Специальное исследование

Оценка уровня удовлетворенности системами SIEM, установленными в организациях в России

Ксения Ефимова Марк Чайлд

МНЕНИЕ IDC

- Проведенный опрос показывает, что российский рынок SIEM далек от насыщения: средний уровень проникновения среди российских организаций не превышает 15%. Эта величина может сильно колебаться в зависимости от размера организаций, их отраслевой принадлежности, сферы деятельности. Более того, опрос выявил, что не все ИТ-специалисты хорошо знакомы с SIEM-системами. Такая ситуация представляет собой существенную возможность – не только с точки зрения рыночного потенциала, но и в связи с вероятным эффектом от кампаний по ознакомлению потенциальных потребителей с концепцией SIEM и по продвижению таких решений.
- Организации, планирующие внедрение SIEM, должны ориентироваться на тех поставщиков, у которых есть своя экспертиза в области безопасности, и которые предлагают системы SIEM, способные обнаруживать новые угрозы и наименее подверженные действию «человеческого фактора». Возможности автоматизации и оркестрации могут существенно облегчить бремя управления инцидентами, снижая нагрузку на корпоративных экспертов по безопасности и позволяя им сосредоточиться на наиболее критичных задачах, а также на стратегии безопасности.
- Большинство пользователей удовлетворены работой систем SIEM. Тем не менее, 32% респондентов выразили неудовлетворенность тем, как работает внедренная у них система. В их ответах просматриваются следующие заслуживающие внимания проблемы: необходимость значительных регулярных вложений в поддержку системы, дефицит квалифицированных специалистов в области ИБ, а также неспособность систем выявлять новые угрозы до наступления инцидента (хакеры имеют очевидное преимущество в этой «гонке вооружений»).
- Конечные пользователи должны принимать во внимание, что системы SIEM требуют серьезных инвестиций. Однако, успешное внедрение и эффективное использование системы SIEM не только существенно повышает уровень безопасности, но в долгосрочной перспективе помогает снизить затраты на информационную безопасность и ИТ в целом.

В ЭТОМ ИССЛЕДОВАНИИ

Определение SIEM

IDC определяет Security intelligence and event management (SIEM) как продукты, предназначенные для сбора данных из различных источников с целью выявления последовательностей событий, которые могут означать атаки, вторжения, злоупотребления или выход из строя. Выявление корреляций между сетевыми событиями упрощает и ускоряет их мониторинг за счет консолидации оповещений и журнала ошибок в краткий, легкий для понимания формат. Продукты могут также консолидировать и хранить обработанные с помощью SIEM данные журнала. SIEM также включает в себя продукты, которые собирают и распространяют информацию об угрозах, предоставляют услуги раннего предупреждения об угрозах, а также могут давать информацию о контрмерах. Данные из продуктов SIEM передаются тем ИТ-решениям, которые управляют политиками и соответствием регулятивным требованиям, для последовательного представления в отчетности.

Методология

Компания Positive Technologies обратилась к IDC с просьбой провести опрос с целью оценки удовлетворенности российских организаций системами SIEM.

- Опрос проводился среди компаний-пользователей SIEM на следующих вертикальных рынках: «Ресурсы и энергетика» (добыча, извлечение и переработка полезных ископаемых, выработка электроэнергии), «Дискретное и процессное производство», «Финансовые услуги» (банки, страховые компании, услуги в сфере ценных бумаг и инвестиций), «Торговля» (розничная и оптовая), «Государственный сектор», «Операторы связи».
- Опрос был разработан IDC и одобрен заказчиком до начала его проведения.
- Сбор данных осуществлялся с помощью методов CATI и CAWI.
- Респонденты были сотрудниками компаний, наиболее осведомленными об использовании систем SIEM (например, директора по безопасности или старшие специалисты по безопасности).
- Размер выборки n = 102.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

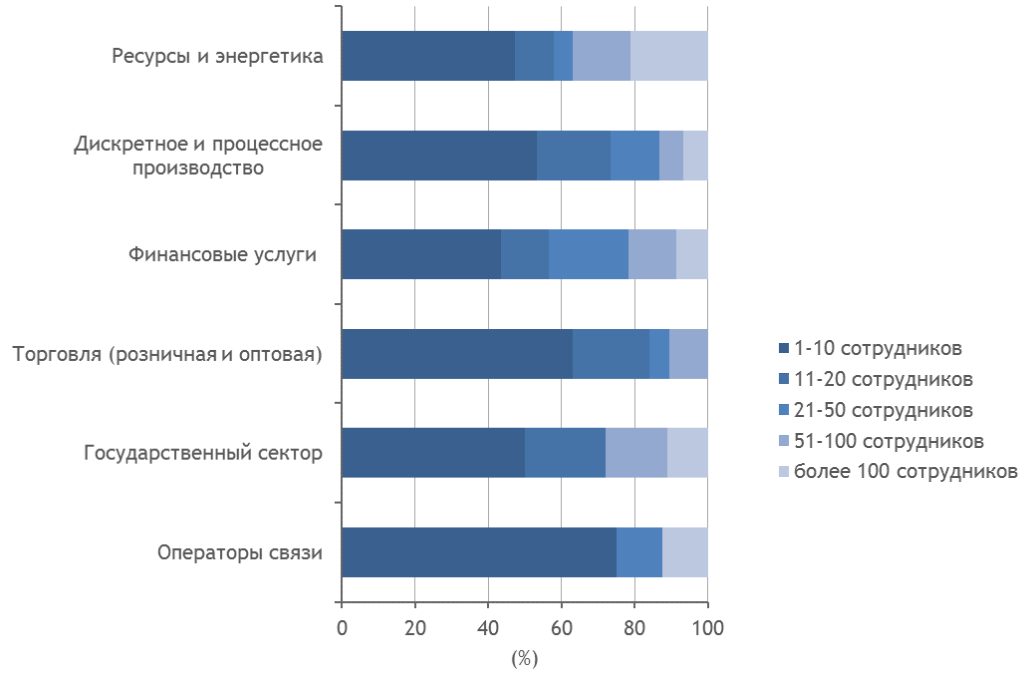
Q1. Сколько сотрудников в вашей организации занимаются информационной безопасностью?

В целом по выборке 26,5% организаций имеет до 5 человек, занимающихся ИТ-безопасностью, и столько же - от 5 до 10 человек. Еще 15,7% имеют 10-20 специалистов, а остальные 31,4% - более 20. Количество людей, занятых в ИТ-безопасности в компаниях, сильно варьируется в зависимости от размера компании и ее отраслевой принадлежности. Как и ожидалось, чем крупнее компания, тем больше в ней людей, занимающихся ИТ-безопасностью: например, свыше 50% предприятий с более чем 5000 сотрудниками имеют в штате 50 или больше человек, занятых обеспечением ИТ-безопасности. Напротив, почти в половине предприятий с менее чем 500 сотрудниками всего 1-2 специалиста занимаются вопросами ИТ-безопасности.

Размеры выборок после разделения респондентов по отраслям оказываются слишком маленькими для того, чтобы результаты были статистически значимыми. Однако можно заметить, что в секторе «Ресурсы и энергетика» обеспечением безопасности занимаются большие группы (свыше 50 сотрудников), а в финансовом секторе - 20 или более сотрудников.

РИСУНОК 1

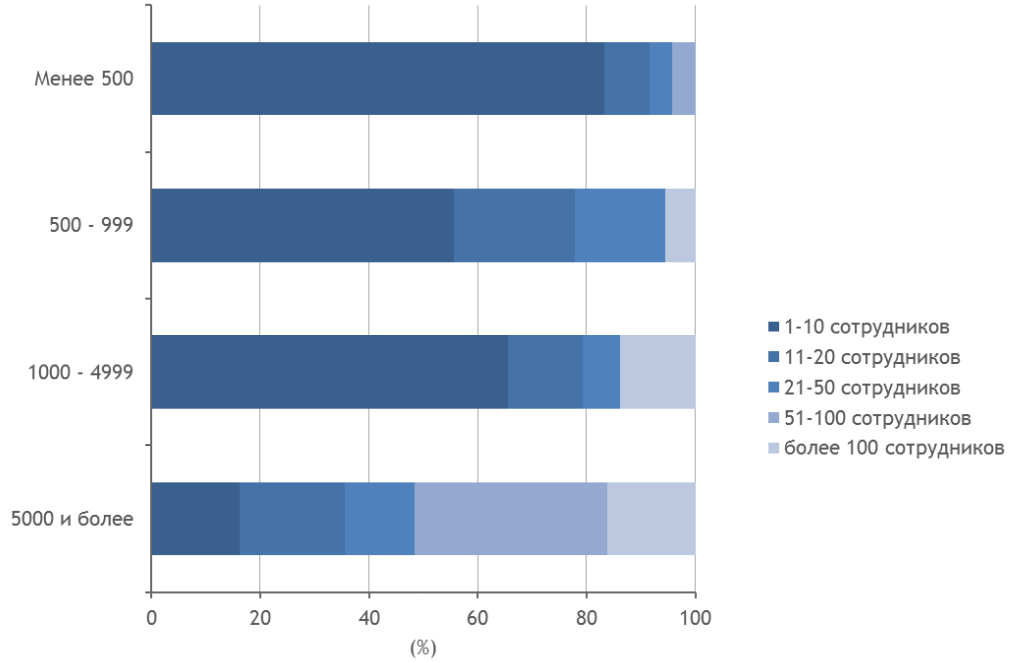
Число сотрудников ИБ в компаниях-респондентах по секторам



Источник: IDC, 2018

РИСУНОК 2

Число сотрудников ИБ в компаниях-респондентах по размеру компаний



Источник: IDC, 2018

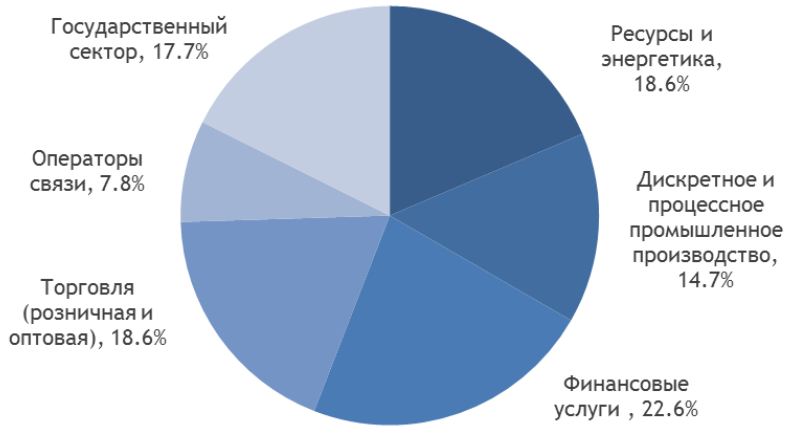
Q2: К какой отрасли относится ваша компания?

Опрос проводился на следующих вертикальных рынках:

- «Ресурсы и энергетика» (добыча, извлечение и переработка полезных ископаемых, выработка электроэнергии)
- «Дискретное и процессное производство»
- «Финансовые услуги» (банки, страховые компании, услуги в сфере ценных бумаг и инвестиций)
- «Торговля» (розничная и оптовая)
- «Государственный сектор»
- «Операторы связи»

РИСУНОК 3

Отраслевая структура компаний-респондентов

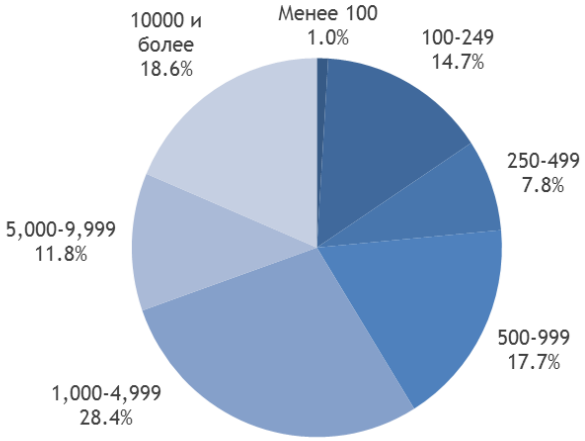


Источник: IDC, 2018

По размеру компании-респонденты распределены следующим образом:

РИСУНОК 4

Структура компаний-респондентов по числу сотрудников



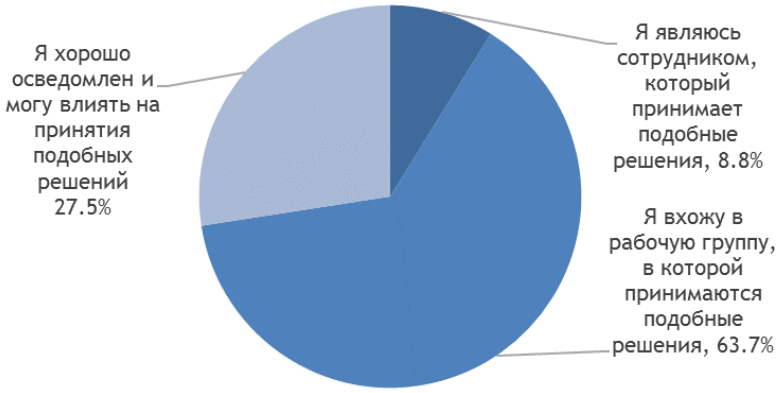
Источник: IDC, 2018

Q3. Что из нижеперечисленного лучше всего описывает ваше участие в принятии решений по ИТ-безопасности, влияющих на вашу организацию?

Приблизительно 64% проинтервьюированных были членами рабочих групп, принимающих решения, связанные с информационной безопасностью. Остальные респонденты имеют право принимать такие решения в индивидуальном порядке или оказывают влияние на принятие таких решений. На стадии скрининга интервью прерывалось, если респондент оказывался не вовлечен в процесс принятия решений по безопасности.

РИСУНОК 5

Статус лиц, отвечавших на вопросы, в компаниях-респондентах



Источник: IDC, 2018

Q4. Есть ли у вас внедренные системы SIEM?

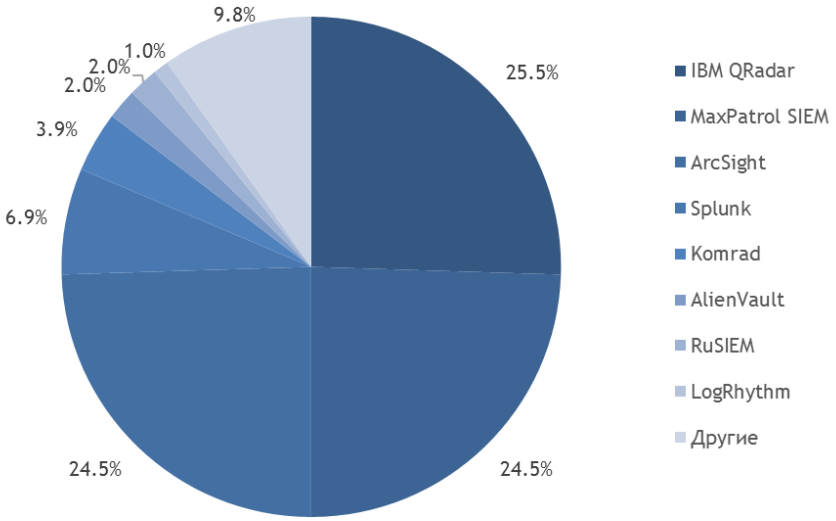
Первоначальная оценка уровня насыщения российского рынка SIEM была произведена на первом этапе исследования, в ходе которого были опрошены 100 российских организаций. В полном варианте опроса приняли участие те организации, которые ответили положительно на этот вопрос. Другие организации с установленными системами SIEM, вошедшие в окончательную выборку (n = 102), были определены и опрошены позже. После первого раунда скрининговых интервью был установлен контакт еще с более чем 1000 российских компаний, которые, как выяснилось, не используют SIEM. В целом по результатам всех скрининговых интервью оказалось, что проникновение SIEM в российских организациях составляет менее 15%.

Q5. Какие решения SIEM вы используете?

Тремя лидерами российского рынка систем SIEM являются, со значительным отрывом, IBM QRadar, MaxPatrol SIEM и ArcSight, каждой из которых пользуется примерно четверть выборки. Из остальных только Splunk внедрен более чем у 5 респондентов.

РИСУНОК 6

Доля рынка SIEM в России, занимаемая различным системами



Источник: IDC, 2018

Небольшая часть организаций назвали SIEM, отсутствующие в списке, или отказались назвать внедренную систему. Они объединены в группе "Другое". Эти компании работают в секторах «Дискретное и процессное производство», «Торговля» (розничная и оптовая), «Операторы связи».

Просматриваются некоторые отраслевые предпочтения:

- ArcSight преобладает в секторе «Ресурсы и энергетика», доля 47%;
- IBM QRadar доминирует (62%) в секторе «Операторы связи», но там малая выборка;
- Использование систем SIEM в секторе «Финансовые услуги» имеет более сбалансированный характер; ArcSight, Splunk и QRadar занимают там первое, второе и третье место соответственно;
- MaxPatrol SIEM, продукт Positive Technologies, лидирует в секторах «Дискретное и процессное производство», «Торговля» (розничная и оптовая) и «Государственный сектор»;
- QRadar – единственная другая система с заметной долей в «Государственном секторе».

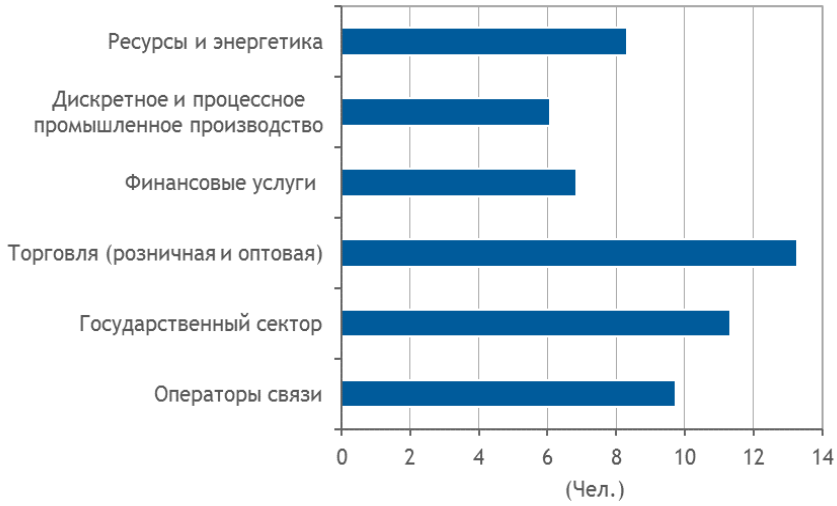
Можно ожидать, что организации из российского государственного сектора будут предпочитать отечественные системные решения. MaxPatrol SIEM может рассматриваться торговыми и производственными компаниями, а также представителями энергетиков и операторов связи, как более доступный. Прочие локальные системы, такие как Komrad и RuSIEM, имеют ограниченное проникновение даже на российском рынке.

Q6. Сколько человек работает на регулярной основе с системами SIEM?

В среднем, в опрошенных компаниях работают с SIEM на регулярной основе 9 сотрудников. Отметим, что некоторые организации задействуют для работы с SIEM сравнительно большие команды; медианное же количество сотрудников, которое может более точно характеризовать ситуацию в большинстве компаний, составляет 5 человек на организацию.

РИСУНОК 7

Среднее число сотрудников, работающих с SIEM, в компаниях-респондентах по секторам



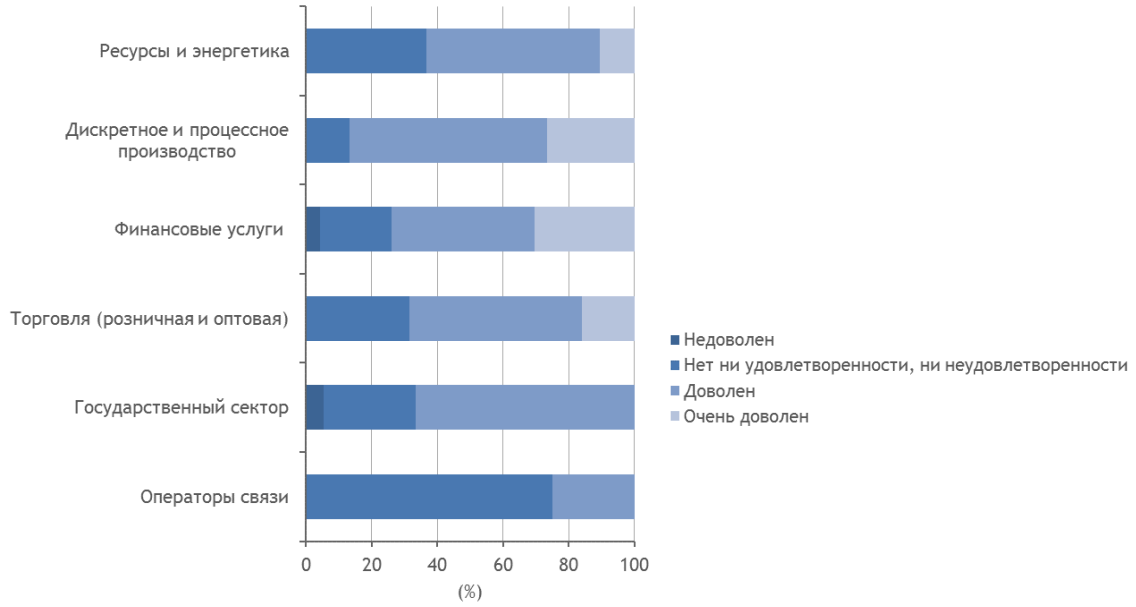
Источник: IDC, 2018

Q7. Насколько вы удовлетворены эффективностью обнаружения инцидентов с использованием системы SIEM?

Большинство (68%) потребителей SIEM удовлетворены или очень удовлетворены эффективностью системы в выявлении инцидентов. 30% были нерешительны в своих оценках, заявив, что они ни довольны, ни недовольны внедренной у них системой. Лишь незначительное меньшинство - 2% респондентов - выразило неудовлетворенность существующим решением. В остальном, в плане вертикальных рынков, у компаний не было особых различий в степени удовлетворенности их решением SIEM; это справедливо и для компаний разных размеров.

РИСУНОК 8

Степень удовлетворенности используемой системой SIEM в компаниях-респондентах по секторам



Источник: IDC, 2018

Q8. Каковы причины вашего недовольства текущей SIEM?

Основными причинами недовольства существующей системой являются: зависимость от экспертов, необходимость инвестировать в постоянную поддержку, а также неспособность SIEM обнаруживать новые угрозы до инцидента - считается, что инструментарий хакеров гораздо богаче и пополняется чаще, чем происходят обновления SIEM. Компании также назвали несколько других причин, которые не были перечислены в опросе и могут быть объединены в три группы:

- Недостаточно быстрая реакция SIEM;
- Трудности, связанные с настройкой системы;
- Не хватает функциональности (отсутствие статистических отчетов, отсутствие возможности интеграции с другими системами).

РИСУНОК 9

Причины неудовлетворенности системой SIEM, указанные компаниями-респондентами

Источник: IDC, 2018

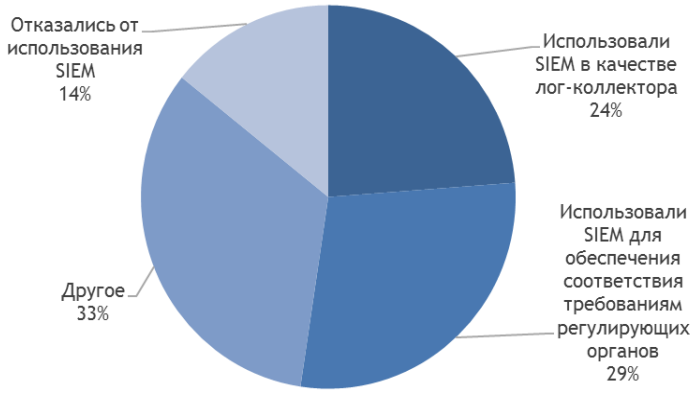
Q9: Считаете ли вы, что использование SIEM требует слишком больших инвестиций в регулярную поддержку системы? Если да, то пытались ли вы оптимизировать ее стоимость? Если да, то каким образом вы пытаетесь оптимизировать ее стоимость?

По словам 47% респондентов, использование системы SIEM требует слишком больших вложений. Компании средних размеров (менее 1000 сотрудников) ощущают это сильнее, чем крупные организации (1000 и более сотрудников). Попытки оптимизировать затраты были сделаны в 44% тех организаций, которые ответили утвердительно на предыдущий вопрос.

Организации по-разному оптимизировали издержки на свои системы SIEM: одни компании использовали ее для обеспечения соответствия требованиям регулирующих органов, другие – в качестве лог-коллектора, а некоторые – для автоматизации процессов. Кроме того, компании пытались использовать дополнительные настройки системы SIEM, использовали ее только для критически важных проблем или попросту меняли систему.

РИСУНОК 10

Как вы пытались оптимизировать стоимость поддержки SIEM?



Источник: IDC, 2018

Q10. Пожалуйста, оцените расходы на поддержку SIEM в виде процента от общего бюджета информационной безопасности в прошлом финансовом году

Почти 70% респондентов указали, что стоимость поддержки составляет до 25% от общего бюджета ИБ, еще 26% сообщили, что эта стоимость меньше 50% бюджета. Очень немногие организации отметили, что они расходовали на SIEM более 50% своего ИБ-бюджета. Среднее отношение стоимости поддержки системы SIEM к общей сумме бюджета ИБ составляло около 20%.

Q11: Рассматриваете ли вы возможность замены существующей системы SIEM на новую?

Несмотря на то что респонденты отметили различные проблемы и ограничения в имеющихся у них системах SIEM, только 34% рассматривают возможность замены системы SIEM, причем большинство из них - 60% - планирует это сделать из-за политики импортозамещения.

На открытый вопрос анкеты «Каковы ТОП-3 требования к SIEM-системе?» респонденты могли дать три ответа в произвольной форме. Невзирая на большое разнообразие формулировок у респондентов, оказалось возможным выделить несколько групп этих ответов, касающихся той или иной стороны процесса выбора и использования SIEM

Упомянуто более 10 раз:

- Цена/ценность (стоимость, эффективность, окупаемость)
- Надежность (стабильность, безопасность, отсутствие неполадок)

Упомянуто 5-10 раз:

- Эффективная идентификация и фиксация событий, установление их корреляций
- Пользовательский опыт (удобство использования, гибкость)
- Быстрый сбор, обработка, хранение больших объемов данных

Можно отметить, что эти ответы указывают на типичные дилеммы (цена vs. надежность, надежность vs. гибкость), с которыми сталкиваются руководители бизнес-подразделений и служб ИБ, и над разрешением которых работают компании, предлагающие SIEM-системы.

Q12. Планируете ли вы продолжать использовать систему SIEM в ближайшие 5 лет?

Большинство респондентов (97%) намерено продолжать использование систем SIEM, и только несколько респондентов из секторов «Дискретное и процессное производство» и «Торговля» планируют прекратить их использование. Таким образом, можно сделать вывод, что, невзирая на проблемы, упомянутые в ответах на вопросы 7-9, и на требования к ресурсам, компании в целом признают ту ценность, которую SIEM приносит в работу системы безопасности и в обеспечение ИБ организации в целом.

РЕКОМЕНДАЦИИ

- Пользователи должны принимать во внимание то, что системы SIEM требуют серьезных инвестиций, и планировать ежегодное выделение до 25% своего бюджета ИБ на SIEM. При этом успешное внедрение и эффективное использование системы SIEM не только существенно повысит уровень безопасности, но и поможет снизить затраты на информационную безопасность и на ИТ в целом в долгосрочной перспективе.
- Организации должны также соотнести стоимость системы SIEM с многообразными издержками, возникающими при утечке данных: стоимость восстановления или замены системы, стоимость простоя, потерю интеллектуальной собственности, потерю доверия и репутации, потерю клиентов (их переход к конкурентам), ущерб отношениям с партнерами, возможные штрафы и другие санкции. Многие из этих элементов становятся все более значимы по мере того, как компании совершают переход к цифровому бизнесу, и ценность их цифровых активов и данных возрастает. Руководители высшего звена часто недооценивают масштабы издержек, описанных выше, и возражают против видимой дороговизны систем SIEM. Менеджеры по ИТ и безопасности должны работать со своим предпочтительным поставщиком SIEM над обоснованием ROI для системы и представлять соответствующие бизнес-кейсы своим советам директоров.
- Исследования IDC в Западной Европе и США показали ту огромную цену, которую компании платят за инциденты безопасности при обработке данных - платят временем и трудозатратами. Отдельное исследование Vanson Bourne оценивает соотношение стоимости человеческого труда и технологических расходов в управлении инцидентами как 40:1 и более. Развертывание и интеграция платформы SIEM, оптимизация ее конфигурации, использование всех ее возможностей в плане автоматизации и оркестрации могут очень существенно помочь в решении этих ресурсных проблем.
- Компаниям, планирующим внедрить системы SIEM, следует:
  - Выбирать тех поставщиков систем SIEM, у которых есть своя экспертиза в области безопасности, и которые предлагают системы SIEM, способные обнаруживать новые угрозы и наименее подверженные действию «человеческого фактора».
  - Разработать долгосрочную «дорожную карту», позволяющую извлечь максимальный эффект из системы SIEM. Как правило, чем больше компетенций наработала компания и чем более интенсивно в ней работают с системой, тем больше пользы она приносит.
  - Исходить из того, что системы SIEM, безусловно, не относятся к решениям, работающим по принципу «включил и работай» или «настроил и забыл» - и что при их внедрении невозможно добиться всех поставленных целей за несколько месяцев. Следует для начала сосредоточиться на защите критически важных систем и активов, спланировать постепенное расширение охвата и разработку процессов и политик, а также запустить непрерывно действующую программу подготовки и образования для сотрудников, позволяющую наработать необходимые знания и навыки.
- Проведенные интервью выявили не только невысокий уровень проникновения SIEM, но и недостаточное понимание сущности этих решений, выполняемых функций и приносимых ими благ. Например, на вопрос о том, какой системой они пользуются, некоторые компании упомянули продукт «Лаборатории Касперского» – решение для безопасности конечных устройств, а не SIEM. Рынок нуждается в образовательной и рекламной деятельности - от поставщиков и их партнеров до служб ИТ и

безопасности, от служб ИТ и безопасности до менеджеров и членов совета директоров.

- Поставщикам SIEM-систем стоит направить усилия на усовершенствование функционала в двух направлениях:
  - Более оперативное выявление инцидентов
  - Снижение потребности в обслуживании системы высококвалифицированными экспертами.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Подробные результаты опроса и опросник, а также аудиозапись интервью прилагаются.

О компании IDC

International Data Corporation (IDC) – ведущий поставщик информации, консультационных услуг и организатор мероприятий на рынках информационных технологий, телекоммуникаций и потребительской техники. IDC помогает профессионалам ИТ, руководителям и инвесторам принимать обоснованные решения о закупке техники и выборе бизнес-стратегии. Более 1100 аналитиков IDC в 110 странах изучают технологии, тенденции и возможности отрасли на мировом, региональном и местном уровнях. Уже 50 лет IDC помогает своим клиентам в решении важнейших задач. IDC – дочернее предприятие IDG, компании, лидирующей на мировом рынке ИТ-изданий, исследований и специализированных мероприятий.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com