Sber500xGigaChat 2 Batch Top-50:
Product Demo

SECURITY CAPSULE SIEM



ICP Framing & Context

Контекст заказчика и зачем ИИ в SC SIEM

SOC и ИБ-команды тонут не в нехватке сигналов, а в нехватке времени на их первичную интерпретацию и приоритизацию.



Скорость / реакции

Точность / оценки

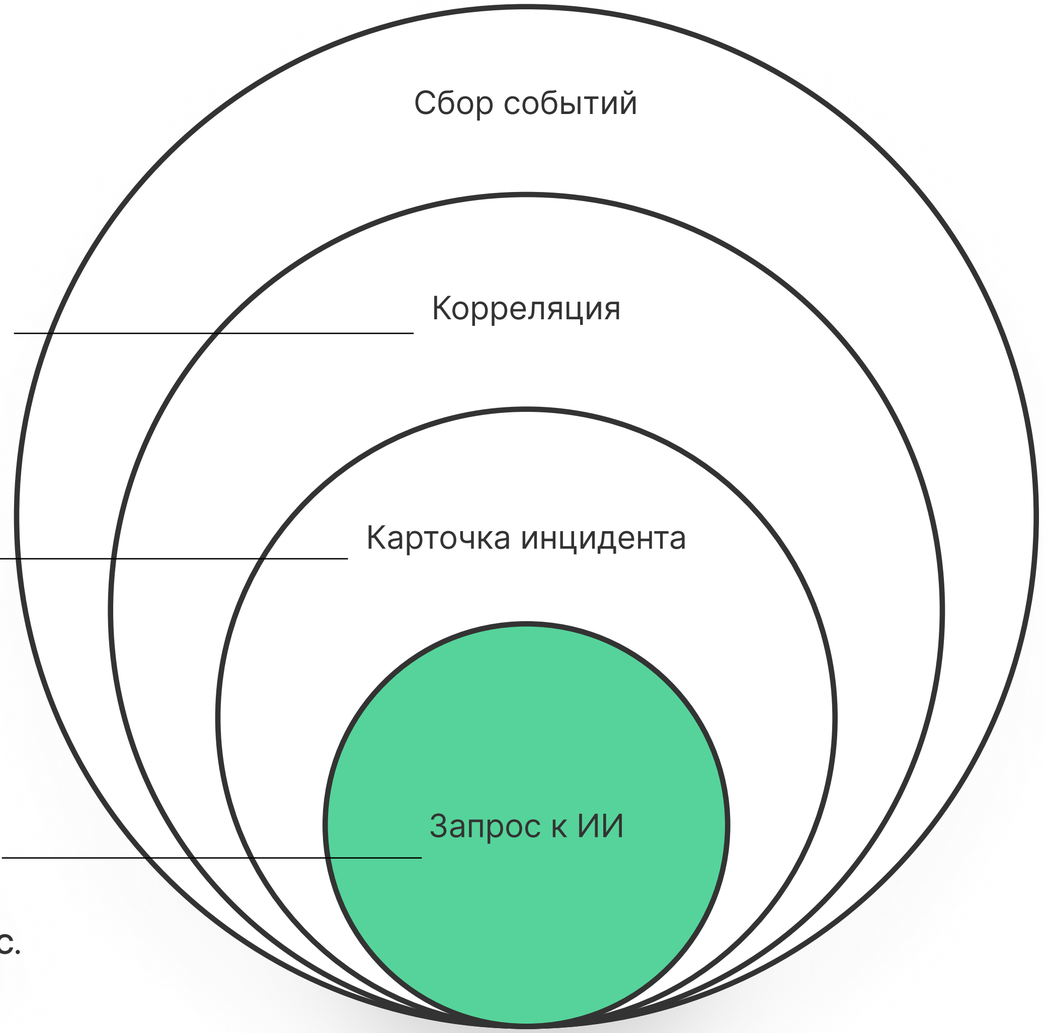
Персонал / затраты

Обучение / затраты

Live Use Case Walkthrough

Живой сценарий: от сигнала к решению оператора

Пример demo-кейса: подозрительная активность пользователя и запуск цепочки действий, которая требует быстрого объяснения



Правила связывают события и формируют инцидент, если видят опасную последовательность действий.

Оператор открывает карточку и видит описание, расследование, управление и связанный контекст.

ИИ встроен в карточку события/инцидента и помогает принять решение там, где оператор уже работает. Мы не уводим пользователя в отдельный чат и не ломаем привычный процесс SOC.

GigaChat in Action

GigaChat в действии: что именно получает оператор

В интерфейсе SC SIEM оператор может запросить несколько типов пояснений по событию или инциденту.

Краткое описание

- быстро объясняет, что произошло

Top 5 и контекст

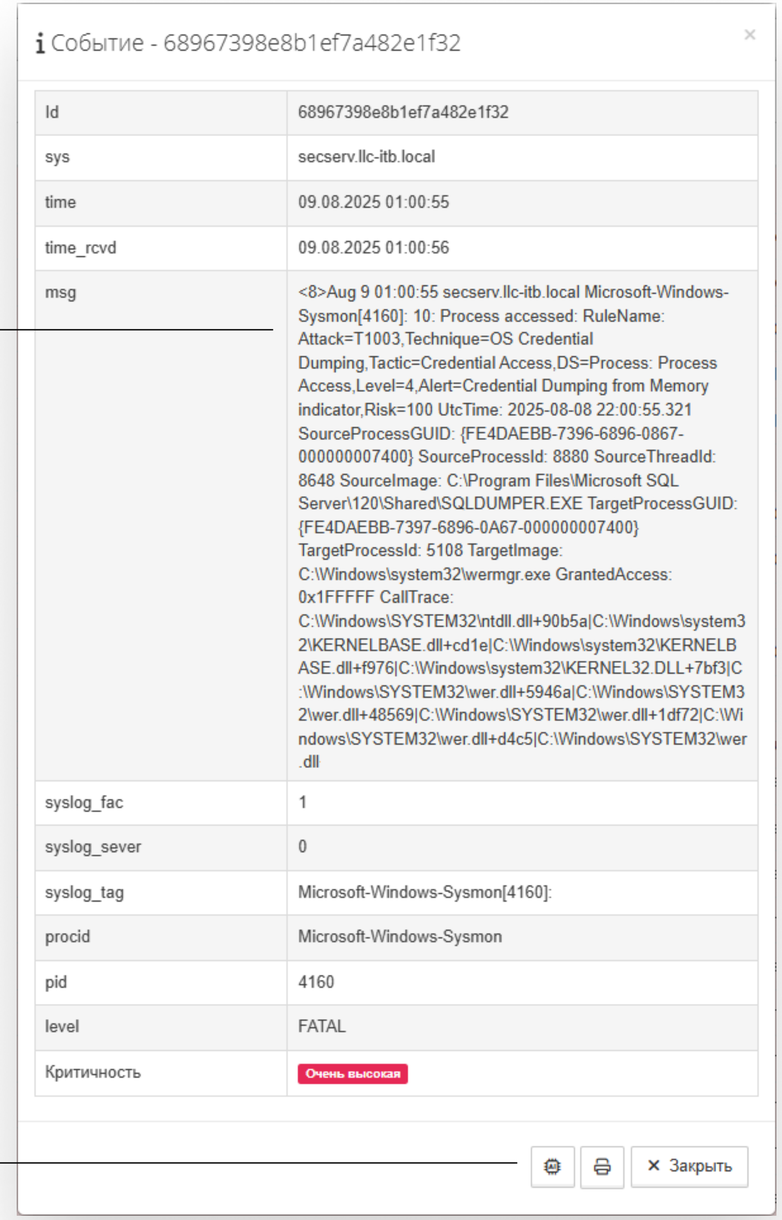
- выделяет ключевые артефакты и факторы

Рекомендации

- подсказывает следующие действия

False positive

- оценивает вероятность ложного срабатывания



Id	68967398e8b1ef7a482e1f32
sys	secserv.llc-itb.local
time	09.08.2025 01:00:55
time_rcvd	09.08.2025 01:00:56
msg	<8>Aug 9 01:00:55 secserv.llc-itb.local Microsoft-Windows-Sysmon[4160]: 10: Process accessed: RuleName: Attack=T1003,Technique=OS Credential Dumping,Tactic=Credential Access,DS=Process: Process Access,Level=4,Alert=Credential Dumping from Memory indicator,Risk=100 UtcTime: 2025-08-08 22:00:55.321 SourceProcessGUID: {FE4DAEBB-7396-6896-0867-000000007400} SourceProcessId: 8880 SourceThreadId: 8648 SourceImage: C:\Program Files\Microsoft SQL Server\120\Shared\SQLDUMPER.EXE TargetProcessGUID: {FE4DAEBB-7397-6896-0A67-000000007400} TargetProcessId: 5108 TargetImage: C:\Windows\system32\wermgr.exe GrantedAccess: 0x1FFFFF CallTrace: C:\Windows\SYSTEM32\ntdll.dll+90b5a|C:\Windows\system32\KERNELBASE.dll+cd1e|C:\Windows\system32\KERNELBASE.dll+f976|C:\Windows\system32\KERNEL32.DLL+7bf3|C:\Windows\SYSTEM32\wer.dll+5946a|C:\Windows\SYSTEM32\wer.dll+48569|C:\Windows\SYSTEM32\wer.dll+1df72|C:\Windows\SYSTEM32\wer.dll+d4c5|C:\Windows\SYSTEM32\wer.dll
syslog_fac	1
syslog_sever	0
syslog_tag	Microsoft-Windows-Sysmon[4160]:
procid	Microsoft-Windows-Sysmon
pid	4160
level	FATAL
Критичность	Очень высокая


Справка от ИИ - Краткое описание
Сообщение указывает на обнаружение подключения нового устройства (название со
бытия "Подключение дополнительных устройств"). Это классифицируется как аппара
тное событие с высоким приоритетом. Событие зафиксировано программой Sysmon,
которая отслеживает системные активности в операционной системе Windows. Инфо
рмация передается через протокол UDP на адрес 192.168.1.2:514.

Справка от ИИ - Подробное описание

Это сообщение относится к системе мониторинга безопасности и содержит детали о б обнаруженных событиях, связанных с работой операционной системы Windows. Во т подробное объяснение каждой части сообщения:

1. Время и дата

- **Дата:** 9 апреля (Apr)
- **Время:** 17:21:54 (часы:минуты:секунды)

2. Идентификатор процесса Sysmon

- **ProcessGuid:** {4a53bcb9-1b9d-67f6-dfd2-000000006900}
- **ProcessId:** 8480
- **Image:** C:\WINDOWS\Explorer.EXE

Процесс `C:\WINDOWS\Explorer.EXE` является основным процессом проводника Windo ws, который отвечает за взаимодействие пользователя с интерфейсом операционно й системы.

3. Классификация события

- **Классификация:** "Hardware Event"
- **Приоритет:** 1 (важное событие)

Это означает, что произошло событие, связанное с аппаратным обеспечением.

4. Событие Sysmon

- **EventType:** CreateKey

EventType `CreateKey` указывает на то, что был создан новый ключ в реестре Window s. В данном случае этот ключ находится по пути:

```
HKU\S-1-5-21-677228384-831708996-13535863-1655\SOFTWARE\Microsoft\Windows\CurrentVe rsion\Explorer\MountPoints2
```

5. Обнаруженное устройство

- **Описание:** "Подключение дополнительных устройств"
- **Тип устройства:** Mountpoints2
- **Действие:** "Обнаружено подключение нового устройства"

Эти строки указывают на то, что система обнаружила новое устройство, которое исп ользует запись в реестре `MountPoints2`. Этот раздел реестра используется для хран ения информации о монтированных устройствах, таких как съемные диски или сетев ые папки.

6. Источник сообщения

- **Программа:** Microsoft-Windows-Sysmon
- **Транспортный протокол:** UDP
- **IP-адреса:** 192.168.1.2

Sysmon — это системная утилита, которая собирает информацию о различных дейст виях, происходящих в системе, и отправляет их на указанный сервер для анализа. В данном случае, сообщение отправляется через протокол UDP с использованием IP-а дресов 192.168.1.2.

7. Пользователь, выполнивший действие

- **Пользователь:** LLC-ITB\suter

Здесь указано имя пользователя, который произвел действия, приведшие к создани ю нового ключа в реестре.

Таким образом, это сообщение говорит о том, что была создана новая запись в реес тре, связанная с подключенным устройством (`MountPoints2`), а также о том, что проц есс проводника Windows участвовал в этом событии.

Справка от ИИ - Рекомендации

В сообщении упоминается техника **MITRE ATT&CK** под названием **"Hardware Additi ons" (T1200)**. Эта техника относится к категории **Initial Access** и включает установку новых аппаратных компонентов для последующего использования в атаке.

Рекомендации по минимизации негативного эффекта:

1. **Мониторинг активности USB-портов**: Регулярный мониторинг подключения новых USB-устройств с помощью Sysmon или других инструментов может выя вить аномальные действия, связанные с подключением новых устройств. Это поможет предотвратить несанкционированное использование USB-портов зло умышленниками.
2. **Политики безопасности USB-устройств**: Настройка политик безопасности, о граничивающих доступ к USB-портам только авторизованным пользователям или приложениям, может значительно снизить риск атак через подключенные устройства.
3. **Ограничение доступа к реестру**: Контроль доступа к системному реестру так же важен для защиты от потенциального внедрения вредоносного ПО через д обавление ключей или изменения в реестре.
4. **Регулярное обновление программного обеспечения**: Установка последних патчей безопасности и обновлений операционной системы и приложений пом огает устранить уязвимости, которые могут быть использованы злоумышленни ками для проведения подобных атак.
5. **Использование антивирусного ПО**: Использование современных решений д ля защиты от вредоносного ПО может обнаружить и заблокировать попытки ус тановки или использования новых устройств в системе.
6. **Логирование и анализ событий**: Ведение логов и регулярный анализ событи й, связанных с подключением устройств, позволяет оперативно реагировать н а подозрительные действия и предпринимать меры по их устранению.

Эти меры помогут уменьшить вероятность успешной атаки через подключение новы х устройств и повысить уровень безопасности вашей инфраструктуры.

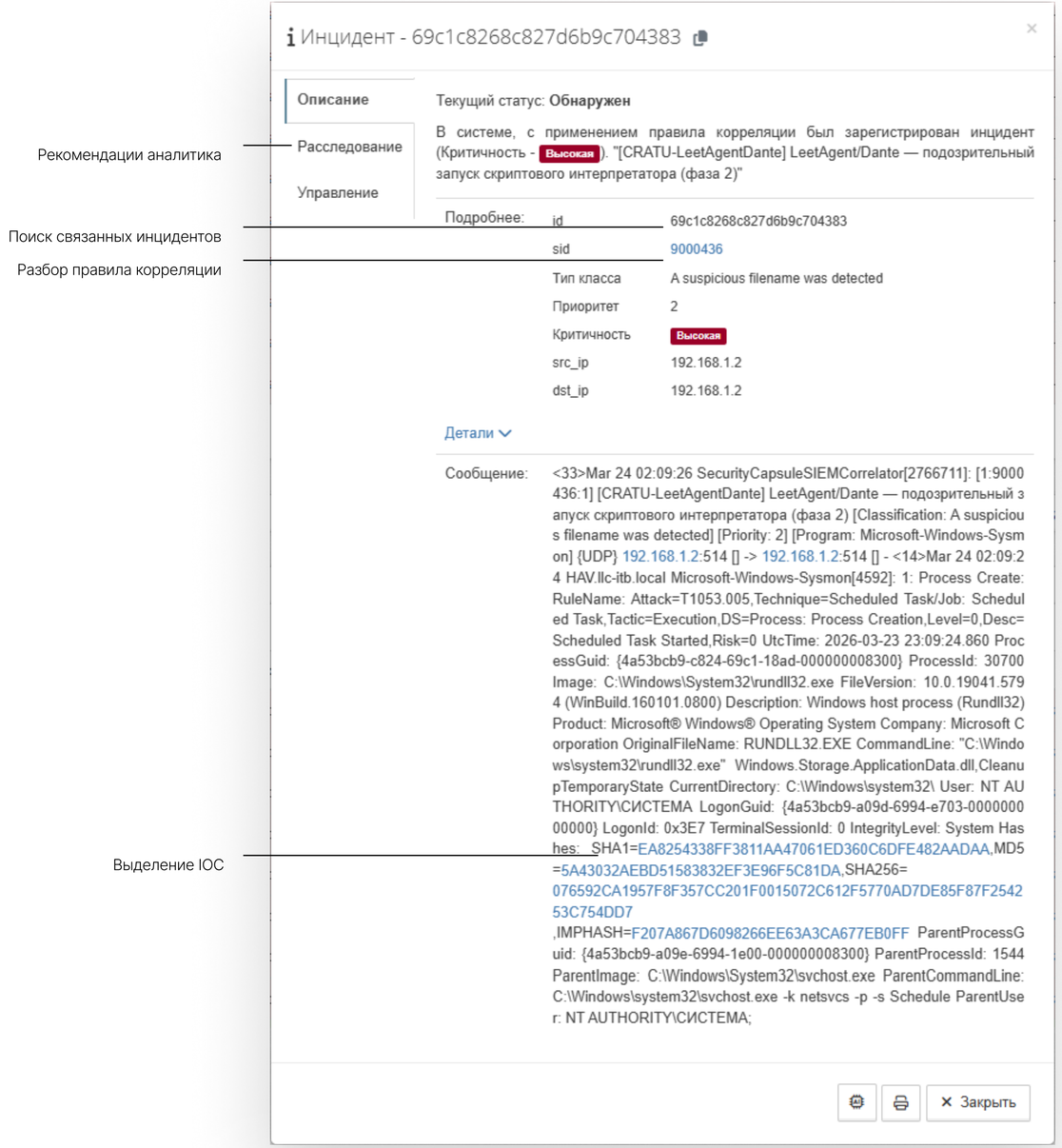
GigaChat in Action

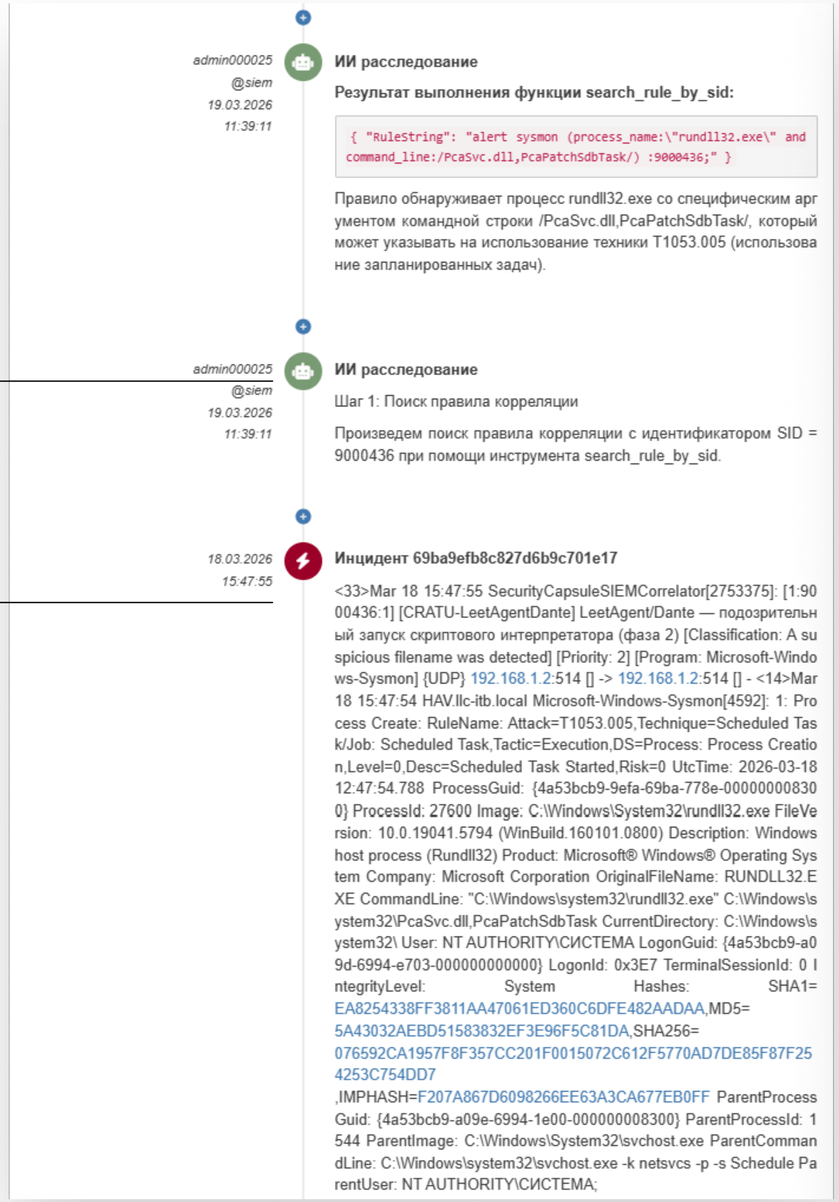
Первая итерация ИИ-расследования инцидента

В рамках Sber500 мы реализовали первый сценарий, в котором ИИ-ассистент не только объясняет alert, но и проводит первичное расследование прямо в карточке инцидента.

Что делает ИИ

- анализирует правило корреляции
- выделяет IOC
- ищет связанный контекст
- формирует рекомендации





admin000025
@siem
19.03.2026
11:39:11

ИИ расследование

Результат выполнения функции search_rule_by_sid:

```
{ "RuleString": "alert sysmon (process_name:\"rundll32.exe\" and command_line:/PcaSvc.dll,PcaPatchSdbTask/) :9000436;" }
```

Правило обнаруживает процесс rundll32.exe со специфическим аргументом командной строки /PcaSvc.dll,PcaPatchSdbTask/, который может указывать на использование техники T1053.005 (использование запланированных задач).

admin000025
@siem
19.03.2026
11:39:11

ИИ расследование

Шаг 1: Поиск правила корреляции

Произведем поиск правила корреляции с идентификатором SID = 9000436 при помощи инструмента search_rule_by_sid.

18.03.2026
15:47:55

Инцидент 69ba9efb8c827d6b9c701e17

<33>Mar 18 15:47:55 SecurityCapsuleSIEMCorrelator[2753375]: [1:9000436:1] [CRATU-LeetAgentDante] LeetAgent/Dante — подозрительный запуск скриптового интерпретатора (фаза 2) [Classification: A suspicious filename was detected] [Priority: 2] [Program: Microsoft-Windows-Sysmon] {UDP} 192.168.1.2:514 [] -> 192.168.1.2:514 [] - <14>Mar 18 15:47:54 HAV.llc-itb.local Microsoft-Windows-Sysmon[4592]: 1: Process Create: RuleName: Attack=T1053.005,Technique=Scheduled Task/Job: Scheduled Task,Tactic=Execution,DS=Process: Process Creation,Level=0,Desc=Scheduled Task Started,Risk=0 UtcTime: 2026-03-18 12:47:54.788 ProcessGuid: {4a53bcb9-9efa-69ba-778e-000000008300} ProcessId: 27600 Image: C:\Windows\System32\rundll32.exe FileVersion: 10.0.19041.5794 (WinBuild.160101.0800) Description: Windows host process (Rundll32) Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: RUNDLL32.EXE CommandLine: "C:\Windows\system32\rundll32.exe" C:\Windows\system32\PcaSvc.dll,PcaPatchSdbTask CurrentDirectory: C:\Windows\system32\ User: NT AUTHORITY\СИСТЕМА LogonGuid: {4a53bcb9-a09d-6994-e703-000000000000} LogonId: 0x3E7 TerminalSessionId: 0 IntegrityLevel: System Hashes: SHA1=EA8254338FF3811AA47061ED360C6DFE482AADAA,MD5=5A43032AEBD51583832EF3E96F5C81DA,SHA256=076592CA1957F8F357CC201F0015072C612F5770AD7DE85F87F254253C754DD7,IMPHASH=F207A867D6098266EE63A3CA677EB0FF ParentProcessGuid: {4a53bcb9-a09e-6994-1e00-000000008300} ParentProcessId: 1544 ParentImage: C:\Windows\System32\svchost.exe ParentCommandLine: C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule ParentUser: NT AUTHORITY\СИСТЕМА;

admin000025
@siem
19.03.2026
11:39:11

ИИ расследование

Шаг 4: Рекомендации по времени поиска событий

Исходя из того, что правило использует источник данных Sysmon, учитывает запуск процесса rundll32.exe, и связанно с правилом корреляции рекомендуется искать события за последние 2 часа, что бы выявить потенциальные аномалии или дополнительные активности, связанные с этим процессом или техникой атаки.

admin000025
@siem
19.03.2026
11:39:11

ИИ расследование

В базе данный индикаторов уязвимостей обнаруженны связанные индикаторы:

```
{ "SHA-256": "e3060223977da8f21e95f6df338863429d0d547e68063658c875b629e27d4b6f", "report_refs": ["https://en.wikipedia.org/wiki/Mirai_(malware)", "https://researchcenter.paloaltonetworks.com/2018/09/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/"] }
```

Сработавшие движки Lionic (malicious): Trojan.Linux.Mirai.K!cElastic (malicious): Linux.Trojan.MiraiMicroWorld-eScan (malicious): Trojan.Linux.Mirai.1

admin000025
@siem
19.03.2026
11:39:11

ИИ расследование

Шаг 3: Индикаторы компрометации

Из текста инцидента выделим возможные индикаторы компрометации:

- IP адрес: 192.168.1.2
- Имя домена: HAV.llc-itb.local
- Хеши файла rundll32.exe:
  - SHA1: EA8254338FF3811AA47061ED360C6DFE482AADAA
  - MD5: 5A43032AEBD51583832EF3E96F5C81DA
  - SHA256: 076592CA1957F8F357CC201F0015072C612F5770AD7DE85F87F254253C754DD7
  - IMPHASH: F207A867D6098266EE63A3CA677EB0FF

Эти данные могут быть использованы для дальнейшего анализа и сопоставления с известными угрозами.

admin000025
@siem
19.03.2026
11:39:11

ИИ расследование

Шаг 2: Анализ правила корреляции

Правило обнаруживает подозрительные процессы rundll32.exe, запущенные с использованием PcaSvc.dll и задачи PcaPatchSdbTask. Это правило нацелено на выявление использования легитимных инструментов операционной системы Windows (в данном случае rundll32.exe) для скрытного выполнения кода или запуска вредоносных действий через запланированные задачи.

Шаг 1
Поиск правила корреляции

Исходный инцидент

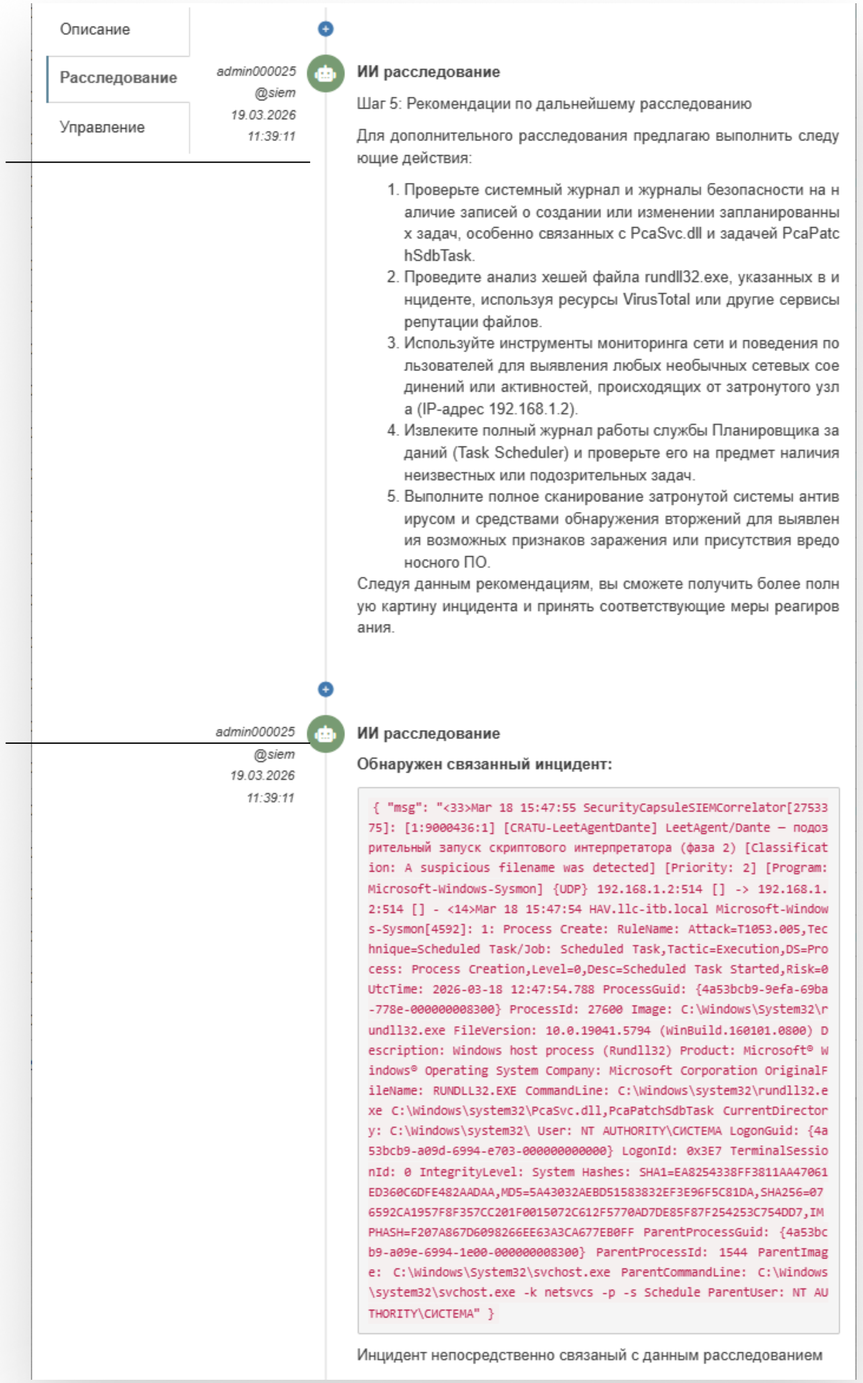
Шаг 4
Рекомендации по поиску связанных событий

Шаг 3
Поиск индикаторов компрометации

Шаг 2
Анализа правила корреляции

Шаг 5
Рекомендации по дальнейшему расследованию

Обнаружен связанный инцидент



Outcome & Value

Результат и ценность для заказчика

- быстрее первичный разбор событий и инцидентов
- снижение порога входа для новых операторов
- меньше времени на объяснение, больше времени на реагирование

−27,6%
Скорость реакции

−26,8%
Скорость разбора

82,8%
Полезные ответы

7,8%
Чистый эффект

Product Edge

Продуктовое преимущество SC SIEM

SC SIEM не просто находит инцидент, а помогает быстрее его понять и правильно отработать.

