



Отчет по итогам опроса

Трудозатраты

специалистов по ИБ

на работу с SIEM-системами

Содержание

| | |
|--|----|
| Ключевые результаты | 2 |
| Профиль респондентов | 3 |
| Отрасль | 3 |
| Размер компании | 3 |
| Трудозатраты на работу в SIEM-системе | 4 |
| Ежедневные трудозатраты | 4 |
| Динамика трудозатрат | 5 |
| Наиболее трудоемкие действия в SIEM-системе | 6 |
| Как помочь специалистам по ИБ снизить трудозатраты | 8 |
| Заключение | 9 |
| Приложение. Опросник | 10 |

Г Ключевые результаты

Мы провели анонимный опрос среди специалистов по ИБ. Цель исследования — узнать, сколько времени они проводят за работой в SIEM-системах, какие задачи занимают больше всего времени и как можно снизить трудозатраты.

Опрос проводился с 27 августа по 17 сентября 2019 года. Предварительно мы попросили пять специалистов по ИБ, работающих с SIEM-системами, ответить на вопросы в анкете — и затем по их рекомендациям дополнили ее тремя вариантами ответа. В итоге в анкету вошло 9 вопросов.

Опрос был размещен на официальном сайте Positive Technologies, анкета также распространялась на интернет-порталах, посвященных ИБ, в тематических чатах в Телеграме и в социальных сетях. Мы получили 225 заполненных анкет.

Результаты:

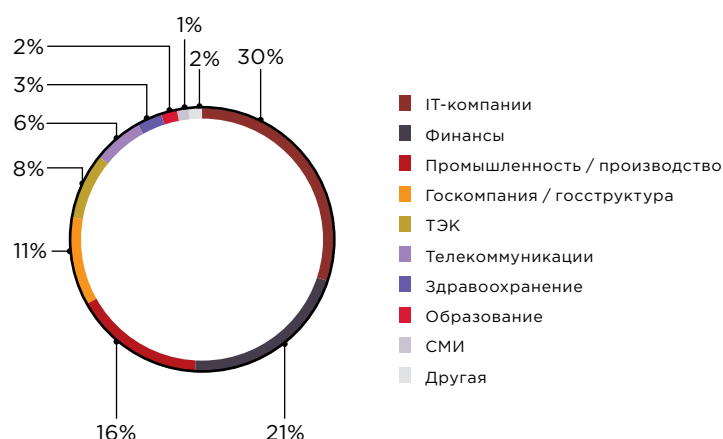
- Почти в 70% случаев с SIEM-системой в компаниях работают не более пяти специалистов по ИБ, чаще всего (47% случаев) один-два человека.
- Ежедневно в SIEM-системе проводят от двух до четырех часов 25% опрошенных, больше половины рабочего дня — 22%. Причем 62% респондентов отметили, что за последний год время работы увеличилось.
- Больше половины респондентов регулярно разбирают инциденты, отслеживают ситуацию ИБ в организации с помощью дашбордов и расследуют с помощью SIEM инциденты.
- К самым трудоемким задачам участники опроса отнесли работу с ложными срабатываниями (58%) и разбор инцидентов (52%).
- С помощью SIEM специалисты по ИБ хотели бы оценивать реализуемость атак (39%), проводить ретроспективный анализ (35%), анализировать уязвимости на IT-активах организации (34%), создавать собственные правила корреляции (32%) и обновлять сведения об инфраструктуре (30%).
- По мнению респондентов, снизить трудозатраты на SIEM-систему помогут:
 - поставка вендором способов детектирования угроз (53%),
 - руководство по донстройке правил для снижения количества ложных срабатываний (49%),
 - возможность писать собственные правила корреляции без изучения специального языка (44%).

Профиль респондентов

Отрасль

В опросе участвовали в основном специалисты по ИБ из сферы информационных технологий, финансовой, промышленной сфер и госсектора. Вероятно, IT-сектор лидирует потому, что больше всего на вопросы отвечали представители компаний-интеграторов.

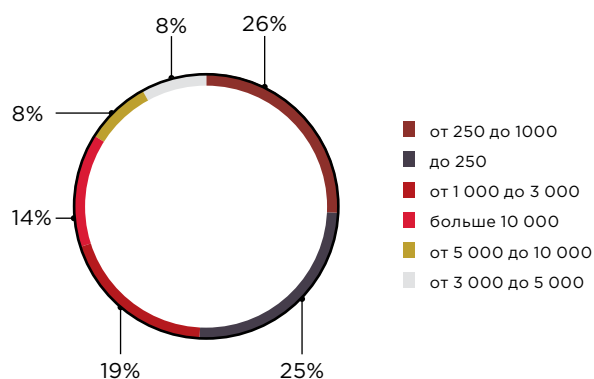
Какой сектор представляет компания, в которой ты работаешь?



Размер компании

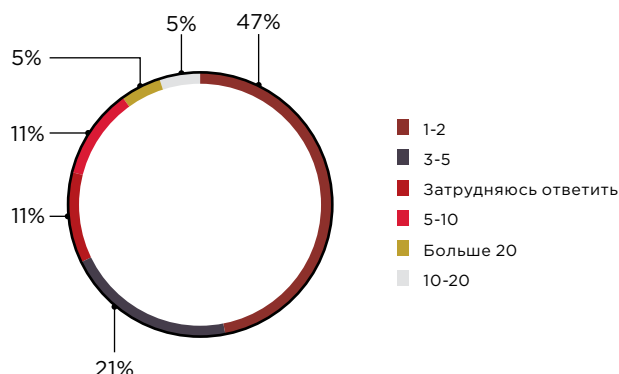
Четверть специалистов по ИБ представляют малый и средний бизнес (до 250 работников), остальные — крупный бизнес. Больше всего в опросе участвовало специалистов компаний, в которых работает от 250 до 1000 человек: их доля составила 26%.

Сколько сотрудников работает в компании?



В целом в компаниях регулярно работают с SIEM-системой не более пяти человек. Почти в половине компаний (47%) это один-два человека, в 21% компаний — от 3 до 5 человек. Чаще всего SIEM-команда с 3–5 специалистами встречается в крупных компаниях (от 1000 до 3000 сотрудников).

**Сколько сотрудников
в вашей компании
регулярно работают
с SIEM-системой?**



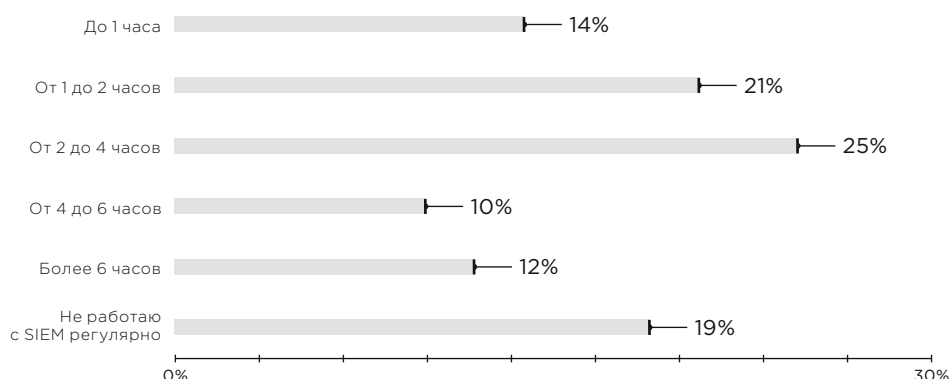
Интересное распределение SIEM-команд среди компаний, где работают больше 10 000 человек: в каждой четвертой компании с SIEM-системой работают от 3 до 5 специалистов, в каждой пятой — либо один-два специалиста, либо больше 20.

Трудозатраты на работу в SIEM-системе

Ежедневные трудозатраты

Чаще всего специалисты проводят за работой в SIEM-системе от 2 до 4 часов в день — такой вариант ответа выбрали 25% респондентов. А 22% специалистов проводят в SIEM-системе более половины рабочего дня.

**Сколько времени ты ежедневно проводишь
за работой в SIEM-системе?**



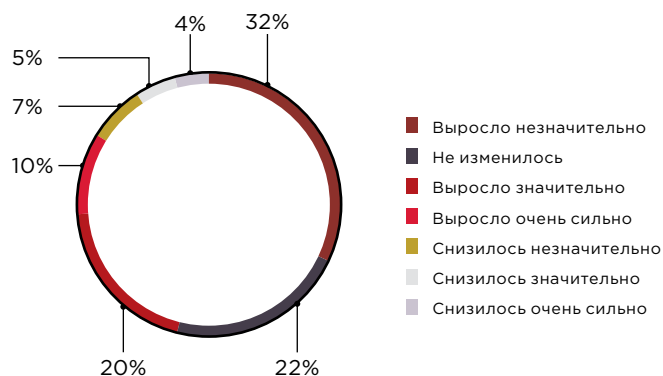
Прослеживается тенденция: чем больше размер SIEM-команды, тем больше времени занимает работа в системе. Вероятно, это связано с тем, что те, кто обслуживают SIEM-систему небольшим составом (один-два человека), — и есть вся команда отдела ИБ. Это, как правило, означает, что каждый сотрудник занимается сразу всеми средствами безопасности и нет ресурсов (временных, денежных) на повышение экспертизы в части SIEM.

| Время работы с SIEM/ Размер SIEM-команды | 1-2 | 3-5 | 5-10 | 10-20 | Больше 20 |
|--|-----|-----|------|-------|-----------|
| До 1 часа | 19% | 11% | 8% | 9% | 17% |
| От 1 до 2 часов | 25% | 30% | 8% | 18% | - |
| От 2 до 4 часов | 23% | 32% | 38% | 45% | 25% |
| От 4 до 6 часов | 8% | 15% | 8% | 18% | 17% |
| Более 6 часов | 9% | 13% | 17% | 9% | 25% |
| Не работаю с SIEM регулярно | 16% | - | 21% | - | 17% |

Динамика трудозатрат

Шестьдесят два процента специалистов отметили, что за последний год временные затраты на SIEM-систему выросли, 22% — что затраты не изменились, а 17% опрошенных смогли их снизить.

Как за последний год изменилось количество времени, проводимого тобой в SIEM?



Сорок три участника опроса оказались новичками: еще год назад они не работали с SIEM-системой. Половина из них сейчас работает с SIEM нерегулярно.

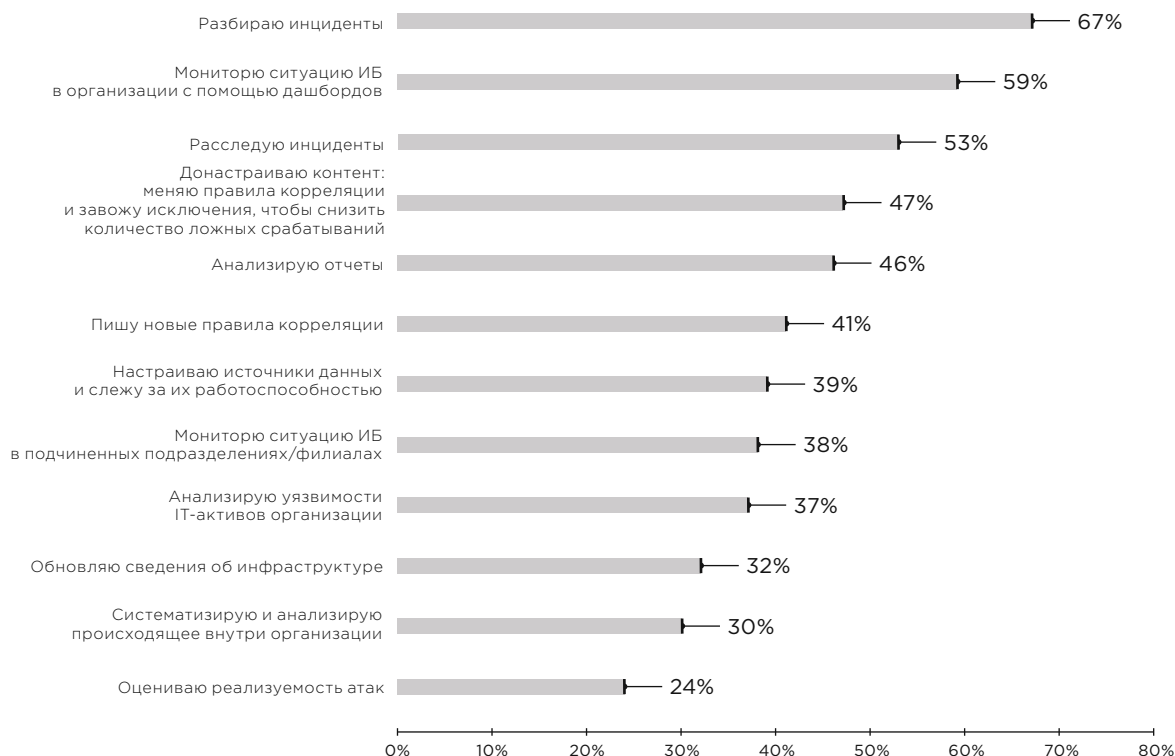
Наиболее трудоемкие действия в SIEM-системе

Участники опроса отметили пять самых популярных задач, которые они выполняют с помощью SIEM-системы:

- разбор инцидентов (67%);
- мониторинг ситуации ИБ в организации с помощью дашбордов (59%);
- расследование инцидентов (53%);
- донастройка контента: изменение правил корреляции и ввод исключений, чтобы снизить количество ложных срабатываний (47%);
- анализ отчетов (46%).

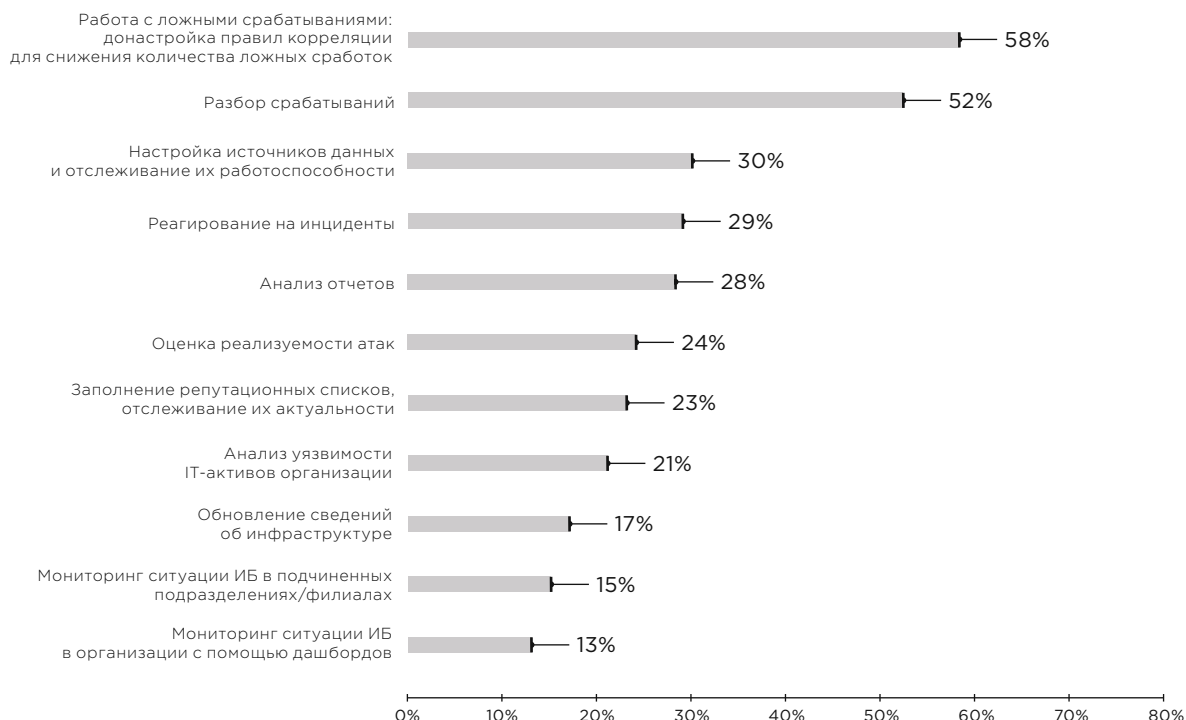
Все предложенные в опроснике варианты действий оказались востребованы: как минимум каждый третий выполняет их в SIEM-системе. Самым непопулярным вариантом оказалась оценка реализуемости атак — ее выполняет только каждый четвертый респондент. Что любопытно, в следующем вопросе специалисты по ИБ ответили, что хотели бы выполнять оценку реализуемости атак в SIEM-системе, но пока нет возможности.

Какие действия ты регулярно выполняешь в SIEM?



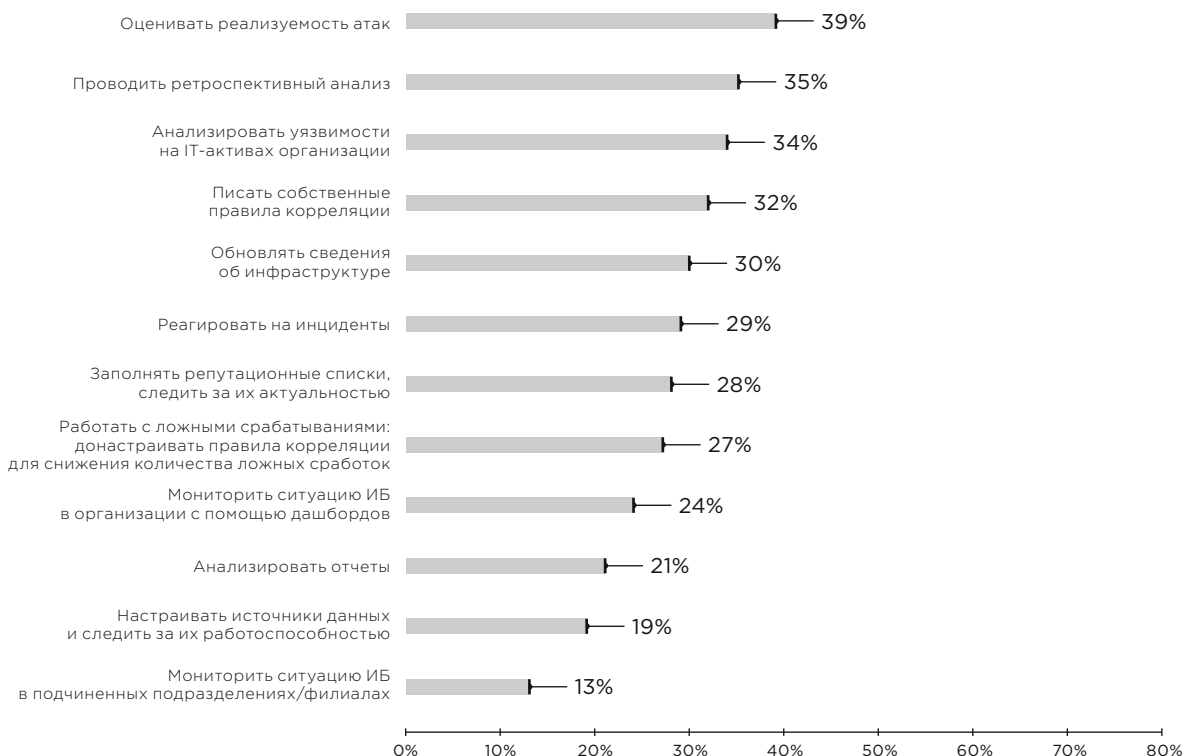
К наиболее трудоемким задачам участники опроса отнесли работу с ложными срабатываниями (донастройку правил корреляции) и разбор инцидентов: их отметили 58% и 52% респондентов соответственно. У 30% специалистов по ИБ много времени отнимают настройка источников данных и отслеживание их работоспособности.

Какие действия наиболее трудоемкие для тебя?



Затем мы решили узнать, какие задачи специалисты по ИБ хотели бы решать в SIEM-системе, но не имеют такой возможности — потому что не хватает времени или функциональности самой системы. Больше всего специалисты по ИБ хотели бы оценивать реализуемость атак (39%), проводить ретроспективный анализ (35%), анализировать уязвимости на IT-активах организации (34%) и писать собственные правила корреляции (32%).

Какие задачи ты бы хотел решать с помощью SIEM, но пока нет возможности



Как помочь ИБ-специалистам снизить трудозатраты

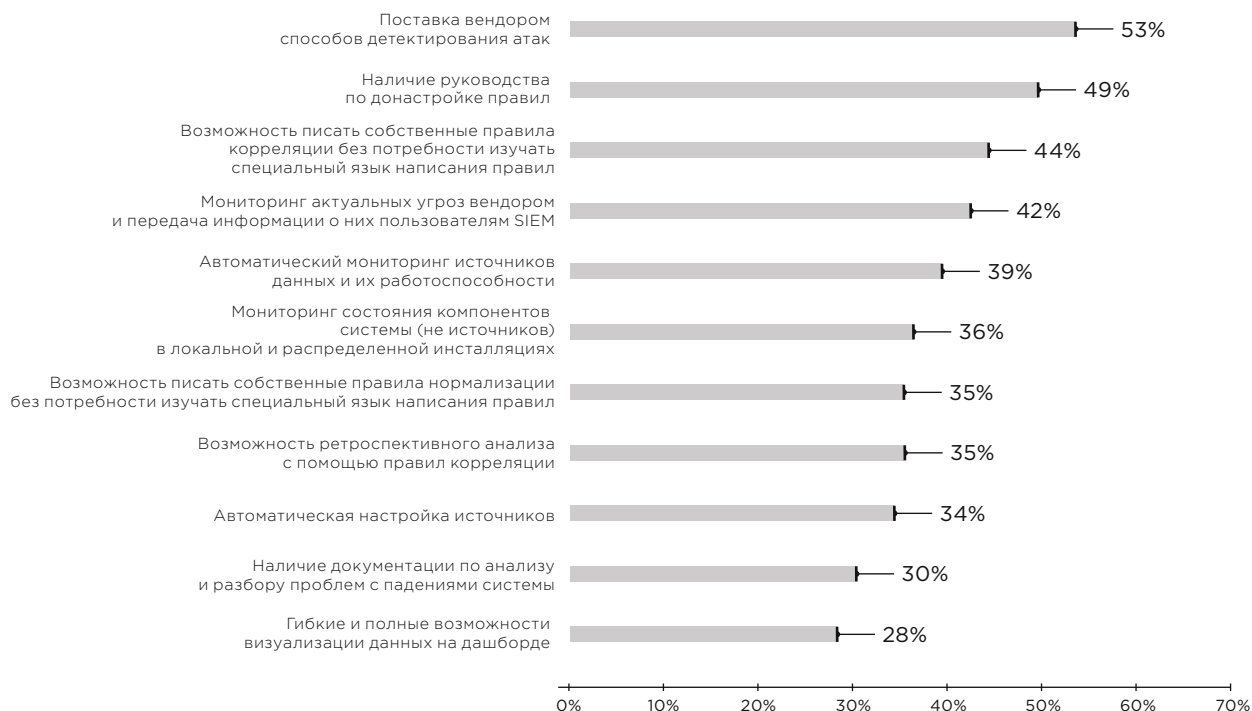
Больше всего нам, как представителям вендора, было интересно узнать, какие улучшения в SIEM-системах, по мнению специалистов, помогут им снизить трудозатраты. Мы попросили выбрать не более пяти самых полезных улучшений или предложить свой вариант. Более половины специалистов (53%) считают, что им поможет поставка вендором способов детектирования угроз. Чуть меньше (49%) хотели бы иметь руководства по донстройке правил для снижения количества ложных срабатываний. Третий по популярности ответ — возможность писать собственные правила корреляции без необходимости изучать специальный язык (44%). Сорок два процента специалистов отметили, что им поможет мониторинг актуальных угроз вендором и передача информации о них пользователям.

Остальные варианты тоже оказались востребованы: почти каждый из них набрал более 30% голосов. Двенадцать человек предложили собственные варианты:

- наличие простых способов интеграции с решениями класса IRP/SOAR,
- обучение продукту для операторов,
- оптимизация поисковых запросов,
- более быстрый поиск при ретроспективном анализе,
- специальный гибкий язык для написания правил.

Один участник опроса отметил, что сейчас ему мешает ограничение по количеству собираемых событий.

Какие улучшения в SIEM помогли бы тебе снизить трудозатраты в работе с системой?



Г Заключение

Исследование показало, что трудозатраты на работу с SIEM-системой — больной вопрос для большинства компаний. Размер SIEM-команды почти в половине случаев не превышает двух человек, а их время работы с системой растет. Больше всего времени отнимают ложные срабатывания (58%) и разбор инцидентов (52%). При этом больше четверти респондентов отметили, что у них нет возможности выполнять эти действия: реагировать на инциденты не успевают 29%, работать с ложными срабатываниями — 27%.

Чтобы дать специалистам возможность выполнять больше полезных задач в SIEM-системе, нужно развивать функциональность, которая бы максимально упростила выполнение типовых действий, в особенности работу с ложными срабатываниями и разбор инцидентов.

Результаты опроса выявили два ключевых вектора развития SIEM-систем, которые помогут снизить трудозатраты специалистов по ИБ: это поставка экспертизы от вендора и возможность выполнять дополнительные задачи, которые выходят за рамки традиционного SIEM.

Поддержка от вендора должна включать мониторинг актуальных угроз, поставку новых способов детектирования инцидентов, разработку руководств по донстройке правил для снижения количества ложных срабатываний. Все это облегчит работу специалистов и освободит время для выполнения других задач.

В топ-5 задач, которые специалисты по ИБ хотят выполнять, но пока не имеют такой возможности, вошли действия, которые выходят за рамки классического SIEM. Среди них оценка реализуемости атак, ретроспективный анализ, анализ уязвимости на IT-активах организации и обновление сведений об инфраструктуре. Это говорит о том, что специалисты хотят, чтобы все данные о сети компании, ее активах и их безопасности были собраны в одном месте и были доступны из единого интерфейса. Для этого необходимо решение, имеющее функциональность не только SIEM, но и asset management и vulnerability management. Детальное знание своей инфраструктуры даст, среди прочего, возможность точнее донстроить работу правил детектирования, что уменьшит количество ложных срабатываний.

Пользователи **MaxPatrol SIEM** ежемесячно получают наборы экспертных правил детектирования вместе с подробными инструкциями по настройке источников событий и удобными для заполнения белыми списками, часть из которых предзаполнены на основе нашего опыта работы с реальными инфраструктурами.

Пакеты экспертизы готовятся специалистами **PT Expert Security Center** и **R&D-подразделений Positive Technologies**. Они анализируют актуальные угрозы, исследуют полный цикл атак и разрабатывают способы их обнаружения. Пакеты содержат новые правила, обновления параметров сбора и обработки событий ИБ, рекомендации по реагированию, репутационные списки.

Приложение. Опросник

Трудозатраты специалистов по ИБ на работу с SIEM-системами

Positive Technologies проводит исследование о том, сколько времени тратят специалисты по ИБ на работу в SIEM-системах. Если ты работаешь с SIEM-системой (вендор не имеет значения), пожалуйста, ответь анонимно на несколько вопросов. Все участники опроса получат отчет с результатами исследования.

Какой сектор представляет компания, в которой ты работаешь?

- Финансы
- Госкомпания, госструктура
- ТЭК
- Промышленность, производство
- Образование
- Здравоохранение
- Телекоммуникации
- СМИ
- IT
- Другое: _____

Сколько сотрудников работает в компании?

- До 250
- От 250 до 1000
- От 1 000 до 3 000
- От 3 000 до 5 000
- От 5 000 до 10 000
- Больше 10 000

Сколько сотрудников в вашей компании регулярно работают с SIEM-системой?

- 1-2
- 3-5
- 5-10
- 10-20
- Больше 20
- Затрудняюсь ответить

Сколько времени ты ежедневно проводишь за работой в SIEM-системе? Учитывай время только в рабочие дни:

- До 1 часа
- От 1 до 2 часов

- От 2 до 4 часов
- От 4 до 6 часов
- Более 6 часов
- Не работаю с SIEM регулярно

Как за последний год изменилось количество времени, которое ты проводишь в SIEM-системе?

- Выросло незначительно (менее чем на 20%)
- Выросло значительно (от 20% до 50%)
- Выросло очень сильно (на 50% и более)
- Снизилось незначительно (менее чем на 20%)
- Снизилось значительно (от 20% до 50%)
- Снизилось очень сильно (на 50% и более)
- Не изменилось
- Год назад не работал с SIEM

Какие улучшения в SIEM-системе помогли бы тебе снизить трудозатраты в работе с системой? Выбери не более пяти самых полезных улучшений:

- Поставка вендором способов детектирования атак (новые правила, индикаторы компрометации)
- Мониторинг актуальных угроз вендором и передача информации о них пользователям
- Наличие руководства по донстройке правил для снижения количества ложных срабатываний
- Автоматическая настройка источников
- Автоматический мониторинг источников данных и их работоспособности
- Возможность писать собственные правила корреляции без необходимости изучать специальный язык
- Возможность писать собственные правила нормализации без необходимости изучать специальный язык
- Наличие документации по анализу и разбору проблем в работе системы
- Гибкие и полные возможности визуализации данных на дашборде (многочисленные виды представления данных, возможность работать с данными для оптимального представления на виджете)
- Возможность ретроспективного анализа с помощью правил корреляции
- Мониторинг состояния компонентов системы (не источников) в локальной и распределенной инсталляциях
- Другое: _____

Какие действия ты регулярно выполняешь в SIEM-системе?

- Отслеживаю ситуацию ИБ в организации с помощью дашбордов
- Отслеживаю ситуацию ИБ в подчиненных подразделениях (филиалах)

- Разбираю инциденты
- Расследую инциденты
- Донастраиваю правила корреляции и завожу исключения, чтобы снизить количество ложных срабатываний
- Пишу новые правила корреляции
- Настраиваю источники данных и слежу за их работоспособностью
- Анализирую отчеты
- Систематизирую и анализирую происходящее внутри организации
- Оцениваю реализуемость атак
- Анализирую уязвимости IT-активов организации
- Обновляю сведения об инфраструктуре
- Другое: _____

Какие действия наиболее трудоемки для тебя?

Отметь не более пяти:

- Мониторинг ситуации ИБ в организации с помощью дашбордов
- Мониторинг ситуации ИБ в подчиненных подразделениях (филиалах)
- Разбор срабатываний
- Реагирование на инциденты
- Работа с ложными срабатываниями: донастройка правил корреляции
- Заполнение репутационных списков, отслеживание их актуальности
- Настройка источников данных и отслеживание их работоспособности
- Анализ отчетов
- Оценка реализуемости атак
- Анализ уязвимости IT-активов организации
- Обновление сведений об инфраструктуре
- Другое: _____

Какие задачи ты бы хотел решать с помощью SIEM-системы, но пока нет возможности (не хватает времени или каких-то функций системы)?

- Отслеживать ситуацию ИБ в организации с помощью дашбордов
- Отслеживать ситуацию ИБ в подчиненных подразделениях (филиалах)
- Реагировать на инциденты
- Работать с ложными срабатываниями: донастраивать правила корреляции
- Писать собственные правила корреляции
- Заполнять репутационные списки, следить за их актуальностью
- Настраивать источники данных и следить за их работоспособностью
- Анализировать отчеты

- Оценивать реализуемость атак
- Анализировать уязвимости на IT-активах организации
- Обновлять сведения об инфраструктуре
- Проводить ретроспективный анализ
- Другое: _____

Оставьте корпоративный адрес электронной почты, чтобы одним из первых получить отчет по результатам исследования:

Рабочая почта: _____

Спасибо за участие в опросе!

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.