ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

КИБЕРКВЕСТ

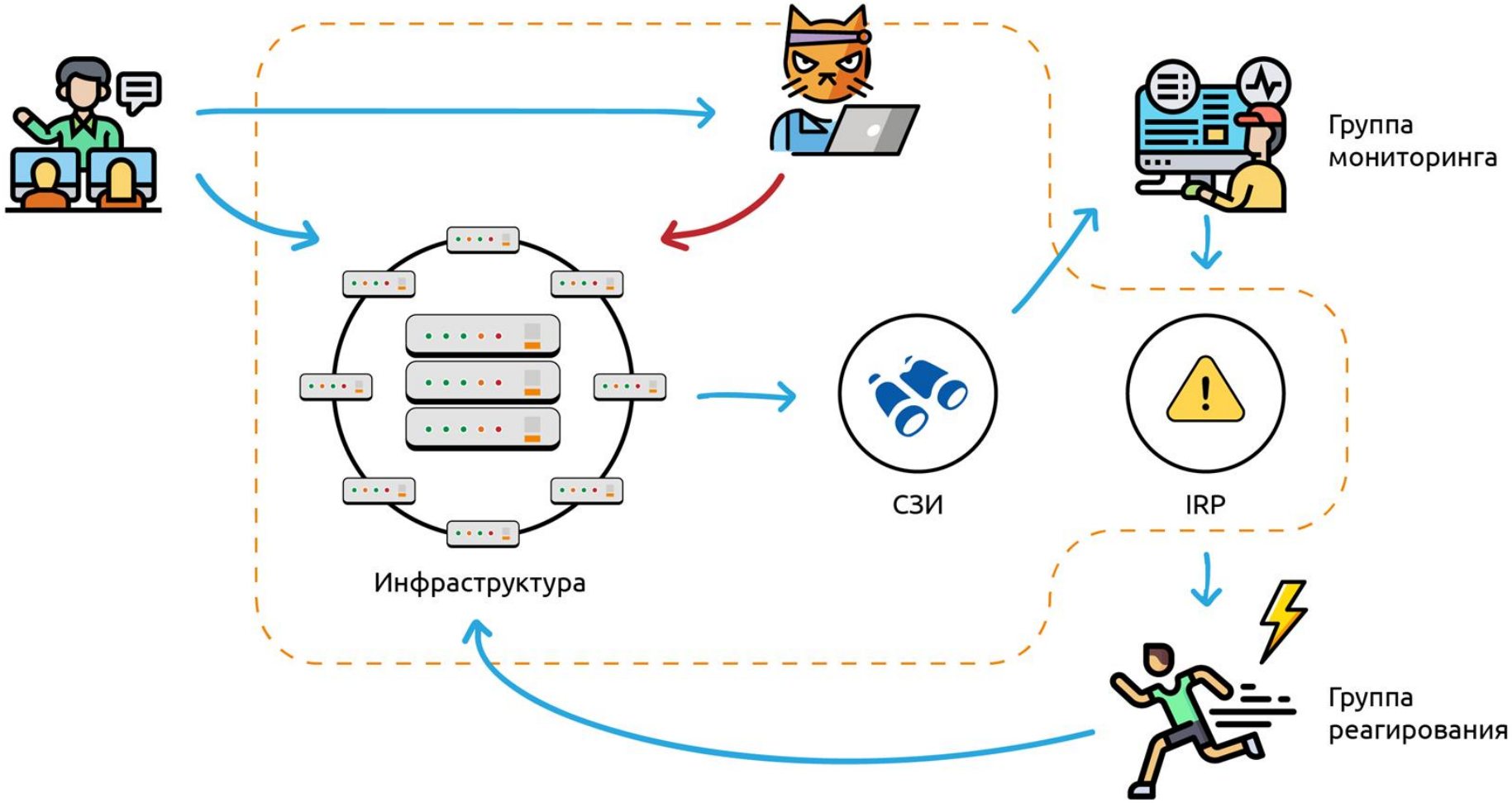
Защита базы данных предприятия

Яна Баринова
АО «Перспективный мониторинг»

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

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

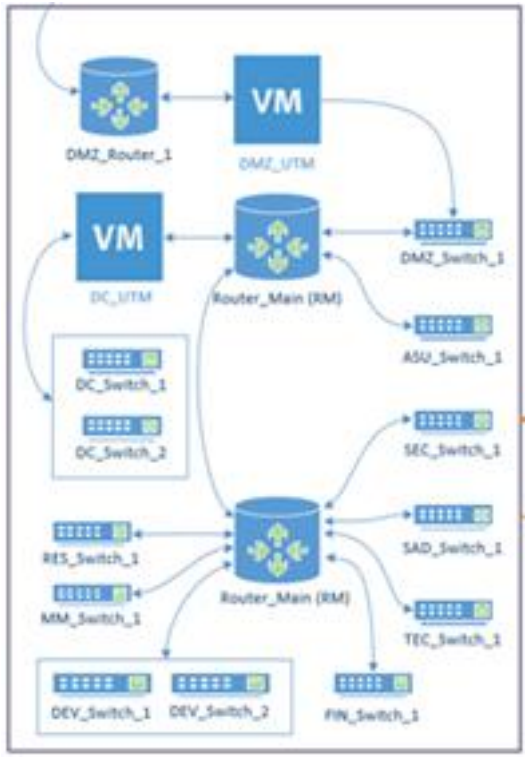
AMPIRE


Группа
мониторинга
СЗИ
IRP
Инфраструктура
Группа
реагирования

AMPIRE - это платформа

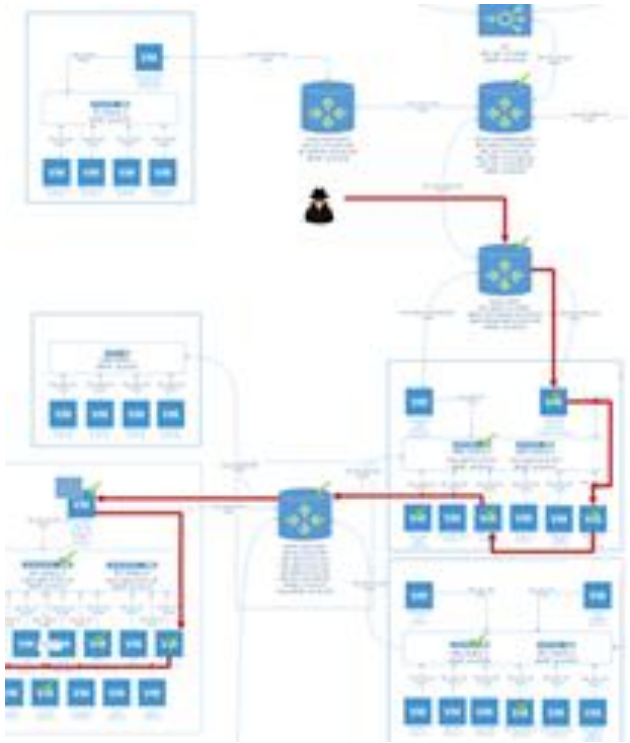
Практические занятия на цифровом двойнике реальной инфраструктуры

Симуляция сети с ИТ и SCADA-сегментами



Security Operations Center

Проприетарный автоматический нарушитель



Задачи групп

Мониторинг

Анализ событий ИБ

Заведение карточек инцидентов

Описание вектора атаки

(Cyber Kill Chain)

Реагирование

Расследование инцидентов

Восстановление рабочего состояния ИС

Устранение уязвимостей

Легенда:

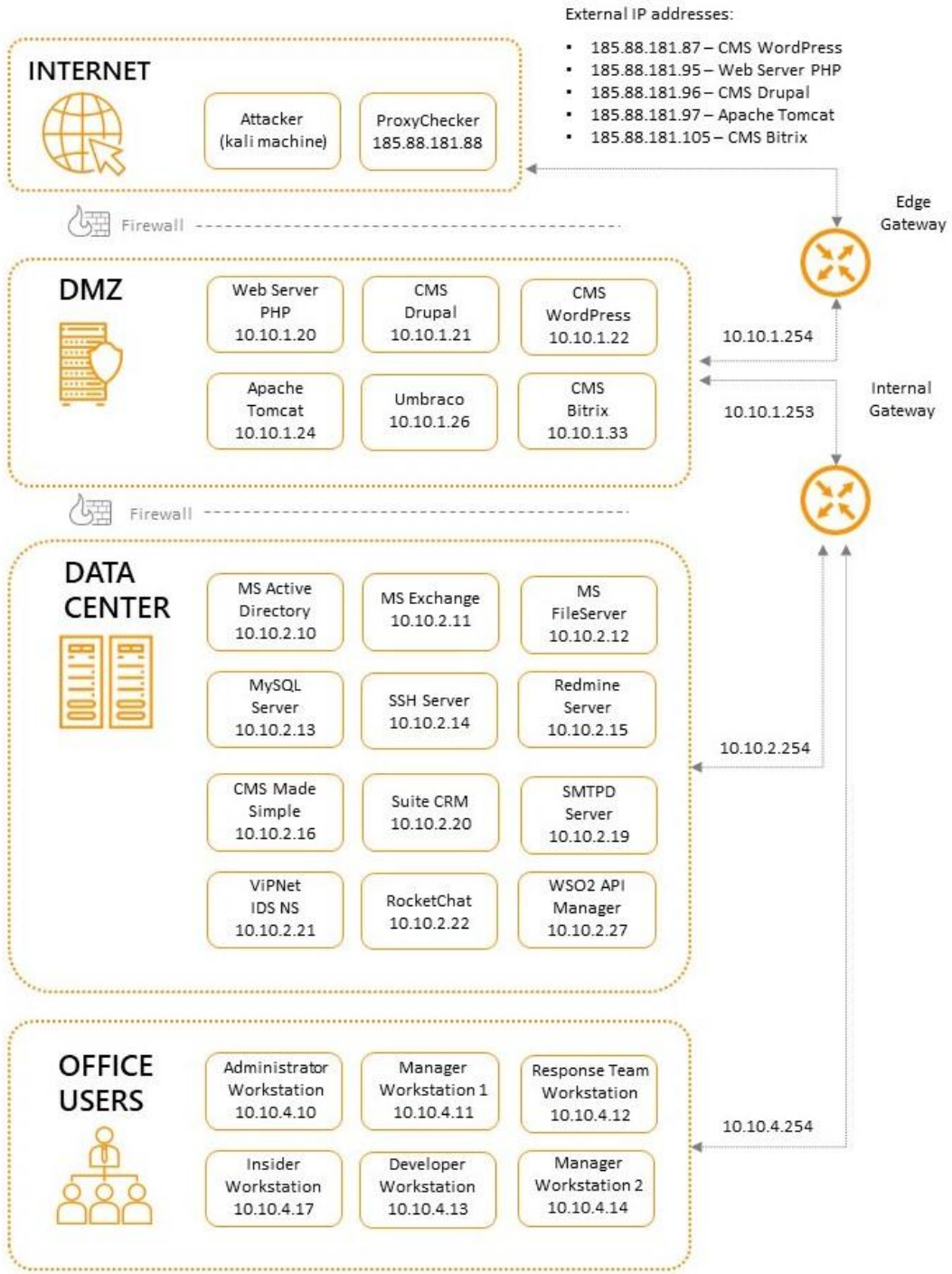
Внешний злоумышленник находит в интернете сайт Компании и решает провести атаку на него с целью получения доступа к внутренним ресурсам. Обнаружив и проэксплуатировав уязвимость на сайте, нарушитель получает доступ к серверу, который помимо основной информационной задачи предоставляет пользователям Компании инструмент для генерации отчетов. С помощью данного вектора нарушитель пробует получить доступ на рабочие машины сотрудников. Главная цель – выполнить дамп корпоративной базы данных.

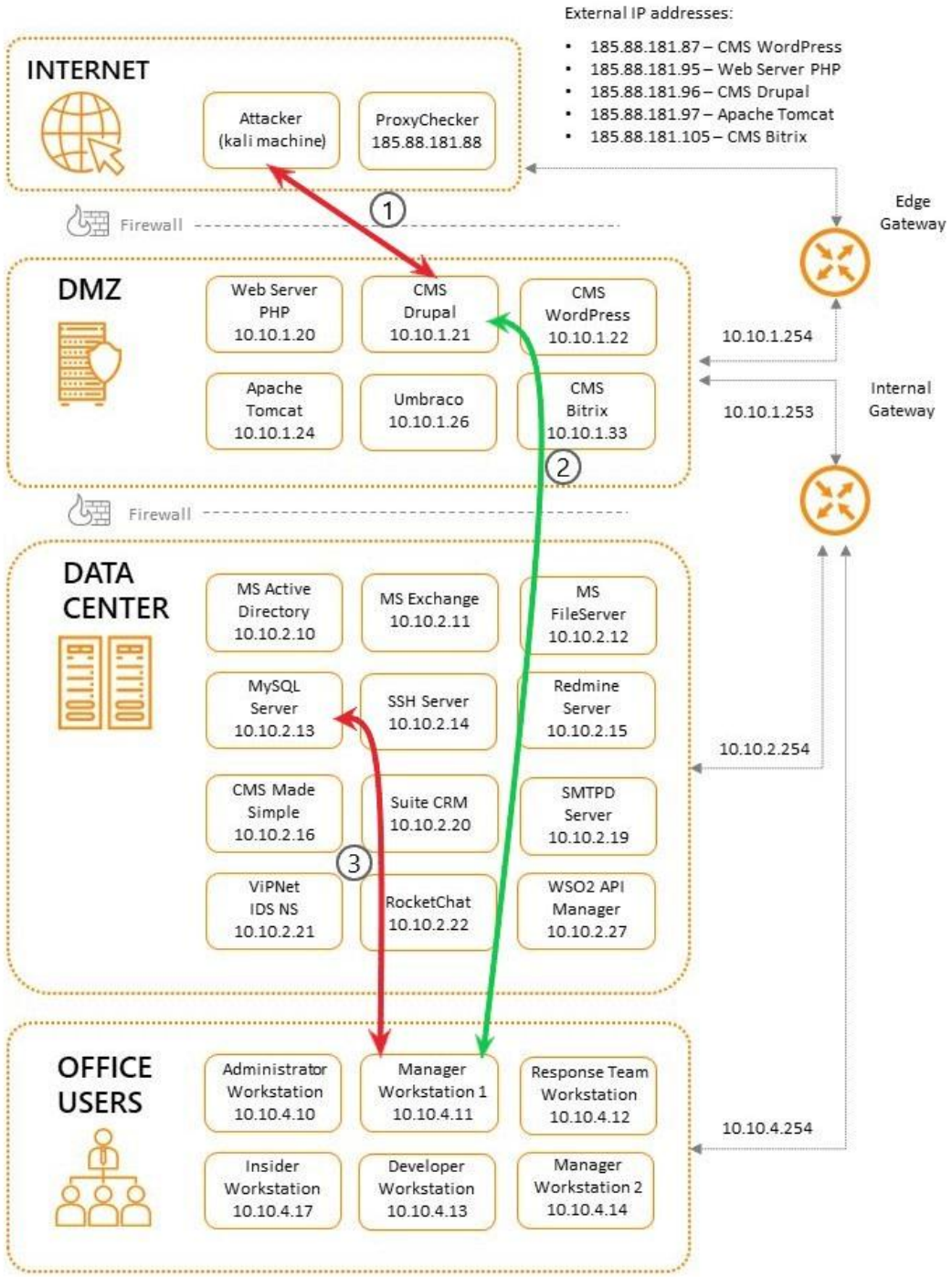
Квалификация нарушителя средняя. Нарушитель умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

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 сайте, нарушитель получает доступ к серверу, который помимо основной информационной задачи предоставляет пользователям Компании инструмент для генерации отчетов. С помощью данного вектора нарушитель пробует получить доступ на рабочие машины сотрудников. Главная цель – выполнить дамп корпоративной базы данных.

Квалификация нарушителя средняя. Нарушитель умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.


External IP addresses:
185.88.181.87 – CMS WordPress
185.88.181.95 – Web Server PHP
185.88.181.96 – CMS Drupal
185.88.181.97 – Apache Tomcat
185.88.181.105 – CMS Bitrix
INTERNET
Attacker (kali machine)
ProxyChecker 185.88.181.88
Firewall
Edge Gateway
DMZ
Web Server PHP 10.10.1.20
CMS Drupal 10.10.1.21
CMS WordPress 10.10.1.22
Apache Tomcat 10.10.1.24
Umbraco 10.10.1.26
CMS Bitrix 10.10.1.33
10.10.1.254
10.10.1.253
Internal Gateway
Firewall
DATA CENTER
MS Active Directory 10.10.2.10
MS Exchange 10.10.2.11
MS FileServer 10.10.2.12
MySQL Server 10.10.2.13
SSH Server 10.10.2.14
Redmine Server 10.10.2.15
CMS Made Simple 10.10.2.16
Suite CRM 10.10.2.20
SMTPD Server 10.10.2.19
ViPNet IDS NS 10.10.2.21
RocketChat 10.10.2.22
WSO2 API Manager 10.10.2.27
10.10.2.254
OFFICE USERS
Administrator Workstation 10.10.4.10
Manager Workstation 1 10.10.4.11
Response Team Workstation 10.10.4.12
Insider Workstation 10.10.4.17
Developer Workstation 10.10.4.13
Manager Workstation 2 10.10.4.14
10.10.4.254


External IP addresses:
185.88.181.87 – CMS WordPress
185.88.181.95 – Web Server PHP
185.88.181.96 – CMS Drupal
185.88.181.97 – Apache Tomcat
185.88.181.105 – CMS Bitrix
INTERNET
Attacker (kali machine)
ProxyChecker 185.88.181.88
Firewall
1
Edge Gateway
DMZ
Web Server PHP 10.10.1.20
CMS Drupal 10.10.1.21
CMS WordPress 10.10.1.22
Apache Tomcat 10.10.1.24
Umbraco 10.10.1.26
CMS Bitrix 10.10.1.33
10.10.1.254
10.10.1.253
Internal Gateway
2
Firewall
DATA CENTER
MS Active Directory 10.10.2.10
MS Exchange 10.10.2.11
MS FileServer 10.10.2.12
MySQL Server 10.10.2.13
SSH Server 10.10.2.14
Redmine Server 10.10.2.15
10.10.2.254
CMS Made Simple 10.10.2.16
Suite CRM 10.10.2.20
SMTPD Server 10.10.2.19
3
ViPNet IDS NS 10.10.2.21
RocketChat 10.10.2.22
WSO2 API Manager 10.10.2.27
OFFICE USERS
Administrator Workstation 10.10.4.10
Manager Workstation 1 10.10.4.11
Response Team Workstation 10.10.4.12
10.10.4.254
Insider Workstation 10.10.4.17
Developer Workstation 10.10.4.13
Manager Workstation 2 10.10.4.14

Проактивная позиция

Не можем повлиять

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

Можем повлиять

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

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Яна Баринова
Специалист по информационной безопасности

yana.barinova@amonitoring.ru

amonitoring.ru

ampire.team