



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

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

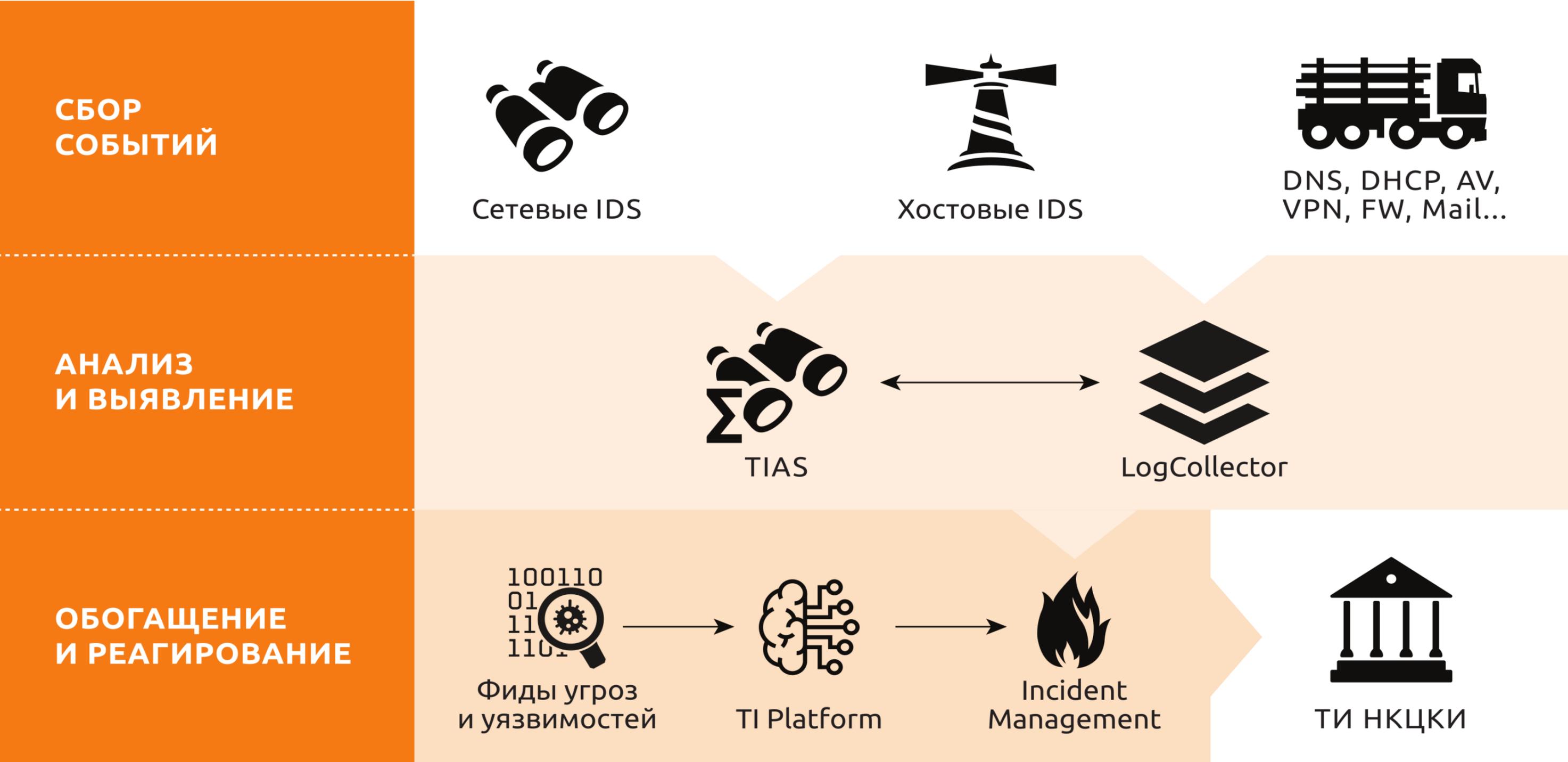
Александр Сальников
старший специалист по ИБ

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



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.

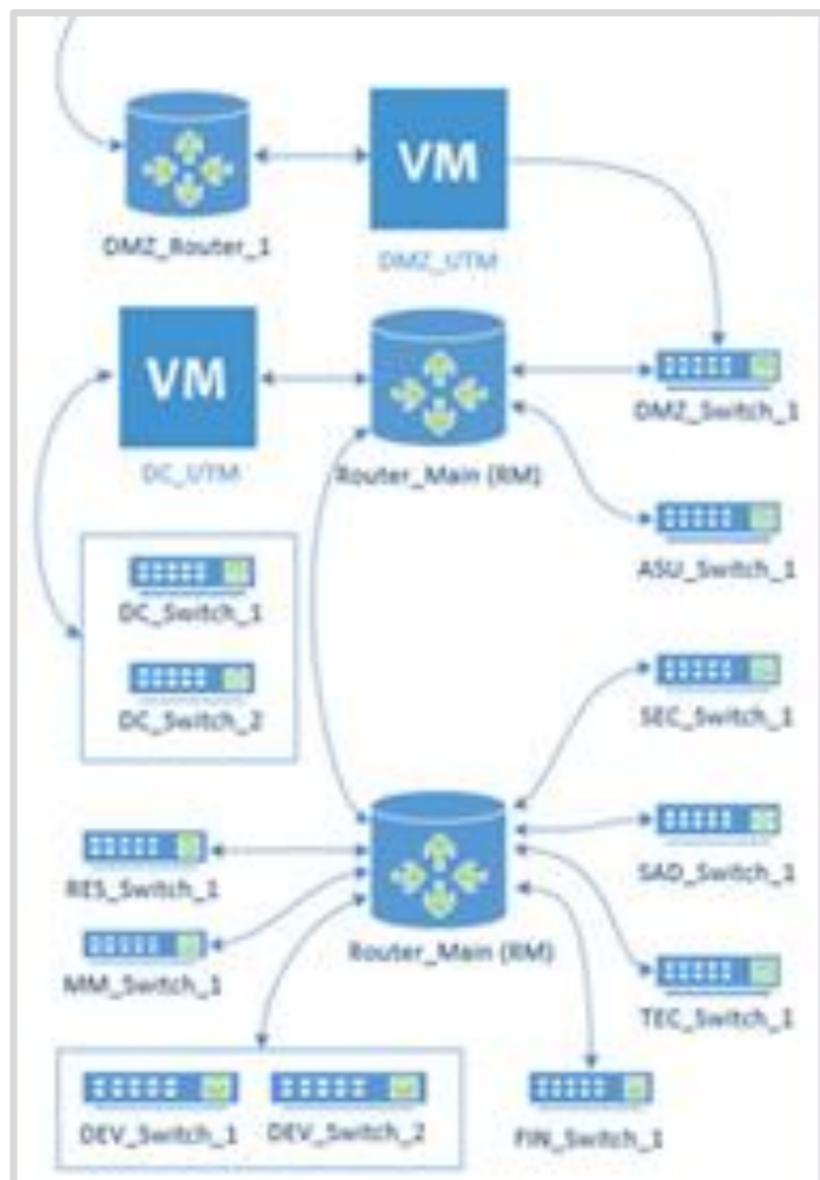


Ampire - это платформа



Практические занятия на цифровом двойнике реальной инфраструктуры

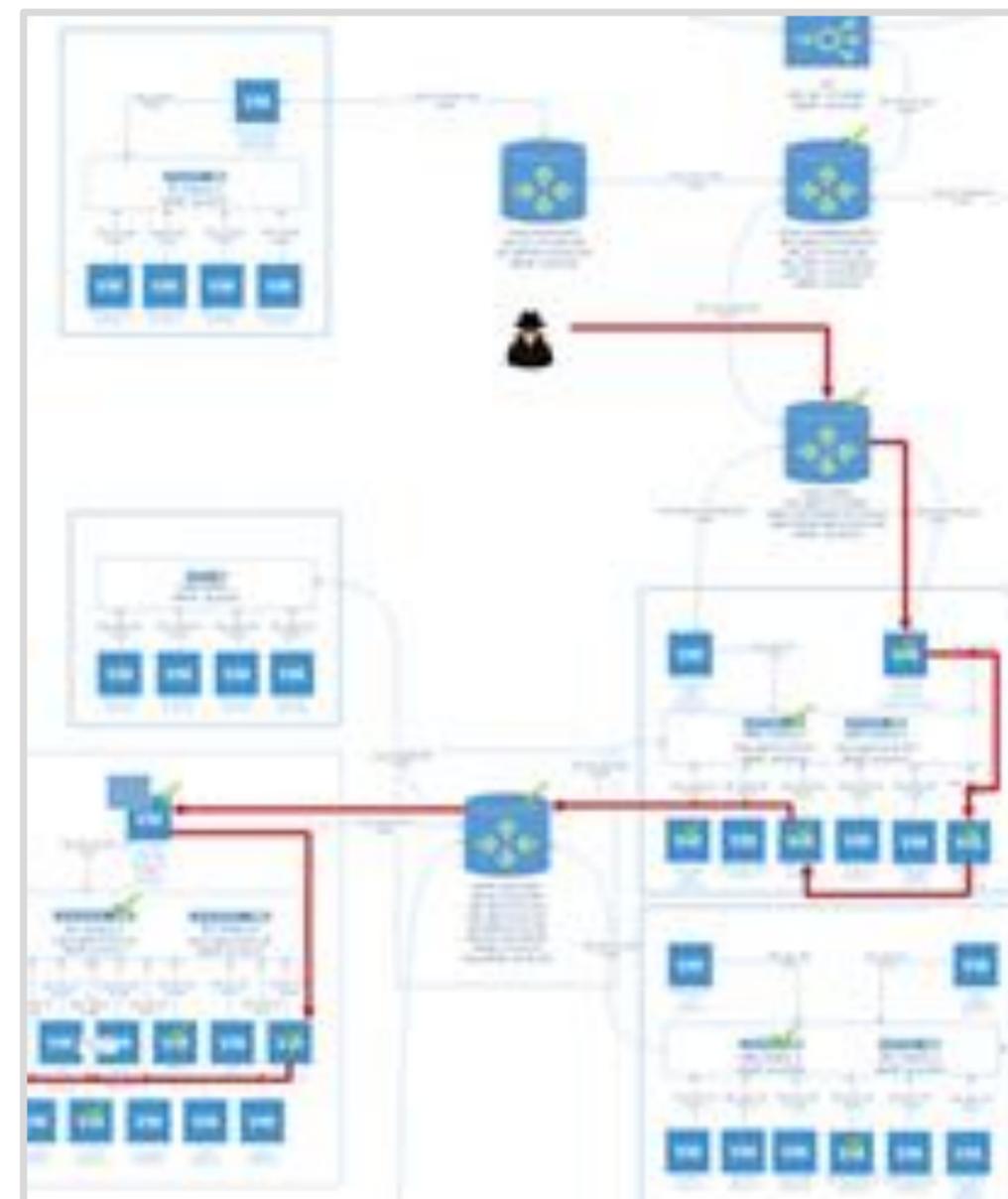
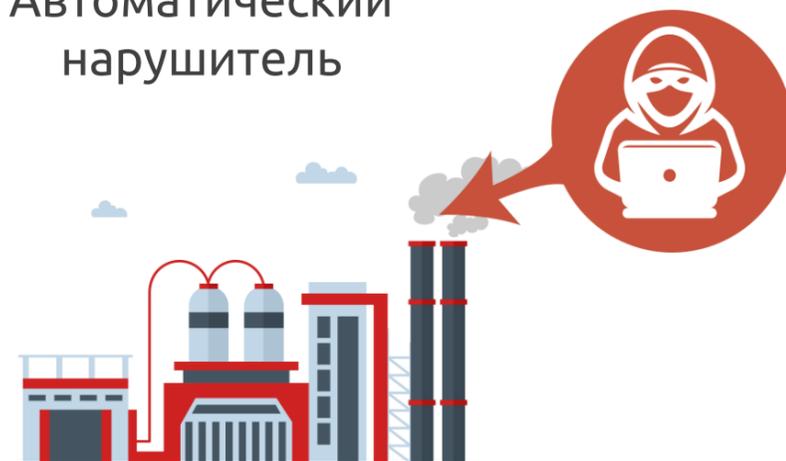
Симуляция сети с ИТ и SCADA-сегментами



Security Operations Center



Автоматический нарушитель



Базовые сценарии



Шаблоны и сценарии



Мои шаблоны



Офис (Конфигуратор)

Описание:
Каркас шаблона Предприятие для конфигуратора сценариев



АСУ ТП

Описание:
ASU template WinCC Unified



Телеком оператор

Описание:
Сеть Телеком-оператора



Офис

Описание:
Корпоративная сеть предприятия Stable version

Последствие

Уязвимость

Поиск



Название	Сложность	Рекомендуемая длительность (мин.)	Действия
Защита данных файлового сервера v2	Средняя	90	
Защита контролера домена v2	Низкая	90	
Защита данных сегмента АСУ ТП v2	Низкая	90	
Защита корпоративного мессенджера	Средняя	90	
Zerologon-ExchangeDLP	Средняя	90	
КиберРИТ	Средняя	90	
КиберРИТ_v2	Средняя	90	
КиберРИТ_v3	Средняя	90	
КиберРИТ_v4	Средняя	90	
КиберРИТорика_2023	Низкая	90	
КиберРИТорика 2023 сценарий	Низкая	90	
postgres	Средняя	90	

Конфигуратор



Мои шаблоны

Последствие Уязвимость Поиск

Название	Сложность	Рекомендуемая длительность (мин.)	Действия
Защита данных файлового сервера v2	Средняя	90	
Защита контролера домена v2	Низкая	90	
Защита данных сегмента АСУ ТП v2	Низкая	90	
Защита корпоративного мессенджера	Средняя	90	

База знаний

Шаблон Сегмент ОС Поиск

MS File Server Уязвимостей: 1 Последствий: 1 Шаблон: Офис (Конфигуратор) Сегмент: Data Center Операционная система: Windows	SCADA IGSS Уязвимостей: 1 Последствий: 1 Шаблон: Офис (Конфигуратор) Сегмент: ASU Операционная система: Windows	CMS WordPress Уязвимостей: 3 Последствий: 8 Шаблон: Офис (Конфигуратор) Сегмент: DMZ Операционная система: Linux
MS Exchange Уязвимостей: 3 Последствий: 17 Шаблон: Офис (Конфигуратор) Сегмент: Data Center Операционная система: Windows	GitLab Уязвимостей: 1 Последствий: 3 Шаблон: Офис (Конфигуратор) Сегмент: Data Center Операционная система: Linux	OpenSMTPD Уязвимостей: 1 Последствий: 3 Шаблон: Офис (Конфигуратор) Сегмент: Data Center Операционная система: Linux

Узлы

55

Уязвимости и последствия

140

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	Meterpreter Backdoor User Deleter
GravCMS*	CVE-2021-21425	Meterpreter 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



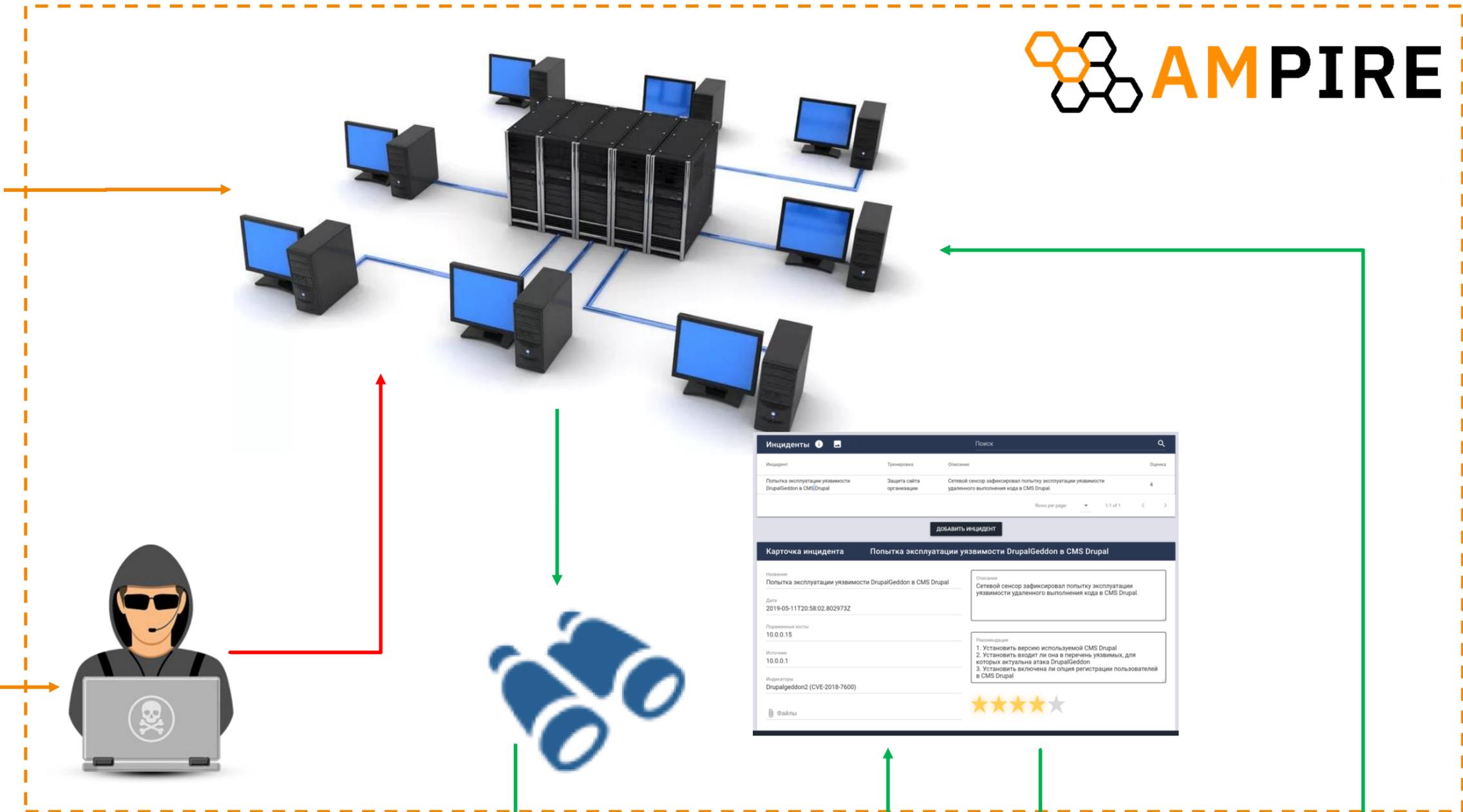
Научиться выявлять компьютерные атаки



Наладить взаимодействие между подразделениями



Устранить существующие уязвимости



Инцидент	Тренировка	Описание	Оценка
Попытка эксплуатации уязвимости DrupalGeddon в CMS Drupal	Защита сайта организации	Сетевой сенсор зафиксировал попытку эксплуатации уязвимости удаленного выполнения кода в CMS Drupal.	4

Поиск

Выводы на страницу: 1-1 of 1

ДОБАВИТЬ ИНЦИДЕНТ

Карточка инцидента: Попытка эксплуатации уязвимости DrupalGeddon в CMS Drupal

Название: Попытка эксплуатации уязвимости DrupalGeddon в CMS Drupal

Дата: 2019-05-11T20:58:02.802973Z

Параметры хоста: 10.0.0.15

Источник: 10.0.0.1

Индикаторы: Drupalgeddon2 (CVE-2018-7600)

Описание: Сетевой сенсор зафиксировал попытку эксплуатации уязвимости удаленного выполнения кода в CMS Drupal.

Рекомендации:
1. Установить версию используемой CMS Drupal!
2. Установить входит ли она в перечень уязвимых, для которых актуальна атака DrupalGeddon
3. Установить включена ли опция регистрации пользователей в CMS Drupal!

★★★★★

Файлы

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.

Проексплуатировав 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

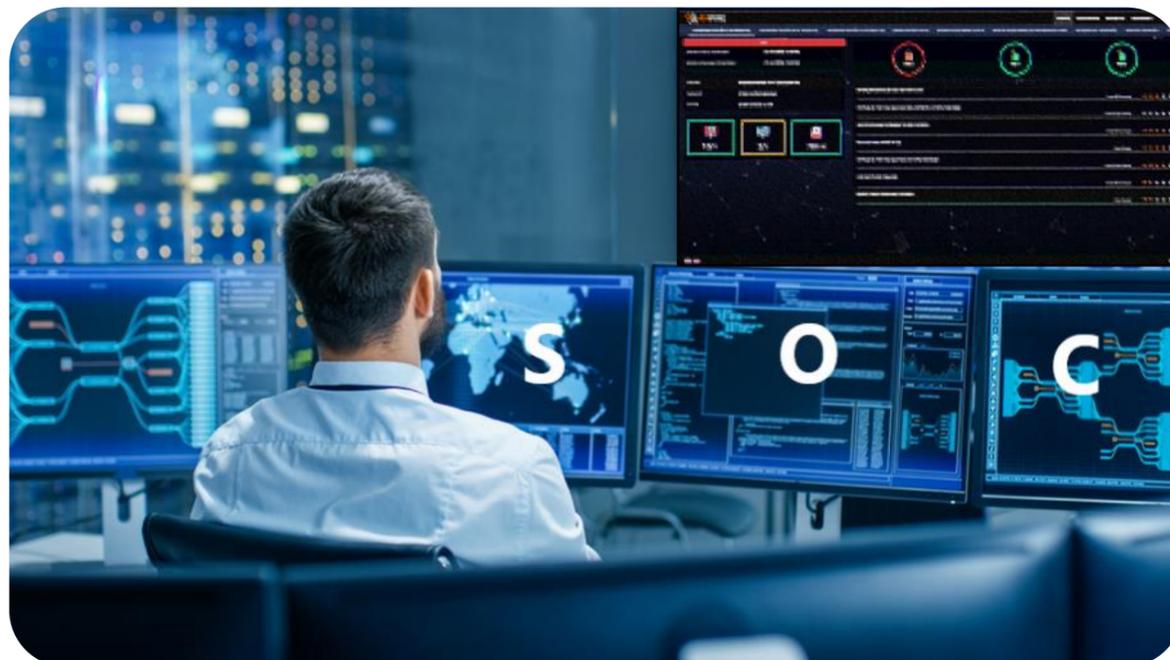
Расследование инцидентов

Устранение уязвимостей

Задачи групп



Мониторинг



Реагирование



Анализ событий ИБ

Заведение карточек инцидентов

Описание вектора атаки (Cyber Kill Chain)

Расследование инцидентов

Устранение уязвимостей

Информационная панель



AMPIRE

Sa_AI 3108_ЗБДП_2

Группа Учебная группа 1
Шаблон Офис
Сценарий Защита базы данных предприятия
Время начала 31.08.2023 15:53
Время окончания 31.08.2023 19:23

00:00:00
ЧЧ ММ СС

100%

Нет последствий

Уязвимости

- DRUPALGEDDON 2**
УСТРАНЕНО
Петров Петр
- SSH PASSWORD**
УСТРАНЕНО
Петров Петр
- MYSQL PASSWORD**
УСТРАНЕНО

Сканирование SSH-scan

В работе

Автор **Иванов Иван**
Ответственный **Сергеев Сергей**

☆☆☆☆☆

Атака на веб-ресурс

В работе

Автор **Иванов Иван**
Ответственный **Петров Петр**

☆☆☆☆☆

Стартовая страница



Авторизация

Логин

tfmon1

Пароль

11111111



ВОЙТИ

Мониторинг



Главная 

Шаблонов **2**

Сценариев **10**

Активных тренировок **0**

Тренировок пройдено **26**

Тренировки 

ВСЕ ТЕКУЩИЕ ЗАВЕРШЕННЫЕ

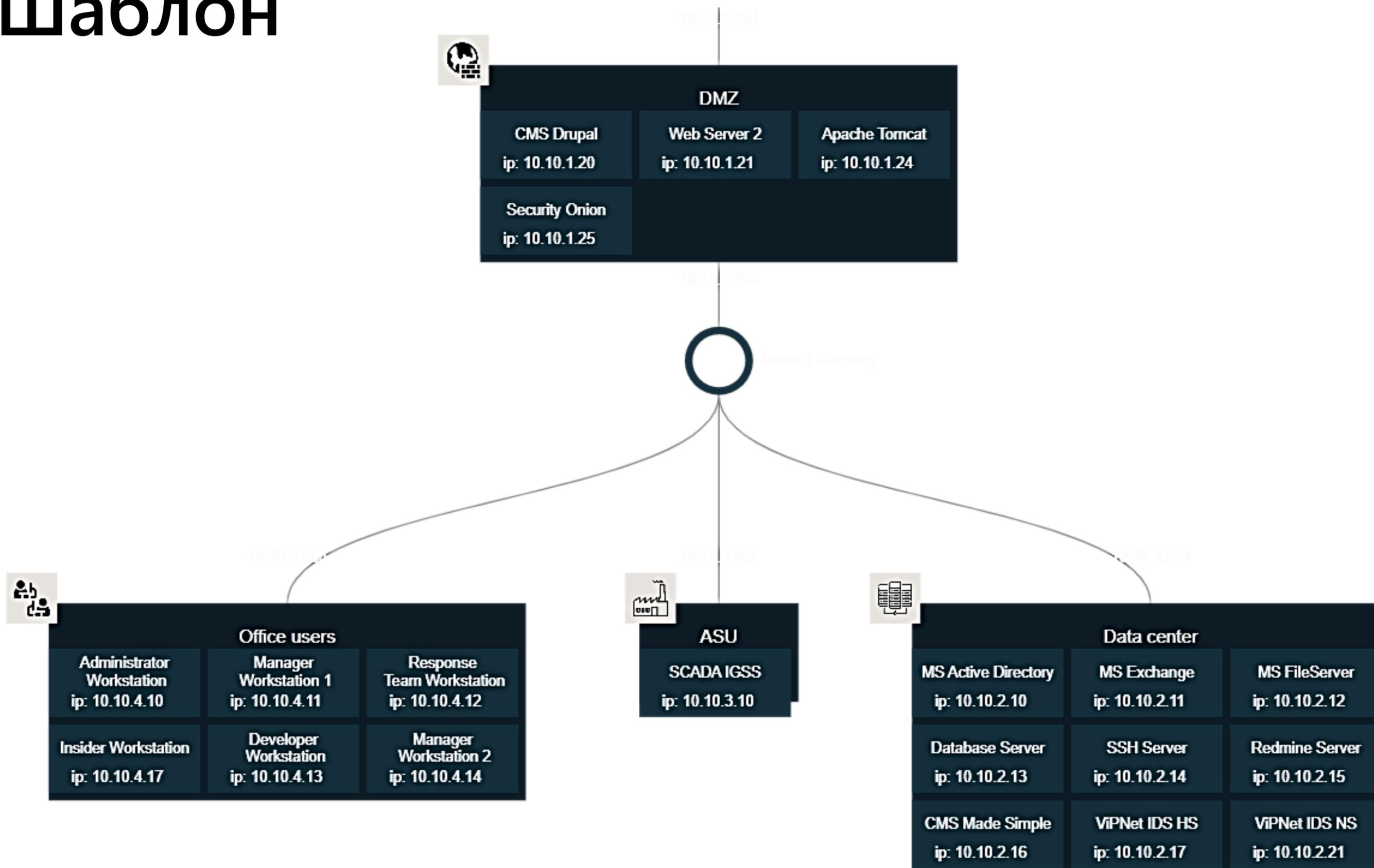
Завершена Sa_AI 0109_ЗБДП_1

Формат тренировки - BlueTeam Шаблон - Офис

Сценарий - Защита базы данных предприятия Длительность - 90

Группа - Учебная группа 1 Уязвимостей устранено: 3/3 Количество инцидентов: 1 

Шаблон



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

Доступные ресурсы

SecOnion	10.10.210.162 🔑
ViPNet TIAS	10.10.210.98 🔑
ViPNet IDS NS	10.10.210.208 🔑

Мои инциденты

Новые	0/0
В работе	0/0
Закрытые	0/0

Уязвимость 1

Уязвимость без последствий

Уязвимость 3

Уязвимость без последствий

00:00:00

чч мм cc

NS ViPNet IDS NS

Имя учетной записи

Пароль

Войти

+ СОЗДАТЬ НОВЫЙ ИНЦИДЕНТ

ЦЕПОЧКА КИБЕРАТАКИ

Интерфейс ViPNet IDS NS



NS ViPNet IDS NS mon19

Инфопанель

Мониторинг

- Инфопанель
- События**
- Отчеты

Управление

- Сетевое окружение
- Методы анализа
- Правила анализа
- Оповещение
- Интеграция

Система

- Сетевые настройки
- Дата и время
- Учетные записи
- Резервное копирование
- Сервисные функции

Аудит

- Журнал аудита

Состояние сенсора

- Версия базы правил от 16.08.2023. Активно 43624 правила из 43682
- Malware detection включен
Версия базы Malware detection 5855 от 18.08.2023.
- Отключен анализ IP-пакетов, зашифрованных с помощью ПО ViPNet
- Включен эвристический анализ

Производительность

- Загрузка ЦПУ **25%**
- Использование ОЗУ **28%**
- Потери пакетов **0%**
- Трафик, Мбит/сек **6.435**

100%

10 МБит/с

Счётчик событий

За день За месяц За год **Всего**

Общее количество: **2 128**

По уровням важности:

Высокий	167
Средний	721
Низкий	1 240
Информационный	0

События ИБ в ViPNet IDS NS



- Мониторинг
- Инфопанель
- События**
- Отчеты
- Управление
- Сетевое окружение
- Методы анализа
- Правила анализа
- Оповещение
- Интеграция
- Система
- Сетевые настройки
- Дата и время
- Учетные записи
- Резервное копирование
- Сервисные функции
- Аудит
- Журнал аудита

События

События за последние 24 часа [Filter] [Refresh]

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 инцидента ИБ



Создать новый инцидент ✕

Название ⓘ	Индикаторы компрометации ⓘ
Атака на веб-портал с CMS Drupal	web-application-attack
Источник ⓘ	Поражённые активы ⓘ
185.88.181.55 ✕	10.10.1.21 ✕
Дата и время события ⓘ	Прикрепить файл ⓘ
2023-08-31 10:20	IDS_packet...23574.pcap
Описание ⓘ	
Атака внешнего нарушителя на веб-портал на базе CMS Drupal с эксплуатацией уязвимости Drupalgeddon2	
99 / 500	
Рекомендации ⓘ	
<ol style="list-style-type: none">1. Проверить версию CMS Drupal на наличие уязвимости Drupalgeddon2.2. В панели администрирования отключить свободную регистрацию пользователей, если она включена.	
164 / 500	

ОТМЕНА СОХРАНИТЬ

Реагирование (роль Лидера)



Новый Компрометация пароля БД MySQL ✕

Дата и время события
01.09.2023 14:19

Источник
10.10.4.11

Поражённые активы
10.10.2.13

Индикаторы компрометации
нестандартные запросы получения информации по сети

Описание
Пароль БД найден в файле bash_history

Рекомендации
Почистить файл bash_history и не вводить пароль напрямую

IDS_packet_time-2023-09-01T11_22_20.610873Z_ruleid-3105863 (1).pcap

Сергеев Сергей **Нет ответственного**

Комментарии

Комментарий...

Реагирование (роль Лидера)



Тренировка **AMPIRE**

ОСНОВНАЯ ИНФОРМАЦИЯ ИНЦИДЕНТЫ УЧАСТНИКИ СХЕМА ШАБЛОНА ЛОГИ СОБЫТИЙ АТАКИ

Основная информация о тренировке

Название: Sa_AI 0109_ЗБДП_1
Шаблон: Офис
Сценарий: Защита базы данных предприятия
Статус: **Завершена**
Доступные действия: **УДАЛИТЬ ТРЕНИРОВКУ**, **СКАЧАТЬ ОТЧЁТ**

Время начала: 01.09.2023 14:16
Время окончания: 01.09.2023 19:23

ПРОГРЕСС АТАКИ 100%

Участники

Группа: Учебная группа 1

Команда мониторинга	В СЕТИ	0 / 1
Мониторинг реагирования	В СЕТИ	0 / 1
Мониторинг реагирования	НЕ В СЕТИ	

Выберите ответственного

Уязвимость: **DrupalGeddon 2**

Иванов Иван Васильевич Василий Алексеев Алексей

Устранено

ОТМЕНА **СОХРАНИТЬ**

Инциденты

1/1
0/1
0/1
0/1

Доступные ресурсы

Удалённое рабочее место	Информация отсутствует
SecOnion	Информация отсутствует
ViPNet TIAS	Информация отсутствует

Уязвимость без последствий

Уязвимость без последствий

Реагирование



The image shows a composite screenshot of the AMPiRE interface. On the left, the 'Тренировка' (Training) page displays configuration details for a training environment named 'SaAI 0609 ЗБДП'. The status is 'Запущена' (Running). Below this, a 'Уязвимость 1' (Vulnerability 1) section is visible. The main part of the screen is overlaid with a Windows 'Подключение к удаленному рабочему столу' (Remote Desktop Connection) dialog box. This dialog shows the 'Общие' (General) tab with the 'Компьютер:' field set to '10.10.211.190'. A yellow warning message states: 'Не удастся проверить подлинность компьютера. Вы хотите установить его в любом случае?' (Cannot verify the identity of the computer. Do you want to connect anyway?). The 'Подключить' (Connect) button is highlighted with a red box. In the background, the AMPiRE web interface shows a 'Подключение к удаленному рабочему столу' application card. On the right, a Windows login screen for 'Other user' is shown with the username 'ampire\it1' and a password field. The login screen also includes the text 'Sign in to: ampire' and 'How do I sign in to another domain?'. At the bottom right, the text 'Sign-in options' is visible.

Внутри удаленного АРМ



10.10.211.172 — Подключение к удаленному рабочему столу



IT-infrastructure Passwords.pdf

File | C:/IT-infrastructure%20Passwords.pdf

1 of 1

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



10.10.211.172 — Подключение к удаленному рабочему столу

Recycle Bin, Updates, Firefox, IT-infrastruct... Passwords, Google Chrome, Microsoft Edge, WinSCP, Bitvise SSH Client, Wireshark, PuTTY, Remote Desktop ...

IT-infrastructure Passwords.pdf

File | C:/IT-infrastructure%20Passwords.pdf

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	admin\administrator	qwe123!@#
MS FileServer	RDP: 10.10.2.12		
Database Server	SSH: 10.10.2.13		
	MySQL DB		
SSH Server	SSH: 10.10.2.14		
CMS Drupal	SSH: 10.10.1.20		
	MySQL DB		
CMS Made Simple	RDP: 10.10.2.16		
	WEB: http://10.10.2.16/cm		
Apache Tomcat	SSH: 10.10.1.24		
	WEB: http://10.10.1.24:808		
Web Server 2	SSH: 10.10.1.21		
	WEB: http://10.10.1.21		
Redmine Server	SSH: 10.10.2.15		
	WEB: http://redmine.ampir		
SCADA IGSS	RDP: 10.10.3.10		
Administrator Workstation	RDP: 10.10.4.10		
Developer Workstation	RDP: 10.10.4.13		
Manager Workstation 1	RDP: 10.10.4.11		
Manager Workstation 2	SSH: 10.10.4.14		

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

Not secure | 10.10.1.21

JSC "TOP PRO"

HOME

HOWO

12 wheeler Oil tanker truck 30m3 fuel tank transport truck

Read more

About us

JSC "TOP PRO" is a large network of fuel stations, providing services for the storage and transport of diesel fuel, gasoline, heating oil, as well as for the sale and storage of oils & lubricants. The Company has been operating in the oil product market since 2006.

The Company is improving its knowledge and innovation management system, which accumulates the intellectual potential of employees and increases the efficiency of applying knowledge. Employees of JSC TOP PRO are its key resource, and professional development of personnel is a strategic priority of the Company.

INSPECT

Ctrl+Shift+I

Внутри удаленного АРМ



10.10.211.172 — Подключение к удаленному рабочему столу

IT-infrastructure Passwords.pdf

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

EdgeGW.ampire corp - Status: De x

Not secure | <https://10.10.1.254>

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ **Firewall** ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / Dashboard

System Information

Name	EdgeGW.ampire.corp
User	admin@10.10.1.253 (0
System	VMware Virtual Machine Netgate Device ID: 3ce1c92d8a58278fcc5c
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Wed Dec 12 2018
CPU Type	Intel(R) Xeon(R) Silver 4210R CPU @ 2.40GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Disabled
Uptime	18 Hours 57 Minutes 00 Seconds
Current date/time	Tue Feb 15 12:16:33 MSK 2022
Last config change	Wed Sep 23 14:22:32 MSK 2020

Firewall Logs

Act	Time	IF	Source	Destination
✓	Feb 15 12:16	WAN	185.88.181.95	185.88.181.88:8888
✓	Feb 15 12:16	DMZ	10.10.1.253	185.88.181.88:8888
✓	Feb 15 12:16	WAN	185.88.181.97	185.88.181.88:8888
✓	Feb 15 12:16	DMZ	10.10.1.24	185.88.181.88:8888
✓	Feb 15 12:16	WAN	185.88.181.95	185.88.181.57:53

Interfaces

WAN	↑	1000baseT <full-duplex>	185.88.181.95
DMZ	↑	1000baseT <full-duplex>	10.10.1.254

Внутри удаленного АРМ



10.10.211.172 — Подключение к удаленному рабочему столу

IT-infrastructure Passwords.pdf

Remote Desktop Connection

Remote Desktop Connection

General Display Local Resources Experience Advanced

Logon settings

Enter the name of the remote computer.

Computer: 10.10.4.11

User name: **ampire\manager1**

The remote computer name is not valid. Enter a valid remote computer name.

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

Save Save As... Open...

Hide Options Connect Help

Edge Gateway			
Internal Gateway			
MS Active Directory			
MS FileServer			
Database Server			
SSH Server			
CMS Drupal			
CMS Made Simple			
Apache Tomcat			
Web Server 2			
Redmine Server			
SCADA IGSS			
Administrator Workstation	RDP: 10.10.4.10	ampire\administrator	qwe123!@#
Developer Workstation	RDP: 10.10.4.10	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

Recycle Bin Updates Firefox IT-infrastructure Passwords Google Chrome Microsoft Edge WinSCP Bitvise SSH Client Wireshark PuTTY Remote Desktop ...

Внутри удаленного АРМ

The image shows a Windows desktop environment with a remote session. On the left, the desktop has icons for Recycle Bin, Updates, Firefox, IT-infrastructure Passwords, Google Chrome, Microsoft Edge, WinSCP, Bitvise SSH Client, WinShare, PuTTY, and Remote Desktop. The main window is a PDF viewer displaying a table of server access information. The Bitvise SSH Client 8.44 window is open, showing the configuration for a default profile. Red arrows point to the Host, Port, Username, and Password fields in the configuration. The Bitvise SSH Client window also shows a log of system messages.

Access to virtu	
Edge Gateway	WEB: https://10.1
Internal Gateway	WEB: https://10.1
MS Active Directory	RDP: 10.10.2.10
MS FileServer	RDP: 10.10.2.12
Database Server	SSH: 10.10.2.13 MySQL DB
SSH Server	SSH: 10.10.2.14
CMS Drupal	SSH: 10.10.1.20 MySQL DB
CMS Made Simple	RDP: 10.10.2.16 WEB: http://10.10
Apache Tomcat	SSH: 10.10.1.24 WEB: http://10.10
Web Server 2	SSH: 10.10.1.21 WEB: http://10.10
Redmine Server	SSH: 10.10.2.15 WEB: http://redm
SCADA IGSS	RDP: 10.10.3.10
Administrator Workstation	RDP: 10.10.4.10
Developer Workstation	RDP: 10.10.4.13
Manager Workstation 1	RDP: 10.10.4.11
Manager Workstation 2	SSH: 10.10.4.14

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

Bitvise SSH Client 8.44

Default profile

Load profile
Save profile as
New profile
Reset profile

Server
Host: 10.10.1.21
Port: 22
Enable obfuscation:
Obfuscation keyword:

Authentication
Username: user
Initial method: password
Store encrypted password in profile:
Password:
Enable password over kbdi fallback:
Elevation: Default

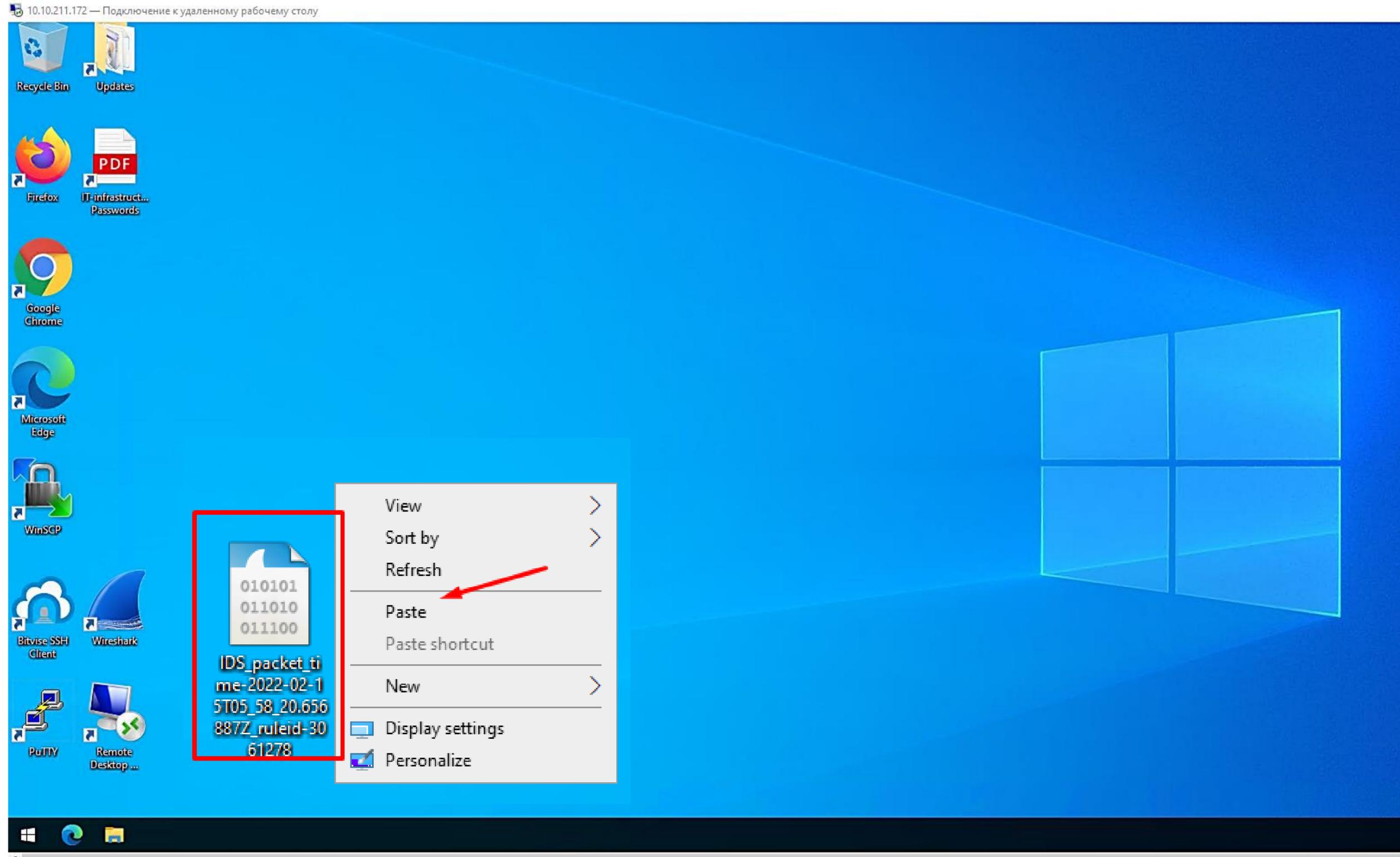
Kerberos
SPN:
GSS/Kerberos key exchange:
Request delegation:
gssapi-keyex authentication:

Proxy settings Host key manager Client key manager Help

12:24:09.117 Current date: 2022-02-15
12:24:09.117 Bitvise SSH Client 8.44, a fully featured SSH client for Windows.
Copyright (C) 2000-2020 by Bitvise Limited.
12:24:09.117 Visit www.bitvise.com for latest information about our SSH software.
12:24:09.117 Run 'BvSsh -help' to learn about supported command-line parameters.
12:24:09.117 Cryptographic provider: Windows CNG (x86) with additions
12:24:09.608 Version status: Unknown
The status of the currently installed version is unknown because there has not been a recent, successful check for updates.
12:24:09.665 Loading default profile.

Log in Exit

Внутри удаленного АРМ



Внутри удаленного АРМ



10.10.211.172 — Подключение к удаленному рабочему столу

IDS_packet_time-2022-02-15T05_58_20.656887Z_ruleid-3061278.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	10.10.1.20	HTTP	265	POST /site/login HTTP/1.1 (application/x-www-form-urlencoded)

Host: ampire.com\r\n
Accept: */*\r\n
Content-Type: application/x-www-form-urlencoded\r\n
User-Agent: Wfuzz/2.2.11\r\n
> Content-Length: 44\r\n
\r\n
[Full request URI: http://ampire.com/site/login]
[HTTP request 1/1]
File Data: 44 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "email" = "manager1@ampire.corp"
 - Key: email
 - Value: manager1@ampire.corp
- Form item: "password" = "1qaz2wsx"

```
0010  00 fb 6c 81 40 00 3f 06 54 ce b9 58 b5 37 0a 0a  ..l.@.?.T.X.7..
0020  01 14 86 d2 00 50 7d d5 a4 af 31 8a 15 6d 80 18  .....P}. ..1..m..
0030  01 f6 df 3b 00 00 01 01 08 0a c9 5c 34 74 00 d5  ...;.... ..\4t..
0040  8c 31 50 4f 53 54 20 2f 73 69 74 65 2f 6c 6f 67  .1POST / site/log
0050  69 6e 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73  in HTTP/ 1.1..Hos
0060  74 3a 20 61 6d 70 69 72 65 2e 63 6f 6d 0d 0a 41  t: ampir e.com..A
0070  63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 74  ccept: */*..Cont
0080  65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63  ent-Type : applic
0090  61 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d  ation/x- ww-form
00a0  2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 55 73 65  -urienco ded Use
00b0  72 2d 41 67 65 6e 74 3a 20 57 66 75 7a 7a 2f 32  r-Agent: Wfuzz/2
00c0  2e 32 2e 31 31 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  .2.11..C ontent-L
00d0  65 6e 67 74 68 3a 20 34 34 0d 0a 0d 0a 65 6d 61  ength: 4 4....ema
00e0  69 6c 3d 6d 61 6e 61 67 65 72 31 40 61 6d 70 69  il=manag er1@ampi
00f0  72 65 2e 63 6f 72 70 26 70 61 73 73 77 6f 72 64  re.corp& password
0100  3d 31 71 61 7a 32 77 73 78  =1qaz2ws x
```

Спасибо за внимание!

