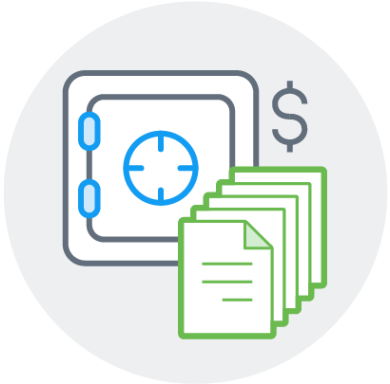
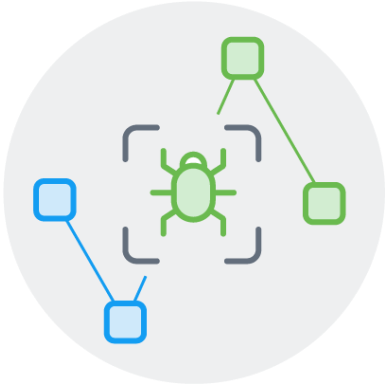
СИСТЕМА АНАЛИЗА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ EXABEAM ADVANCED ANALYTICS

Ванерке Роман
Технический директор АО «ДиалогНаука»
07 апреля 2020 года

Преимущества Exabeam



Экономия средств на журналировании



Улучшенное выявление угроз

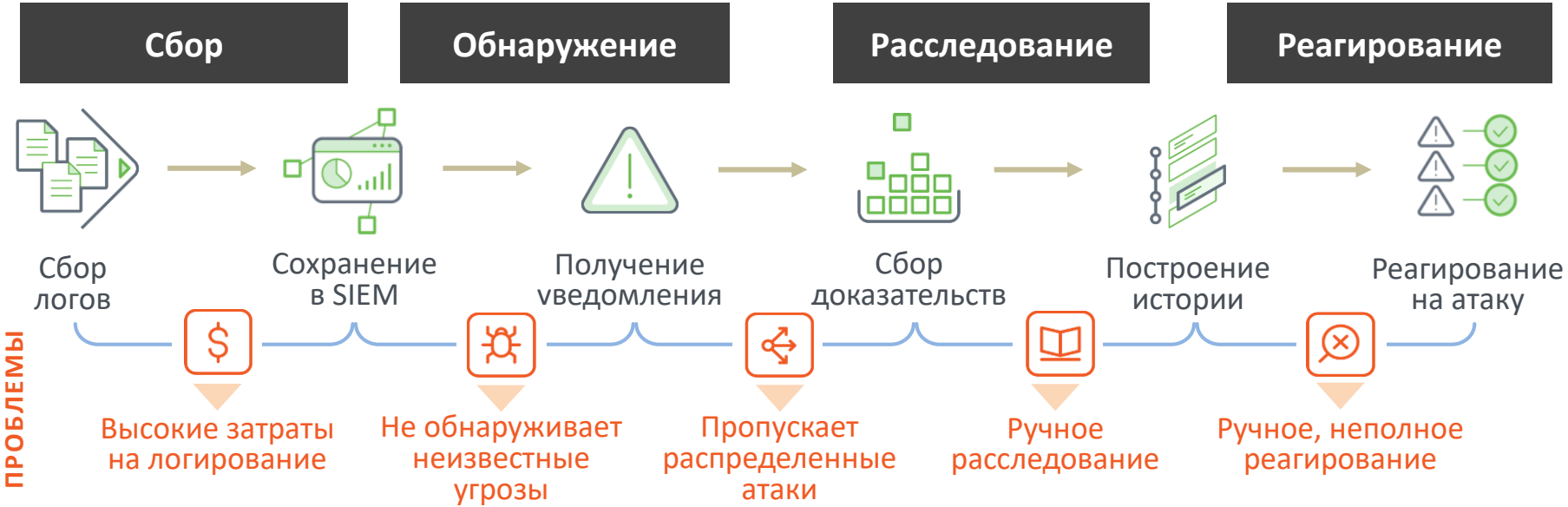
Повышение продуктивности аналитиков

Процесс выявления инцидента в SIEM

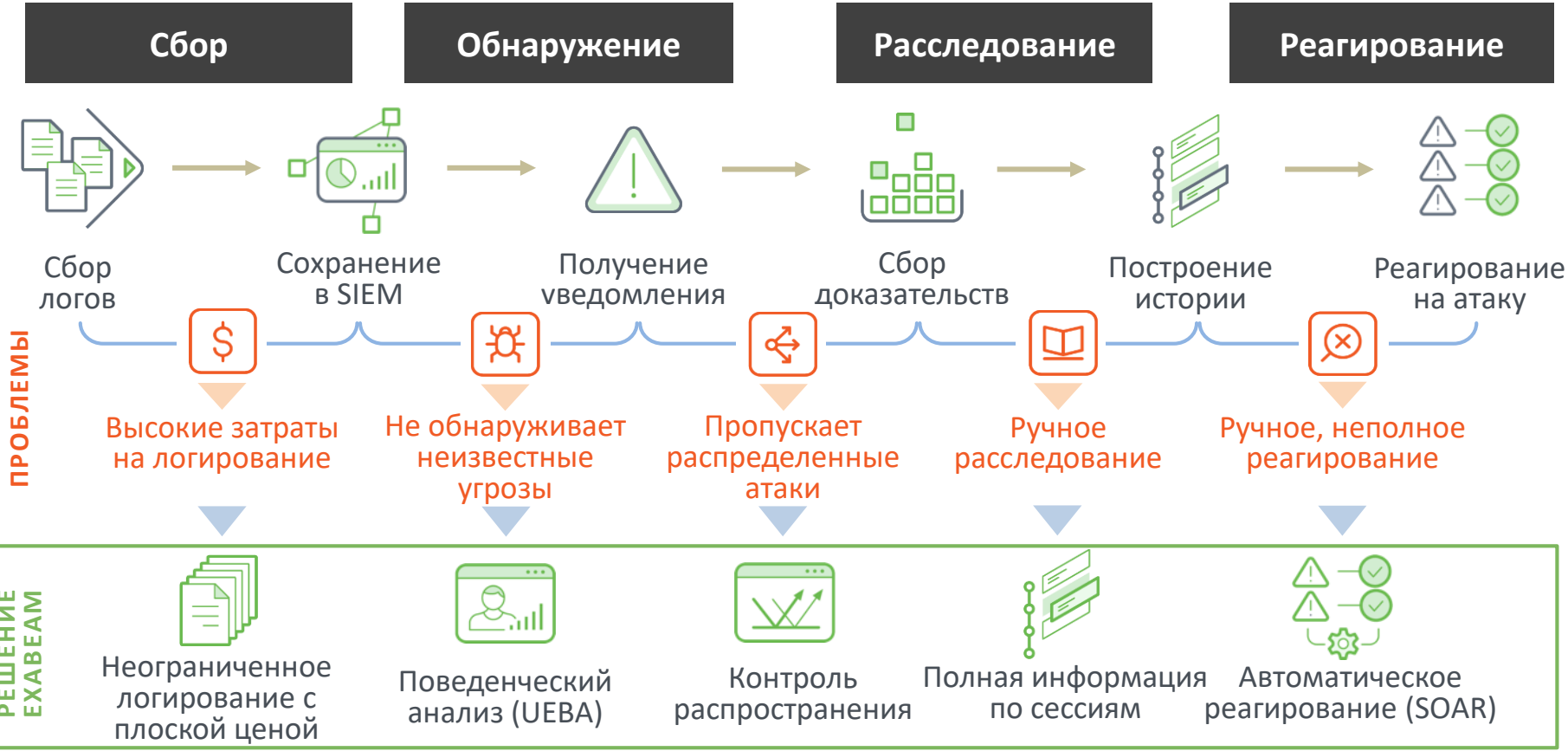
Сбор | **Обнаружение** | **Расследование** | **Реагирование**

Сбор логов → Сохранение в SIEM → Получение уведомления → Сбор доказательств → Построение истории → Реагирование на атаку

Проблемы на каждом шаге

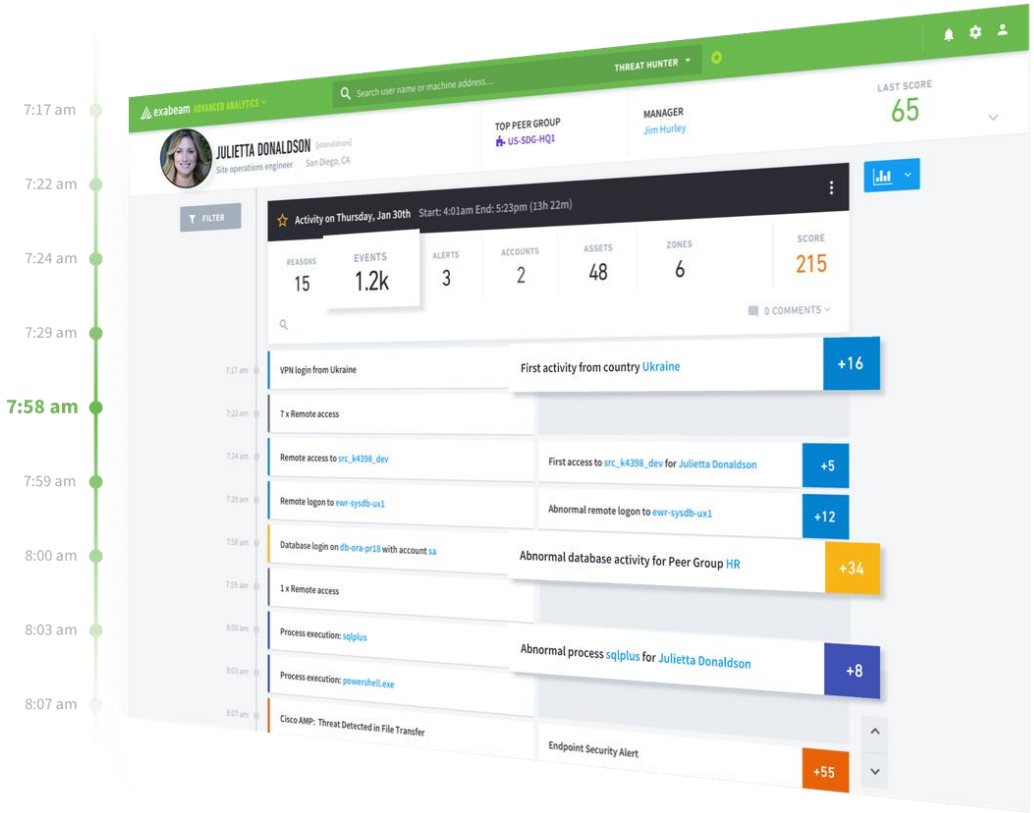


Что предлагает Exabeam

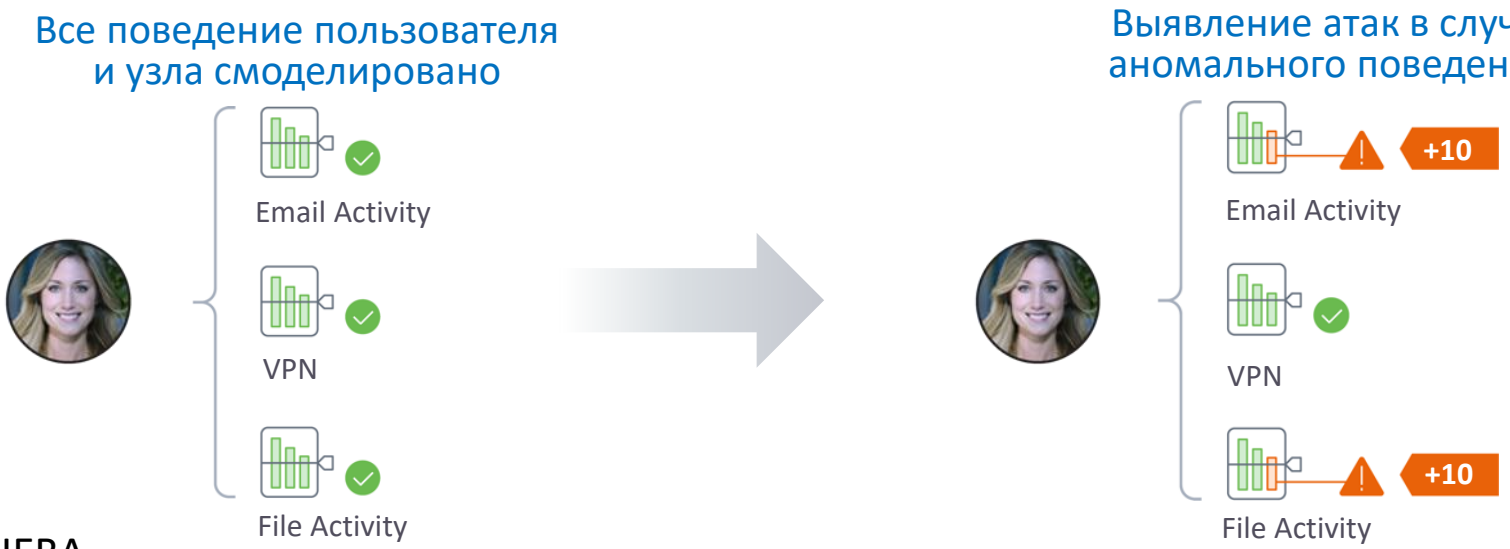


Информационная модель Exabeam

Интеллектуальные временные шкалы Exabeam Smart Timelines автоматически объединяет последовательность, поведение, личность и область действия в новый тип информационной модели



Exabeam выявляет неизвестные атаки

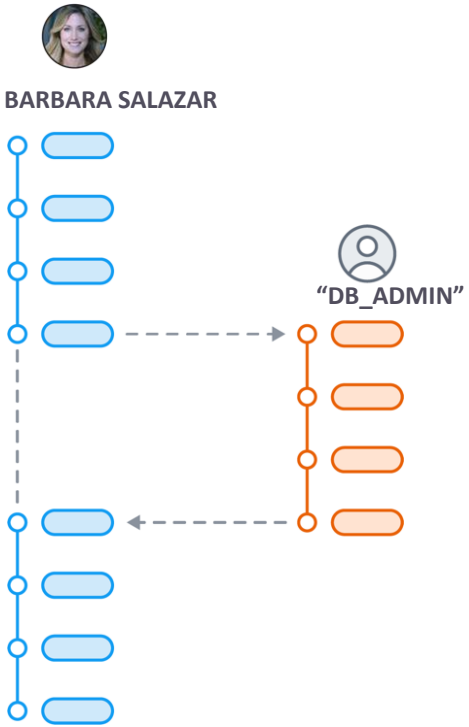


UEBA

- Выявляет как известные, так и неизвестные атаки
- Не требует построения и поддержания правил корреляции для обнаружения
- Снижает ложные срабатывания за счет понимания ролей, групп и нормального поведения

Обнаружение дальнейшего распространения с Smart timeline

Lateral movement без Smart Timelines



Часть атаки не обнаруживается из-за изменений в:

- IP адресе
- Учетных данных
- Узлов

Lateral movement с Smart Timelines

Отслеживая изменения, Exabeam Smart Timelines могут связывать эту активность с Barbara

Журналы не содержат данных, необходимых для понимания атаки

Аналитики должны вручную найти связь или есть риск пропустить часть атаки

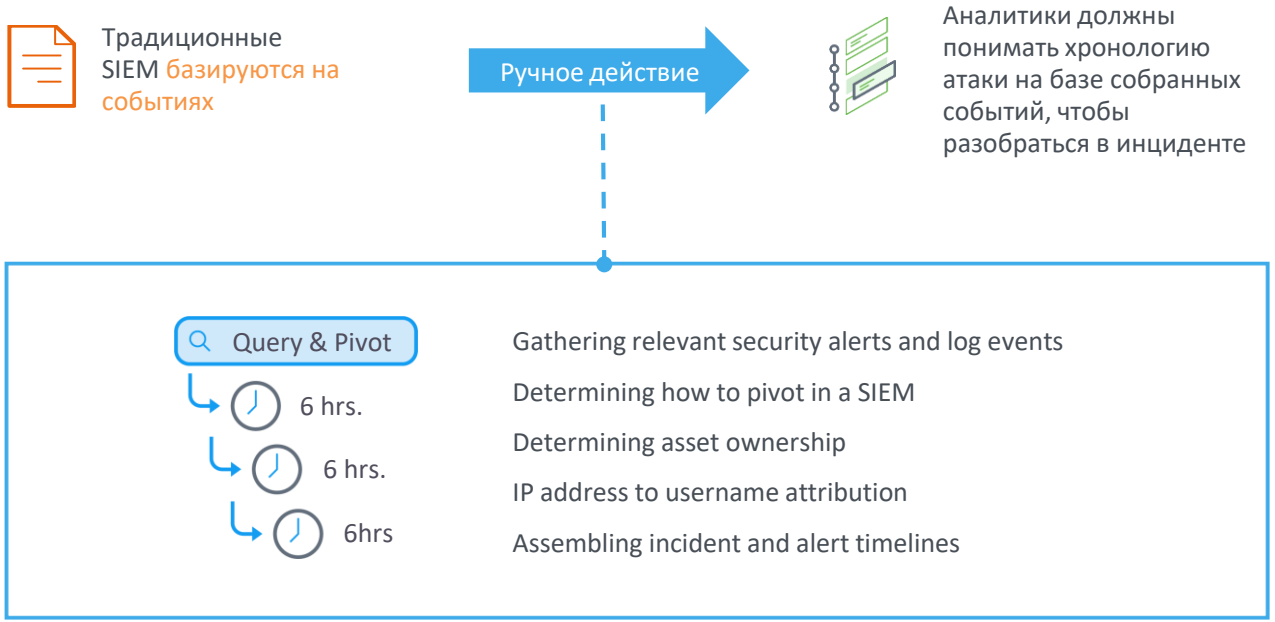
	⚠ Неполная шкала		
Log 1	Barry		Device_1
Log 2	?	142.1.12.68	Device_1
Log 3	Barry	142.1.12.68	
Log 4	Barry		
Log 5	Barry	37.4.1.23	Device_2
Log 6	?	37.4.1.23	Device_2

Smart timeline автоматически находит связи и заполняет данными

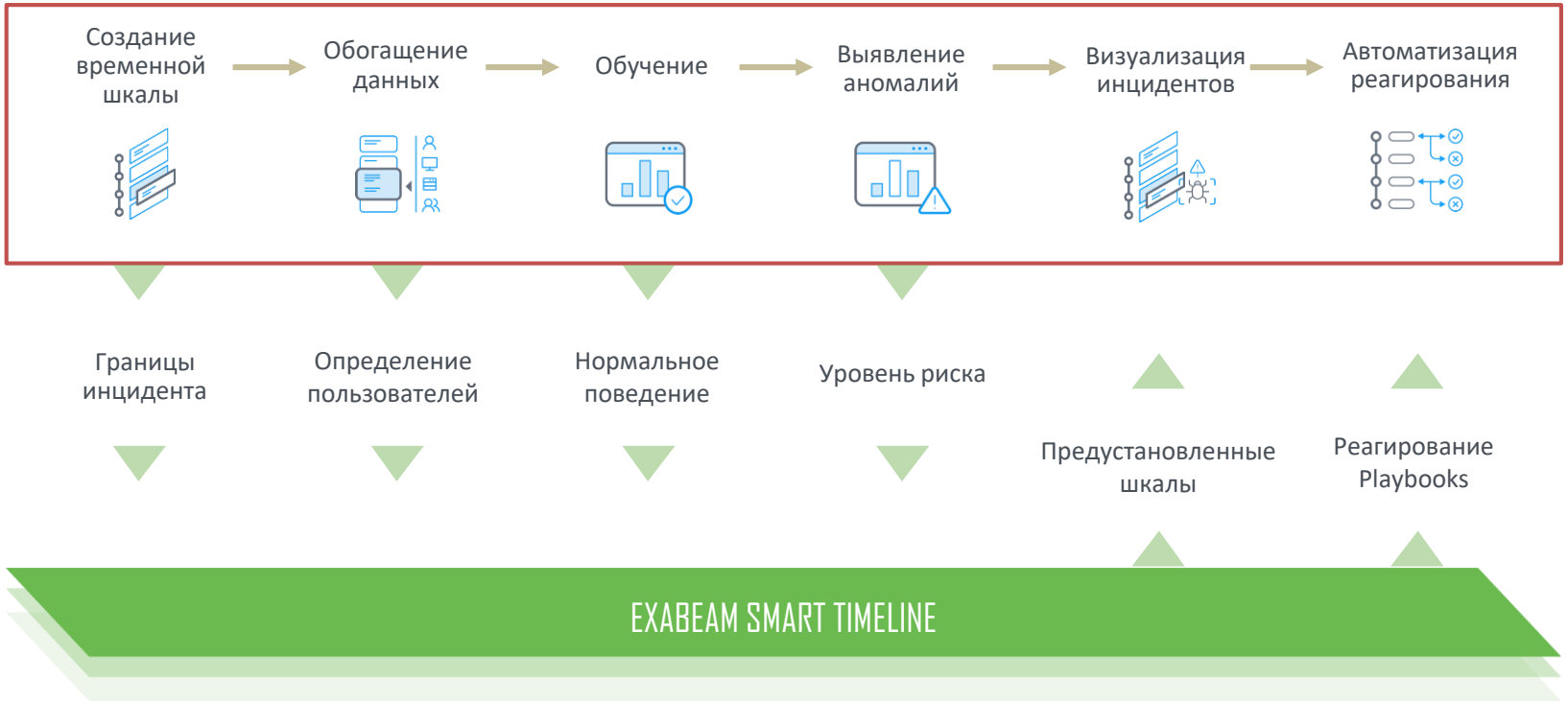
Smart Timelines связывает данные из логов вместе в режиме реального времени, чтобы заполнить пробелы, из:

- Миллионов логов
- Тысяч пользователей и узлов
- IP адресов, которые меняются постоянно

Автоматизация систем управления требует другого похода



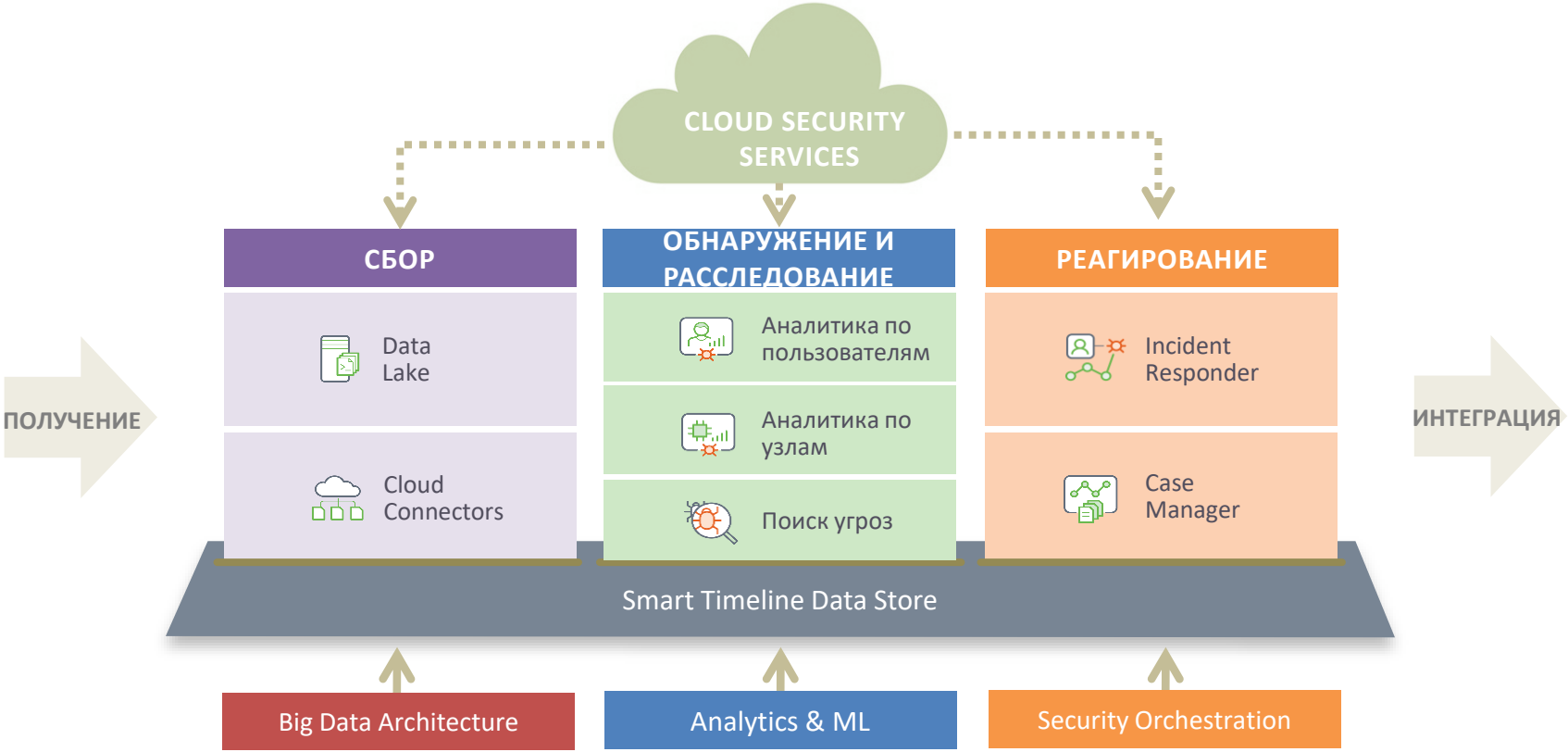
Должно начинаться со временной шкалы



Конкурентный анализ по типу технологии

	 Неограниченное реагирование по фиксированной цене	 Анализ поведения (UEBA)	 Контроль распространения	 Автоматическое создание временных шкал	 Автоматизированное реагирование (SOAR)
Традиционные SIEM	Нет	Сильно зависят от правил корреляции	Вручную	Вручную	Вручную
Splunk	Нет	Частично	Вручную	Вручную	Автоматизированное реагирование **Incomplete scope**
Другие современные SIEMs	Зависит от вендора	Базовый UEBA или сильная зависимость от правил корреляции	Неполные результаты. Требуется много запросов	Неполные временные шкалы – отсутствует нормальное поведение и дальнейшее распространение	Автоматизированное реагирование **Incomplete scope**
Exabeam	**Да**	**Да**	**Автоматически**	**Автоматически**	Автоматизированное реагирование **Complete scope**

Платформа Exabeam



Модульный подход позволяет улучшить существующие SIEM

- Комбинируйте с вашими решениями для повышение возможностей существующих SIEM

- Позволяет отделам по ИБ получить доступ к возможностям современных SIEM без необходимости полной замены с целью:
  - Повышение эффективности выявления угроз
  - Расширить контроли ИБ в облаке
  - Снизить издержки на логирование
  - Автоматическое реагирование

- Подход по поэтапному обновление технологий, снижения стоимости обновления и трудозатрат

Признание рынком и клиентами

250+ Enterprise Customers

BARCLAYS
Royal Bank of Scotland
DISCOVER
Freddie Mac
UNITED
DELTA
Caltrans
MTA Metropolitan Transportation Authority
Louisiana
Anthem
Cigna
Cleveland Clinic
Cincinnati Children's
Anadarko Petroleum Corporation
DUKE ENERGY
First Solar
Black Hills Corporation
P&G Procter & Gamble
Levi's
UNDER ARMOUR
SAFEWAY
GAP
THOMSON REUTERS
ebay
verizon telematics
NTT DATA

Select Awards & Recognition

Gartner COOL VENDOR
SC 2017 awards Winner
Inc. 5000 #12 2018
Gartner peerinsights customers' choice 2018
WSJ Tech Companies to Watch 2018 #8
Forbes 2018 THE Cloud100 RISING STARS

РАССМОТРИМ ВОЗМОЖНОСТИ СИСТЕМЫ НА БАЗЕ НЕСКОЛЬКИХ СЦЕАНИРЕВ

Решение ключевых проблем

- Внутренний злоумышленник
- Lateral Movement
- DLP / Data Exfiltration
- Приоритезация

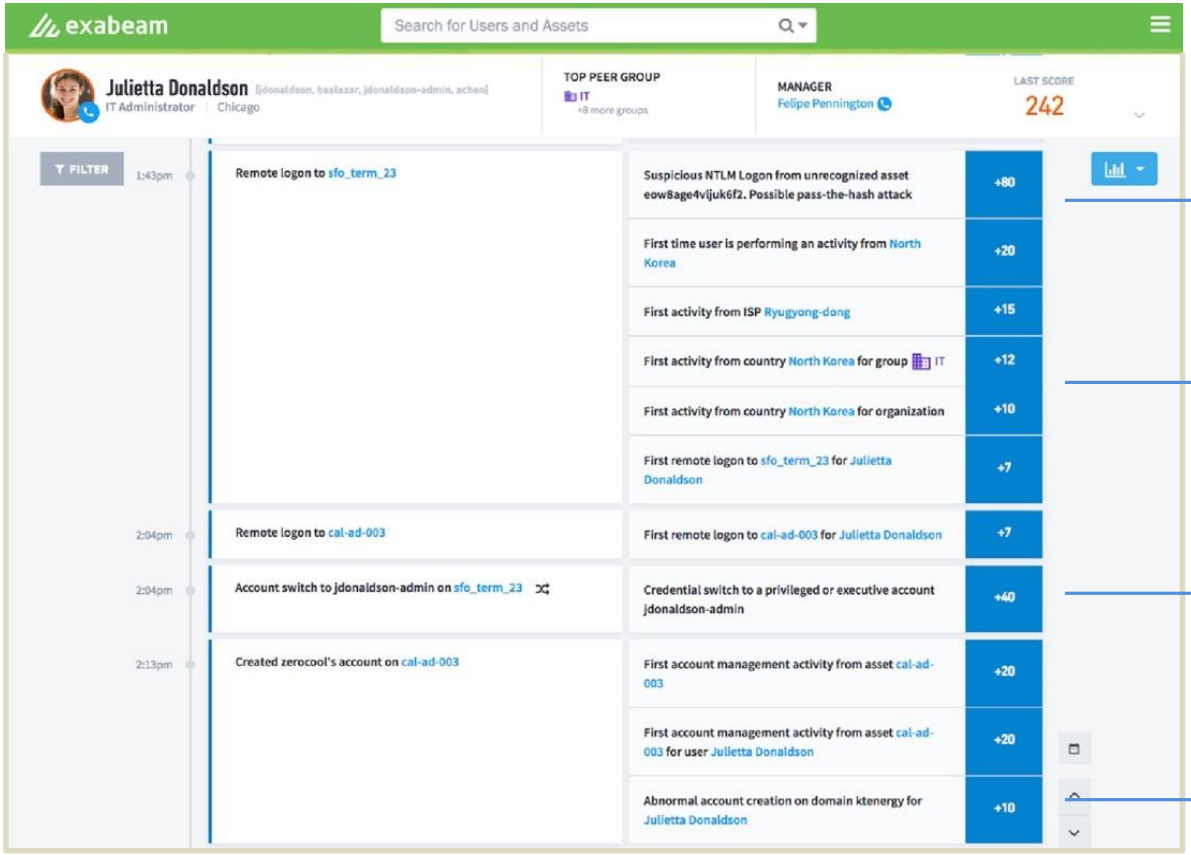
Compliance	Обнаружение угроз	Облачная безопасность	Безопасность IoT	Автоматизация SOC
GDPR ▪ Sarbanes Oxley ▪ PCI	▪ Ransomware	Безопасность и мониторинг облачной инфраструктуры	End-to-end Visibility ▪ Machine-based Threat Detection	Приоритезация инцидентов ▪ Автоматическое реагирование

Внутренний злоумышленник

Внутренние угрозы остаются необнаруженными традиционными средствами безопасности:

- Сбор всех значимых данных безопасности без чрезмерных расходов
- Обнаружение внутренних угроз в режиме реального времени с использованием поведенческого анализа
- Загрузка и анализ данных со всех развернутых систем безопасности для повышения точности результатов
- Выявление дальнейшего распространения через любой узел, IP адрес или учетные данные
- Быстрое расследование угроз с использование smart timeline
- Автоматизация реагирования с помощью SOAR

Обнаружение индикаторов внутренней угрозы с помощью Exabeam



Подозрительный доступ с неизвестного узла

Обнаружено много доступов «в первый раз» для пользователя и группы

Обнаружено дальнейшее распространение
- Пользователь переключился в учетную запись администратора

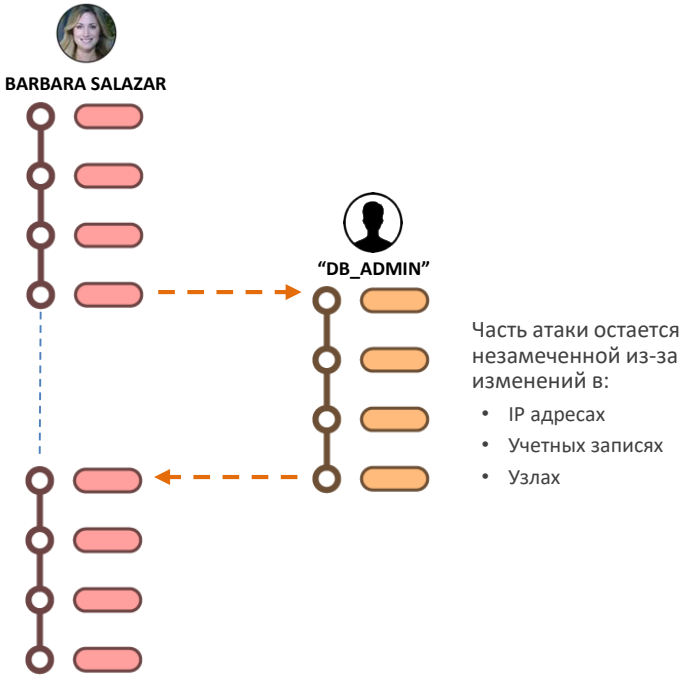
Неавторизованное создание учетной записи

Lateral Movement

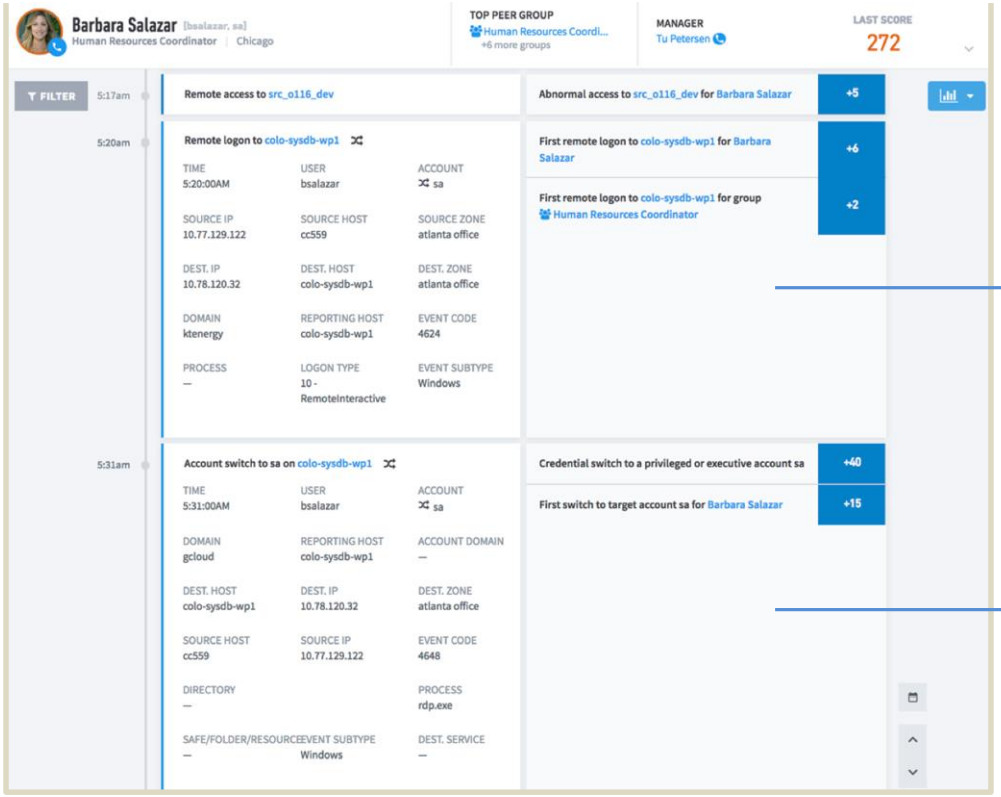
В порядке 60% атаке используется дальнейшее распространение, но не многие решения могут его детектировать

Exabeam обеспечивает автоматическое обнаружение распространения на начальных этапах взлома

- Маппинг Host-to-IP и контекстное обогащение показывают реальную картинку по всем пользователям и системам
- Запантентованная технология отслеживания атак показывает перемещение внутри организации и реконструирует всю цепочку атаки
- Smart Timelines полностью показывает инцидент, включая все задействованные учетные записи, систем и связанные события



Обнаружение индикаторов распространения с Exabeam

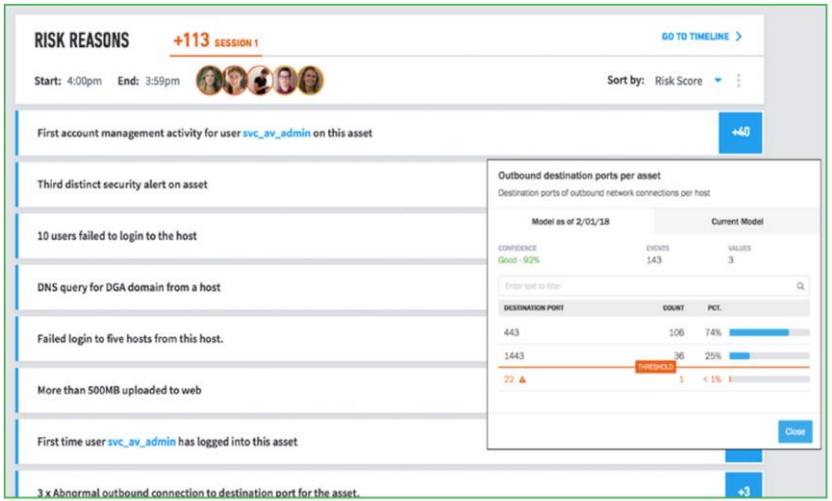


Обнаружение нетипичного входа на удаленный узел

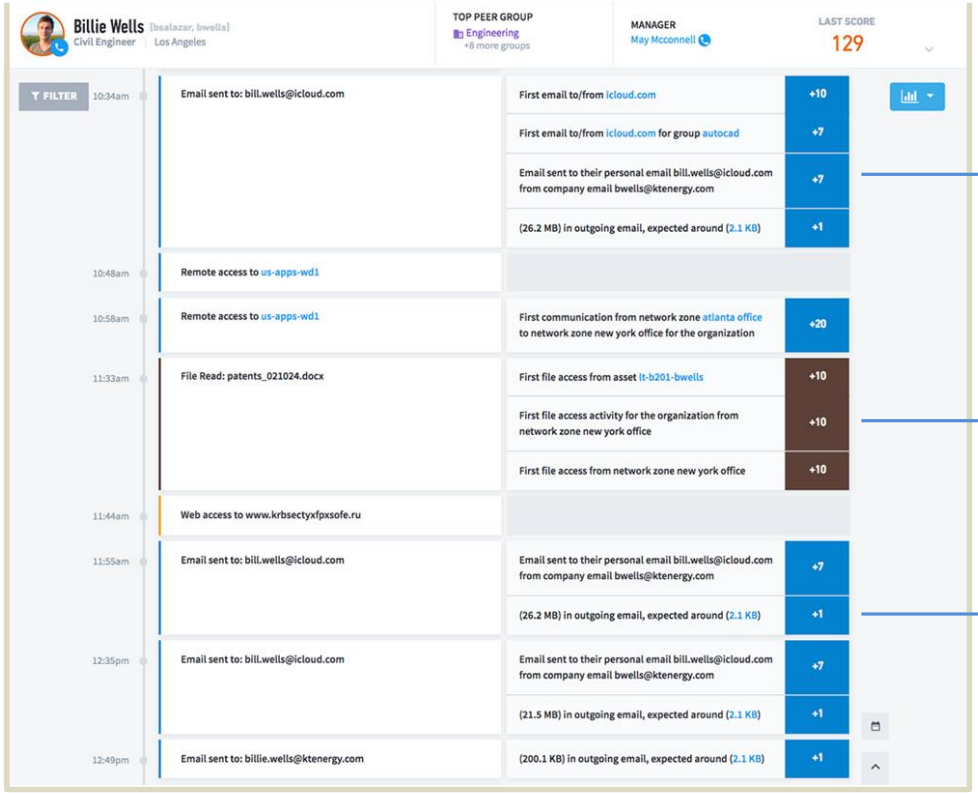
Вход под учетной записью “sa” на удаленном узле

Решения, выявляющие выгрузки данных, дают много ложных срабатываний и аналитики перегружены оповещениями от них. В результате на решения DLP затрачивается много времени на тонкую настройку или они не перестают использоваться

- Включение всех политик DLP без страха быть заваленным оповещениями
- Анализ оповещений DLP в комбинации с другими система защиты
- Машинное обучение приоритезирует оповещения DLP для сессий, где наблюдаются аномалии в поведении
- В результате: возможность обработать все оповещения, без необходимости в дополнительных ресурсах



Индикаторы DLP



Обнаружение письма, отправленного на личный ящик

Аномальный доступ к узлу для данного сегмента сети

Обнаружение нетипичных объемов данных, передаваемых по почте

Приоритезация

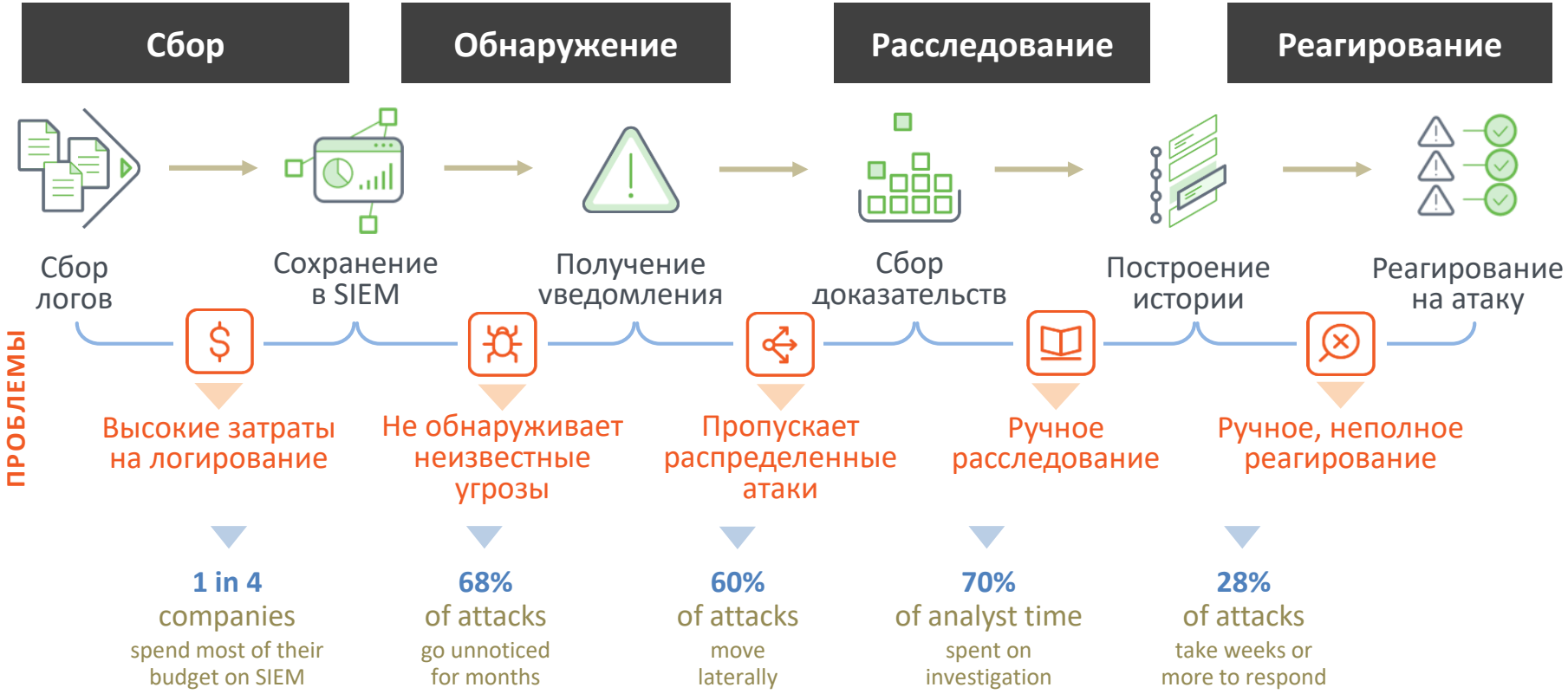
Слишком много инцидентов = очень плохо

Необходима приоритезация

- Сбор всех событий ИБ и инцидентов без чрезмерных плат
- Использование UEBA для поведенческого анализа событий с учетом всех данных событий, включая облако, рабочие станции, DLP и другие
- Машинное обучение приоритезирует инциденты
- Временная шкала повышает эффективность расследования

Gartner 2018 - SIEM

Традиционные SIEM сталкиваются с трудностями на каждом шаге



Вопросы?

Спасибо за внимание!

АО «ДиалогНаука»
Телефон: +7 (495) 980-67-76,162
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: rv@DialogNauka.ru