

117 приказ ФСТЭК России.

Мониторинг и реагирование с точки зрения регулятора

- **Алексей Федотов**
Продуктовый менеджер SOCRAT
- **Александр Кирий**
Руководитель центра мониторинга SOCRAT





Время вебинара ~ 50 мин



Обменивайтесь сообщениями
во вкладке «Чат»



Запись вебинара направим всем
участникам на указанный
при регистрации e-mail
в течение 2-3 рабочих дней



Задавайте вопросы во вкладке
«Вопросы»



**Среди заданных вами вопросов, каждый
Эксперт выберет лучший, на его взгляд, вопрос,
и мы наградим 2-х авторов фирменным мерчем!**



Системный интегратор в сфере
информационной безопасности
и импортозамещения
информационных технологий



Входим в ГК «Кейсистемс»



Лицензиат ФСТЭК России
Лицензиат ФСБ России

80+

регионов
внедрения

4000+

реализованных
проектов

Новые требования к защите информации в ГИС и иных ИС ОГВ



Приказ ФСТЭК России от 11 апреля 2025 г. № 117. Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

Вступает в силу 01 марта 2026 г.

Приказ распространяется на:

Государственные органы,
государственные унитарные предприятия,
государственные учреждения

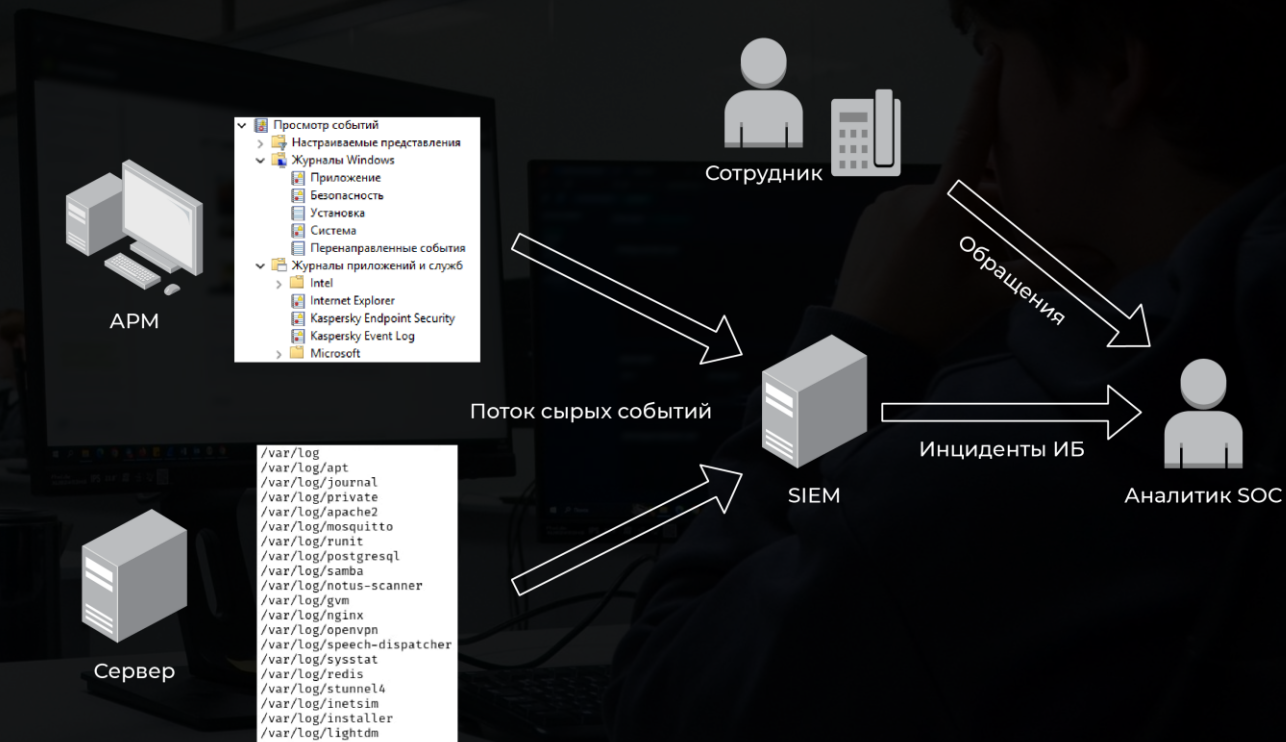
Организации-подрядчики
государственных органов,
имеющие подключение к ИС

Как организовать сбор событий безопасности?

05

Приказ № 117, раздел 3, пп.49;
ГОСТ Р 59547-2021, раздел 4, п.4.1

- Внедрить SIEM-систему;
- Собирать события с узлов ИС: ОС, ПО, СЗИ и прочее;
- Принимать обращения от сотрудников организации;
- Информировать ответственного.



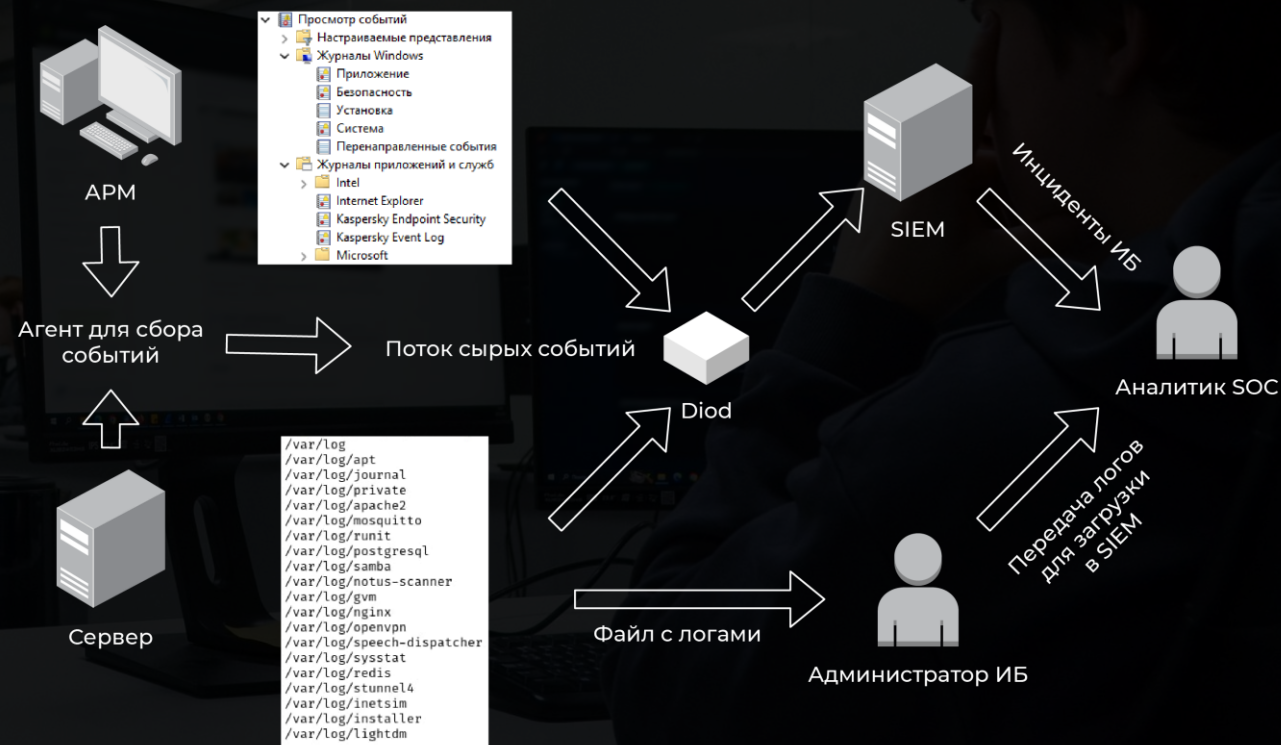
Как организовать сбор событий безопасности?

06

Приказ № 117, раздел 3, пп.49

Для изолированных и локальных ИС:

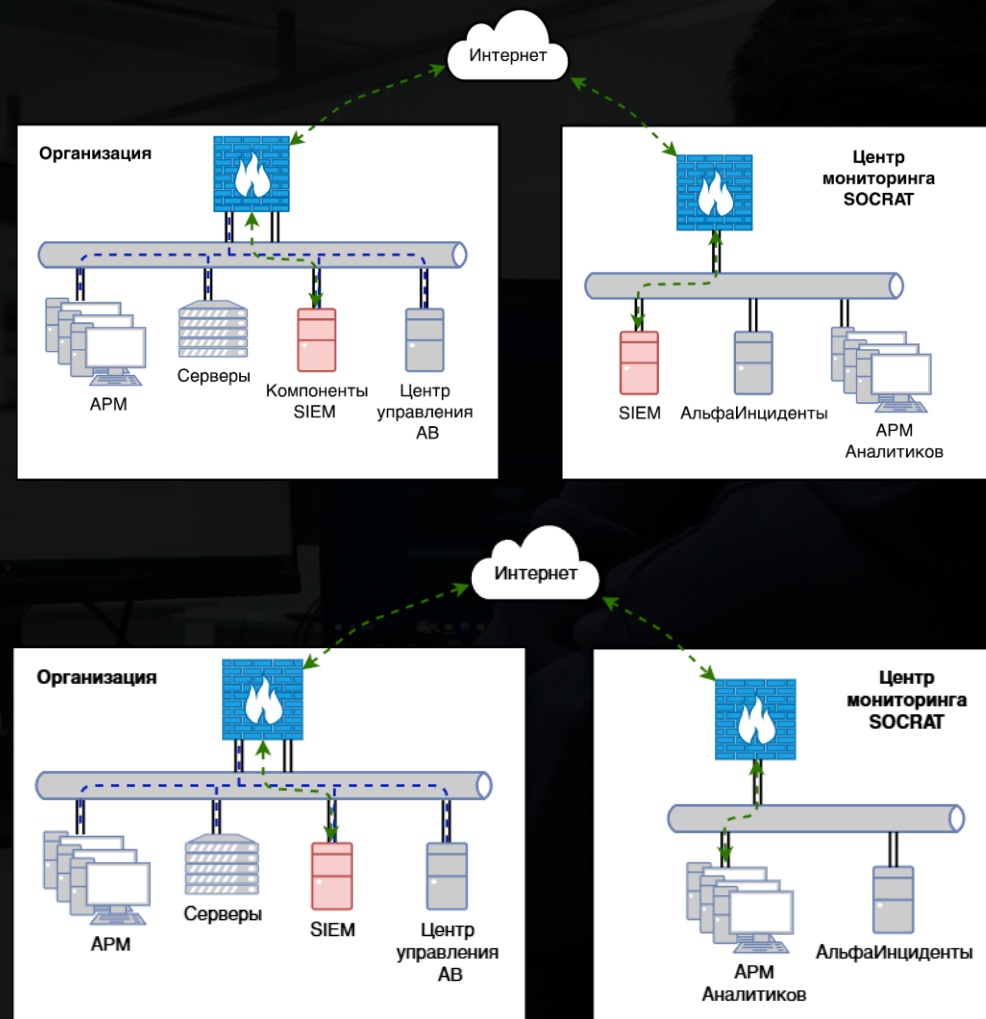
- Агентский сбор событий и их передача через средство одностороннего потока данных
- Сбор событий через агент SIEM с последующей загрузкой в SIEM



Как реализовано в SOCRAT?

07

- Проектирование архитектуры
- Внедрение SIEM-системы:
 - On-premise
 - MSSP
- Заведение источников событий совместно с заказчиком
- Приема обращений и взаимодействие через АльфаИнциденты



Что контролировать?

08

ГОСТ Р 59547-2021, раздел 4, п.4.2 а)

- Аномалии в поведении ИС;
- Подозрительный сетевой трафик;
- Подозрительные действия пользователей;
- Нарушение политик безопасности;
- Срабатывание средств защиты;
- Информировать ответственного.

Как реализовано в SOCRAT?

09

- В процессе мониторинга фиксируются:
 - Нарушения политик безопасности;
 - Уязвимости ПО и ОС;
 - Подозрительные действия пользователей;
 - Реакция систем защиты.
- По итогу фиксации создаются карточки инцидентов и направляются ответственному лицу.

The screenshot displays a detailed incident card within the SOCRAT system. At the top, two tabs are visible: '(Не КИИ) Наличие уязвимости' (selected) and '(Не КИИ) Уязвимый ресурс'. The card contains the following information:

- Название:** Уязвимость OpenSSH
- Уровень:** Средний
- Статус:** Требуется действие пользователя
- Линия поддержки:** Линия 1
- Время регистрации:** 10/11/2025 12:44:20
- Описание:** Выявлено использование OpenSSH версии 7.4. Данная версия содержит множественные уязвимости, эксплуатация которых может привести к удаленному выполнению кода и повышению привилегий.
- Сведения о средстве или способе выявления:** SIEM
- IP адрес назначения:** 192.168.10.152
- Рекомендации:**
 - ☐ Обновить версию OpenSSH до версии 10.2
 - ☐ При отсутствии возможности обновить версию OpenSSH, сообщить для выдачи компенсирующих мер
 - ☐ Сообщить о результатах обновления

A link at the bottom right of the description area reads: 'Переключиться на редактирование в формате Markdown'.

Как анализировать?

10

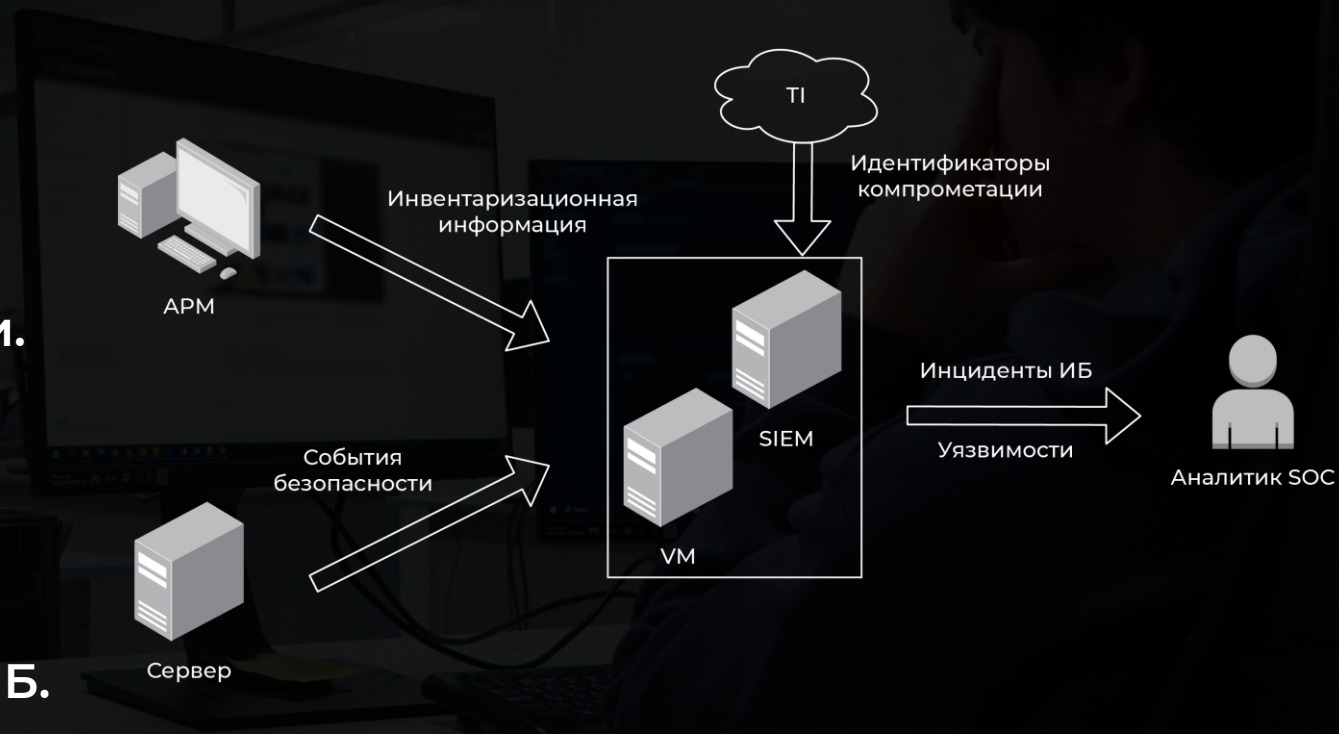
ГОСТ Р 59547-2021, раздел 4, п.4.2 г)

Поток событий обогащать:

- данными об уязвимостях;
- идентификаторами компрометации.

В процессе мониторинга:

- дорабатывать правила;
- фильтровать ложные инциденты;
- фиксировать нарушения политик ИБ.



Как реализовано в SOCRAT?

11

При выявлении подозрения на инцидент, аналитик:

- Проверяет, был ли подобный инцидент;
- Сверяется с информацией об инфраструктуре и результатами анализа уязвимостей;
- Собирает информацию из открытых источников;
- Проверяет совпадение по базам с идентификаторами компрометации.

Для ложных инцидентов добавляются исключения
Инциденты вносятся в базу инцидентов в виде кейса

The screenshot shows the VirusTotal analysis page for a file named 'ShellExtension' (SHA256: 8b2e701e91101955c73865589a4c72999aeabc11043f712e05fdb1c17c4ab19a). The file size is 249.00 KB and it was last analyzed 7 days ago. The community score is 59/72, with a warning that 59/72 security vendors flagged this file as malicious. The file is categorized as a trojan.zbot/foreign threat. The 'Security vendors' analysis table shows detections from Acronis, AliCloud, Arcabit, Avast, and Avira, all identifying it as a Trojan or suspicious file.

Security vendors' analysis	Threat categories	Family labels
Acronis (Static ML)	Suspicious	TrojanSpy:Win32/Obfuscator.c21d32b2
AliCloud	Trojan(spy):Win/Zbot.AMV	Trojan.Foreign.Gen.2
Arcabit	Trojan.Foreign.Gen.2	Unsafe
Avast	Win32:Cryptor	Win32:Cryptor
Avira (no cloud)	TR/Spy.Zbot.ikzv	Trojan.Foreign.Gen.2

Как снизить вероятность инцидента ИБ?

12

ГОСТ Р 59547-2021, раздел 4, п.4.2 б)

Контроль (анализ) защищенности:

- Выявлять и описывать уязвимости
- Контролировать установку обновлений;
- Проводить инвентаризацию;
- Контролировать настройку ПО и СЗИ в соответствии с политиками ИБ;
- Информировать ответственного.



Как реализовано в SOCRAT?

13

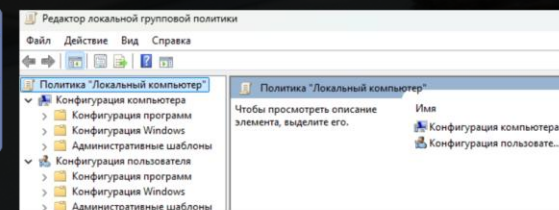
В рамках одного из пакетов услуг периодически проводятся:

- Инвентаризация;
- Анализ уязвимостей;
- Тестирование на проникновение.

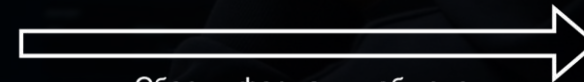
Предоставляется услуга по управлению уязвимостями.



APM



Имя	Издатель	Установле...	Размер	Версия
7-Zip 22.01 (64-bit edition)	Igor Pavlov	05.11.2024	5.65 MB	22.01.2024
Kaspersky Endpoint Security для Windows	AO "Лаборатория Касперского"	05.11.2024	341 MB	12.0.0.438
Microsoft ASP.NET MVC 2	Microsoft Corporation	13.11.2024	850 KB	2.0.60526.0
Microsoft Edge	Корпорация Майкрософт	06.12.2024	131.0.2903.86	16.0.4286.1001
Microsoft Office профессиональный плюс 2016	Microsoft Corporation	05.11.2024	16.0.4286.1001	24.221.1951.0003
Microsoft OneDrive	Microsoft Corporation	05.12.2024	383 MB	16.0.4286.1001
Microsoft Visual C++ 2010 x86 Redistributable (x86) - 10.0.40219	Microsoft Corporation	06.11.2024	13.2 MB	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable (x86) - 10.0.40219	Microsoft Corporation	06.11.2024	10.1 MB	10.0.40219
Microsoft Visual C++ 2010 x86 Redistributable (x86) - 10.0.40219	Microsoft Corporation	06.11.2024	11.1 MB	10.0.40219
Microsoft Visual C++ 2010 x86 Redistributable (x86) - 10.0.40219	Microsoft Corporation	06.11.2024	17.1 MB	12.0.30901.0
Microsoft Visual C++ 2010 x86 Redistributable (x86) - 14.0.24212	Microsoft Corporation	06.11.2024	19.5 MB	14.0.24212.0
Microsoft Visual C++ 2010 x86 Redistributable (x86) - 14.0.33816	Microsoft Corporation	06.11.2024	20.7 MB	14.0.33816.0



Сбор информации об узле



VM



Сервер

description	Version	Architecture	D
7zip	24.08+dfsg-1	amd64	7
7zip file archiver with a high compression ratio	23.13.9-7	amd64	q
accountsservice	2.3.2-2+b1	amd64	a
acl	2.3.2-2+b1	amd64	a
access control list - utilities	3.137	all	a
adduser	3.137	all	d
add and remove users and groups	47.0-2	all	d
adwaita-icon-theme	47.0-2	all	d
default icon theme of GNOME			
ImageMagick-6	gophish	miredo.conf	sane.d
ModemManager	gprofng.rc	mke2fs.conf	scalpel
NetworkManager	groff	modprobe.d	screenrc
000CDataSources	group	modules.conf.d	sdm.conf.d
OpenCL	group	modules-load.d	searchsploit_rc
UPower	grub.d	mosquitto	security
x11	gshadow	motd	selinux
alternatives	gshadow	mysql	sensors.d
adduser.conf	gtk-3.0	nanorc	sensors3.conf
apache2	gtk-3.0	netconfig	sgml
apparmor	gtk-3.0	netconfig	sgml
apparmor.d	gtk-3.0	netconfig	sgml
apt	gtk-3.0	netconfig	sgml
arp-scan	gtk-3.0	netconfig	sgml
avahi	gtk-3.0	netconfig	sgml
bash.bashrc	gtk-3.0	netconfig	sgml
bash_completion	gtk-3.0	netconfig	sgml

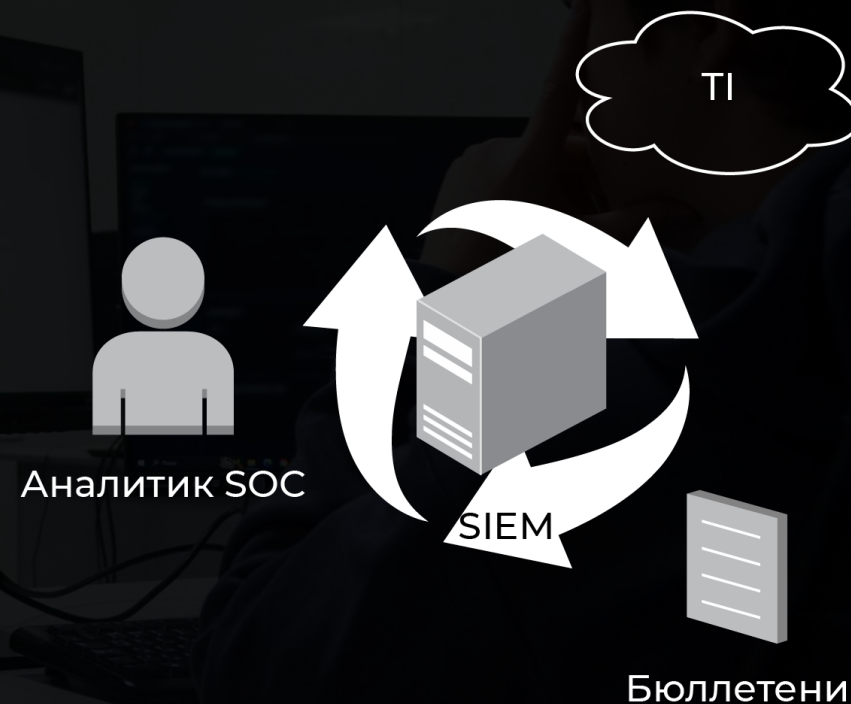
Как поддерживать актуальность?

14

ГОСТ Р 59547-2021, раздел 4, п.4.2 г)

Анализ угроз:

- Внесение в SIEM идентификаторов компрометации от TI-платформы, рассылки регуляторов и на основе анализа угроз аналитиков;
- Выявление аномалий и актуализация правил в SIEM
- Формировать предложения по расширению зоны действия мониторинга (на основе недостаточной информации и изменений ландшафта угроз)



Как реализовано в SOCRAT?

15

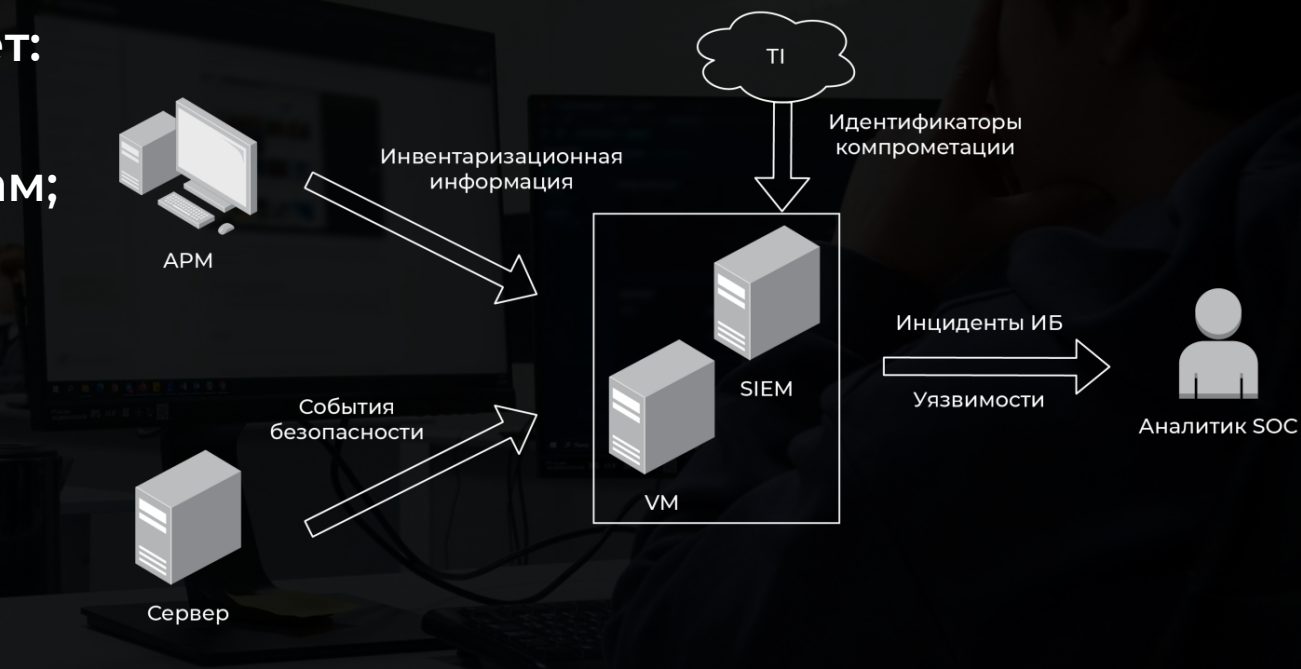
Актуализация экспертизы SIEM за счет:

- Идентификаторов компрометации;
- Исключений по ложным инцидентам;
- Доработки правил на основе трендов угроз.

Интеграция SIEM с TI;

Интеграция SIEM с VM;

Предложения по расширению
зоны мониторинга.

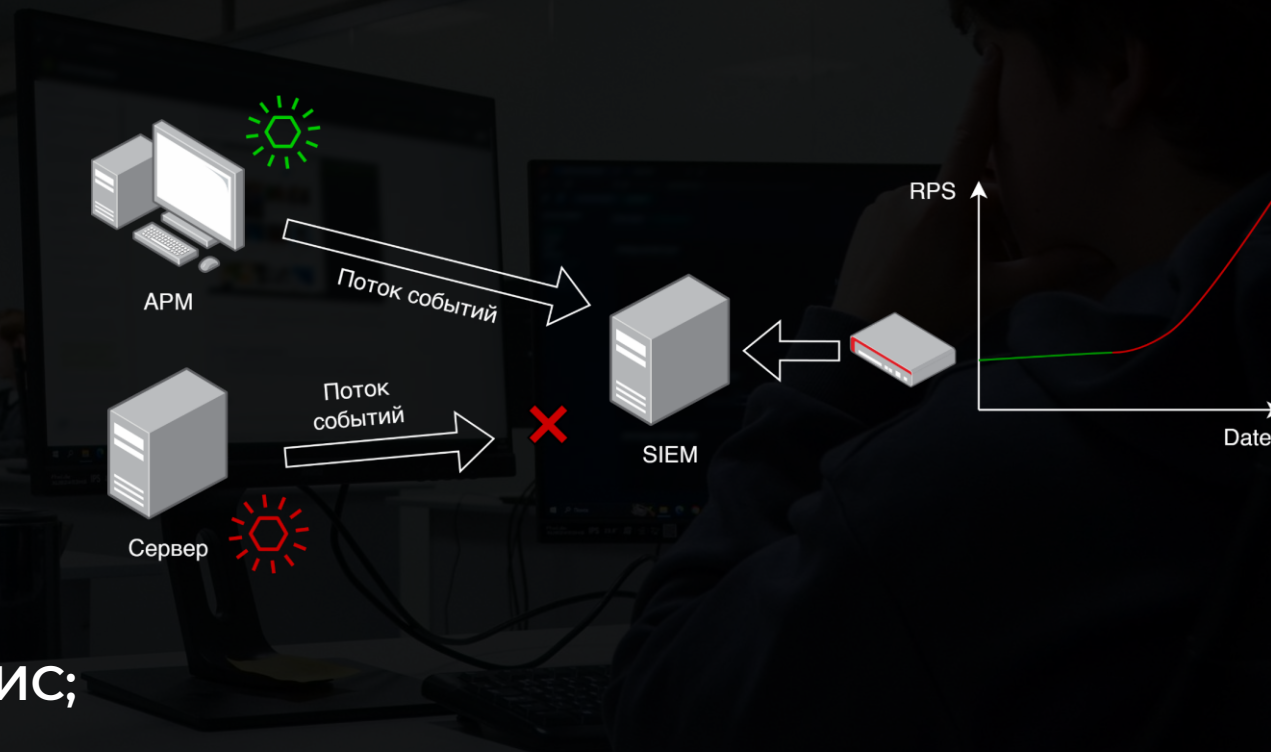


Инцидент может быть не только из-за атаки?

16

ГОСТ Р 59547-2021, раздел 4, п.4.2 в)
Анализ оценки функционирования систем защиты информации в ИС:

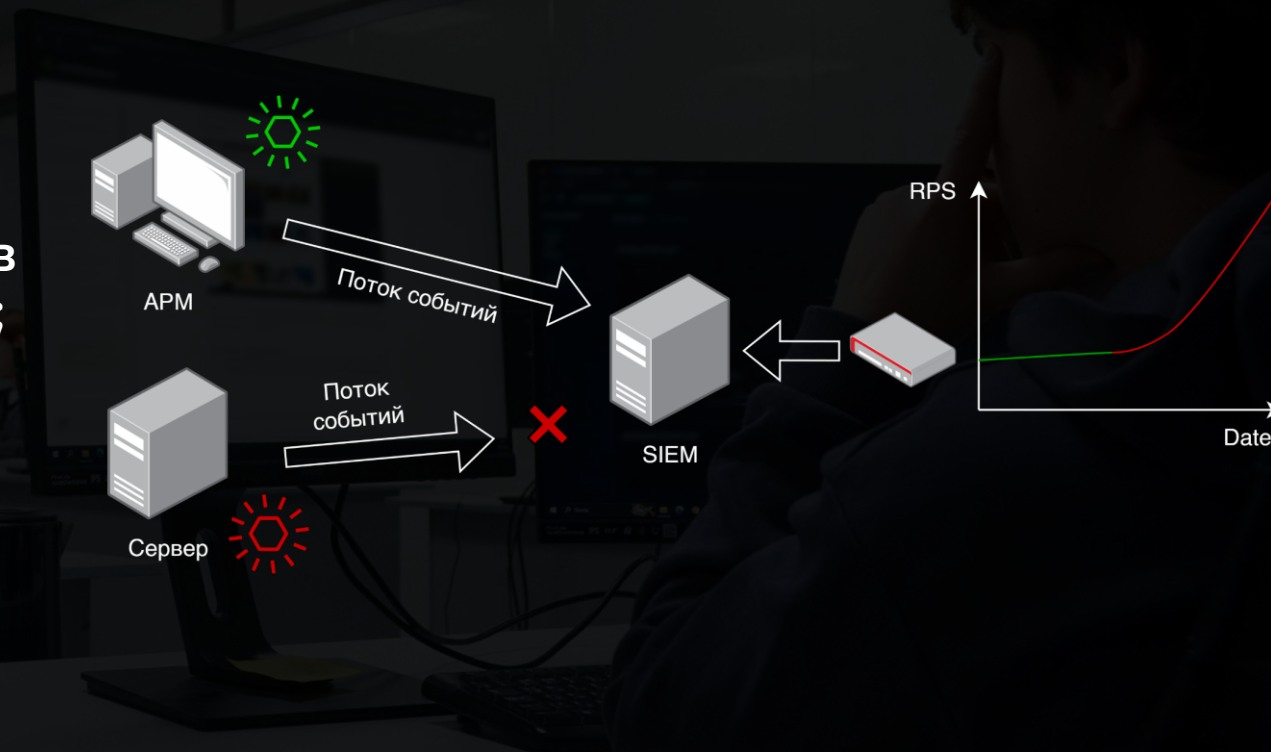
- Контроль работоспособности ПО и СЗИ;
- Проверка соответствия среды функционирования требованиям документации на СЗИ;
- Контроль потоков информации влияющих на производительность ИС;
- Информировать ответственного.



Как реализовано в SOCRAT?

17

- Контроль функционирования системы мониторинга и источников событий на основе потока событий;
- Контроль потока событий на наличие аномальных всплесков.

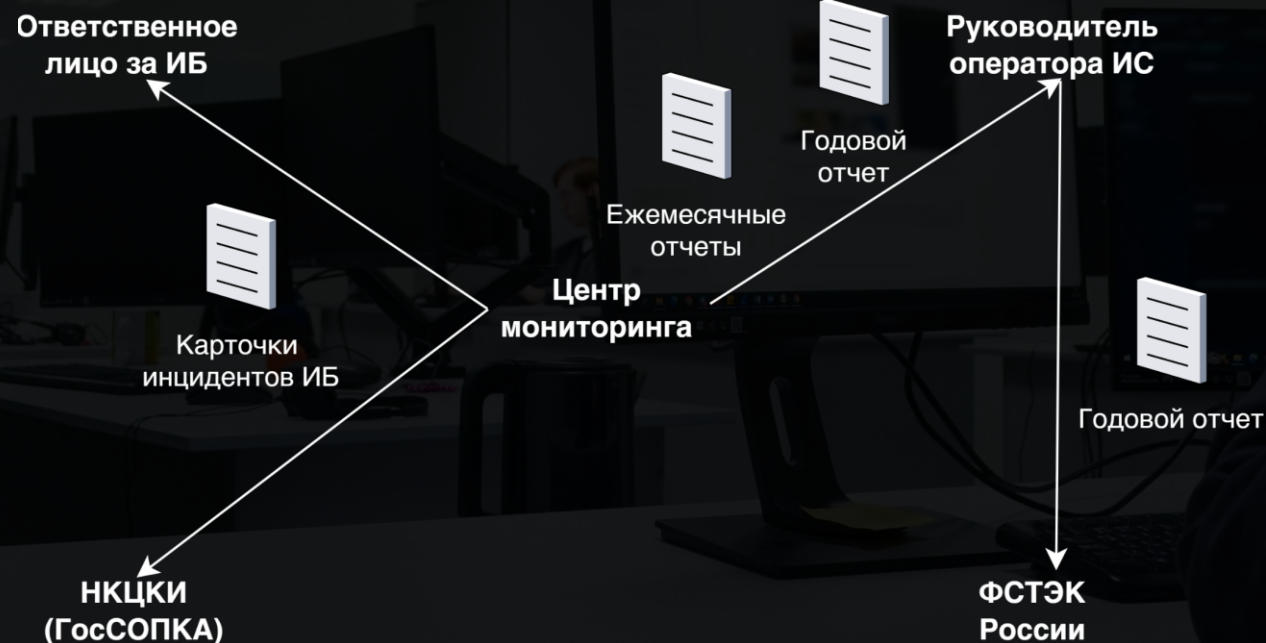


Кому сообщать об инцидентах ИБ?

18

Приказ № 117, раздел 3, пп.49

Приказ № 117, раздел 3, х)



Итоговый отчет отправляется руководителем оператора ИС во ФСТЭК России

Как реализовано в SOCRAT?

19

В случае обнаружения инцидента, либо подозрения на инцидент:

- Отправка карточки инцидента через АльфаИнциденты;
- Подготовка ежемесячных отчетов через АльфаИнциденты и отправка ответственному;
- Подготовка годового отчета и отправка ответственному;

В рамках пакета услуг производится взаимодействие с ГосСОПКА (интеграция АльфаИнциденты с ЛК ГосСОПКА)

Для самостоятельного взаимодействия, через АльфаИнциденты выгружается карточка в формате НКЦКИ для отправки на почту НКЦКИ

**Выполняйте требования
по мониторингу событий ИБ
согласно 117 приказу ФСТЭК
России за 1,9 млн.руб.**

с командой SOC RAT

100

Анализ
до 100 активов

НПА

Мониторинг по ГОСТ Р
59547-2021 и 117
приказу ФСТЭК России

24/7

Непрерывный
мониторинг

A

Корпоративный
центр ГосСОПКА
(класс A)



SOCRAT – ЭТО ЦЕНТР МОНИТОРИНГА КСБ-СОФТ

20

Режим работы **24x7**

Инвентаризация

Анализ Уязвимостей

Тестирование на проникновение

Корпоративный
центром **ГосСОПКА** (класс А)

Пакетная система предоставления
услуг (выбор только необходимого)

Год создания: **2020**

С чего начать?

21

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить качество предоставляемых услуг **SOCRAT**



РАБОТАЙТЕ С НАМИ!



ksb-soft.ru



info@ksb-soft.ru



Telegram-канал
«Мнение Интегратора»



8 800 3333-872



Подкаст
«Голос Интегратора»



428000, г. Чебоксары,
пр-т Максима Горького,
18 Б, пом. 9