Автоматическая адаптация планов реагирования в SOAR 2.0

Роман Душков
Ведущий пресейл менеджер

Security Vision

Кирилл Михайлянц
Ведущий специалист по информационной безопасности

ДиалогНаука

Security Vision

ДиалогНаука

План вебинара

1. Какую роль играет **платформа**
2. Какую задачу выполняет продукт **SOAR 2.0**
3. Как выстраивается **цепочка атаки** (зачем интеграции с 3rd party)
4. Как выстроено **объектно-ориентированное реагирование**
5. Как применяется **граф взаимосвязей**
6. Где искать **лучшие практики**

ПЛАТФОРМА

Единая гибкая платформа

~ CRM

~ BPM

~ BI

Объекты, карточки и внешний вид

Ролевая модель и настройка меню

Рабочие процессы и структура

Security Vision

Визуализация и аналитика

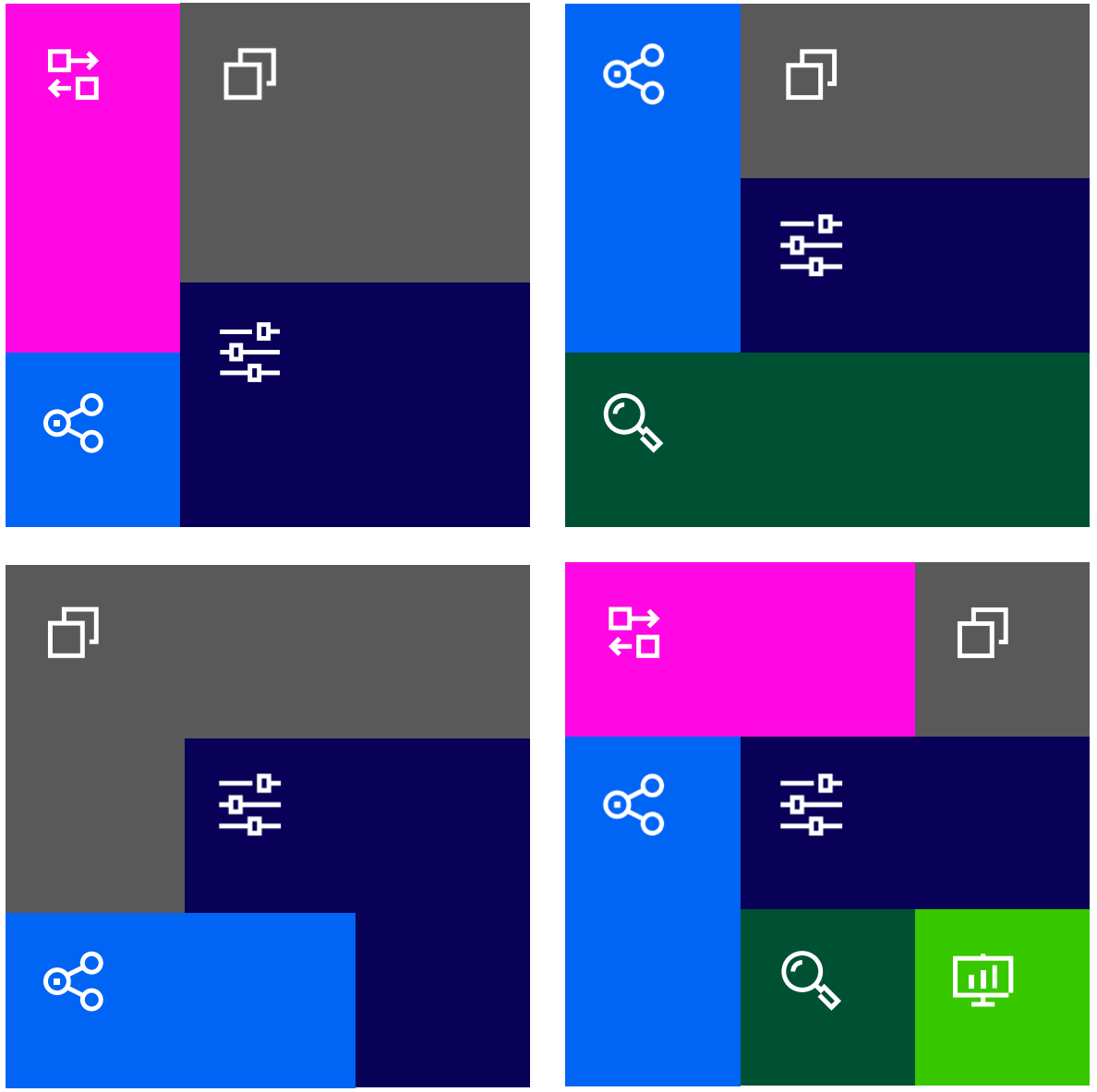
~ RPA

~ Word

Интеграции с внешними системами

Отчёты и логирование действий

Собирайте модули под ваши задачи без навыков программирования с помощью гибких конструкторов



СБЕР

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- 100+ сотрудников команды SOC+IRP
- Разработка плейбуков, управление проблемами и др.
- 50+ интеграций с ИТ и ИБ системами

ПОЧТА РОССИИ

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- 15+ плейбуков и процесс управления уязвимостями
- Управление внутренними проектами подразделения ИБ

Импортозамещение продуктов для автоматизации процессов ИБ/ИТ

CISCO SecureX

ivanti Platform

Siemplify

IBM OpenPages with Watson

cyberbit SOC 3D

The Hive

Anomali

RSA Archer GRC

paloalto NETWORKS Cortex XSOAR

SAS OpRisk Management

MICRO FOCUS ArcSight

SAP Enterprise Risk Management

IBM Resilient

FORTINET FortiSOAR

Security Vision

Управление инцидентами
SOAR
Security Orchestration, Automation and Response

Управление уязвимостями
VM
Vulnerability Management

Управление активами
AM
Asset Management

Анализ угроз, киберразведка
TIP
Threat Intelligence Platform

Поведенческий анализ
UEBA
User and Entity Behavior Analysis

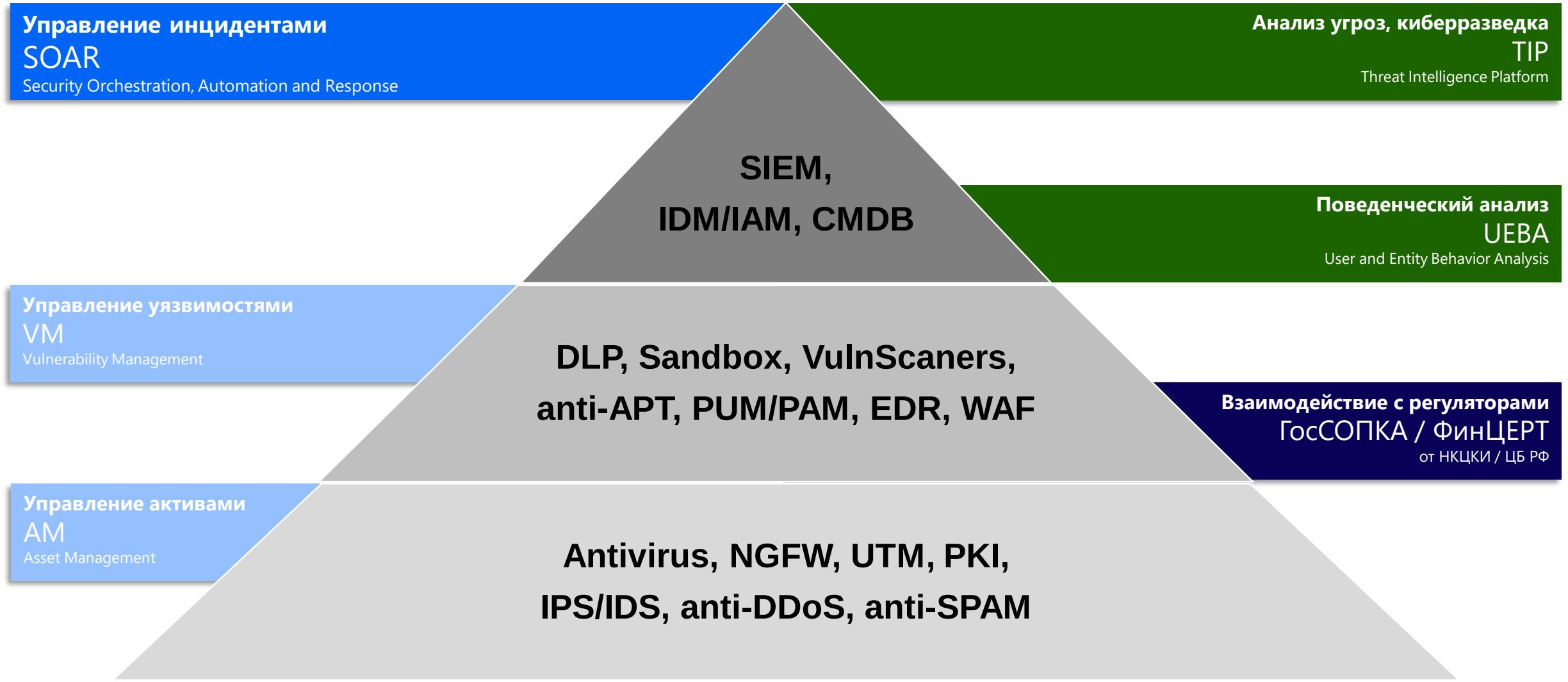
Поиск аномалий с ML
AD
Anomaly Detection with Machine Learning

Управление рисками
SGRC
Governance, Risk Management and Compliance

Проверка соответствия
КИИ
Критическая Информационная Инфраструктура

Взаимодействие с регуляторами
ГосСОПКА / ФинЦЕРТ
от НКЦКИ / ЦБ РФ

Пирамида зрелости процессов практической безопасности



SOAR 2.0

Управление инцидентами

в Security Vision 5

1. Сбор инцидентов
2. Ведение задач
3. Реагирование

Управление инцидентами

в Security Vision 5

1

Сбор данных

Интеграция с СЗИ, группировка событий и дедупликация

2

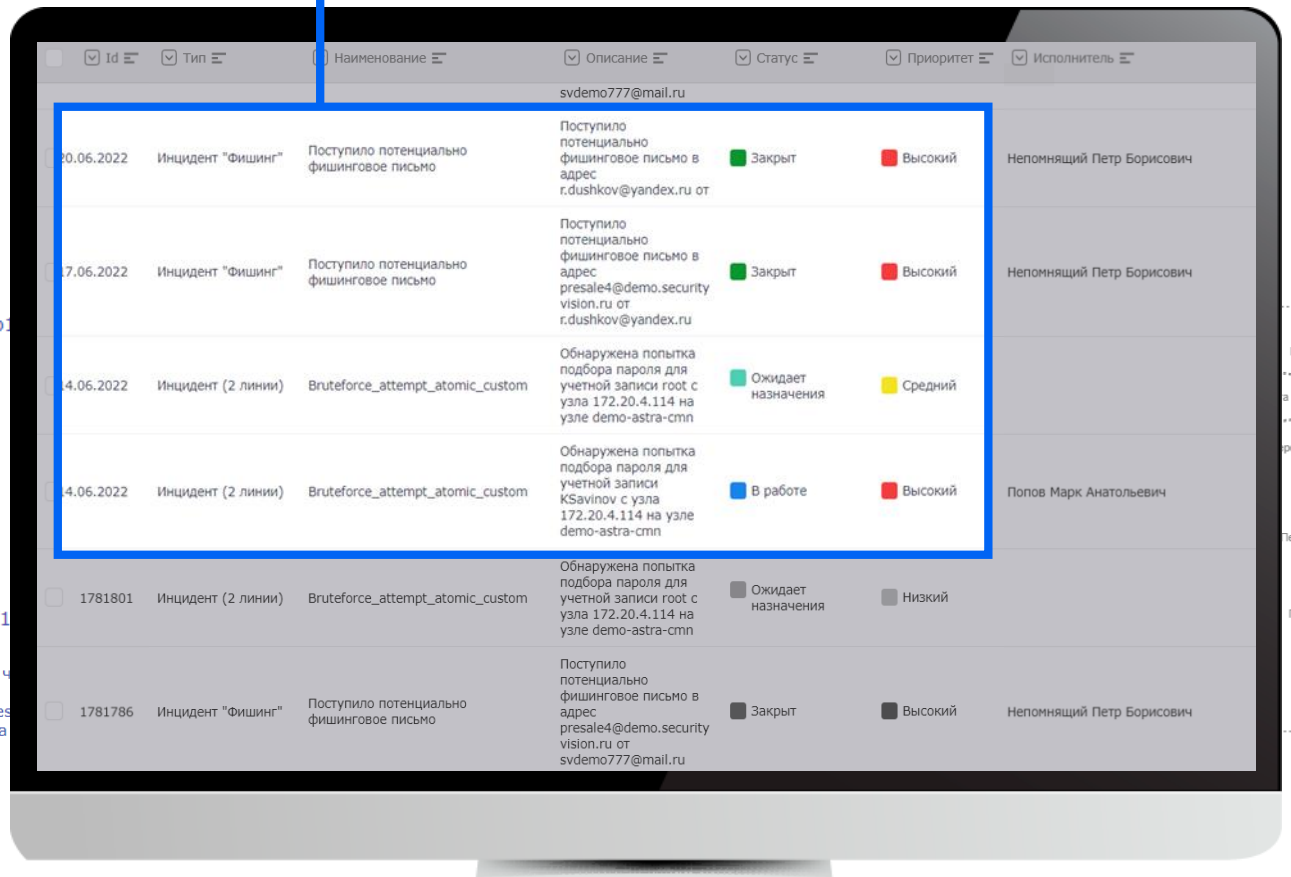
Тикетинг

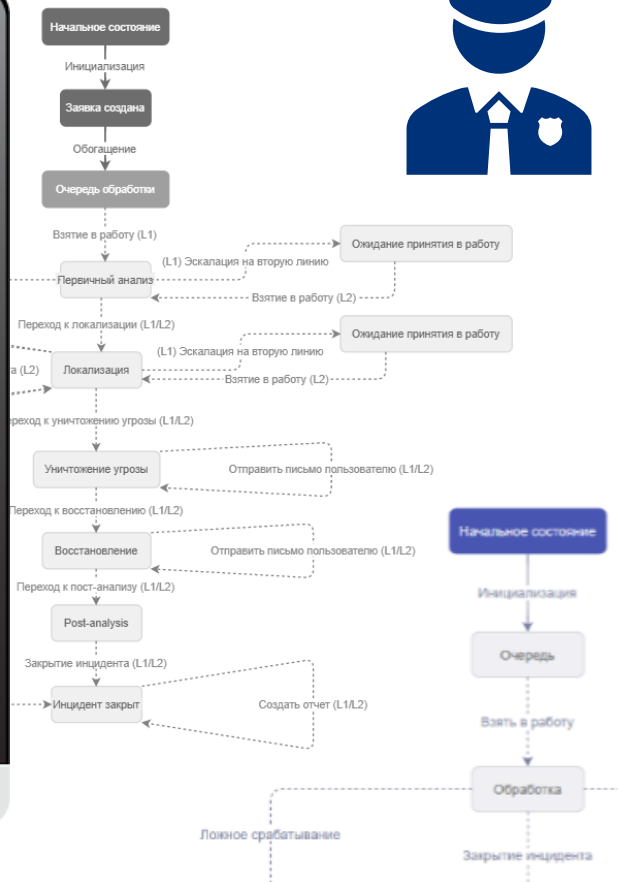
Передача в группу реагирования, обогащение данными из других систем

3

Реагирование

Управление СЗИ из единого окна, SLA, формирование процессов





Результат анализа https://tuiaazul.com.br/www.netflix/0cb1

Домен: tuiaazul.com.br
Страна: US
Город:
Сервер: Apache
IP-адрес: 192.185.177.73
ASN: AS26337
Имя ASN: OIS1, US

UrlSCAN Score: 100
True

Ссылка на результат проверки: https://urlscan.io/result/1

Результат анализа сигнатуры EICAR-Test-File

Описание сигнатуры: Под именем "EICAR-Tes
COM-файл, который вирусом НЕ ЯВЛЯЕТСЯ, а
возвращает управление DOS.

Дата обнаружения:

Класс: DangerousObject
Дата публикации в базе: 19/04/2016

Управление инцидентами

1 Анализ письма

выделение темы, содержимого, текста и ссылок

15 мин

2 Поиск деталей

проверка отправителя, домена, вложений и ссылок

25 мин

3 Поиск похожих

поиск других получателей

10 мин

4 Блокировка

добавление отправителя и домена в чёрный список

10 мин

5 Очистка сервера

от опасных писем или вложений

10 мин

6 Оповещение пользователя

запуск проверки на рабочих станциях пользователей

5 мин

75 минут без SOAR

Управление инцидентами с автоматизацией

HYBRID ANALYSIS · urlscan.io · WhoisXML API · ThreatCrowd · MaxPatrol SIEM · kaspersky · Exchange

1

- **Анализ письма** — выделение темы, содержимого, текста и ссылок
- **Поиск деталей** — проверка отправителя, домена, вложений и ссылок
- **Поиск похожих** — поиск других получателей
- **Блокировка** — добавление отправителя и домена в чёрный список
- **Очистка сервера** — от опасных писем или вложений

4 мин

2

- **Оповещение пользователя** — запуск проверки на рабочих станциях пользователей

1 мин

снижение влияния человеческого фактора

ускорение за счёт автоматизации

5 минут без SOAR

ИНТЕГРАЦИИ И ЦЕПОЧКА АТАКИ

Реализованные интеграции

Сбор

MICRO FOCUS ArcSight

kaspersky

Реагирование

Exchange

Microsoft Active Directory

virustotal

Управление инцидентами

Добавление пользователя в группу AD

Шаг 1 | Шаг 2 | Шаг 3 | Шаг 4

1 **Обогащение данных по инциденту**

Получение данных по УЗ из AD, в т.ч. адрес почты

Microsoft Active Directory

2 **Отправка письма на почтовый ящик пользователя**

с запросом номера заявки на добавление в группу AD

Exchange

3 **Проверка номера заявки**

4 **Закрытие инцидента**

написание отчёта

ДиалогНаука

Управление инцидентами
Обнаружение ВПО

Шаг 1 | Шаг 2 | Шаг 3 | Шаг 4

1 **Обогащение данных по инциденту**

в зависимости от наличия индикаторов

virustotal

Microsoft Active Directory

2 **Запрос информации у пользователя**

по электронной почте, парсинг ответа

Exchange

3 **Создание задачи на сканирование АРМ**

сбор статуса выполнения задачи

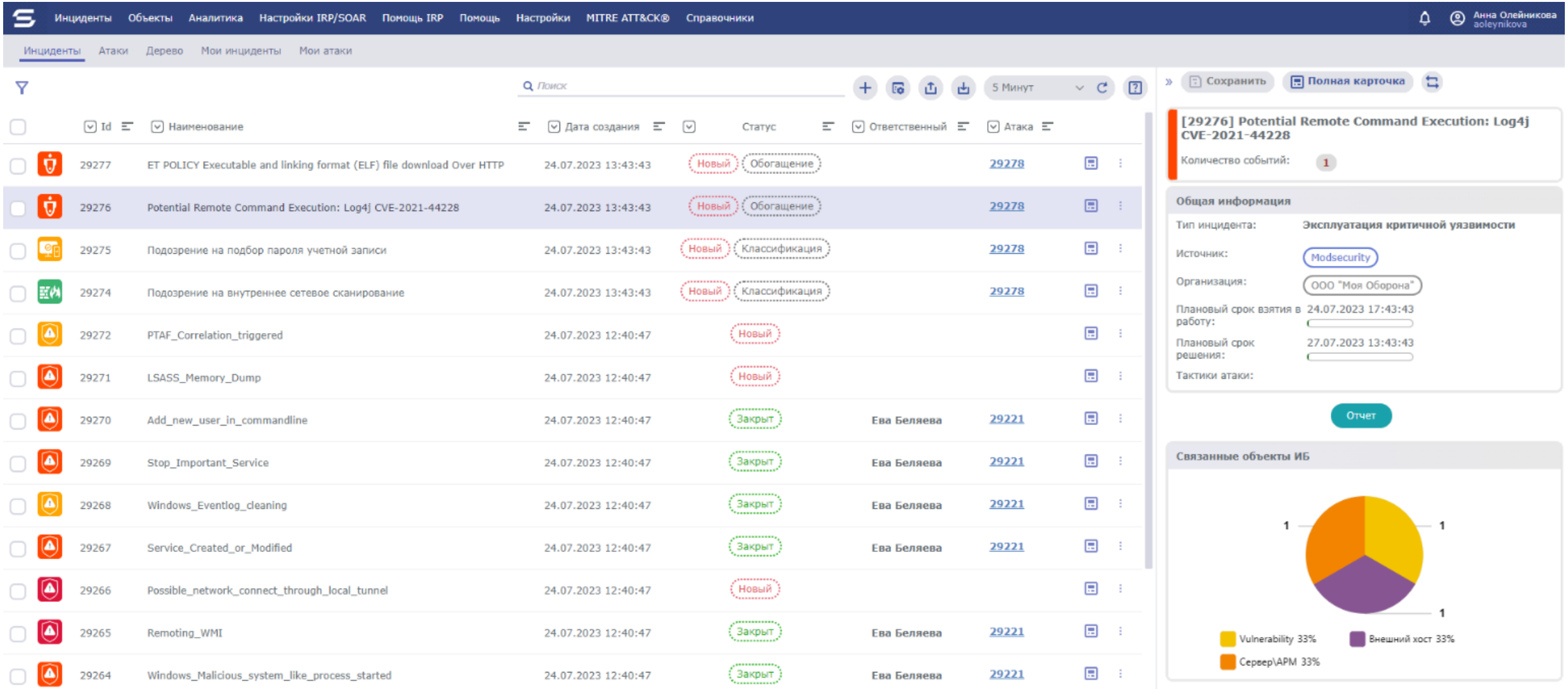
kaspersky

4 **Закрытие инцидента**

написание отчёта

ДиалогНаука

Что видит аналитик ИБ



Принятие качественных стратегических и тактических решений

Актуальная информация в режиме реального времени

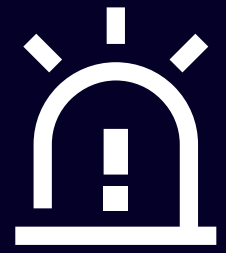
Создания интеграций с любыми ИС при помощи веб-интерфейса

Сокращение трудовых ресурсов и исключение человеческого фактора

Автоматизация сбора информации и реагирования

Единый инсталлятор и платформенное решение

Снижение ущерба и времени воздействия инцидентов ИБ



Сокращение времени в среднем в 10 раз за счёт автоматизации

Любая сложность сценария и логика бизнес-процесса

Конструктор коннекторов

email | Syslog | файлы | БД | API | DNS | LDAP | скрипты

создание новых коннекторов **без участия вендоров**

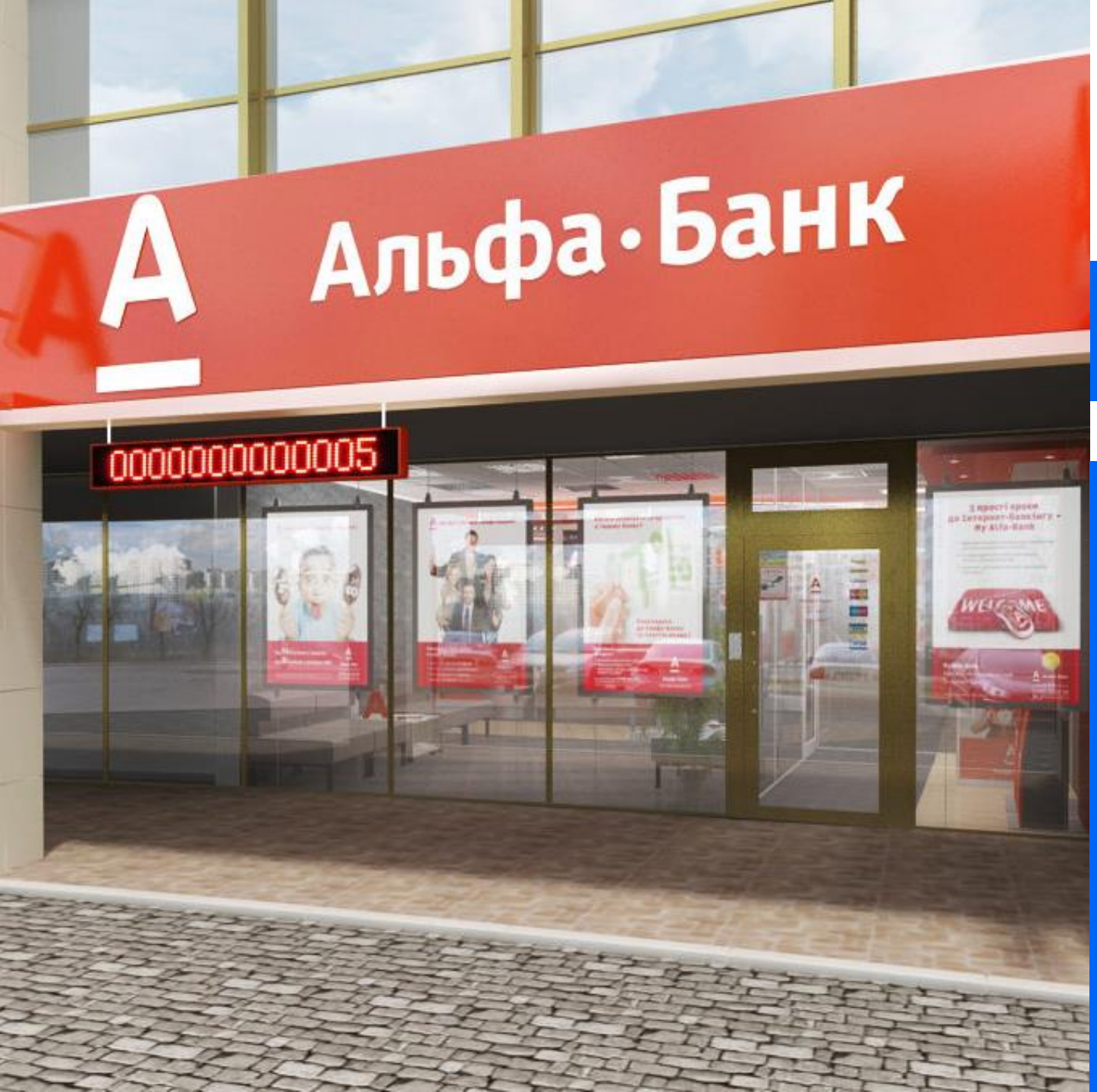
Сбор и обогащение

Реагирование на события

X5 Group

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- 15+ автоматизированных плейбуков реагирования
- Глубокие процессы обработки инцидентов
- 20+ интеграций с ИТ-системами и СЗИ



УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- 20+ автоматизированных плейбуков реагирования
- Реализация процесса управление уязвимостями
- 30+ интеграций, включая взаимодействие с ФинЦЕРТ

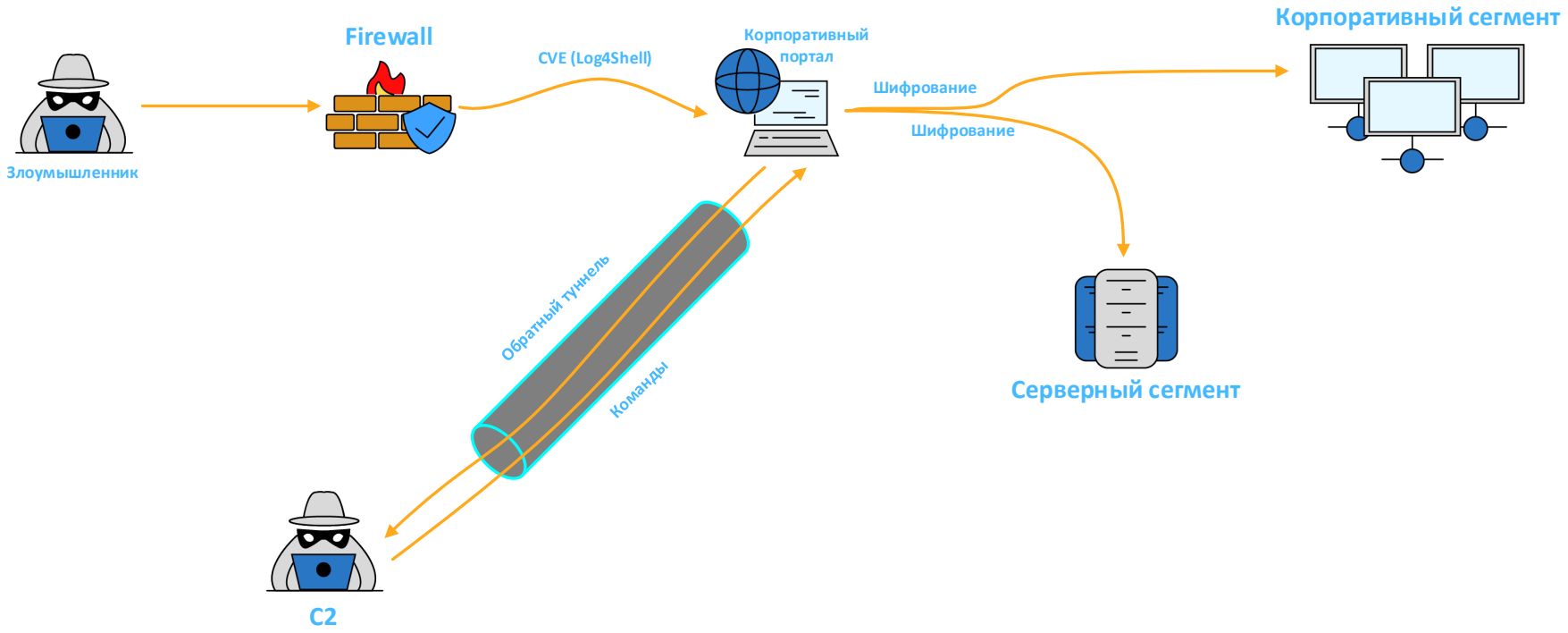
открытие

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- 30+ автоматизированных плейбуков и 50+ интеграций
- Проектная реализация процесса управление ИТ-активами
- Интеграция с Data Lake и использование ML модели

Сценарий атаки

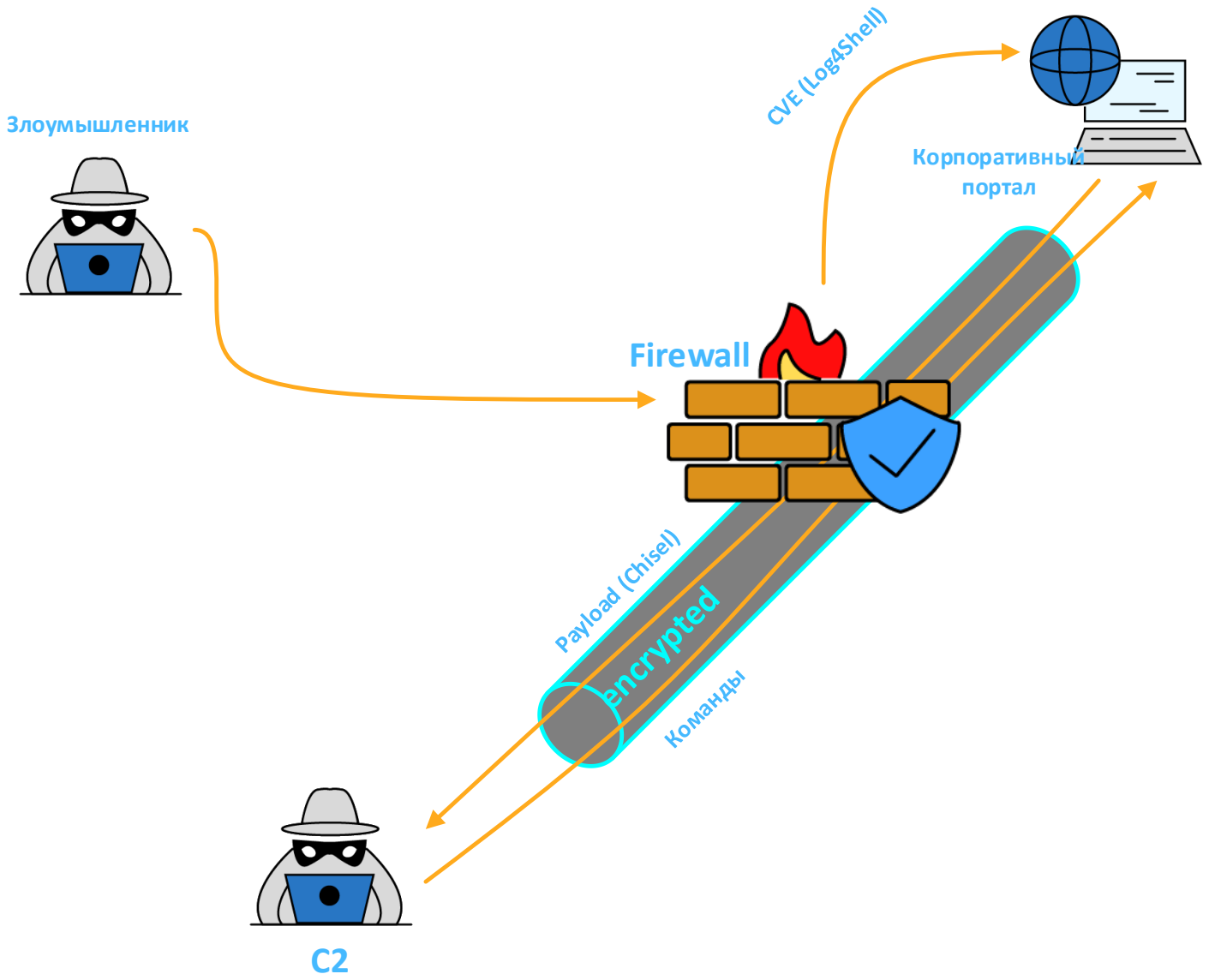
Путь злоумышленника



периметр

- MP SIEM
- Suricata
- ModSecurity
- KSC

Злоумышленник: шаг 1



обратный туннель c2

РЕЗУЛЬТАТ

MP SIEM

обогащение chisel

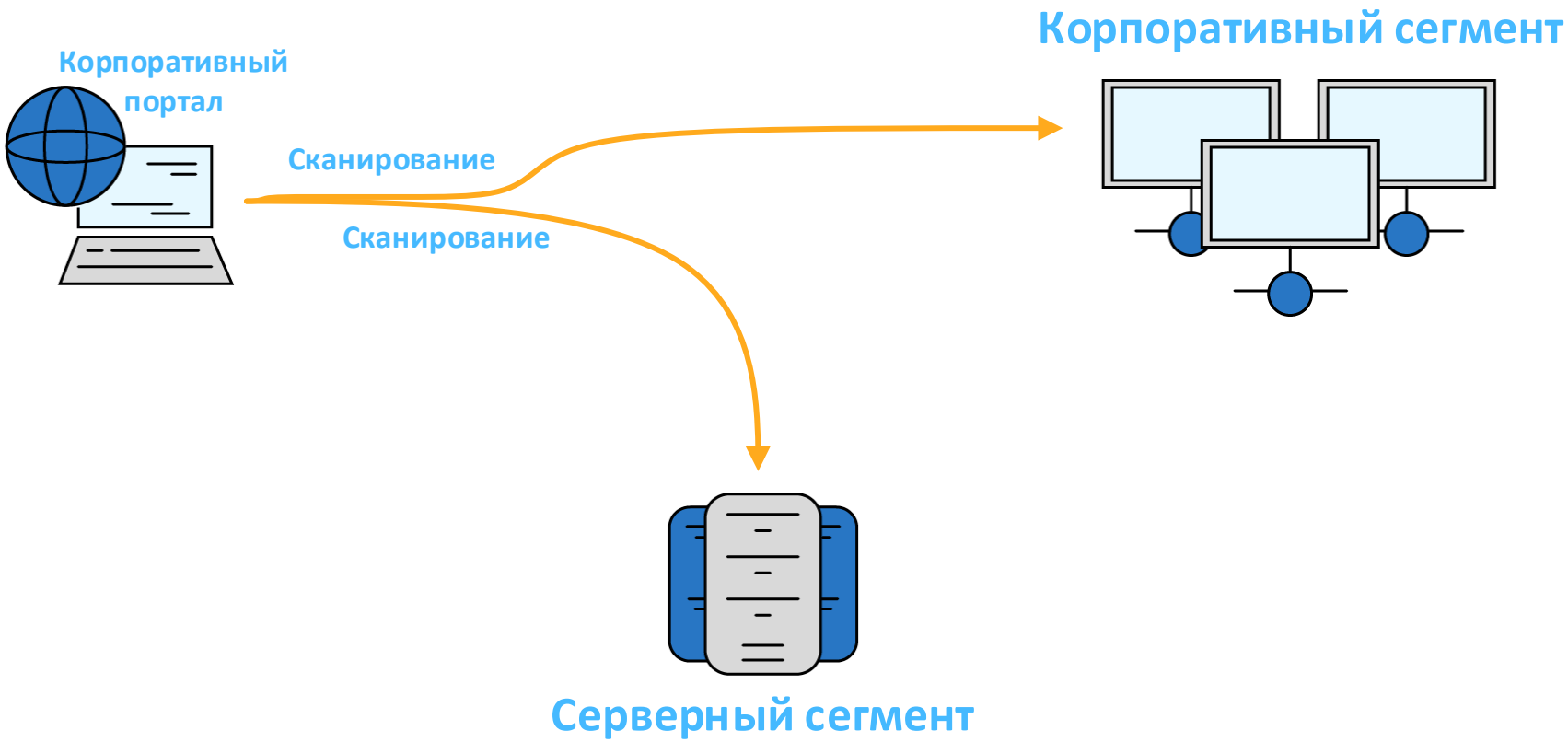
Suricata

эксплуатация log4shell
detect ELF

ModSecurity

KSC

Злоумышленник: шаг 2



FQDN хостов

РЕЗУЛЬТАТ

MP SIEM

логи

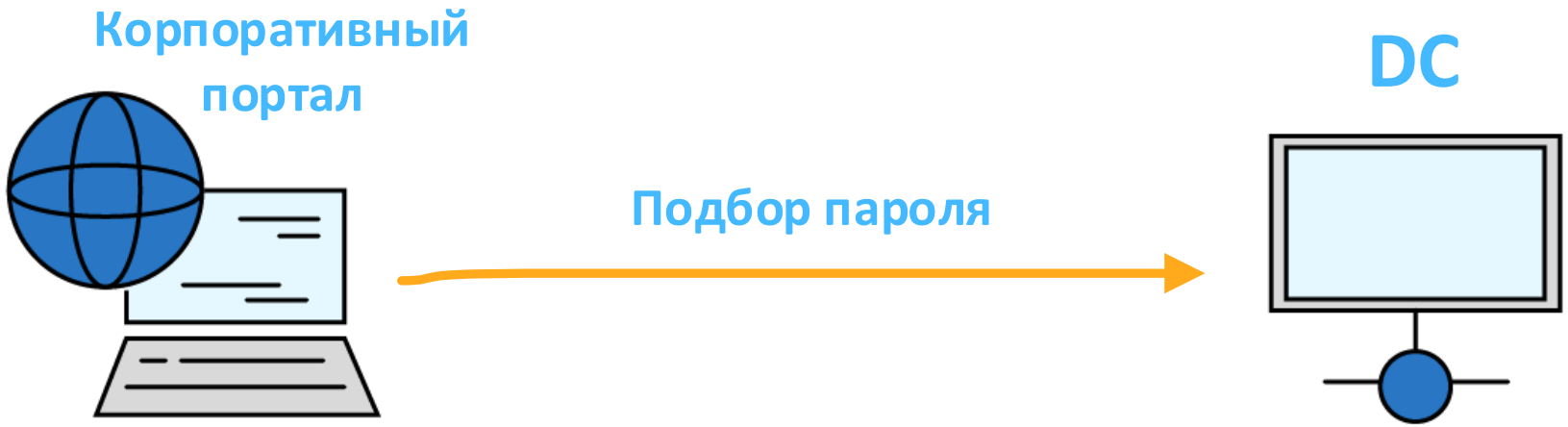
Suricata

ModSecurity

detect scan

KSC

Злоумышленник: шаг 3



account successfully logged on

РЕЗУЛЬТАТ

MP SIEM

event log

Suricata

ModSecurity

KSC

Злоумышленник: шаг 4

добавление в группу администраторов

РЕЗУЛЬТАТ

MP SIEM

event log

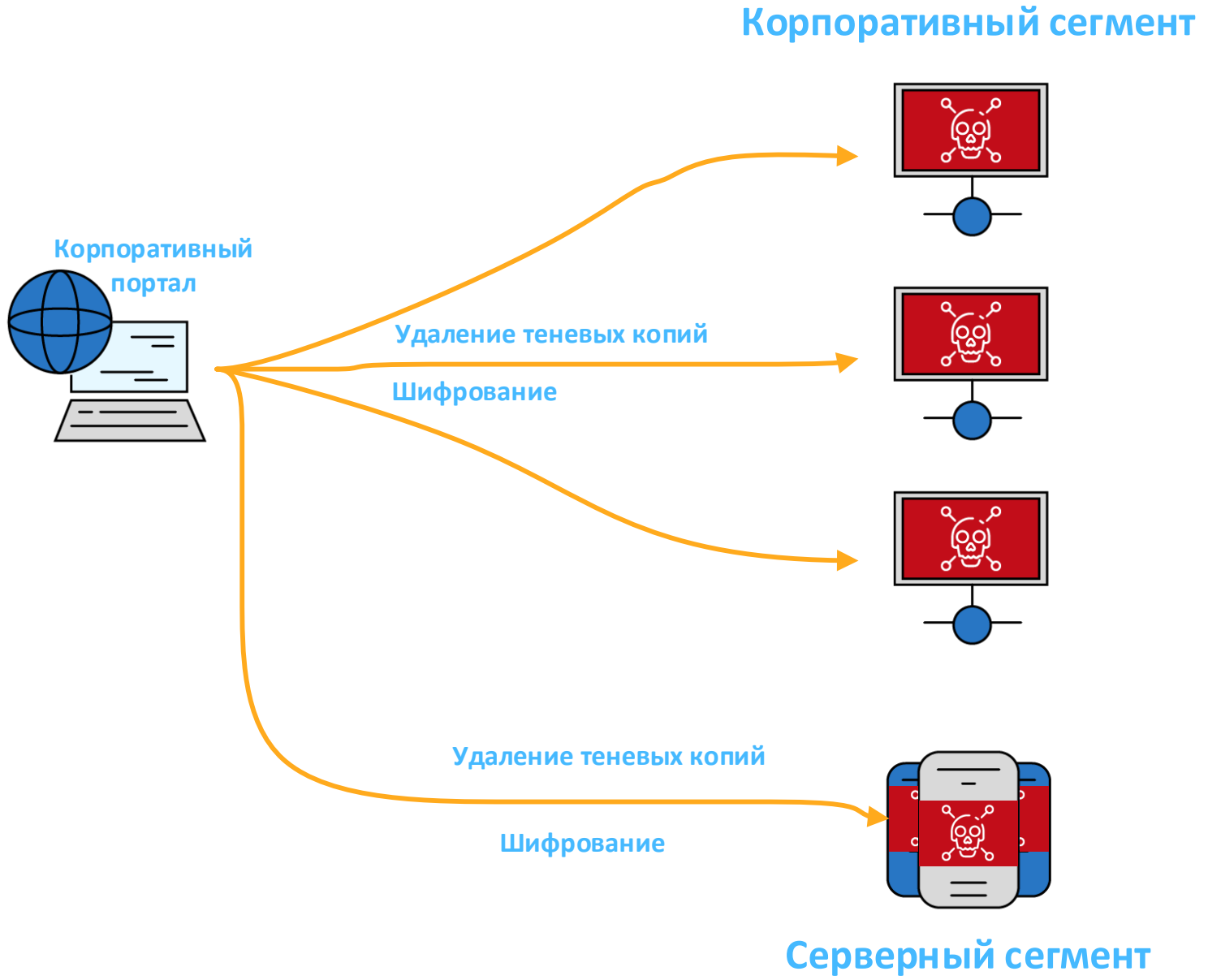
Suricata

ModSecurity

эксплуатация CVE PrintNighmare

KSC

Злоумышленник: шаг 5



теневые копии удалены, информация на АРМ и серверах зашифрована

РЕЗУЛЬТАТ

MP SIEM

создан инцидент

Suricata

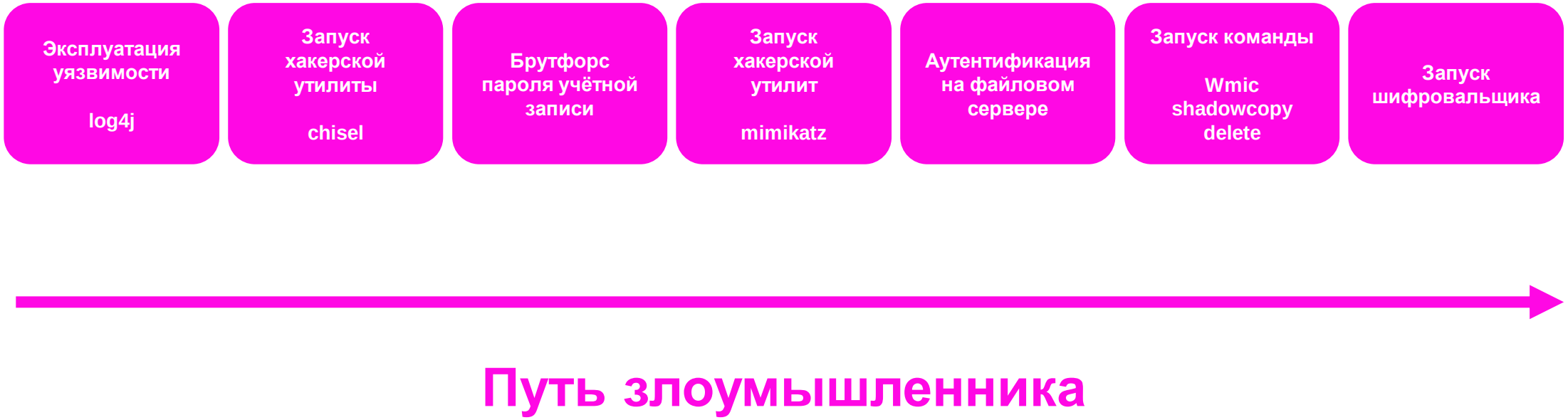
ModSecurity

detect scan

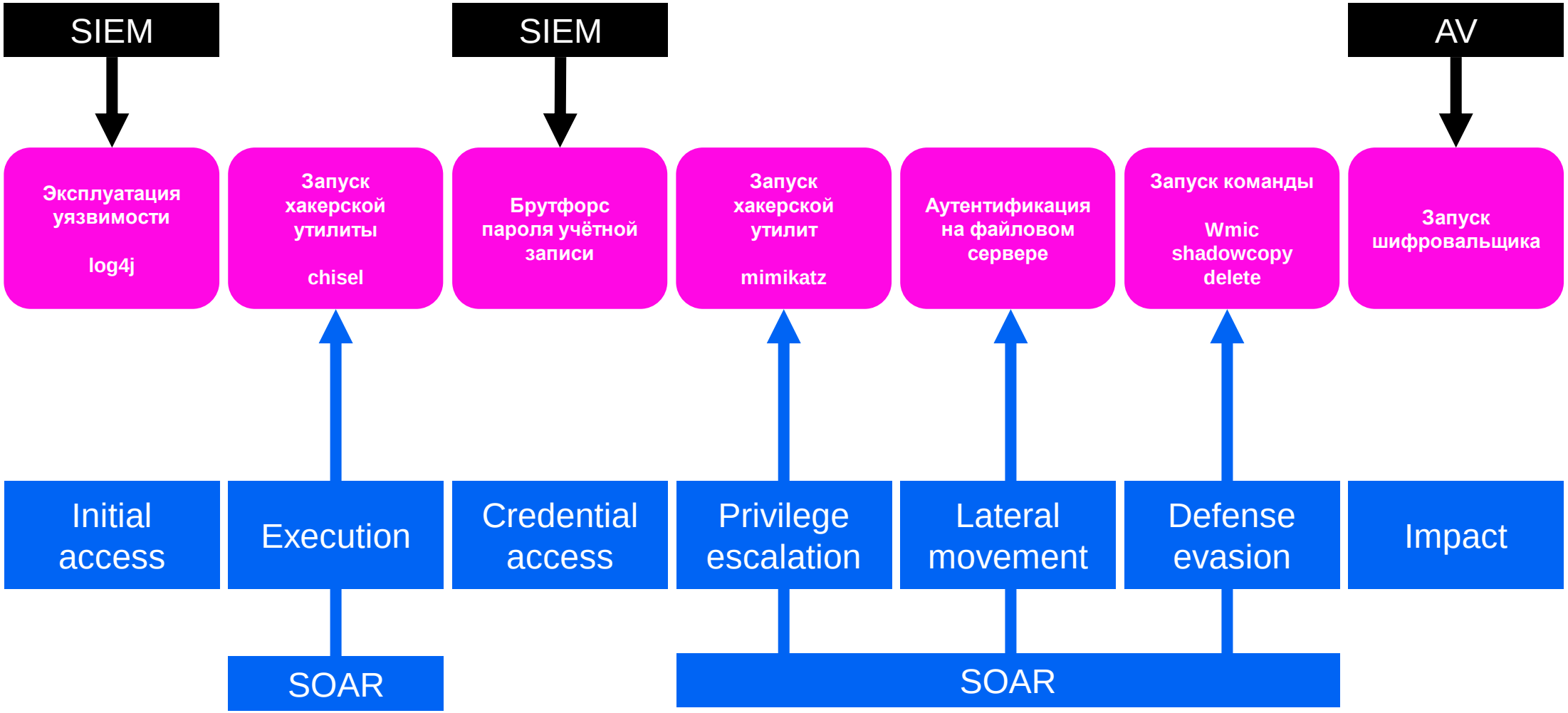
KSC

alert

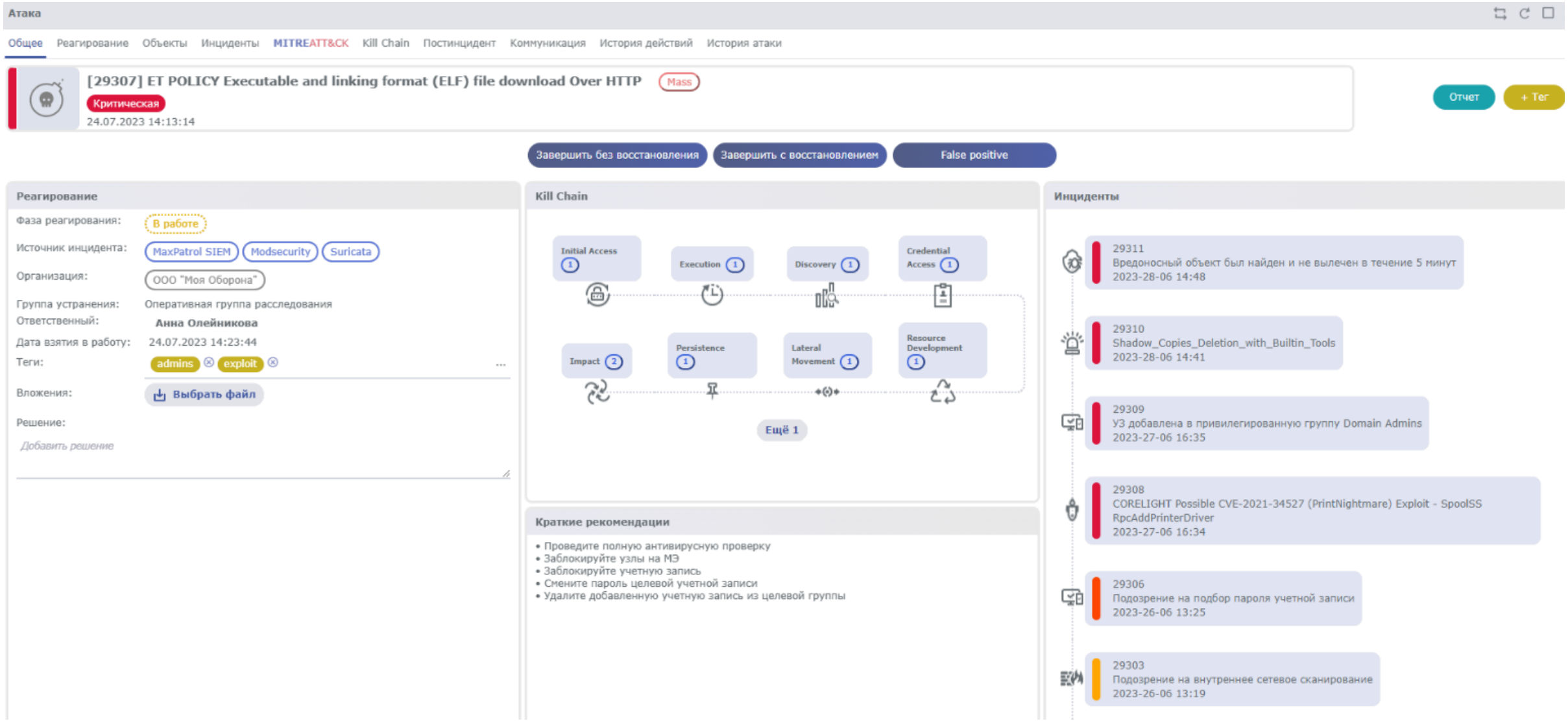
Автоматическое построение Kill Chain



Автоматическое построение Kill Chain



Автоматическое построение Kill Chain



ОБЪЕКТО-ОРИЕНТИРОВАННОЕ РЕАГИРОВАНИЕ

Рост количества атак и влияния человеческого фактора

$4.24 млн.

максимальная за 17 лет аналитики и отчётов средняя стоимость утечки данных

+141%
количество утечек различных типов данных

+55%
утечек ПДн в области здравоохранения

33%
доля массовых атак от общего количества

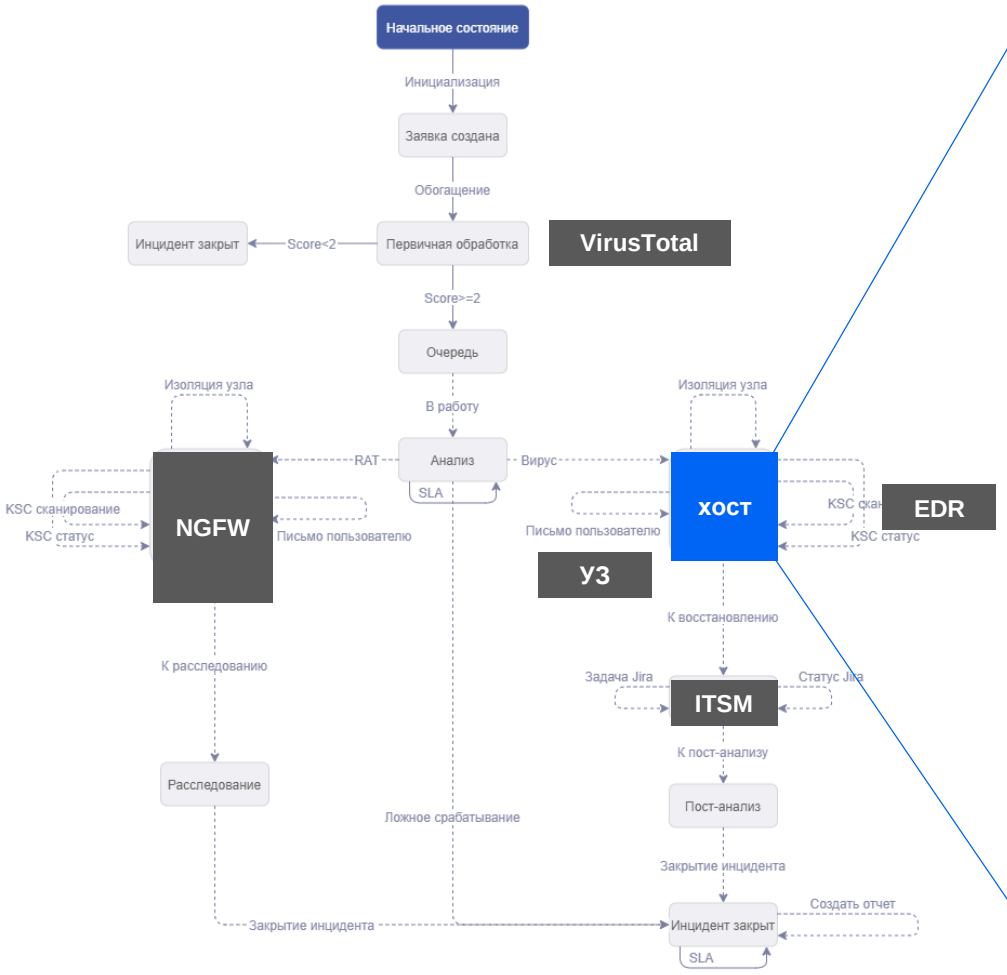
x3.5
атаки с использованием троянов-вымогателей

x2
атак на веб-ресурсы

3 млрд.
фишинговых писем отправляется ежедневно

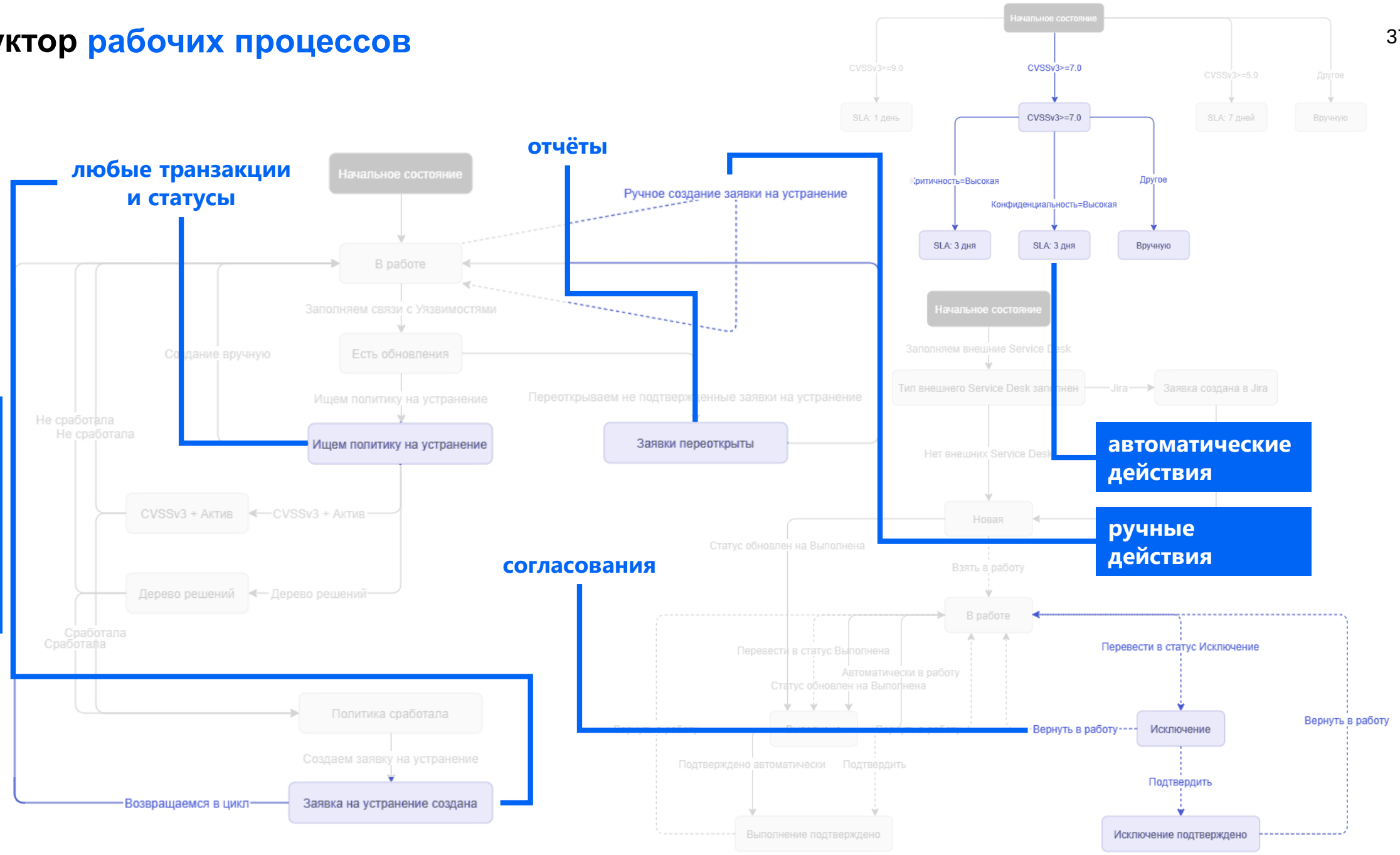
https://www.securitymentor.com/security-awareness-training-statistics-and-trends

Динамические плейбуки

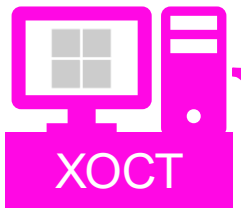


Не требуется заранее рассчитывать маршруты атаки и карты сетевой достижимости
Система реагирует в условиях изменчивости атак и инфраструктуры

Конструктор рабочих процессов



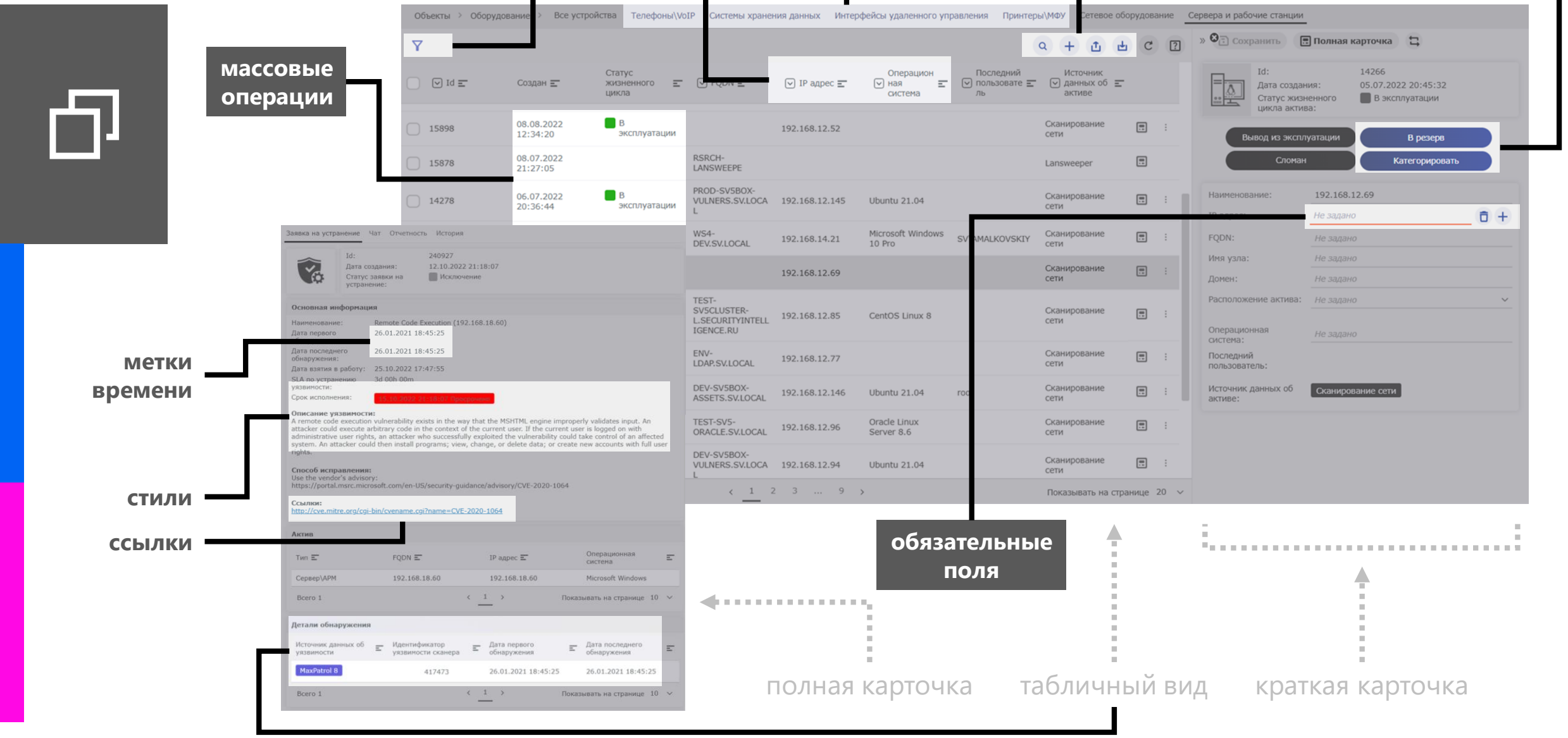
Объектно-ориентированное реагирование



- сетевая информация
  - Получить сетевые настройки
  - Получить соединения TCP/IP
  - Получить список текущих сетевых соединений
  - Получить информацию о настройках DNS
  - Получить DNS кэш
  - Получить список сетевых маршрутов
  - Получить список правил МЭ
  - Получить SMB общие ресурсы
- администрирование
  - Запустить произвольную команду
  - Перезагрузить хост
  - Выключить хост
  - Удалить папку
  - Удалить файл
  - Удалить ПО
  - Удалить ключ реестра
  - Восстановить ключ реестра
  - Запустить полное сканирование хоста AV
  - Запустить полное сканирование хоста AV
- общая информация
  - Получить список ПО
  - Получить список установленных обновлений
  - Получить информацию об установленных пакетах
  - Создать заявку на обновление ПО
  - Получить информацию о системе
  - Получить список локальных администраторов
  - Получить список sudo пользователей
  - Получить результаты сканирование
  - Создать заявку на устранение уязвимости
  - Получить связанные уязвимости из VM
  - Получить информацию о загрузке CPU/RAM
- процессы и службы
  - Остановить сервис
  - Запустить сервис
  - Получить список сервисов
  - Удалить сервис
  - Получить список сервисов
  - Завершить процесс
  - Удалить процесс из автозагрузки
  - Разблокировать процесс в AV
  - Заблокировать процесс в AV
  - Получить список процессов
- пользователи и сессии
  - Завершить сессии УЗ
  - Заблокировать локальную УЗ
  - Разблокировать локальную УЗ
  - Завершить все RDP сеансы
  - Получить информацию о текущих сессиях
  - Удалить УЗ из локальных администраторов

ГРАФ ВЗАИМОСВЯЗЕЙ И ВИЗУАЛИЗАЦИЯ

Конструктор объектов



Конструктор отчётов

различные форматы

хранение данных

редактор документа

Прогресс устранения:

Исполнитель:
Петров Петр Петрович

Дата взятия в работу:
15.06.2022 21:21:29

SLA по устранению уязвимости:
90d 00h 00m

Срок исполнения:

12.09.2022 15:57:02

Потрачено планового времени:
32%

Остаток времени до окончания срока исполнения:
61d 07h 27m

Данные по хосту:

' ия	FQDN	IP адрес	Операционная система
..ервер\APM	DEMO-DC	192.168.18.50	Microsoft Windows Server 2019 St

Общая информация:

Статус:
В работе

Срок исполнения:
12.09.2022 15:57:02

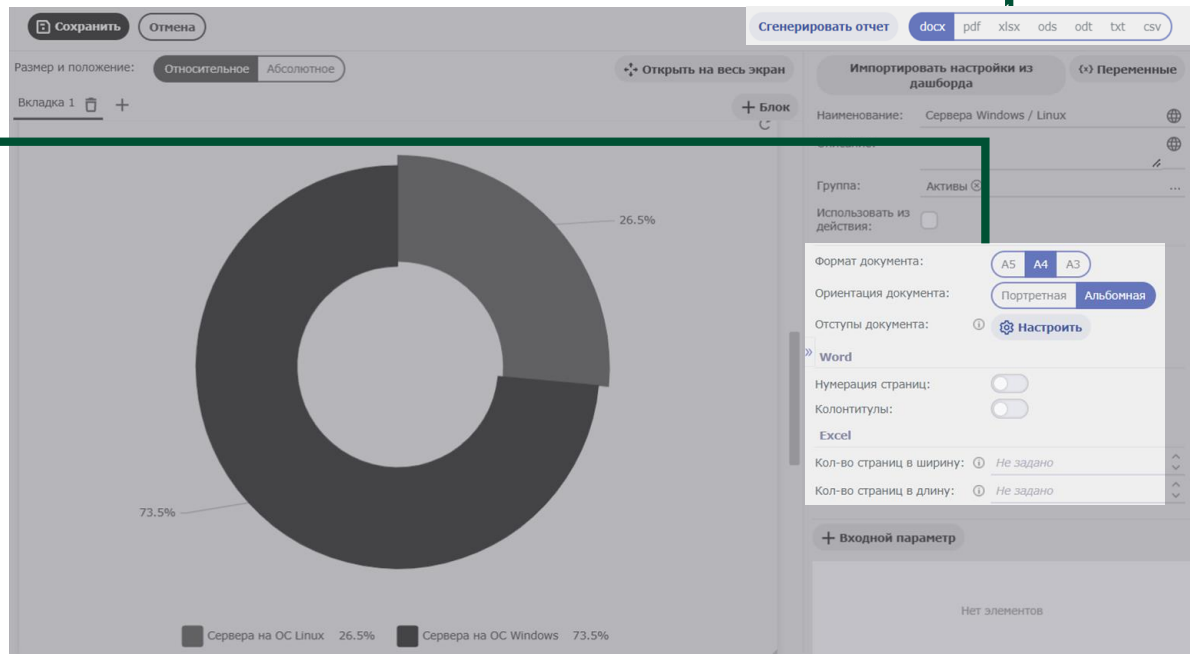
Описание уязвимости:
A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize user inputs. An un-authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected ADFS server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run scripts in the security context of the current user.

Способ исправления:
Use the vendor's advisory:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1055

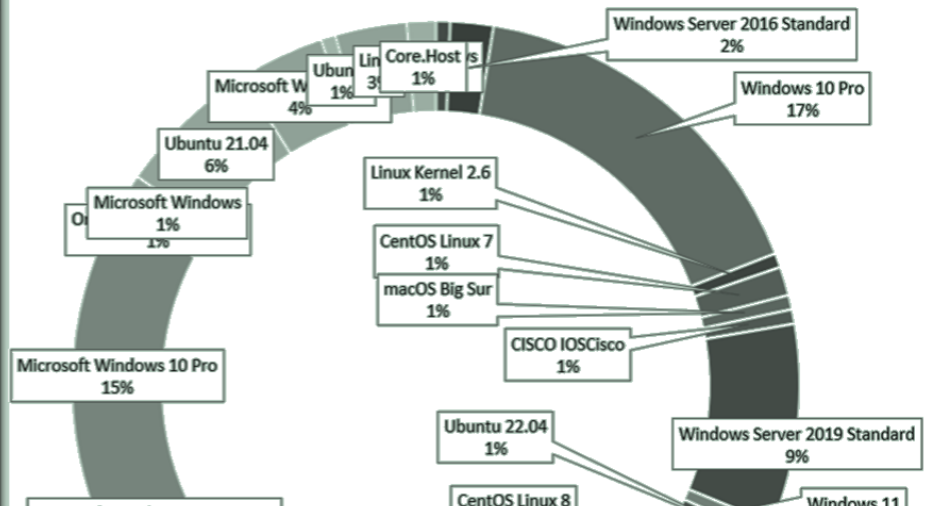
Прогресс устранения:

Исполнитель:
Петров Петр Петрович

Дата взятия в работу:
15.06.2022 21:21:29



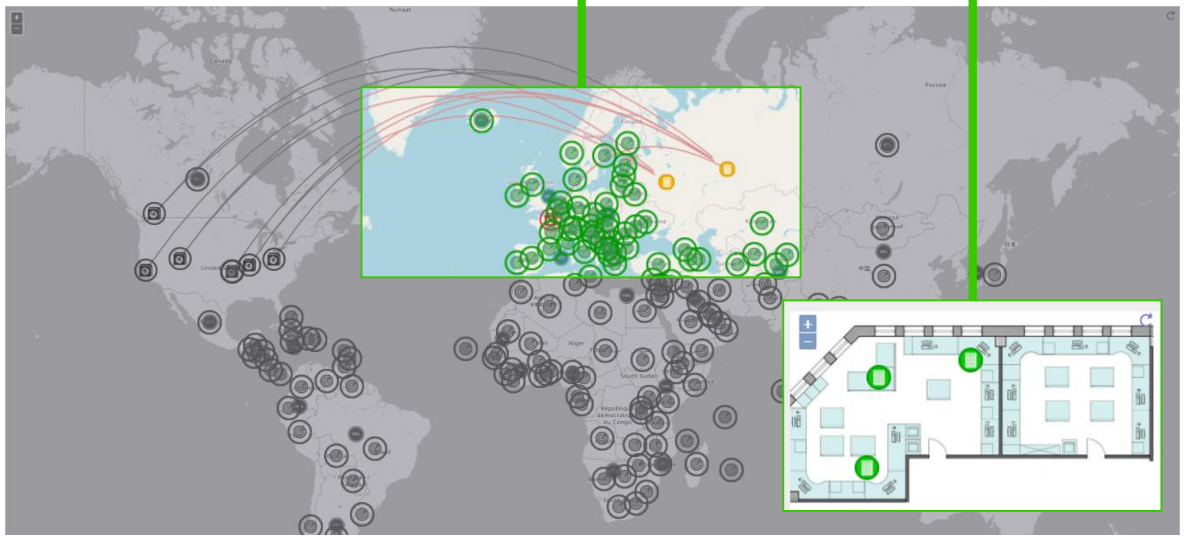
	A	B
1	Windows	1
2	Windows Server 2016 Standard	3
3	Windows 10 Pro	26
4	Linux Kernel 2.6	1
5	CentOS Linux 7	2
6	macOS Big Sur	1
7	CISCO IOSCisco	1
8	Windows Server 2019 Standard	14
9	Windows 11	1
10	Ubuntu 22.04	1
11	CentOS Linux 8	10
12	Microsoft Windows Server 2019	2
13	Microsoft Windows 11 Pro	1
14	Windows 10 x	1
15	Microsoft Windows Server 2016	10
16	Microsoft Windows Server 2019	17
17	Майкрософт Windows 10 Pro	8
18	Windows 10	1



Конструктор виджетов

карты и планы помещений

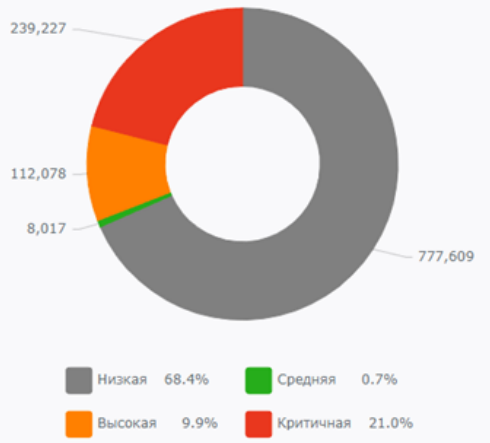
дашборды



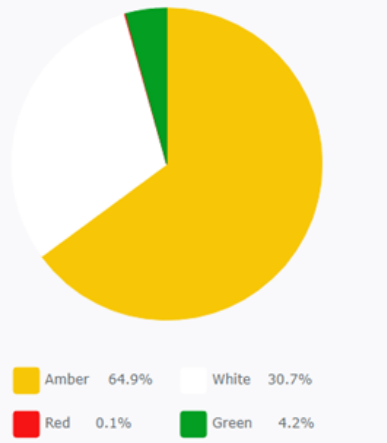
Топ-5 активных критичных инцидентов

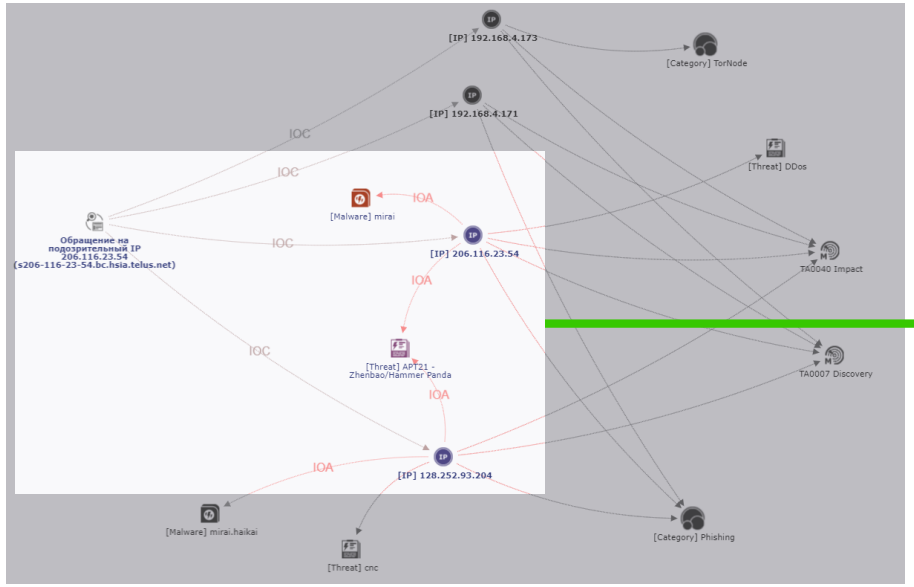
Наименование	Критичность	Статус
Отправка письма с подозрительного домена: acmetek.com	Критичная	Новый
Обращение на подозрительный домен cutt.ly	Высокая	Новый
Обращение на подозрительный домен conect-app.com	Высокая	Новый
Обращение с подозрительного IP 192.168.4.173 (ws4-dev.sv.local)	Высокая	Новый

Критичность индикаторов



TLP для индикаторов





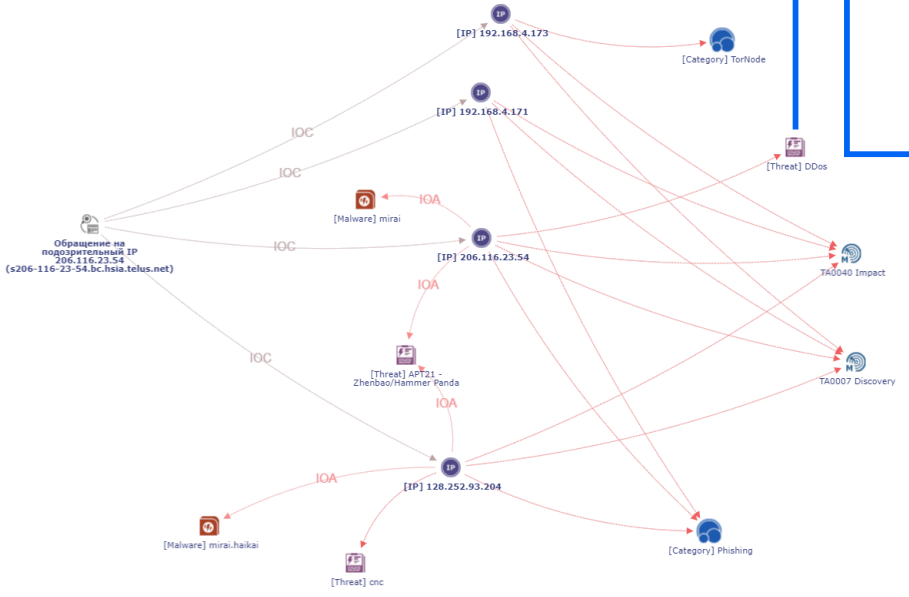
графы связей

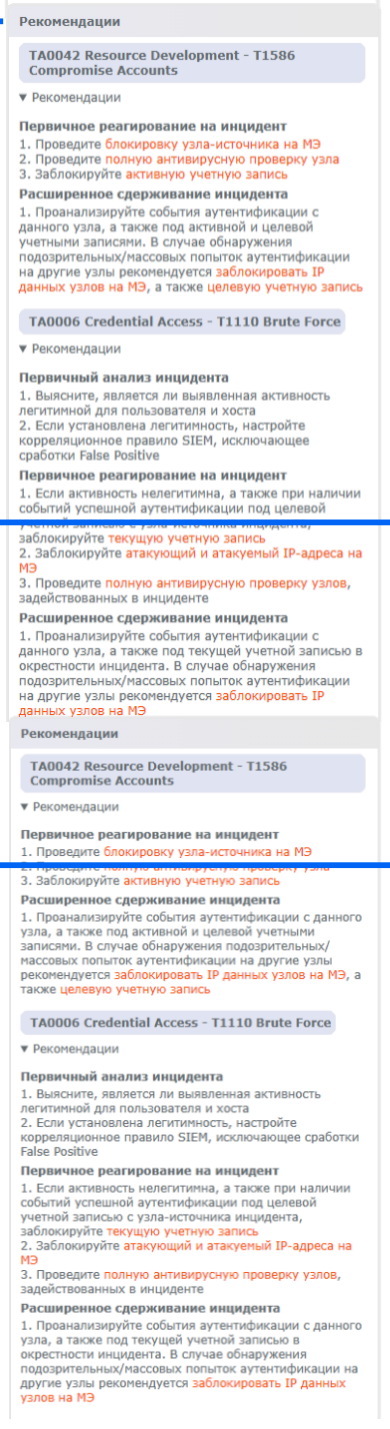
интерактивная аналитика и связанные графики

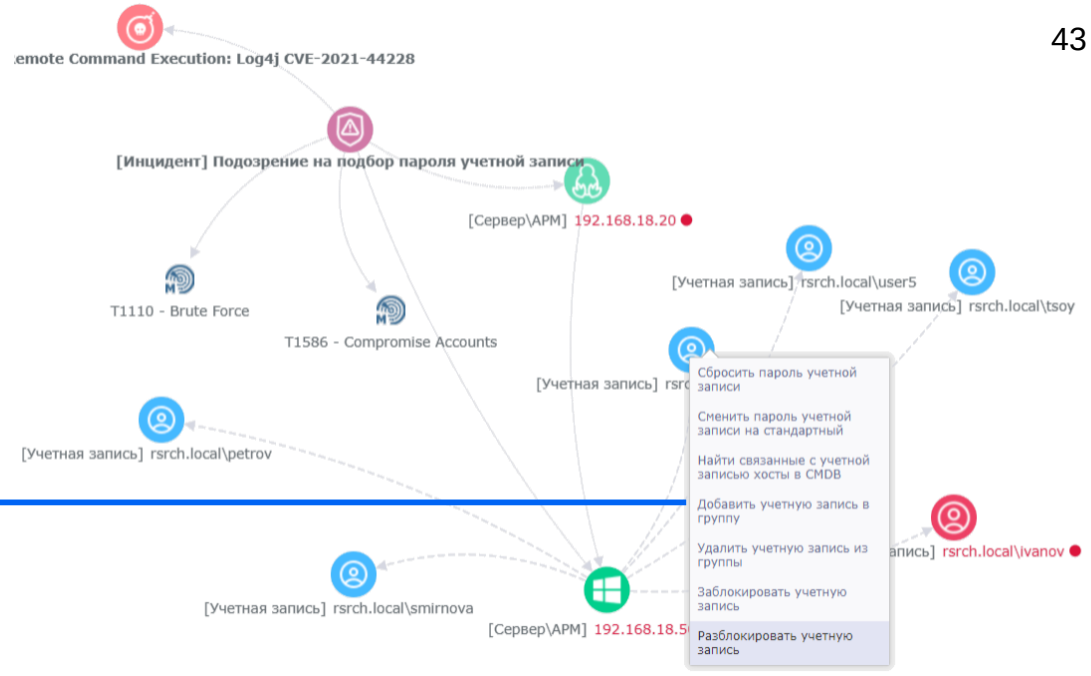
Количество активных индикаторов за период	Количество активных инцидентов за период
934676	7

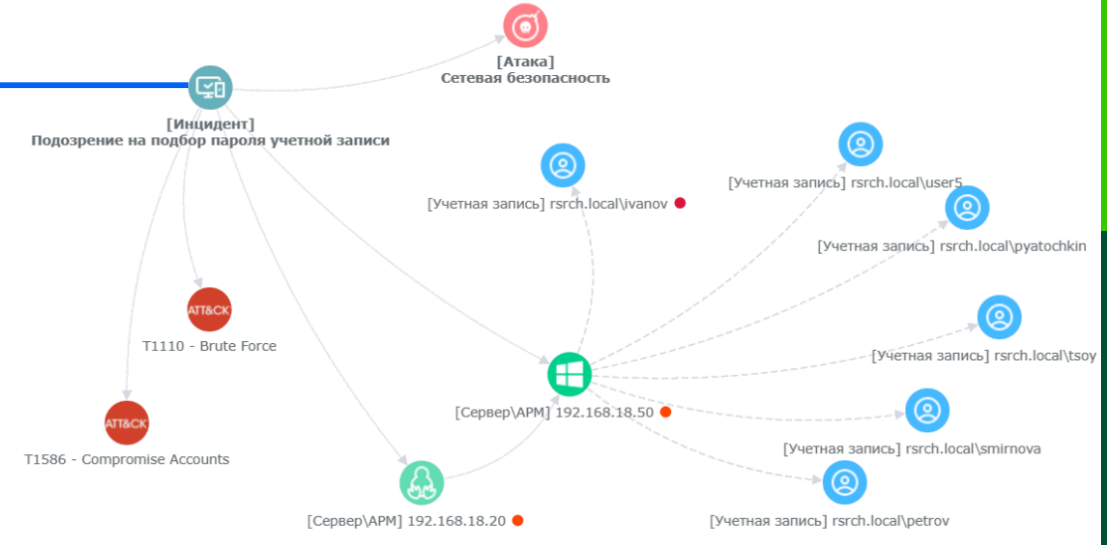
Граф связей

1. рекомендации экспертов
2. запуск действий из графа
3. интерактивные переходы
2. неочевидные связи



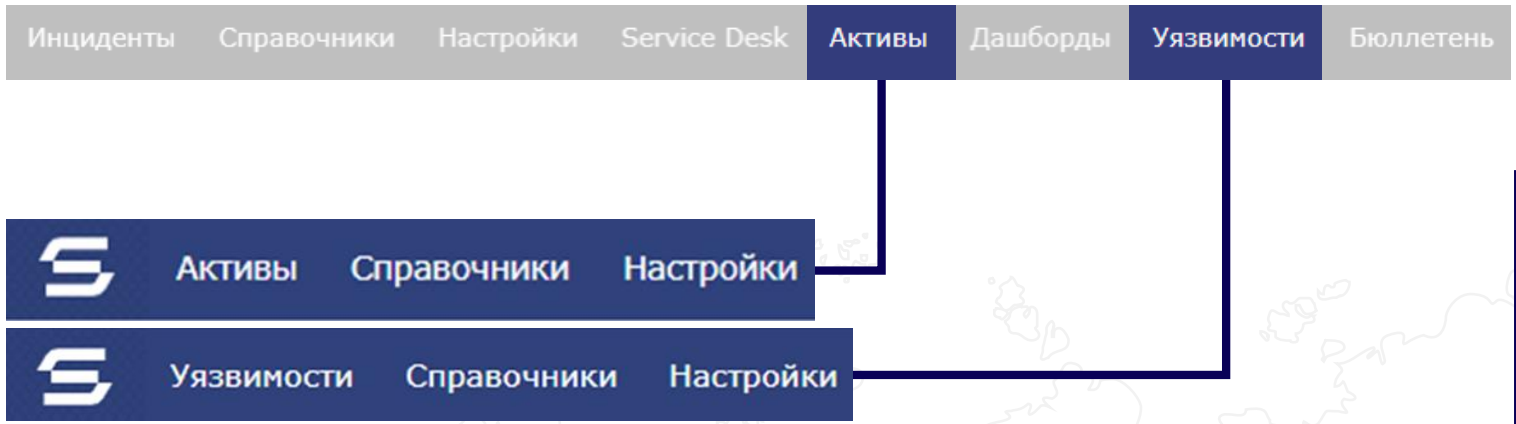


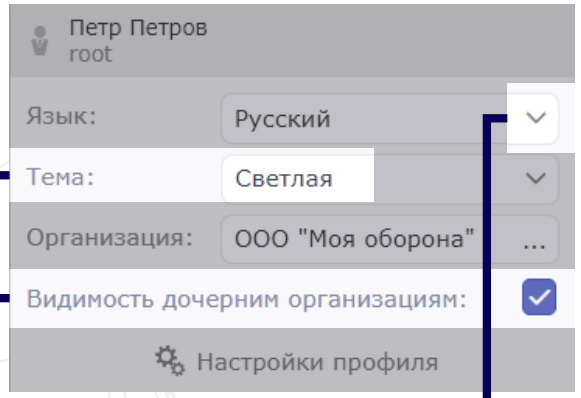




ЛУЧШИЕ ПРАКТИКИ

Конструктор ролей и меню

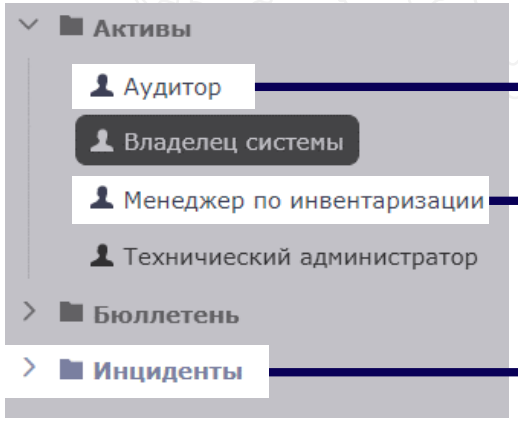




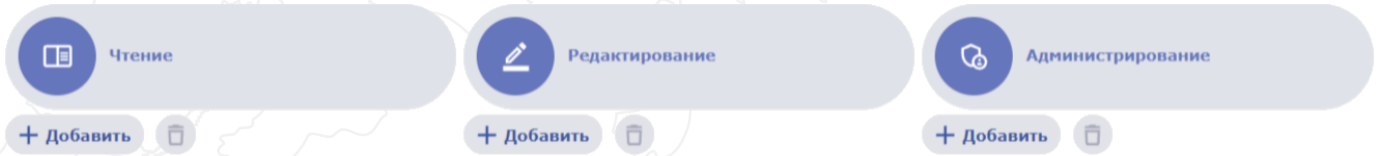
темы оформления

multitenancy

мультиязычность



персональная витрина



гранулярные настройки

ЛУЧШИЕ ПРАКТИКИ

1. NIST

Этапы обработки инцидентов (NIST)

+ экспертные рекомендации

ПОДГОТОВКА

Описание используемых инструментов и процессов:
внутренние и внешние сервисы, СЗИ, списки исключений, состав команд SOC

ОБОГАЩЕНИЕ

Сбор данных в окрестностях инцидента:
ретро-поиск, sigma-правила, аналитические сервисы

АНАЛИЗ

Классификация и анализ инцидента:
матрица MITRE ATT&CK, слепок хостов, цифровые свидетельства, Kill Chain

СДЕРЖИВАНИЕ

Блокирование и изоляция:
учётных записей, хостов, вредоносных URL/Email/доменов

РЕАГИРОВАНИЕ

Реагирование на основе ключевых объектов:
70+ преднастроенных действий для хостов, 20+ для УЗ, +другие объекты

ВОССТАНОВЛЕНИЕ

Возврат скомпрометированных объектов в исходное состояние:
разблокировка, проведение восстановления из бэкапа

LESSONS LEARNED

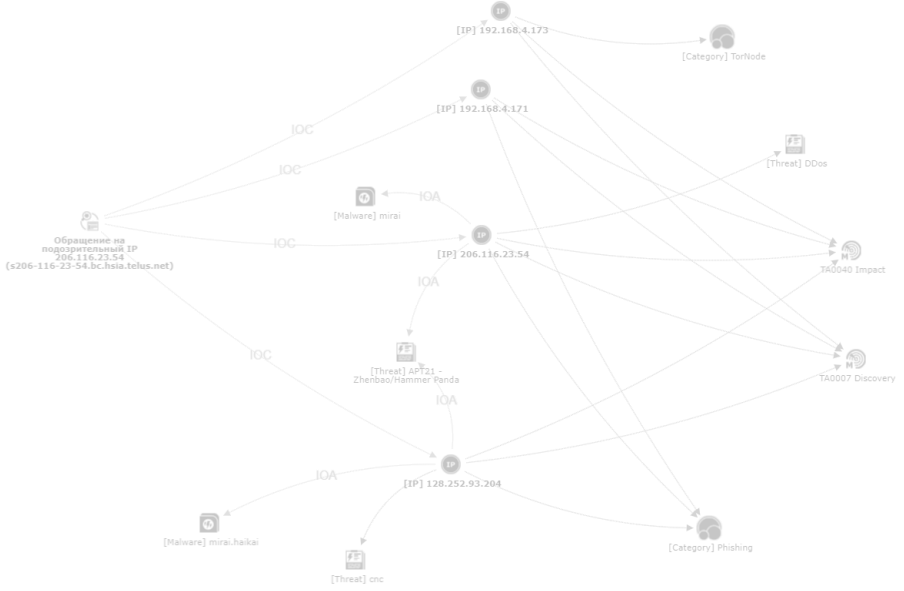
Выполнение работы над ошибками:
недопущения повторения аналогичных инцидентов

ЛУЧШИЕ ПРАКТИКИ

2. ЭКСПЕРТИЗА SV

Граф связей

1. рекомендации экспертов
2. запуск действий из графа
3. интерактивные переходы
2. неочевидные связи



Рекомендации

TA0042 Resource Development - T1586 Compromise Accounts

▾ Рекомендации

Первичное реагирование на инцидент
1. Проведите блокировку узла-источника на МЭ
2. Проведите полную антивирусную проверку узла
3. Заблокируйте активную учетную запись

Расширенное сдерживание инцидента
1. Проанализируйте события аутентификации с данного узла, а также под активной и целевой учетными записями. В случае обнаружения подозрительных/массовых попыток аутентификации на другие узлы рекомендуется заблокировать IP данных узлов на МЭ, а также целевую учетную запись

TA0006 Credential Access - T1110 Brute Force

▾ Рекомендации

Первичный анализ инцидента
1. Выясните, является ли выявленная активность легитимной для пользователя и хоста
2. Если установлена легитимность, настройте корреляционное правило SIEM, исключающее сработки False Positive

Первичное реагирование на инцидент
1. Если активность нелегитимна, а также при наличии событий успешной аутентификации под целевой учетной записью с узла-источника инцидента, заблокируйте текущую учетную запись
2. Заблокируйте атакующий и атакуемый IP-адреса на МЭ
3. Проведите полную антивирусную проверку узлов, задействованных в инциденте

Расширенное сдерживание инцидента
1. Проанализируйте события аутентификации с данного узла, а также под текущей учетной записью в окрестности инцидента. В случае обнаружения подозрительных/массовых попыток аутентификации на другие узлы рекомендуется заблокировать IP данных узлов на МЭ

Рекомендации

TA0042 Resource Development - T1586 Compromise Accounts

▾ Рекомендации

Первичное реагирование на инцидент
1. Проведите блокировку узла-источника на МЭ
2. Проведите полную антивирусную проверку узла
3. Заблокируйте активную учетную запись

Расширенное сдерживание инцидента
1. Проанализируйте события аутентификации с данного узла, а также под активной и целевой учетными записями. В случае обнаружения подозрительных/массовых попыток аутентификации на другие узлы рекомендуется заблокировать IP данных узлов на МЭ, а также целевую учетную запись

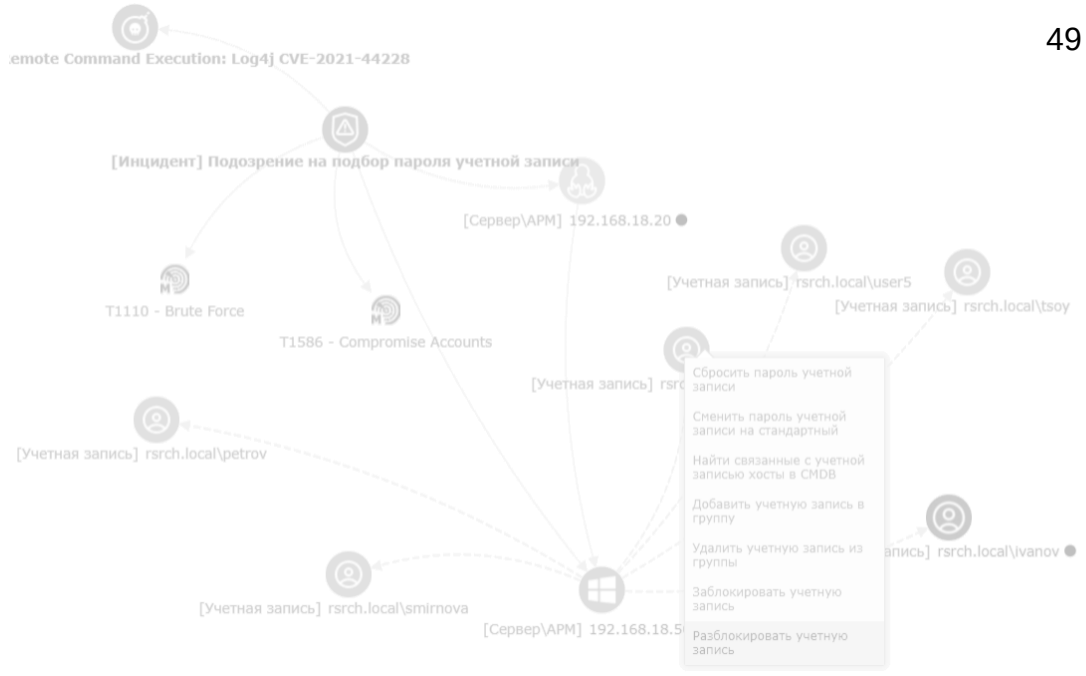
TA0006 Credential Access - T1110 Brute Force

▾ Рекомендации

Первичный анализ инцидента
1. Выясните, является ли выявленная активность легитимной для пользователя и хоста
2. Если установлена легитимность, настройте корреляционное правило SIEM, исключающее сработки False Positive

Первичное реагирование на инцидент
1. Если активность нелегитимна, а также при наличии событий успешной аутентификации под целевой учетной записью с узла-источника инцидента, заблокируйте текущую учетную запись
2. Заблокируйте атакующий и атакуемый IP-адреса на МЭ
3. Проведите полную антивирусную проверку узлов, задействованных в инциденте

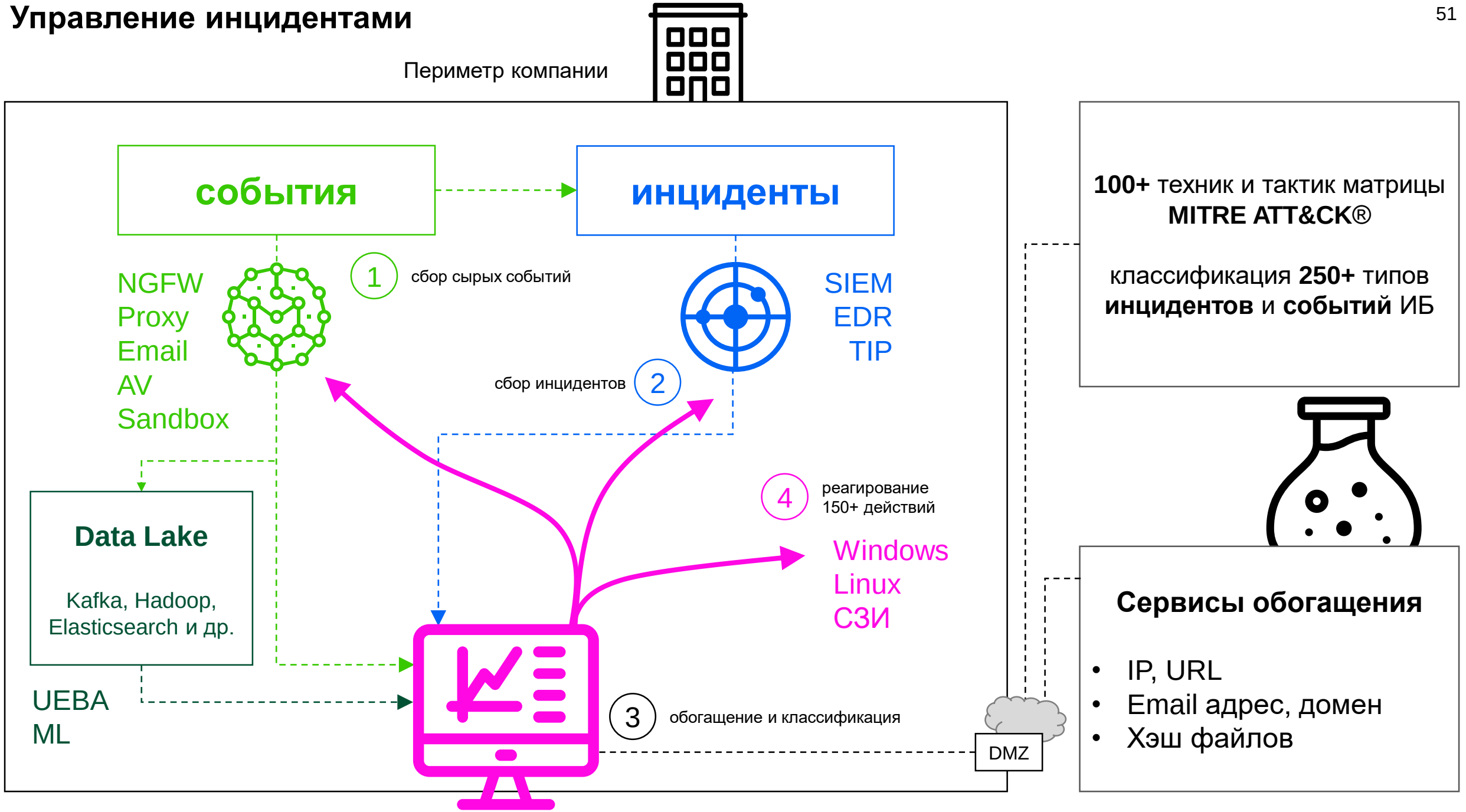
Расширенное сдерживание инцидента
1. Проанализируйте события аутентификации с данного узла, а также под текущей учетной записью в окрестности инцидента. В случае обнаружения подозрительных/массовых попыток аутентификации на другие узлы рекомендуется заблокировать IP данных узлов на МЭ



ЛУЧШИЕ ПРАКТИКИ

3. СЗИ

Управление инцидентами



ЛУЧШИЕ ПРАКТИКИ

4. ОБОГАЩЕНИЕ ИЗ 3RD PARTY

MITRE ATT&CK


MITRE ATT&CK:
User Execution
Command and Scripting Interpreter
Brute Force
Compromise Accounts
System Network Configuration Discovery
Network Service Discovery
System Network Connections Discovery
Account Manipulation
Exploitation of Remote Services
Inhibit System Recovery
Remote Access Software
Data Encrypted for Impact
Reconnaissance
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Phishing for Information
Search Closed Sources
Search Open Technical Databases
Search Open Website/Domain
Search Victim-Owned Websites
Resource Development
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities
Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
Command and Scripting Interpreter
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation
Persistence
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
External Remote Services
Hijack Execution Flow
Implant Internal Image
Modify Authentication Process
Office Application Startup
Pre-OS Boot
Scheduled Task/Job
Server Software
Privilege Escalation
Abuse Elevation Control Mechanism
Access Token Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain Policy Modification
Escape to Host
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts
Defense Evasion
Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Indicator Removal
Indirect Command Execution
Credential Access
Adversary-in-the-Middle
Brute Force
Credentials from Password
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
Modify Authentication Process
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Discovery
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Lateral Movement
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material
Collection
Adversary-in-the-Middle
Archive Collected Data
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Screen Capture
Video Capture
Command and Control
Application Layer Protocol
Communication Through Removable Media
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Remote Access Software
Traffic Signaling
Web Service
Exfiltration
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Transfer Data to Cloud Account
Impact
Account Access Removal
Data Destruction
Data Manipulation
Data Encrypted for Impact
Defacement
Disk Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Resource Hijacking
Network Denial of Service
Service Stop
System Shutdown/Reboot
Other
ВПО: Вирус не вылечен
Атака на сайт
Эксплуатация уязвимости
НСД
Нарушение политик

MITRE ATT&CK

техники

T1217 — Browser Bookmark Discovery

Adversaries may enumerate browser bookmarks to learn more about compromised hosts. Browser bookmarks may reveal personal information about users (ex: banking sites, interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.

Browser bookmarks may also highlight additional targets after an adversary has access to valid credentials, especially [Credentials In Files](https://attack.mitre.org/techniques/T1552/001) associated with logins cached by a browser.

Specific storage locations vary based on platform and/or application, but browser bookmarks are typically stored in local files/databases.

T1596 — Search Open Technical Databases

Adversaries may search freely available technical databases for information about victims that can be used during targeting. Information about victims may be available in online databases and repositories, such as registrations of domains/certificates as well as public collections of network data/artifacts gathered from traffic and/or scans.(Citation: WHOIS)(Citation: DNS Dumpster)(Citation: Circl Passive DNS)(Citation: Medium SSL Cert)(Citation: SSLShopper Lookup)(Citation: DigitalShadows CDN)(Citation: Shodan)

Adversaries may search in different open databases depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

подтехники

T1573.002 — Asymmetric Cryptography

Adversaries may employ a known asymmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Asymmetric cryptography, also known as public key cryptography, uses a keypair per party: one public that can be freely distributed, and one private. Due to how the keys are generated, the sender encrypts data with the receiver's public key and the receiver decrypts the data with their private key. This ensures that only the intended recipient can read the encrypted data. Common public key encryption algorithms include RSA and ElGamal.

For efficiency, many protocols (including SSL/TLS) use symmetric cryptography once a connection is established, but use asymmetric cryptography to establish or transmit a key. As such, these protocols are classified as [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002).

T1484.001 — Group Policy Modification

Adversaries may modify Group Policy Objects (GPOs) to subvert the intended discretionary access controls for a domain, usually with the intention of escalating privileges on the domain. Group policy allows for centralized management of user and computer settings in Active Directory (AD). GPOs are containers for group policy settings made up of files stored within a predicable network path <code>\\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\</code>.(Citation: TechNet Group Policy Basics)(Citation: ADSecurity GPO Persistence 2016)

Like other objects in AD, GPOs have access controls associated with them. By default all user accounts in the domain have permission to read GPOs. It is possible to delegate GPO access control permissions, e.g. write access, to specific users or groups in the domain.

Malicious GPO modifications can be used to implement many other malicious behaviors such as [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001), [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105), [Create Account](https://attack.mitre.org/techniques/T1136), [Service Execution](https://attack.mitre.org/techniques/T1569/002), and more.(Citation: ADSecurity GPO Persistence 2016)(Citation: Wald0 Guide to GPOs)(Citation: Harmj0y Abusing GPO Permissions)(Citation: Mandiant M Trends 2016)(Citation: Microsoft Hacking Team Breach) Since GPOs can control so many user and machine settings in the AD environment, there are a great number of potential attacks that can stem from this GPO abuse.(Citation: Wald0 Guide to GPOs)

For example, publicly available scripts such as <code>New-GPOImmediateTask</code> can be leveraged to automate the creation of a malicious [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053) by modifying GPO settings, in this case modifying <code><GPO_PATH>\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml</code>.(Citation: Wald0 Guide to GPOs)(Citation: Harmj0y Abusing GPO Permissions) In some cases an adversary might modify specific user rights like SeEnableDelegationPrivilege, set in <code><GPO_PATH>\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf</code>, to achieve a subtle AD backdoor with complete control of the domain because the user account under the adversary's control would then be able to modify GPOs.(Citation: Harmj0y SeEnableDelegationPrivilege Right)

Внешние сервисы обогащения

анализ подозрительных файлов на предмет выявления вирусов, червей, троянов и всевозможных ВПО

фильтр ISAPI, который экранирует и анализирует HTTP-запросы по мере их получения

получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем

Управление инцидентами в SOAR 2.0

250+ типов инцидентов

100+ техник MITRE

170+ коннекторов из коробки

140+ инструментов реагирования

200+ рекомендаций по реагированию

7 этапов проработки инцидента по NIST

ДИНАМИЧЕСКИЙ ПЛЕЙБУК

Типы событий
Объекты инцидента
Техники атаки

АВТОМАТИЧЕСКОЕ ПОСТРОЕНИЕ KILL CHAIN

ЭКСПЕРТНЫЕ РЕКОМЕНДАЦИИ

Сбор сведений
Сдерживание
Реагирование

ОБЪЕКТНО-ОРИЕНТИРОВАННОЕ РЕАГИРОВАНИЕ

Спасибо за внимание

sales@securityvision.ru

Интеллектуальная платформа информационной безопасности и ИТ

Security Vision

ДиалогНаука

securityvision.ru