



SECURITY CAPSULE

SIEM

ПЕРВАЯ ОТЕЧЕСТВЕННАЯ



ПРЕМИЯ

**ЦИФРОВЫЕ
ВЕРШИНЫ**

Лауреат в номинации
Лучшее решение
для информационной безопасности

Руководитель проекта:

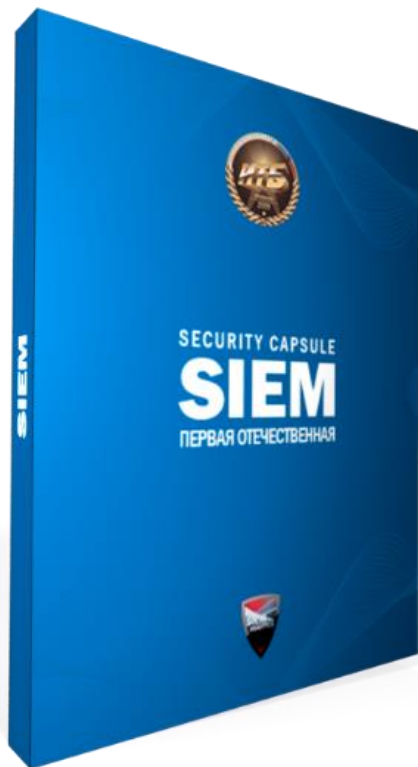
Графов Сергей

Тел. +7 (911) 920-09-87

sag@itb.spb.ru



SECURITY CAPSULE SIEM



Security Capsule SIEM (SC SIEM) - это система мониторинга и корреляции событий информационной безопасности, разработанная в России и внедряемая с 2009 года.

Импортозамещающее решение, адаптированное к потребностям как государственных структур, так и бизнеса.

SC SIEM соответствует требованиям регуляторов ФСТЭК России и ФСБ России, совместимо с российскими операционными системами и средствами защиты информации.



Security Capsule SIEM – лауреат премии
«Цифровые Вершины 2025»

Смотрите, читайте

СЕРТИФИКАТЫ И СВИДЕТЕЛЬСТВА



Сертификат Федеральной службы по
техническому и экспортному контролю
№ 4735 от 01 ноября 2023 года
Требования доверия(4), ТУ.



Запись в едином реестре российских
программ для электронных
вычислительных машин и баз данных
Минцифры России №1139 от 14 июня
2016 года.



НАС ВЫБИРАЮТ ЛИДЕРЫ ОТРАСЛИ

Решение уже используется в ключевых отраслях — от энергетики и транспорта до здравоохранения и госсектора — помогая снизить операционные риски, и соответствовать требованиям регуляторов.

2024

АО Ямальская железнодорожная компания

Оператор железнодорожной инфраструктуры Ямала, обслуживает ключевые грузовые и пассажирские направления в регионе.

2023

ТФОМС ЛО

Ключевой институт системы ОМС, обеспечивающий финансирование и контроль качества медицинской помощи.

2022

ООО «Цифровое Приморье»

Динамично развивающаяся компания, специализирующаяся на цифровизации бизнеса и аналитике данных.

ДОСТОИНСТВА

- Подходит для малых и распределённых ИТ-инфраструктур
- Выявляет инциденты ИБ в реальном времени и ретроспективно
- Контролирует безопасность Active Directory: доступы, изменения, аномалии
- Аудирует события безопасности в ОС Linux и Windows
- Интеграция с ГосСОПКА и НКЦКИ: экспорт инцидентов и отчётность по ФСТЭК
- Обогащает инциденты Threat Intelligence от F6
- Работает с IoC: загрузка, фильтрация и автоматический поиск компрометации
- CRATU: экспертная база атак и правил для SIEM
- Упрощает обработку уязвимостей: сводка, фильтрация, анализ
- ИИ-ассистент помогает в анализе событий и формировании выводов
- Превосходит отечественные SIEM по скорости выявления инцидентов
- ПНР выполняются специалистами вендора — **бесплатно**



The illustration depicts a superhero on the left, wearing a blue suit and cape, holding a large shield. The shield has a red and blue design with a white diagonal line. On the right is a robot made of stacked server units, with a sign that reads 'ELK' and 'INDEX LOGS'. In the background, a man in a dark jacket stands behind a console with a glowing screen displaying a bar chart. The scene is set in a server room with blue and orange lighting and floating dust particles.

SIEM
Security Capsule

ELK
INDEX LOGS

SC SIEM ПРОТИВ SIEM НА ELK-СТЕКЕ

Критерий	SC SIEM	SIEM на ELK стеке
Скорость реакции	Срабатывает почти сразу (поточковая обработка)	Часто есть задержки (индексация перед алертом)
Корреляция событий	Легко задать «N раз за X минут» (готовые конструкции)	Настраивается сложно (DSL/джобы)
Правила	Пишутся быстро и понятно (уникальный мастер работы с правилами)	Правила сложнее и разрознены (логика в DSL/KQL + пайплайны)
Ресурсы	Работает на «скромном» железе	Требует много памяти и CPU (JVM, индексация, хранение)
Развёртывание	Ставится быстро и просто	Много компонентов, дольше настройка (Beats/Logstash/ES/Kibana)
Стоимость владения	Ниже: меньше серверов и поддержки	Выше: мощное железо и админка
Пики нагрузки	Держит поток стабильно (нет очередей индексации)	На пиках растут задержки (бекпрешер/очереди)
Время до обнаружения	Меньше — за счёт онлайн-аналитики	Больше — из-за архитектуры

ПОСТАВКА



SC SIEM доступна как в виде программных модулей, так и в виде программно-аппаратных комплексов.

Для небольших IT-инфраструктур SC SIEM предлагается в формате All-in-one.

Варианты лицензирования:

- All-in-one
- Коробочная версия
- Подписка
- MSSP

СРАВНЕНИЕ МОДЕЛЕЙ ЛИЦЕНЗИРОВАНИЯ

Модель	Срок действия	Тип установки	Лицензирование источник./коннектор.	Техподдержка	Продление техподдержки	Особенности
All-in-one	Бессрочная	ПАК на сервере	Да	1 год	25% от стоимости лицензий	Поставляется как ПАК
Коробочная версия	Бессрочная	Дистрибутив на инфраструктуре клиента	Да	1 год	25% от стоимости лицензий	Стандартная коробка. Требуется контроль источников/модулей
<u>Подписка</u>	12/24 мес.	Любая (cloud/on-prem)	Нет	На весь срок	Не требуется	Безлимитная модель. Простой расчёт, SLA возможно
<u>MSSP</u>	Бессрочная	Любая	Да	1 год	25% от стоимости лицензий	Покупка лицензий под каждого клиента. Повышенная скидка. + бонус скидка при покупке «впрок»

КОМПЛЕКТ ПОСТАВКИ

В базовый комплект поставки SC SIEM входит:

- Модуль сбора событий
- Модуль нормализации
- Модуль корреляции
- Модуль хранения
- Консоль

Дополнительно лицензируемые модули:

- Модуль ГосСОПКА



ГОССОПКА

В SC SIEM реализован модуль «ГосСОПКА», который обеспечивает возможность отправки уведомлений о зафиксированных на объекте информатизации компьютерных инцидентах в Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

Уведомления о компьютерных инцидентах отправляются в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) в соответствии с установленным НКЦКИ регламентом.



ВНЕДРЕНИЕ

Внедрение SC SIEM делится на четыре этапа:

- Этап 1 – Обследование
- Этап 2 – Идентификация источников
- Этап 3 – Установка модулей
- Этап 4 – Настройка

Внедрение и опытная эксплуатация SC SIEM, включая устранение ложноположительных срабатываний (False positive) правил корреляции, выполняются экспертами вендора.



ЭТАП 0. Оценка защищенности

Бесплатный экспресс-пентест до пилота SC SIEM

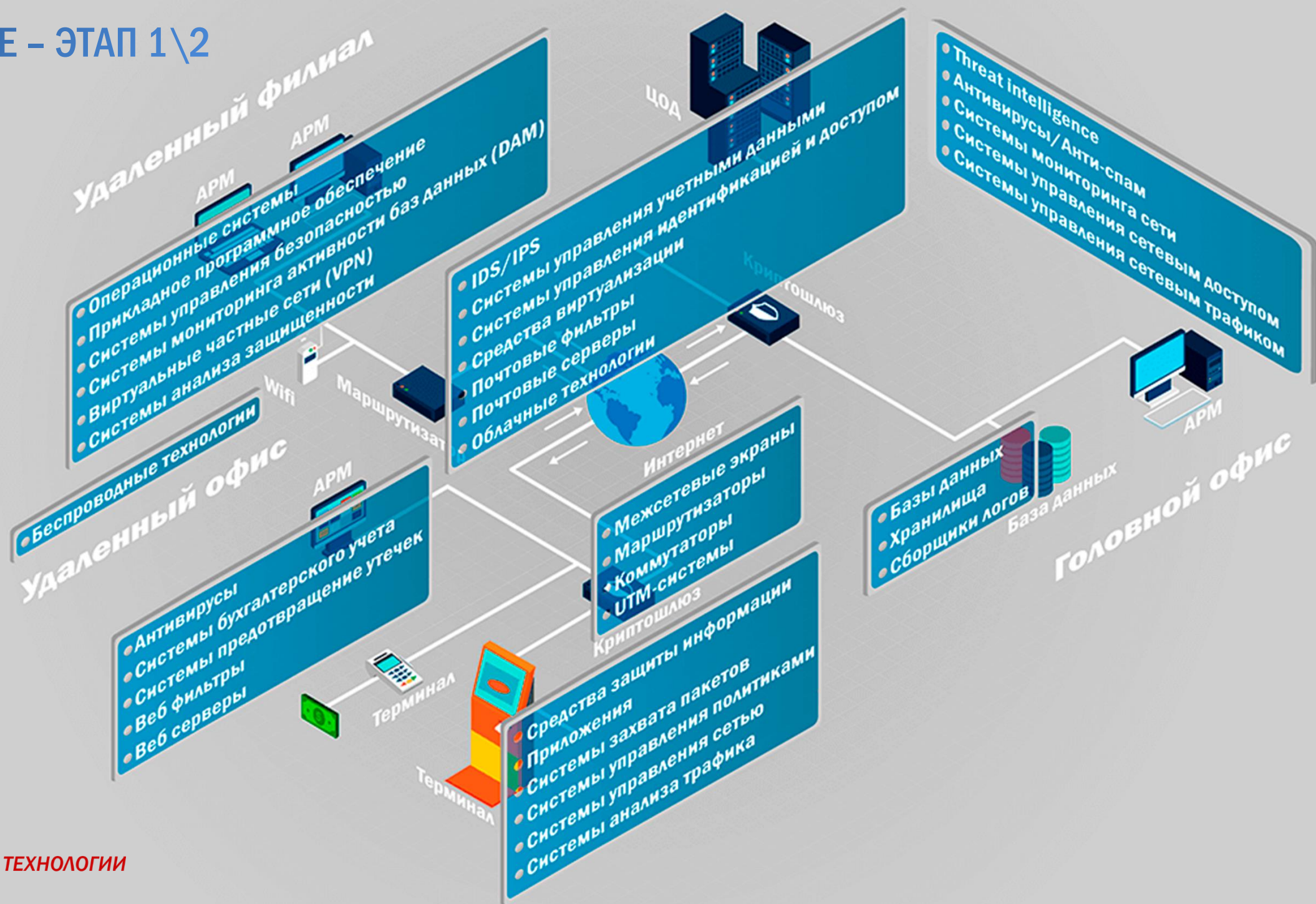
Выявим слабые места, сравним эффективность защиты до и после внедрения SIEM.

Что входит:

- Тест до 5 IP/доменов
- Автоскан + ручная верификация
- Проверка периметра;
- Два отчета: для ИБ и руководства.

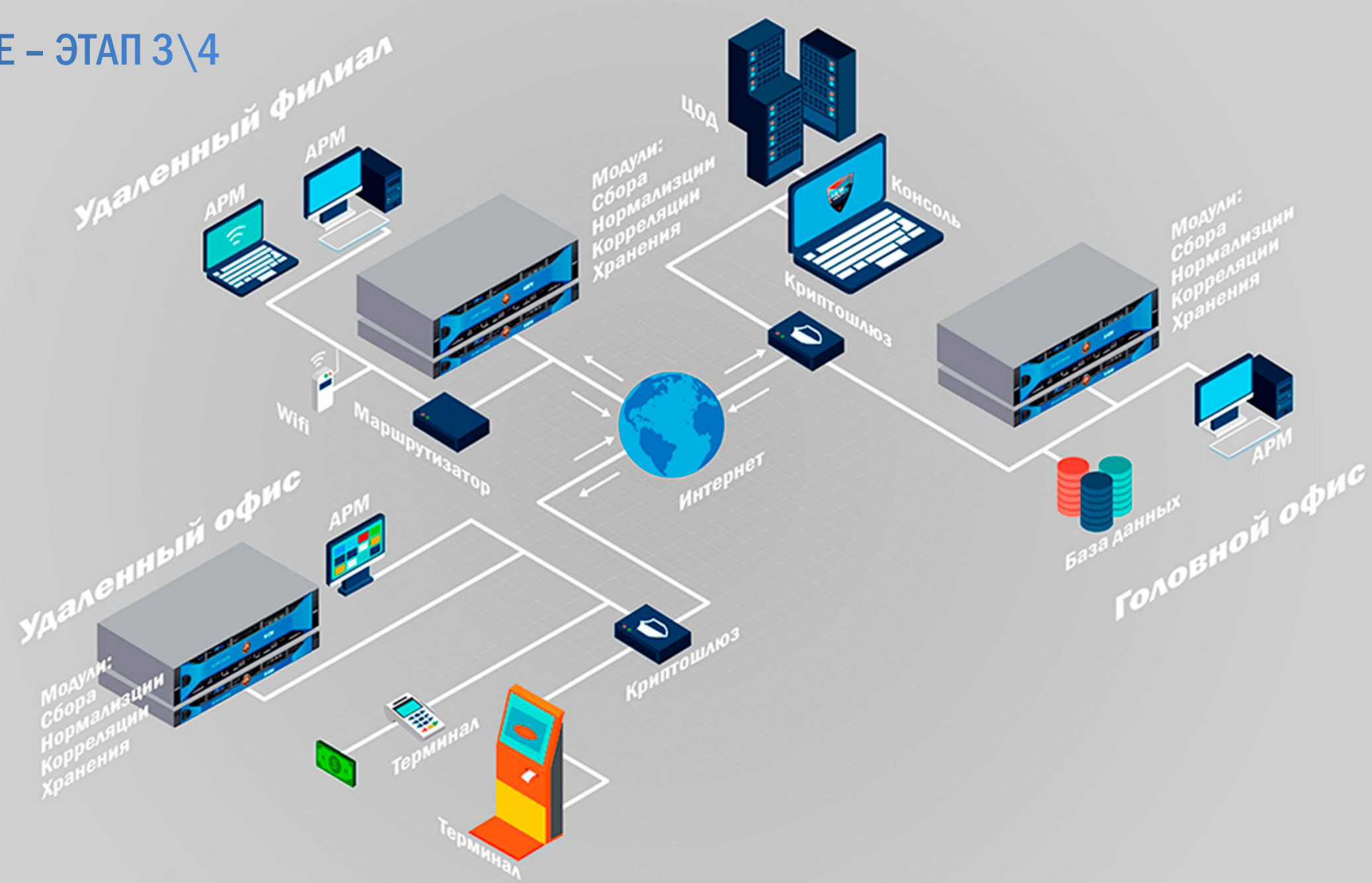
Кейс: Перед пилотом SIEM, мы провели Pentest госорганизации и выявили критические инциденты ИБ

ВНЕДРЕНИЕ – ЭТАП 1\2





ВНЕДРЕНИЕ – ЭТАП 3\4



CRATU (R&D ЦЕНТР)



Для пользователей SC SIEM: вместе с каждой рассылкой CRATU вы получаете готовые правила корреляции, которые можно сразу импортировать в SC SIEM.

CRATU — Центр исследования атакующих техник и уязвимостей — обеспечивает SC SIEM:

- актуальными индикаторами компрометации (IoCs)
- сценариями реагирования на реальные атаки (по MITRE ATT&CK)
- автоматическими обновлениями правил корреляции

>500

Новых IOC выявлено и направлено в рассылках пользователям SC SIEM

>120

Правил корреляции направлено пользователям SC SIEM за месяц

>7

Аналитических кейсов о реальных атаках опубликовано

THREAT INTELLIGENCE



Модуль интеграции с системой Threat Intelligence от компании F6 в SC SIEM предоставляет возможность обогащения инцидентов информационной безопасности по следующим типам индикаторов:

- Хеш
- IP-адрес
- Домен

44%

В 2024 году количество кибератак с использованием программ-вымогателей увеличилось на

\$3 млн

Рекорд по сумме запрошенного выкупа

x2

Число прогосударственных хакерских групп, атаковавших Россию и страны СНГ

ИИ-АССИСТЕНТ



Использование передовых возможностей генеративных языковых моделей позволило автоматизировать анализ данных о событиях и инцидентах, а также получение рекомендации по устранению угроз в режиме реального времени.

30-40%

Снижение операционных и административных расходов

~ 60 %

Сокращение времени реагирования на инциденты

20-30%

Увеличение точности анализа инцидентов

<33>Mar 6 17:33:14 SecurityCapsuleSIEMCorrelator[9907]: [1:800006
9:1] [sysmon-custom] Службы удаленного доступа - Обнаружено ис
пользование служб удаленного доступа для обеспечения удаленно
го доступа к системе или сети. Службы удаленного доступа могут в
арьироваться в зависимости от операционной системы и конфигу
рации, и могут включать такие протоколы [Classification: Network eve
nt] [Priority: 2] [Program: Microsoft-Windows-Sysmon] {UDP}
[192.168.1.8:514 \[\] -> 192.168.1.8:514 \[\]](#) - <14>Mar 6 17:33:13 SID.Ilc-it
b.local Microsoft-Windows-Sysmon[3548]: 1: Process Create: RuleNa
me: Attack=T1021.003,Technique=Distributed Component Object Mod
el,Tactic=Lateral Movement,DS=Process: Process Creation,Level=0,D
esc=DCOM Launch UtcTime: 2025-03-06 14:33:13.261 ProcessGuid:
{cccca16c-b229-67c9-a602-000000000100} ProcessId: 8180 Image:
C:\Windows\System32\dllhost.exe FileVersion: 10.0.19041.1 (WinBuil
d.160101.0800) Description: COM Surrogate Product: Microsoft® Wind
ows® Operating System Company: Microsoft Corporation OriginalFileN
ame: dllhost.exe CommandLine: C:\Windows\system32\DllHost.exe /Pr
ocessid:{7966B4D8-4FDC-4126-A10B-39A3209AD251} CurrentDirecto
ry: C:\Windows\system32\ User: LLC-ITB\sid LogonGuid: {cccca16c-78
15-67c9-d068-080000000000} LogonId: 0x868D0 TerminalSessionId: 1
IntegrityLevel: High Hashes: SHA1=
[45E05A31CBAE71818816EC86AA6152F6D8C22E8C](#),MD5=
[C6723950D1A8CD49D93C8D082B175D41](#),SHA256=
[FFBFD4EA38939327584779F31F46CC8A8AFA0AD03A783A35D1C1
66C335E7B910](#)
,IMPHASH=[CF79FCE90FCED31836373F3E48251A5D](#) ParentProcess
Guid: {cccca16c-7808-67c9-1000-000000000100} ParentProcessId: 58
4 ParentImage: C:\Windows\System32\svchost.exe ParentCommandLi
ne: C:\Windows\system32\svchost.exe -k DcomLaunch -p ParentUser:
NT AUTHORITY\СИСТЕМА

В сообщении упоминается техника **MITRE ATT&CK** под названием **"T1021.003 – Distributed Component Object Model"** (или просто "DCOM"). Эта техника относится к категории **"Lateral Movement"** (поздняя стадия атаки), где злоумышленник использует уязвимости или некорректные настройки для получения доступа к другим системам в сети той же сети.

Рекомендации по минимизации негативного эффекта:

- 1. Установка патчей и обновлений безопасности:** Убедитесь, что все системы защищены последними обновлениями безопасности, включая патчи для устранения известных уязвимостей.
- 2. Настройка политики безопасности:** Проверьте политику безопасности и настройте её таким образом, чтобы предотвратить несанкционированный доступ к компонентам DCOM.
- 3. Мониторинг событий безопасности:** Настройте систему мониторинга событий безопасности, которая будет отслеживать активность, связанную с DCOM, и уведомлять администраторов о подозрительных действиях.
- 4. Контроль учетных записей (ACE):** Ограничьте права пользователей на выполнение задач, которые они не должны выполнять, например, доступ к службам удаленного управления.
- 5. Использование инструментов обнаружения аномалий:** Внедрите инструменты, которые могут автоматически распознавать необычные действия, связанные с DCOM, например, изменение прав доступа или нестандартное поведение процессов.
- 6. Регулярное обучение персонала:** Важно обучать сотрудников основам кибербезопасности, чтобы они могли своевременно реагировать на подозрительные активности.

Эти меры помогут снизить риск успешной реализации атак, использующих DCOM, и

Сообщение, которое ты привел, содержит несколько ключевых элементов, которые можно разобрать по частям для более глубокого понимания:

1. Время и дата события

Сообщение указывает время обнаружения события: **Mar 6 17:33:14**. Это означает, что событие произошло 6 марта в 17 часов 33 минуты и 14 секунд.

2. Тип события

Текст **1: Process Create** говорит о том, что было зафиксировано создание нового процесса в системе. Процесс создается через другую программу, известную как COM Surrogate (**dllhost.exe**), который используется для запуска DLL-библиотек.

3. Анализ детализированного описания события

- Процесс создания:** В сообщении указано, что был создан процесс с именем **dllhost.exe**. Этот процесс используется для выполнения динамически загружаемых библиотек (.dll), которые часто являются библиотеками общего назначения. Он запускается с параметрами командной строки, указывающими на конкретный идентификатор процесса.
- Изменение учетной записи пользователя:** Указаны данные о пользователе, который запустил этот процесс. Пользователь называется **LLC-ITB\sid**, что означает, что процесс был запущен от имени пользователя с таким именем в домене **LLC-ITB**.
- Логин-идентификаторы:** Для идентификации сеанса используются два логина: **SID.llc-itb.local** и **SID.llc-itb.local\sid**. Эти значения уникальны для каждого компьютера и представляют собой идентификаторы безопасности (SID).
- Интеграция уровня доверия:** Интегральный уровень доверия процесса указа



Бессрочные лицензии



Поддержка
территориально распределенных
инсталляций



1000 +
Правил корреляции



В реестре
Минцифры России



Сертифицировано
ФСТЭК России



SECURITY CAPSULE
SIEM
ПЕРВАЯ ОТЕЧЕСТВЕННАЯ



Совместимость с Российскими
операционными системами



Контроль
Active Directory



Развитая
Партнерская
Сеть



Threat Intelligence
F6



Web интерфейс



ИИ ассистент

Бесплатное
онлайн
обучение



Расширенный
Аудит событий

Улучшенная работа
с уязвимостями



ГОССОПКА



СПАСИБО ЗА ВНИМАНИЕ!



Руководитель проекта:

Графов Сергей Александрович

Почта: sag@itb.spb.ru

Телефон: +7 (911) 920-09-87 ([Telegram](#)\WhatsApp)

Мы в соц. сетях:

 [/itb_spb/](#)

 [/itb/](#)

 [/profile/14089663908?lr=2](#)

 [/t.me/ttl_news](#)

Контакты

По общим вопросам: manager@itb.spb.ru

Обучение: learning@itb.spb.ru

Техническая поддержка: support@itb.spb.ru



 Подпишитесь на CRATU — наш исследовательский центр атакующих техник и уязвимостей

Только там: реальные кейсы APT-групп, свежие техники атак, юмор, внутренняя кухня.

Если вы на одной волне с теми, кто пишет правила для SIEM не по бумажке, а по-боевому — вам сюда:

 https://t.me/cratu_team — разведка без галстуков