КРЕДО-С
системный интегратор

ОТ WAZUH ДО ПРИКАЗА №117: РЕАЛЬНАЯ СТОИМОСТЬ «БЕСПЛАТНОГО» SOC

Конференция

2026

Регламенты напишем потом, когда появится время

Жизненный цикл инцидента станет 1 час

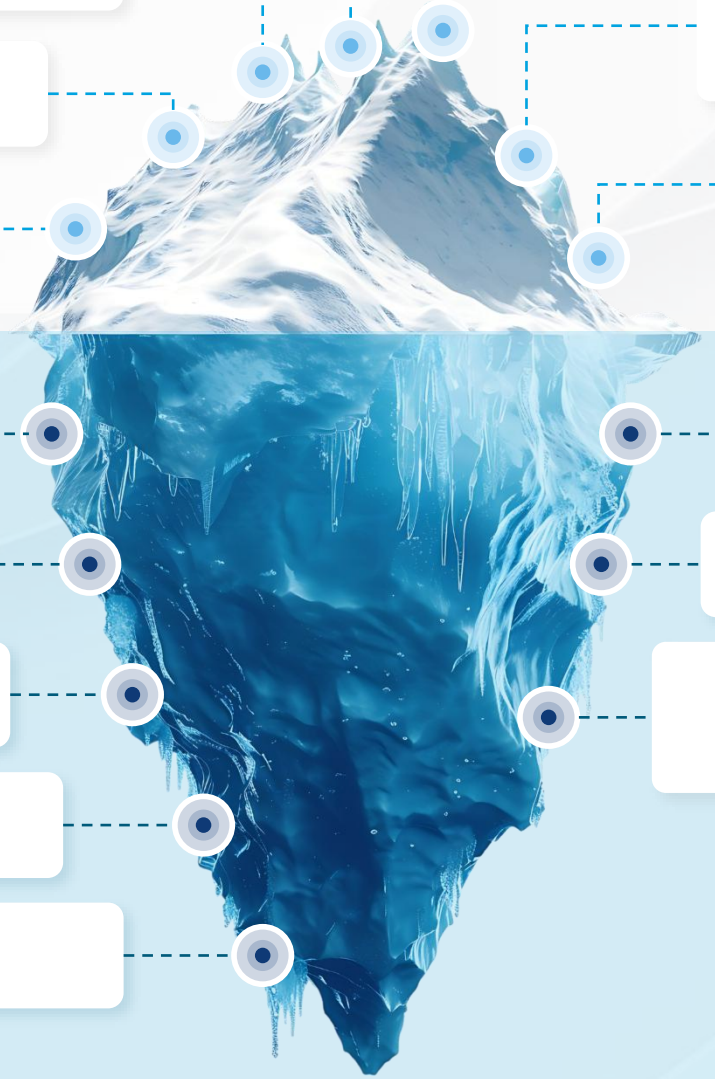
Свои ребята всё настроят за выходные

Будем мониторить события

Наймём двух студентов на позицию L1 Аналитика – будут выявлять атаки

Wazuh — это же готовый SOC, просто поставим и забудем

Ни один хакер не проберется



0 алертов за неделю

15 000 алертов за неделю

ФОТ вырос на 30 млн в год…

Декодер под 1С пишется третью неделю

Согласование блокировки длится 4 часа

Playbook пишет ChatGPT…

Учения не проводились ни разу

SIEM начала терять события на пиковой нагрузке

КРЕДО-С

Три столпа эффективного SOC

КРЕДО-С

Столп 1: Люди

- 2 взаимозаменяемых Senior-специалиста, DevOps SOC;
- Мониторинг 24/7: 5-7 специалистов 1-2 линий;
- Обучение/повышение квалификации.

Команда — это не зарплаты, а система сменности, передачи контекста и удержания

Столп 2: Технологии

- SIEM;
- NTA;
- IRP/SOAR;
- XDR.

Инструменты без правильной архитектуры и интеграций — это просто сбор логов

Столп 3: Процессы

- Playbook’и реагирования;
- SLA;
- Установленные процедуры эскалации;
- Регулярная отработка «А что мы будем делать если…?».

Процессы превращают инструменты и людей в предсказуемую систему

Люди: роли и требования

КРЕДО-С

Роль	Обязанности	Требуемые качества и компетенции
L1-аналитик	24/7 мониторинг, первичная фильтрация ложных срабатываний.	Стрессоустойчивость, внимание к деталям, базовые знания ИБ.
L2-аналитик	Расследование инцидентов, охота за угрозами (threat hunting), работа с EDR, форензика.	Глубокие знания ТТП атак, опыт работы с SIEM/EDR, навыки анализа.
L3 / архитектор	Разработка правил корреляции, написание декодеров, проектирование архитектуры SOC, интеграция с инфраструктурой.	Опыт проектирования SOC, знание стеков ELK/OpenSearch, Wazuh internals.
DevOps SOC	Поддержка инфраструктуры: кластер OpenSearch, Kafka, балансировщики, резервное копирование, обновления, мониторинг производительности.	Навыки администрирования высоконагруженных систем, автоматизация (Ansible, Terraform).

Люди: расчет затрат

КРЕДО-С

Роль	Расчет затрат	Сумма (руб./год)
Заработная плата (на руки)	Первая линия: 40 000 – 100 000 ₽/мес. × 12	480 000 – 1 200 000 ₽ 900 000 – 2 160 000 ₽ 1 560 000 – 3 600 000 ₽
	Вторая линия: 75 000 – 180 000 ₽/мес. × 12	
	Третья линия/Архитектор: 130 000 – 300 000 ₽/мес. × 12	
Налоги (НДФЛ + страховые взносы)	~43% от ФОТ	
Соцпакет (ДНС, обучение, сертификации, корпоративные мероприятия)	15 000 ₽/мес. × 12	180 000 ₽
Инфраструктура (рабочее место, лицензии ПО, оборудование)	10 000 ₽/мес. × 12	120 000 ₽

Высокая сложность качественной эксплуатации

КРЕДО-С

1. Отсутствие технической поддержки
2. Не сертифицирован ФСТЭК
3. Сырой продукт из коробки
4. Отсутствие квалифицированного сайзинга
5. Высокий порог вхождения в эксплуатацию

Технологический стек зрелого SOC: SIEM – это только начало

1. SIEM
2. IRP
3. NTA
4. XDR

Процессы: организационная зрелость SOC

КРЕДО-С

- Playbook (инструкции)
- Учения (отработка инцидентов)
- Распределение ролей и ответственности
- Контроль качества
- Интеграция с IT / Бизнесом
- Формализация

Свой vs Внешний: честное сравнение

КРЕДО-С

Внешний SOC

- Предсказуемый бюджет.
- Доступ к качественной внешней экспертизе.
- Мониторинг 24/7.
- Отсутствие капитальных вложений.

- Непрозрачность процесса мониторинга.

Свой SOC

- Быстрая эскалация.
- Контроль всего жизненного цикла инцидента.
- Расширение штата специалистов по ИБ.
- Полный контроль над инфраструктурой, правилами, регламентами.

- Высокая стоимость содержания (ФОТ + лицензии).
- Дефицит/текучка кадров.
- Сложность первоначальной интеграции в процессы ИБ компании.
- При необходимости закупки «железа» — большие капитальные затраты.

Когда пора звать внешнюю экспертизу?

КРЕДО-С

1

Наличие регуляторных требований

2

Уровень зрелости ИБ в компании

3

Недостаток бюджета

4

Отсутствие квалифицированной команды

Почему выбирают наш SOC?

КРЕДО-С

30+ лет практического опыта в сфере ИБ и ИТ

ТОП-20 ведущих частных интеграторов на рынке ИБ по версии TAdviser

70+ экспертов в штате компании

1 000+ реализовано успешных проектов

Глубокая экспертиза и проверенный опыт команды SOC

Быстрое внедрение

Гибкая модель

Фокус на российском регулировании

Получите демонстрацию решения нашего центра мониторинга

Мы знаем вашу ИТ-инфраструктуру (как интегратор ИБ), поэтому быстрее понимаем контекст инцидентов

ОСТАЛИСЬ ВОПРОСЫ?

Телефон: (4872) 71-71-74, доб. 772
Мобильный: +7 (963) 932-92-61
Почта: d.eliseev@credos.ru

Спасибо

КРЕДО-С
системный интегратор

www.credos.ru

Подписывайтесь на наш Телеграм-канал, чтобы знать больше про ИБ