



SECURITY CAPSULE SIEM

РЕШЕНИЕ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ФИНАЛ

12 марта 2025
«Умный Город» на ВДНХ

Руководитель проекта:
Графов Сергей
Тел. +7 (911) 920-09-87
sag@itb.spb.ru



ПРОБЛЕМАТИКА И ВЫЗОВЫ

- Минцифры: ущерб от **киберпреступлений** в РФ = 160 млрд рублей в год.
- ФСТЭК России: у 47% из 170 организаций, относящихся к КИИ (банки, операторы связи, промышленность и т.д.), состояние защиты от киберугроз находится в **критическом состоянии**.
К типовым недостаткам относится **отсутствие централизованного сбора событий безопасности**.
- InfoWatch: Россия в 2024 году заняла третье место по количеству **утечек** в финансовой отрасли, вслед за США и Индией.
- ПМЭФ 2024: К 2027 году **дефицит кадров** на рынке информационной безопасности России достигнет 60 000 человек.
- С 30 мая 2025 года **увеличение штрафов** за утечку персональных данных.





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



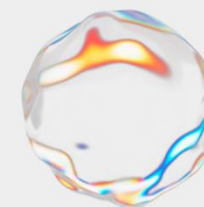
Развитая
Партнерская
Сеть



Threat Intelligence
F6



Web интерфейс



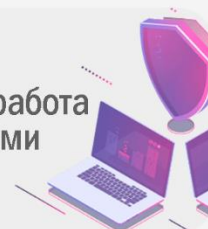
ИИ ассистент
GigaChat

Бесплатное
онлайн
обучение



Расширенный
Аудит событий

Улучшенная работа
с уязвимостями



ГОССОПКА

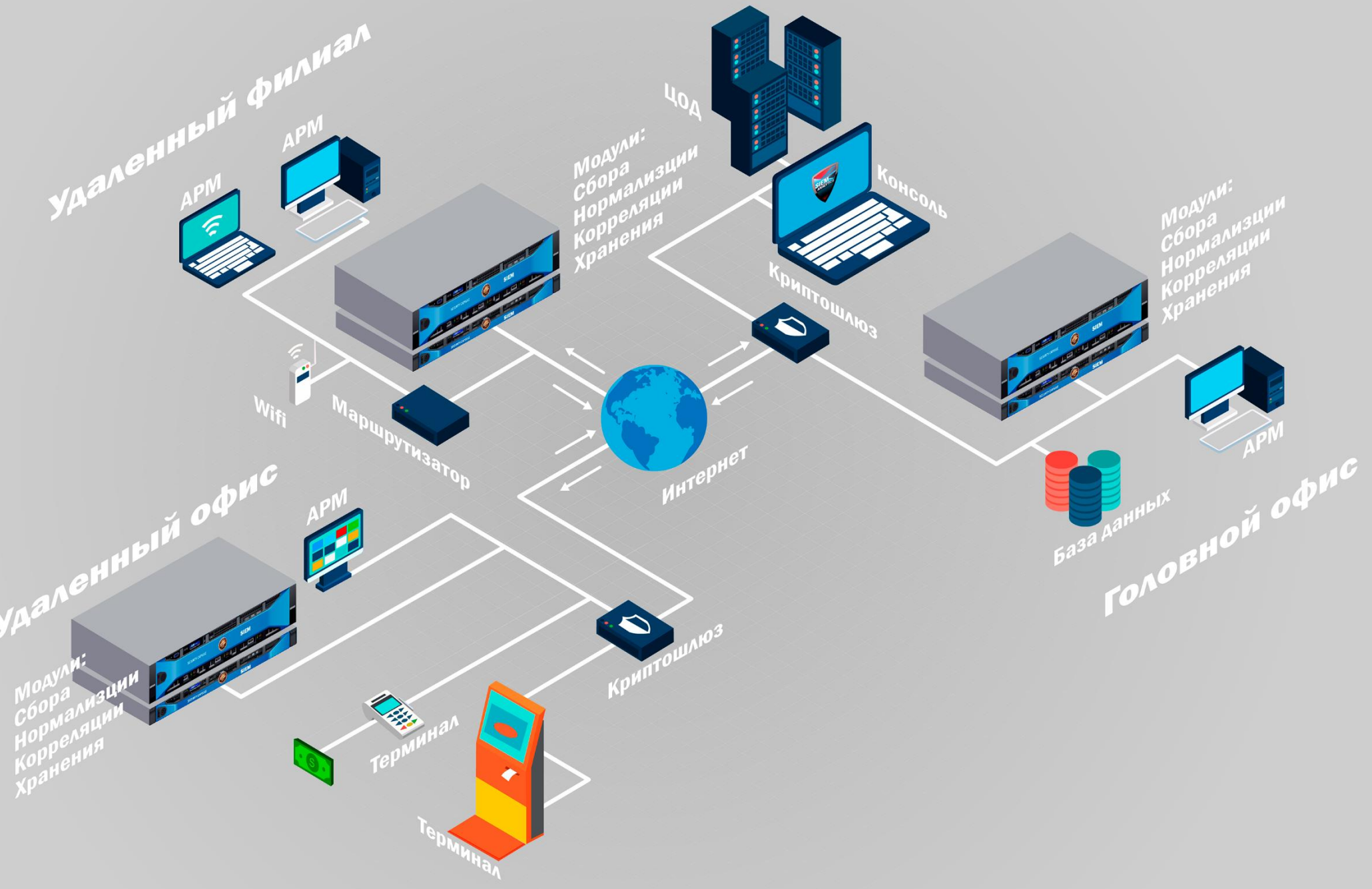




Удаленный филиал

Удаленный офис

Главной офис



Удаленный филиал

- Операционные системы
- Прикладное программное обеспечение
- Системы управления безопасностью баз данных (DBMS)
- Системы мониторинга активности сети (VPN)
- Виртуальные частные сети (VPN)
- Системы анализа защищенности

Удаленный офис

- Антивирусы
- Системы бухгалтерского учета
- Системы предотвращения утечек
- Веб фильтры
- Веб серверы

ЦОД

- IDS/IPS
- Системы управления учетными данными
- Системы управления идентификацией
- Средства виртуализации
- Почтовые фильтры
- Почтовые серверы
- Облачные технологии

Интернет

- Средства защиты информации
- Приложения
- Системы захвата пакетов
- Системы управления сетью
- Системы анализа трафика

- Threat intelligence
- Антивирусы / Анти-спам
- Системы мониторинга сети
- Системы управления сетевым доступом
- Системы управления сетевым трафиком

Головной офис

- Базы данных
- Хранилища
- Сборщики логов



ИИ-АССИСТЕНТ



Использование передовых возможностей генеративных языковых моделей GigaChat 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 configura
ции, 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\dlhhost.exe FileVersion: 10.0.19041.1 (WinBuil
d.160101.0800) Description: COM Surrogate Product: Microsoft® Wind
ows® Operating System Company: Microsoft Corporation OriginalFileN
ame: dlhhost.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

> 40 РЕАЛИЗОВАННЫХ ПРОЕКТОВ

Более чем в 40 системах наши клиенты уже получают преимущества в виде ускоренного реагирования, снижения операционных рисков и обеспечения непрерывности работы критических процессов.

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

2021

АО «ЕИРЦ Петроэлектросбыт»

Ведущий единый информационно-расчетный центр, обеспечивающий эффективное управление расчетами и информационными потоками в сфере энергетики





ФИНАЛ

12 марта 2025
«Умный Город» на ВДНХ



СОЗДАЕМ БУДУЩЕЕ
ОПИРАЯСЬ НА ПРОШЛОЕ
ИНТЕГРИРУЯ В НАСТОЯЩЕЕ

Руководитель проекта:

Графов Сергей

Тел. +7 (911) 920-09-87

sag@itb.spb.ru

