ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Мониторинг, анализ и расследование инцидентов с помощью программного комплекса обучения «Ampire»

Александр Сальников
старший специалист по ИБ

Персонал

Первая линия	Вторая линия	Третья линия
Взаимодействие с пользователями	Помощь в расследовании и установлении причин инцидентов	Подготовка и улучшение нормативной базы, описание сценариев выявленных инцидентов
Анализ событий и обнаружение компьютерных атак и инцидентов	Координация действий при реагировании на инциденты ИБ	Разработка сигнатурных правил и правил корреляции
Регистрация инцидентов ИБ и оповещение заинтересованных лиц	Анализ уязвимостей, анализ защищенности, тестирование на проникновение	Углубленный анализ инцидентов ИБ, сбор доказательной базы

Схема подключения

СБОР СОБЫТИЙ

Сетевые IDS

Хостовые IDS

DNS, DHCP, AV,
VPN, FW, Mail...

АНАЛИЗ И ВЫЯВЛЕНИЕ

TIAS

LogCollector

ОБОГАЩЕНИЕ И РЕАГИРОВАНИЕ

Фиды угроз
и уязвимостей

TI Platform

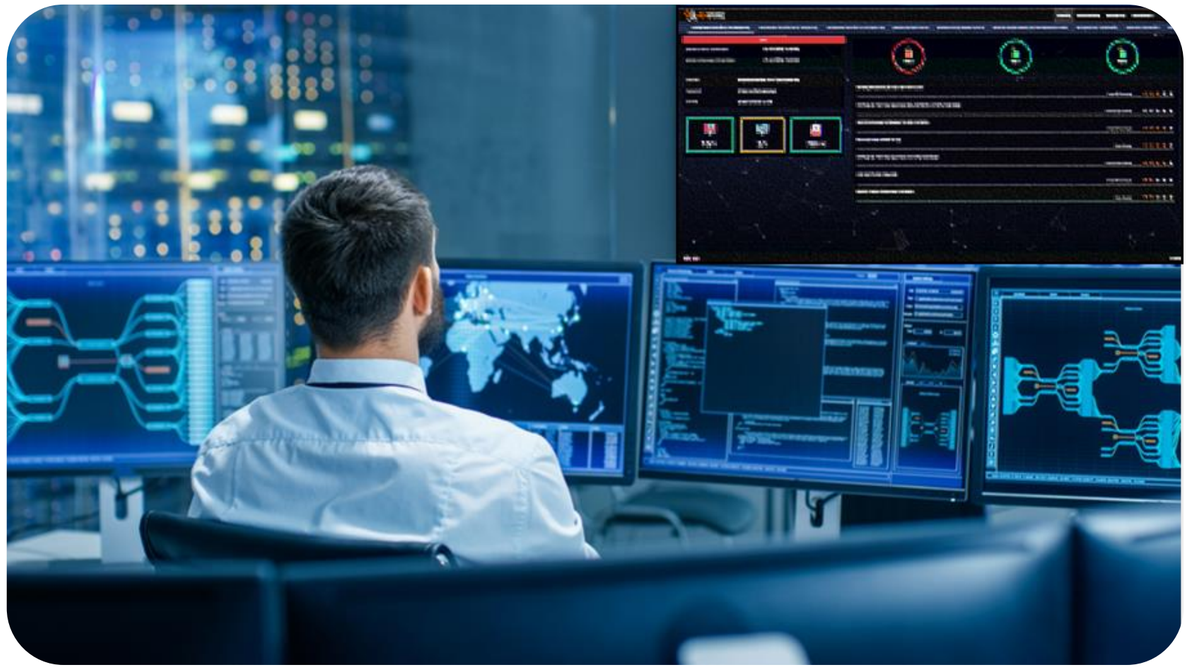
Incident
Management

ТИ НКЦКИ

Проведение киберучений на базе ПК

Киберучения – это процесс моделирования целевых компьютерных атак на некую ИТ-инфраструктуру с акцентом в сторону отработки навыков защиты:

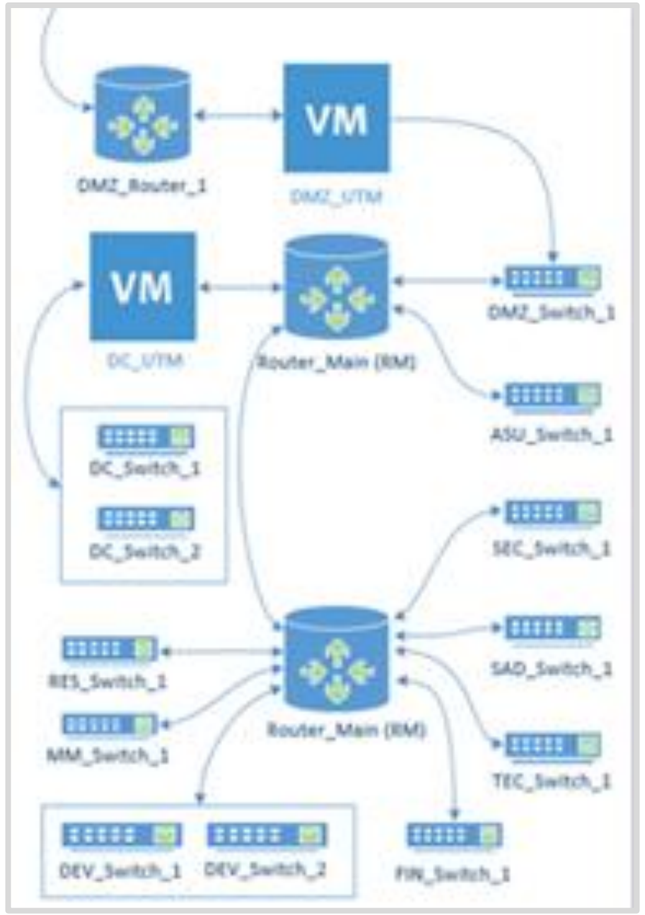
- анализ событий ИБ;
- регистрация и расследование инцидентов ИБ;
- устранение причин успешного выполнения КА;
- командное взаимодействие.



Ampire - это платформа

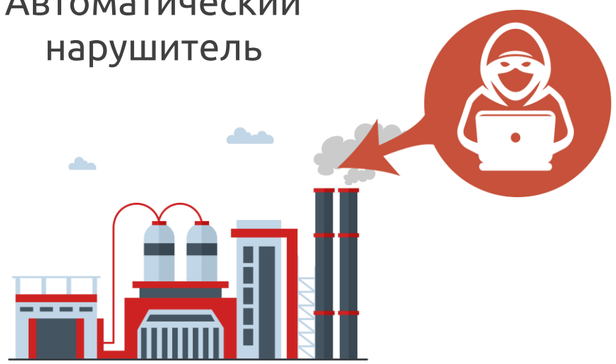
Практические занятия на цифровом двойнике реальной инфраструктуры

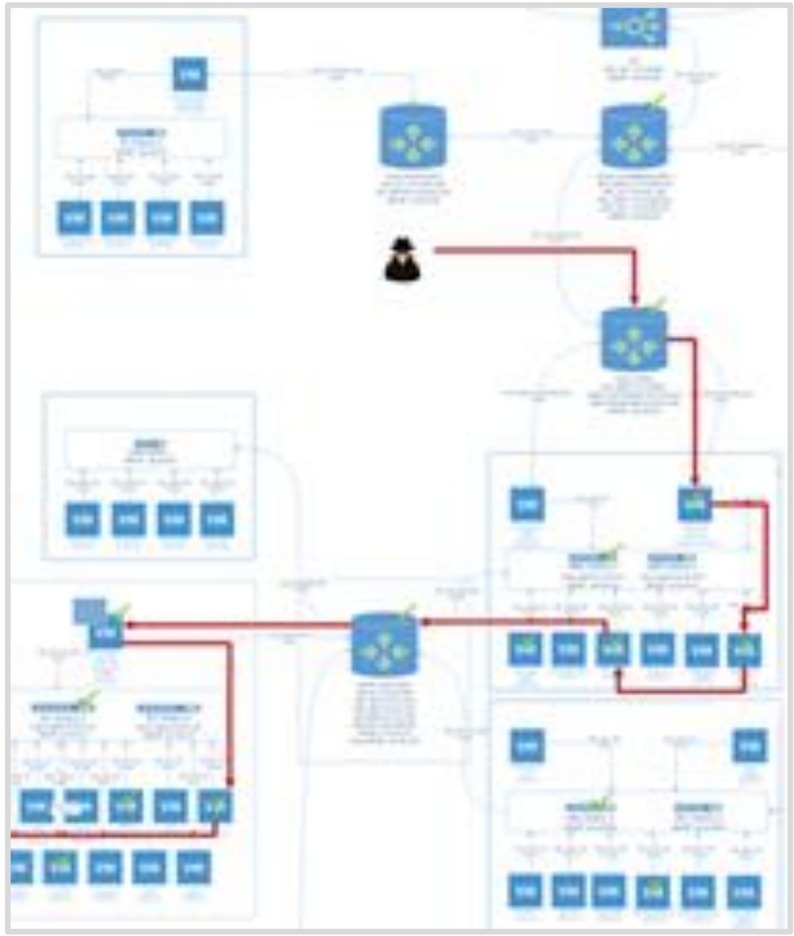
Симуляция сети с ИТ и SCADA-сегментами



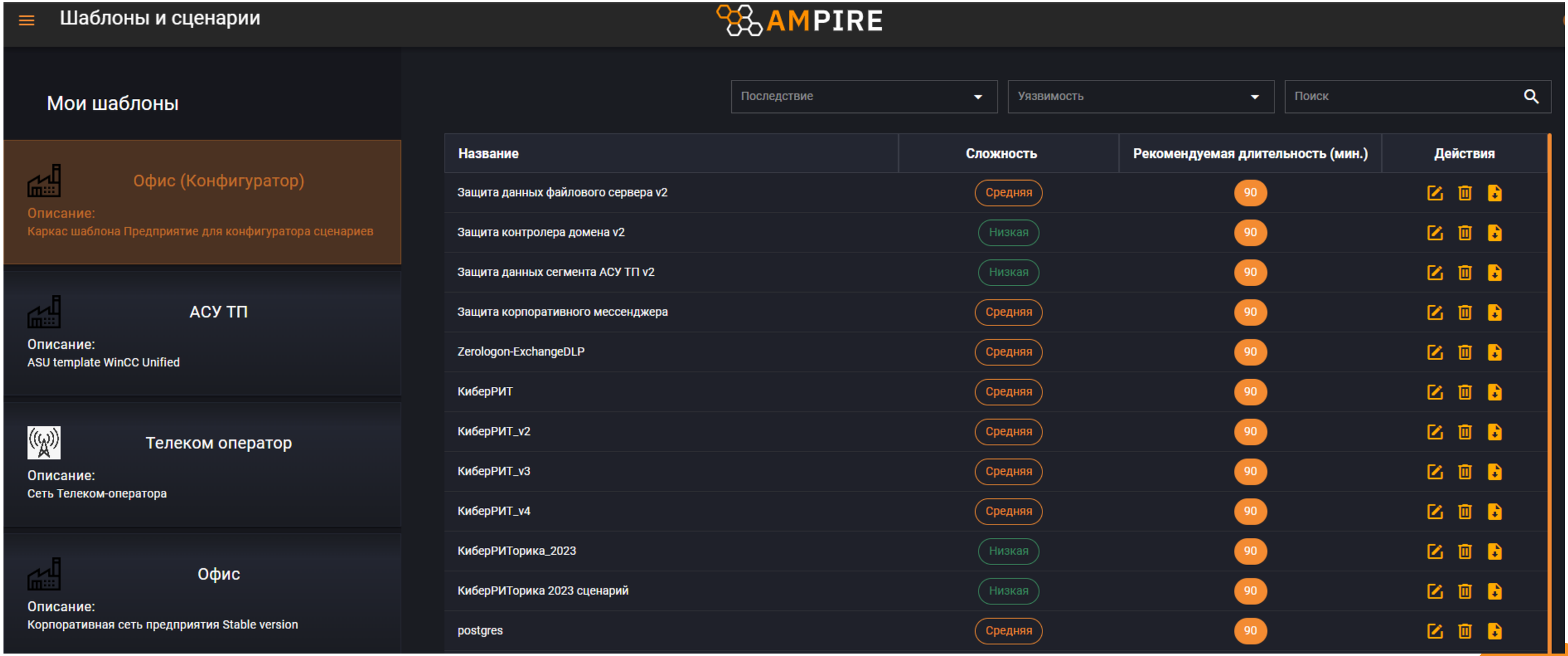
Security Operations Center

Автоматический нарушитель

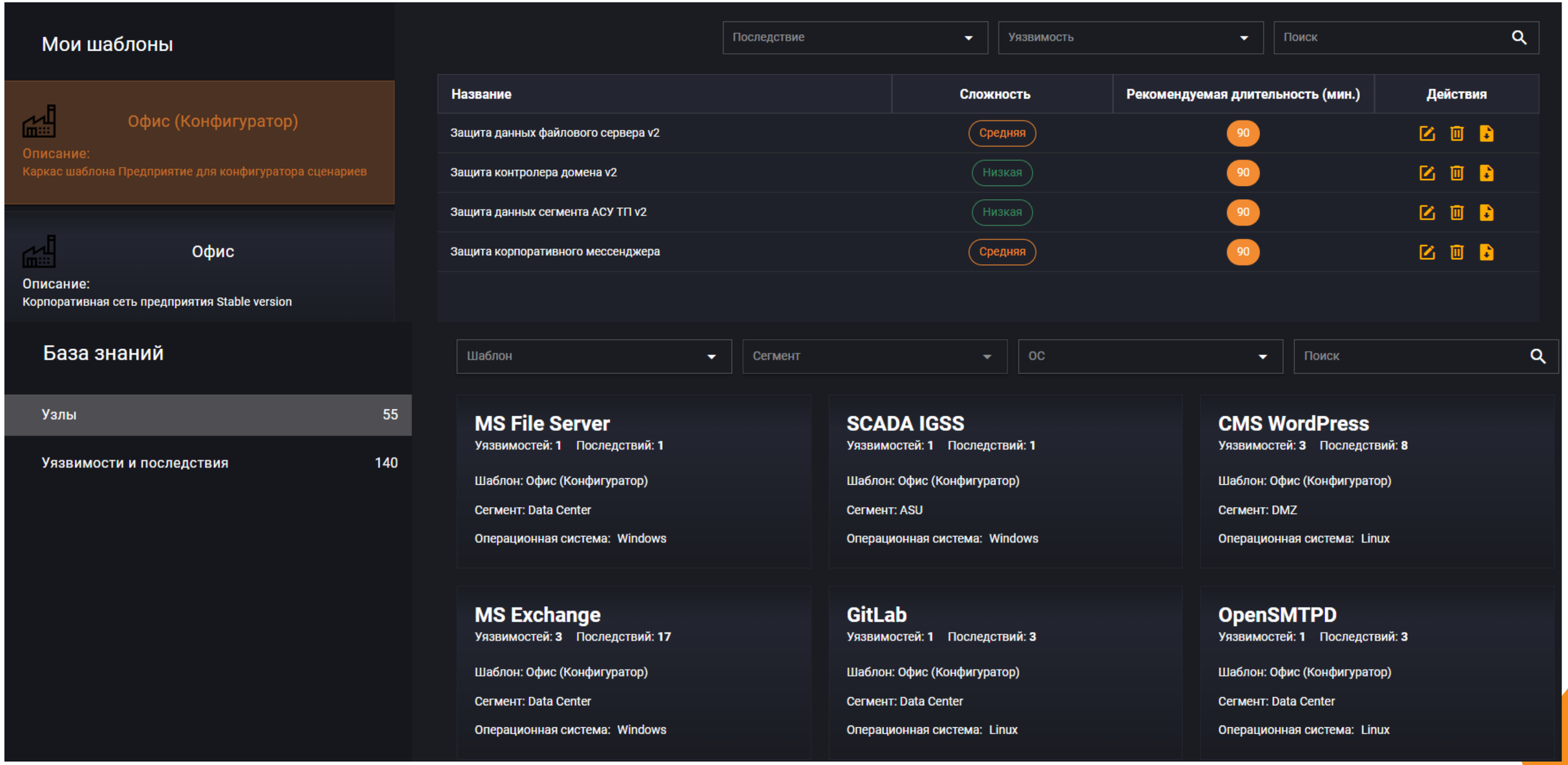




Базовые сценарии



Конфигуратор



Конфигуратор

Узел	Уязвимость	Последствие
WebPortal_3	Duplicator	Meterpreter Deface DB dump
Mail	ProxyLogon	Crypt DB Registry backdoor Service backdoor IIS backdoor China Chopper
GitLab*	GitLab RCE	Deleter Meterpreter Dump
AD	Zerologon	Backdoor Autorun User Crypt Python backdoor Registry
OpenSMTPD	CVE-2020-7247	User Meterpreter Backdoor
WebPortal_3_2	wpDiscuz	Deface Meterpreter

Узел	Уязвимость	Последствие
SuiteCRM	CVE-2021-41773	Backdoor Deface Meterpreter
	CVE-2021-4034	Meterpreter User Deleter Dump Backdoor
RocketChat	CVE-2021-22911 CVE-2022-0847	Meter Backdoor User Deleter
GravCMS*	CVE-2021-21425	Meter Deface Dump LPE
Apache Solr*	CVE-2021-44228	Shell Add user
Umbraco*	CVE-2020-9472	Meterpreter Add user Reg backdoor Service backdoor Webshell backdoor

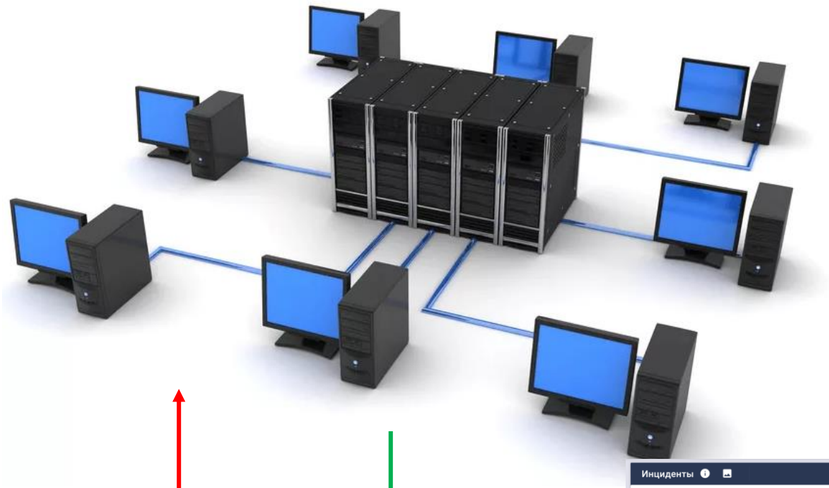
Цели киберучений

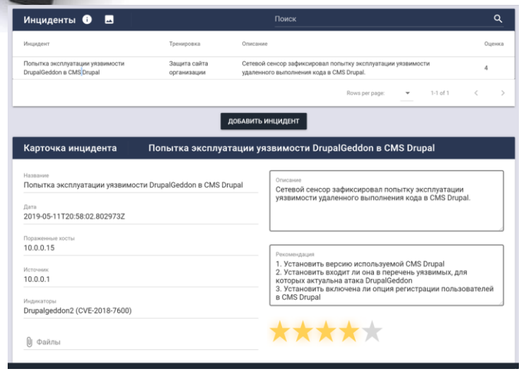
Отработка действий SOC

Научиться выявлять компьютерные атаки

Наладить взаимодействие между подразделениями

Устранить существующие уязвимости





Группа мониторинга

Группа реагирования

Легенда

Защита сегмента АСУ ТП

Внешний злоумышленник находит в Интернете сайт Компании, использующий CMS Wordpress, и решает провести атаку на него с целью получения доступа к внутренним ресурсам.

Проэксплуатировав обнаруженную на сайте уязвимость, нарушитель стремится захватить управление над другими ресурсами защищаемой сети, в том числе закрепиться на контроллере домена Active Directory.

Далее злоумышленник успешно развивает атаку в сторону сегмента АСУ ТП.

Квалификация нарушителя высокая. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

Задачи групп

Группа мониторинга

mon1
mon2
mon3
mon4

Анализ событий ИБ

Заведение карточек инцидентов

Описание вектора атаки (Cyber Kill Chain)

Группа реагирования

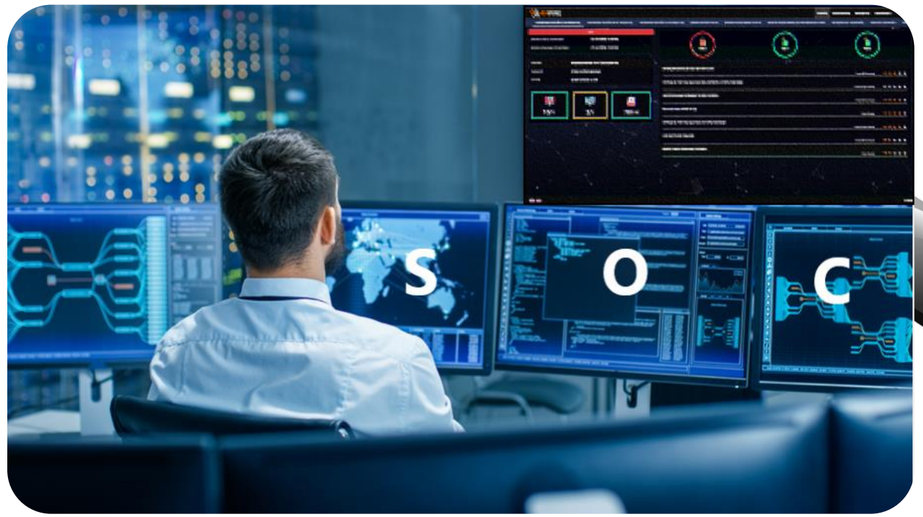
it1 лидер
it2
It3
it4

Расследование инцидентов

Устранение уязвимостей

Задачи групп

Мониторинг



Анализ событий ИБ

Заведение карточек инцидентов

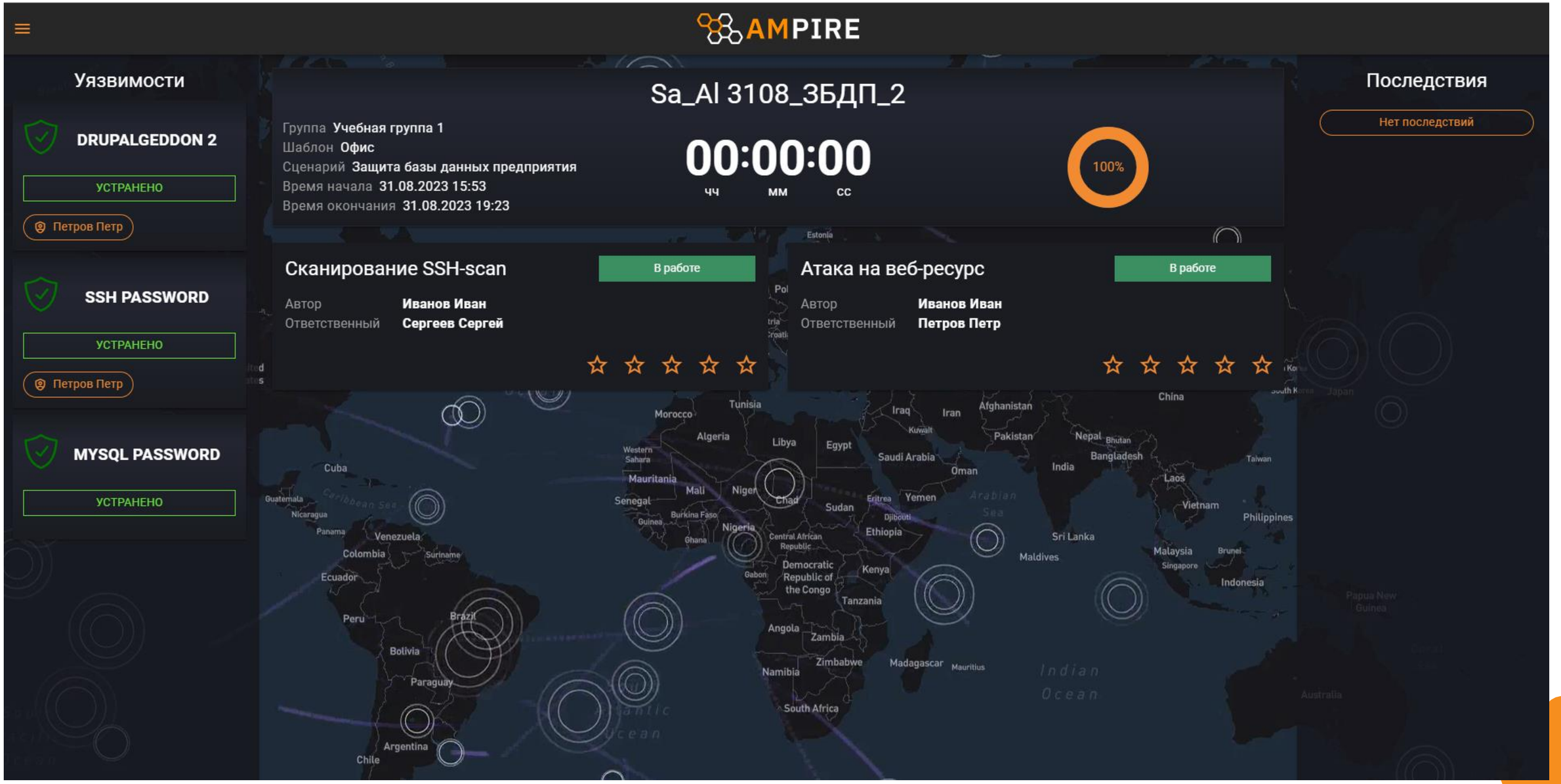
Описание вектора атаки (Cyber Kill Chain)

Реагирование

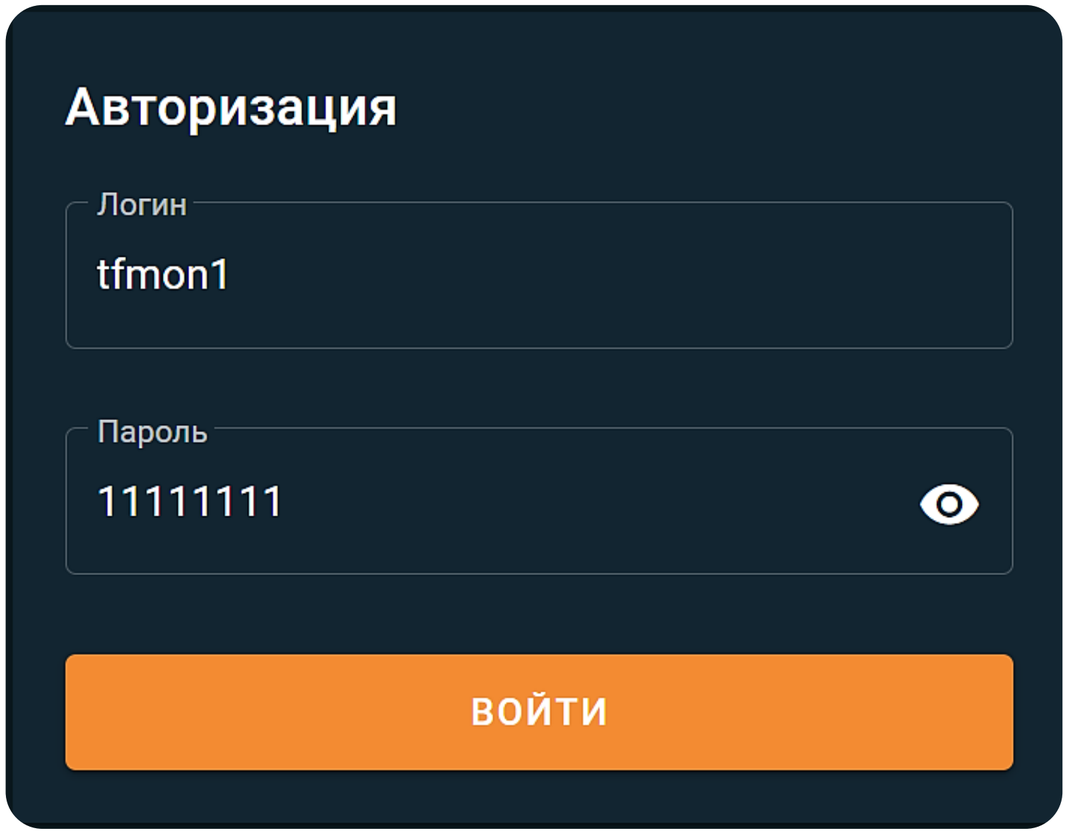
Расследование инцидентов

Устранение уязвимостей

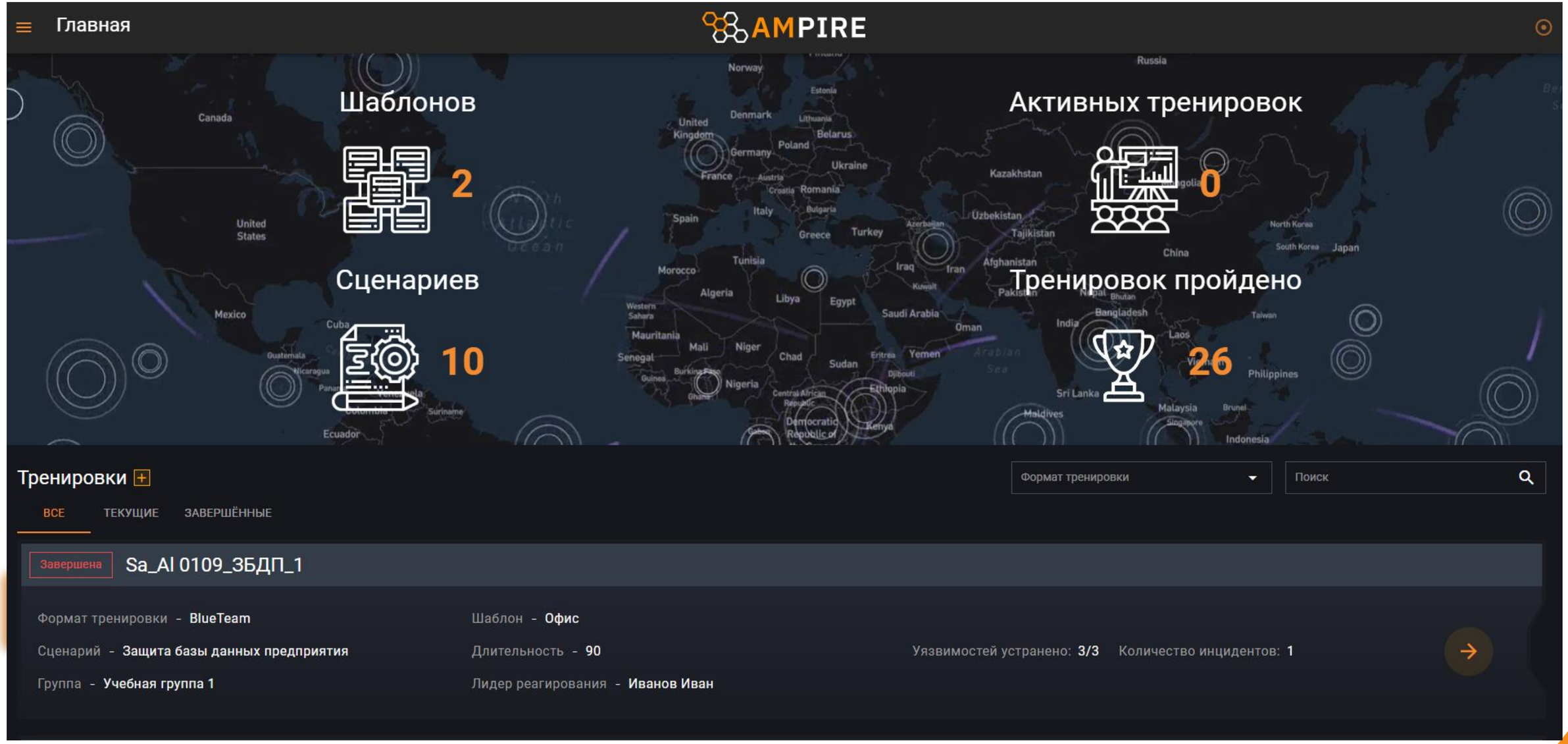
Информационная панель



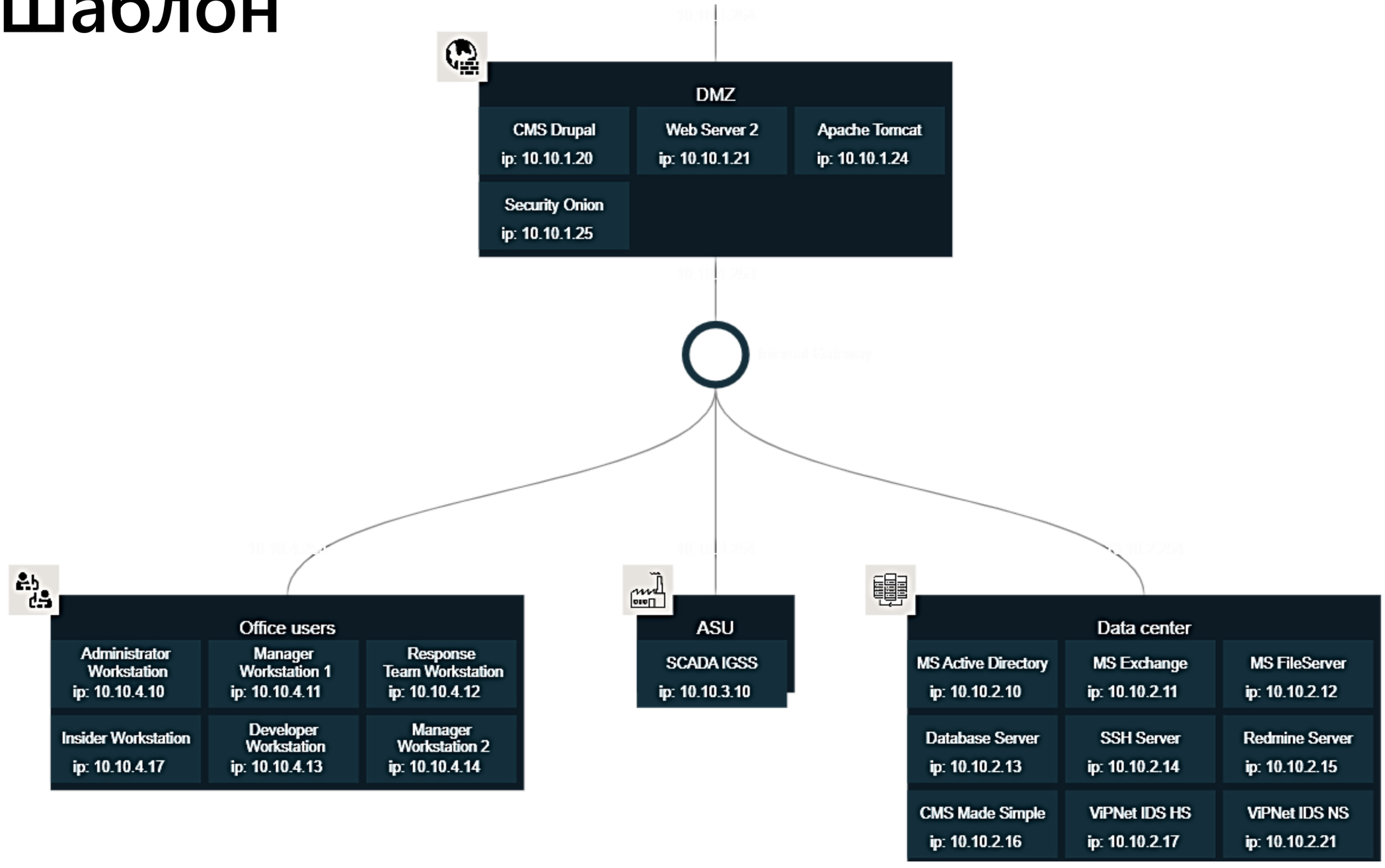
Стартовая страница



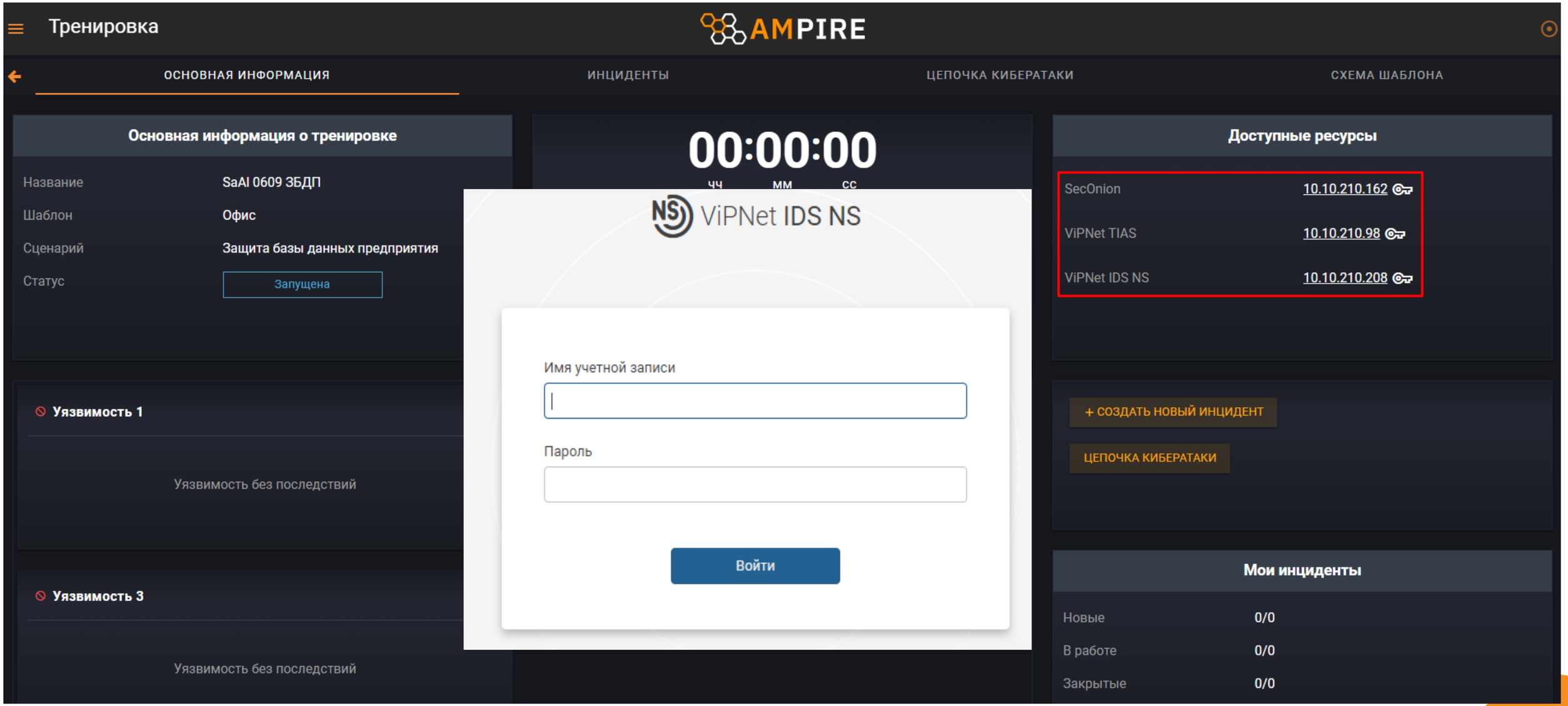
Мониторинг


Главная
AMPIRE
Шаблонов
2
Сценариев
10
Активных тренировок
0
Тренировок пройдено
26
Тренировки
Формат тренировки
Поиск
ВСЕ
ТЕКУЩИЕ
ЗАВЕРШЁННЫЕ
Завершена
Sa_AI 0109_ЗБДП_1
Формат тренировки - BlueTeam
Шаблон - Офис
Сценарий - Защита базы данных предприятия
Длительность - 90
Уязвимостей устранено: 3/3
Количество инцидентов: 1
Группа - Учебная группа 1
Лидер реагирования - Иванов Иван

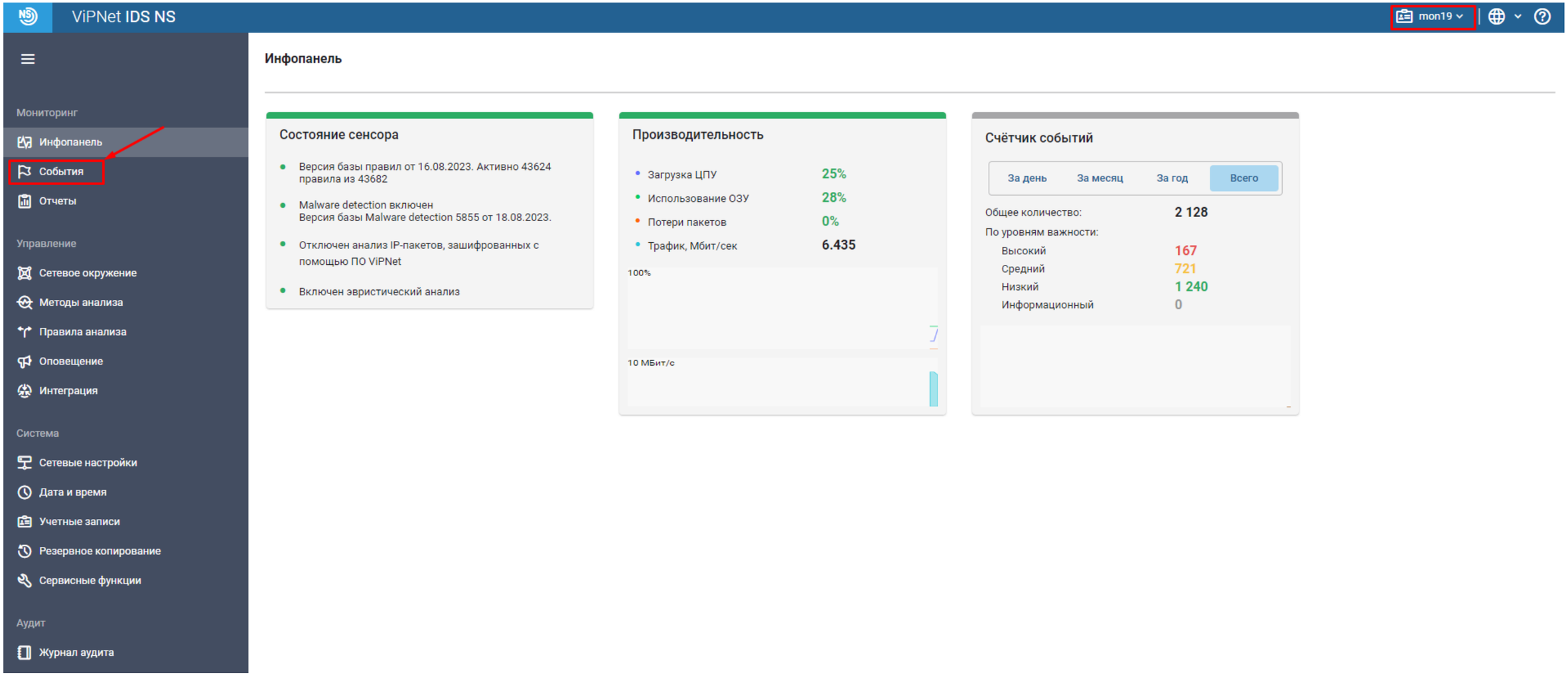
Шаблон


DMZ
CMS Drupal
ip: 10.10.1.20
Web Server 2
ip: 10.10.1.21
Apache Tomcat
ip: 10.10.1.24
Security Onion
ip: 10.10.1.25
Office users
Administrator Workstation
ip: 10.10.4.10
Manager Workstation 1
ip: 10.10.4.11
Response Team Workstation
ip: 10.10.4.12
Insider Workstation
ip: 10.10.4.17
Developer Workstation
ip: 10.10.4.13
Manager Workstation 2
ip: 10.10.4.14
ASU
SCADA IGSS
ip: 10.10.3.10
Data center
MS Active Directory
ip: 10.10.2.10
MS Exchange
ip: 10.10.2.11
MS FileServer
ip: 10.10.2.12
Database Server
ip: 10.10.2.13
SSH Server
ip: 10.10.2.14
Redmine Server
ip: 10.10.2.15
CMS Made Simple
ip: 10.10.2.16
ViPNet IDS HS
ip: 10.10.2.17
ViPNet IDS NS
ip: 10.10.2.21

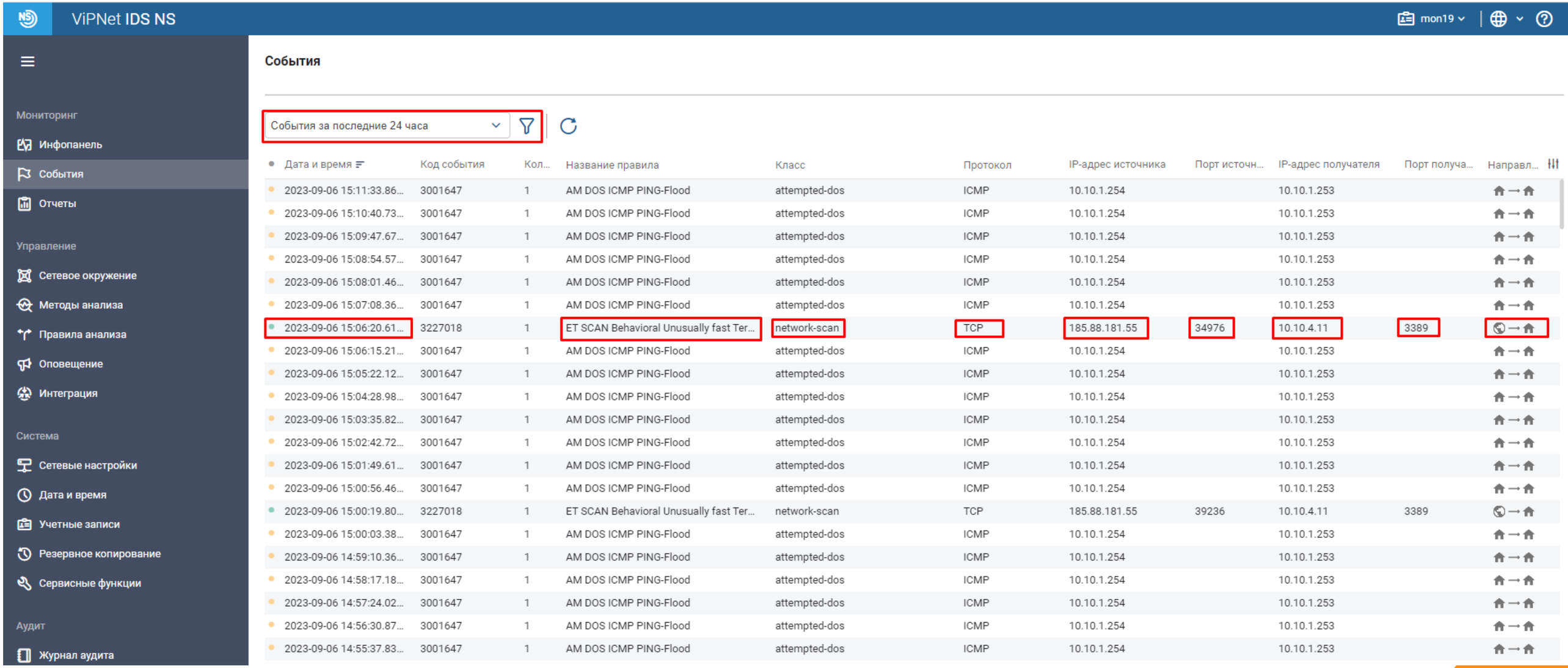
Мониторинг


Тренировка
AMPIRE
ОСНОВНАЯ ИНФОРМАЦИЯ
ИНЦИДЕНТЫ
ЦЕПОЧКА КИБЕРАТАКИ
СХЕМА ШАБЛОНА
Основная информация о тренировке
Название
SaAI 0609 ЗБДП
Шаблон
Офис
Сценарий
Защита базы данных предприятия
Статус
Запущена
00:00:00
ЧЧ
ММ
СС
ViPNet IDS NS
Имя учетной записи
Пароль
Войти
Доступные ресурсы
SecOnion
10.10.210.162
ViPNet TIAS
10.10.210.98
ViPNet IDS NS
10.10.210.208
Уязвимость 1
Уязвимость без последствий
Уязвимость 3
Уязвимость без последствий
+ СОЗДАТЬ НОВЫЙ ИНЦИДЕНТ
ЦЕПОЧКА КИБЕРАТАКИ
Мои инциденты
Новые
0/0
В работе
0/0
Закрытые
0/0

Интерфейс ViPNet IDS NS

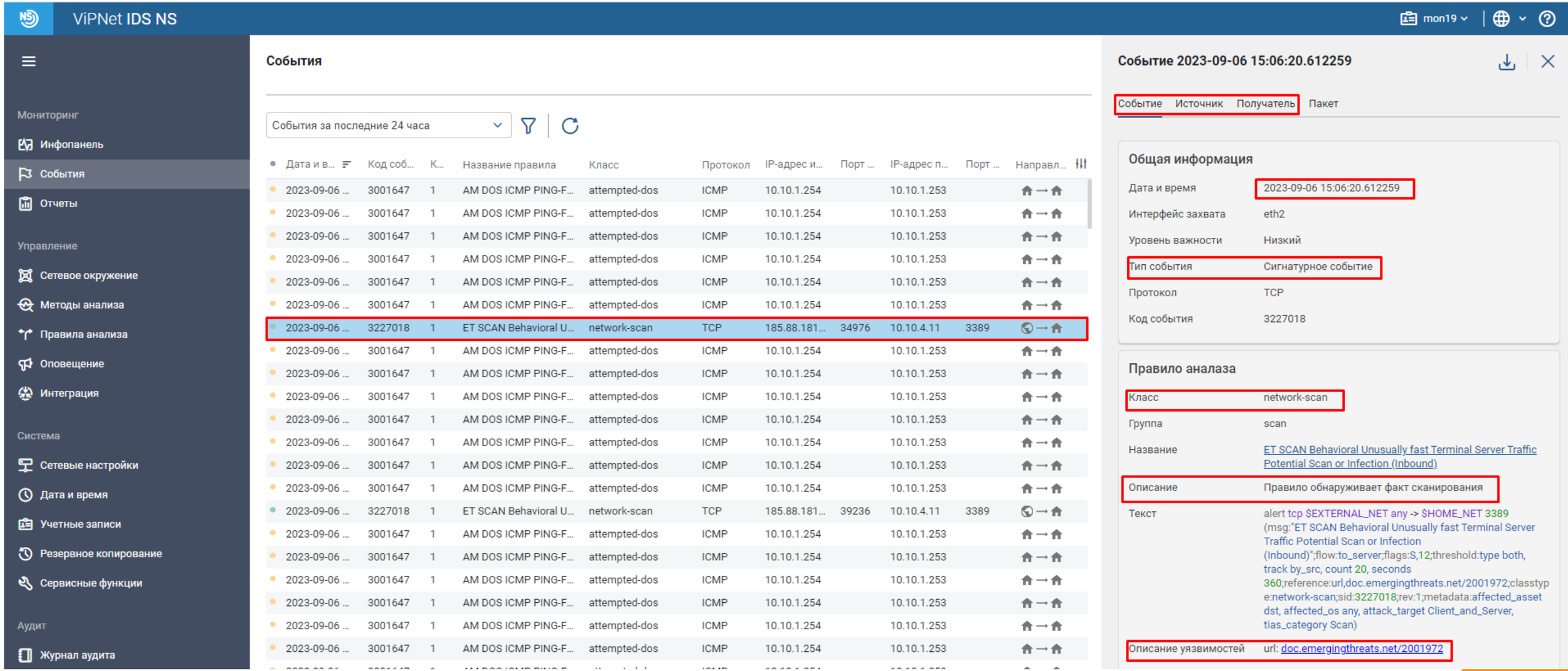


События ИБ в ViPNet IDS NS

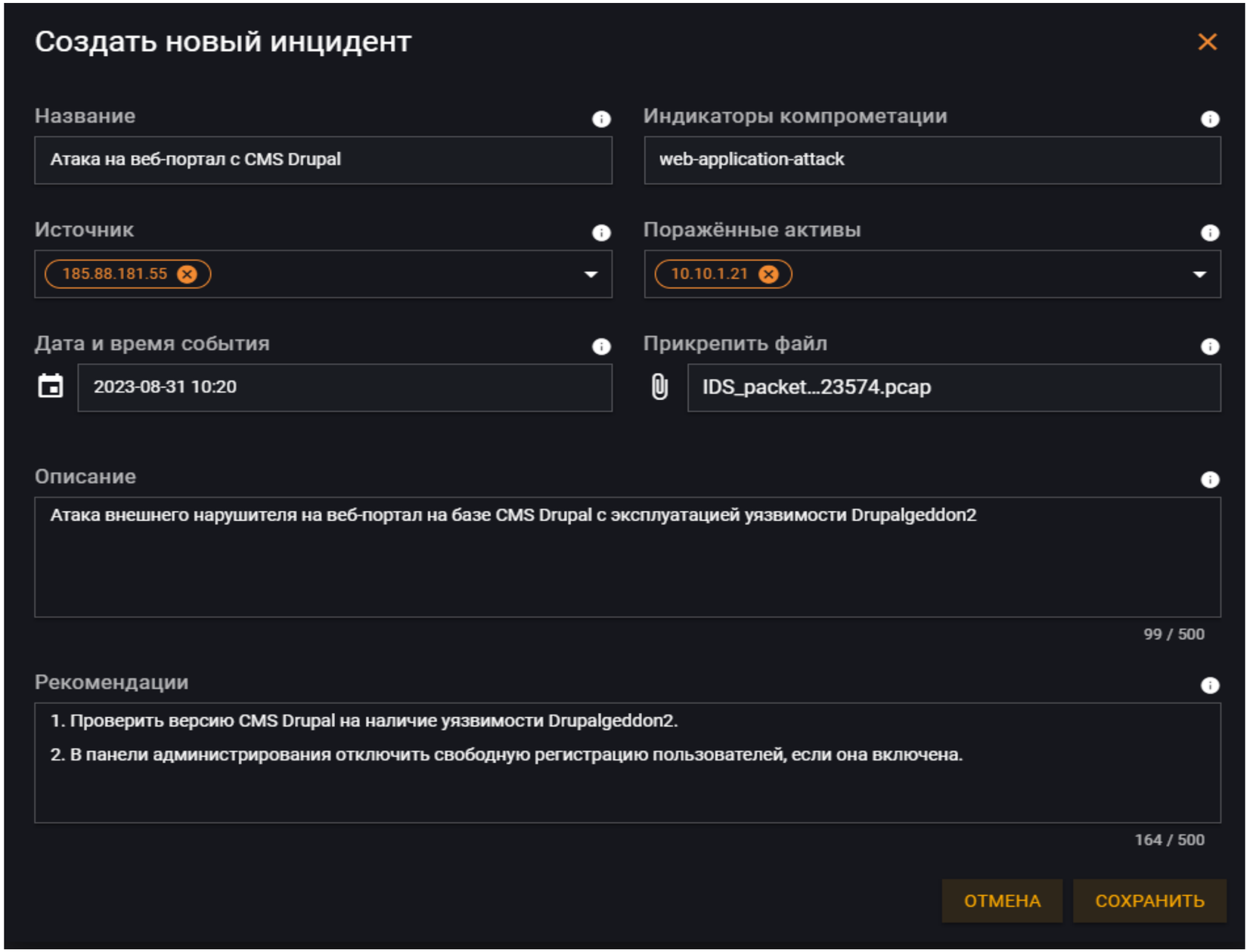


Дата и время	Код события	Кол...	Название правила	Класс	Протокол	IP-адрес источника	Порт источн...	IP-адрес получателя	Порт получа...	Направл...
2023-09-06 15:11:33.86...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:10:40.73...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:09:47.67...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:08:54.57...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:08:01.46...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:07:08.36...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:06:20.61...	3227018	1	ET SCAN Behavioral Unusually fast Ter...	network-scan	TCP	185.88.181.55	34976	10.10.4.11	3389	
2023-09-06 15:06:15.21...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:05:22.12...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:04:28.98...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:03:35.82...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:02:42.72...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:01:49.61...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:00:56.46...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 15:00:19.80...	3227018	1	ET SCAN Behavioral Unusually fast Ter...	network-scan	TCP	185.88.181.55	39236	10.10.4.11	3389	
2023-09-06 15:00:03.38...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 14:59:10.36...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 14:58:17.18...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 14:57:24.02...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 14:56:30.87...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		
2023-09-06 14:55:37.83...	3001647	1	AM DOS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		

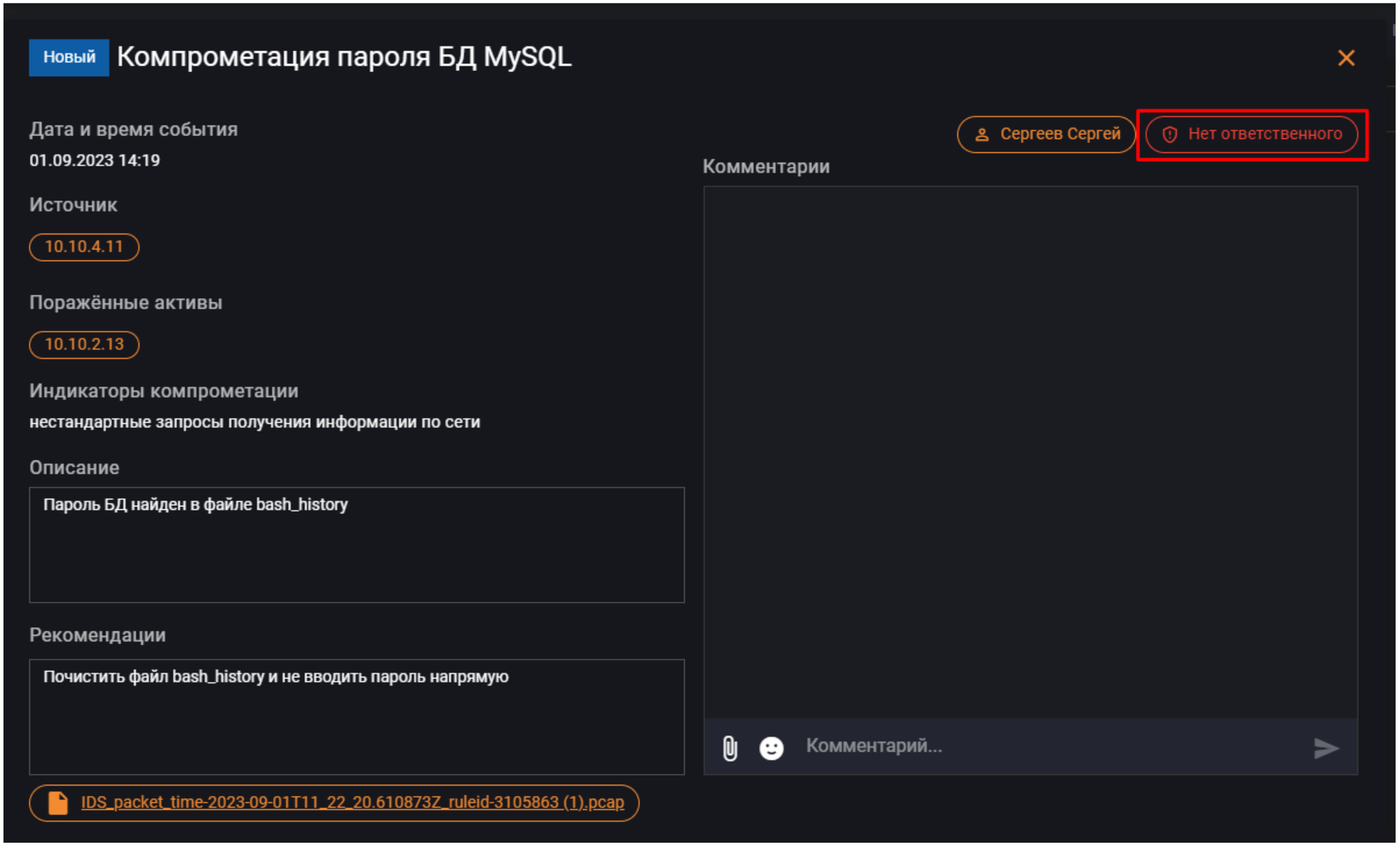
Карточка события ИБ



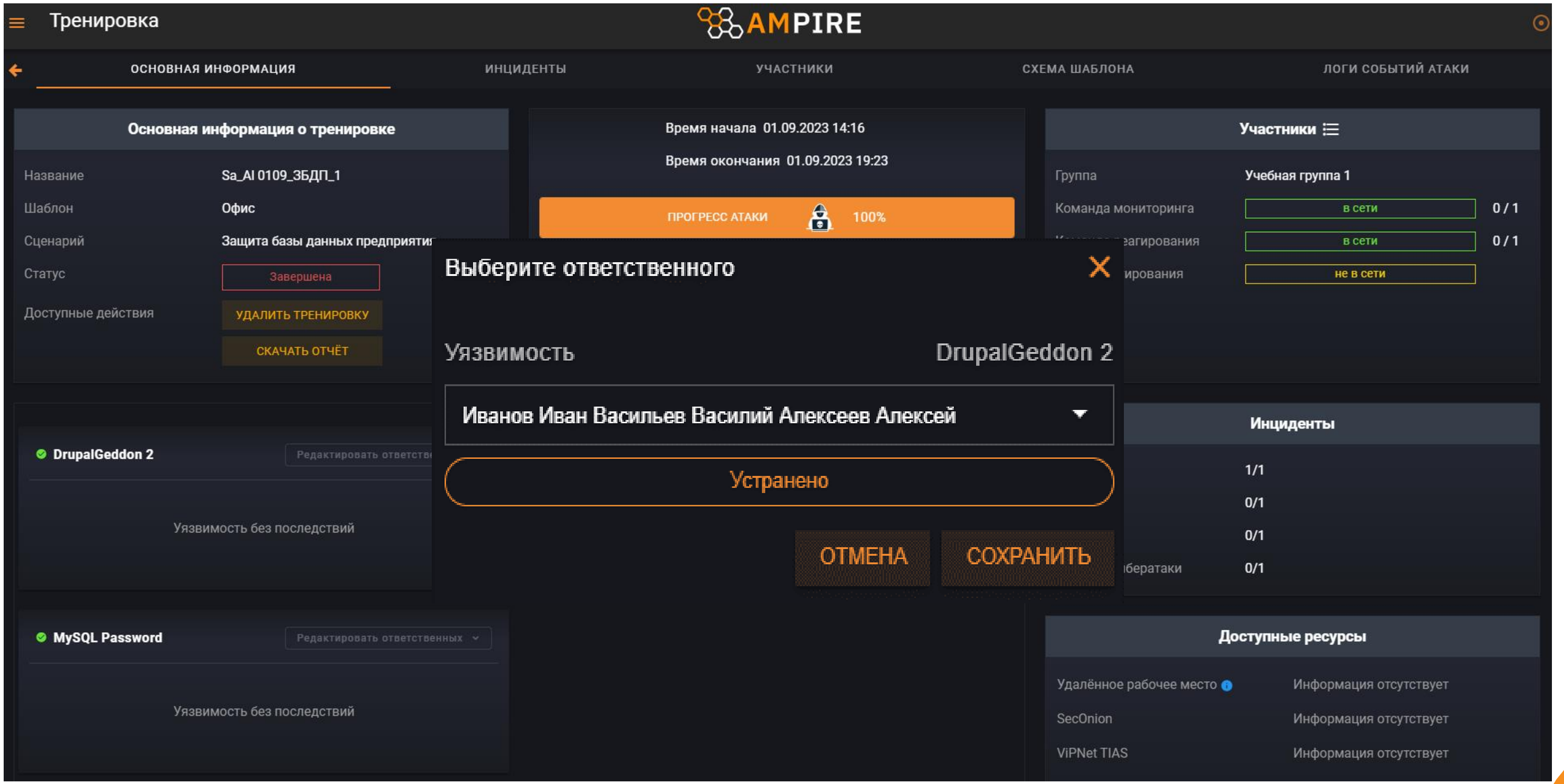
Карточка инцидента ИБ



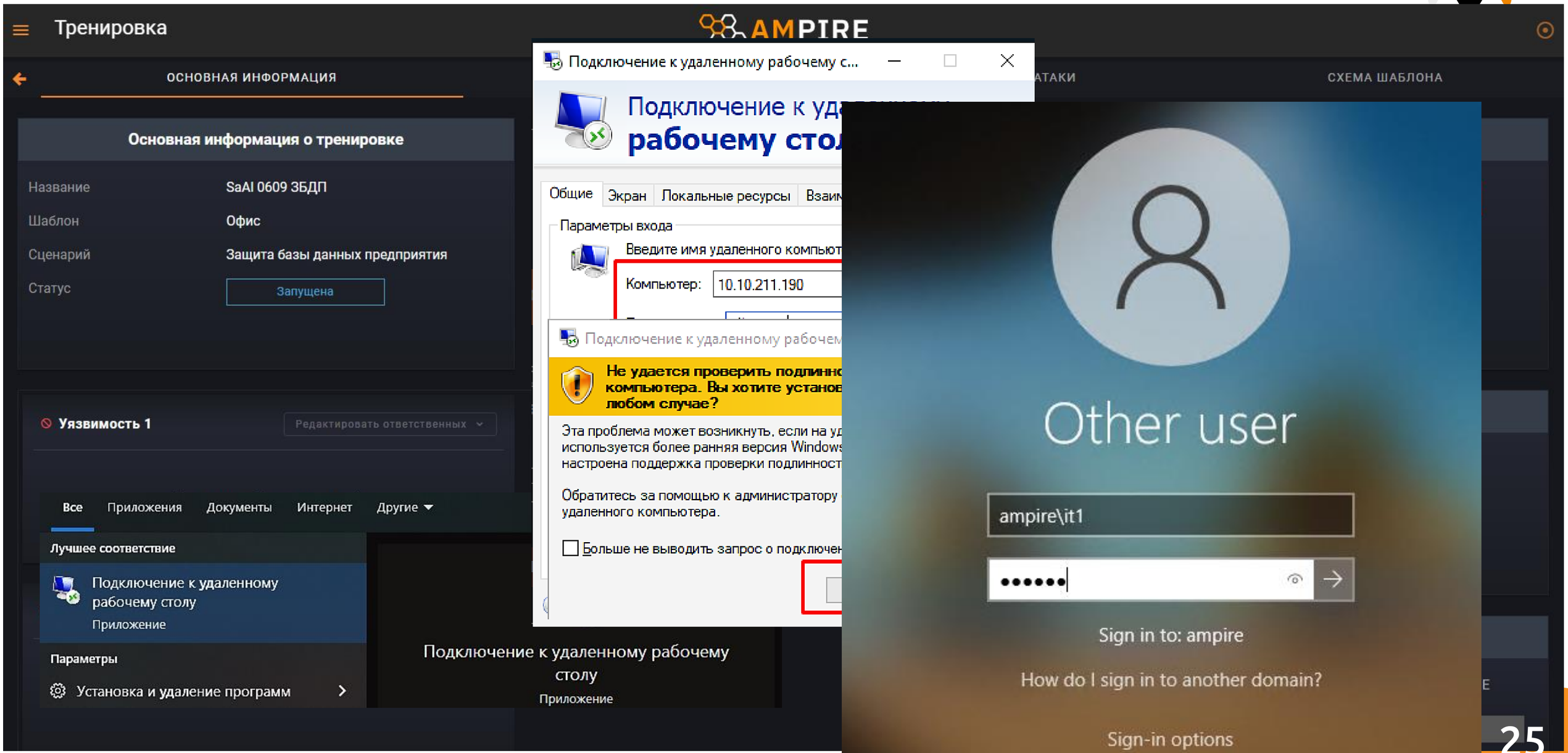
Реагирование (роль Лидера)



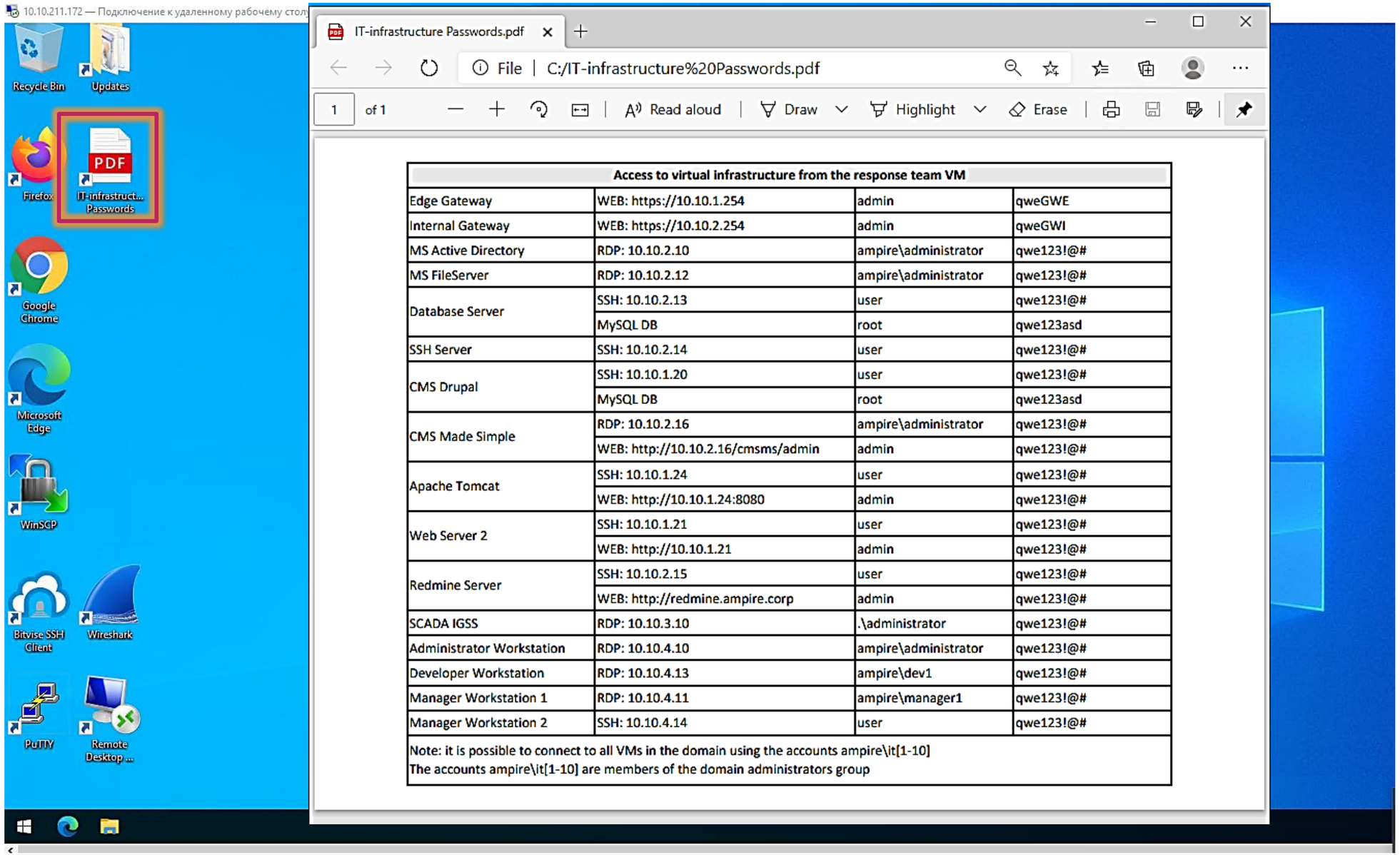
Реагирование (роль Лидера)



Реагирование



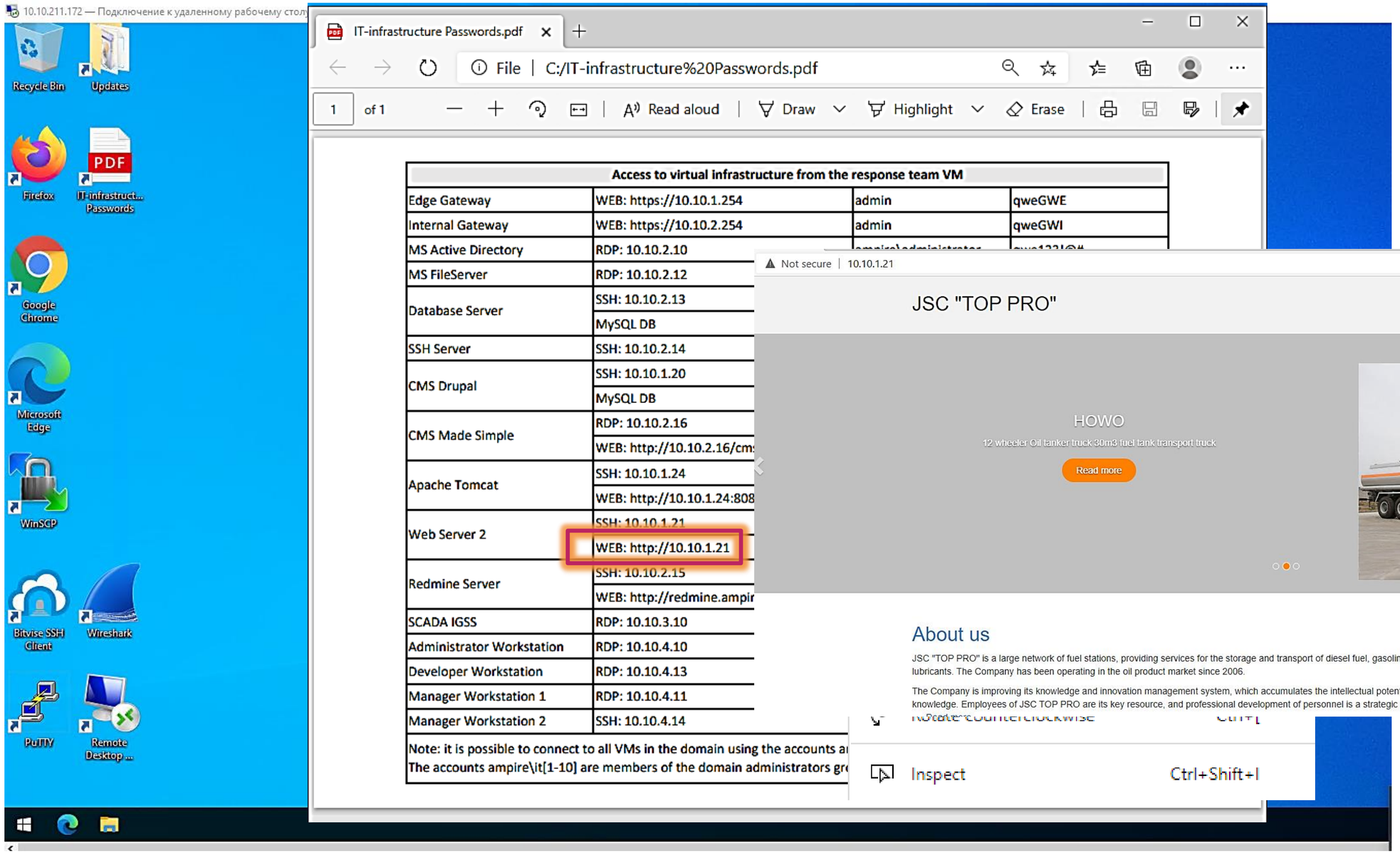
Внутри удаленного АРМ



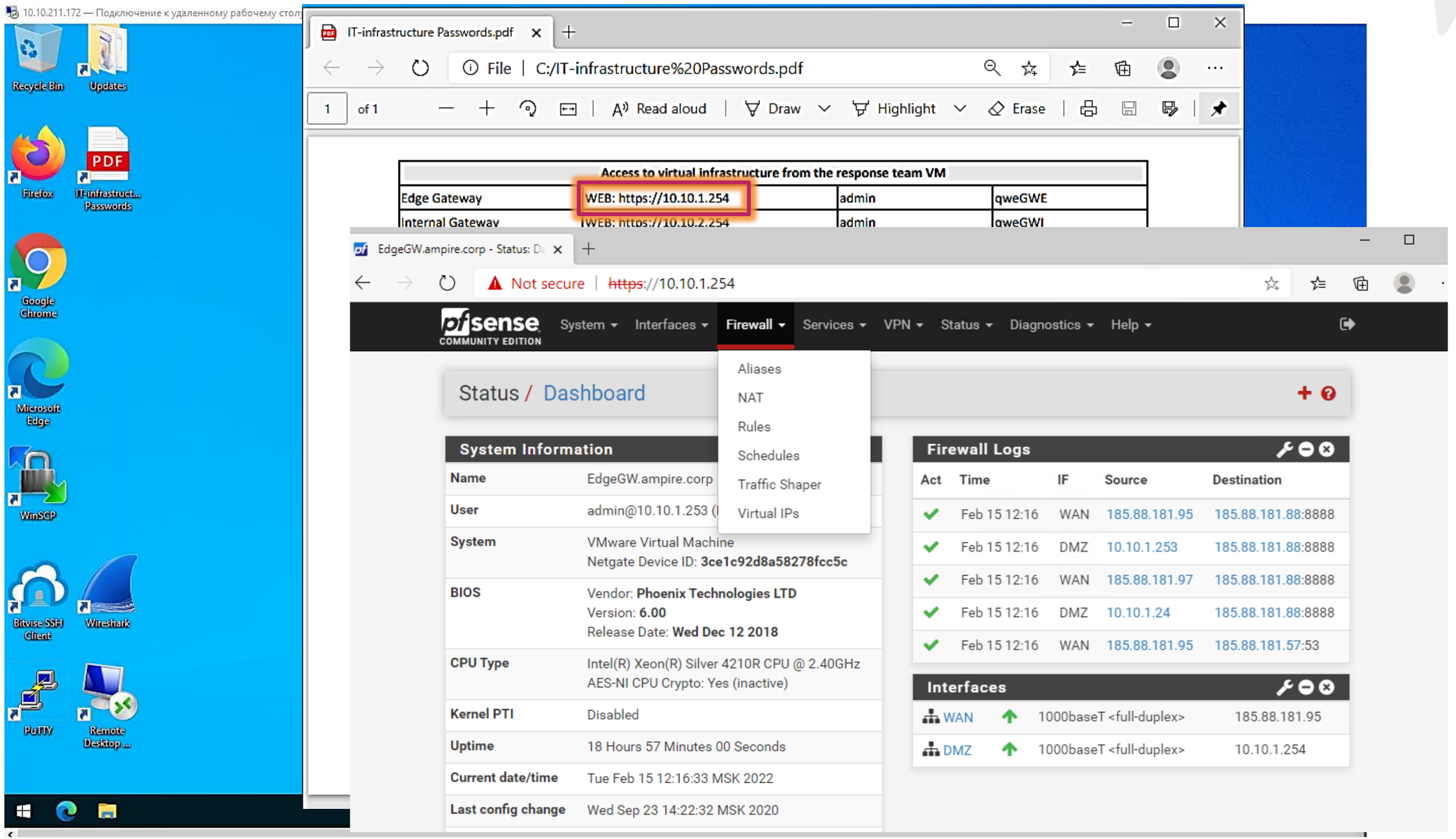
Access to virtual infrastructure from the response team VM			
Edge Gateway	WEB: https://10.10.1.254	admin	qweGWE
Internal Gateway	WEB: https://10.10.2.254	admin	qweGWI
MS Active Directory	RDP: 10.10.2.10	ampire\administrator	qwe123!@#
MS FileServer	RDP: 10.10.2.12	ampire\administrator	qwe123!@#
Database Server	SSH: 10.10.2.13	user	qwe123!@#
	MySQL DB	root	qwe123asd
SSH Server	SSH: 10.10.2.14	user	qwe123!@#
CMS Drupal	SSH: 10.10.1.20	user	qwe123!@#
	MySQL DB	root	qwe123asd
CMS Made Simple	RDP: 10.10.2.16	ampire\administrator	qwe123!@#
	WEB: http://10.10.2.16/cmsms/admin	admin	qwe123!@#
Apache Tomcat	SSH: 10.10.1.24	user	qwe123!@#
	WEB: http://10.10.1.24:8080	admin	qwe123!@#
Web Server 2	SSH: 10.10.1.21	user	qwe123!@#
	WEB: http://10.10.1.21	admin	qwe123!@#
Redmine Server	SSH: 10.10.2.15	user	qwe123!@#
	WEB: http://redmine.ampire.corp	admin	qwe123!@#
SCADA IGSS	RDP: 10.10.3.10	.\administrator	qwe123!@#
Administrator Workstation	RDP: 10.10.4.10	ampire\administrator	qwe123!@#
Developer Workstation	RDP: 10.10.4.13	ampire\dev1	qwe123!@#
Manager Workstation 1	RDP: 10.10.4.11	ampire\manager1	qwe123!@#
Manager Workstation 2	SSH: 10.10.4.14	user	qwe123!@#

Note: it is possible to connect to all VMs in the domain using the accounts ampire\it[1-10]
The accounts ampire\it[1-10] are members of the domain administrators group

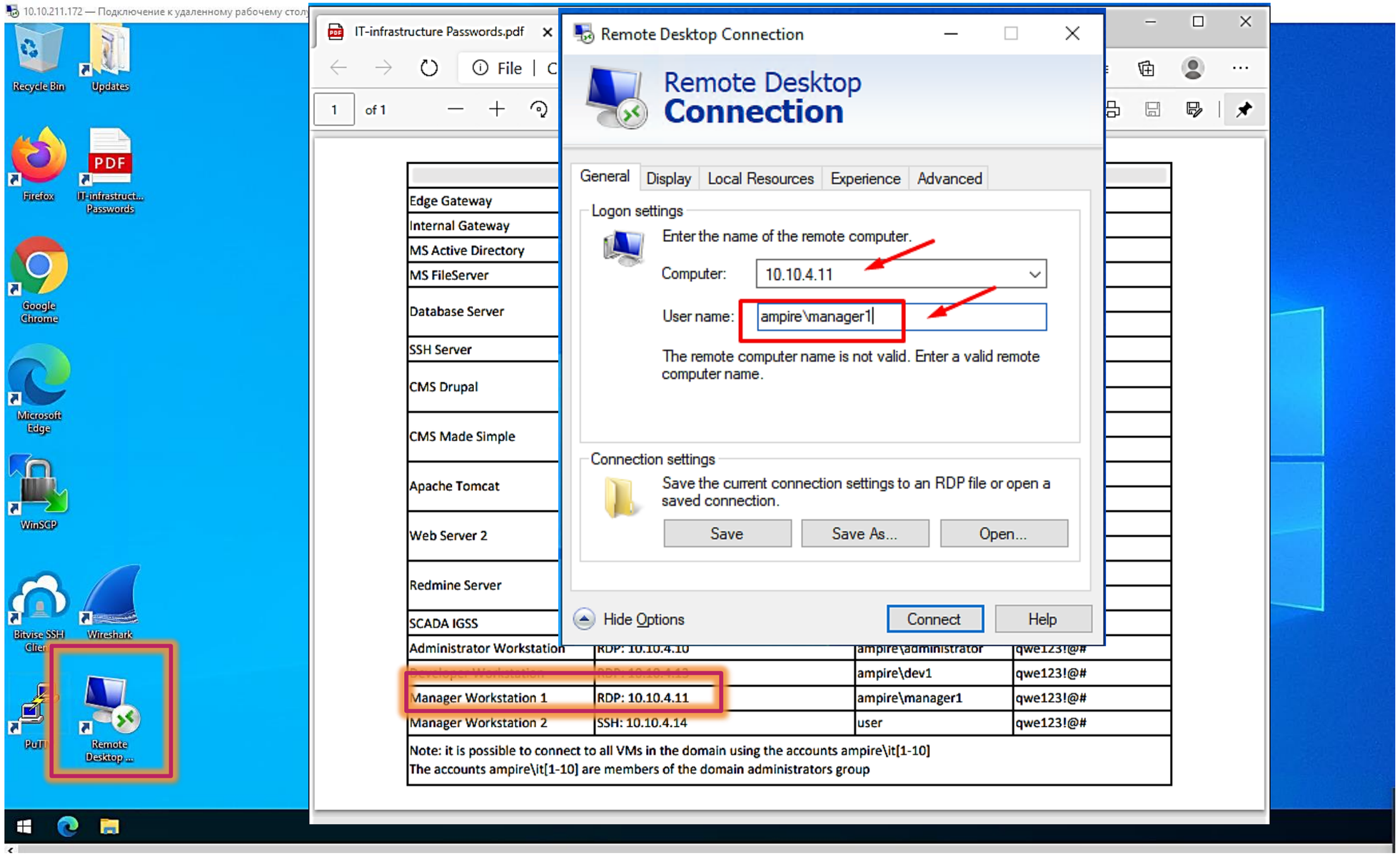
Внутри удаленного АРМ



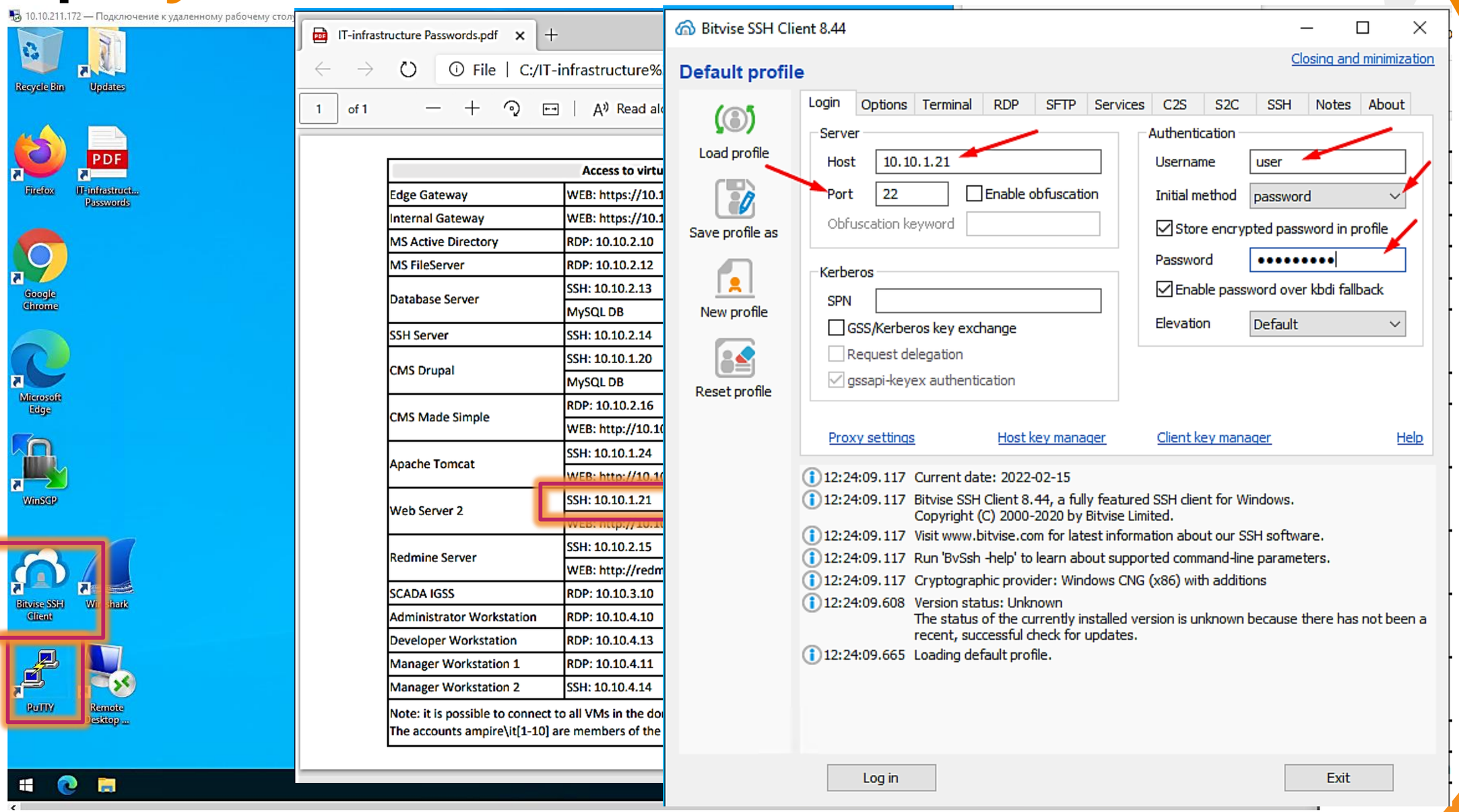
Внутри удаленного АРМ



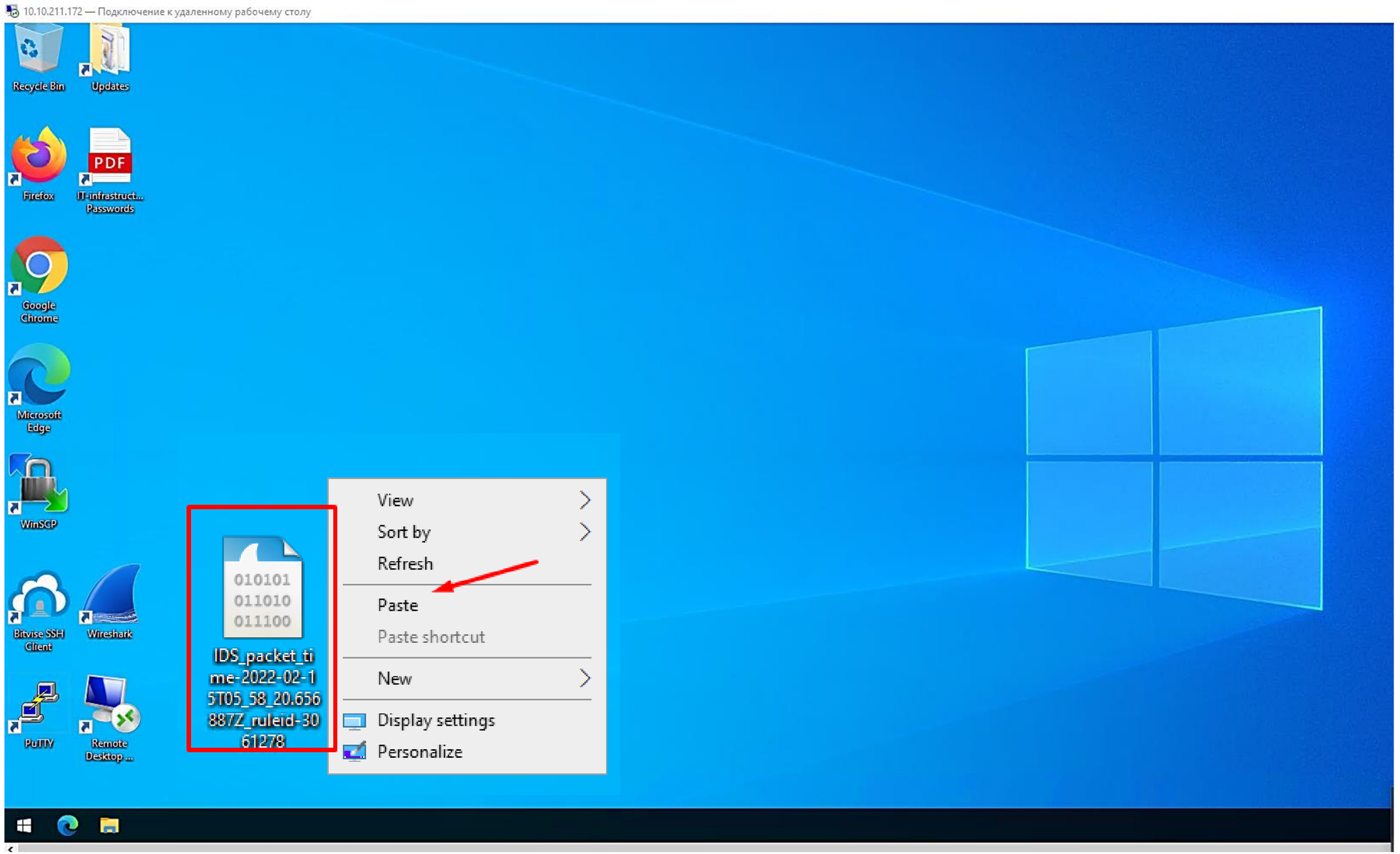
Внутри удаленного АРМ



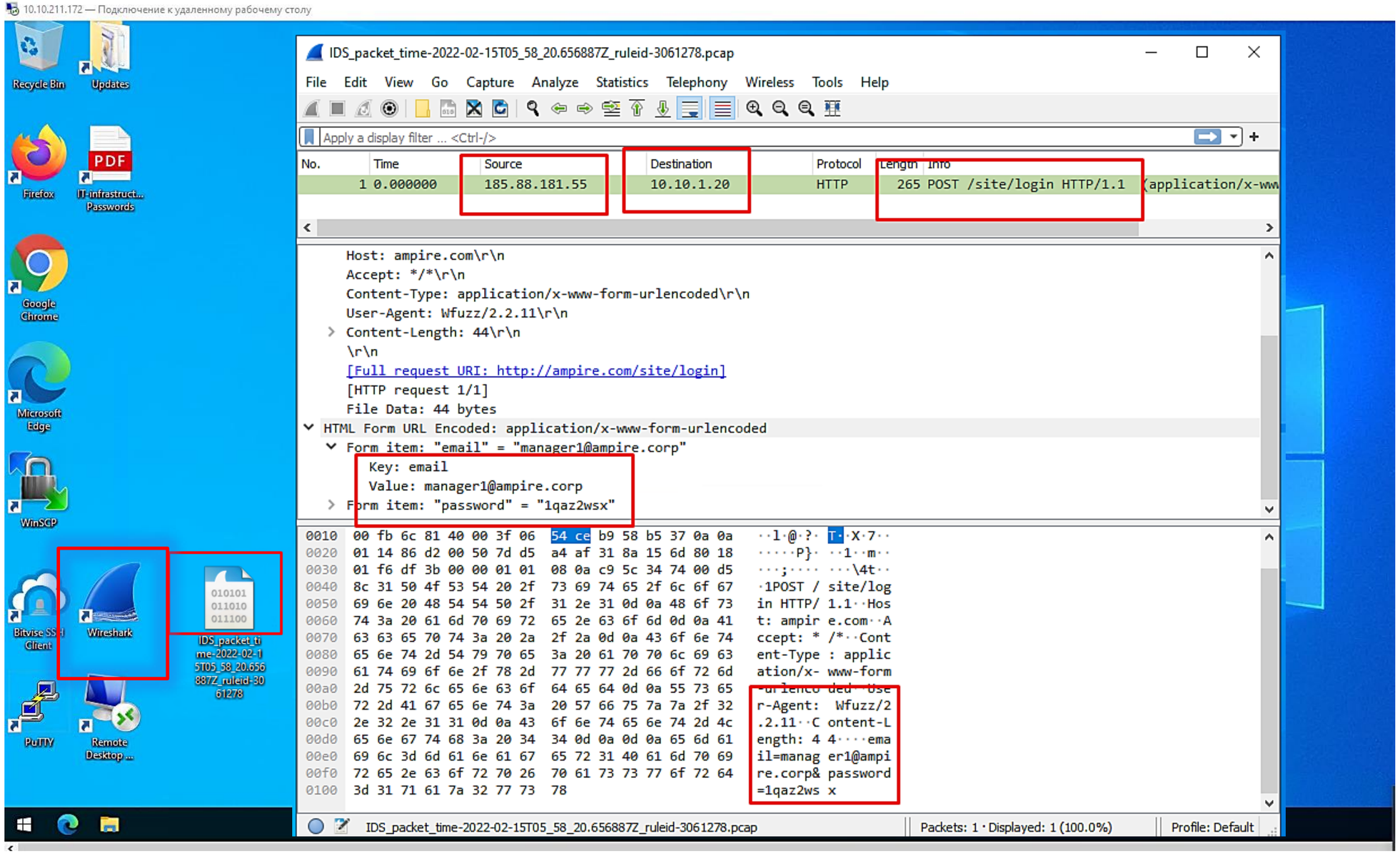
Внутри удаленного АРМ



Внутри удаленного АРМ



Внутри удаленного АРМ



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо за внимание!