// ВВЕДЕНИЕ

ЧТО ТАКОЕ SIEM?

ОПРЕДЕЛЕНИЕ

Security Information and Event Management (SIEM) объединяет сбор логов в реальном времени, обнаружение угроз и реагирование на инциденты в единую платформу для команд по безопасности.



КАК ЭТО РАБОТАЕТ

SIEM агрегирует логи с каждого устройства, сервера, приложения и сети в организации — коррелирует события по правилам и с использованием AI, чтобы обнаруживать угрозы, которые не смог бы выявить ни один отдельный инструмент.



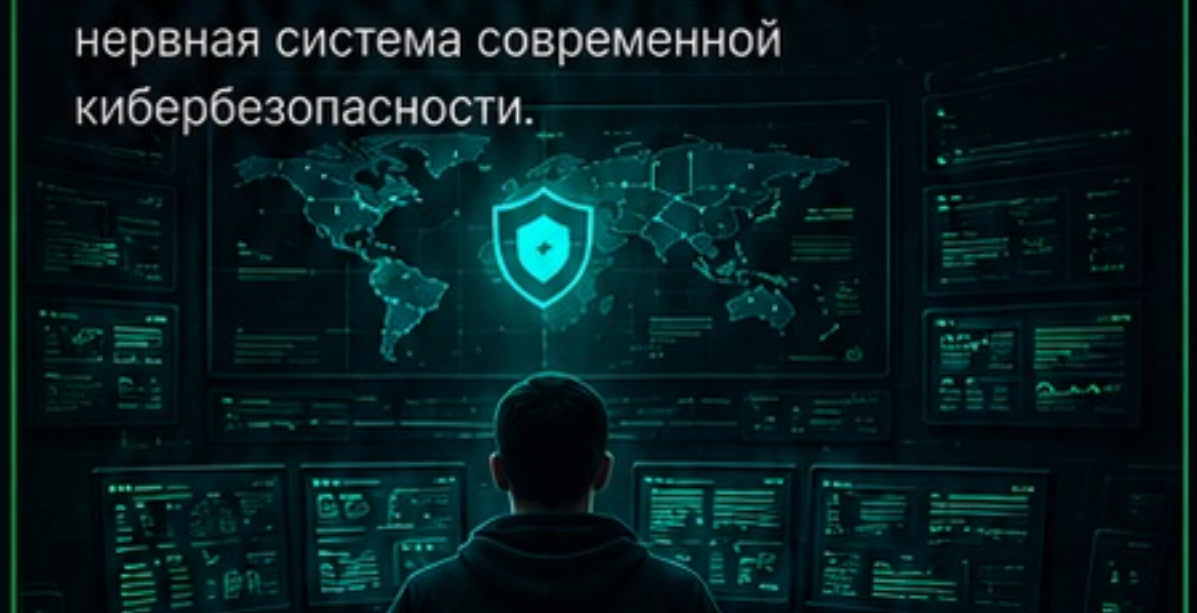
ПОЧЕМУ ЭТО ВАЖНО

В среднем утечку обнаруживают через 207 дней без SIEM.
При правильном внедрении SIEM команды безопасности обнаруживают угрозы за минуты — и реагируют до того, как ущерб становится катастрофическим.



КТО ИСПОЛЬЗУЕТ

Любой Enterprise SOC (Security Operations Center), государственные учреждения, банки, больницы и облачные провайдеры используют SIEM. Это центральная нервная система современной кибербезопасности.



СБОР ЛОГОВ
в реальном времени

ОБНАРУЖЕНИЕ УГРОЗ
с помощью AI и правил

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ
до наступления ущерба

ЗАЩИТА ОРГАНИЗАЦИИ
на всех уровнях

// КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

ЧТО НА САМОМ ДЕЛЕ ДЕЛАЕТ SIEM

LOG

Сбор и агрегация логов

Собирает логи из файрволов, серверов, конечных точек, облачных сервисов и приложений в единое центральное хранилище. Обрабатывает миллионы событий в секунду в реальном времени.



COR

Корреляция и анализ событий

Применяет правила и AI/ML для связи кажущихся несвязанными событий в разных системах — выявляя паттерны атак, боковое перемещение и попытки утечки данных, невидимые для отдельных инструментов.



ALT

Оповещения в реальном времени и дашборды

Генерирует приоритетные оповещения при обнаружении подозрительной активности. Аналитики видят угрозы, отсортированные по уровню критичности с полным контекстом, что снижает количество ложных срабатываний.



COM

Отчеты по соответствию и форензика

Автоматизирует отчеты по соответствию требованиям PCI-DSS, HIPAA, GDPR, ISO 27001 и SOX. Хранит полные журналы аудита для проведения форензик-расследований после любого инцидента.

// SIEM ИНСТРУМЕНТ 01 ИЗ 10

01 SPLUNK ENTERPRISE SIEM

ЛИДЕР ОТРАСЛИ — КОРПОРАТИВНОГО УРОВНЯ

ТИП: Коммерческий · Облако + Локально

ПРОИЗВОДИТЕЛЬ
Splunk (Cisco)

РАЗВЕРТЫВАНИЕ
Облако, Локально, Гибрид

ЛУЧШЕ ПОДХОДИТ ДЛЯ
Крупные предприятия, SOC-команды

ЦЕНОВАЯ МОДЕЛЬ
$$$$ — Премиум (зависит от объёма данных)

ПОЧЕМУ SPLUNK ЛИДИРУЕТ НА РЫНКЕ

SPL (Search Processing Language) Splunk позволяет аналитикам выполнять запросы к миллиардам событий за секунды. Маркетплейс включает 2000+ приложений и интеграций. Используется 90% компаний из списка Fortune 100.

Фактический стандарт корпоративных SOC по всему миру.



КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Мощный язык запросов SPL
- Движок корреляции в реальном времени
- Обнаружение угроз с помощью AI (ES)

ИСПОЛЬЗУЕТСЯ

- Компании из списка Fortune 500
- Государственные учреждения
- Финансовые организации

// SIEM ИНСТРУМЕНТ 02 ИЗ 10

02 IBM QRADAR SIEM

IBM — РЕШЕНИЕ ДЛЯ РАЗВЕДКИ УГРОЗ КОРПОРАТИВНОГО УРОВНЯ

ТИП: Коммерческий · Облако + Локально

ПРОИЗВОДИТЕЛЬ
IBM Security

РАЗВЕРТЫВАНИЕ
Облако, Локально, SaaS

ЛУЧШЕ ПОДХОДИТ ДЛЯ
Регулируемые отрасли, соответствие требованиям

ЦЕНОВАЯ МОДЕЛЬ
$$$ — Лицензирование на EPS/FPM

МАСШТАБНОЕ ОБНАРУЖЕНИЕ УГРОЗ С ИСПОЛЬЗОВАНИЕМ РАЗВЕДДАННЫХ

QRadar автоматически коррелирует сетевые потоки, журналы событий и данные об уязвимостях, чтобы формировать приоритетные оповещения об угрозах. Встроенная интеграция с IBM X-Force Threat Intelligence предоставляет актуальный глобальный контекст угроз в реальном времени. Доверие со стороны 2100+ организаций в 130+ странах.



КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Автоматическая корреляция инцидентов
- Интеграция с разведданными IBM X-Force
- Анализ сетевых потоков (QFlow)

ИСПОЛЬЗУЕТСЯ

- Банки и финансовые организации
- Медицинские организации
- Государственные учреждения

БЫСТРЫЙ АНАЛИЗ
Миллиарды событий за секунды

КОМПЛЕКСНАЯ ЗАЩИТА
Корреляция, выявление и реагирование

AI И АВТОМАТИЗАЦИЯ
Меньше ложных срабатываний больше точных оповещений

СООТВЕТСТВИЕ НОРМАМ
Соответствие требованиям и готовность к аудиту

// SIEM ИНСТРУМЕНТ 03 ИЗ 10

03 MICROSOFT SENTINEL

MICROSOFT — ОБЛАЧНЫЙ SIEM С AI

ТИП: Коммерческий · Cloud-Native (Azure)



ПРОИЗВОДИТЕЛЬ
Microsoft

РАЗВЕРТЫВАНИЕ
Cloud-native (Azure)

ЛУЧШЕ ПОДХОДИТ ДЛЯ
Среды Microsoft / Azure

ЦЕНОВАЯ МОДЕЛЬ
$$ — Оплата за объём данных (Pay-per-GB)

ПОЧЕМУ MICROSOFT SENTINEL УНИКАЛЕН

Microsoft Sentinel использует AI и машинное обучение, чтобы устранять до 90% усталости от оповещений (alert fatigue). Глубокая интеграция со всей экосистемой Microsoft 365 и Azure. SOAR-возможности автоматизируют сценарии реагирования — команды реагируют за секунды вместо часов.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- AI/ML-обнаружение угроз
- Встроенная автоматизация SOAR
- Язык запросов KQL

ИСПОЛЬЗУЕТСЯ

- Компании Microsoft 365
- Azure облачные организации
- От среднего бизнеса до крупных корпораций

// SIEM ИНСТРУМЕНТ 04 ИЗ 10

04 ELASTIC SIEM (ELK)

OPEN SOURCE POWER — ELASTIC STACK

ТИП: Open Source + Коммерческий · Cloud/On-Prem



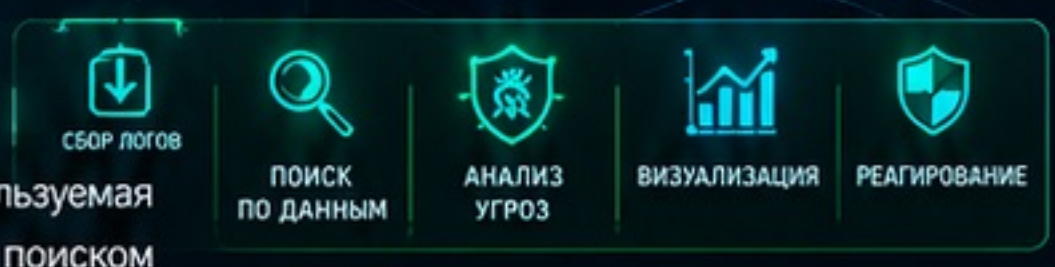
ПРОИЗВОДИТЕЛЬ
Elastic N.V.

СТЕК
Elasticsearch, Logstash, Kibana

ЛУЧШЕ ПОДХОДИТ ДЛЯ
DevSecOps, гибкие развёртывания

ЦЕНОВАЯ МОДЕЛЬ
Бесплатно (OSS) до $$$ (управляемая версия)

ГИБКАЯ OPEN-SOURCE ПЛАТФОРМА



ELK Stack (Elasticsearch + Logstash + Kibana) + Beats — самая широко используемая open-source платформа SIEM в мире. Обрабатывает петабайты данных с поиском на уровне долей секунды. Модуль Elastic Security добавляет SIEM, EDR и угрозы охоты — всё на одной платформе.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Поиск субсекундных петабайт данных
- Интеграция с Beats (сбор данных)
- Визуализация в Kibana

ИСПОЛЬЗУЕТСЯ

- Технологические стартапы и DevSecOps
- Исследователи безопасности
- Средние предприятия

// SIEM ИНСТРУМЕНТ 05 ИЗ 10

05 WAZUH

FREE & OPEN SOURCE — COMMUNITY FAVORITE

ТИП: Open Source • Бесплатный • Self-Hosted

wazuh.
Open Source Security Platform



ПРОИЗВОДИТЕЛЬ
Wazuh Inc.
(Open Source)

СТОИМОСТЬ
100% бесплатно и открытый исходный код

ЛУЧШЕ ПОДХОДИТ ДЛЯ
Малый бизнес, студенты, домашние лаборатории, MSSP-провайдеры

ПОДДЕРЖИВАЕМЫЕ АГЕНТЫ
Linux, Windows, macOS, контейнеры

ПОЧЕМУ WAZUH — ЛУЧШИЙ БЕСПЛАТНЫЙ SIEM В МИРЕ

Wazuh — это полноценный open-source SIEM с более чем 20 млн загрузок. Объединяет анализ логов, обнаружение вторжений (HIDS), мониторинг целостности файлов, обнаружение уязвимостей и отчёты по соответствию в единой бесплатной платформе.

Идеально подходит для этичных хакеров и студентов SOC, создающих свою первую домашнюю лабораторию.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Мониторинг целостности файлов (FIM)
- Обнаружение вторжений (HIDS)
- Встроенный сканер уязвимостей
- Анализ логов и корреляция событий

ИСПОЛЬЗУЕТСЯ

- Студенты и домашние лаборатории
- Малый и средний бизнес
- MSSP-провайдеры и SOC-команды

// SIEM ИНСТРУМЕНТ 06 ИЗ 10

06 LOGRHYTHM SIEM

NEXT-GEN SIEM + SOAR PLATFORM

ТИП: Коммерческий • On-Premise + Облако



ПРОИЗВОДИТЕЛЬ
LogRhythm Inc.

РАЗВЕРТЫВАНИЕ
On-Premise, Облако, Self-Managed

ЛУЧШЕ ПОДХОДИТ ДЛЯ
Средние и крупные корпоративные SOC

КЛЮЧЕВАЯ ОСОБЕННОСТЬ
Встроенные SOAR + UEBA

SIEM + SOAR + UEBA В ОДНОЙ ПЛАТФОРМЕ

LogRhythm объединяет SIEM, SOAR (оркестрацию безопасности) и UEBA (аналитику поведения пользователей и сущностей) в единую платформу. Запатентованная технология Machine Data Intelligence Fabric обрабатывает структурированные и неструктурированные данные из любых источников — выявляя внутренние угрозы и сложные атаки, которые другие инструменты упускают.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Аналитика воведения пользователей (UEBA)
- Встроенные SOAR-плейбуки
- Правила обнаружения на AI-движке
- Интеллектуальная корреляция событий

ИСПОЛЬЗУЕТСЯ

- Средние и крупные корпоративные SOC
- Энергетика и коммунальные службы
- Розничная торговля и e-commerce

КОРРЕЛЯЦИЯ СОБЫТИЙ
Из разных источников в реальном времени

АВТОМАТИЗАЦИЯ (SOAR)
Автоматические сценарии реагирования

UEBA АНАЛИТИКА
Выявление аномального поведения пользователей

ОБЛАЧНАЯ / ЛОКАЛЬНАЯ
Гибкое развёртывание под ваши задачи

// SIEM ИНСТРУМЕНТ 07 ИЗ 10

07 SUMO LOGIC

CLOUD-FIRST SIEM & ANALYTICS

ТИП: Коммерческий • SaaS Cloud-Native



ПРОИЗВОДИТЕЛЬ
Sumo Logic Inc.

РАЗВЕРТЫВАНИЕ
100% SaaS — только облако

ЛУЧШЕ ПОДХОДИТ ДЛЯ
Cloud-native и DevSecOps команд

СИЛЬНЫЕ СТОРОНЫ
Интеграция с AWS, GCP, Azure

★ ПОЧЕМУ SUMO LOGIC — ЛИДЕР ОБЛАЧНЫХ SIEM

Sumo Logic — это 100% облачный SIEM и платформа аналитики логов, обрабатывающая более 100 ПБ данных ежедневно. Бесшовная интеграция с AWS CloudTrail, GCP, Azure, Kubernetes и CI/CD пайплайнами DevOps. Объединяет безопасность и наблюдаемость (Observability) в единой платформе.

- Масштабируемость по требованию
- Упрощённое управление
- AI-анализ и корреляция событий

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Мониторинг облачной инфраструктуры
- Анализ безопасности Kubernetes
- Интеграция Threat Intelligence
- Корреляция событий в реальном времени
- Поддержка Observability и Security

ИСПОЛЬЗУЕТСЯ

- Cloud-native организации
- DevSecOps и SRE команды
- SaaS продуктовые компании
- ИТ-безопасность в облаке

// SIEM ИНСТРУМЕНТ 08 ИЗ 10

08 GRAYLOG

OPEN SOURCE LOG MANAGEMENT SIEM

ТИП: Open Source + Коммерческий



ПРОИЗВОДИТЕЛЬ
Graylog Inc.

СТОИМОСТЬ
Бесплатно (OSS) / Платная enterprise

ЛУЧШЕ ПОДХОДИТ ДЛЯ
Управление логами, комплаенс

СИЛЬНЫЕ СТОРОНЫ
Быстрый поиск, простое развертывание

★ ПОЧЕМУ GRAYLOG — МОЩНЫЙ И ПРОСТОЙ SIEM

Graylog обеспечивает молниеносный поиск и анализ миллиардов логов благодаря MongoDB и Elasticsearch. Разворачивается быстро, легко масштабируется и имеет открытый код с поддержкой коммерческих функций для предприятий.

- Высокая производительность
- Гибкие пайплайны
- Открытый код и расширяемость

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Пайплайны обработки логов
- Быстрый поиск по миллиардам записей
- Настраиваемые дашборды и алерты
- Интеграция с внешними источниками
- SIEM-алерты и автоматизация

ИСПОЛЬЗУЕТСЯ

- ИТ и инфраструктурные команды
- Комплаенс и аудит
- Малый и средний бизнес
- Организации, ищущие доступный SIEM

ОТКРЫТЫЙ КОД
Активное сообщество и прозрачность

БЫСТРОЕ РАЗВЕРТЫВАНИЕ
Минуты вместо часов

НИЗКАЯ СТОИМОСТЬ
Гибкое лицензирование

ГОТОВ К ПРОИЗВОДСТВУ
От стартапов до крупных предприятий

// SIEM ИНСТРУМЕНТ 09 ИЗ 10

09 EXABEAM FUSION SIEM

AI-DRIVEN UEBA + NEXT-GEN SIEM

exabeam
Smarter security operations.

ТИП: Коммерческий · Cloud-Native SaaS

ПРОИЗВОДИТЕЛЬ
Exabeam

РАЗВЕРТЫВАНИЕ
Cloud SaaS

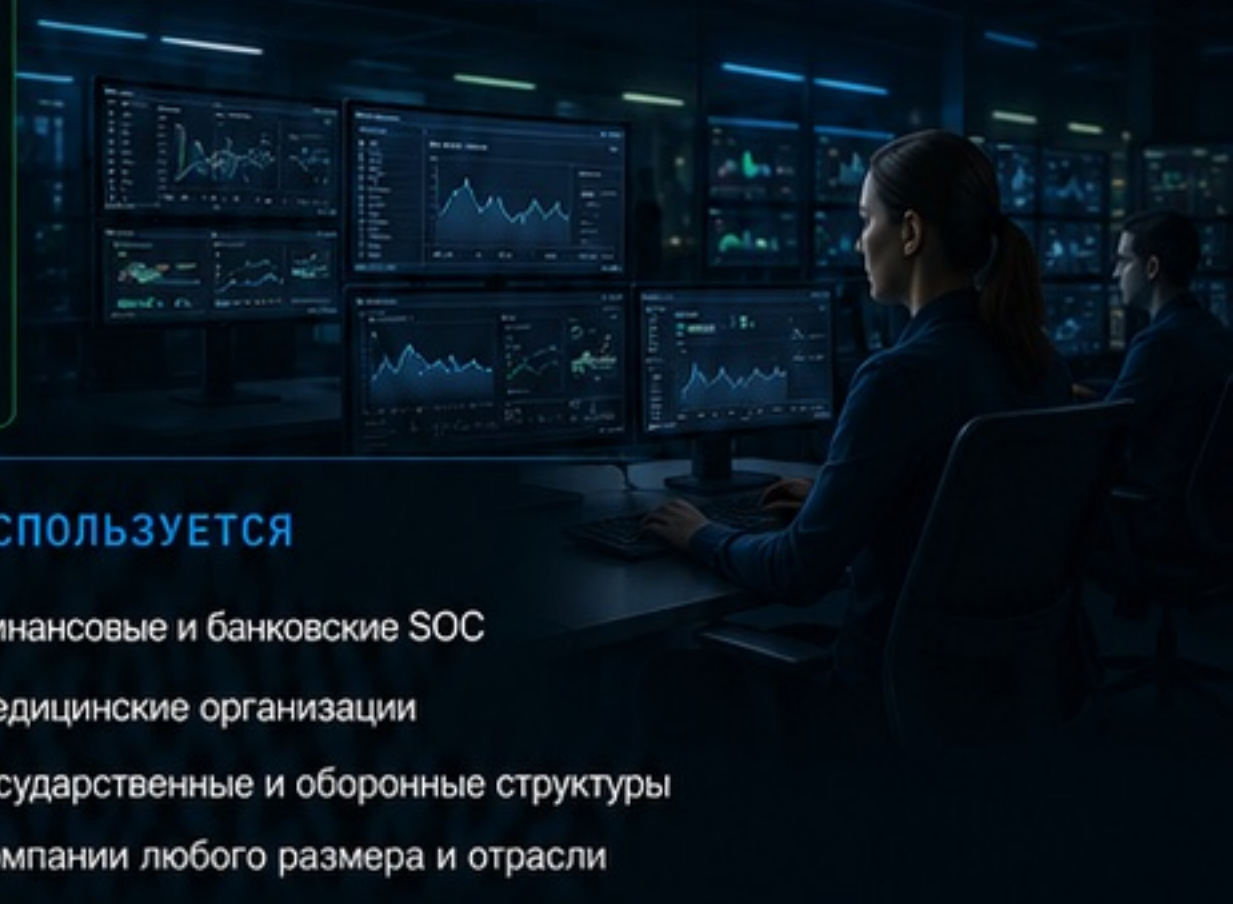
ЛУЧШЕ ПОДХОДИТ ДЛЯ
Выявление внутренних угроз, UEBA (аналитика поведения пользователей и сущностей)

ОТЛИЧИТЕЛЬНАЯ ОСОБЕННОСТЬ
Поведенческое обнаружение аномалий на основе UEBA



ПОЧЕМУ EXABEAM — ЛИДЕР В UEBA

Exabeam использует аналитику поведения для построения временной шкалы каждого пользователя и устройства, автоматически выявляя аномалии, которые указывают на скомпрометированные аккаунты, внутренние угрозы или латеральное перемещение. Умные временные линии связывают события, позволяя аналитикам видеть полную картину атаки в одном представлении вместо тысяч разрозненных алертов.



КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Умные временные линни (цепочки атак)
- Базирование поведения UEBA
- Автоматизированная триаж и оценка
- Коррелация событий с помощью ИИ

ИСПОЛЬЗУЕТСЯ

- Финансовые и банковские SOC
- Медицинские организации
- Государственные и оборонные структуры
- Компании любого размера и отрасли

UEBA АНАЛИТИКА
Поведенческий анализ пользователей и сущностей

ИНТЕГРАЦИИ
AWS, GCP, Azure, Kubernetes, CI/CD и др.

БЕЗОПАСНОСТЬ
Cloud-native, шифрование и соответствие стандартам

ВИЗУАЛИЗАЦИЯ
Интуитивные дашборды и умные оповещения

// SIEM ИНСТРУМЕНТ 10 ИЗ 10

10 GOOGLE CHRONICLE SIEM

GOOGLE — PLANET-SCALE SECURITY ANALYTICS

Google Chronicle
Security analytics at scale.

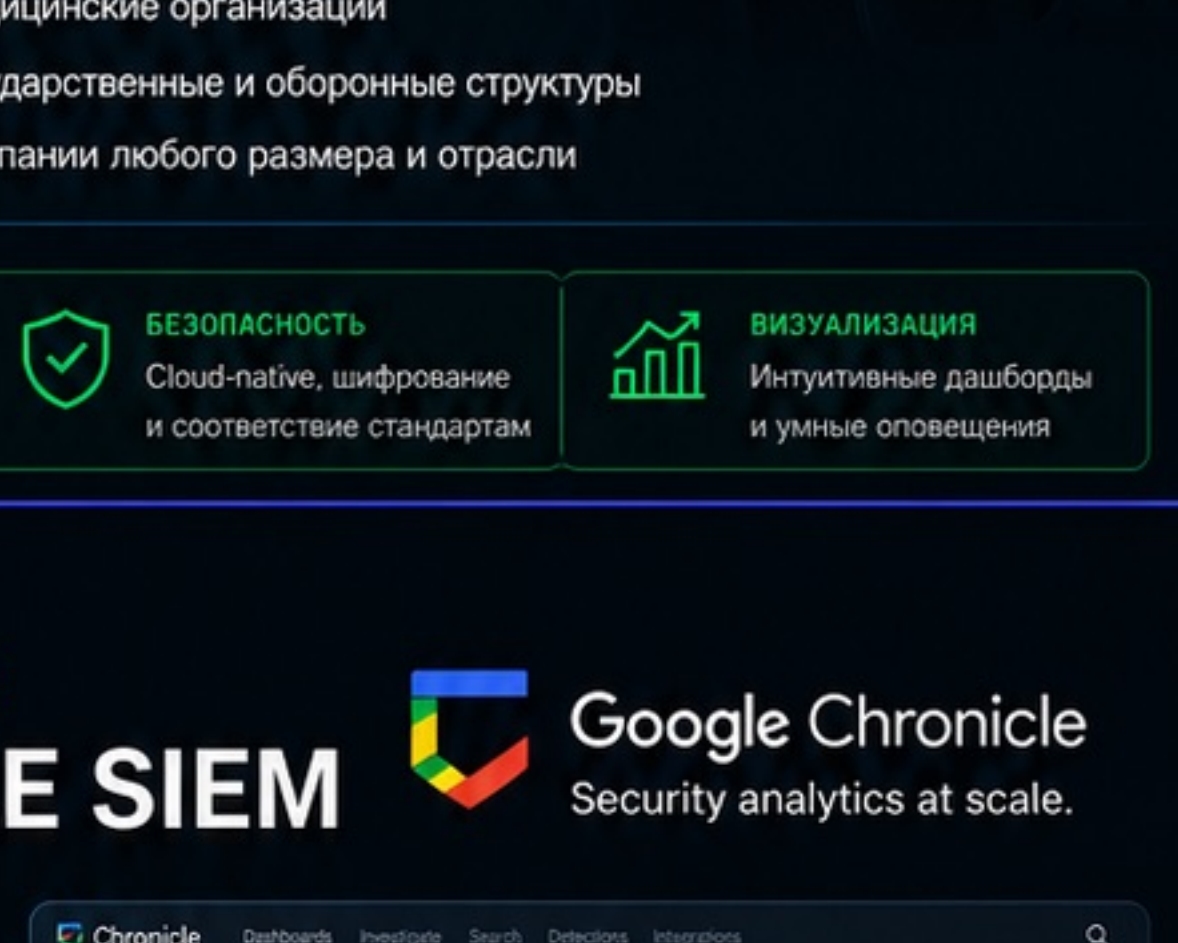
ТИП: Коммерческий · Google Cloud Native

ПРОИЗВОДИТЕЛЬ
Google Cloud (Alphabet)

РАЗВЕРТЫВАНИЕ
Google Cloud — SaaS

ЛУЧШЕ ПОДХОДИТ ДЛЯ
Масштабная аналитика, охота на угрозы

ОТЛИЧИТЕЛЬНАЯ ОСОБЕННОСТЬ
Фиксированная цена — неограниченные данные



GOOGLE-МАСШТАБ БЕЗ ПЕРЕПЛАТ

Chronicle работает на глобальной инфраструктуре Google — той же самой, что обеспечивает работу Поиска и YouTube. Хранит и анализирует годы телеметрии безопасности по фиксированной цене (не за 1 ГБ), что делает её самой экономичной SIEM-платформой для крупных организаций. Встроенные интеграции с VirusTotal и Mandiant Threat Intelligence.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Обработка данных в масштабе Google
- Интеграция с VirusTotal и Mandiant
- Язык обнаружения YARA-L
- Быстрый поиск по триллионам событий

ИСПОЛЬЗУЕТСЯ

- Крупные предприятия и корпорации
- Команды Threat Hunting
- Организации на базе GCP
- Государственный сектор и критическая инфраструктура

МАСШТАБ И ПРОИЗВОДИТЕЛЬНОСТЬ
Обработка триллионов событий с высокой скоростью

ИНТЕГРАЦИИ
VirusTotal, Mandiant, GCP и другие

ЯЗЫК ОБНАРУЖЕНИЯ
Поддержка YARA-L для правил детектирования

ФИКСИРОВАННАЯ ЦЕНА
Неограниченные данные без доплат за объём

// КРАТКИЙ СПРАВОЧНИК

СРАВНЕНИЕ ВСЕХ 10 SIEM ИНСТРУМЕНТОВ

Наглядное сравнение популярных SIEM решений для бизнеса любого масштаба

ИНСТРУМЕНТ	ПРОИЗВОДИТЕЛЬ	СТОИМОСТЬ	ЛУЧШЕ ПОДХОДИТ ДЛЯ	КЛЮЧЕВАЯ СИЛЬНАЯ СТОРОНА
Splunk Enterprise	Cisco	$$$$ Премиум (по объему данных)	Крупные предприятия, SOC-команды	Мощный язык SPL и экосистема 2000+ интеграций
IBM QRadar	IBM	$$$ Модель лицензии EPS/FPM	Регулируемые отрасли, комплаенс	Корреляция событий и встроенная аналитика угроз
Microsoft Sentinel	Microsoft	$$ Оплата за гигабайт	Организации в экосистеме Microsoft / Azure	Нативная интеграция с Microsoft 365 и Azure
ELK Stack (Elastic SIEM)	elastic	Free/$ (Открытый код / управляемая версия)	DevSecOps, гибкие развертывания	Гибкость, масштабируемость и открытый код
Wazuh	WAZUH (Open Source)	БЕСПЛАТНО (Открытый код)	Малый бизнес, образование, лаборатории	HIDS, FIM, анализ уязвимостей и корреляция событий
LogRhythm	LogRhythm	$$$ (По объему данных)	Средние и крупные SOC-команды	UEBA, SOAR и поведенческая аналитика
Sumo Logic	sumo logic	$$ 100% SaaS, облако	Cloud-native и DevSecOps команды	Облачный SIEM с аналитикой больших данных
graylog	graylog inc.	Free/$ (OSS / платная версия)	ИТ и инфраструктурные команды, комплаенс	Быстрый поиск, простота установки и использования
exabeam fusion	exabeam	$$$ Cloud SaaS	Организации с акцентом на внутренние угрозы	UEBA, поведенческий анализ и умные таймлайны
Google Chronicle	Google Cloud	$$$ Фиксированная цена	Крупные предприятия, охота на угрозы, масштаб	Масштаб Google, интеграция с VirusTotal и Mandiant

КАКОЙ SIEM ВЫБРАТЬ?

ДЛЯ КРУПНЫХ ПРЕДПРИЯТИЙ



Splunk Enterprise
или
Exabeam Fusion

ДЛЯ КОМПЛАЕНС И РЕГУЛИРУЕМЫХ ОТРАСЛЕЙ



IBM QRadar
или
Graylog

ДЛЯ MICROSOFT ЭКОСИСТЕМЫ



Microsoft Sentinel

ДЛЯ ОТКРЫТОГО КОДА И ГИБКОСТИ



ELK Stack
или
Wazuh

ДЛЯ ОБЛАЧНЫХ И DEVSECOPS КОМАНД



Sumo Logic
или
Google Chronicle

ЧТО ТАКОЕ SIEM?

SIEM (Security Information and Event Management) — это решение, которое собирает, анализирует и коррелирует события безопасности из различных источников в реальном времени, помогая выявлять угрозы, реагировать на инциденты и соответствовать требованиям.

// КАК РАБОТАЕТ SIEM

АРХИТЕКТУРА SIEM

Путь данных от источников до реагирования на инциденты

01 ИСТОЧНИКИ ДАННЫХ — ВСЁ ОТПРАВЛЯЕТ ЛОГИ

Межсетевые экраны, IDS/IPS, конечные точки, серверы, облачные API, Active Directory, почтовые шлюзы и приложения отправляют логи в SIEM через syslog, агенты или API-коннекторы.



02 СБОР И НОРМАЛИЗАЦИЯ

Сырые логи поступают в разных форматах. SIEM приводит все данные к единой схеме — чтобы можно было коррелировать события между разными системами и вендорами.

СЫРЫЕ ЛОГИ

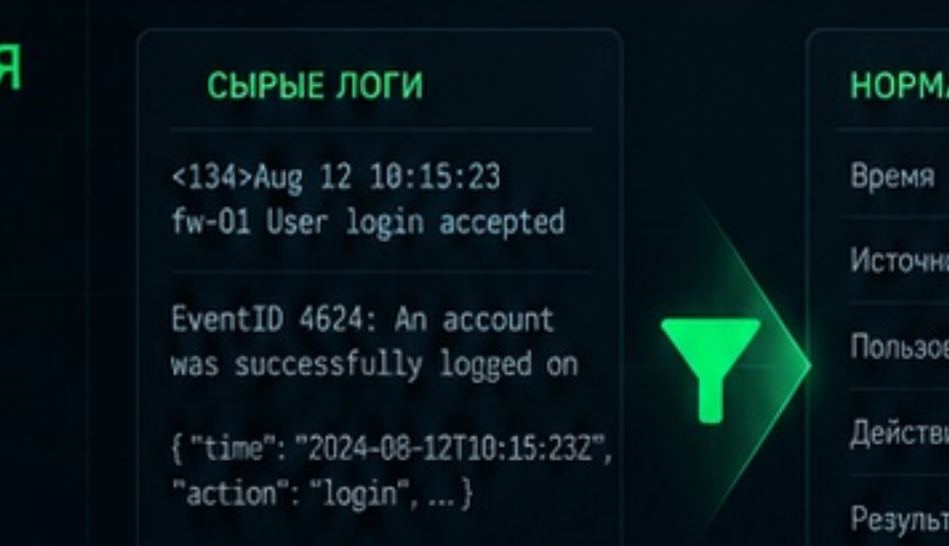
```
<134>Aug 12 10:15:23
fw-01 User login accepted

EventID 4624: An account
was successfully logged on

{ "time": "2024-08-12T10:15:232",
"action": "login", ... }

Aug 12 10:15:23, user=admin
login success

...
```

НОРМАЛИЗОВАННЫЕ ДАННЫЕ

Время	2024-08-12 10:15:23
Источник	fw-01
Пользователь	admin
Действие	login
Результат	success
IP-адрес	10.0.0.5
Тип события	authentication

03 КОРРЕЛЯЦИЯ — ПОИСК АТАК

Правила, AI и ML анализируют нормализованные данные в реальном времени — связывают события между временем и системами, чтобы выявить паттерны атак, индикаторы компрометации (IoCs) и угрозы (TTPs).



ОБНАРУЖЕНА АТАКА

- Необычный вход из нового IP
- Множественные неудачные попытки
- Повышение привилегий
- Подозрительное перемещение по сети

04 АЛЕРТ — ПРОВЕРКА АНАЛИТИКОМ — РЕАГИРОВАНИЕ

Оповещения с контекстом поступают на дашборды аналитиков SOC. Интеграция с SOAR автоматически запускает сценарии реагирования — блокирует IP, изолирует хосты и уведомляет команды.



// РЕАЛЬНЫЕ ПРИМЕРЫ ПРИМЕНЕНИЯ

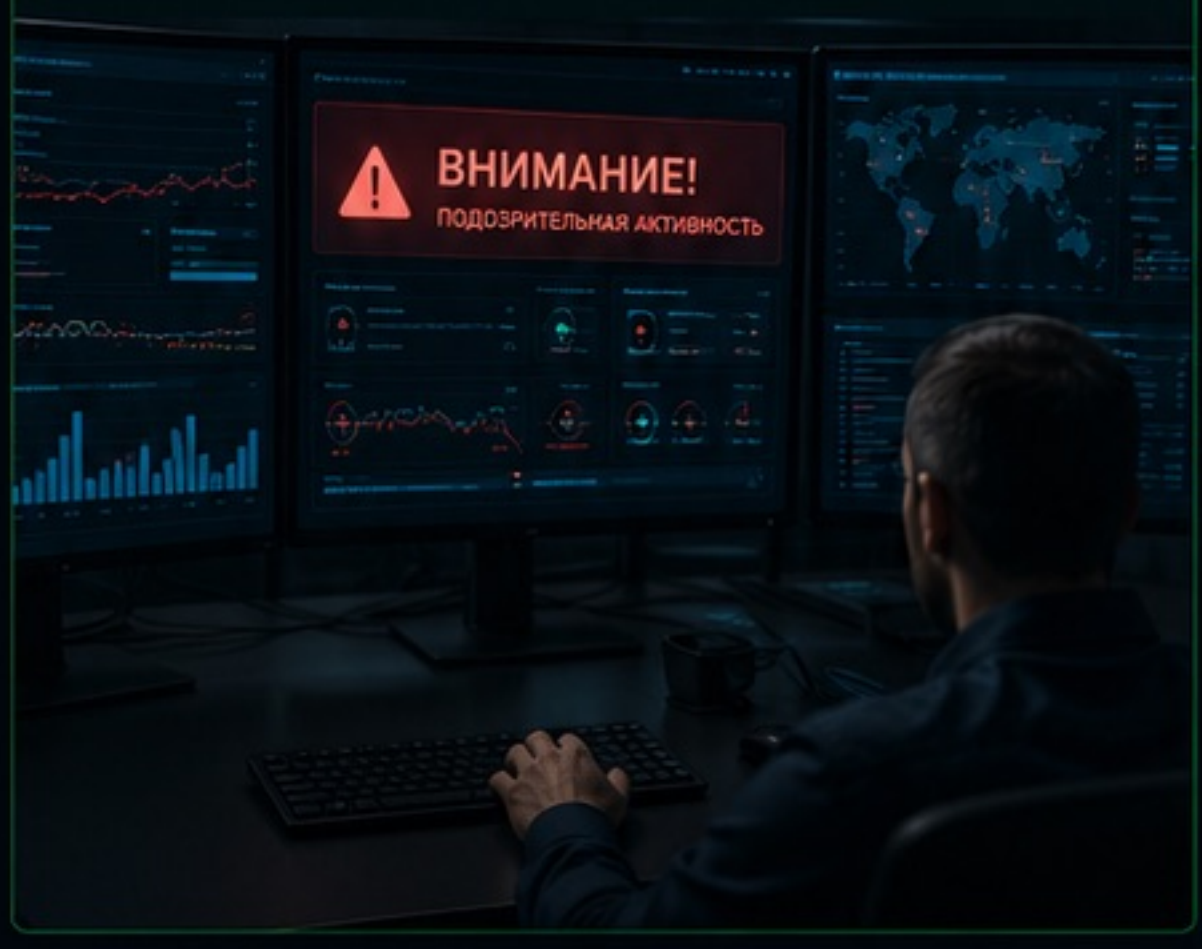
ТОП SIEM КЕЙСЫ ИСПОЛЬЗОВАНИЯ

Как SIEM помогает находить угрозы, соответствовать требованиям и быстро реагировать на инциденты.

ОБНАРУЖЕНИЕ УГРОЗ

Выявление атак, вредоносной активности и подозрительного поведения в реальном времени

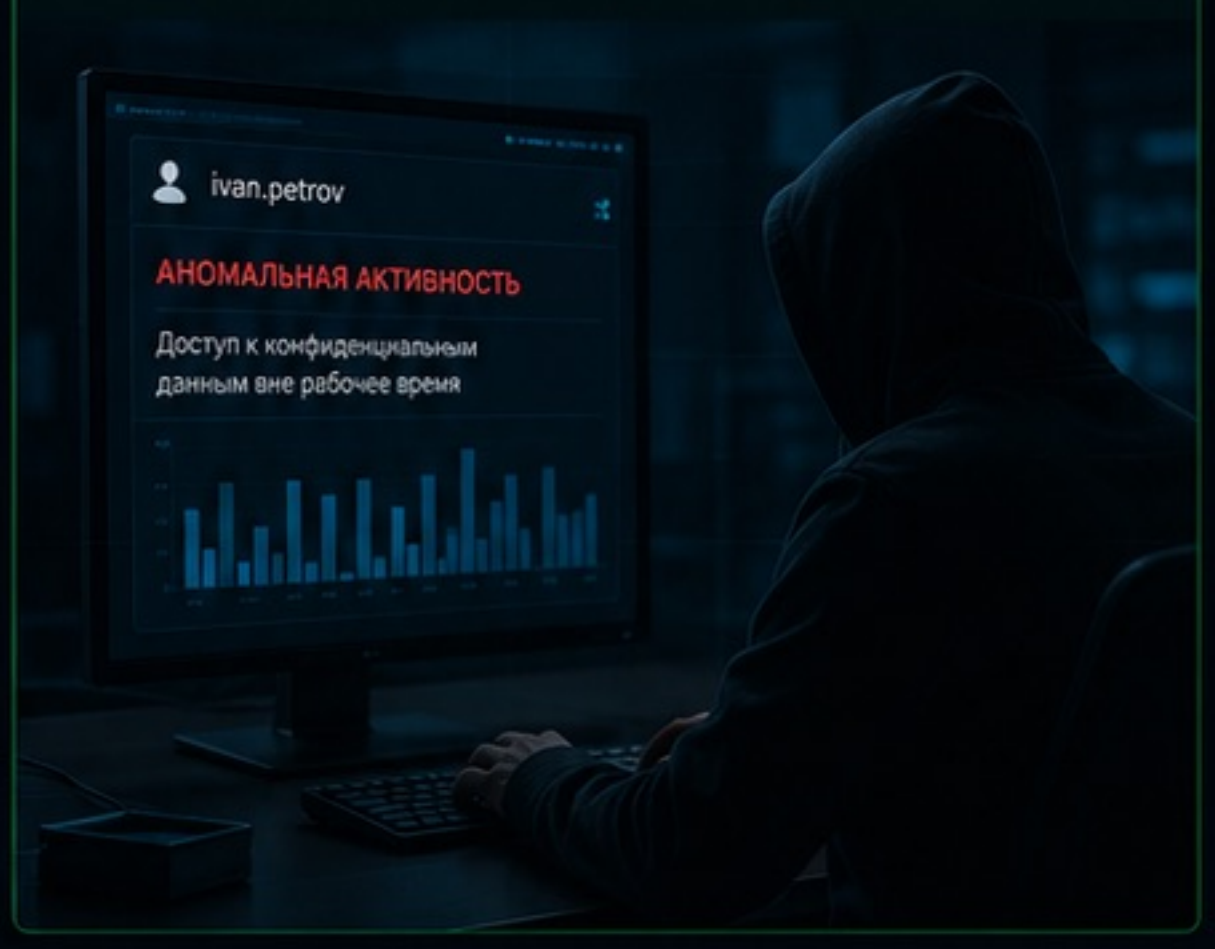
- Атаки перебором паролей
- SQL-инъекции и веб-атаки
- Перемещение внутри сети (lateral movement)
- Вывод данных и утечки



ВНУТРЕННИЕ УГРОЗЫ

Анализ поведения пользователей и выявление аномалий для предотвращения инсайдерских угроз

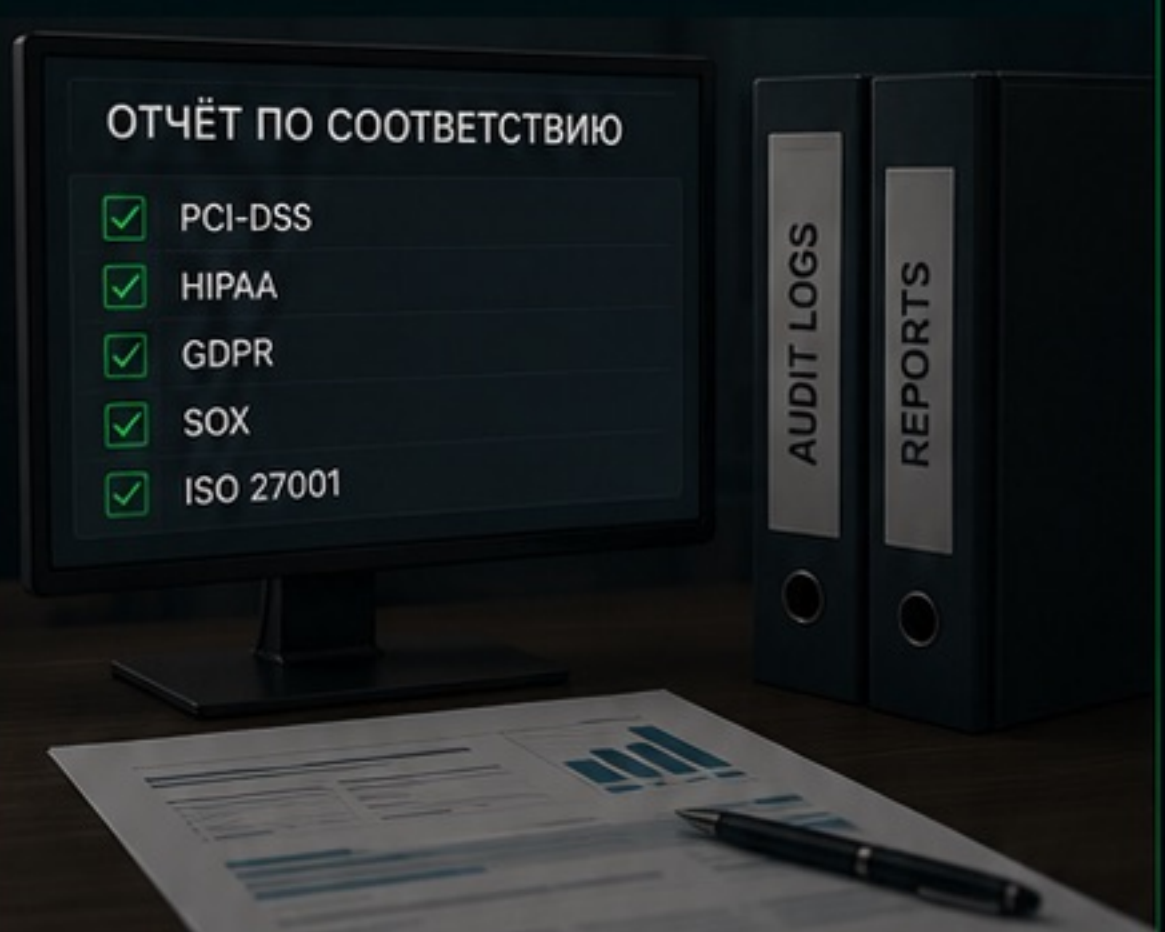
- Аномальный доступ к данным
- Использование привилегий не по роли
- Работа в нерабочее время
- Риск утечки конфиденциальной информации



СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

Автоматизация сбора доказательств и формирование отчётности для аудитов и регуляторных стандартов

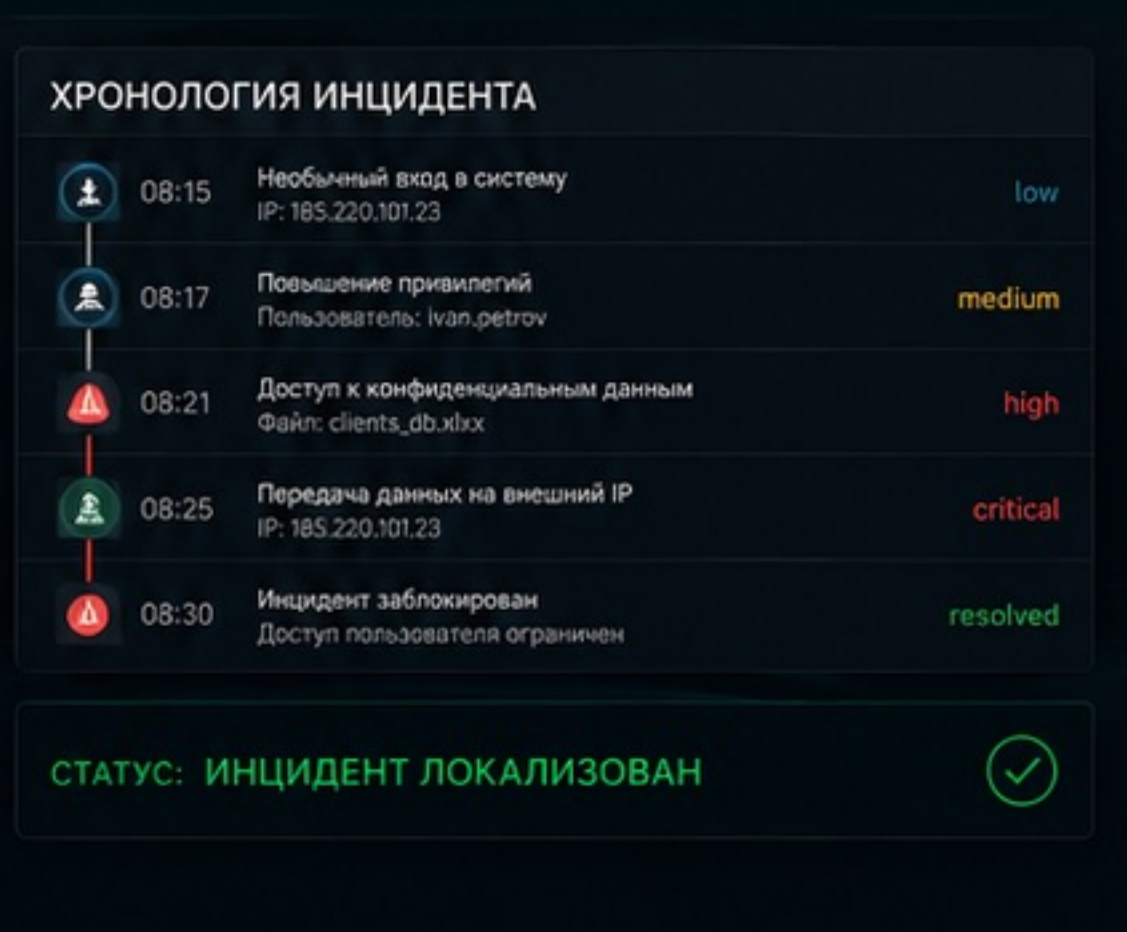
- PCI-DSS, HIPAA, GDPR, SOX, ISO 27001
- Хранение журналов и цепочек аудита
- Готовые шаблоны отчётов
- Упрощение внутренних и внешних проверок



РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

Полная картина инцидента: что произошло, когда и как — для быстрого расследования и устранения последствий

- Хронология событий до, во время и после атаки
- Корреляция событий из разных источников
- Интеграция с SOAR для автоматизации
- Ускорение работы SOC и снижение ущерба



SIEM — ЕДИНАЯ ПЛАТФОРМА БЕЗОПАСНОСТИ

Сбор, нормализация, корреляция и анализ событий из всех источников в реальном времени.

// ГИД ПО ВЫБОРУ

БЕСПЛАТНЫЕ VS ПЛАТНЫЕ SIEM

Что выбрать: бесплатное решение или корпоративную платформу?

FREE

WAZUH

ЛУЧШИЙ БЕСПЛАТНЫЙ SIEM В ЦЕЛОМ

Идеально для студентов, домашних лабораторий, малого бизнеса и всех, кто только начинает работать с SOC-анализом.

- Полный HIDS, FIM, сканер уязвимостей
- Отчёты по соответствию (compliance)
- Нулевая стоимость



FREE

ELK STACK (ELASTIC OSS)

ЛУЧШИЙ ВЫБОР ДЛЯ РАЗРАБОТЧИКОВ И DEVSECOPS

Гибкая, масштабируемая и настраиваемая платформа с открытым кодом без стоимости лицензии.

- Elasticsearch, Logstash, Kibana
- Полный контроль и кастомизация
- Требует экспертизы для настройки



PAID

SPLUNK / QRADAR / SENTINEL

ДЛЯ ПРЕДПРИЯТИЙ И КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Корпоративные SIEM с профессиональной поддержкой, ИИ-аналитикой, автоматизацией соответствия и SOAR.

- Продвинутая аналитика и детектирование
- Соответствие стандартам (PCI-DSS, ISO и др.)
- Поддержка и SLA от вендора

CLOUD

SENTINEL / CHRONICLE / SUMO LOGIC

ЛУЧШИЕ ОБЛАЧНЫЕ SIEM-ПЛАТФОРМЫ

Облачные SIEM с нулевым управлением инфраструктурой. Идеальны для организаций, уже использующих Azure, AWS или GCP.

- Мгновенное развёртывание
- Автоматическое масштабирование
- Глубокая интеграция с облаком



ИТОГ

Бесплатные SIEM отлично подходят для обучения и небольших задач.
Платные и облачные решения — для масштаба, соответствия и скорости реагирования.

// КАРЬЕРНЫЕ НАВЫКИ

SIEM ДЛЯ АНАЛИТИКОВ SOC

Ключевые навыки, уровни экспертизы и сертификации для успешной карьеры в SOC

$95K
СРЕДНЯЯ ЗАРПЛАТА SOC АНАЛИТИКА

3.5M
ОТКРЫТЫХ ВАКАНСИЙ ПО КИБЕРБЕЗОПАСНОСТИ

#1
НАВЫК: SIEM В ТОПЕ ДЛЯ SOC

01 УРОВЕНЬ 1 — TRIAGE

Мониторинг SIEM-дашбордов, триаж алертов по критичности, фильтрация ложных срабатываний и эскалация подтверждённых угроз.
Первичный уровень — SIEM ваш основной инструмент каждый день.

- Мониторинг дашбордов
- Триаж по уровням критичности
- Фильтрация ложных срабатываний
- Эскалация реальных угроз



02 УРОВЕНЬ 2 — INVESTIGATION

Глубокий анализ SIEM-данных, исследование эскалированных алертов. Корреляция событий из разных источников, маппинг на MITRE ATT&CK и написание отчётов по инцидентам.

- Глубокий поиск и анализ данных
- Корреляция событий из разных источников
- Маппинг на MITRE ATT&CK
- Создание отчётов



03 УРОВЕНЬ 3 — THREAT HUNTING

Проактивный поиск скрытых угроз в SIEM-данных до того, как сработают алерты. Создание новых детектирующих правил, настройка корреляции и постоянное улучшение покрытия SOC.

- Проактивный поиск угроз
- Разработка правил детектирования
- Настройка корреляционной логики
- Улучшение покрытия SOC



04 СЕРТИФИКАЦИИ

Профессиональные сертификации подтверждают экспертизу в SIEM и SOC-аналитике и повышают ценность на рынке труда.

- CompTIA CySA+
- Splunk Core Certified
- IBM QRadar Administrator
- Microsoft SC-200
- GIAC GCIA



ИТОГ

SIEM — ключ к успешной карьере в SOC.
Развивайте навыки по уровням, получайте сертификации и становитесь экспертом в кибербезопасности.

// ОБЩАЯ КАРТИНА

SIEM · SOAR · XDR · EDR

Современная кибербезопасность — это не один инструмент,
а комбинация технологий, которые вместе обеспечивают
обнаружение, реагирование и защиту.



SIEM

УПРАВЛЕНИЕ СОБЫТИЯМИ И ИНФОРМАЦИЕЙ О БЕЗОПАСНОСТИ

Сбор логов и событий со всех систем,
их корреляция, оповещения и соответствие
требованиям. «Мозг» SOC — видит всё,
что происходит в инфраструктуре.

- Централизованный сбор и хранение логов
- Корреляция и выявление инцидентов
- Оповещения и отчёты
- Соответствие требованиям (compliance)



SOAR

ОРКЕСТРАЦИЯ, АВТОМАТИЗАЦИЯ И РЕАГИРОВАНИЕ

Автоматизирует рутинные задачи и сценарии
реагирования, запускаемые алертами из SIEM —
блокировка IP, изоляция хостов, уведомления.

- Автоматизация процессов SOC
- Интеграция с инструментами безопасности
- Реагирование в один клик
- Сокращение времени на инциденты

Пример сценария реагирования



XDR

РАСШИРЕННОЕ ОБНАРУЖЕНИЕ И РЕАГИРОВАНИЕ

Объединяет телеметрию из конечных точек,
сети, почты и облаков в один уровень обнаружения.
Работает вместе с SIEM для глубокой видимости
и быстрого реагирования.

- Корреляция данных из разных слоёв
- Поиск сложных и скрытых атак
- Автоматическое реагирование
- Глубокая видимость по всей инфраструктуре



EDR

ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

Контроль и защита устройств: мониторинг активности,
выявление вредоносного воведения, блокировка угроз
и реагирование на инциденты на уровне endpoints.

- Обнаружение угроз на устройствах
- Поведенческий анализ
- Карантин и устранение угроз
- Интеграция с XDR и SIEM

