



Автоматизация SecOps: IRP/SOAR

Екатеринбург, 22.02.2022



Что такое SOAR, IRP и SGRC?

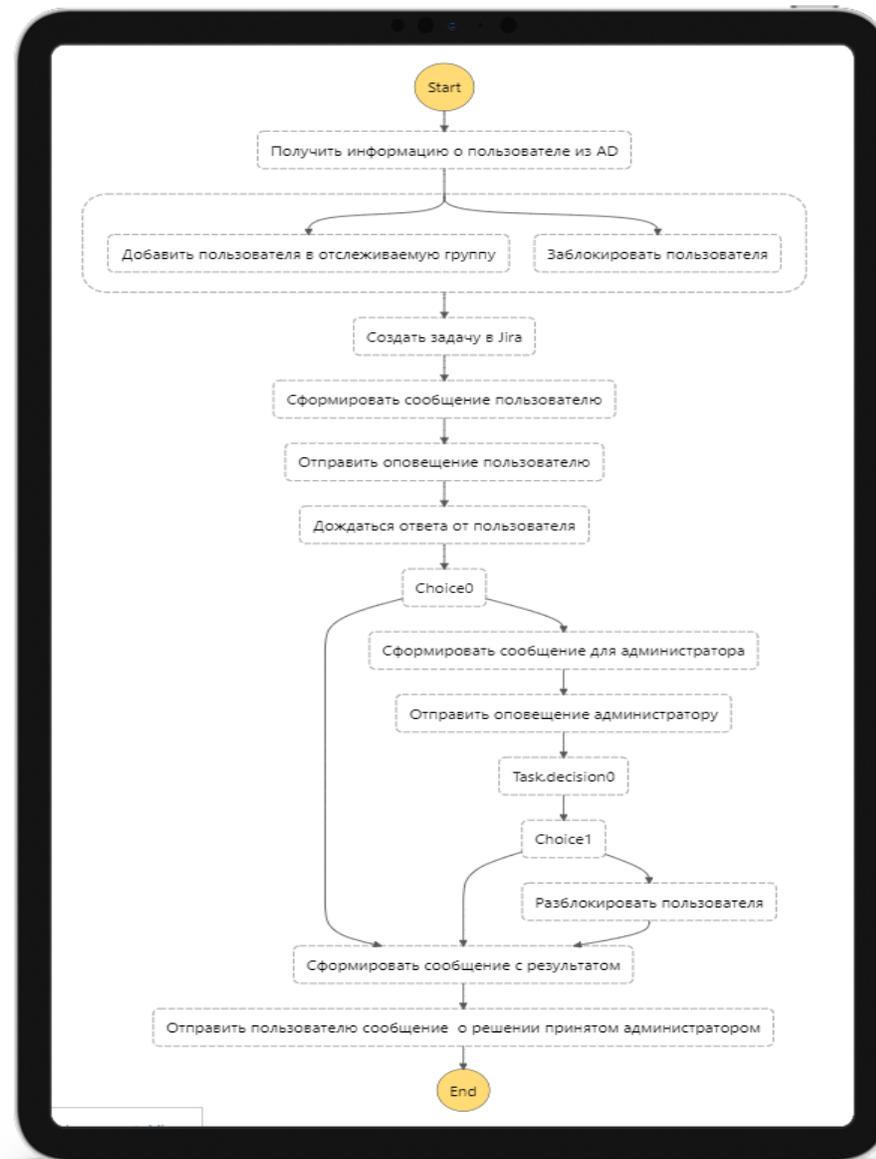


В чём выгода?

Действие	До SOAR	SOAR	Пример
Эскалация через SIEM, EDR или NGFW	5 мин	10 сек	Эскалация инцидента из SIEM – подозрительная активность на рабочей станции
Идентификация активов – CMDB/AD/IAM	5-10 мин	10 сек	Запросы в CMDB по рабочей станции и в Active Directory по пользователю
Проверка IOC в Threat Intelligence базах	5 мин	10 сек	В инциденте есть hash связанный с ВПО
Историческая корреляция инцидентов	10-20 мин	мгновенно	2 других инцидента за последний месяц имеют тот же hash и исходящий трафик
Ручное обогащение – активности с рабочих станций, внутренней сети, логи VPN, DNS записи, сетевая инфраструктура	30-55 мин	30 сек	Используем EDR решение чтобы получить всю информацию с рабочей станции. DNS с web проху для выявления сервера управления
Записи по инциденту – детальные записи и задачи на протяжении всего инцидента	неизвестно	мгновенно	ePlat4m автоматически сохраняет все выполненные задачи и действия по реагированию, все записи аналитиков хранятся на платформе
Эскалация через SIEM, EDR или NGFW	неизвестно	мгновенно	Все действия дотируются в ePlat4m и не могут быть модифицированы. При разборе инцидента руководство может анализировать отчеты
Отчет по статусу инцидента и визуализация для руководства	неизвестно	мгновенно	Встроенные консоли для руководства и внешние уведомления предоставляют всю информацию в режиме реального времени без лишней работы
Итого	85 минут	1 минута	

При обнаружении передачи учетной записи работника другому работнику:

- Пользователь автоматически добавляется в группу недобросовестных юзеров
- Блокируется учетная запись
- Пользователю направляется уведомление с запросом получения объяснительной
- После получения объяснительной информация передаётся администратору для принятия решения о разблокировке учетной записи





Пример реальной архитектуры

Сегменты ОКИИ

Сегмент SOC

ЛВС клиента SOC

CL DATAPK

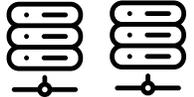


СОБЫТИЯ

Коллектор SIEM



Тенант SOAR



СОБЫТИЯ

Другие источники событий

Платформа оркестровки средств защиты Eplat4m SOAR



IRP/SOAR

Платформа реагирования на инциденты ИБ Eplat4m Orchestra



ДАННЫЕ ПО ИНЦИДЕНТАМ

ПОТЕНЦИАЛЬНЫЕ ИНЦИДЕНТЫ



SIEM

СОБЫТИЯ

СОБЫТИЯ

ОТПРАВКА ИНЦИДЕНТОВ В НКЦКИ

Адаптер интеграции с ГосСОПКА Eplat4m Orchestra

VPN туннель

VPN туннель

Коллектор SIEM



СОБЫТИЯ



Тенант SOAR

СОБЫТИЯ



Источники событий

ЛВС НКЦКИ

Головной центр ГосСОПКА



Блок управления активами (CMDB)	Выявление активов Обогащение информации об активах
Блок управления инцидентами	Сбор сведений об инцидентах из смежных систем (SIEM) Формирование карточек инцидентов Обеспечение полного цикла расследования и реагирования Выстраивание процессов управления инцидентами
Блок реагирования	Создание и использование сценариев реагирования (плейбуков) Создание и использование скриптов автоматизации Управление расписанием Управление секретами Витрина плейбуков
Блок визуализации и отчетности	Визуализация информации: дашборды, карты, схемы, диаграммы Формирование, отображение и экспорт отчетных материалов

Функции:

- Выявление активов
- Обогащение данных об установленном ПО, обновлениях, уязвимостях

Данные об активах собираются посредством коннекторов к:

- MaxPatrol
 - DATAPK
 - Efros CI
 - Microsoft SCCM
 - Kaspersky Security Center
- и другие коннекторы

Инвентаризация активов

USSC-SOC

Администрирование - Безопасность - Система - Поиск... 1043

Справочник

Объекты защиты

Наименование ОЗ	IP ОЗ	Тип	Описание ОЗ	Event Assignment group	Код стикера	Помещение	Стойка	Нужен мониторинг...
USSC-SOC								
(Продолжение на следующей странице)								
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(03) ПЛК	ПЛК			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(02) Сервер						<input type="checkbox"/> <input checked="" type="checkbox"/>
		(02) Сервер						<input type="checkbox"/> <input checked="" type="checkbox"/>
		(04) Сетевое оборудование	Коммутатор сети приложений АСУ ТП			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(04) Сетевое оборудование	Коммутатор сети приложений АСУ ТП			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(04) Сетевое оборудование	Коммутатор сети приложений АСУ ТП			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(04) Сетевое оборудование	Коммутатор сети приложений АСУ ТП			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(04) Сетевое оборудование	Коммутатор сети автоматизации АСУ ТП			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(04) Сетевое оборудование	Коммутатор сети автоматизации АСУ ТП			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(04) Сетевое оборудование	Коммутатор сети автоматизации АСУ ТП			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(04) Сетевое оборудование	Коммутатор сети автоматизации АСУ ТП			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(04) Сетевое оборудование	Коммутатор сети автоматизации АСУ ТП			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>
		(04) Сетевое оборудование	Коммутатор сети автоматизации АСУ ТП			ЭТУ. Пом. ПТК (207)		<input type="checkbox"/> <input checked="" type="checkbox"/>

Всего записей: 596 < 1 из 12 >

Инвентаризация активов

USSC-SOC Корпоративный центр мониторинга информационной безопасности объектов и систем информатизации

Администрирование | Безопасность | Система | Поиск... | 1043

Справочник | Карточка ОЗ

Объект защиты

Сетевое имя * Включение в мониторинг *

Назначение

Код ОКВИ Филиал Категория значимости Тип Код стикера

Event Assignment Group *

IP

MAC

Наименование ПТК

Модель

Версия ОС

Основное специальное ПО

Последствия нарушения работы

Расположение (помещение)

Расположение (стойка, шкаф)

Функции:

- Обогащение данных об инциденте путем привязки дополнительной информации об объектах защиты
- Обогащение путем агрегации связанных событий безопасности
- Сбор дополнительных данных из внешних сервисов

Сведения для обогащения собираются посредством коннекторов к:

- Whois
- VirusTotal
- Active Directory
- Elastic Search
- DATAPK
- Коннекторы САПУИБ

Карточка инцидента

USSC-SOC | Потенциальные инциденты ИБ | Карточка инцидента | Карточка инцидента

Инцидент ИБ № **1433782**

Взять в работу до: 12.01.2022 20:52:42 | Информировать Заказчика до: 12.01.2022 21:07:42 | Выдать рекомендации до: 15.01.2022 20:37:42 | Инцидент закрыт

Обнаружен новый ОЗ | 12.01.2022 20:52:42 | 12.01.2022 21:07:42 | 15.01.2022 20:37:42 | Приоритет: Высокий

Общая информация | Анализ (расследование) | Рекомендации | Повторяющиеся инциденты | История изменений | Комментарии Заказчика | Вопросы/Комментарии

Организация: [redacted]
 Филиал: [redacted]
 Что произошло: Обнаружен новый ОЗ
Описание правила: Зафиксировано событие о появлении неизвестного ОЗ. Данное событие может свидетельствовать как о санкционированном расширении системы, так и о появлении в сети нарушителя
Описание сигнатуры IDS: Подставится автоматически
[Обновить описание IDS]
Источник (Сторона1): Не найден | Назначение (Сторона2): Не найден
 Дата и время возникновения: 12.01.2022 20:37:42
 Приоритет: Высокий
 Описание инцидента: Обнаружен новый ОЗ ip: [redacted]
 Источник активности: --Пользователь-- | Является администратором? | --Произошла операция-- | Подставится автоматически
 Сетевое имя источника событий: [redacted]
 Тип источника событий: (13) DATAPK в составе СБОКИИ
 Описание источника событий: [redacted] DTRK01
 IP источника событий: [redacted]
 Наименование АСУ ТП (ГИС): [redacted] | Справочник классов/подклассов инцидента
 Класс инцидента: Мошенничество с использованием ИКТ (fraud)
 Подкласс инцидента: Злоупотребление при использовании ИР (ОКИИ) (unauthorized purposes)
box_id datark: [redacted]
Время отправки события: 12.01.2022 20:38:19 | Время получения события: 12.01.2022 20:38:20
Источник инцидента SOC: Подставится автоматически

Тип инцидента: Предполагаемый
Ответственный за инцидент: admin
Требуемые параметры обработки инцидента:
Время реакции (ТЗ), мин: 15
Время информирования (ТЗ), мин: 30
Время закрытия (ТЗ), мин: 4320
Дата и время реакции: 12.01.2022 20:52:41
Дата и время оповещения: 12.01.2022 20:55:01

Общая информация по инциденту | Просмотр аналогичных инцидентов | Инвентаризационная информация по ОЗ

[Сохранить] [Перевести в ложное срабатывание]

Обогащение инцидента данными из Security CMDb



Инцидент ИБ № 1433782

Взять в работу до:

Информировать Заказчика до:

Выдать рекомендации до:

Инцидент закрыт

Обнаружен новый ОЗ

12.01.2022 20:52:42

12.01.2022 21:07:42

15.01.2022 20:37:42

Приоритет

Высокий

Общая информация Анализ (расследование) Рекомендации Повторяющиеся инциденты История изменений Комментарии Заказчика Вопросы/Комментарии

Сетевое имя:	
Филиал:	
Тип:	(13) DATAPK в составе СБОКИИ
Назначение (краткое описание):	
IP-адрес:	
ОКИИ	
Event Assignment Group:	
Наименование ПТК (производитель ПТК, линейка оборудования):	СБОКИИ
Модель:	
MAC-адрес:	
Расположение (помещение):	
Расположение (стойка, шкаф):	

Категория значимости:	
Номер стикера:	
Версия ОС:	
Основное специальное ПО:	
Последствия нарушения работы:	

Общая информация по инциденту

Просмотр аналогичных инцидентов

Инвентаризационная информация по ОЗ

Поиск аналогичных инцидентов

USSC-SOC Корпоративный центр мониторинга информационной безопасности (центр и систем информатизации)

Администрирование - Безопасность - Система - Поиск #843

Потенциальные инциденты ИБ | Карточка инцидента | Карточка инцидента | Карточка инцидента

Инцидент ИБ № 1403554 Взять в работу до: 19.11.2021 15:29:12 Информировать Заказчика до: 19.11.2021 15:44:12 Выдать рекомендации до: 20.11.2021 15:14:12 Инцидент закрыт

События IDS с группировкой по источнику

Общая информация | **Анализ (расследование)** | Рекомендации | Повторяющиеся инциденты | История изменений | Комментарии Заказчика | Вопросы/Комментарии

Выберите критерии поиска аналогичных инцидентов

Наименование
 Пользователь
 ОЗ

Дата и время возникновения	Номер инцидента	Наименование	Пользователь	ОЗ	Статус
25.10.2021 19:36:11	1369698	События IDS с высоким приоритетом по группам	Не найден	q	Выбрать...
25.10.2021 19:36:11	1369699	События IDS по группам	Не найден		Повторка
25.10.2021 19:36:11	1369700	События IDS по группам	Не найден		Повторка
25.10.2021 19:36:11	1369701	События IDS с высоким приоритетом по группам	Не найден		Отключен
25.10.2021 19:36:11	1369702	События IDS по группам	Не найден		Отключен
25.10.2021 21:36:11	1370351	События IDS по группам	Не найден		Повторка
25.10.2021 21:36:11	1370352	События IDS по группам	Не найден		Повторка
25.10.2021 21:36:11	1370353	События IDS с группировкой по источнику	Не найден		Повторка
25.10.2021 21:36:11	1370354	События IDS с группировкой по источнику	Не найден		Повторка
25.10.2021 21:36:11	1370355	События IDS с группировкой по источнику	Не найден		Повторка

Всего записей: 1737 < 1 из 174 >

Оповестить Заказчика

Дополнительная информация (анализ)
Просмотр аналогичных инцидентов
Информация из DATAPK (включая исходные события)
Проверка IP
Просмотр оповещения

Агрегация связанных событий

USSC-SOC Корпоративный центр мониторинга информационной безопасности людей и систем информации

Администрирование - Безопасность - Система - Поиск... 1043

Потенциальные инциденты ИБ | Карточка инцидента | Карточка инцидента | Карточка инцидента

Инцидент ИБ № 1403554

Взять в работу до: 19.11.2021 15:29:12 | Информировать Заказчика до: 19.11.2021 15:44:12 | Выдать рекомендации до: 20.11.2021 15:14:12 | Инцидент закрыт

События IDS с группировкой по источнику

Приоритет: **Высокий**

Общая информация | Анализ (расследование) | Рекомендации | Повторяющиеся инциденты | История изменений | Комментарии Заказчика | Вопросы/Комментарии

Что произошло:

Обнаружено 1 срабатываний сигнатуры ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response (Client Init Vuln Server) с источником: [redacted]

Как произошло:

Корреляция Esper: Обнаружено 1 срабатываний сигнатуры ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response (Client Init Vuln Server) с источником [redacted]. События IDS с группировкой по источнику, count(id): 1, window(id): 29089d9e-9c5b-44cc-b527-ccfbc5dab253, host_id: 602aa4dd-7ca6-4344-6765-843590239942, box_id: 602aa4dd-7ca6-4344-6765-843590239942, description: ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response (Client Init Vuln Server); source_ip: [redacted] Link for search: 29089d9e-9c5b-44cc-b527-ccfbc5dab253; OZ: 602aa4dd-7ca6-4344-6765-843590239942; stage: новый; priority: Высокий; control: нет; confirmation: предполагаемый; response: нет; incident_type: неизвестно;

source_events

29089d9e-9c5b-44cc-b527-ccfbc5dab253

связанные события (datapk)

```
suricata[70]: {"timestamp": "2021-11-19T08:43:08.789159+0000", "flow_id": [redacted], "in_iface": "enp7s0", "event_type": "alert", "src_ip": [redacted], "dest_port": 49922, "proto": "TCP", "metadata": [{"flowbits": [{"ET.HB.Response.SI", "ET.HB.Response.CI"}], "alert": [{"action": "allowed", "gid": 1, "signature_id": 2018377, "rev": 4, "signature": "ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response (Client Init Vuln Server)", "category": "Potentially Bad Traffic", "severity": 2, "metadata": [{"updated_at": "[2014_04_09]", "former_category": "[CURRENT_EVENTS]", "created_at": "[2014_04_09]"}], "app_proto": "smb", "flow": [{"pkts_toserver": 6844024, "pkts_toclient": 3364407, "bytes_toserver": 10238409282, "bytes_toclient": 394478288, "start": "2021-11-19T08:26:00.070922+0000"}]}
```

Дополнительная информация (анализ)
Просмотр аналогичных инцидентов
Информация из DATAPK (включая исходные события)
Проверка IP
Просмотр оповещения

Оповестить Заказчика

Обогащение из внешних сервисов

USSC-SOC

Информационная безопасность
Система

Администрирование - Безопасность - Система - Поиск... 1043

Инцидент ИБ № 1403554

Взять в работу до: 19.11.2021 15:29:12
Информировать Заказчика до: 19.11.2021 15:44:12
Выдать рекомендации до: 20.11.2021 15:14:12
Инцидент закрыт

События IDS с группировкой по источнику

Приоритет: Высокий

Общая информация | Анализ (расследование) | Рекомендации | Повторяющиеся инциденты | История изменений | Комментарии Заказчика | Вопросы/Комментарии

IP для проверки: 173.82.163.43

WHOIS Белый IP

geo.city	geo.country	geo.ip_w	geo.loc	geo.org	geo.postal	geo.region	geo.timezone
Los Angeles	US	173.82.163.43	34.0522,-118.2437	AS35916 MULTACOM CORPORATION	90009	California	America/Los_Angeles

WHOIS Серый IP

geo.bogon	geo.ip
	173.82.163.43

VIRUS TOTAL

clean	error.code	error.message	malicious	malware	phishing	spam	suspicious	unrated
82								11

Оповестить Заказчика

Проверить IP whois | Проверить IP virus total

Дополнительная информация (анализ)
Просмотр аналогичных инцидентов
Информация из DATAPK (включая исходные события)
Проверка IP
Просмотр оповещений

Плейбук обогащения инцидента на VirusTotal

Обогащение через VT

Узлы | Подпроцессы

Активности ▾

- Открыть форму
- Решение пользователя
- Задача
- Статус
- Сообщение
- Инцидент/Событие
- Скрипт
- Выполнение по условию
- Параллельное выполнение
- Цикличное выполнение

События ▾

- Завершение
- Завершение с ошибкой
- Передача
- Ожидание

Настройка активности "Скрипт"

Общие настройки | Retry/Catch

Название узла *

Обогатить в VT

Исходный код *

```
grpc:127.0.0.1:5678:check_url_VT
```

Перейти к *

Вернуть в еплат

Комментарий

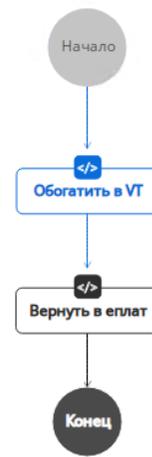
Комментарий для отображения на схеме

Значение Путь JsonPath

Таймаут, сек: 60 | Сигнал, сек: 10

> Обработка ввода ?

> Обработка вывода ?



```
graph TD; A((Начало)) --> B[Обогатить в VT]; B --> C[Вернуть в еплат]; C --> D((Конец));
```

Скрипты

Q vt × [Скрипты](#) Плейбуки

Создать скрипт



Наименование	Комментарий	Список тегов	Версия	Группа	Тип рантайма
check_url_VT		Добавьте теги		-	python3.8
VT_back-to_eplat		Добавьте теги		-	python3.8

< 1 2 >

1-15 из 30 записей



Пример скрипта сбора данных VirusTotal

```
1 import json
2 import sys
3 import requests
4 import time
5
6
7 def main(input_json):
8     # url = '187.1.188.158'
9     url = input_json['ip']
10    api_key_virustotal = input_json.get('api_key_virustotal_virustotal',
11
12    if 'api_key_virustotal' in input_json:
13        del input_json['api_key_virustotal']
14
15    result_counter = {}
16
17    data = {'url': url}
18    api_url = 'https://www.virustotal.com/api/v3/urls'
19    headers = {'x-apikey': api_key_virustotal}
20    response_query = requests.post(api_url, headers=headers, data=data)
21    if response_query.status_code != 200:
22        print(json.dumps(**response_query.json(), **input_json))
23        return
24
25    while True:
26        (variable) headers: dict[str, Any] om/api/v3/analyses/{response_query.json()["data"]["id"]}
27        headers = {'x-apikey': api_key_virustotal}
28        response = requests.get(api_url, headers=headers)
29        if response.status_code == 200:
30            response = response.json()
31            if response['data']['attributes']['status'] == "completed":
32                for i in response['data']['attributes']['results']:
33                    if response['data']['attributes']['results'][i]['result'] in result_counter:
34                        result_counter[response['data']['attributes']['results'][i]['result']] += 1
35                    else:
36                        result_counter[response['data']['attributes']['results'][i]['result']] = 1
37                break
38            else:
39                time.sleep(2)
40        else:
41            time.sleep(2)
42
43    print(json.dumps(**result_counter, **input_json))
44
45 if __name__ == '__main__':
46     input_str = sys.argv[1]
47     input_json = json.loads(input_str)
48     main(input_json)
```

Обогащение инцидента справочной информацией

USSC-SOC

Администрирование - Безопасность - Системы - Поиск

1943

Справочник типов входа

Код	Описание	Подробное описание	
Q	Q	Q	
3	Сетевой. Пользователь по сети подключился к этому компьютеру и авторизовался на нем	Обычно такое событие появляется при подключении по сети к разделяемым (shared) ресурсам - папкам, файлам, принтерам. Подключение с типом входа = 3 может быть установлено и с локального компьютера	✗
4	Планетный	Этот тип входа используется при выполнении планетных заданий без непосредственного участия пользователя. Например, когда запускается задание планировщика. Когда используется планировщик Windows и приходит время запустить задание, Windows может создать новую пользовательскую сессию, чтобы выполнить задание от имени пользователя. При этом регистрируется событие (4648, 4624\4625). Если запланированное задание сконфигурировано так, что не должно запускаться без интерактивного сеанса пользователя, то новая сессия не создается и события не регистрируются	✗
2	Интерактивный. Пользователь непосредственно вошел на этот компьютер	Событие с типом входа = 2 записывается в журнал безопасности когда пользователь вошел или попытается войти в систему непосредственно локально, используя клавиатуру и ввод или пользователь и пароль в окне входа в систему. Событие с типом входа = 2 возникает при использовании как локальной так и доменной учетной записи. Если пользователь входит с доменной учетной записью, событие с типом входа = 2 появится если пользователь будет действительно аутентифицирован в домене (контроллером домена) В случае, если контроллер домена недоступен, но пользователь предоставил валидный пароль, зашифрованный в локальном компьютере, Windows поставит тип входа = 11	✗
0	System		✗
5	Служба Service Control Manager запустил службу (service)	Такое событие возникает когда Windows запускает службу от имени пользователя. Windows создает новую сессию для запуска такой службы. Так происходит только, если служба использует обычную учетную запись. Если используется специальная учетная запись, например, "Local System", "NT AUTHORITY\LocalService" или "NT AUTHORITY\NetworkService", то Windows не создает новых сессий. Когда сервис остановится, новая сессия будет закрыта и будет зарегистрировано событие выхода (4634). Имейте в виду, что описание события не содержит информации о запуске сервиса или процессе. Когда регистрируется событие Аудит отказа (4625) с типом входа = 5, это обычно означает что пароль учетной записи для запуска сервиса был изменен пользователем и следует обновить параметры учетной записи для запуска службы в настройках того приложения, чья служба запускается	✗
7	разблокирование. Рабочая станция разблокирована	Событие с типом входа = 7 происходит когда пользователь разблокирует (или пытается это сделать) ранее заблокированный компьютер. Имейте в виду, что когда пользователь разблокирует компьютер, Windows создает новую сессию (или даже 2 сессии в зависимости от полномочий пользователя) и сразу же их завершает, после прохождения аутентификации (событие 4634). При переключении между учетными записями уже осуществившим вход в систему с помощью функции быстрого переключения учетной записи (Fast User Switching), Windows создает событие 4624 с типом входа = 2 (интерактивный). Когда регистрируется событие отказа 4625 с типом входа = 7, это обычно означает что вы ошиблись при вводе пароля или кто-то пытался подобрать пароль, чтобы разблокировать компьютер	✗
8	NetworkCredential. Пользователь вошел на данный компьютер через сеть. Пароль пользователя передан в пакет проверки подлинности в его нешифрованной форме. Встроенная проверка подлинности использует все зашифрованные учетные записи перед их отправкой через сеть. Учетные данные не передаются через сеть открытым текстом	Это событие возникает, если пароль пользователя был получен по сети открытым текстом. Такое событие может произойти когда пользователь входит в IIS (Internet Information Services) с базовым методом аутентификации. Передача паролей в формате открытого текста опасна потому что пароли могут быть перехвачены и расшифрованы. Если нет возможности использовать более надежную аутентификацию, то стоит хотя бы зашифровать сетевое соединение (используя зашифрованные протоколы типа SSL/TLS, создав зашифрованную виртуальную частную сеть и т.д.)	✗
9	NetUserEnumerate. Посетитель клонировал свой текущий маркер и указал новые учетные записи для исходящих соединений. Новый сеанс входа в систему имеет ту же самую локальную тождественность, но использует отличающиеся учетные записи для сетевых соединений	Это событие регистрируется, когда используется команда "Запустить от имени" вместе с опцией "/netonly". Это нужно для запуска программы с дополнительными привилегиями для сетевых компьютеров. Например, нужно запустить Event Log Explorer и дать ему дополнительные права для некоторого компьютера или домена (это может показаться если вы запустите определенный компьютер в качестве сервера описаний событий, но ваши текущие права не достаточно для доступа к администраторским ресурсам этого сервера). В таком случае вы можете запустить Event Log Explorer через команду строку со следующими параметрами: <code>cmd.exe /netonly /user:SERVER\Administrator "c:\program files\event log explorer\expl.exe" /de:SERVER - имя сервера, с которого предполагается брать описания событий (также потребуется настроить имя сервера в программе). При запуске программы, Windows потребует ввести пароль пользователя Administrator для сервера SERVER. Event Log Explorer запустится даже если вы введете неправильный пароль. При этом будет создана новая пользовательская сессия с учетными данными текущего пользователя и в журнал будет записано событие 4624 с типом входа = 9. А событие выхода из системы для этой сессии будет записано после того, как приложение будет завершено. Также, в журнале безопасности сервера SERVER будут записаны события 4624 или 4625 с типом входа = 3, но только в момент обращения нашего приложения к разделяемым ресурсам сервера SERVER. То есть, когда Event Log Explorer попытается открыть файл описаний событий на сервере SERVER.</code>	✗
10	RemoteInteractive. Пользователь выполнил удаленный вход на этот компьютер, используя Terminal Services или Remote Desktop	Этот тип входа похож на 2 (интерактивный), но пользователь подключается к компьютеру с удаленного компьютера через RDP, используя Удаленный рабочий стол (Remote Desktop), сервисы терминального доступа (Terminal Services) или удаленный помощник (Remote Assistance)	✗
11	CacheInteractive. Пользователь вошел на этот компьютер с сетевыми учетными данными, которые хранились локально на компьютере. Контроллер домена не использовался для проверки учетных данных	Когда пользователь входит в домен, Windows кширует учетные данные пользователя локально, так что он позже может войти даже если контроллер домена будет недоступен. По умолчанию, Windows кширует 10-25 последних использованных доменных учетных записей (это зависит от версии Windows). Когда пользователь пытается войти с доменной учетной записью, а контроллер домена не доступен, Windows проверяет учетные данные по сохраненным хэшам и регистрирует события 4624 или 4625 с типом входа = 11. Пользователь вошел в систему на этом компьютере с сетевыми учетными данными, которые хранились локально на компьютере. Не удалось связаться с контроллером домена для проверки учетных данных	✗

1 из 2

Обогащение инцидента классами/подклассами

USSC-SOC

Администрирование • Безопасность • Система

Справочник связей класс-подкласс-правило

Перечень связей правил корреляций с классами и подклассами

Наименование правила	Класс инцидента	Подкласс инцидента
Обнаружен новый поток с интерфейсом из внешней сети	Мошенничество с использованием ИКТ (fraud), Распространение вредоносного программного обеспечения (malware distribution)	Злоупотребление при использовании IP (ОКИИ) (unauthorized purposes), Использование контролируемого IP (ОКИИ) для распространения ВПО (malware command and control)
Несанкционированное изменение системного времени	Нарушение безопасности информации (information content security)	Несанкционированное изменение информации, обрабатываемой в контролируемом IP (ОКИИ) (unauthorised modification)
Включение алгоритма шифрования слабой стойкости или использование техники Kerberoast	Несанкционированный доступ в систему (intrusion)	Компрометация учетной записи в контролируемом IP (ОКИИ) (account compromise)
Обнаружение неизвестных потоков данных за интервал времени	Распространение вредоносного программного обеспечения (malware distribution), Нарушение или замедление работы контролируемого информационного ресурса (availability), Распространение информации с неприемлемым содержанием (abusive content)	Использование контролируемого IP (ОКИИ) для распространения ВПО (malware command and control), Компьютерная атака типа "отказ в обслуживании", направленная на контролируемый IP (ОКИИ) (dos), Распределенная компьютерная атака типа "отказ в обслуживании", направленная на контролируемый IP (ОКИИ) (ddos), Рассылка спам-сообщений с контролируемого IP (ОКИИ) (spam)
Новое удаленное подключение к коммутатору Eltex по SSH	Попытки несанкционированного доступа в систему или к информации (intrusion attempt)	Попытки авторизации в контролируемом IP (ОКИИ) (login attempt)
Сброс пароля пользователя	Нарушение безопасности информации (information content security)	Несанкционированное изменение информации, обрабатываемой в контролируемом IP (ОКИИ) (unauthorised modification)
События IDS с высоким приоритетом	Сбор сведений с использованием ИКТ (information gathering)	Сканирование информационного ресурса (ОКИИ) (scanning)
Использование планировщика задач для gansoftware	Заражение вредоносным программным обеспечением (malware)	Внедрение в контролируемый IP (ОКИИ) модулей ВПО (malware infection)
SAM dump в AppData	Несанкционированный доступ в систему (intrusion)	Компрометация учетной записи в контролируемом IP (ОКИИ) (account compromise)
Ошибка сбора данных с ОЗ	Нарушение или замедление работы контролируемого информационного ресурса (availability)	Непреднамеренное (без злого умысла) отключение IP (ОКИИ) (outage), Несанкционированный вывод IP (ОКИИ) из строя (sabotage)

5 10 20 50

Всего записей: 152 < 1 из 16 >

Функции:

- Создание и использование сценариев реагирования (плейбуков)
- Создание и использование скриптов автоматизации
- Управление расписанием
- Управление секретами
- Витрина плейбуков

Реагирование осуществляется при помощи:

- Языка описания плейбуков Amazon States Language
- Скриптов на языках программирования Python, PowerShell, Bash

Пример плейбука реагирования

100% 90°

Получение рекомендац...

+ [icon] ▶

Узлы Подпроцессы

Активности ▾

- Открыть форму
- Решение пользователя
- Задача
- Статус
- Сообщение
- Инцидент/Событие
- Скрипт
- Выполнение по условию
- Параллельное выполнение
- Цикличное выполнение

События ▾

- Завершение
- Завершение с ошибкой
- Передача
- Ожидание



Настройка активности "Скрипт"

Общие настройки Retry/Catch

Название узла *

Отправить в еплат

Исходный код *

grpc:127.0.0.1:5678:get_recomends_from_confluence-

Перейти к *

Конец

Комментарий

Комментарий для отображения на схеме

Значение Путь JsonPath

Таймаут, сек

60

Сигнал, сек

10

> Обработка ввода ?

> Обработка вывода ?

Пример выдачи рекомендаций по реагированию

Автоматический подбо... ⋮ ☰

Узлы Подпроцессы

Активности ▾

- Открыть форму
- Решение пользователя
- Задача
- Статус
- Сообщение
- Инцидент/Событие
- Скрипт
- Выполнение по условию
- Параллельное выполнение
- Цикличное выполнение

События ▾

- Завершение
- Завершение с ошибкой
- Передача
- Ожидание

Начало

Генерация рекомендаций

Конец

Настройка активности "Скрипт"

Общие настройки Retry/Catch

Название узла *

Генерация рекомендаций

Исходный код *

```
grpc:127.0.0.1:5678:auto_recomends-generate_recom
```

Перейти к *

Конец

Комментарий

Комментарий для отображения на схеме

Значение Путь JsonPath

Таймаут, сек 60

Сигнал, сек 10

> Обработка ввода ?

> Обработка вывода ?

Рекомендации сформированы

USSC-SOC Информационный центр мониторинга информационной безопасности средств и систем информатизации

Администрирование - Безопасность - Система - Поиск... 1043

Потенциальные инциденты ИБ | Карточка инцидента

Инцидент ИБ № 1435191 Взять в работу до: 14.01.2022 23:15:08 Информировать Заказчика до: 14.01.2022 23:30:08 Выдать рекомендации до: 17.01.2022 23:00:08 Инцидент закрыт: Приоритет: Высокий

Общая информация | Анализ (расследование) | **Рекомендации** | Повторяющиеся инциденты | История изменений | Комментарии Заказчика | Вопросы/Комментарии

Итоги расследования инцидента (в таком виде будет отправлено на почту Заказчику).

1. Определить легитимность нового объекта защиты:
1.1 В случае нелегитимности отключить сетевой узел и провести расследование по возможному негативному влиянию на ОКИИ.
1.2. Внести легитимный объект защиты в каталог объектов защиты DATAPK, передать подробную информацию по объекту защиты в SOC

Итоги расследования инцидента (поле для редактирования) *

1. Определить легитимность нового объекта защиты:

1.1 В случае нелегитимности отключить сетевой узел и провести расследование по возможному негативному влиянию на ОКИИ.

1.2. Внести легитимный объект защиты в каталог объектов защиты DATAPK, передать подробную информацию по объекту защиты в SOC

Дата и время возникновения: 14.01.2022 23:00:08

Класс инцидента: Мошенничество с использо... x

Подкласс инцидента *: Злоупотребление при испо... x

Объект защиты: DTRK01

Ответственный: admin

2. Направить рекомендации Заказчику

Вернуть в работу

Дата и время рекомендации: 14.01.2022 23:27:22

Не является инцидентом

Информирование НЕ произведено

Рекомендации направлены

Обновить рекомендации

Выгрузить отчет по инциденту

Требуется ли обратная связь со стороны Заказчика?
Комментарии не требуются x

< Мониторинг плейбуков



Активные Архив

🔍 Поиск по плейбукам ✕

Наименование ▾	Версия ▾	Состояние ▾	Запущен ▾	Остановлен / Завершен ▾
key_error		Failed	30.12.2021 14:28:16	30.12.2021 14:28:16
playbook_timeout		Succeeded	14.12.2021 13:11:15	14.12.2021 13:11:15
newPlaybook		Failed	14.12.2021 16:35:57	14.12.2021 16:35:57
Вредоносная активность - оба не локальные		Failed	14.12.2021 16:16:15	14.12.2021 16:16:15
playbook_timeout		Succeeded	11.01.2022 14:25:48	11.01.2022 14:25:48
CallMicroservice		Failed	20.12.2021 15:46:39	20.12.2021 15:46:39
Вредоносная активность - оба не локальные		Failed	14.12.2021 16:16:20	14.12.2021 16:16:20
import_error		Failed	30.12.2021 14:28:36	30.12.2021 14:28:36
Вредоносная активность - оба не локальные		Failed	14.12.2021 16:16:20	14.12.2021 16:16:20
ыфвыфв		Succeeded	17.01.2022 14:29:49	17.01.2022 14:29:49
playbook_with_nested2	4.2	Failed	20.12.2021 15:57:05	20.12.2021 15:57:05
newPlaybook		Failed	14.12.2021 16:18:05	14.12.2021 16:18:05
playbook_timeout		Succeeded	11.01.2022 14:25:48	11.01.2022 14:25:48
CallMicroservice		Failed	17.01.2022 14:24:58	17.01.2022 14:24:58
CallbackPattern		Failed	10.01.2022 11:57:30	10.01.2022 11:57:30

< 1 2 3 4 5 ... 25 > 15 записей на странице ▾

1-15 из 365 записей

< Мониторинг задач



06 Feb - 12 Feb



Создать задачу

SUN, 06 Feb

13:00 !

TaskTimer

MON, 07 Feb

19:00 !

TaskTimer

TUE, 08 Feb

WED, 09 Feb

THU, 10 Feb

FRI, 11 Feb

03:00 !

TaskTimer

SAT, 12 Feb

04:00 !

TaskTimer

Редактор и отладчик плейбуков

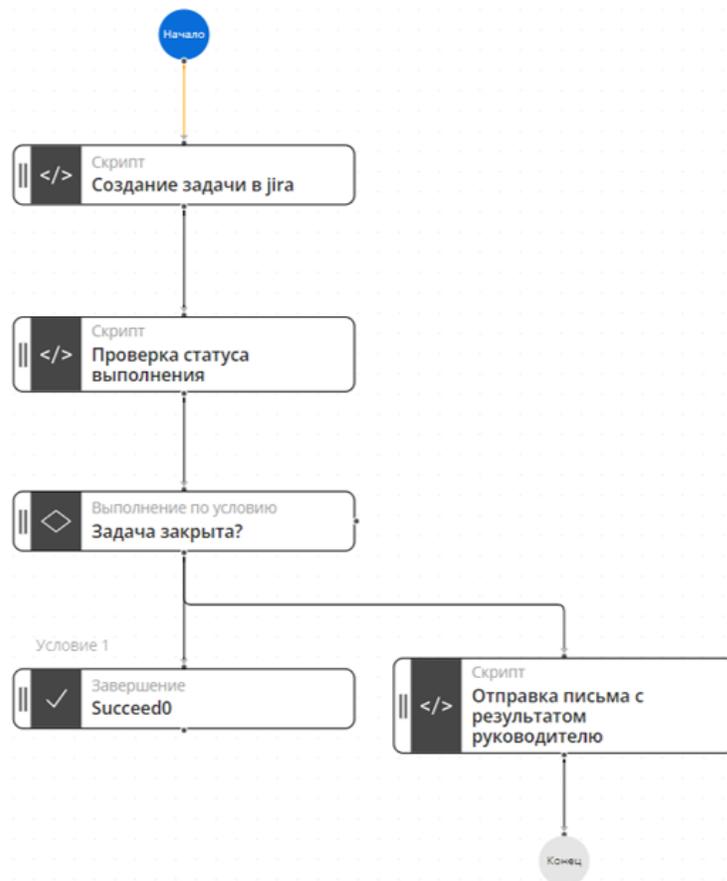
113% ▾ ⌵ 90°

Вредоносная активность - бел...



Ход Выполнения

Действия	Статус
Вредоносная активность - белый и серый	Завершено с ошибкой 31-01-2022
Вредоносная активность - белый и серый	Завершено с ошибкой 31-01-2022
Вредоносная активность - белый и серый	Завершено с ошибкой 31-01-2022
Вредоносная активность - белый и серый	Завершено с ошибкой 31-01-2022
Вредоносная активность - белый и серый	Завершено с ошибкой 31-01-2022
Вредоносная активность - белый и серый	Завершено с ошибкой 31-01-2022
Вредоносная активность - белый и серый	Завершено с ошибкой 31-01-2022
Вредоносная активность - белый и серый	Завершено с ошибкой 31-01-2022
Вредоносная активность - белый и серый	Завершено с ошибкой 31-01-2022



Изменение данных для доступа (Секретов) ×

[+ Добавить секрет](#)

dev × prod ×



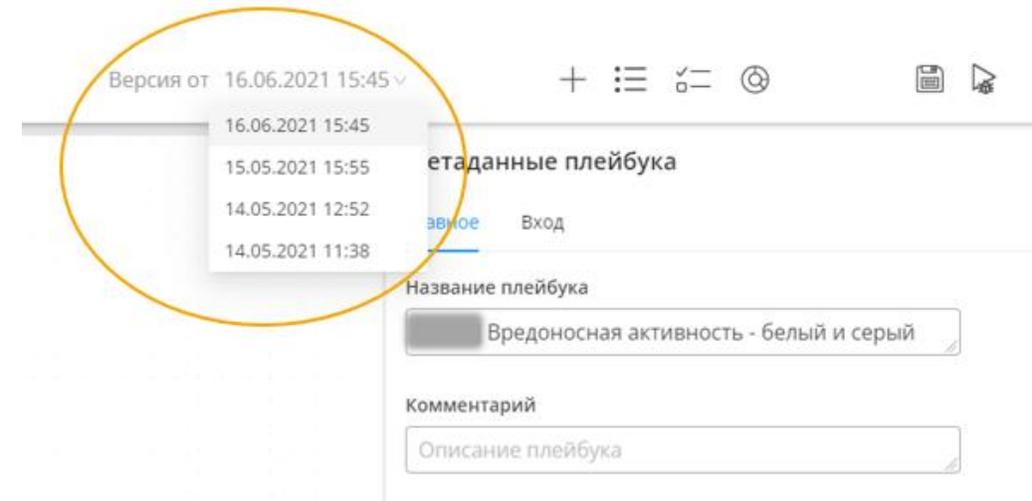
Ключ	Значение
ACCESS_TOKEN_TEST	Данные скрыты.
Tojen	Данные скрыты.
ACCESS_TOKEN	Данные скрыты.
AAA	

Закреть

Централизованное версионированное хранилище

Обеспечивает единый механизм распространения сценариев обогащения, реагирования и восстановления для:

- Плейбуков
- Скриптов
- Секретов



Дашборд с общими показателями

Главный дашборд

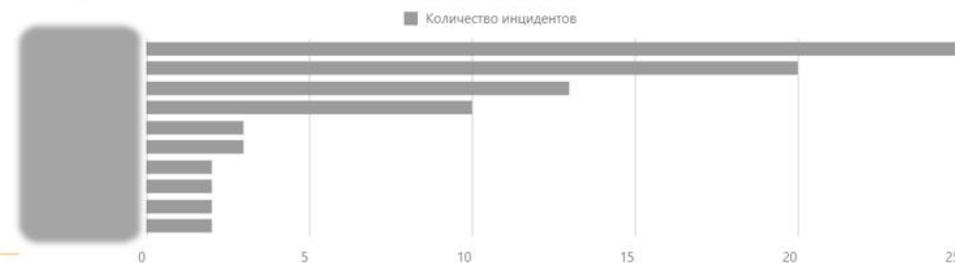
Организация: [redacted]

ИНЦИДЕНТЫ

Ложные 255
 На расследовании 1
 Закрытые 97

ВЗЯТЫЕ В РАБОТУ

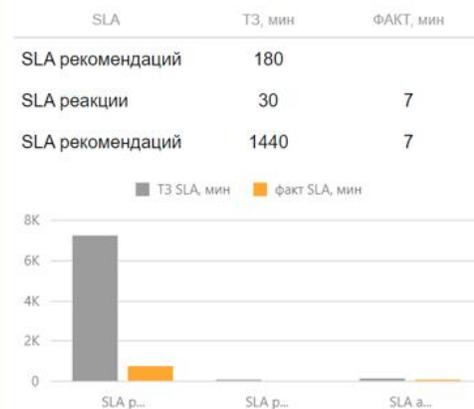
ТОП-10 ОЗ с инцидентами



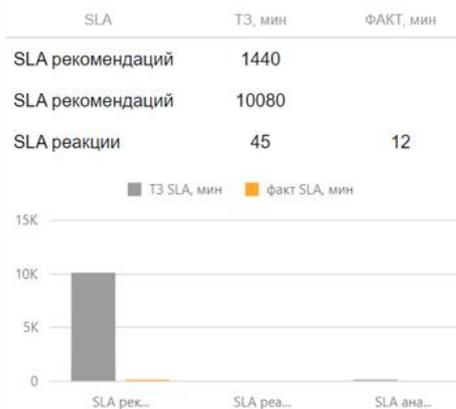
SLA для инцидентов с высоким приоритетом



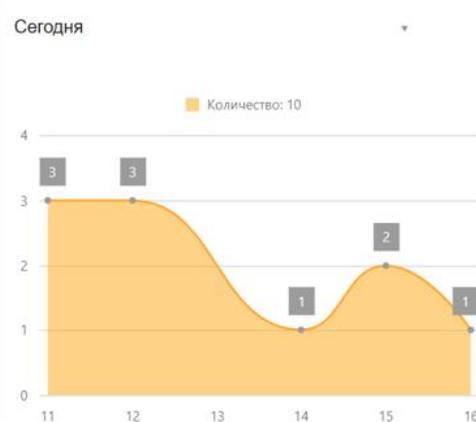
SLA для инцидентов со средним приоритетом...

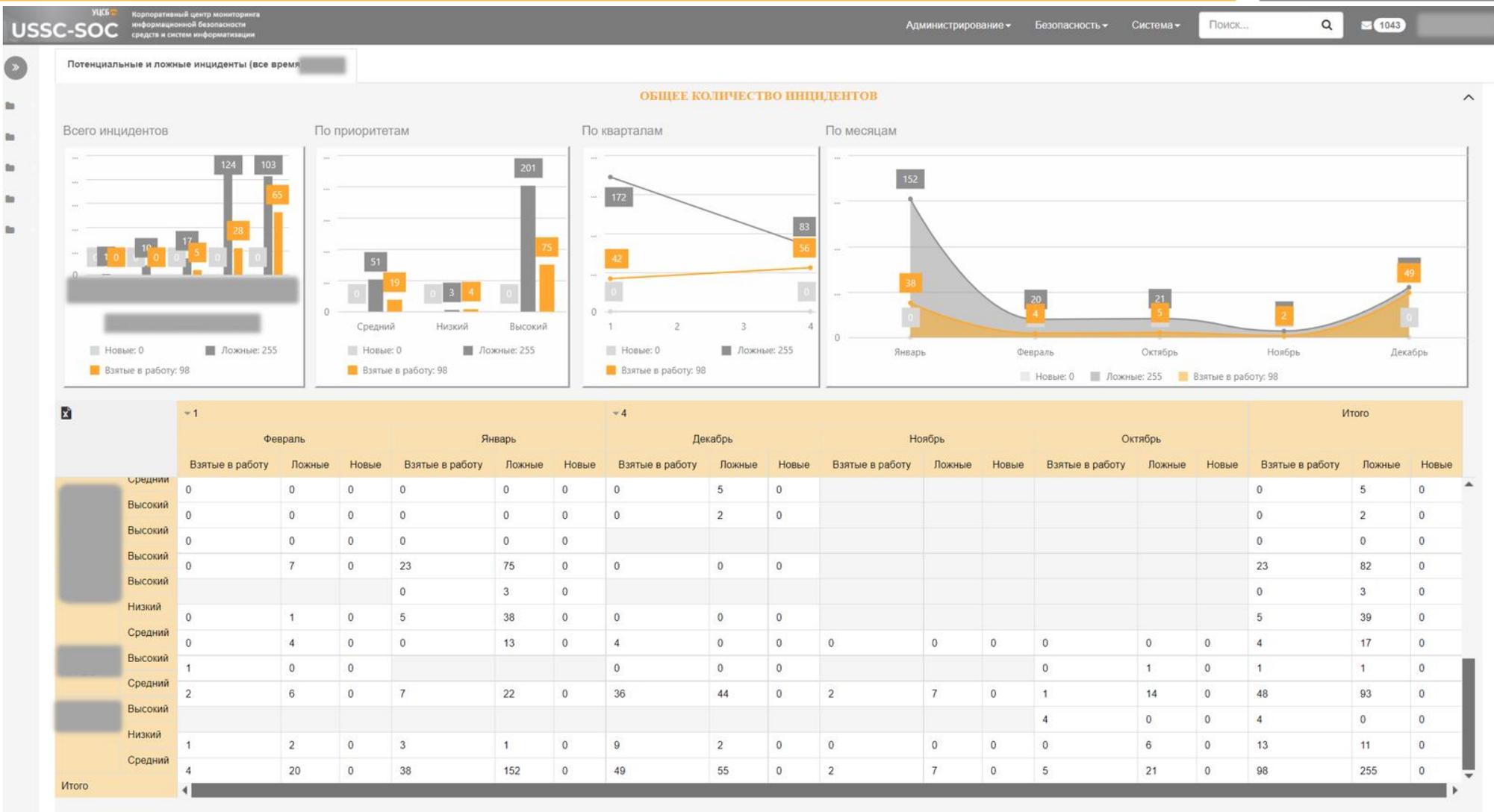


SLA для инцидентов с низким приоритетом

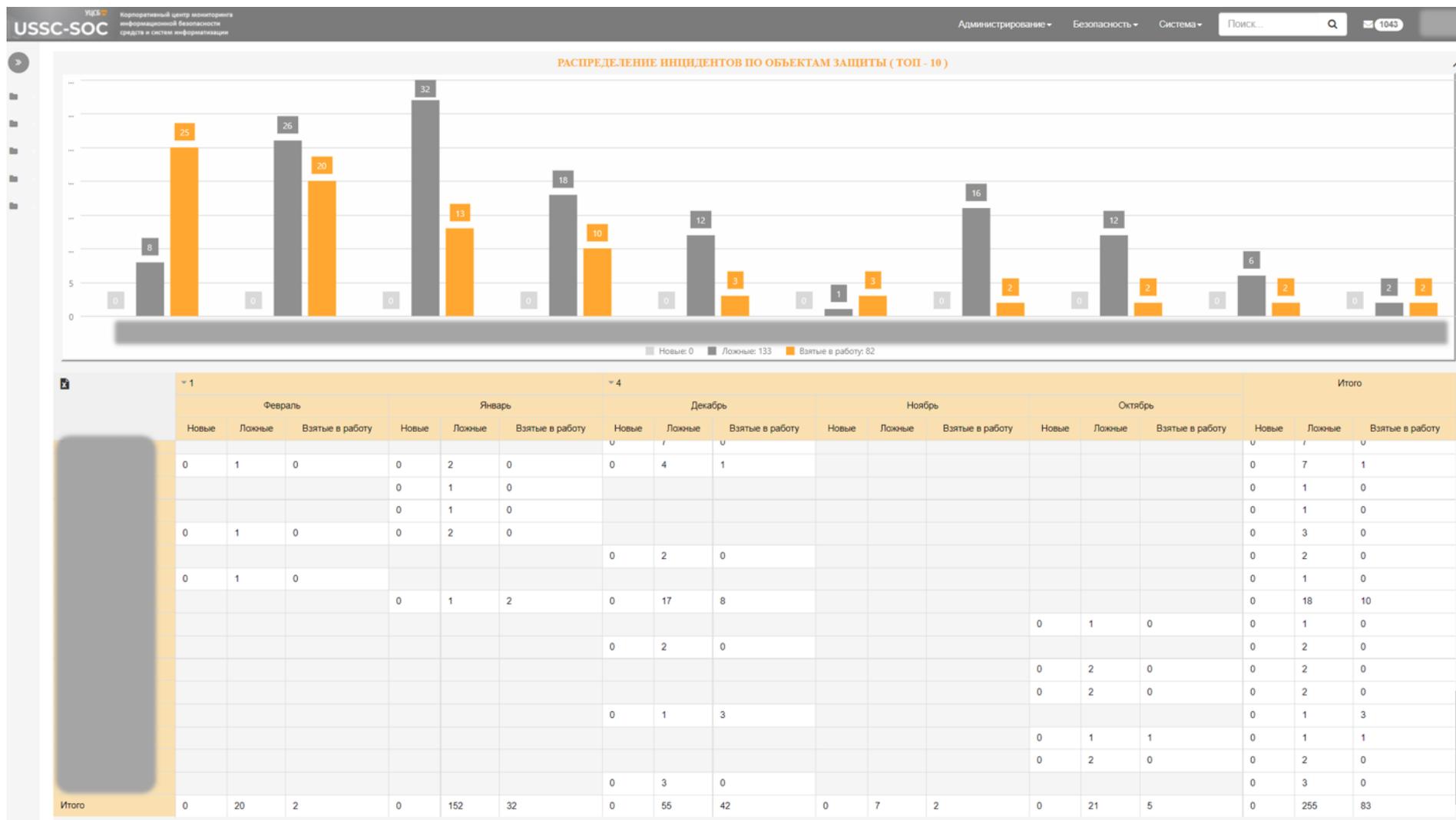


Статистика выявления инцидентов *



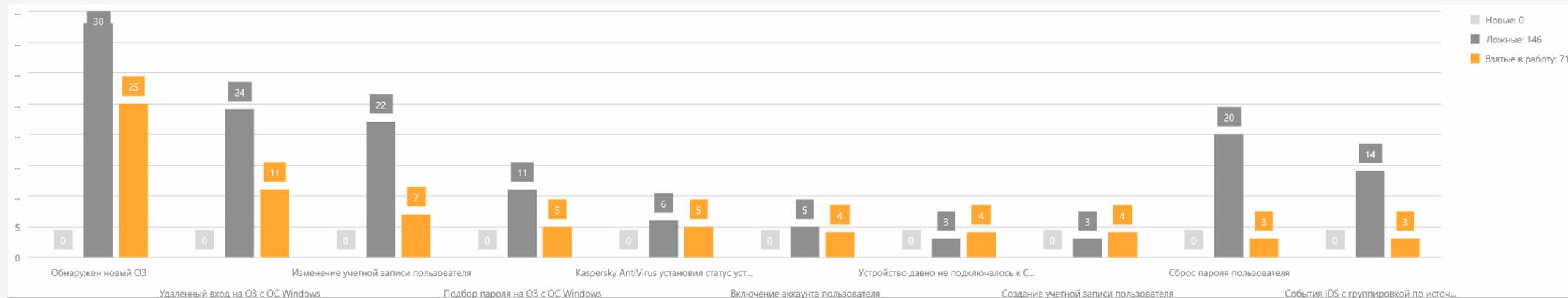


Отчетность по объектам защиты (активам)



Причины возникновения инцидентов

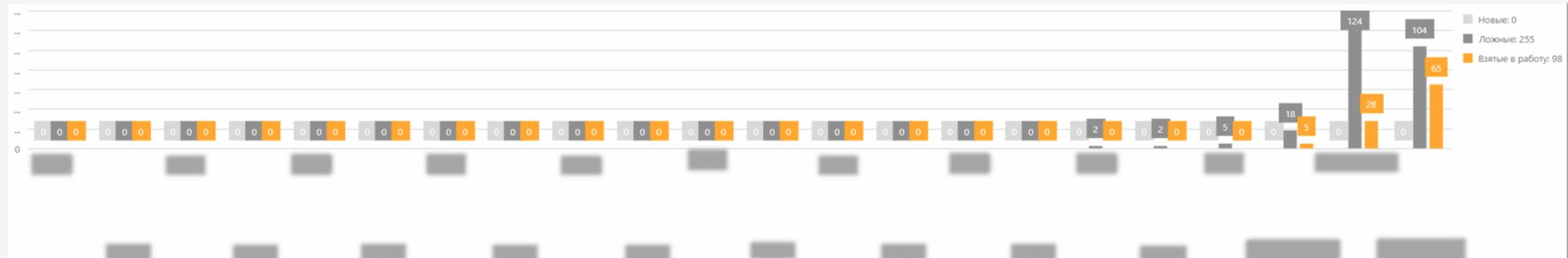
РАСПРЕДЕЛЕНИЕ ИНЦИДЕНТОВ ПО ПРИЧИНАМ ВОЗНИКНОВЕНИЯ (ТОП-10)



	1															4			Итого		
	Февраль			Январь			Декабрь			Ноябрь			Октябрь			Взяты в работу	Ложные	Новые			
	Взяты в работу	Ложные	Новые																		
Kaspersky AntiVirus выключен	0	2	0				1	0	0							1	2	0			
Kaspersky AntiVirus назначил управляемому устройству статус 'Критический' по неизвестной причине							0	1	0							0	1	0			
Kaspersky AntiVirus назначил управляемому устройству статус 'Предупреждение' по неизвестной причине							0	4	0							0	4	0			
Kaspersky AntiVirus обнаружил инцидент информационной безопасности							0	4	0							0	4	0			
Kaspersky AntiVirus установил статус устройства 'критический'							5	6	0							5	6	0			
Аккаунт пользователя был добавлен в глобальную группу	1	0	0	0	2	0	1	0	0							2	2	0			
Аккаунт пользователя был добавлен в локальную группу	0	1	0	0	13	0	2	0	0				0	7	0	2	21	0			
Аккаунт пользователя был удален из глобальной группы				0	1	0	0	1	0							0	2	0			
Блокировка учетной записи							2	0	0							2	0	0			
Включение аккаунта пользователя	0	1	0	0	3	0	4	1	0							4	5	0			

Распределение инцидентов по ОКИИ

РАСПРЕДЕЛЕНИЕ ИНЦИДЕНТОВ ПО ОКИИ



Средство	Февраль			Январь			Декабрь			Ноябрь			Октябрь			Итого		
	Взяты в работу	Ложные	Новые															
	Высокий	0	0	0	0	0	0	5	0							0	5	0
Высокий	0	0	0	0	0	0	2	0							0	2	0	
Высокий	0	0	0	0	0										0	0	0	
Высокий	0	7	0	23	75	0	0	0							23	82	0	
Высокий				0	3	0									0	3	0	
Низкий	0	1	0	5	38	0	0	0							5	39	0	
Средний	0	4	0	0	13	0	4	0	0	0	0	0	0	0	4	17	0	
Высокий	1	0	0				0	0					0	1	1	1	0	
Средний	2	6	0	7	22	0	36	44	0	2	7	0	1	14	48	93	0	
Высокий													4	0	4	0	0	
Низкий	1	2	0	3	1	0	9	2	0	0	0	0	0	6	13	11	0	
Средний																		
Итого	4	20	0	38	152	0	49	55	0	2	7	0	5	21	98	255	0	

Распределение инцидентов по классам

РАСПРЕДЕЛЕНИЕ ИНЦИДЕНТОВ ПО КЛАССАМ



	Необработанные	Ложные инциденты	Взяты в работу	Необработанные	Ложные инциденты	Взяты в работу	Необработанные	Ложные инциденты	Взяты в работу	Необработанные	Ложные инциденты	Взяты в работу	Необработанные	Ложные инциденты	Взяты в работу	Необработанные	Ложные инциденты	Взяты в работу
Мошенничество с использованием ИКТ (fraud)	0	1	1	0	45	22	0	8	2				0	54	25			
Нарушение безопасности информации (information content security)	0	13	2	0	75	6	0	34	38				0	10	1	0	132	47
Нарушение или замедление работы контролируемого информационного ресурса (availability)	0	2	0				0	0	1				0			0	2	1
Несанкционированный доступ в систему (intrusion)				0	2	0							0			0	2	0
Попытки несанкционированного доступа в систему или к информации (intrusion attempt)	0	4	1	0	30	10	0	2	6				0			0	36	17
Сбор сведений с использованием ИКТ (information gathering)	0	0	0	0	0	0	0	11	2	0	7	2	0	11	4	0	29	8
Итого	0	20	4	0	152	38	0	55	49	0	7	2	0	21	5	0	255	98



**Уменьшение
числа обрабатываемых
вручную инцидентов**



**Снижение времени
реагирования**



**Автоматизация обогащения
и агрегации инцидентов**



СПАСИБО ЗА ВНИМАНИЕ

ВОПРОСЫ?



УРАЛЬСКИЙ ЦЕНТР
СИСТЕМ БЕЗОПАСНОСТИ | **USSC.RU**