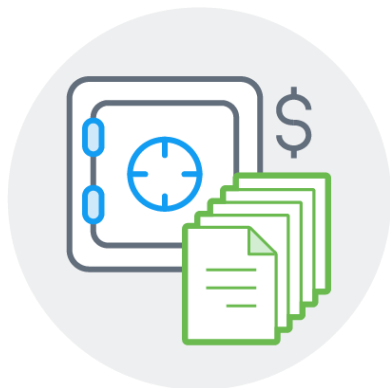
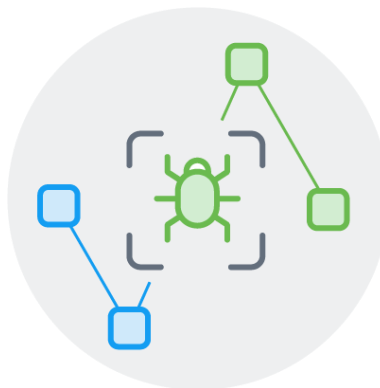

СИСТЕМА АНАЛИЗА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ EXABEAM ADVANCED ANALYTICS

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

Преимущества Exabeat



Экономия
средств на
журналировании



Улучшенное
выявление
угроз

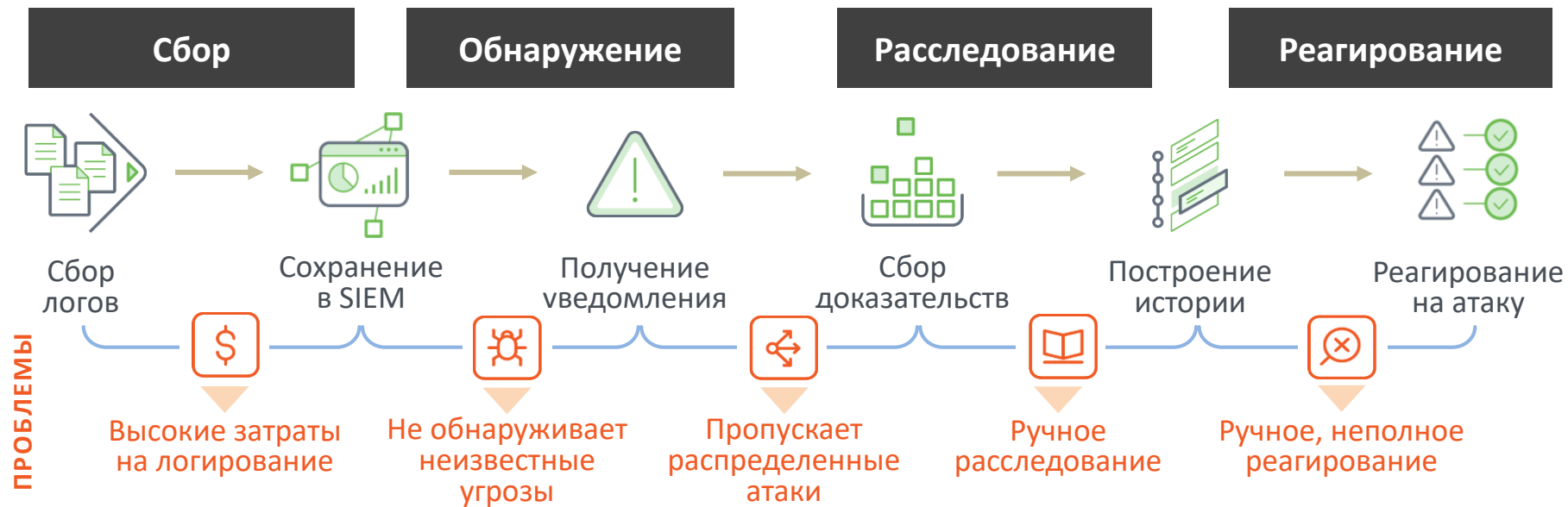


Повышение
продуктивности
аналитиков

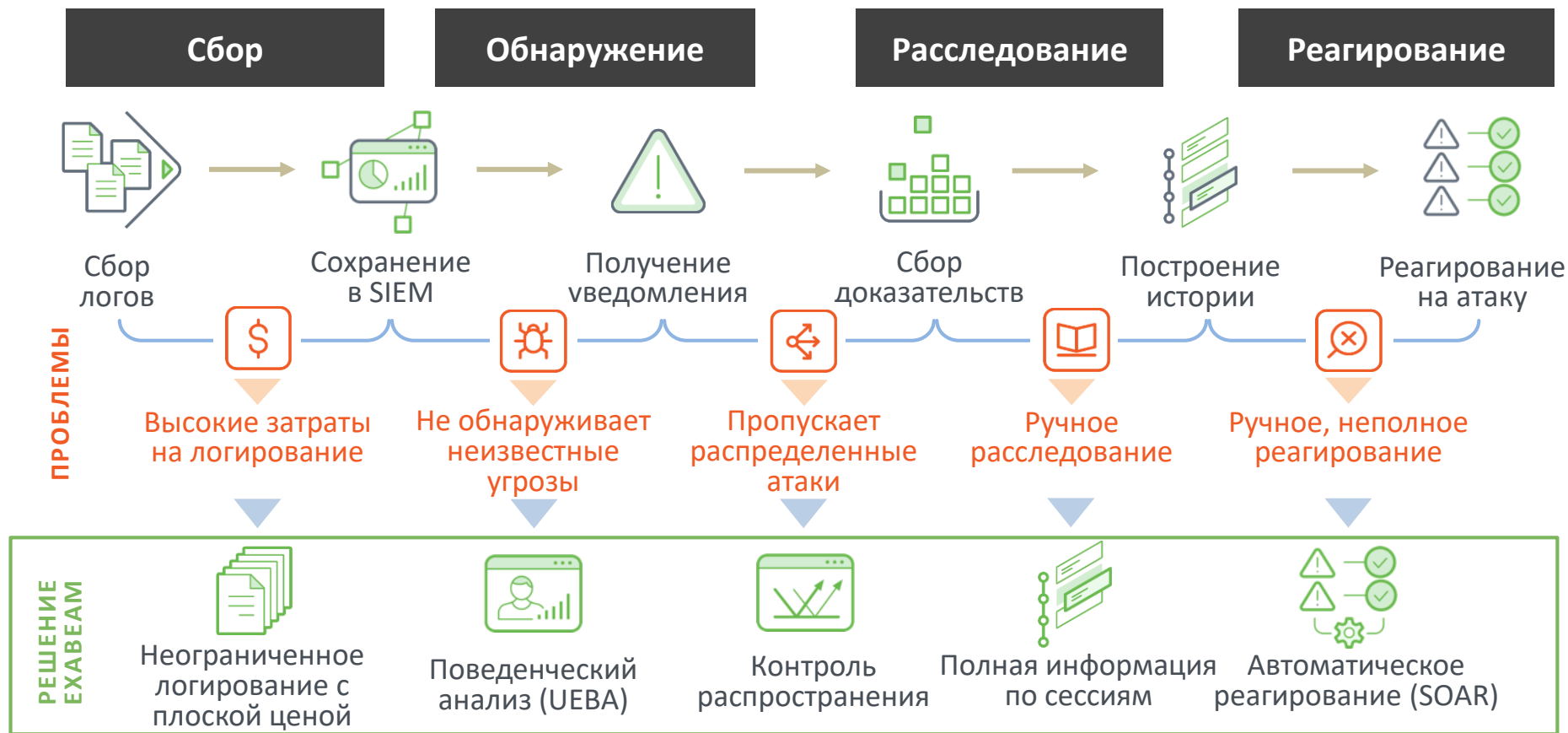
Процесс выявления инцидента в SIEM



Проблемы на каждом шаге

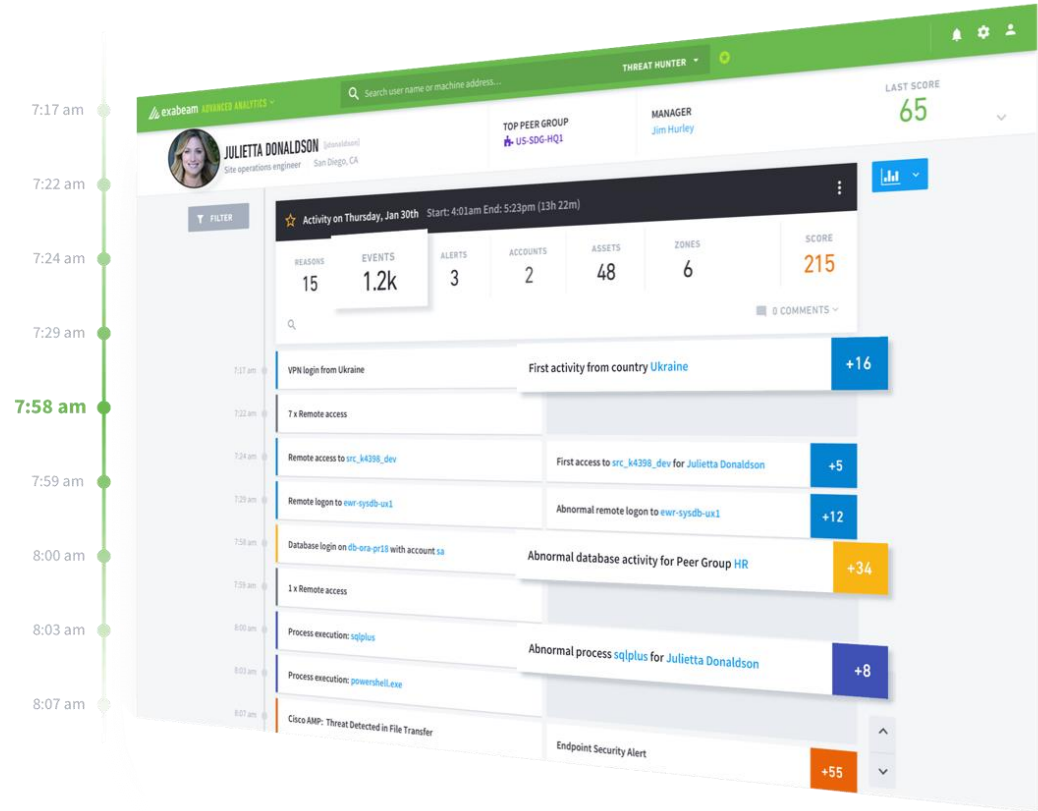


Что предлагает Exabeam



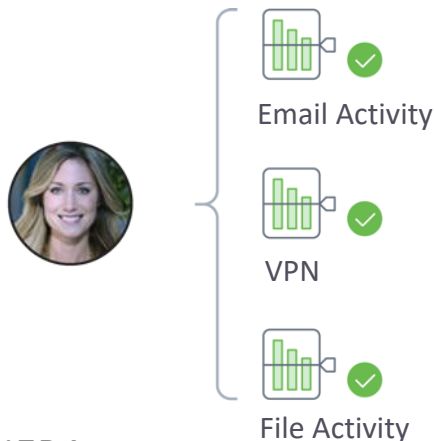
Информационная модель Exabeam

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

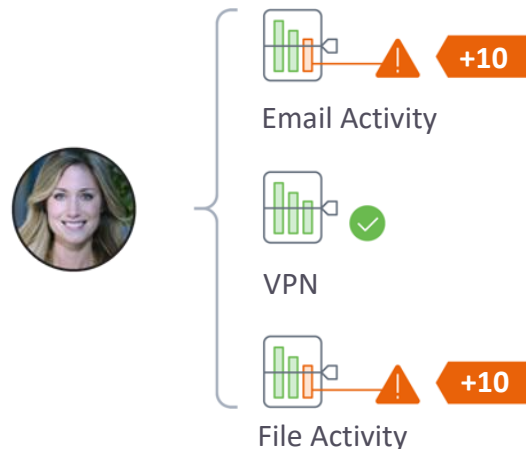


Exabeat выявляет неизвестные атаки

Все поведение пользователя
и узла смоделировано



Выявление атак в случае
аномального поведения



UEBA

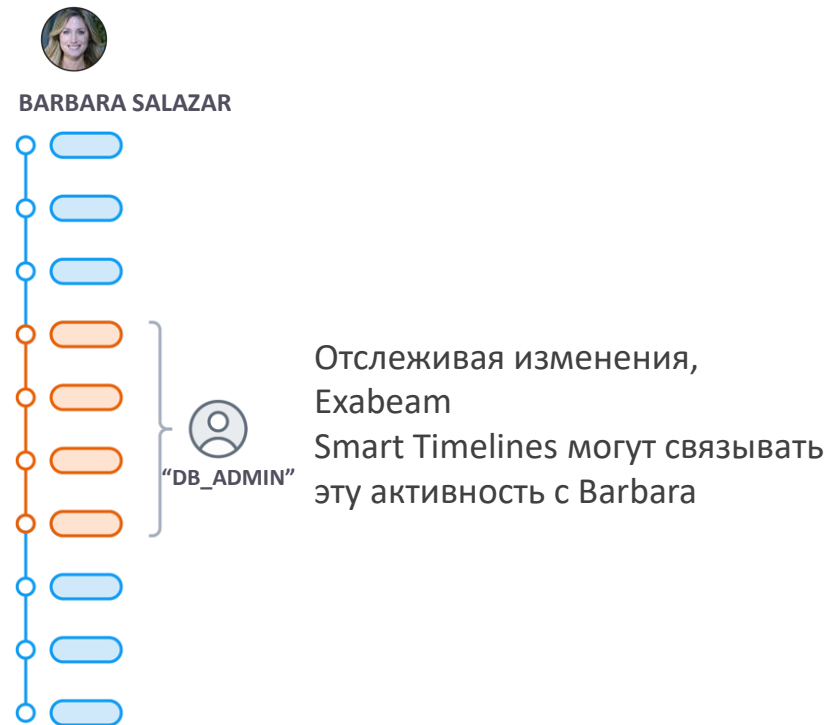
- Выявляет как известные, так и неизвестные атаки
- Не требует построения и поддержания правил корреляции для обнаружения
- Снижает ложные срабатывания за счет понимания ролей, групп и нормального поведения

Обнаружение дальнейшего распространения с Smart timeline

Lateral movement без Smart Timelines









Lateral movement с Smart Timelines



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

Неполная временная шкала

	Incomplete Timeline		
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

Другие SIEM решения

Автоматический маппинг Host-to-IP-to-User

TIME	USER	IP ADDRESS
12:03	Barry	142.1.12.68
12:03	Barry	37.4.1.23

12:03	Barry	Device_1
12:03	Barry	Device_2

TIME	IP ADDRESS	HOST
12:03	142.1.12.68	Device_1
12:03	37.4.1.23	Device_2

Полная информация

Log 1	Barry	142.1.12.68	Device_1
Log 2	Barry	142.1.12.68	Device_1
Log 3	Barry	142.1.12.68	Device_1
Log 4	Barry	37.4.1.23	Device_2
Log 5	Barry	37.4.1.23	Device_2
Log 6	Barry	37.4.1.23	Device_2

Только Exabeam

Автоматизация систем управления требует другого подхода



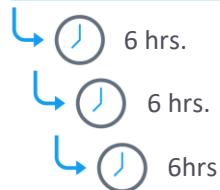
Традиционные
SIEM базируются на
событиях

Ручное действие



Аналитики должны
понимать хронологию
атаки на базе собранных
событий, чтобы
разобраться в инциденте

Query & Pivot



Gathering relevant security alerts and log events

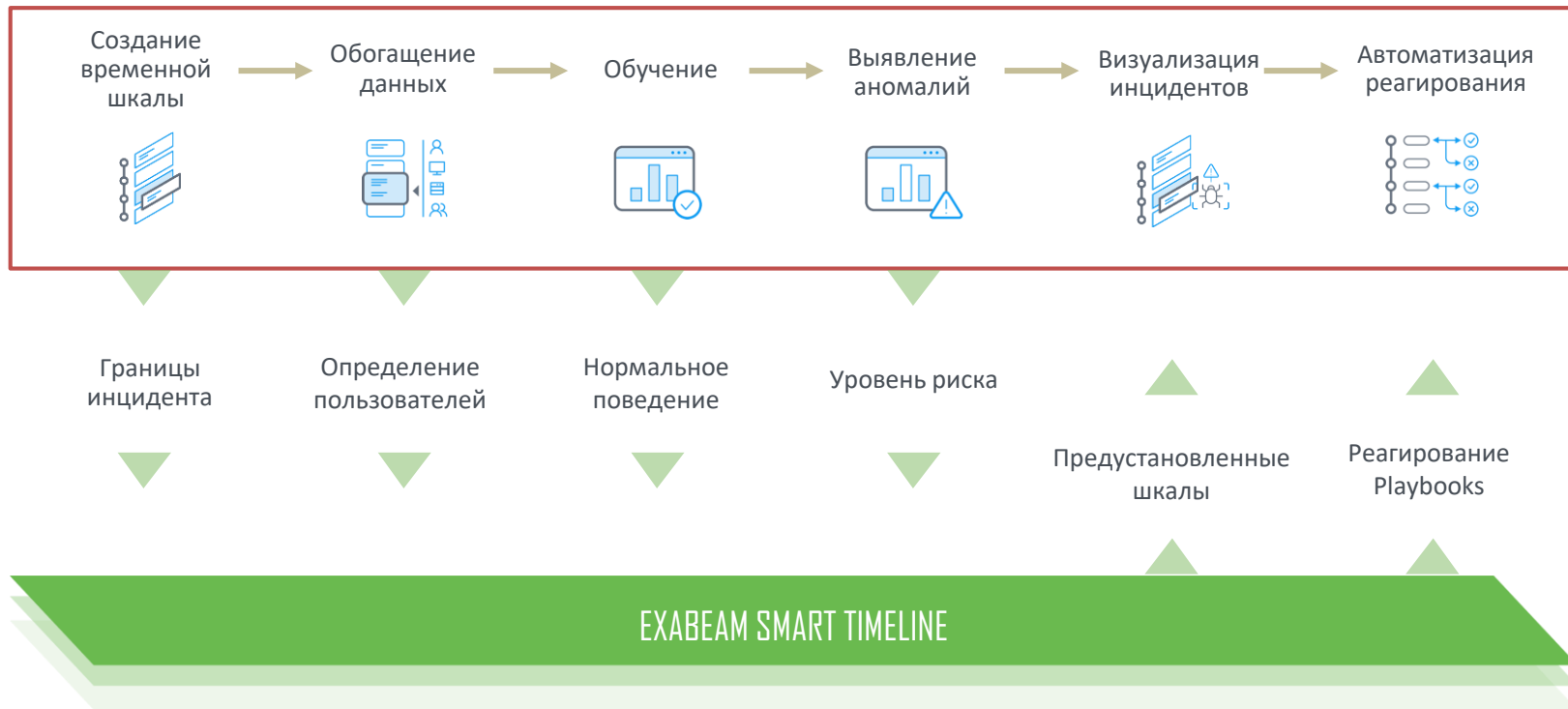
Determining how to pivot in a SIEM

Determining asset ownership

IP address to username attribution

Assembling incident and alert timelines

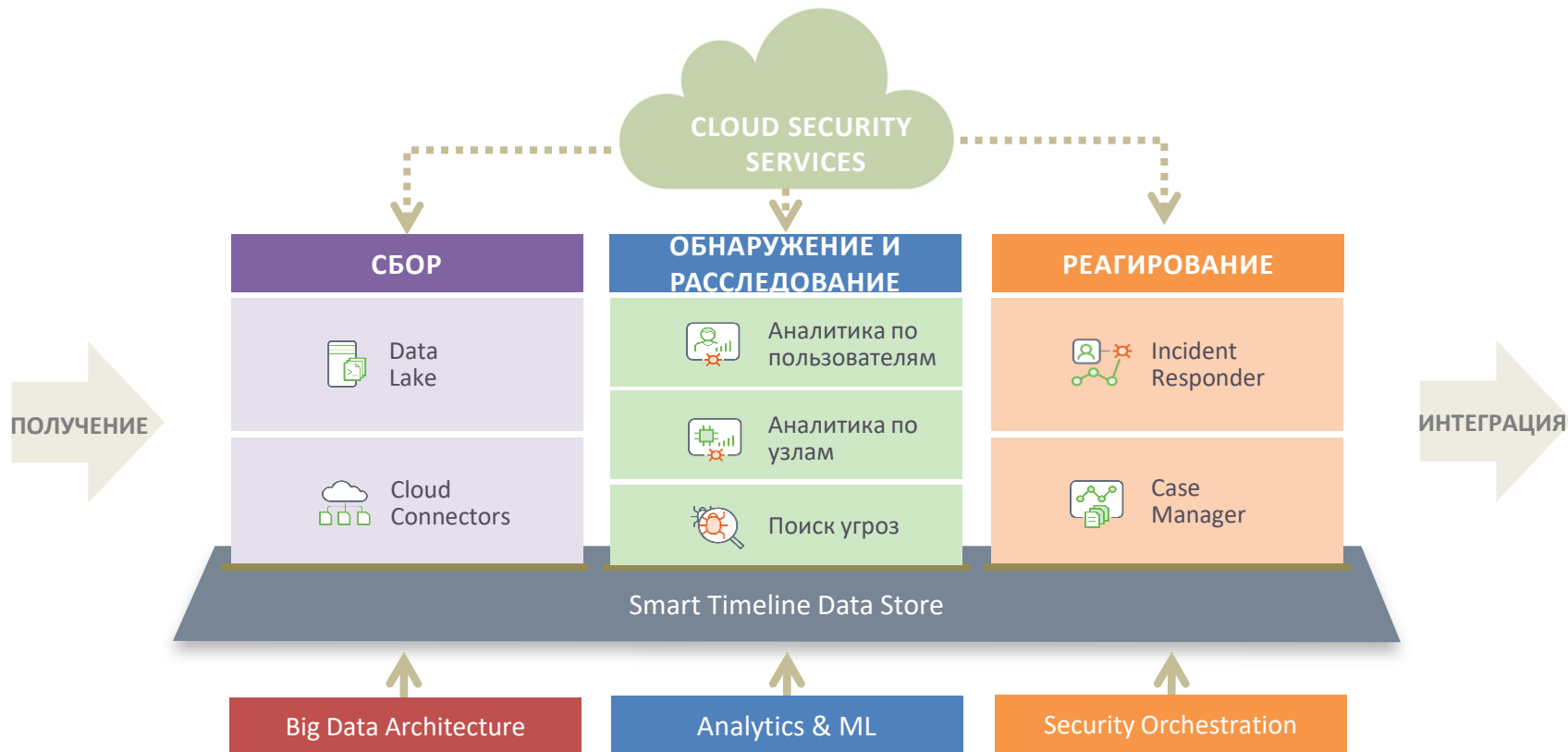
Должно начинаться со временной шкалы



Конкурентный анализ по типу технологии

	 <p>Неограниченное реагирование по фиксированной цене</p>	 <p>Анализ поведения (UEBA)</p>	 <p>Контроль распространения</p>	 <p>Автоматическое создание временных шкал</p>	 <p>Автоматизированное реагирование (SOAR)</p>
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 Exabeat



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 обновлению технологий, снижения стоимости обновления и трудозатрат



Признание рынком и клиентами

250+ Enterprise Customers



Select Awards & Recognition



РАССМОТРИМ ВОЗМОЖНОСТИ СИСТЕМЫ НА БАЗЕ НЕСКОЛЬКИХ СЦЕНАРИЕВ

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

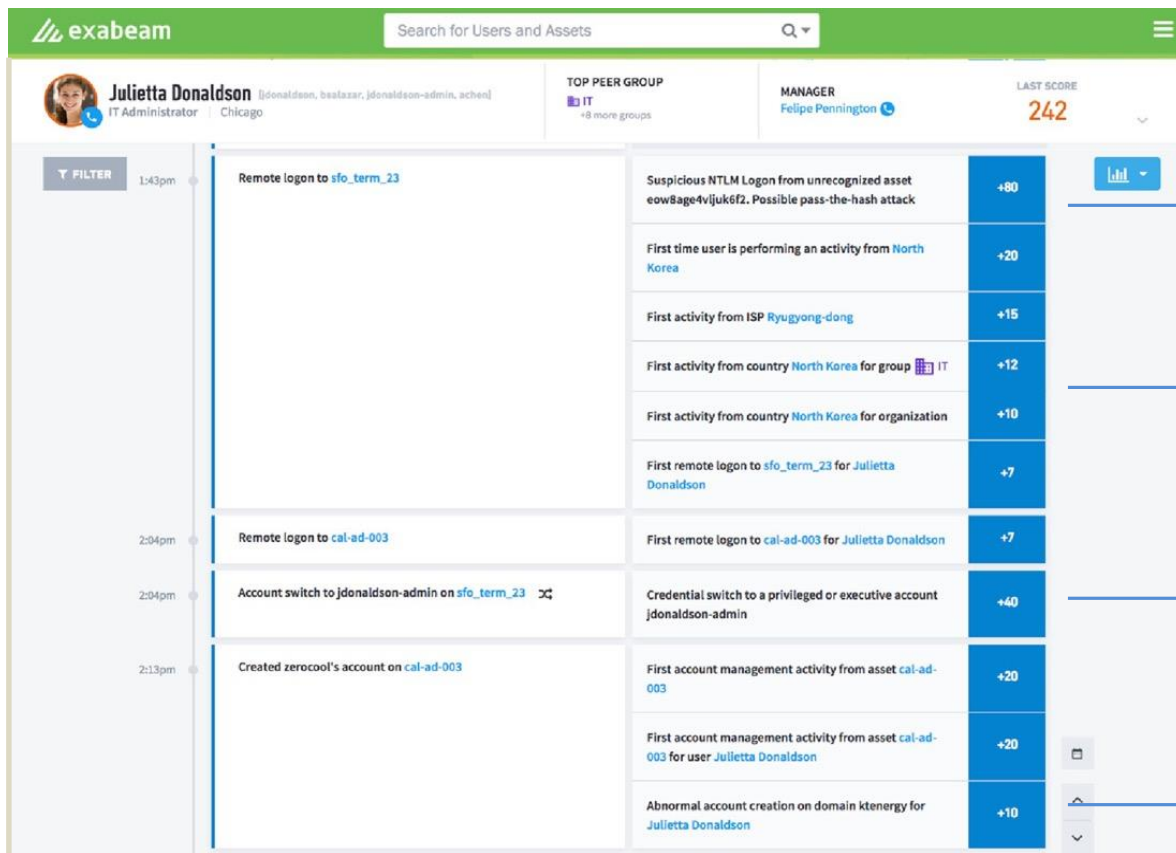
Внутренний злоумышленник

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 использованием 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

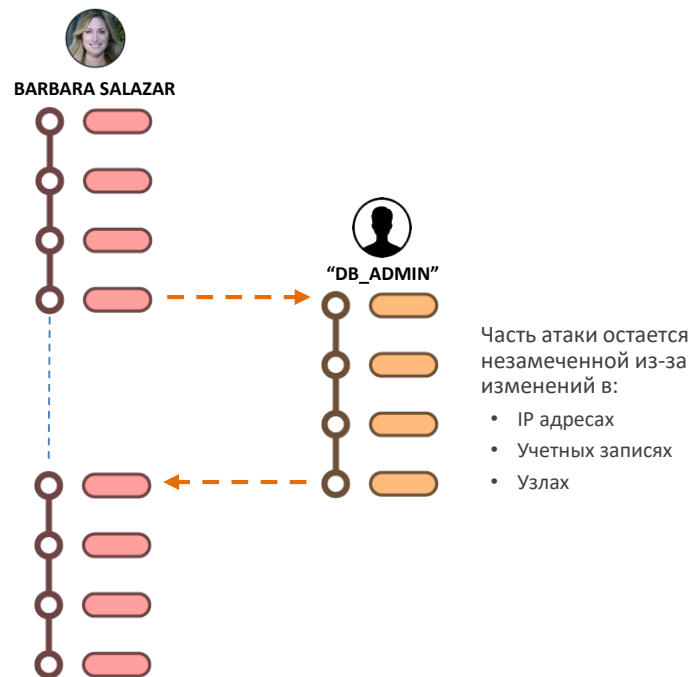
Обнаружено дальнейшее распространение
- Пользователь переключился в учетную запись администратора

Неавторизованное создание учетной записи




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
- Запатентованная 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 Exabeat

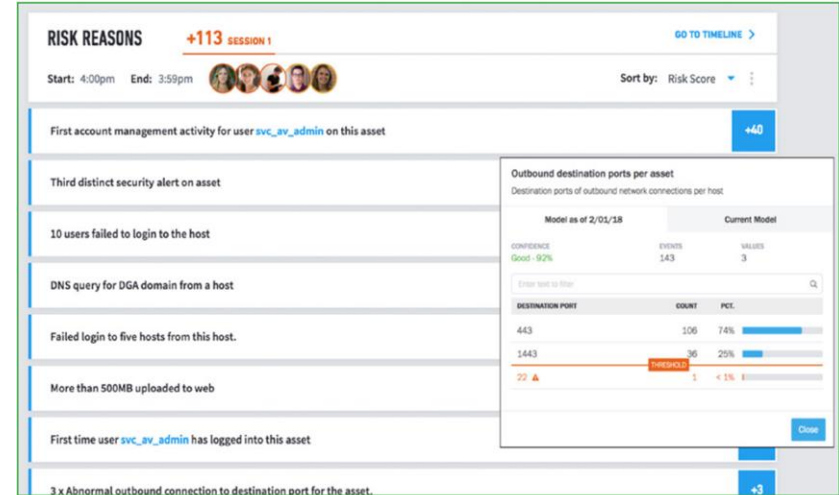
 Barbara Salazar [bsalazar, sa] Human Resources Coordinator Chicago			TOP PEER GROUP  Human Resources Coord... +6 more groups			MANAGER Tu Petersen 			LAST SCORE 272		
T FILTER 5:17am			Remote access to src_o116_dev			Abnormal access to src_o116_dev for Barbara Salazar			+5		
5:20am			Remote login to colo-sysdb-wp1			First remote login to colo-sysdb-wp1 for Barbara Salazar			+6		
			TIME	USER	ACCOUNT						
			5:20:00AM	bsalazar	sa						
			SOURCE IP	SOURCE HOST	SOURCE_ZONE						
			10.77.129.122	cc559	atlanta office						
			DEST. IP	DEST. HOST	DEST._ZONE						
			10.78.120.32	colo-sysdb-wp1	atlanta office						
			DOMAIN	REPORTING_HOST	EVENT_CODE						
			ktenergy	colo-sysdb-wp1	4624						
			PROCESS	LOGON_TYPE	EVENT_SUBTYPE						
			—	10 - RemoteInteractive	Windows						
5:31am			Account switch to sa on colo-sysdb-wp1			Credential switch to a privileged or executive account sa			+40		
			TIME	USER	ACCOUNT						
			5:31:00AM	bsalazar	sa						
			DOMAIN	REPORTING_HOST	ACCOUNT_DOMAIN						
			gcloud	colo-sysdb-wp1	—						
			DEST. HOST	DEST. IP	DEST._ZONE						
			colo-sysdb-wp1	10.78.120.32	atlanta office						
			SOURCE_HOST	SOURCE_IP	EVENT_CODE						
			cc559	10.77.129.122	4648						
			DIRECTORY	—	PROCESS						
			—	—	rdp.exe						
			SAFE/FOLDER/RESOURCE	EVENT_SUBTYPE	DEST_SERVICE						
			—	Windows	—						

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




Billie Wells

[bealazar, bwells]
Civil Engineer Los Angeles

TOP PEER GROUP


 Engineering
+8 more groups

MANAGER

May McConnell


LAST SCORE

129

<div>Y FILTER</div> <div>10:34am</div>	Email sent to: bill.wells@icloud.com	First email to/from icloud.com	+10	
		First email to/from icloud.com for group autocad	+7	
		Email sent to their personal email bill.wells@icloud.com from company email bwells@ktenergy.com	+7	
		(26.2 MB) in outgoing email, expected around (2.1 KB)	+1	
10:48am	Remote access to us-apps-wd1			
10:58am	Remote access to us-apps-wd1	First communication from network zone atlanta office to network zone new york office for the organization	+20	
11:33am	File Read: patents_021024.docx	First file access from asset it-5201-bwells	+10	
		First file access activity for the organization from network zone new york office	+10	
		First file access from network zone new york office	+10	
11:44am	Web access to www.krbsectyfxpxsofe.ru			
11:55am	Email sent to: bill.wells@icloud.com	Email sent to their personal email bill.wells@icloud.com from company email bwells@ktenergy.com	+7	
		(26.2 MB) in outgoing email, expected around (2.1 KB)	+1	
12:35pm	Email sent to: bill.wells@icloud.com	Email sent to their personal email bill.wells@icloud.com from company email bwells@ktenergy.com	+7	
		(21.5 MB) in outgoing email, expected around (2.1 KB)	+1	
12:49pm	Email sent to: billie.wells@ktenergy.com	(200.1 KB) in outgoing email, expected around (2.1 KB)	+1	

Обнаружение письма, отправленного на личный ящик

Аномальный доступ к узлу для данного сегмента сети

Обнаружение нетипичных объемов данных, передаваемых по почте

Слишком много инцидентов = очень плохо

Необходима приоритезация

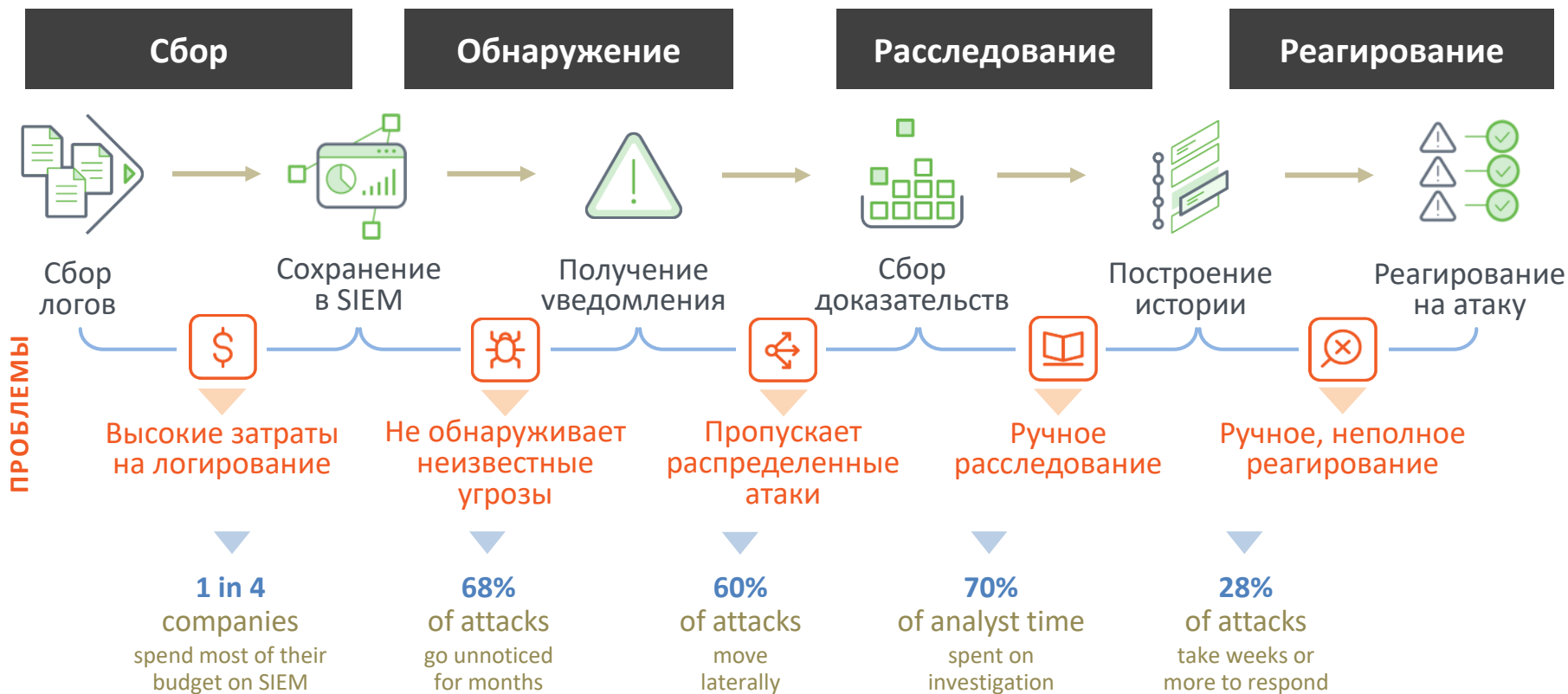
- Сбор всех событий ИБ и инцидентов без чрезмерных плат
- Использование UEBA для поведенческого анализа событий с учетом всех данных событий, включая облако, рабочие станции, DLP и другие
- Машинное обучение приоритезирует инциденты
- Временная шкала повышает эффективность расследования



Gartner 2018 - SIEM



Традиционные SIEM сталкиваются с трудностями на каждом шаге



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