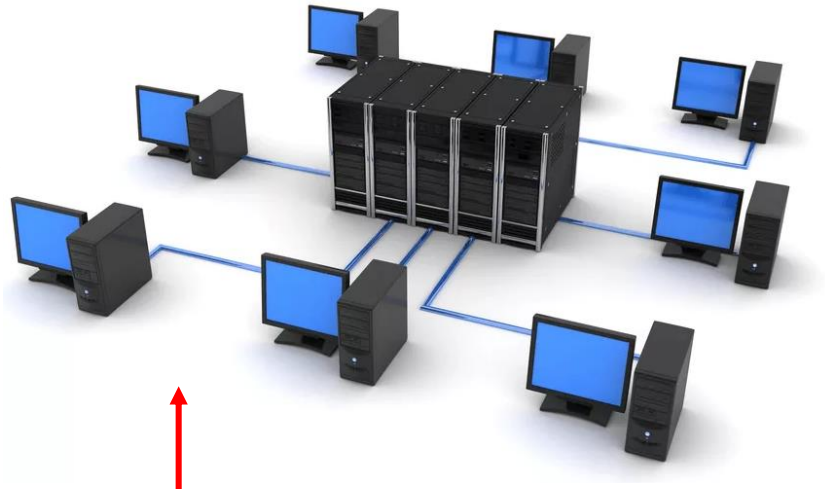


Группа мониторинга

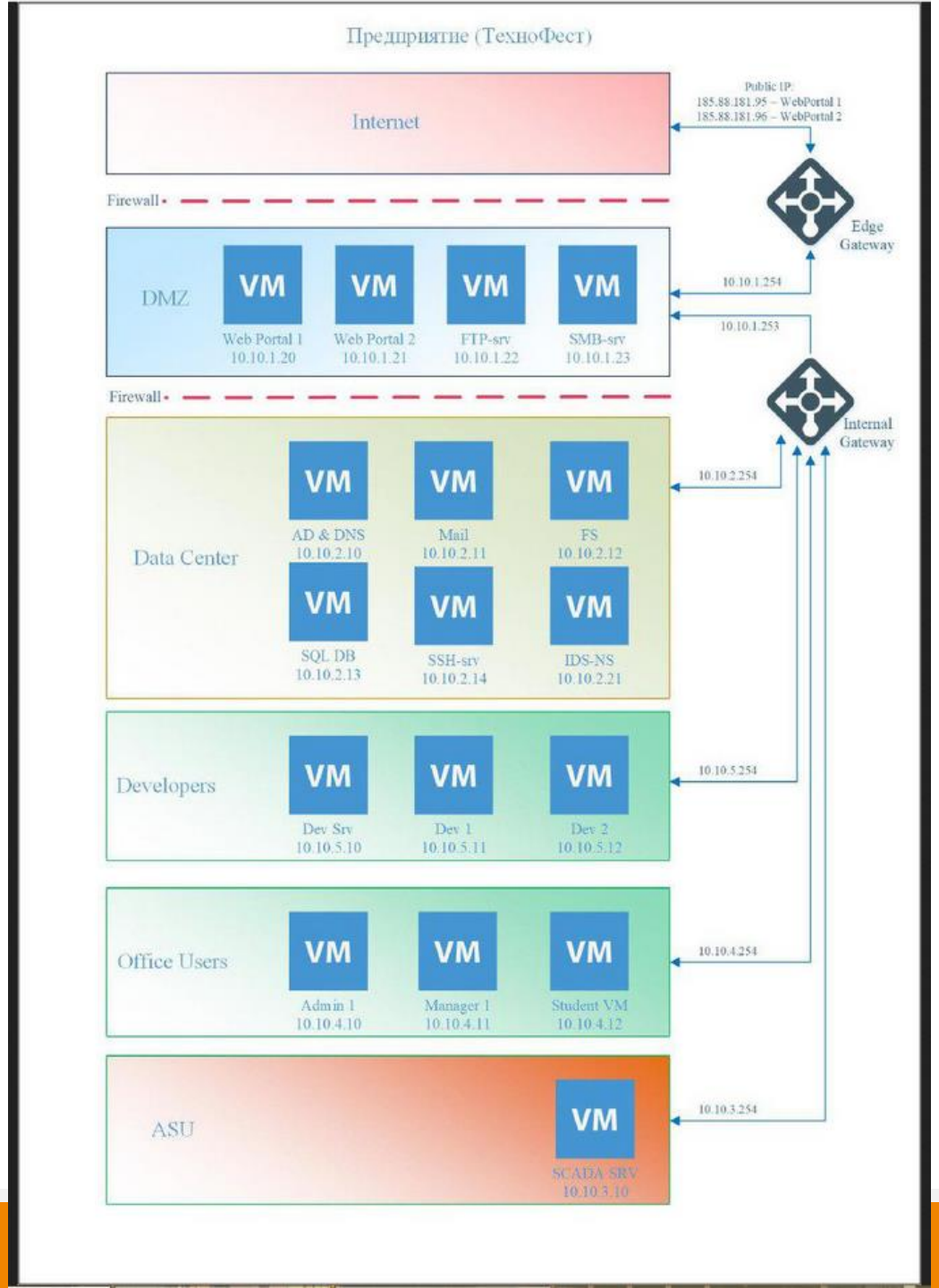
Группа реагирования

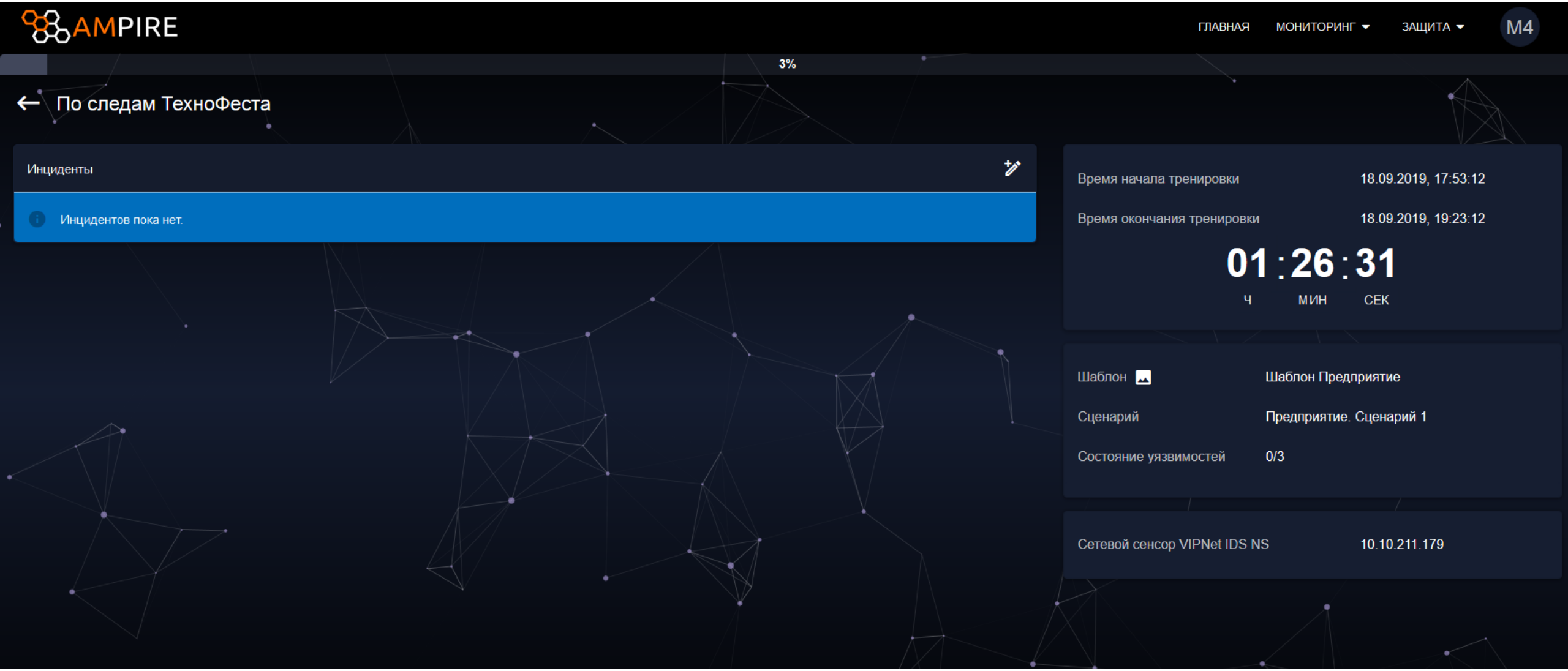

AMPIRE
ГЛАВНАЯ
ПОЛЬЗОВАТЕЛИ
ИНЦИДЕНТЫ
ТРЕНИРОВКИ
АП
0%
По следам ТехноФеста
готова к запуску
НАЧАТЬ
Состояние уязвимостей
DrupalGeddon 2
MySQL Pswd
SSH Pswd
Команда мониторинга
Алексей Николаев
Monitoring 4
Денис Матисов
Команда защиты
Ольга Горлова
Максим Терешкин
Василий Дубков
Инциденты
Логирование событий тренировки
Логов пока нет

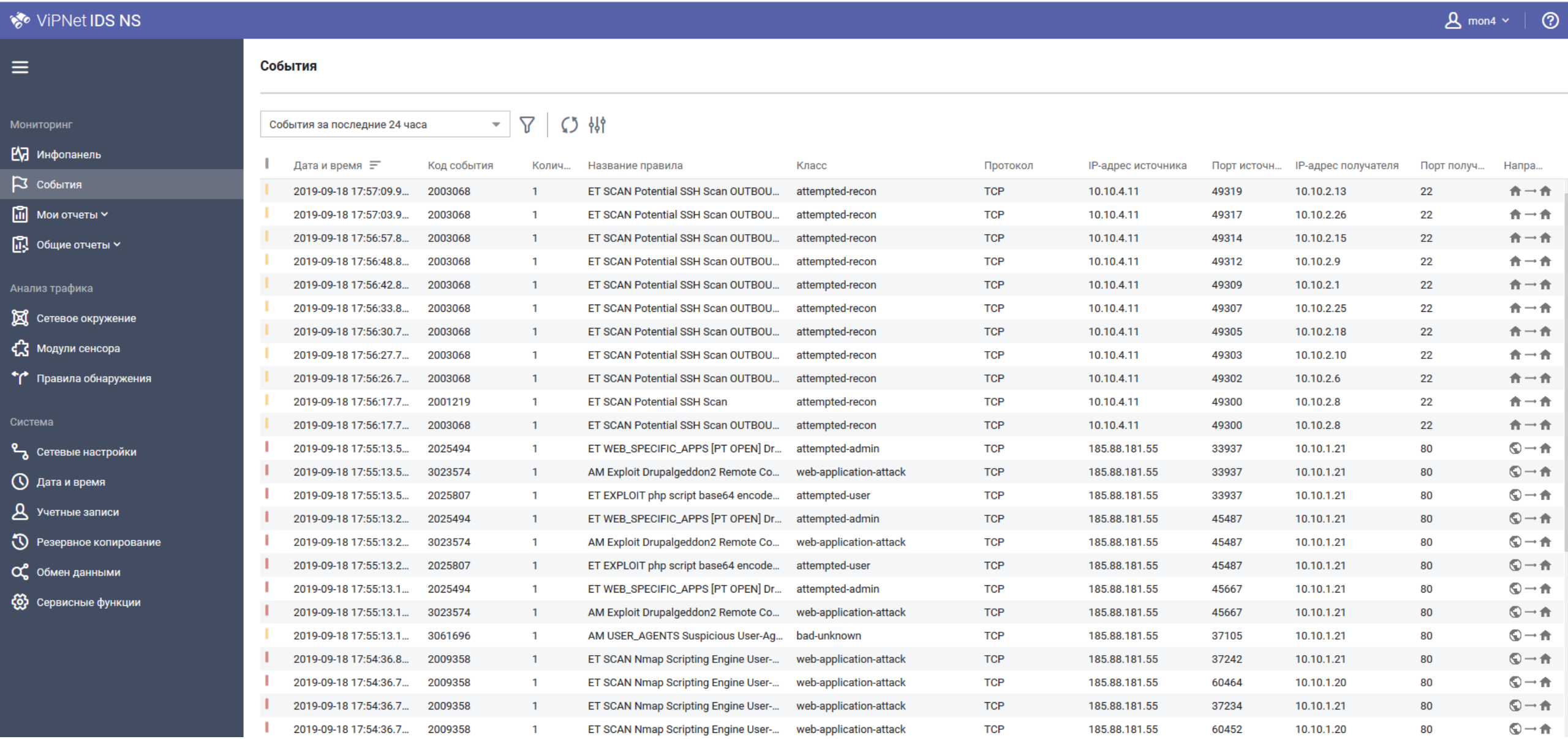

AMPIRE
ГЛАВНАЯ
ПОЛЬЗОВАТЕЛИ
ИНЦИДЕНТЫ
ТРЕНИРОВКИ
АП
FOCUS TEST
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 1
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 2
ПО СЛЕДАМ ТЕХНОФЕСТА
Время начала тренировки
18.09.2019, 17:53:12
Время окончания тренировки
18.09.2019, 19:23:12
01 : 27 : 23
Ч
МИН
СЕК
Шаблон
Шаблон Предприятие
Сценарий
Предприятие. Сценарий 1
Группа
Технофест 1
0 / 0
0 / 3
0 / 100
17%
Vuln
Vuln2
Vuln3
Данных нет



Группа мониторинга


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


AMPIRE
ГЛАВНАЯ
МОНИТОРИНГ
ЗАЩИТА
M4
3%
По следам ТехноФеста
Инциденты
Инцидентов пока нет.
Время начала тренировки
18.09.2019, 17:53:12
Время окончания тренировки
18.09.2019, 19:23:12
01 : 26 : 31
Ч
МИН
СЕК
Шаблон
Шаблон Предприятие
Сценарий
Предприятие. Сценарий 1
Состояние уязвимостей
0/3
Сетевой сенсор VIPNet IDS NS
10.10.211.179


ViPNet IDS NS
mon4
Мониторинг
Инфопанель
События
Мои отчеты
Общие отчеты
Анализ трафика
Сетевое окружение
Модули сенсора
Правила обнаружения
Система
Сетевые настройки
Дата и время
Учетные записи
Резервное копирование
Обмен данными
Сервисные функции
События
События за последние 24 часа
Дата и время
Код события
Колич...
Название правила
Класс
Протокол
IP-адрес источника
Порт источн...
IP-адрес получателя
Порт получ...
Напра...
2019-09-18 17:57:09.9... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49319 10.10.2.13 22
2019-09-18 17:57:03.9... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49317 10.10.2.26 22
2019-09-18 17:56:57.8... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49314 10.10.2.15 22
2019-09-18 17:56:48.8... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49312 10.10.2.9 22
2019-09-18 17:56:42.8... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49309 10.10.2.1 22
2019-09-18 17:56:33.8... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49307 10.10.2.25 22
2019-09-18 17:56:30.7... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49305 10.10.2.18 22
2019-09-18 17:56:27.7... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49303 10.10.2.10 22
2019-09-18 17:56:26.7... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49302 10.10.2.6 22
2019-09-18 17:56:17.7... 2001219 1 ET SCAN Potential SSH Scan attempted-recon TCP 10.10.4.11 49300 10.10.2.8 22
2019-09-18 17:56:17.7... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49300 10.10.2.8 22
2019-09-18 17:55:13.5... 2025494 1 ET WEB_SPECIFIC_APPS [PT OPEN] Dr... attempted-admin TCP 185.88.181.55 33937 10.10.1.21 80
2019-09-18 17:55:13.5... 3023574 1 AM Exploit Drupalgeddon2 Remote Co... web-application-attack TCP 185.88.181.55 33937 10.10.1.21 80
2019-09-18 17:55:13.5... 2025807 1 ET EXPLOIT php script base64 encode... attempted-user TCP 185.88.181.55 33937 10.10.1.21 80
2019-09-18 17:55:13.2... 2025494 1 ET WEB_SPECIFIC_APPS [PT OPEN] Dr... attempted-admin TCP 185.88.181.55 45487 10.10.1.21 80
2019-09-18 17:55:13.2... 3023574 1 AM Exploit Drupalgeddon2 Remote Co... web-application-attack TCP 185.88.181.55 45487 10.10.1.21 80
2019-09-18 17:55:13.2... 2025807 1 ET EXPLOIT php script base64 encode... attempted-user TCP 185.88.181.55 45487 10.10.1.21 80
2019-09-18 17:55:13.1... 2025494 1 ET WEB_SPECIFIC_APPS [PT OPEN] Dr... attempted-admin TCP 185.88.181.55 45667 10.10.1.21 80
2019-09-18 17:55:13.1... 3023574 1 AM Exploit Drupalgeddon2 Remote Co... web-application-attack TCP 185.88.181.55 45667 10.10.1.21 80
2019-09-18 17:55:13.1... 3061696 1 AM USER_AGENTS Suspicious User-Ag... bad-unknown TCP 185.88.181.55 37105 10.10.1.21 80
2019-09-18 17:54:36.8... 2009358 1 ET SCAN Nmap Scripting Engine User-... web-application-attack TCP 185.88.181.55 37242 10.10.1.21 80
2019-09-18 17:54:36.7... 2009358 1 ET SCAN Nmap Scripting Engine User-... web-application-attack TCP 185.88.181.55 60464 10.10.1.20 80
2019-09-18 17:54:36.7... 2009358 1 ET SCAN Nmap Scripting Engine User-... web-application-attack TCP 185.88.181.55 37234 10.10.1.21 80
2019-09-18 17:54:36.7... 2009358 1 ET SCAN Nmap Scripting Engine User-... web-application-attack TCP 185.88.181.55 60452 10.10.1.20 80

События

События за последние 24 часа

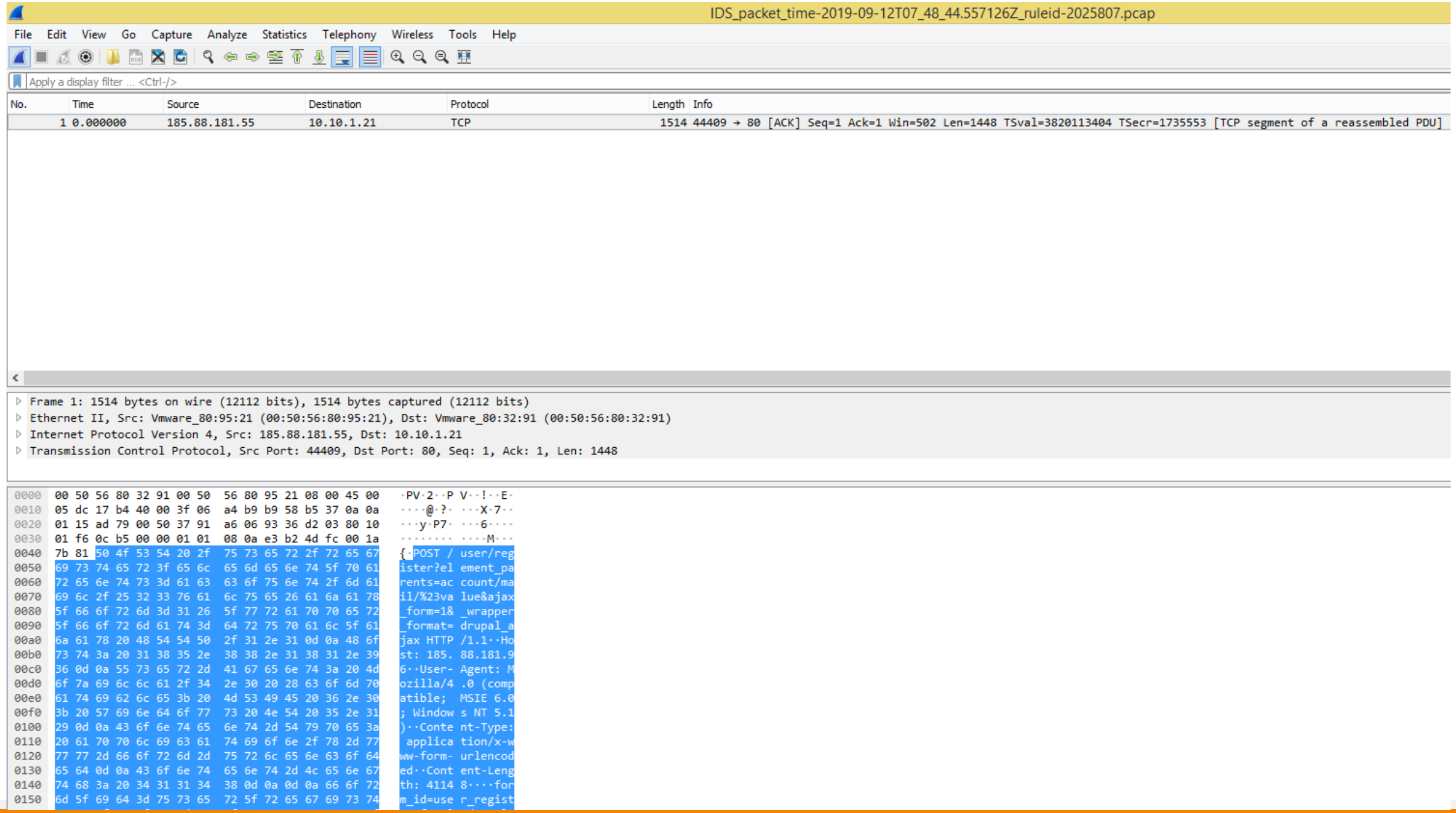
Дата и вре...	Код соб...	К...	Название правила	Класс	Протокол	IP-адрес и...	Порт ...	IP-адрес п...	Порт ...	Напра...
2019-09-18 ...	2003068	1	ET SCAN Potential S...	attempted-recon	TCP	10.10.4.11	49319	10.10.2.13	22	
2019-09-18 ...	2003068	1	ET SCAN Potential S...	attempted-recon	TCP	10.10.4.11	49317	10.10.2.26	22	
2019-09-18 ...	2003068	1	ET SCAN Potential S...	attempted-recon	TCP	10.10.4.11	49314	10.10.2.15	22	
2019-09-18 ...	2003068	1	ET SCAN Potential S...	attempted-recon	TCP	10.10.4.11	49312	10.10.2.9	22	
2019-09-18 ...	2003068	1	ET SCAN Potential S...	attempted-recon	TCP	10.10.4.11	49309	10.10.2.1	22	
2019-09-18 ...	2003068	1	ET SCAN Potential S...	attempted-recon	TCP	10.10.4.11	49307	10.10.2.25	22	
2019-09-18 ...	2003068	1	ET SCAN Potential S...	attempted-recon	TCP	10.10.4.11	49305	10.10.2.18	22	
2019-09-18 ...	2003068	1	ET SCAN Potential S...	attempted-recon	TCP	10.10.4.11	49303	10.10.2.10	22	
2019-09-18 ...	2003068	1	ET SCAN Potential S...	attempted-recon	TCP	10.10.4.11	49302	10.10.2.6	22	
2019-09-18 ...	2001219	1	ET SCAN Potential S...	attempted-recon	TCP	10.10.4.11	49300	10.10.2.8	22	
2019-09-18 ...	2003068	1	ET SCAN Potential S...	attempted-recon	TCP	10.10.4.11	49300	10.10.2.8	22	
2019-09-18 ...	2025494	1	ET WEB_SPECIFIC_A...	attempted-admin	TCP	185.88.18...	33937	10.10.1.21	80	
2019-09-18 ...	3023574	1	AM Exploit Drupalged...	web-application-at...	TCP	185.88.18...	33937	10.10.1.21	80	
2019-09-18 ...	2025807	1	ET EXPLOIT php scri...	attempted-user	TCP	185.88.18...	33937	10.10.1.21	80	
2019-09-18 ...	2025494	1	ET WEB_SPECIFIC_A...	attempted-admin	TCP	185.88.18...	45487	10.10.1.21	80	
2019-09-18 ...	3023574	1	AM Exploit Drupalged...	web-application-at...	TCP	185.88.18...	45487	10.10.1.21	80	
2019-09-18 ...	2025807	1	ET EXPLOIT php scri...	attempted-user	TCP	185.88.18...	45487	10.10.1.21	80	
2019-09-18 ...	2025494	1	ET WEB_SPECIFIC_A...	attempted-admin	TCP	185.88.18...	45667	10.10.1.21	80	
2019-09-18 ...	3023574	1	AM Exploit Drupalged...	web-application-at...	TCP	185.88.18...	45667	10.10.1.21	80	
2019-09-18 ...	3061696	1	AM USER_AGENTS S...	bad-unknown	TCP	185.88.18...	37105	10.10.1.21	80	
2019-09-18 ...	2009358	1	ET SCAN Nmap Scrip...	web-application-at...	TCP	185.88.18...	37242	10.10.1.21	80	
2019-09-18 ...	2009358	1	ET SCAN Nmap Scrip...	web-application-at...	TCP	185.88.18...	60464	10.10.1.20	80	
2019-09-18 ...	2009358	1	ET SCAN Nmap Scrip...	web-application-at...	TCP	185.88.18...	37234	10.10.1.21	80	

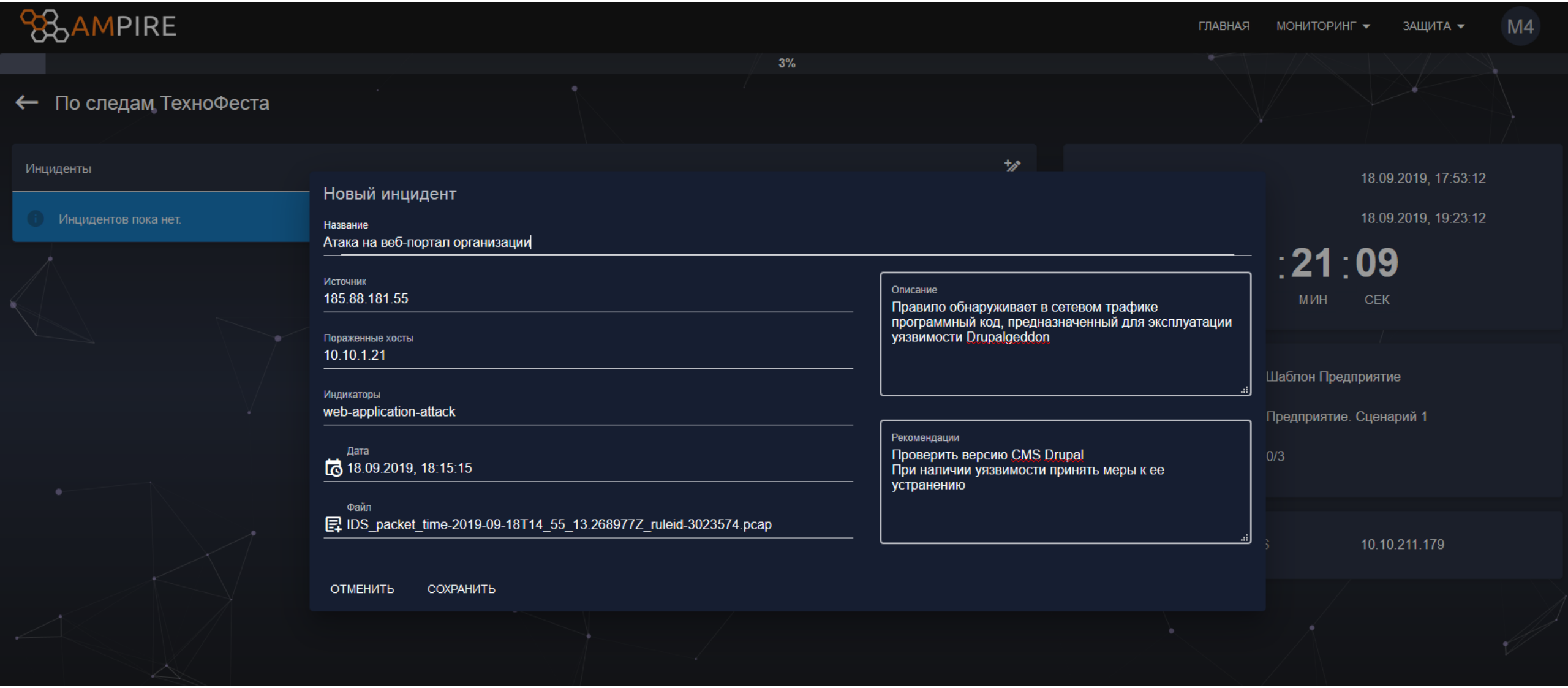
Событие 2019-09-18 17:55:13.268977

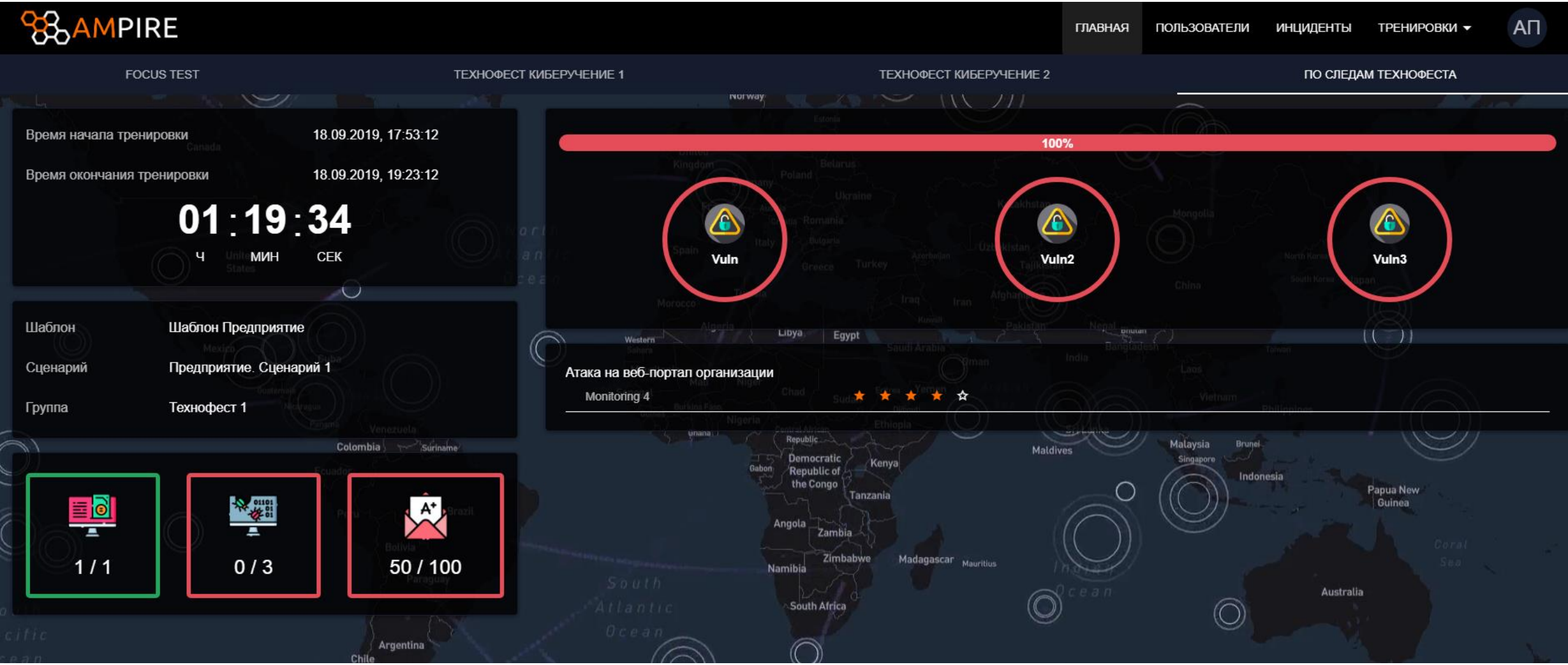
Событие высокой важности

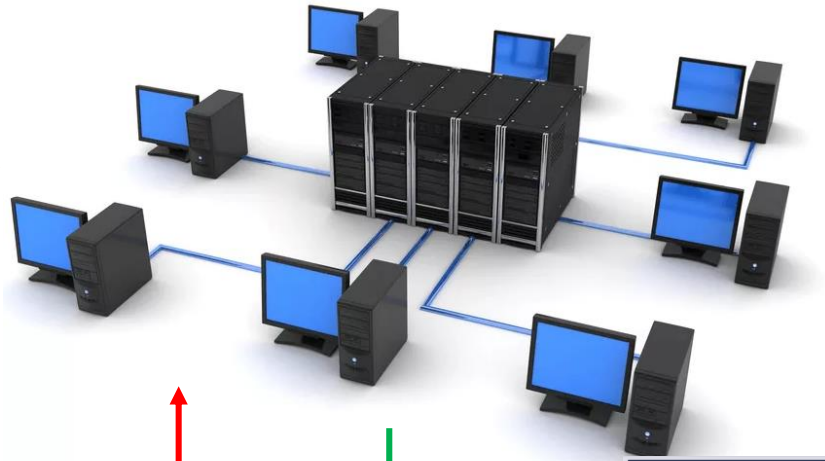
Событие | Источник | Получатель | Пакет

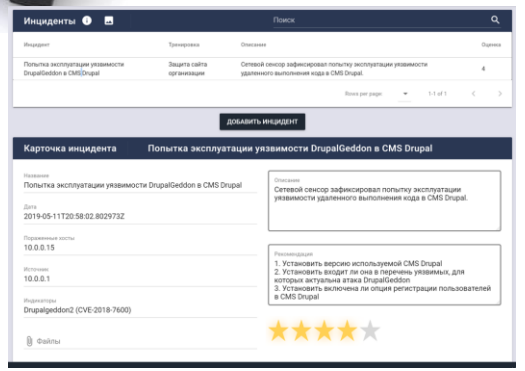
Дата и время обнаружения:	2019-09-18 17:55:13.268977
Тип события:	Сигнатурное событие
Протокол:	TCP
Код события:	3023574
Класс правила:	web-application-attack
Группа правил:	exploit
Название правила:	AM Exploit Drupalgeddon2 Remote Code Execute
Описание правила:	Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости
Текст правила:	alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"AM Exploit Drupalgeddon2 Remote Code Execute";flow:to_server;content:"POST";http_method;content:"|2f|user|2f|register|3f|element|5f|parents|3d|";http_uri;nocase;content:"#value&ajax|5f|form|3d|";http_uri;nocase;content:"wrapper|5f|format|3d|drupal|5f|ajax";http_uri;nocase;pcre:"/POST.*?(account\/mail\/%23value)|(timezone\/timezone\/%23value).*?\x20http\/\d\.\d/si";reference:cve,2018-7600;reference:url,research.checkpoint.com/uncovering-drupalgeddon-2/;reference:url,github.com/a2u/CVE-2018-7600/blob/master/exploit.py;classtype:web-application-attack;sid:3023574;rev:5)
Описание уязвимостей:	cve: 2018-7600 url: research.checkpoint.com/uncovering-drupalgeddon-2/ url: github.com/a2u/CVE-2018-7600/blob/master/exploit.py


IDS_packet_time-2019-09-12T07_48_44.557126Z_ruleid-2025807.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 185.88.181.55 10.10.1.21 TCP 1514 44409 → 80 [ACK] Seq=1 Ack=1 Win=502 Len=1448 TSval=3820113404 TSecr=1735553 [TCP segment of a reassembled PDU]
Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Vmware_80:95:21 (00:50:56:80:95:21), Dst: Vmware_80:32:91 (00:50:56:80:32:91)
Internet Protocol Version 4, Src: 185.88.181.55, Dst: 10.10.1.21
Transmission Control Protocol, Src Port: 44409, Dst Port: 80, Seq: 1, Ack: 1, Len: 1448
0000 00 50 56 80 32 91 00 50 56 80 95 21 08 00 45 00 ·PV·2··P V··!··E·
0010 05 dc 17 b4 40 00 3f 06 a4 b9 b9 58 b5 37 0a 0a ····@·?· ···X·7··
0020 01 15 ad 79 00 50 37 91 a6 06 93 36 d2 03 80 10 ···y·P7· ···6····
0030 01 f6 0c b5 00 00 01 01 08 0a e3 b2 4d fc 00 1a ········ ····M···
0040 7b 81 50 4f 53 54 20 2f 75 73 65 72 2f 72 65 67 {·POST / user/reg
0050 69 73 74 65 72 3f 65 6c 65 6d 65 6e 74 5f 70 61 ister?el ement_pa
0060 72 65 6e 74 73 3d 61 63 63 6f 75 6e 74 2f 6d 61 rents=ac count/ma
0070 69 6c 2f 25 32 33 76 61 6c 75 65 26 61 6a 61 78 il/%23va lue&ajax
0080 5f 66 6f 72 6d 3d 31 26 5f 77 72 61 70 70 65 72 _form=1& _wrapper
0090 5f 66 6f 72 6d 61 74 3d 64 72 75 70 61 6c 5f 61 _format= drupal_a
00a0 6a 61 78 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f jax HTTP /1.1··Ho
00b0 73 74 3a 20 31 38 35 2e 38 38 2e 31 38 31 2e 39 st: 185. 88.181.9
00c0 36 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6··User- Agent: M
00d0 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28 63 6f 6d 70 ozilla/4 .0 (comp
00e0 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 36 2e 30 atible; MSIE 6.0
00f0 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 ; Window s NT 5.1
0100 29 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a)··Conte nt-Type:
0110 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 applica tion/x-w
0120 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 ww-form- urlencod
0130 65 64 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 ed··Cont ent-Leng
0140 74 68 3a 20 34 31 31 34 38 0d 0a 0d 0a 66 6f 72 th: 4114 8····for
0150 6d 5f 69 64 3d 75 73 65 72 5f 72 65 67 69 73 74 m_id=use r_regist


AMPIRE
ГЛАВНАЯ
МОНИТОРИНГ
ЗАЩИТА
M4
3%
По следам ТехноФеста
Инциденты
Инцидентов пока нет
Новый инцидент
Название
Атака на веб-портал организации
Источник
185.88.181.55
Пораженные хосты
10.10.1.21
Индикаторы
web-application-attack
Дата
18.09.2019, 18:15:15
Файл
IDS_packet_time-2019-09-18T14_55_13.268977Z_ruleid-3023574.pcap
Описание
Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости Drupalgeddon
Рекомендации
Проверить версию CMS Drupal
При наличии уязвимости принять меры к ее устранению
ОТМЕНИТЬ
СОХРАНИТЬ
18.09.2019, 17:53:12
18.09.2019, 19:23:12
:21 :09
МИН
СЕК
Шаблон Предприятие
Предприятие. Сценарий 1
0/3
10.10.211.179

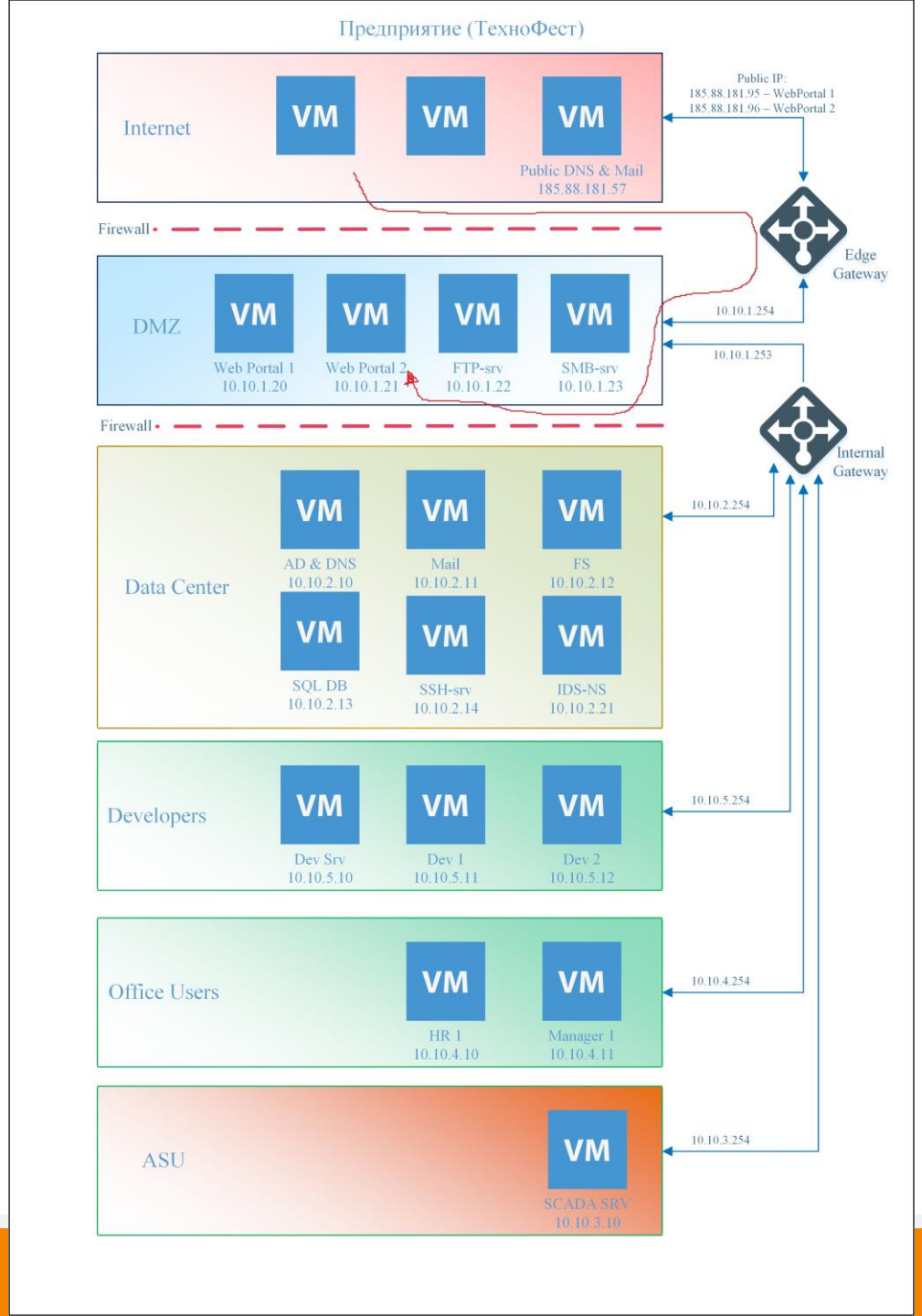

AMPIRE
ГЛАВНАЯ
ПОЛЬЗОВАТЕЛИ
ИНЦИДЕНТЫ
ТРЕНИРОВКИ
АП
FOCUS TEST
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 1
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 2
ПО СЛЕДАМ ТЕХНОФЕСТА
Время начала тренировки
18.09.2019, 17:53:12
Время окончания тренировки
18.09.2019, 19:23:12
01 : 19 : 34
Ч
МИН
СЕК
Шаблон
Шаблон Предприятие
Сценарий
Предприятие. Сценарий 1
Группа
Технофест 1
1 / 1
0 / 3
50 / 100
100%
Vuln
Vuln2
Vuln3
Атака на веб-портал организации
Monitoring 4

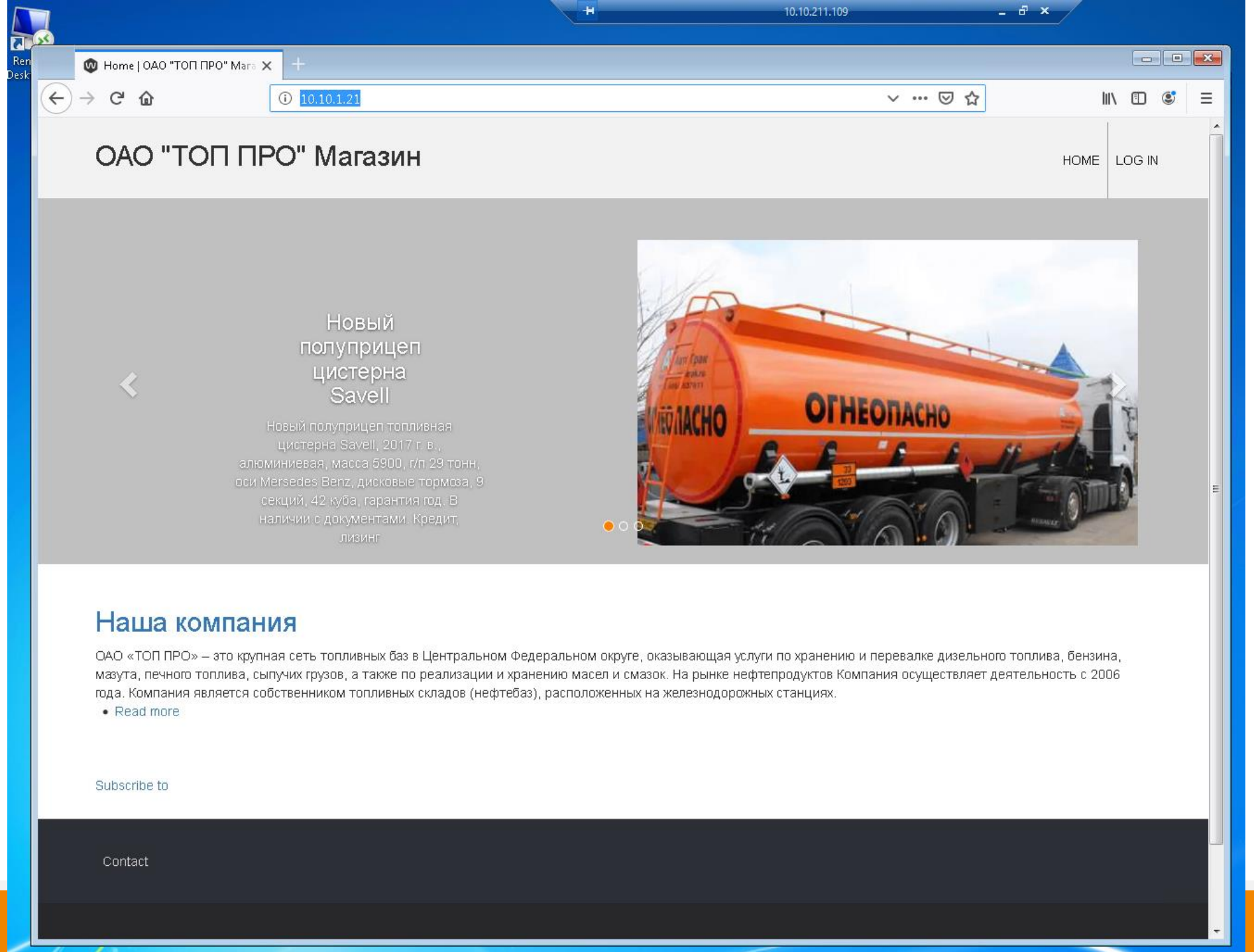


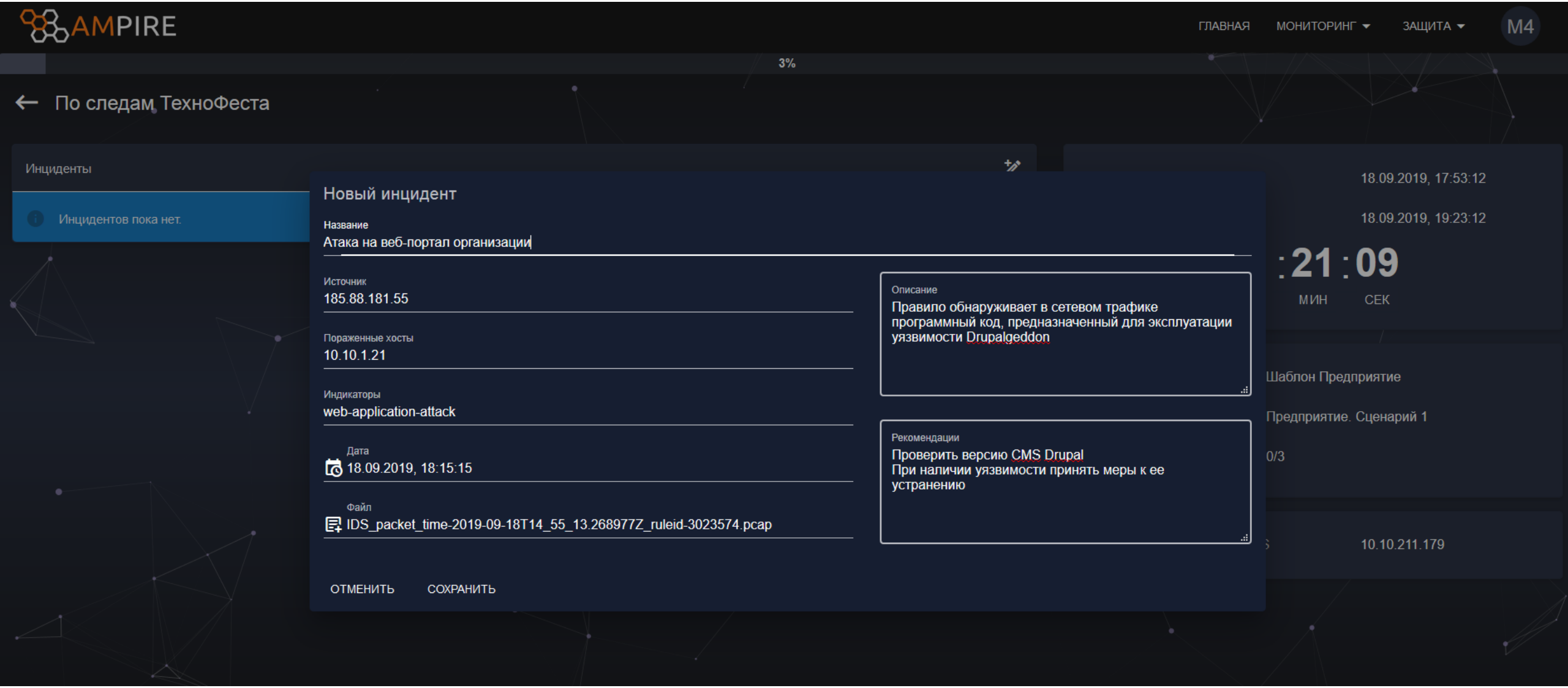


Группа мониторинга

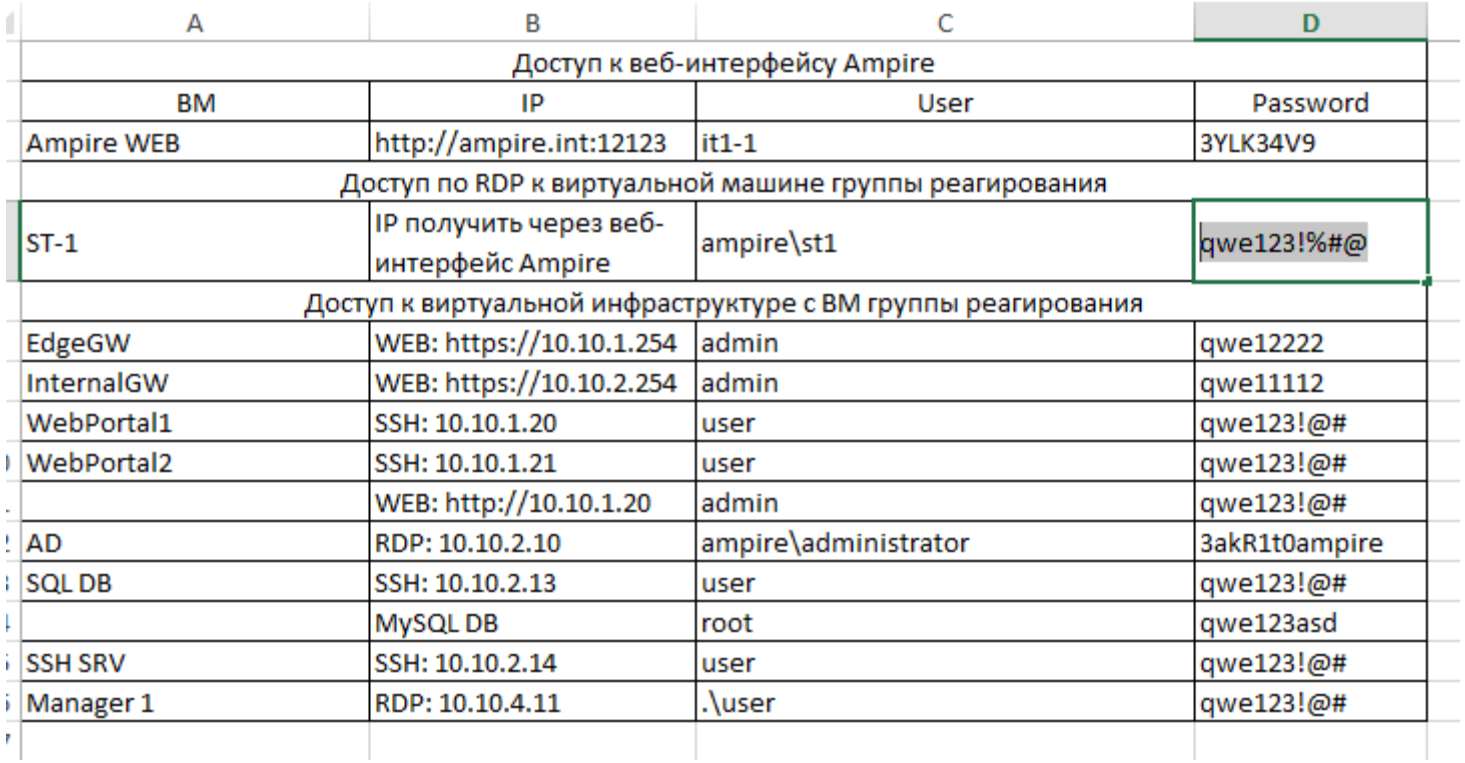
Группа реагирования


Предприятие (ТехноФест)
Internet
VM
VM
VM
Public DNS & Mail
185.88.181.57
Public IP:
185.88.181.95 – WebPortal 1
185.88.181.96 – WebPortal 2
Firewall
Edge
Gateway
DMZ
VM
VM
VM
VM
Web Portal 1
10.10.1.20
Web Portal 2
10.10.1.21
FTP-srv
10.10.1.22
SMB-srv
10.10.1.23
10.10.1.254
10.10.1.253
Firewall
Internal
Gateway
Data Center
VM
VM
VM
AD & DNS
10.10.2.10
Mail
10.10.2.11
FS
10.10.2.12
VM
VM
VM
SQL DB
10.10.2.13
SSH-srv
10.10.2.14
IDS-NS
10.10.2.21
10.10.2.254
Developers
VM
VM
VM
Dev Srv
10.10.5.10
Dev 1
10.10.5.11
Dev 2
10.10.5.12
10.10.5.254
Office Users
VM
VM
HR 1
10.10.4.10
Manager 1
10.10.4.11
10.10.4.254
ASU
VM
SCADA SRV
10.10.3.10
10.10.3.254

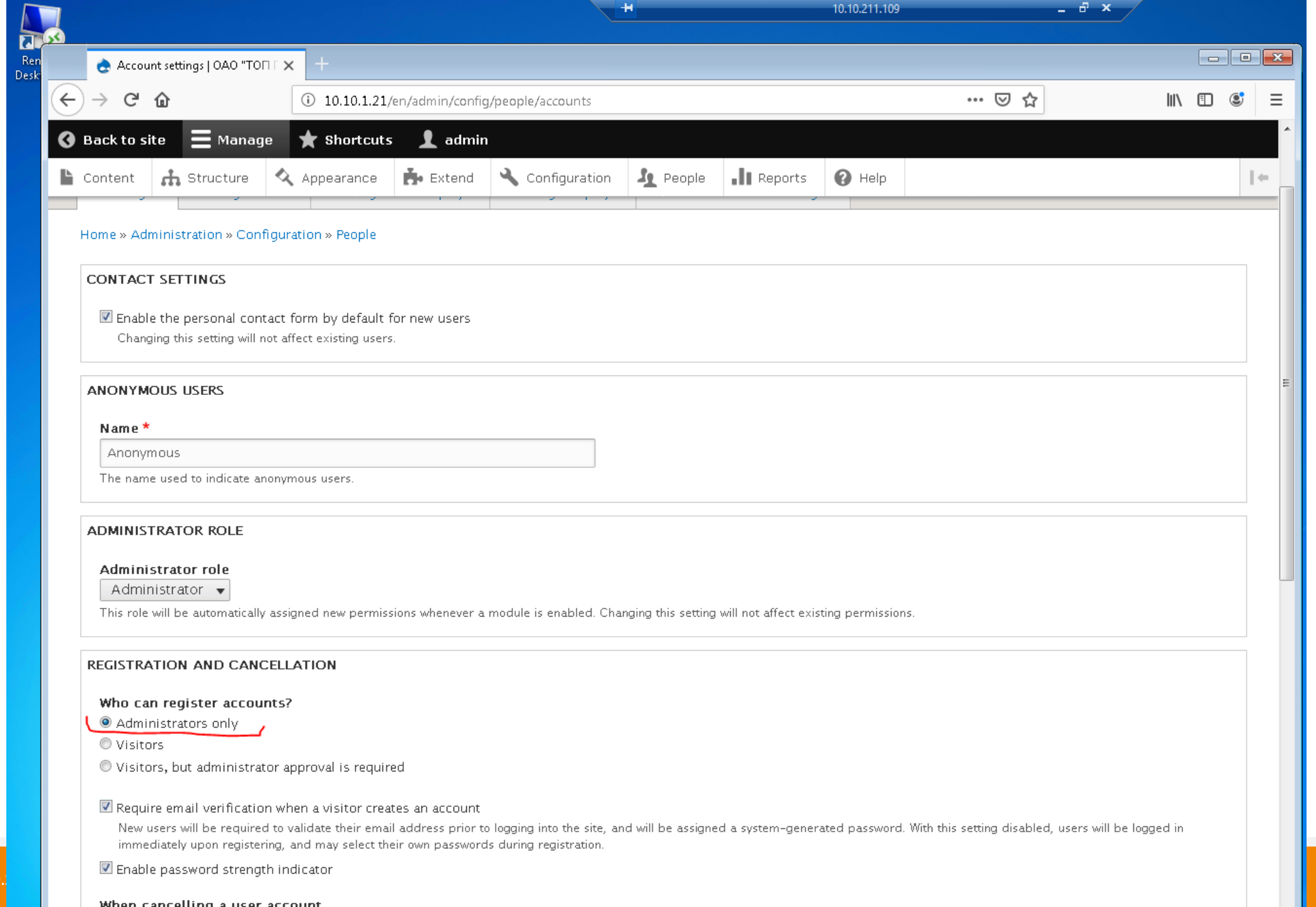

10.10.211.109
Home | ОАО "ТОП ПРО" Маг
10.10.1.21
ОАО "ТОП ПРО" Магазин
HOME
LOG IN
Новый полуприцеп цистерна Savell
Новый полуприцеп топливная цистерна Savell, 2017 г. в., алюминиевая, масса 5900, г/п 29 тонн, оси Mersedes Benz, дисковые тормоза, 9 секций, 42 куба, гарантия год. В наличии с документами. Кредит, лизинг
ОГНЕОПАСНО
Наша компания
ОАО «ТОП ПРО» – это крупная сеть топливных баз в Центральном Федеральном округе, оказывающая услуги по хранению и перевалке дизельного топлива, бензина, мазута, печного топлива, сыпучих грузов, а также по реализации и хранению масел и смазок. На рынке нефтепродуктов Компания осуществляет деятельность с 2006 года. Компания является собственником топливных складов (нефтебаз), расположенных на железнодорожных станциях.
Read more
Subscribe to
Contact

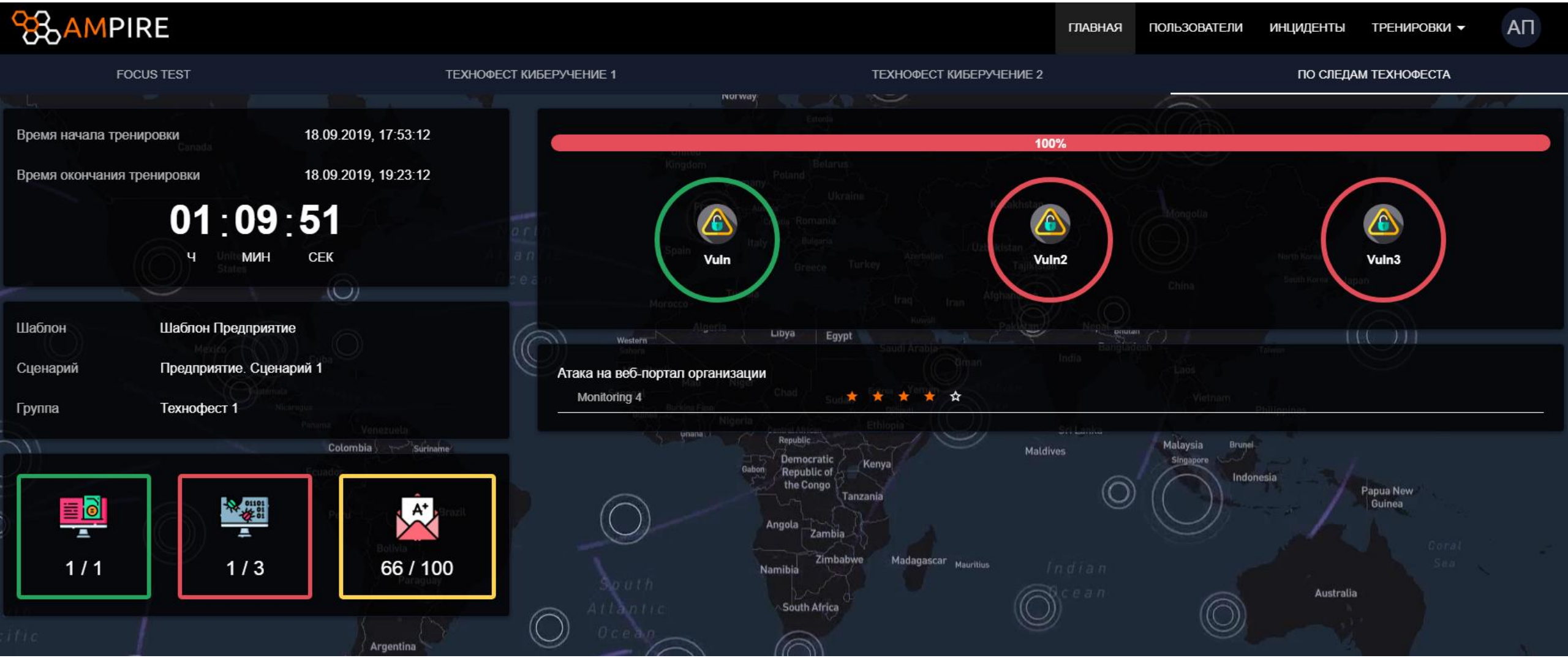

AMPIRE
ГЛАВНАЯ
МОНИТОРИНГ
ЗАЩИТА
M4
3%
По следам ТехноФеста
Инциденты
Инцидентов пока нет.
Новый инцидент
Название
Атака на веб-портал организации
Источник
185.88.181.55
Пораженные хосты
10.10.1.21
Индикаторы
web-application-attack
Дата
18.09.2019, 18:15:15
Файл
IDS_packet_time-2019-09-18T14_55_13.268977Z_ruleid-3023574.pcap
Описание
Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости Drupalgeddon
Рекомендации
Проверить версию CMS Drupal
При наличии уязвимости принять меры к ее устранению
ОТМЕНИТЬ
СОХРАНИТЬ
18.09.2019, 17:53:12
18.09.2019, 19:23:12
:21 :09
МИН
СЕК
Шаблон Предприятие
Предприятие. Сценарий 1
0/3
10.10.211.179

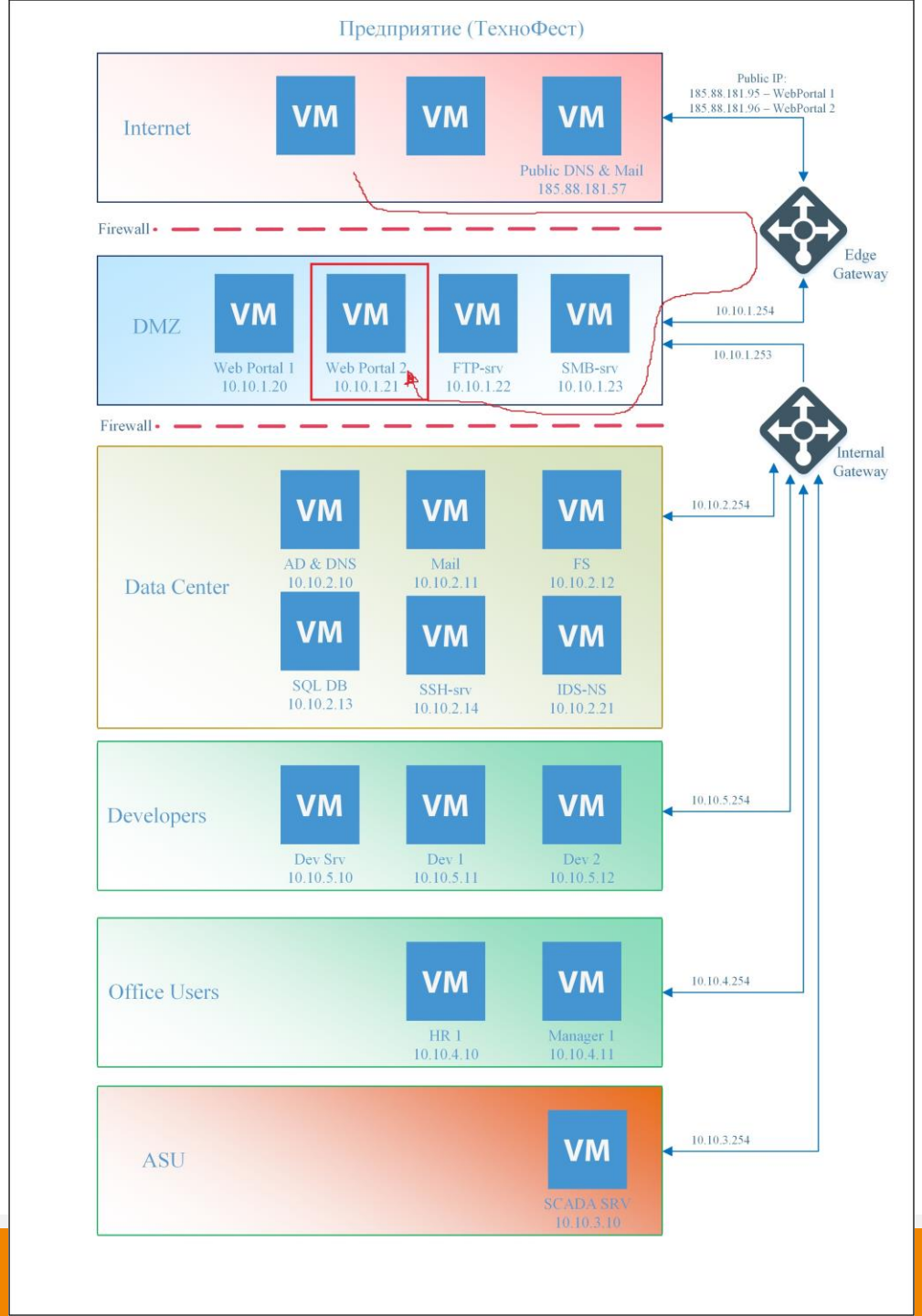

ВЗЛОМ
Друпалгеддон-2. Подробно разбираем новую уязвимость в Drupal
aLLy , 17.04.2018 1 18254

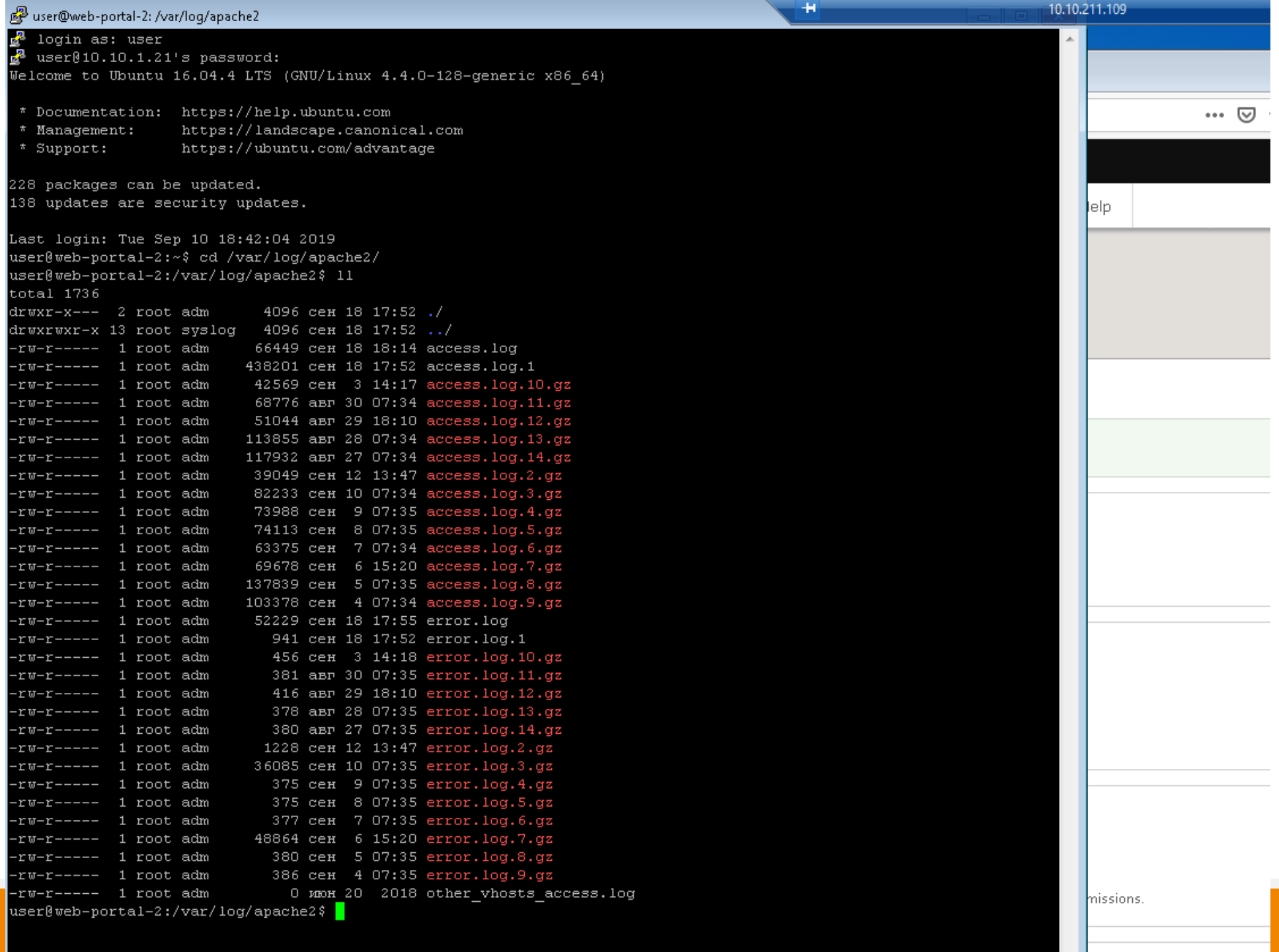


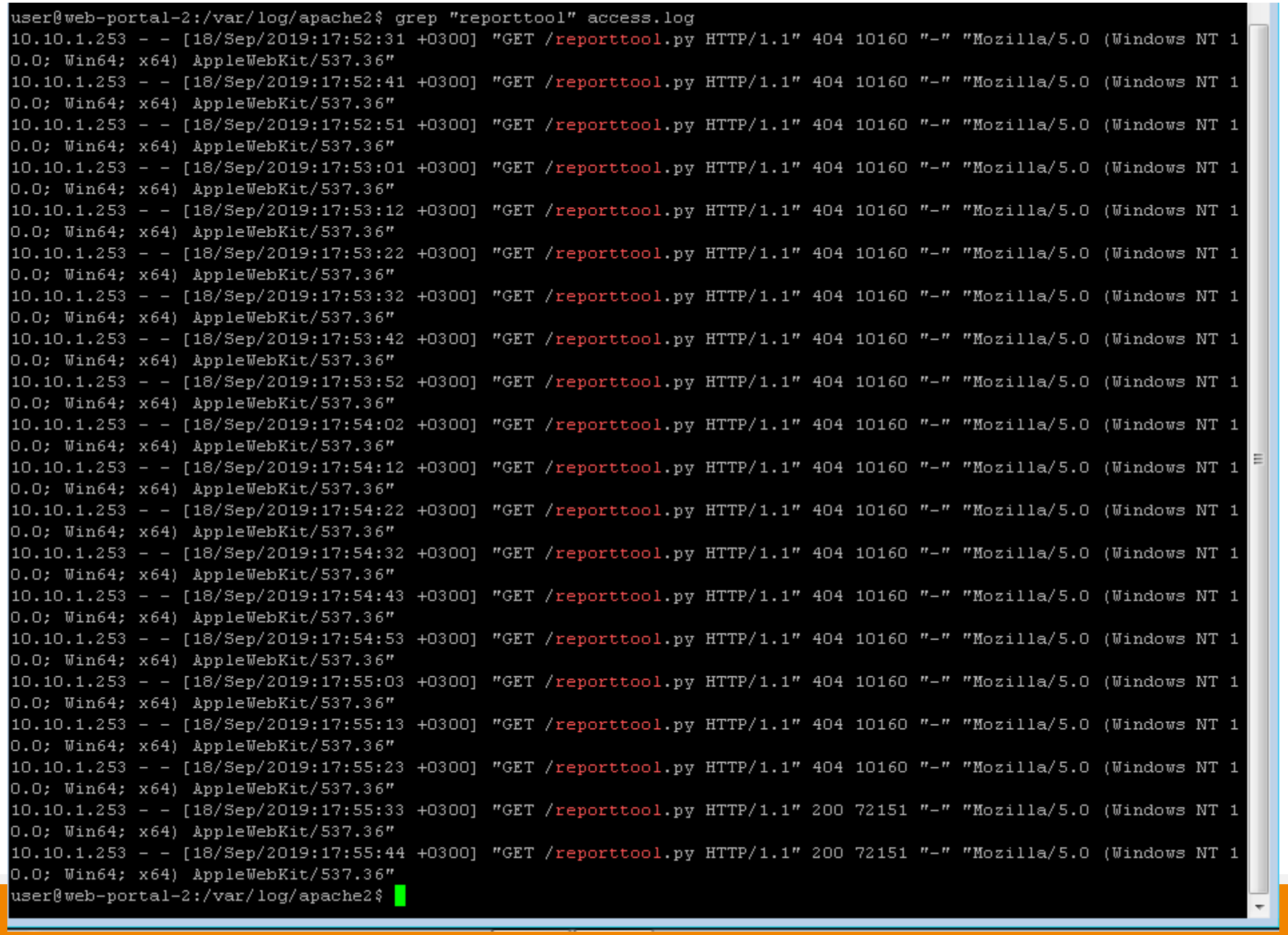
A	B	C	D
Доступ к веб-интерфейсу Ampire			
ВМ	IP	User	Password
Ampire WEB	http://ampire.int:12123	it1-1	3YLK34V9
Доступ по RDP к виртуальной машине группы реагирования			
ST-1	IP получить через веб-интерфейс Ampire	ampire\st1	qwe123!%#@
Доступ к виртуальной инфраструктуре с ВМ группы реагирования			
EdgeGW	WEB: https://10.10.1.254	admin	qwe12222
InternalGW	WEB: https://10.10.2.254	admin	qwe11112
WebPortal1	SSH: 10.10.1.20	user	qwe123!@#
WebPortal2	SSH: 10.10.1.21	user	qwe123!@#
	WEB: http://10.10.1.20	admin	qwe123!@#
AD	RDP: 10.10.2.10	ampire\administrator	3akR1t0ampire
SQL DB	SSH: 10.10.2.13	user	qwe123!@#
	MySQL DB	root	qwe123asd
SSH SRV	SSH: 10.10.2.14	user	qwe123!@#
Manager 1	RDP: 10.10.4.11	.\user	qwe123!@#

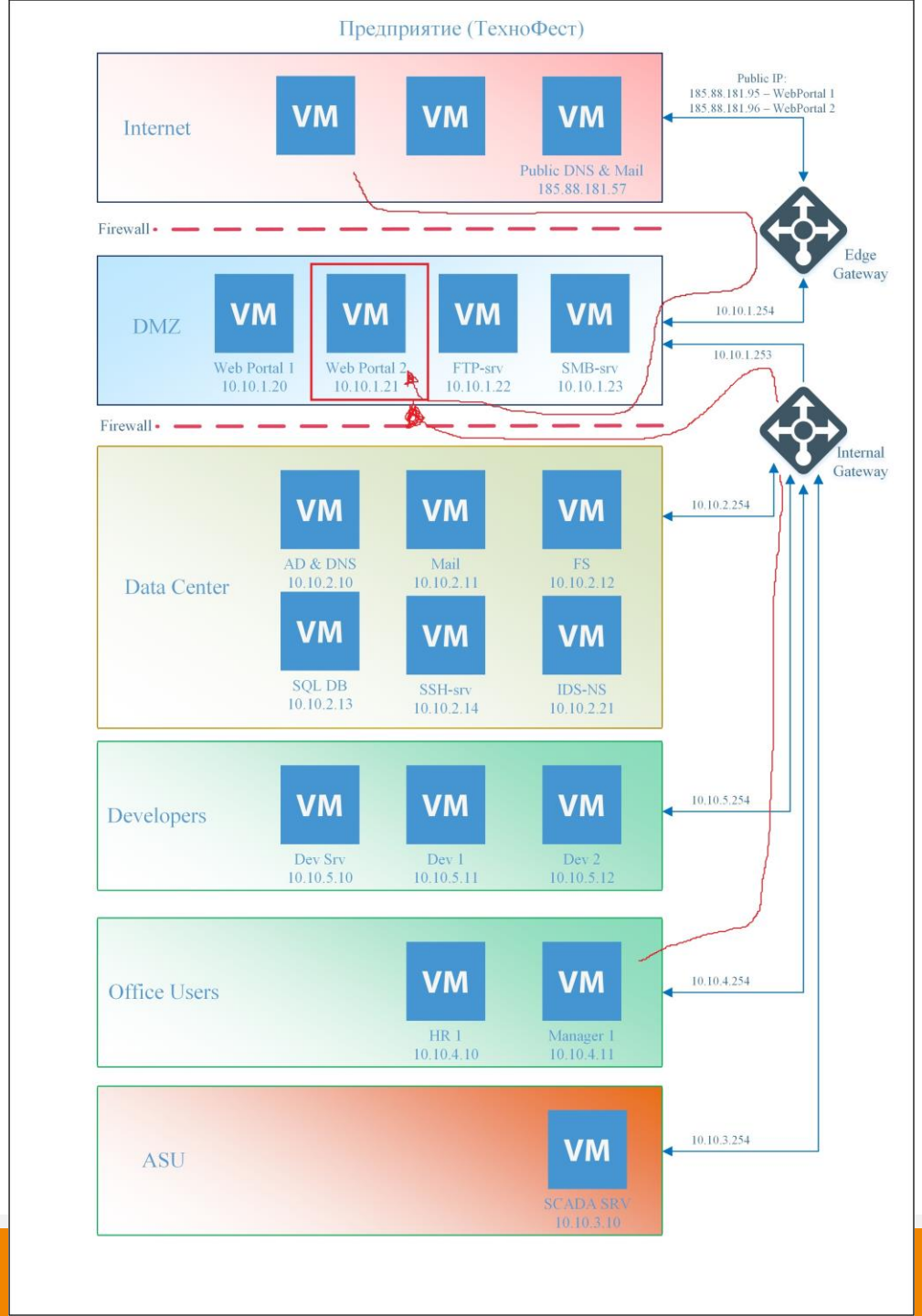

10.10.211.109
Account settings | ОАО "ТОП
10.10.1.21/en/admin/config/people/accounts
Back to site
Manage
Shortcuts
admin
Content
Structure
Appearance
Extend
Configuration
People
Reports
Help
Home » Administration » Configuration » People
CONTACT SETTINGS
Enable the personal contact form by default for new users
Changing this setting will not affect existing users.
ANONYMOUS USERS
Name *
Anonymous
The name used to indicate anonymous users.
ADMINISTRATOR ROLE
Administrator role
Administrator
This role will be automatically assigned new permissions whenever a module is enabled. Changing this setting will not affect existing permissions.
REGISTRATION AND CANCELLATION
Who can register accounts?
Administrators only
Visitors
Visitors, but administrator approval is required
Require email verification when a visitor creates an account
New users will be required to validate their email address prior to logging into the site, and will be assigned a system-generated password. With this setting disabled, users will be logged in immediately upon registering, and may select their own passwords during registration.
Enable password strength indicator

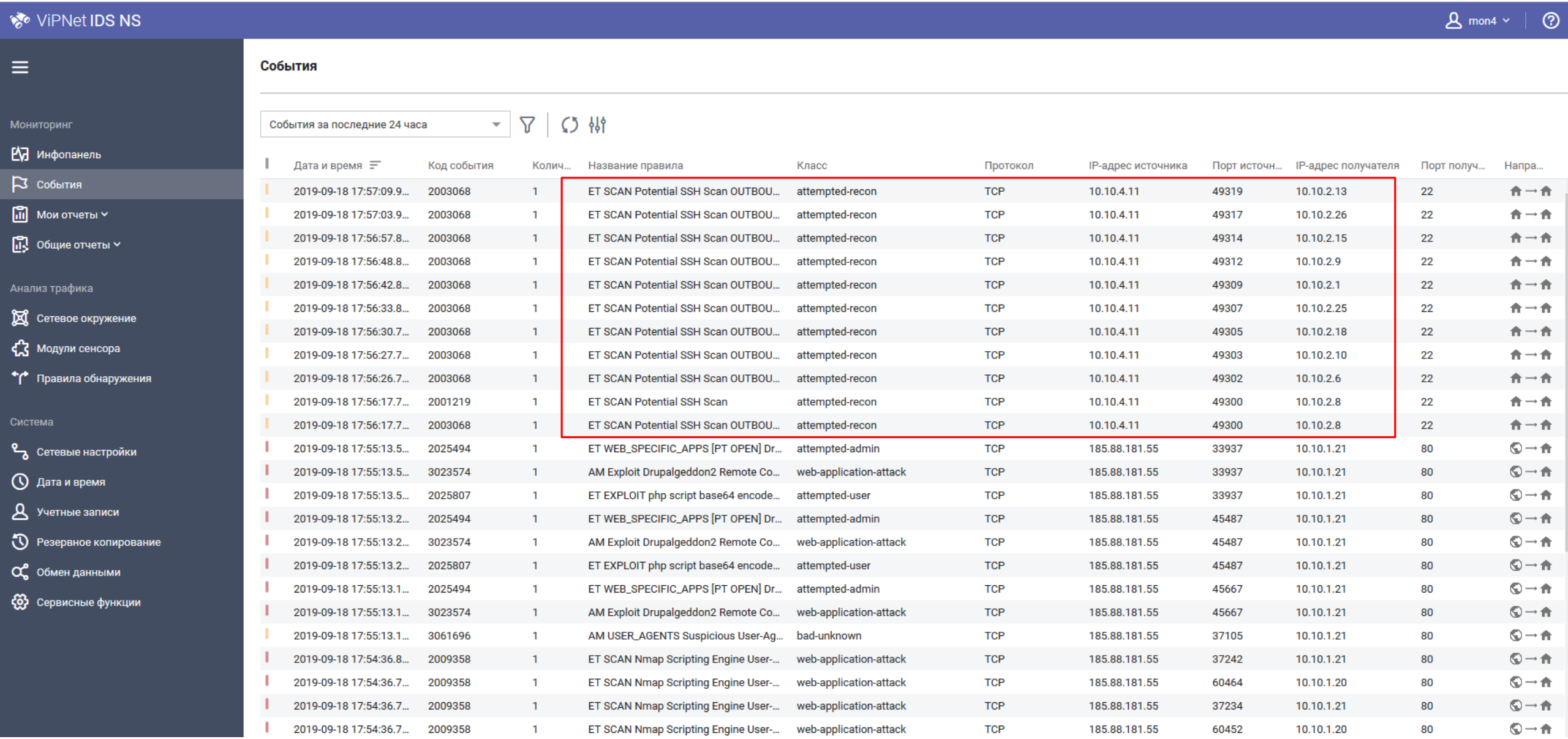

AMPIRE
ГЛАВНАЯ
ПОЛЬЗОВАТЕЛИ
ИНЦИДЕНТЫ
ТРЕНИРОВКИ
АП
FOCUS TEST
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 1
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 2
ПО СЛЕДАМ ТЕХНОФЕСТА
Время начала тренировки
18.09.2019, 17:53:12
Время окончания тренировки
18.09.2019, 19:23:12
01 : 09 : 51
Ч МИН СЕК
Шаблон
Шаблон Предприятие
Сценарий
Предприятие. Сценарий 1
Группа
Технофест 1
1 / 1
1 / 3
66 / 100
100%
Vuln
Vuln2
Vuln3
Атака на веб-портал организации
Monitoring 4

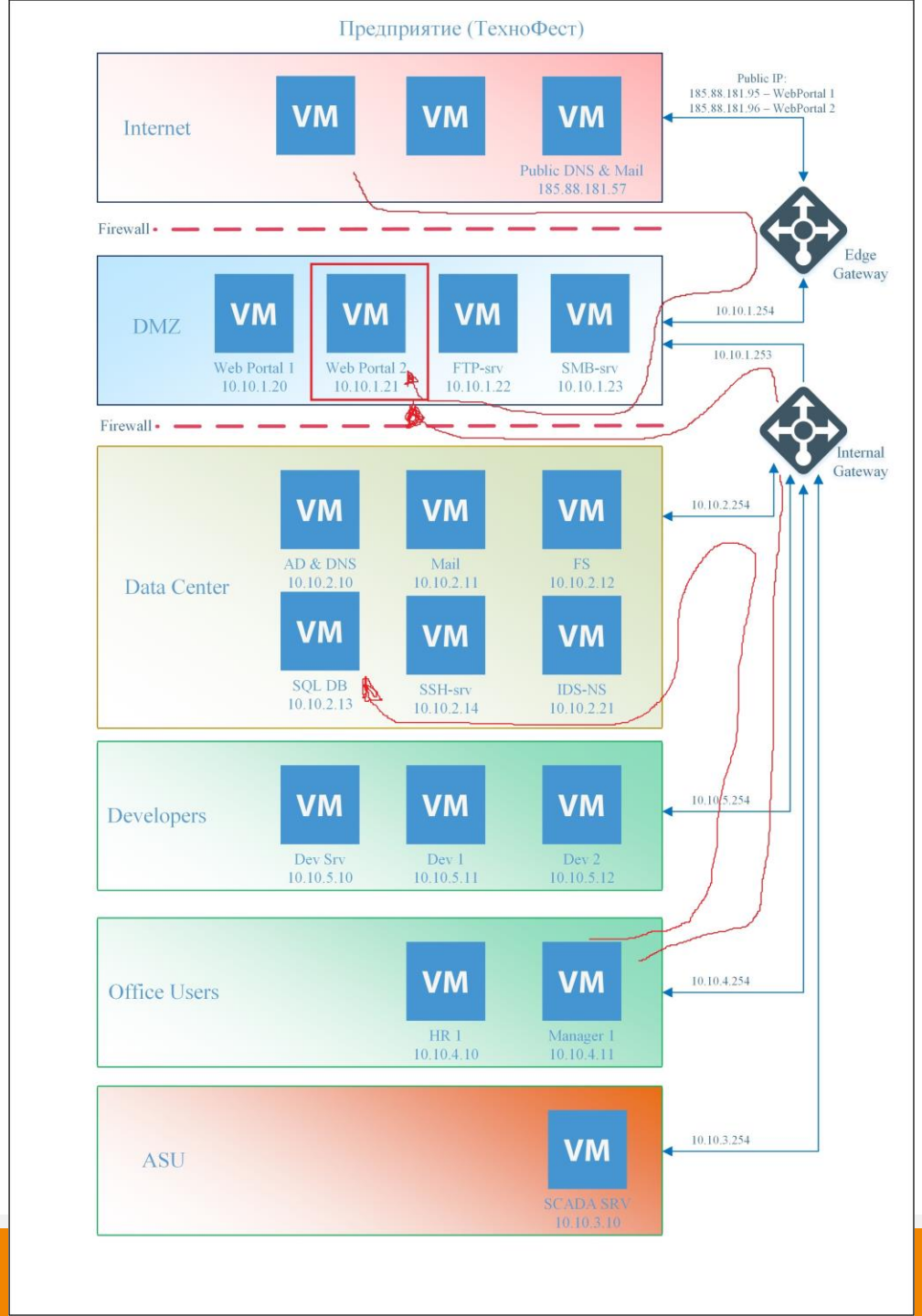

Предприятие (ТехноФест)
Internet
VM
VM
VM
Public DNS & Mail
185.88.181.57
Public IP:
185.88.181.95 – WebPortal 1
185.88.181.96 – WebPortal 2
Firewall
Edge
Gateway
10.10.1.254
10.10.1.253
DMZ
VM
VM
VM
VM
Web Portal 1
10.10.1.20
Web Portal 2
10.10.1.21
FTP-srv
10.10.1.22
SMB-srv
10.10.1.23
Firewall
Internal
Gateway
10.10.2.254
Data Center
VM
VM
VM
AD & DNS
10.10.2.10
Mail
10.10.2.11
FS
10.10.2.12
VM
VM
VM
SQL DB
10.10.2.13
SSH-srv
10.10.2.14
IDS-NS
10.10.2.21
Developers
10.10.5.254
VM
VM
VM
Dev Srv
10.10.5.10
Dev 1
10.10.5.11
Dev 2
10.10.5.12
Office Users
10.10.4.254
VM
VM
HR 1
10.10.4.10
Manager 1
10.10.4.11
ASU
10.10.3.254
VM
SCADA SRV
10.10.3.10


user@web-portal-2: /var/log/apache2
10.10.211.109
login as: user
user@10.10.1.21's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-128-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
228 packages can be updated.
138 updates are security updates.
Last login: Tue Sep 10 18:42:04 2019
user@web-portal-2:~$ cd /var/log/apache2/
user@web-portal-2:/var/log/apache2$ ll
total 1736
drwxr-x--- 2 root adm 4096 сен 18 17:52 ./
drwxrwxr-x 13 root syslog 4096 сен 18 17:52 ../
-rw-r----- 1 root adm 66449 сен 18 18:14 access.log
-rw-r----- 1 root adm 438201 сен 18 17:52 access.log.1
-rw-r----- 1 root adm 42569 сен 3 14:17 access.log.10.gz
-rw-r----- 1 root adm 68776 авг 30 07:34 access.log.11.gz
-rw-r----- 1 root adm 51044 авг 29 18:10 access.log.12.gz
-rw-r----- 1 root adm 113855 авг 28 07:34 access.log.13.gz
-rw-r----- 1 root adm 117932 авг 27 07:34 access.log.14.gz
-rw-r----- 1 root adm 39049 сен 12 13:47 access.log.2.gz
-rw-r----- 1 root adm 82233 сен 10 07:34 access.log.3.gz
-rw-r----- 1 root adm 73988 сен 9 07:35 access.log.4.gz
-rw-r----- 1 root adm 74113 сен 8 07:35 access.log.5.gz
-rw-r----- 1 root adm 63375 сен 7 07:34 access.log.6.gz
-rw-r----- 1 root adm 69678 сен 6 15:20 access.log.7.gz
-rw-r----- 1 root adm 137839 сен 5 07:35 access.log.8.gz
-rw-r----- 1 root adm 103378 сен 4 07:34 access.log.9.gz
-rw-r----- 1 root adm 52229 сен 18 17:55 error.log
-rw-r----- 1 root adm 941 сен 18 17:52 error.log.1
-rw-r----- 1 root adm 456 сен 3 14:18 error.log.10.gz
-rw-r----- 1 root adm 381 авг 30 07:35 error.log.11.gz
-rw-r----- 1 root adm 416 авг 29 18:10 error.log.12.gz
-rw-r----- 1 root adm 378 авг 28 07:35 error.log.13.gz
-rw-r----- 1 root adm 380 авг 27 07:35 error.log.14.gz
-rw-r----- 1 root adm 1228 сен 12 13:47 error.log.2.gz
-rw-r----- 1 root adm 36085 сен 10 07:35 error.log.3.gz
-rw-r----- 1 root adm 375 сен 9 07:35 error.log.4.gz
-rw-r----- 1 root adm 375 сен 8 07:35 error.log.5.gz
-rw-r----- 1 root adm 377 сен 7 07:35 error.log.6.gz
-rw-r----- 1 root adm 48864 сен 6 15:20 error.log.7.gz
-rw-r----- 1 root adm 380 сен 5 07:35 error.log.8.gz
-rw-r----- 1 root adm 386 сен 4 07:35 error.log.9.gz
-rw-r----- 1 root adm 0 июн 20 2018 other_vhosts_access.log
user@web-portal-2:/var/log/apache2$


user@web-portal-2:/var/log/apache2$ grep "reporttool" access.log
10.10.1.253 - - [18/Sep/2019:17:52:31 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:52:41 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:52:51 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:53:01 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:53:12 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:53:22 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:53:32 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:53:42 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:53:52 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:54:02 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:54:12 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:54:22 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:54:32 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:54:43 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:54:53 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:55:03 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:55:13 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:55:23 +0300] "GET /reporttool.py HTTP/1.1" 404 10160 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:55:33 +0300] "GET /reporttool.py HTTP/1.1" 200 72151 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
10.10.1.253 - - [18/Sep/2019:17:55:44 +0300] "GET /reporttool.py HTTP/1.1" 200 72151 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
user@web-portal-2:/var/log/apache2$

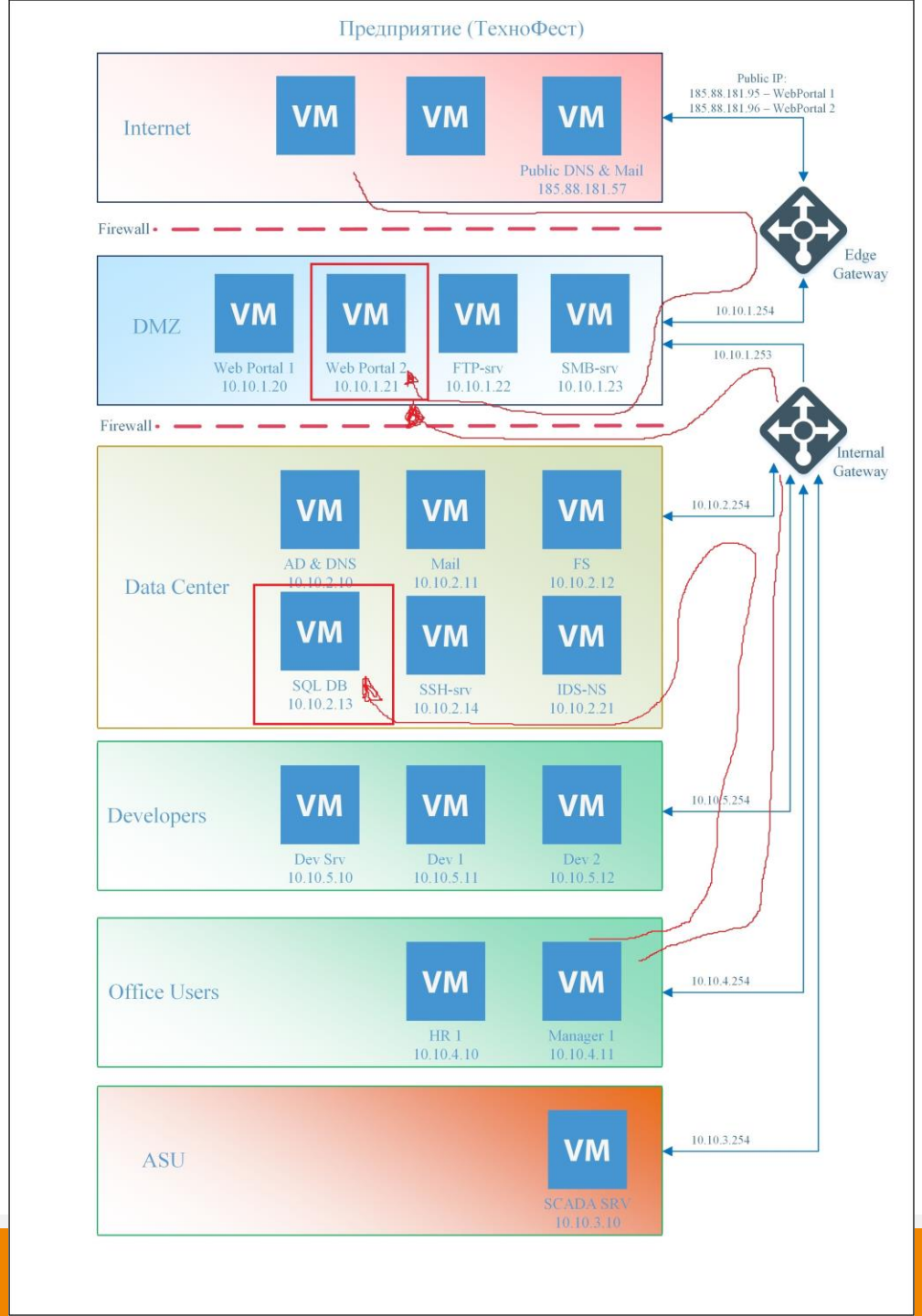

Предприятие (ТехноФест)
Internet
VM
VM
VM
Public DNS & Mail
185.88.181.57
Public IP:
185.88.181.95 – WebPortal 1
185.88.181.96 – WebPortal 2
Firewall
Edge
Gateway
10.10.1.254
10.10.1.253
DMZ
VM
VM
VM
VM
Web Portal 1
10.10.1.20
Web Portal 2
10.10.1.21
FTP-srv
10.10.1.22
SMB-srv
10.10.1.23
Firewall
Internal
Gateway
10.10.2.254
Data Center
VM
VM
VM
AD & DNS
10.10.2.10
Mail
10.10.2.11
FS
10.10.2.12
VM
VM
VM
SQL DB
10.10.2.13
SSH-srv
10.10.2.14
IDS-NS
10.10.2.21
Developers
10.10.5.254
VM
VM
VM
Dev Srv
10.10.5.10
Dev 1
10.10.5.11
Dev 2
10.10.5.12
Office Users
10.10.4.254
VM
VM
HR 1
10.10.4.10
Manager 1
10.10.4.11
ASU
10.10.3.254
VM
SCADA SRV
10.10.3.10

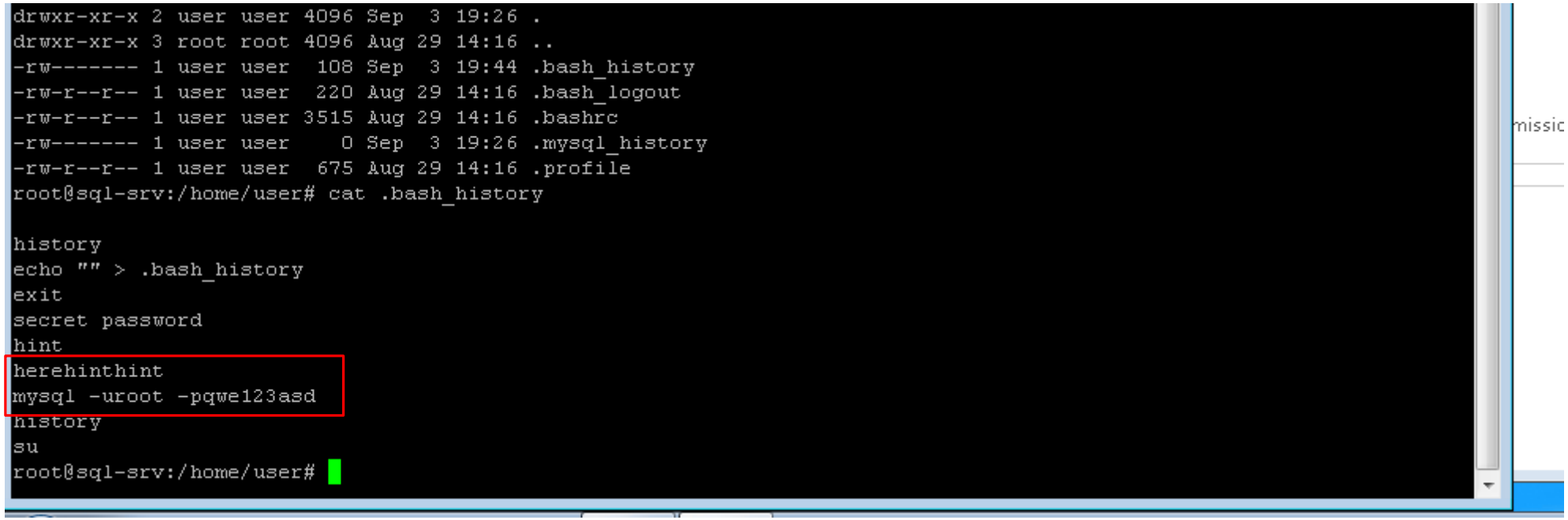

ViPNet IDS NS
mon4
Мониторинг
Инфопанель
События
Мои отчеты
Общие отчеты
Анализ трафика
Сетевое окружение
Модули сенсора
Правила обнаружения
Система
Сетевые настройки
Дата и время
Учетные записи
Резервное копирование
Обмен данными
Сервисные функции
События
События за последние 24 часа
Дата и время
Код события
Колич...
Название правила
Класс
Протокол
IP-адрес источника
Порт источн...
IP-адрес получателя
Порт получ...
Напра...
2019-09-18 17:57:09.9... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49319 10.10.2.13 22
2019-09-18 17:57:03.9... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49317 10.10.2.26 22
2019-09-18 17:56:57.8... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49314 10.10.2.15 22
2019-09-18 17:56:48.8... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49312 10.10.2.9 22
2019-09-18 17:56:42.8... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49309 10.10.2.1 22
2019-09-18 17:56:33.8... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49307 10.10.2.25 22
2019-09-18 17:56:30.7... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49305 10.10.2.18 22
2019-09-18 17:56:27.7... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49303 10.10.2.10 22
2019-09-18 17:56:26.7... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49302 10.10.2.6 22
2019-09-18 17:56:17.7... 2001219 1 ET SCAN Potential SSH Scan attempted-recon TCP 10.10.4.11 49300 10.10.2.8 22
2019-09-18 17:56:17.7... 2003068 1 ET SCAN Potential SSH Scan OUTBOU... attempted-recon TCP 10.10.4.11 49300 10.10.2.8 22
2019-09-18 17:55:13.5... 2025494 1 ET WEB_SPECIFIC_APPS [PT OPEN] Dr... attempted-admin TCP 185.88.181.55 33937 10.10.1.21 80
2019-09-18 17:55:13.5... 3023574 1 AM Exploit Drupalgeddon2 Remote Co... web-application-attack TCP 185.88.181.55 33937 10.10.1.21 80
2019-09-18 17:55:13.5... 2025807 1 ET EXPLOIT php script base64 encode... attempted-user TCP 185.88.181.55 33937 10.10.1.21 80
2019-09-18 17:55:13.2... 2025494 1 ET WEB_SPECIFIC_APPS [PT OPEN] Dr... attempted-admin TCP 185.88.181.55 45487 10.10.1.21 80
2019-09-18 17:55:13.2... 3023574 1 AM Exploit Drupalgeddon2 Remote Co... web-application-attack TCP 185.88.181.55 45487 10.10.1.21 80
2019-09-18 17:55:13.2... 2025807 1 ET EXPLOIT php script base64 encode... attempted-user TCP 185.88.181.55 45487 10.10.1.21 80
2019-09-18 17:55:13.1... 2025494 1 ET WEB_SPECIFIC_APPS [PT OPEN] Dr... attempted-admin TCP 185.88.181.55 45667 10.10.1.21 80
2019-09-18 17:55:13.1... 3023574 1 AM Exploit Drupalgeddon2 Remote Co... web-application-attack TCP 185.88.181.55 45667 10.10.1.21 80
2019-09-18 17:55:13.1... 3061696 1 AM USER_AGENTS Suspicious User-Ag... bad-unknown TCP 185.88.181.55 37105 10.10.1.21 80
2019-09-18 17:54:36.8... 2009358 1 ET SCAN Nmap Scripting Engine User-... web-application-attack TCP 185.88.181.55 37242 10.10.1.21 80
2019-09-18 17:54:36.7... 2009358 1 ET SCAN Nmap Scripting Engine User-... web-application-attack TCP 185.88.181.55 60464 10.10.1.20 80
2019-09-18 17:54:36.7... 2009358 1 ET SCAN Nmap Scripting Engine User-... web-application-attack TCP 185.88.181.55 37234 10.10.1.21 80
2019-09-18 17:54:36.7... 2009358 1 ET SCAN Nmap Scripting Engine User-... web-application-attack TCP 185.88.181.55 60452 10.10.1.20 80

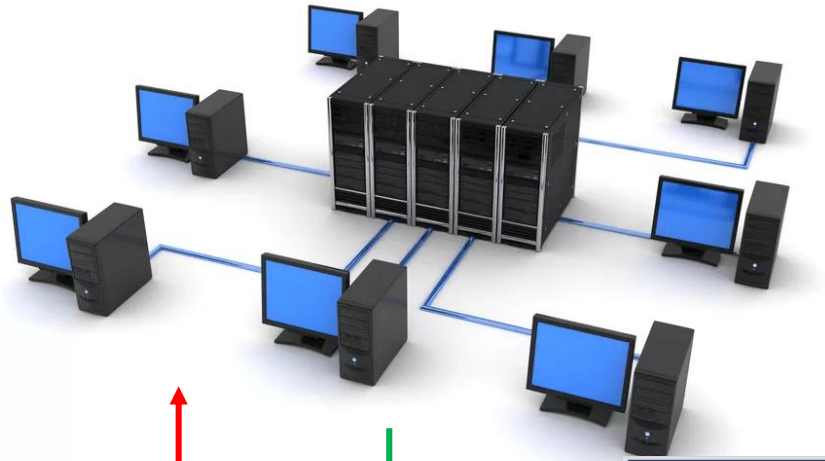

Предприятие (ТехноФест)
Internet
VM
VM
VM
Public DNS & Mail
185.88.181.57
Public IP:
185.88.181.95 – WebPortal 1
185.88.181.96 – WebPortal 2
Firewall
Edge
Gateway
10.10.1.254
10.10.1.253
DMZ
VM
VM
VM
VM
Web Portal 1
10.10.1.20
Web Portal 2
10.10.1.21
FTP-srv
10.10.1.22
SMB-srv
10.10.1.23
Firewall
Internal
Gateway
10.10.2.254
Data Center
VM
VM
VM
AD & DNS
10.10.2.10
Mail
10.10.2.11
FS
10.10.2.12
VM
VM
VM
SQL DB
10.10.2.13
SSH-srv
10.10.2.14
IDS-NS
10.10.2.21
Developers
10.10.5.254
VM
VM
VM
Dev Srv
10.10.5.10
Dev 1
10.10.5.11
Dev 2
10.10.5.12
Office Users
10.10.4.254
VM
VM
HR 1
10.10.4.10
Manager 1
10.10.4.11
ASU
10.10.3.254
VM
SCADA SRV
10.10.3.10

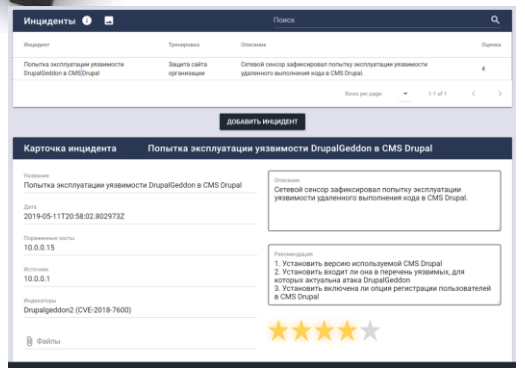
```
Sep 18 17:47:28 sql-srv systemd-logind[461]: New seat seat0.
Sep 18 17:47:28 sql-srv systemd-logind[461]: Watching system buttons on /dev/input/event2 (Power Button)
Sep 18 17:47:28 sql-srv sshd[482]: Server listening on 0.0.0.0 port 22.
Sep 18 17:47:28 sql-srv sshd[482]: Server listening on :: port 22.
Sep 18 17:57:32 sql-srv sshd[1277]: Did not receive identification string from 10.10.4.11
Sep 18 17:59:20 sql-srv sshd[1279]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruse
r= rhost=10.10.4.11  user=user
Sep 18 17:59:22 sql-srv sshd[1279]: Failed password for user from 10.10.4.11 port 49334 ssh2
Sep 18 17:59:24 sql-srv sshd[1279]: Failed password for user from 10.10.4.11 port 49334 ssh2
Sep 18 17:59:28 sql-srv sshd[1279]: Failed password for user from 10.10.4.11 port 49334 ssh2
Sep 18 17:59:28 sql-srv sshd[1279]: Disconnecting: Too many authentication failures for user from 10.10.4.11 port 4
9334 ssh2 [preauth]
Sep 18 17:59:28 sql-srv sshd[1279]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=
10.10.4.11  user=user
Sep 18 17:59:51 sql-srv sshd[1281]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruse
r= rhost=10.10.4.11  user=user
Sep 18 17:59:53 sql-srv sshd[1281]: Failed password for user from 10.10.4.11 port 49335 ssh2
Sep 18 17:59:56 sql-srv sshd[1281]: Failed password for user from 10.10.4.11 port 49335 ssh2
Sep 18 17:59:59 sql-srv sshd[1281]: Failed password for user from 10.10.4.11 port 49335 ssh2
Sep 18 17:59:59 sql-srv sshd[1281]: Disconnecting: Too many authentication failures for user from 10.10.4.11 port 4
9335 ssh2 [preauth]
Sep 18 17:59:59 sql-srv sshd[1281]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=
10.10.4.11  user=user
Sep 18 18:00:22 sql-srv sshd[1283]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruse
r= rhost=10.10.4.11  user=user
Sep 18 18:00:24 sql-srv sshd[1283]: Failed password for user from 10.10.4.11 port 49336 ssh2
Sep 18 18:00:27 sql-srv sshd[1283]: Failed password for user from 10.10.4.11 port 49336 ssh2
Sep 18 18:00:30 sql-srv sshd[1283]: Failed password for user from 10.10.4.11 port 49336 ssh2
Sep 18 18:00:31 sql-srv sshd[1283]: Disconnecting: Too many authentication failures for user from 10.10.4.11 port 4
9336 ssh2 [preauth]
Sep 18 18:00:31 sql-srv sshd[1283]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=
10.10.4.11  user=user
Sep 18 18:00:53 sql-srv sshd[1285]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruse
r= rhost=10.10.4.11  user=user
Sep 18 18:00:55 sql-srv sshd[1285]: Failed password for user from 10.10.4.11 port 49337 ssh2
Sep 18 18:00:56 sql-srv sshd[1285]: Accepted password for user from 10.10.4.11 port 49337 ssh2
Sep 18 18:00:56 sql-srv sshd[1285]: pam_unix(sshd:session): session opened for user user by (uid=0)
Sep 18 18:00:57 sql-srv sshd[1287]: Received disconnect from 10.10.4.11: 11:
Sep 18 18:00:57 sql-srv sshd[1285]: pam_unix(sshd:session): session closed for user user
Sep 18 18:01:32 sql-srv sshd[1288]: Accepted password for user from 10.10.4.11 port 49339 ssh2
Sep 18 18:01:32 sql-srv sshd[1288]: pam_unix(sshd:session): session opened for user user by (uid=0)
Sep 18 18:01:34 sql-srv sshd[1288]: pam_unix(sshd:session): session closed for user user
Sep 18 18:17:01 sql-srv CRON[1299]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 18 18:17:01 sql-srv CRON[1299]: pam_unix(cron:session): session closed for user root
Sep 18 18:18:59 sql-srv sshd[1303]: Accepted password for user from 10.10.4.12 port 49294 ssh2
Sep 18 18:18:59 sql-srv sshd[1303]: pam_unix(sshd:session): session opened for user user by (uid=0)
Sep 18 18:20:10 sql-srv su[1331]: Successful su for root by user
Sep 18 18:20:10 sql-srv su[1331]: + /dev/pts/0 user:root
Sep 18 18:20:10 sql-srv su[1331]: pam_unix(su:session): session opened for user root by user(uid=1000)
(END)
```

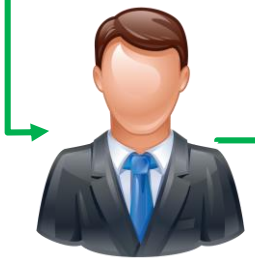
missions.


Предприятие (ТехноФест)
Internet
VM
VM
VM
Public DNS & Mail
185.88.181.57
Public IP:
185.88.181.95 – WebPortal 1
185.88.181.96 – WebPortal 2
Firewall
Edge
Gateway
10.10.1.254
10.10.1.253
DMZ
VM
VM
VM
VM
Web Portal 1
10.10.1.20
Web Portal 2
10.10.1.21
FTP-srv
10.10.1.22
SMB-srv
10.10.1.23
Firewall
Internal
Gateway
10.10.2.254
Data Center
VM
VM
VM
AD & DNS
10.10.2.10
Mail
10.10.2.11
FS
10.10.2.12
VM
VM
VM
SQL DB
10.10.2.13
SSH-srv
10.10.2.14
IDS-NS
10.10.2.21
Developers
10.10.5.254
VM
VM
VM
Dev Srv
10.10.5.10
Dev 1
10.10.5.11
Dev 2
10.10.5.12
Office Users
10.10.4.254
VM
VM
HR 1
10.10.4.10
Manager 1
10.10.4.11
ASU
10.10.3.254
VM
SCADA SRV
10.10.3.10


drwxr-xr-x 2 user user 4096 Sep 3 19:26 .
drwxr-xr-x 3 root root 4096 Aug 29 14:16 ..
-rw------- 1 user user 108 Sep 3 19:44 .bash_history
-rw-r--r-- 1 user user 220 Aug 29 14:16 .bash_logout
-rw-r--r-- 1 user user 3515 Aug 29 14:16 .bashrc
-rw------- 1 user user 0 Sep 3 19:26 .mysql_history
-rw-r--r-- 1 user user 675 Aug 29 14:16 .profile
root@sql-srv:/home/user# cat .bash_history
history
echo "" > .bash_history
exit
secret password
hint
herehinthint
mysql -uroot -pqwe123asd
history
su
root@sql-srv:/home/user#

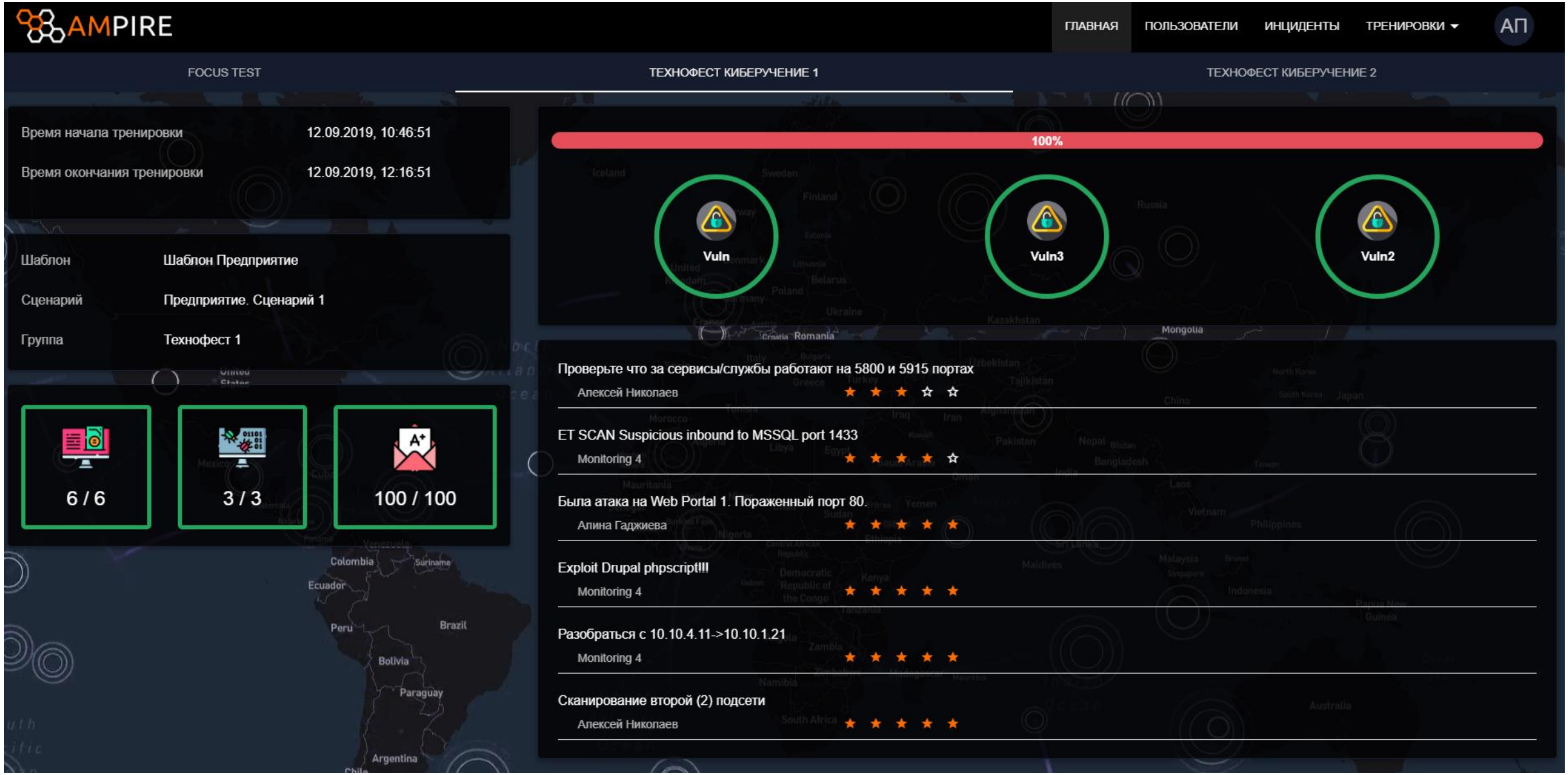






Группа мониторинга

Группа реагирования


AMPIRE
ГЛАВНАЯ
ПОЛЬЗОВАТЕЛИ
ИНЦИДЕНТЫ
ТРЕНИРОВКИ
АП
FOCUS TEST
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 1
ТЕХНОФЕСТ КИБЕРУЧЕНИЕ 2
Время начала тренировки 12.09.2019, 10:46:51
Время окончания тренировки 12.09.2019, 12:16:51
Шаблон Шаблон Предприятие
Сценарий Предприятие. Сценарий 1
Группа Технофест 1
6 / 6
3 / 3
100 / 100
100%
Vuln
Vuln3
Vuln2
Проверьте что за сервисы/службы работают на 5800 и 5915 портах
Алексей Николаев
ET SCAN Suspicious inbound to MSSQL port 1433
Monitoring 4
Была атака на Web Portal 1. Пораженный порт 80.
Алина Гаджиева
Exploit Drupal phpscript!!!
Monitoring 4
Разобраться с 10.10.4.11->10.10.1.21
Monitoring 4
Сканирование второй (2) подсети
Алексей Николаев

Спасибо за внимание!

Пушкин Александр Несергеевич

Технический директор

компании «Перспективный мониторинг»

Aleksandr.Pushkin@amonitoring.ru