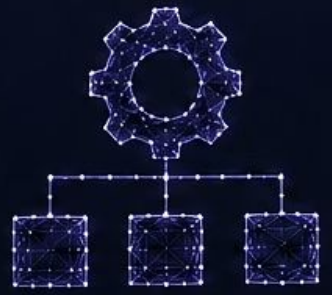
Мотивация: зачем, что и как

Зачем?

Снизить рутинную нагрузку аналитика и повысить качество и скорость разбора инцидентов кибербезопасности.

Что?

Создаём индивидуального помощника на базе Ouroboros для предварительного разбора инцидентов.



Как?

Разрабатываем собственную библиотеку навыков и формируем структурированный отчёт на основе входных данных.

Почему это важно

Реальные инциденты кибербезопасности приводят к сбоям в работе бизнеса, операционным потерям и финансовому ущербу.

- «Аэрофлот» — сбои сервисов и задержки рейсов, убытки оцениваются в **250 млн** руб.
- «СДЭК» — остановка сервисов и операционный ущерб, потери оцениваются в **300 млн–1 млрд** руб.
- SOC перегружен типовыми сетевыми инцидентами и ручной рутиной.
- Рутинная проверка забирает время, которое необходимо для работы с реальными угрозами кибербезопасности.

SOC — Security Operations Center · NDR — система обнаружения сетевых инцидентов · ЛПС — ложноположительное срабатывание

Отчёт о результатах фазы MVP

Заявлено → выполнено: все обязательства Project Proposal закрыты

От реактивной к проактивной кибербезопасности*

Единый маршрут обработки, структурированный отчёт, накопление знаний и эволюция.
Финальное решение — за аналитиком.

1. **Навык обогащения контекста**
   ourosoc-enrich
2. **Навык оценки актуальности / ЛПС**
   ourosoc-relevance
3. **Навык корреляции инцидентов**
   ourosoc-correlation
4. **Навык формирования отчёта**
   ourosoc-investigation-pack
5. **Оркестрация цикла обработки**
   ourosoc-analyst
6. **Цикл обратной связи**
7. **Демо-набор: 10 инцидентов**

Замечание аналитика → Обновление навыка → Следующий цикл лучше → Качество ответа растёт

- В тестовых циклах агент регулярно получал обратную связь аналитика.
- На её основе навыки улучшались и реже повторяли ошибки на похожих кейсах.
- Именно этот механизм был основным способом отладки и улучшения MVP.

** Сергей Лебедь, вице-президент «Сбера» по кибербезопасности, газета «Ведомости», 18.02.2026*

Как работает: один цикл агента, каждая функция — навык

1. Аналитик SOC

JSON сетевого инцидента кибербезопасности

Работа агента · оркестрация маршрута 3 → 4 → 5 → 6

2. ourosoc-analyst

3. ourosoc-enrich

4. ourosoc-relevance

5. ourosoc-correlation

6. ourosoc-investigation-pack

7. Аналитик SOC

Финальное решение

Обратная связь аналитика → правка навыка → review → следующий разбор лучше

Skills

5 семантических навыков: install → review → enable. Эволюционируют навыки, а не ядро.

MCP

3 read-only сервера: ndr-mcp, asset-registry, confluence-mcp

A2A

Корреляция текущего инцидента через внешнего агента ситуационной осведомлённости SOC.

Обратная связь

Замечание аналитика преобразуется в измеримое улучшение поведения навыка.

Routing моделей

Основная модель исполняет навык. Отдельная модельная линия выполняет review навыков и контроль качества.

LLM-модели, использованные при разработке и тестировании

Main
GLM 5.2

Review
GLM 5.2 · MiniMax M3 · Qwen3.6-35B

Fallback
Qwen3.6-35B

Результаты проверки: 10 инцидентов против эталона аналитика

Результаты агента сравнивались с эталонами, вручную подготовленными SOC-аналитиком

Оценка по реальным сценариям: классификация, уверенность, ключевые факты и пробелы в данных

Как проверяли

1. 10 инцидентов по 5 типовым правилам NDR.
   Для каждого сценария использовались один актуальный инцидент и одно ложное срабатывание.
2. SOC-аналитик вручную подготовил эталон для каждого инцидента.
3. Независимая LLM-судья оценила ответы агента по шкале от 0 до 100.

Учитывались классификация, уверенность, решающие факты, пробелы в данных и отсутствие выдуманных сведений.

Результат

10/10

Классификация совпала с эталоном во всех случаях

95/100

Средняя точность сформированных отчётов

Агент корректно обработал все 10 тестовых инцидентов и в среднем набрал 95 баллов из 100 при сравнении с эталоном аналитика.
Качество подтверждено на реальных сценариях разбора инцидентов.

Результат работы агентной системы

Пример итогового отчёта по инциденту, сформированного агентом для аналитика SOC

NET-01

Classification: relevant Confidence: medium

КРАТКОЕ РЕЗЮМЕ

Сработало правило NDR_MONTH_SIMPLE_LDAP_AD_Large_Response: рабочая станция wks-ivanov (10.32.5.50) за 12 минут выгрузила 48 MB LDAP-данных с контроллера домена tvlds-dc0001 (10.16.3.30:389/TCP), используя пользовательскую учётную запись ivanov-ii@DELTA.SBRF.RU. Предварительная классификация — relevant (Нереализованный инцидент / Сетевое сканирование или Попытки разглашения информации) уровнем доверия medium: картина соответствует сценарию «Инцидент» плейбука — рабочая станция, не являющаяся системой IAM/IDM/CMDB, получила массовую выгрузку каталога от DC.

Аргументы за

- Hostname источника 'wks-ivanov' — пользовательская рабочая станция, не IAM/IDM/CMDB/мониторинг AD
- Объём ответа 48 MB при запросе 120 KB (асимметрия 400:1) — массовая выгрузка каталога
- Kerberos-учётка 'ivanov-ii@DELTA.SBRF.RU' — пользовательская, не сервисная
- MITRE тактика 7 (Discovery) и техника 1087 (Account Discovery) — AD-разведка
- Источник 10.32.5.50 не найден в реестре активов

Аргументы против

Опровергающих аргументов не найдено

ИСТОЧНИКИ ДАННЫХ

NDR NDR_MONTH_SIMPLE_LDAP_AD_Large_Response

СЕТЕВЫЕ СЕССИИ

ВРЕМЯ НАЧАЛА	ВРЕМЯ КОНЦА	ИСТОЧНИК	НАЗНАЧЕНИЕ	ПОРТ	ПРОТОКОЛ	ЗАПРОС (KB)	ОТВЕТ (MB)
09:00:00	09:12:00	10.32.5.50 (wks-ivanov)	10.16.3.30 (tvlds-dc0001)	389/TCP	LDAP	120	48

КОРРЕЛЯЦИИ

NET-01 → NET-101 → NET-102

Связь по совпадению rule_id (NDR_MONTH_SIMPLE_LDAP_AD_Large_Response), confidence: low

Пробелы (Gaps)

- Подтверждение владельца хоста 10.32.5.50 о легитимности и наличии ЗНИ/ЗНО — требует ручного запроса
- Отсутствие записи в реестре активов для 10.32.5.50 не доказывает нелегитимность (по заявлению реестра)
- Назначение 10.16.3.30 (tvlds-dc0001) не подтверждено формально через реестр активов

Рекомендации аналитику

1. Запросить владельца хоста 10.32.5.50 о наличии ЗНИ/ЗНО на LDAP-выгрузку
2. Проверить в реестре активов, является ли 10.16.3.30 контроллером домена
3. При неподтверждённой активности — изолировать хост 10.32.5.50
4. Заблокировать учётную запись ivanov-ii@DELTA.SBRF.RU
5. Проверить связанные инциденты NET-101 и NET-102
6. Передать на следующую линию поддержки с этим Investigation Pack

Пример тестового HTML-шаблона. Структура и оформление итогового отчёта могут отличаться.

Почему именно Ouroboros

Управляемый маршрут разбора

Явная цепочка шагов: сбор контекста → оценка → корреляция → отчёт.

Технологии в реальном SOC-процессе

Skills, MCP и A2A встроены в предварительный разбор инцидентов и работают с контекстом, инструкциями и связями между кейсами.

Контролируемая эволюция

Меняются навыки, а не ядро. Обратная связь проходит через review, enable и подтверждение человеком.

Эволюционность в работе

- Ошибка не повторяется на похожих кейсах.
- Качество ответов улучшается.
- Накопление знаний остаётся под контролем человека.

Почему это важно для кибербезопасности

- Единый стандарт предварительного разбора
- Меньше ручной рутины в типовых кейсах
- Масштабирование через навыки и источники контекста

Для SOC важен воспроизводимый процесс, который учится на замечаниях аналитика и остаётся под контролем человека.

Дальнейшее развитие: от MVP к проактивной защите SOC

Паспорт решения

Оценка по критериям

- Сложность — 3/5
- Автономность — 4/5
- Интерпретируемость — 5/5
- Готовность к внедрению — 4/5

1 • MVP — сделано

- Собираем всю необходимую информацию по каждому инциденту.
- Пять простых навыков работают по понятным шагам.
- Есть связь с человеком и обратная связь.

2 • Пилот

- Автоматически анализируем инциденты и ставим их в очередь.
- Используем данные из реальных систем.
- Создаём единую базу знаний.

3 • Расширение SOC

- Подключаем больше систем кибербезопасности для анализа.
- Добавляем новые типы инцидентов: устройства, пользователи, приложения и сервисы.

4 • Масштабирование в банке

- Поддержка разных линий и подразделений.
- Расширяем набор навыков, не усложняя ядро.
- Формируем ядро проактивной защиты и устранения рисков.

Следующий этап — превратить MVP в устойчивый контур накопления знаний и проактивной защиты