Решение «Лаборатории Касперского» для центров анализа событий ИБ (SOC)

Kaspersky for Security Operations Center

kaspersky

Препятствия эффективной работе центра анализа событий ИБ (SOC)

По мере того как бизнес учится лучше защищать себя, киберпреступники разрабатывают все более изощренные способы обходить оборону. Перспективы баснословного обогащения в случае успешной кибератаки постоянно привлекают новых злоумышленников, которые активно ищут и находят еще не обнаруженные уязвимости в системах безопасности. В столь агрессивной среде многие компании организуют специальные центры анализа событий ИБ (SOC) для оперативного реагирования на инциденты безопасности.

Основные выводы исследования рисков корпоративной информационной безопасности, проведенного «Лабораторией Касперского» в 2018 году

- Ущерб от утечек данных возрос почти на четверть. В среднем финансовый ущерб от утечки данных для крупных предприятий сегодня составляет 1,23 млн долл. США (в России 14,3 млн рублей): эта сумма увеличилась на 24% по сравнению с 2017 годом.
- В среднем у крупных компаний по всему миру сегодня уходит 193 тыс. долл. США на то, чтобы улучшить инфраструктуру
- после утечки данных, – на 46% больше, чем в 2017 году, когда затраты на обновление такого рода составляли 132 тыс. долл. США.
- К позитивным тенденциям следует отнести увеличение бюджетов безопасности практически во всей деловой сфере. Так, крупные предприятия в среднем тратят на кибербезопасность 8,9 млн долл. США в год.
- По сравнению с предыдущими годами количество обнаруженных глобальных угроз продолжает расти:

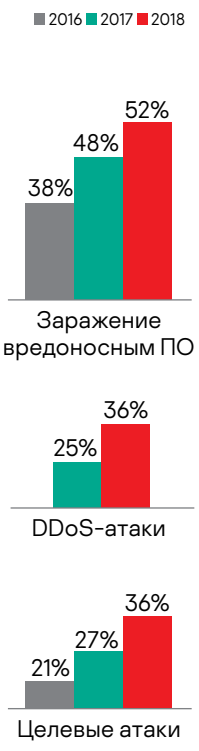


Рис. 1:
Обнаруженные глобальные угрозы

SOC – это структура, ведущая непрерывный мониторинг и анализ угроз для предотвращения инцидентов, связанных с кибербезопасностью, и минимизации последствий атак.

Постоянный рост количества, сложности и критичности современных угроз означает, что документирование процессов, внедрение базовых технологий и создание команды специалистов для мониторинга и реагирования – это лишь первые шаги в организации надежной защиты. Без непрерывной адаптации и совершенствования методов работы в соответствии с динамикой развития ландшафта угроз эффективность SOC может оказаться недостаточной.

Согласно модели адаптивной архитектуры безопасности, разработанной Gartner, для того чтобы организация могла успешно бороться с киберпреступностью в современной среде угроз, ее команда SOC должна уметь прогнозировать, предотвращать и обнаруживать угрозы, а также эффективно реагировать на угрозы и прогнозировать будущие атаки.

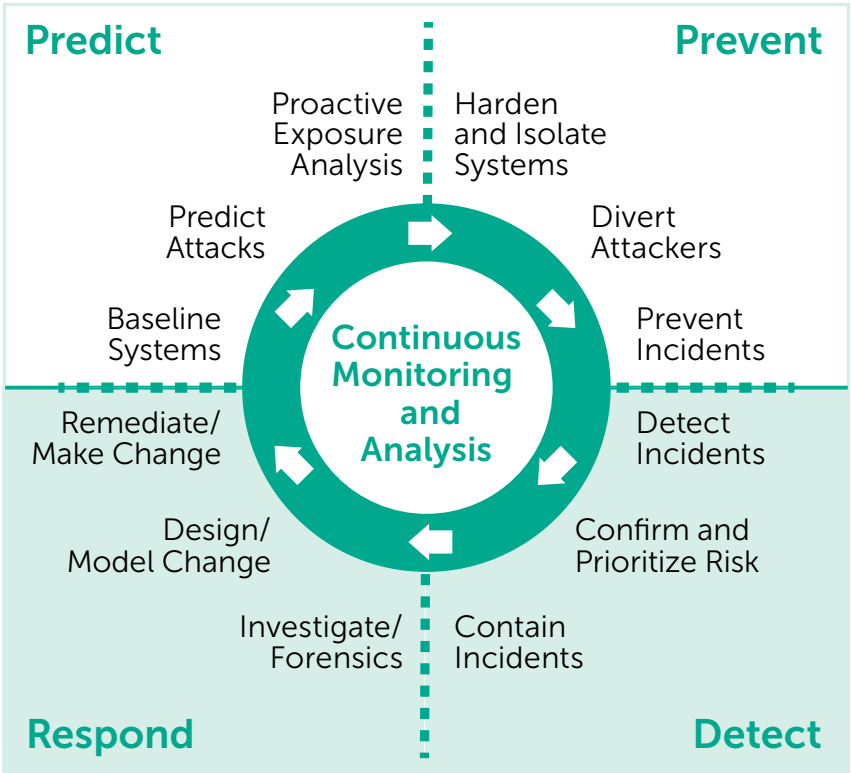


Рис. 2:
Источник: «Проектирование адаптивной архитектуры безопасности для защиты от продвинутых угроз» (Designing an Adaptive Security Architecture for Protection From Advanced

«Security Operations Centers должны изначально проектироваться для работы с аналитическими данными на основе адаптивной архитектуры безопасности, позволяющей эффективно использовать контекст и аналитику. Руководители отделов безопасности должны понимать, каким образом в SOC, работающих на основе аналитики, используются различные инструменты, процессы и стратегии защиты от современных угроз».

Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center, November 2015

Исследование, проведенное центром обеспечения безопасности института SANS 2018 среди организаций, создавших свои собственные SOC, продемонстрировало, что в современном бизнесе существует множество препятствий эффективной налаженной работе SOC.

Основные проблемы SOC

Рис. 3:
Основные проблемы SOC

Источник: исследование SOC института SANS 2018

Проблема нехватки на рынке квалифицированных специалистов в сфере IT-безопасности становится еще более ярко выраженной в случае с SOC, где требуется сочетание определенных навыков и опыта работы. Команда SOC нуждается в высококвалифицированных специалистах узкого профиля, обладающих знаниями и опытом в таких сферах, как анализ вредоносного ПО, цифровая криминалистика, реагирование на инциденты, и многих других. Эти специалисты должны уметь корректно интерпретировать данные SIEM-систем, идентифицировать и извлекать важную информацию из потоков данных общего характера, осуществлять тонкую настройку правил сопоставления и обогащать полученную информацию дополнительным контекстом. Недостаточный опыт аналитика в борьбе со сложными угрозами вкупе с нехваткой знаний о том, как использовать контекстные данные для корректной оценки масштаба инцидента и его расследования может помешать принять оптимальное решение о максимально эффективном реагировании на конкретную угрозу, что в итоге выливается в серьезные убытки для бизнеса.

Нехватка квалифицированных кадров

Недостаточная автоматизация

Еще одна проблема, снижающая эффективность работы SOC, заключается в недостаточной автоматизации. Сегодня многие аналитики вынуждены тратить много времени на рутинные операции, которые, будучи важными и необходимыми, тем не менее вполне могут быть автоматизированы. Автоматизация этих задач позволяет сэкономить большое количество высокооплачиваемых рабочих часов аналитиков; такое уменьшение рабочей нагрузки позволит выделить больше времени на анализ и реагирование на действительно сложные инциденты безопасности.

Отсутствие интеграции

48% респондентов считают проблемой использование слишком большого количества узкопрофильных инструментов, не интегрированных друг с другом. В результате аналитики вынуждены постоянно переключаться между различными инструментами и панелями управления, непродуктивно тратя время и совершая больше ошибок. При подключении дополнительных средств защиты и автоматизации важно учитывать, как они будут интегрироваться с уже существующими решениями и друг с другом.

Избыток оповещений

Инструменты обеспечения безопасности и ключевые бизнес-приложения, подключенные к SIEM-системе, генерируют поток уведомлений, которые необходимо просматривать ежедневно. Однако такой колоссальный переизбыток информации приводит к тому, что многие уведомления остаются без внимания – около 50% всех уведомлений просто игнорируется. Одновременно с этим доля ложноположительных срабатываний может достигать 60–80%. Все это означает, что процесс обнаружения действительно опасных потенциальных угроз выглядит для аналитика как поиск иголки в стоге сена. Соответственно, серьезные инциденты безопасности неизбежно будут пропускаться.

Отсутствие общего представления о происходящем на предприятии

Заваленные огромными объемами данных специалисты SOC вполне предсказуемо не пытаются объять необъятное и ограничиваются мониторингом лишь некоторых систем, но проблема, связанная с таким подходом, заключается в том, что в этом случае команда SOC не видит полную картину событий. А отсутствие общего представления о происходящем на предприятии – это уже следующая проблема. Например, SIEM-системы редко используют журналы событий на конечных устройствах – отчасти из-за ресурсоемкости этой задачи, отчасти из-за большого количества генерируемых при этом ложноположительных срабатываний. Но при этом именно конечные устройства являются ключевой целью организаторов атак. Рабочие станции и серверы – наиболее часто используемые злоумышленниками точки входа в корпоративные IT-инфраструктуры, и именно их данные (процессы, программы, модули, файлы, автозапуски, сетевые подключения и т. д.) играют ключевую роль в расследовании инцидентов. А если учесть, что внедрение нового протокола TLS 1.3 еще более повышает ценность телеметрического анализа конечных устройств, станет окончательно ясно, почему доступ к этим данным имеет столь важное значение.

Отсутствие контекстных данных

Недостаточное понимание мотивации, тактик и методов, используемых атакующими, может помешать специалистам SOC правильно приоритизировать инциденты для расследования – это приводит к тому, что специалисты либо хватаются за все сразу, либо впадают в ступор, не понимая, с чего начать. Без надлежащей информированной приоритизации инцидентов специалисты могут столкнуться с необходимостью анализировать слишком большое количество уведомлений, в результате нагрузка на команду SOC только растет, эффективность ее работы падает и оперативность реагирования снижается. Как следствие, действительно значимые уведомления остаются без внимания, а доля неточных результатов расследований продолжает расти. Сопоставление информации, полученной SOC, с аналитическими данными об угрозах предоставляет контекстную информацию, необходимую для надлежащей приоритизации инцидентов и дальнейшего эффективного расследования.

Ключевые элементы

Для поддержки признанного в индустрии подхода к организации работы SOC, описанного в этом документе, должны присутствовать нижеперечисленные ключевые элементы вкупе с четко определенными процессами и соответствующими технологиями:

- **Управление знаниями.** Члены команды SOC должны быть хорошо подготовлены в сферах цифровой криминалистики, анализа вредоносного ПО и реагирования на инциденты, чтобы предотвращать все более сложные атаки и эффективно реагировать на них.

- **Расширенные технологии защиты,** ориентированные на противостояние сложным угрозам и целевым атакам, помогают повысить эффективность работы SOC, обеспечивая более глубокий анализ и более оперативное реагирование на инциденты. Достичь этого можно за счет автоматизации защитных процессов, включая ответные меры, и обеспечения прозрачности всей инфраструктуры предприятия, а также с помощью добавления в SIEM-систему источников релевантных журналов.

- **Аналитические данные об угрозах,** собранные из релевантных, доверенных и надежных источников, очень важны для быстрого выявления новых угроз. Такими данными/источниками могут являться:
  - внутренние данные об угрозах;
  - аналитические данные из открытых источников (OSINT); отраслевые сообщества (например, FS-ISAC); промышленные группы CERT;
  - закрытые сообщества;
  - глобальные поставщики защитных решений; поставщики аналитических данных об угрозах.

- **Активный поиск угроз** позволяет превентивно выявлять угрозы, не обнаруживаемые традиционными системами безопасности (сетевыми экранами, IPS/IDS, SIEM и т. д.)

- **Возможность расследования инцидентов и реагирования** на них с целью минимизации ущерба от инцидентов и сокращения расходов на устранение их последствий.

- **Тестирование на проникновение и учения** с участием red team для оперативного выявления критически важных уязвимых мест, нуждающихся в укреплении защиты.

Все перечисленные выше элементы одинаково важны и требуют отдельного рассмотрения.

Рис. 4:
Ключевые элементы SOC

Управление знаниями

Для эффективной работы SOC нужны сотрудники, обладающие достаточными практическими знаниями и опытом, которые могут правильно проанализировать большие объемы данных и выбрать направление для дальнейшего расследования.

Из-за ограниченного бюджета укомплектовать SOC необходимыми кадрами бывает проблематично. На текущий момент рынок испытывает нехватку высококвалифицированных профессионалов в сфере кибербезопасности, что ведет к повышению стоимости их найма.

Сотрудник эффективного SOC должен обладать следующими качествами:
- аналитические навыки и способность воссоздать полную картину ситуации из разрозненных фрагментов данных;
- возможность поддерживать постоянную сосредоточенность в стрессовых условиях;
- хорошие знания в сфере IT и кибербезопасности, желательно подкрепленные обширным практическим опытом.

Вне зависимости от того, ищете ли вы нового специалиста для SOC на стороне или собираетесь перевести на новую должность кого-то из своих сотрудников, подобрать подходящего кандидата, уже обладающего всеми необходимыми качествами, будет непросто. Потребуются дополнительные тренинги – не только для того, чтобы привить сотрудникам необходимые навыки, но и чтобы приучить их быстро адаптироваться к изменениям в сфере технологий защиты и переменчивому ландшафту угроз.

В приведенной ниже таблице содержатся описания наиболее типичных ролей сотрудников SOC и сфер их ответственности. Конкретные роли и количество сотрудников вашего SOC будут зависеть от профиля и масштаба вашей организации.

В небольших SOC один сотрудник может выполнять сразу несколько ролей, в то время как в большой команде SOC имеет смысл назначать на одну роль несколько сотрудников.

Роль	Описание	Описание
	Базовые	
Аналитик 1-й линии	Специалист по сортировке	· Регистрация и распределение инцидентов · Классификация, проверка и приоритизация инцидентов безопасности · Мониторинг состояния датчиков безопасности (если применимо) · Сбор данных, требуемых для работы аналитиков 2-й линии
Аналитик 2-й линии	Обработчик инцидентов	· Расследование инцидентов и реагирование на них · Рекомендации по сдерживанию и мерам по ликвидации ущерба · Координация и поддержка реагирования на инциденты · Периодический обзор работы аналитиков 1-й линии
Аналитик вредоносного ПО	Реагирование на инциденты в случае особо сложных угроз требует проведения обратной разработки образцов вредоносного ПО и (или) расширенного криминалистического анализа артефактов. Основная обязанность аналитика вредоносного ПО – осуществление обратной разработки вредоносного ПО и предоставление полезной информации для реагирования на инциденты.	· Статический и динамический углубленный анализ вредоносного ПО · Обратная разработка вредоносных образцов · Участие в расследовании инцидентов компьютерной безопасности и целевых атак · Сбор индикаторов компрометации
Эксперт по цифровой криминалистике	Реагирование на инциденты в случае особо сложных угроз требует проведения обратной разработки образцов вредоносного ПО и (или) расширенного криминалистического анализа артефактов. При необходимости криминалистические улики должны быть собраны и проанализированы с не меньшей тщательностью. Основная обязанность эксперта по цифровой криминалистике – сбор и анализ криминалистических улик в процессе реагирования на инцидент.	· Сбор и анализ цифровых улик · Участие в расследовании инцидентов компьютерной безопасности и целевых атак · Криминалистический анализ ОС, приложений, памяти и сети · Сбор индикаторов компрометации
Специалист по анализу угроз	Когда SOC разрастается до приличных масштабов, имеет смысл выделить отдельную роль для анализа внутренних угроз. Эксперт по анализу угроз отвечает за анализ данных об угрозах из различных источников (аналитические отчеты, OSINT, прошлый опыт и др.) и предоставление команде SOC ценных результатов (информация о методах и тактике злоумышленников (TTP), IoC, аналитика)	· Сбор и анализ данных об угрозах из открытых источников · Анализ и разбор аналитики угроз поставщика · Сбор TTP и IoC из источников аналитических данных об угрозах · Категоризация, приоритизация и проверка потоков данных об угрозах · Создание аналитических отчетов об угрозах для различных заинтересованных сторон · Подготовка актуальных аналитических материалов для рабочей команды SOC и внешних партнеров · Обмен с клиентами информацией о потоках данных об угрозах и IoC
Системный администратор SOC	Системный администратор SOC отвечает за эксплуатацию и обслуживание инфраструктуры SOC.	· Эксплуатация и обслуживание IT- инфраструктуры SOC · Мониторинг состояния инфраструктуры SOC · Создание сценариев и автоматизация · Ведение документации инфраструктуры и инструментария SOC
Руководитель SOC	Руководитель SOC отвечает за координацию действий команды центра и его работу в целом.	· Управление кадрами · Стратегическое планирование · Разработка оперативной стратегии и стратегии развития SOC · Отчетность перед вышестоящим руководством и другими заинтересованными лицами · Управление эффективностью SOC и контроль КПЭ
	Дополнительные роли[1]	
Аналитик 3-й линии (активный поиск угроз)	Аналитик 3-й линии – высококвалифицированный эксперт, основная обязанность которого заключается в проактивном поиске угроз и разработке общей логики обнаруженияугроз. Также он может участвовать в процессе реагирования на инциденты в случае особо сложных угроз и высокоприоритетных инцидентов.	· Активный поиск угроз · Расследование инцидентов и реагирование на них (3-я линия) · Разработка и настройка логики обнаружения угроз · Разработка системы мониторинга службы безопасности · Периодический обзор работы аналитиков 2-й линии

Предложение «Лаборатории Касперского»: тренинги по кибербезопасности

«Лаборатория Касперского» уже более 20 лет постоянно расширяет и совершенствует свои экспертные знания в области кибербезопасности, будь то обнаружение угроз, исследование вредоносного ПО, обратная разработка или цифровая криминалистика. Ежедневно обнаруживая сотни тысяч новых образцов вредоносных программ, наши специалисты хорошо знают, как справиться с новыми угрозами современного изменчивого цифрового мира и как передать эти знания организациям-клиентам.

Программа тренингов по кибербезопасности разработана признанными экспертами в области безопасности.

Курсы включают как теоретические, так и практические (лабораторные) занятия. После завершения каждого курса учащимся предлагается проверить свои знания путем сертификации.

Курсы ориентированы на IT-специалистов, обладающих базовыми или экспертными навыками системного администрирования и программирования. Все учебные курсы проводятся в местных или региональных офисах «Лаборатории Касперского» либо на территории заказчика.

Темы	Длительность	Развиваемые навыки
Цифровая криминалистика в Windows		
На примере симулированного инцидента кибербезопасности, связанного с целевой атакой, курс охватывает следующие темы: · Введение в цифровую криминалистику · Оперативное реагирование и сбор цифровых улик · Анализ компьютеров под управлением Windows после обнаружения инцидента · Внутренняя структура реестра Windows · События Windows · Анализ артефактов в Windows · Криминалистический анализ артефактов браузера Анализ электронной почты · Носители SSD и связанные с ними криминалистические проблемы · Рекомендации по организации лаборатории цифровой криминалистики · Проверка новообретенных навыков на практике с использованием различных артефактов Windows	5 дней	· Сбор различных цифровых улик криминалистически достоверным образом · Поиск следов связанной с инцидентом вредоносной активности по артефактам в ОС Windows · Использование меток времени из различных артефактов Windows для воссоздания сценария инцидента · Поиск и анализ истории браузера и электронной почты · Умение применять инструменты цифровой криминалистики · Понимание процесса создания лаборатории цифровой криминалистики
Анализ и обратная разработка вредоносного ПО		
· Цели и методы анализа и обратной разработки вредоносного ПО · Внутреннее устройство ОС Windows, исполняемые файлы, ассемблер x86 · Базовые методы статического анализа (извлечение строк, анализ импортов, анализ точек входа исполняемого файла, автоматическая распаковка и т. д.) · Базовые методы динамического анализа (отладка, инструменты мониторинга, перехват трафика и т. д.) · Анализ файлов .NET, Visual Basic, Win64 · Методы анализа сценариев и неисполняемых файлов (пакетные файлы, AutoIt, Python, Jscript, JavaScript, VBS)	5 дней	· Построение безопасной среды для анализа вредоносных программ: развертывание песочницы и всех необходимых инструментов · Понимание принципов исполнения программ в ОС Windows · Распаковка, отладка и анализ вредоносного объекта, определение его функций · Обнаружение вредоносных сайтов путем анализа вредоносных скриптов · Проведение экспресс-анализа вредоносных программ
Цифровая криминалистика в Windows (экспертный уровень)		
На примере симулированного инцидента кибербезопасности, связанного с целевой атакой, курс охватывает следующие темы: · Системы счисления · Файловая система FAT · Файловая система NTFS · Углубленная криминалистика Windows · Восстановление данных и файлов из файловой системы, теневых копий и с использованием средств извлечения · Облачные среды и связанные с ними криминалистические проблемы · Криминалистический анализ памяти · Криминалистический анализ сети · Обычный и расширенный (super timeline) хронологический анализ · Проверка новообретенных навыков на практике с использованием полученных цифровых улик	5 дней	· Проведение углубленного анализа файловой системы · Идентификация и восстановление удаленных файлов с использованием различных методик · Анализ сетевого трафика с применением различных инструментов · Идентификация и отслеживание вредоносной активности в дампах памяти · Идентификация и дампинг представляющих интерес областей памяти для дальнейшего анализа · Восстановление хронологии инцидента с использованием меток времени файловой системы · Создание единой хронологии для всех артефактов Windows с целью более глубокого понимания сценария инцидента

Темы	Длительность	Развиваемые навыки
Анализ и обратная разработка вредоносного ПО (экспертный уровень)		
• Дешифрование • Разработка собственных дешифровщиков для распространенных сценариев • Декомпиляция байт-кода • Декомпозиция кода • Распаковка • Дизассемблирование • Реконструкция современных архитектур APT • Распознавание типичных кодовых структур • Идентификация алгоритмов шифрования и сжатия • Реконструкция классов и структур • Архитектуры APT-плагинов (на основе свежих APT-образцов)	5 дней	• Анализ современного APT-инструментария: от получения первоначального образца до создания технического описания с IoC • Использование передовых методов обратной разработки • Анализ шелл-кода эксплойтов, внедренного в различные виды файлов
Реагирование на инциденты в Windows		
В симулированной реальной среде произойдет инцидент, и в рамках этого сценария курс охватит следующие темы: • Введение в реагирование на инциденты и рабочий процесс • Объяснение различий между обычными угрозами и APT-угрозами • Ознакомление с цепочкой поражения APT-атаки • Процесс реагирования на инциденты для различных сценариев инцидентов безопасности • Применение знаний о цепочке поражения в симулированной среде • Применение анализа в режиме реального времени к пораженным машинам при первичном реагировании на атаку • Методы сбора криминалистически достоверных улик • Введение в результаты расследования после инцидента и цифровую криминалистику • Введение в криминалистику памяти • Анализ файлов журналов с помощью регулярных выражений и ELK • Знакомство с аналитическими данными о киберугрозах • Создание IoC (индикаторов компрометации) с помощью YARA и Snort • Введение в анализ вредоносного ПО и работу в песочнице • Введение в криминалистический анализ сетевого трафика • Обсуждение отчетности об анализе инцидента и рекомендации по созданию CSIRT • Проверка новообретенных навыков на практике в другом симулированном сценарии	5 дней	• Понимание этапов процесса реагирования на инциденты • Что следует принимать во внимание при реагировании на киберинциденты • Понимание различных методов атаки и анатомии целевых атак на примере цепочки поражения • Реагирование на различные инциденты принятием соответствующих мер • Способность отделять APT от других угроз • Подтверждение киберинцидентов с помощью инструментов анализа в режиме реального времени • Понимание различий между анализом в режиме реального времени и анализом постфактум и условий применения каждого из них • Идентификация цифровых улик: введение в криминалистический анализ жестких дисков, памяти и сетевого трафика • Запись IoC YARA и Snort для обнаруженной атаки • Анализ файлов журналов • Понимание процессов, задействованных в создании команды реагирования
Эффективное обнаружение угроз с помощью YARA		
• Краткое введение в синтаксис YARA • Советы и приемы по быстрому созданию эффективных правил • YARA-генераторы • Тестирование YARA-правил для ложных срабатываний • Поиск новых необнаруженных образцов на VirusTotal • Использование внешних модулей в YARA для эффективного поиска • Поиск аномалий • Множество (!) реальных примеров • Набор упражнений для совершенствования навыков работы с YARA	2 дня	• Создание эффективных правил YARA • Тестирование правил YARA • Оптимизация правил до такой степени, когда они позволяют находить угрозы, не обнаруживаемые иными способами
Администрирование Kaspersky Anti Targeted Attack (KATA)		
• Стандартная схема развертывания решения и размещения серверов • Системные требования • Модель лицензирования • Сервер «песочницы» • Консоль Central Node • Сенсоры • Интеграция с инфраструктурой • Установка сенсора на рабочих станциях • Добавление лицензии и обновление баз • Алгоритм работы решения	1 день	• Создание плана развертывания, оптимального для среды заказчика • Установка и настройка компонентов KATA • Поддержка и управление решением
Эффективное обнаружение угроз с помощью YARA		
• Интерпретация уведомлений (алертов) KATA • Объяснение технологий обнаружения и анализа • Объяснение механизмов скоринга и оценки риска	1 день	• Понимание того, как работает скоринг и как он используется механизмами оценки риска • Способность уверенно работать с уведомлениями KATA: отслеживать, интерпретировать, реагировать

Передовые технологии защиты

Современные решения для защиты от угроз повышенной сложности ориентированы на работу с SIEM-системами, что помогает компаниям организовывать новые эффективные SOC и оптимизировать работу уже имеющихся. Такая оптимизация может достигаться разными способами.

Во-первых, будет полезна автоматизация процессов обнаружения, анализа и реагирования, связанных с расследованием продвинутых угроз и целевых атак. Автоматизация таких задач, до этого выполнявшихся вручную, предоставляет аналитикам 1-й линии инструменты, время и внутренние ресурсы, необходимые для эффективного практического применения их аналитических навыков – например, при анализе потоков данных об угрозах. В случае старших аналитиков 2-й линии это освободившееся время можно выделить на проактивный поиск угроз, углубленный анализ инцидентов и разработку планов эффективного реагирования на сложные инциденты.

Другой подход заключается в обеспечении аналитикам полной прозрачности всей инфраструктуры и предоставлении SIEM-системе релевантных журналов, а также в организации быстрого доступа к консолидированным метаданным, объектам и вердиктам. Последние также помогают аналитикам эффективно работать даже в тех ситуациях, когда скомпрометированные конечные устройства недоступны или данные были зашифрованы хакерами.

Все это помогает команде SOC получить более полное представление о последовательности осуществленных злоумышленниками действий, одновременно уменьшая количество ложноположительных срабатываний, на которые аналитики вынуждены тратить свое рабочее время, и ускоряя процесс приоритизации уведомлений.

Предложение «Лаборатории Касперского»: Kaspersky Anti Targeted Attack и Kaspersky Endpoint Detection and Response

Решения Kaspersky Anti Targeted Attack для анализа сетевого трафика и Kaspersky Endpoint Detection and Response для конечных устройств базируются на одной и той же технологической платформе, представляющей собой многоуровневое комплексное решение, позволяющее полностью автоматизировать отнимающие много времени процесс сбора улик и рутинные процедуры, связанные с обнаружением следов угроз, анализом и реагированием на сложные инциденты.

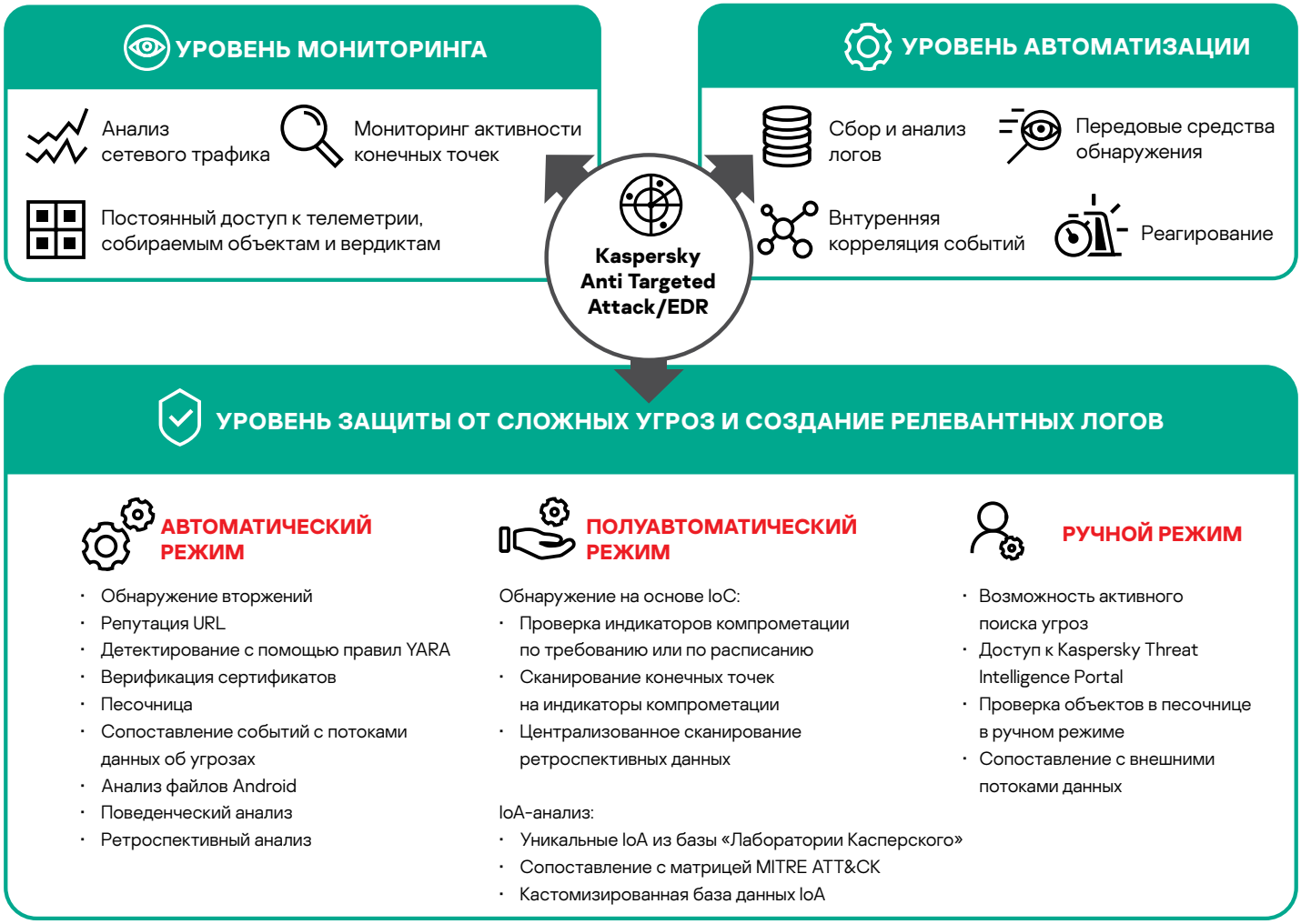


Рис. 5:
Kaspersky Anti Targeted Attack и Kaspersky EDR

Наши технологии представляют собой ценнейший источник данных для SIEM-систем, одновременно с этим предоставляя мощные автоматизированные возможности по обнаружению и активному поиску угроз. Kaspersky Anti Targeted Attack и Kaspersky EDR включают следующие механизмы обнаружения: централизованный антивирус нового поколения, поиск индикаторов компрометации (IoC), сопоставление индикаторов атак (IoA), YARA-правила, песочницу, облачный анализ ML-APK, поведенческий анализ, проверку сертификатов, ретроспективный анализ, систему активного поиска угроз и встроенный автоматический модуль аналитики угроз с доступом к порталу аналитических отчетов об угрозах (Threat Intelligence Portal).

Как следствие, решения обнаруживают даже сложные угрозы, спроектированные специально для обхода традиционных мер обеспечения безопасности, а ваш SOC более эффективно справляется с повседневными задачами, не тратя время на рутинные процедуры и переключение между множеством панелей управления. Также это помогает избежать дополнительных затрат, связанных с анализом журналов, не имеющих отношения к делу, и позволяет значительно сократить время реагирования на инциденты.

Использование Kaspersky Anti Targeted Attack и Kaspersky Endpoint Detection and Response:

- Значительно сокращает временные затраты аналитиков на трудоемкие, но необходимые задачи, связанные со сбором данных и процессами обнаружения и реагирования.
- Позволяет значительно снизить риски за счет повышения эффективности реагирования на инциденты.
- Обогащает SIEM-систему новыми источниками релевантных журналов для сопоставления с журналами других систем, что повышает эффективность контроля и расследований, а также делает инфраструктуру значительно прозрачнее и сокращает время реагирования.
- Предоставляет долгосрочный и всеобъемлющий подход к организации эффективной работы SOC.

Анализ угроз

SOC традиционно создавались со следующими целями:
- управление устройствами для обеспечения безопасности, контроль периметра и предоставление превентивных технологий защиты, таких как IPS/IDS, сетевые экраны, прокси и т. д.;
- мониторинг событий безопасности с помощью системы управления данными и инцидентами безопасности (SIEM-системы);
- реагирование на инциденты и ликвидация их последствий;
- обеспечение соответствия внутренним и нормативным требованиям (например, PCI-DSS или 187-ФЗ).

Многие современные организации создают собственные SOC, чтобы иметь максимально полную картину угроз. Однако некоторые организации, уже имеющие свои SOC, по-прежнему сталкиваются с теми же проблемами, что и раньше. Тому есть несколько причин:
- ошибки приоритизации, в результате которых реальные угрозы остаются незамеченными среди тысяч ежедневно генерируемых и анализируемых незначимых уведомлений безопасности;
- ликвидация последствий инцидентов без надлежащего понимания тактики, методов и процедур организаторов атаки, в результате чего продвинутые атаки легко проглядеть;
- реактивный подход к инцидентам вместо превентивного поиска угроз, которые уже проникли в организацию и начали действовать, оставаясь незамеченными;
- отсутствие стратегического представления о существующем ландшафте угроз и осведомленности об атаках на схожие предприятия и доступных контрмерах;
- проблемы привлечения надлежащих инвестиций в необходимые технологии безопасности – высокопоставленные руководители, не вполне ориентирующиеся в технической стороне вопроса, зачастую недооценивают риски для бизнес- процессов, связанные с нарушениями безопасности.

С учетом всего вышесказанного руководителям, ответственным за безопасность, рекомендуется следовать подходу к организации работы SOC на базе аналитики. Чтобы работа SOC была эффективной, он должен активно использовать новые технологии и средства управления, адаптируясь к постоянно меняющемуся ландшафту угроз.

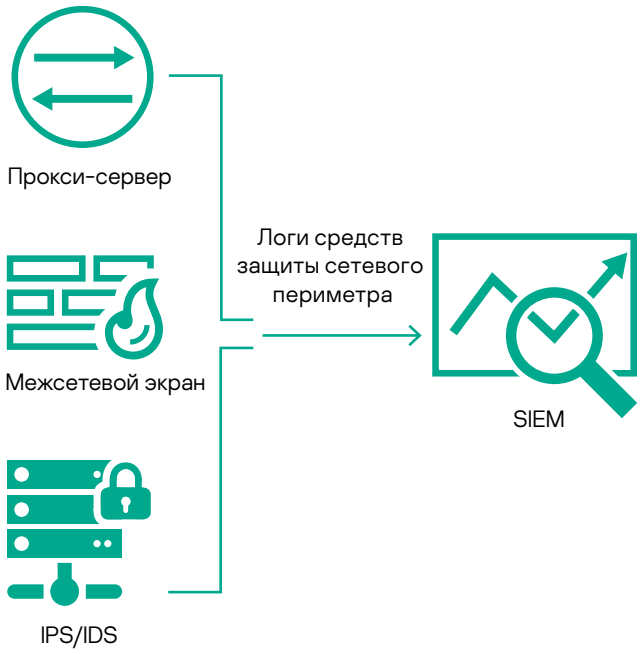


Рис.6:
SOC в традиционном понимании

Gartner дает следующее определение аналитике угроз: «Подкрепленное свидетельствами знание, включая контекст, механизмы, индикаторы, последствия и рекомендуемые действия, о существующих или потенциальных угрозах или опасностях ресурсам, которое может быть использовано для принятия информированного решения о принятии ответных мер в отношении этих угроз или опасностей».

Gartner, How Gartner Defines Threat Intelligence.

Сопоставление внутренних данных об угрозах с информацией, полученных из внешних доверенных и надежных источников (например, OSINT или глобальных поставщиков защитных решений), дает представление о методах злоумышленников и возможных индикаторах атак. Это, в свою очередь, позволяет организациям выработать эффективные стратегии защиты как от обычных, так и от продвинутых целевых атак..

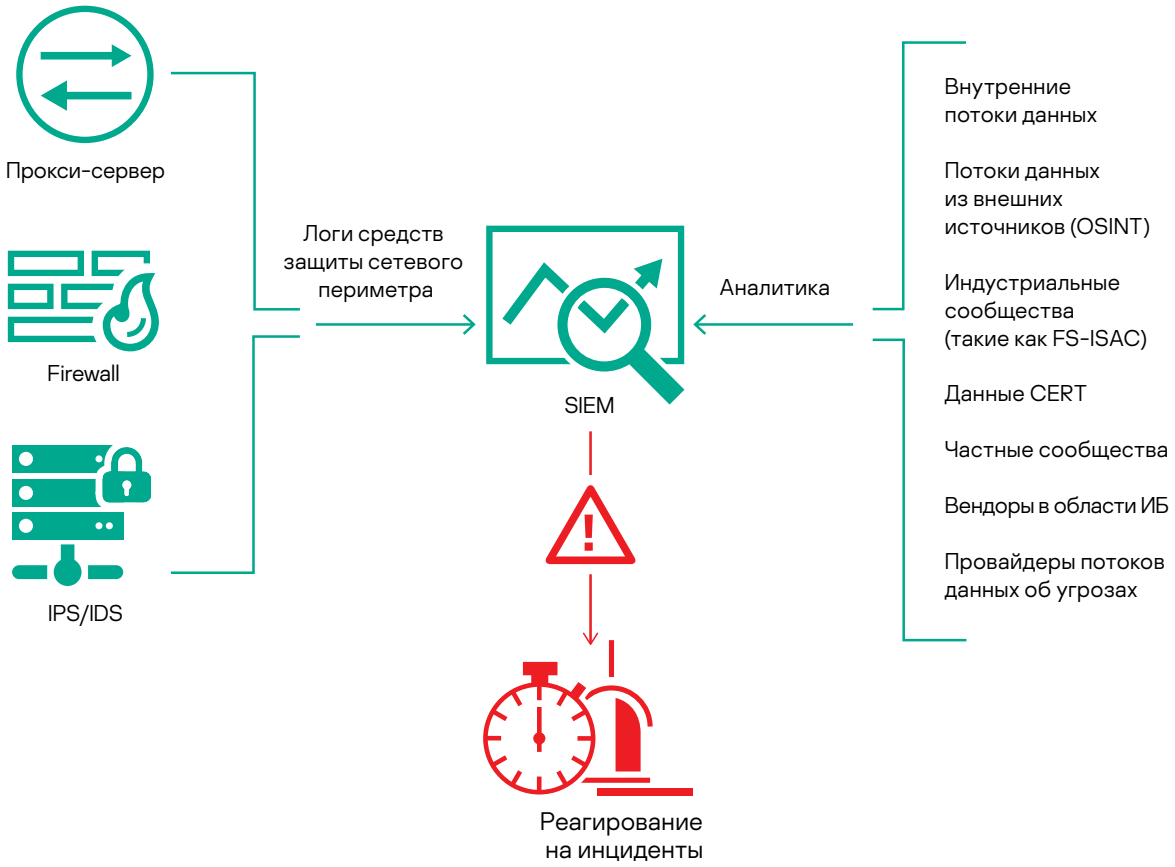


Рис. 7:
SOC на основе аналитики

К выбору источников данных следует подходить с особой тщательностью

Существует прямая корреляция между качеством используемых аналитических данных и эффективностью решений, принимаемых на основе этой аналитики.

Если вы будете полагаться на неточные, неподходящие по контексту, не учитывающие специфику вашей отрасли или несвоевременно получаемые аналитические данные, то качество решений, принимаемых в вашей организации, может серьезно пострадать.

Необработанные данные без контекста не позволяют команде SOC работать с максимальной эффективностью. Например, знание о том, что конкретный URL-адрес является вредоносным, и знание, что этот адрес используется для хостинга эксплойта или определенного вредоносного ПО, – совсем не одно и то же. Этот дополнительный уровень аналитики даст вашим экспертам по безопасности информацию, что именно им следует искать в процессе расследования инцидента.

Общепринятых критериев оценки различных коммерчески доступных предложений аналитических данных об угрозах до сих пор не существует, но следует учитывать следующие рекомендации:

- Ориентируйтесь на аналитические данные с глобальным охватом. Для атак не существует границ; атака, нацеленная на латиноамериканскую компанию, вполне может быть запущена из Европы, и наоборот. Собирает ли поставщик информацию в разных регионах и способен ли он найти взаимосвязь между на первый взгляд разрозненными действиями преступников, объединив их в глобальные кампании? Такие аналитические данные помогут оперативно принимать необходимые меры.
- Если вы ищете контент стратегического уровня, который поможет вам сформировать долгосрочные планы по обеспечению безопасности, такой как:
  - обзоры тенденций атак на высоком уровне;
  - техники и методы, используемые атакующими;
  - мотивы злоумышленников;
  - атрибуция атак и т. д.,

  тогда вам следует обратиться к поставщику аналитических данных об угрозах, который уже зарекомендовал себя как источник, способствующий обнаружению и расследованию сложных угроз в вашем регионе или отрасли. Способность поставщика данных подстраивать свои исследовательские возможности под специфику конкретно вашей компании также очень важна.
- Контекст – вот что отличает аналитику от просто данных. Например, индикаторы угроз вне контекста не имеют никакой ценности – вам нужно искать поставщиков, которые помогут вам ответить на вопросы «почему это важно?» Еще ценнее контекст, выявляющий взаимосвязи (например, домены, соответствующие обнаруженным IP-адресам, или URL, с которых был загружен определенный файл). Все эти данные очень помогают в расследованиях инцидентов, позволяя определять характеристики угроз по индикаторам компрометации, обнаруживаемым в сети.
- Разумеется, давая все эти советы, мы подразумеваем, что в вашей компании уже есть средства контроля безопасности и работают связанные с ними процессы и что вам важно использовать аналитику угроз с помощью уже хорошо знакомых вам инструментов. Поэтому обращайте внимание на методы доставки, механизмы интеграции и форматы, которые позволят вам встроить аналитику угроз в существующие системы управления безопасностью.

Предложение «Лаборатории Касперского»: потоки данных об угрозах

«Лаборатория Касперского» предлагает клиентам постоянно обновляемые потоки данных об угрозах. Используя эти потоки, команда вашего SOC сможет своевременно узнавать об угрозах и возможных кибератаках, что поможет снизить риски и заранее принять меры по защите.

Описание типов данных

- **Данные о репутации IP-адресов** – список IP-адресов с контекстной информацией, сообщающий о подозрительных и вредоносных узлах.
- **URL-адреса вредоносных ссылок** – список URL-адресов, соответствующих опасным ссылкам и веб-сайтам. Доступны записи с масками и без масок.
- **URL-адреса фишинговых ссылок** – список URL-адресов, распознаваемых «Лабораторией Касперского» как фишинговые. Доступны записи с масками и без масок.
- **URL-адреса командных серверов ботнетов** – набор URL-адресов командных серверов ботнетов и связанных с ними вредоносных объектов.
- **URL-адреса программ-вымогателей** – ссылки на страницы, где размещены программы-вымогатели или к которым обращаются такие программы.
- **Индикаторы заражения APT** – вредоносные домены, хосты, IP-адреса и файлы, используемые злоумышленниками для осуществления APT-атак.
- **Passive DNS (pDNS)** – список записей, содержащий результаты разрешений имен DNS для доменов в соответствующие IP-адреса.
- **URL-адреса IoT-угроз** – веб-сайты, которые использовались для загрузки вредоносного ПО, заражающего устройства интернета вещей.
- **Данные белых списков** – систематизированный список хешей надежных файлов, доступный для использования сторонними решениями и сервисами.
- **Хеши вредоносных объектов** – список файловых хешей, охватывающий наиболее опасные и распространенные, а также самые новые вредоносные программы.
- **Хеши вредоносных объектов для мобильных устройств** – список файловых хешей для обнаружения вредоносных объектов, заражающих мобильные устройства.
- **Данные о троянцах P-SMS** – набор хешей троянцев с контекстной информацией для обнаружения SMS-троянцев, которые звонят с мобильных телефонов на платные номера, а также позволяют злоумышленнику перехватывать SMS- сообщения, отвечать на них и удалять их.
- **URL-адреса командных серверов мобильных ботнетов** – набор URL-адресов с контекстной информацией о командных серверах мобильных ботнетов.

Особенности услуги

- Потоки данных генерируются автоматически в режиме реального времени на основе данных, собираемых по всему миру (в сеть Kaspersky Security Network входят десятки миллионов конечных пользователей более чем в 200 странах, что позволяет отслеживать значительный объем интернет-трафика). Это обеспечивает точность и высокую скорость обнаружения.
- Каждая запись в каждом потоке содержит контекстные данные, позволяющие принять меры для защиты (названия угроз, метки времени, географическое положение, установленные IP-адреса зараженных веб-ресурсов, хеши, популярность и т. п.). Эти данные можно широко использовать, например чтобы составить общее представление о ситуации или провести дополнительные проверки. Они помогут найти ответы на вопросы «кто?», «что?», «где?» и «когда?» и выявить источники атак, чтобы вы могли принять своевременные решения и действия, которые защитят именно вашу организацию.
- Простые форматы для распространения данных (JSON, CSV, OpenIoC, STIX) через HTTPS и специализированные методы доставки позволяют без затруднений интегрировать потоки данных в решения безопасности.
- Аналитические данные об угрозах генерируются и отслеживаются мощной отказоустойчивой инфраструктурой,

Предложение «Лаборатории Касперского»: Kaspersky CyberTrace

Количество оповещений от различных систем информационной безопасности, ежедневно обрабатываемых аналитиками в центрах мониторинга и реагирования на инциденты ИБ (SOC), растет в геометрической прогрессии. Такой объем анализируемых данных практически исключает возможность их эффективной приоритизации и классификации для дальнейшего анализа и реагирования. SIEM-системы, средства управления журналами и другие аналитические системы, уменьшают количество событий, требующих дополнительной проверки, но ИБ-специалисты все равно остаются перегружены.

Эффективные классификация, анализ и реагирование на события ИБ

Благодаря интеграции актуальных машиночитаемых аналитических данных об угрозах в существующие средства управления событиями ИБ, такие как SIEM-системы, центры мониторинга могут автоматизировать процесс первоначальной приоритизации и классификации. При этом аналитики 1-й линии получают достаточно контекста, чтобы сразу выявлять события, которые требуют более пристального изучения или эскалации группам реагирования на инциденты для проведения детального расследования. Постоянный рост числа доступных для интеграции потоков данных об угрозах мешает определить источники информации, релевантные конкретной организации. Потоки данных предоставляются в различных форматах и включают огромное количество индикаторов компрометации (IoC), что сильно усложняет их обработку SIEM-системами или средствами управления сетевой безопасностью.

Kaspersky CyberTrace позволяет упростить интеграцию потоков данных с SIEM системами для их дальнейшего более эффективного использования. Это средство позволяет работать с любым потоком аналитических данных об угрозах в форматах JSON, STIX, XML и CSV: open-source, от «Лаборатории Касперского», от других поставщиков, а также собственными кастомизированными потоками. CyberTrace также поддерживает “out-of-the-box” интеграцию с различными SIEM системами и источниками логов. Благодаря автоматическому сопоставлению полученных логов с потоками аналитических данных об угрозах, Kaspersky CyberTrace обеспечивает «ситуационную осведомленность» в режиме реального времени и позволяет аналитикам 1-й линии принимать своевременные и более взвешенные решения.

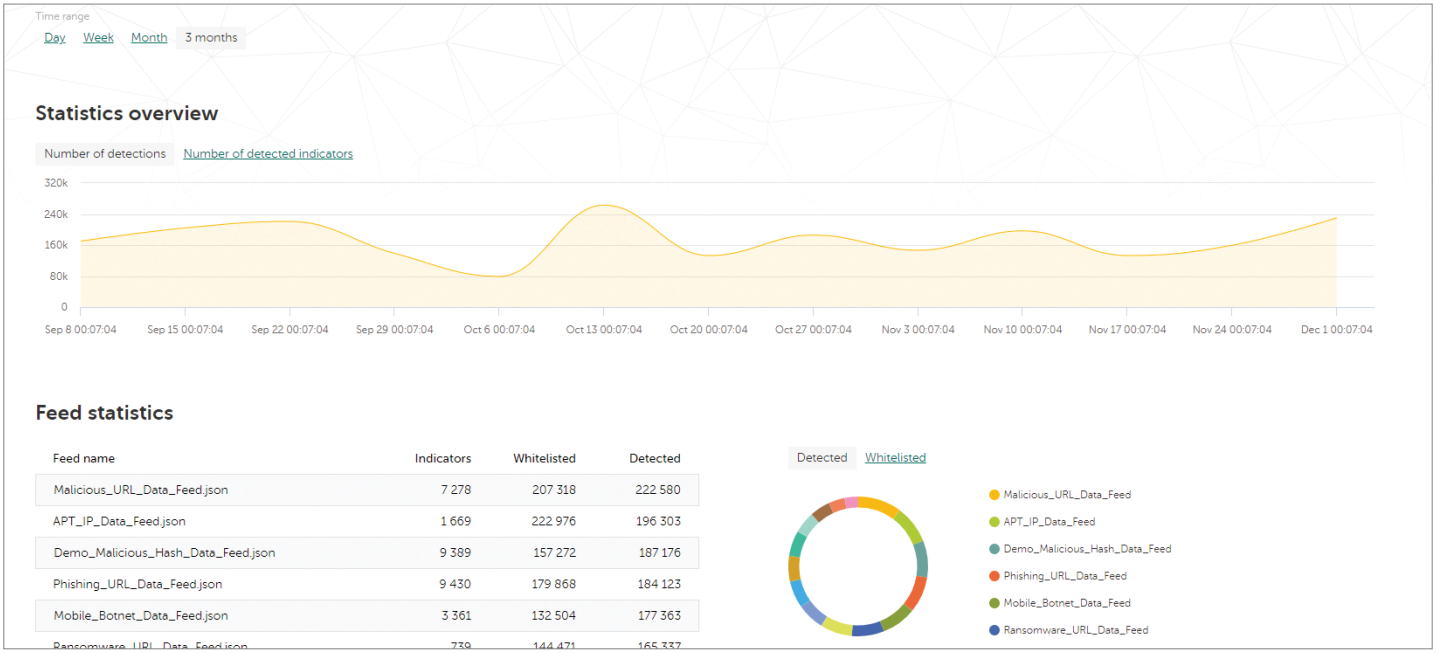


Рис. 8:
Статистика Kaspersky CyberTrace

Kaspersky CyberTrace содержит набор инструментов для эффективной классификации событий ИБ и первоначального реагирования

- в стандартной версии доступны демонстрационные потоки данных об угрозах от «Лаборатории Касперского» и потоки из открытых источников (OSINT);
- SIEM-коннекторы для визуализации данных об обнаружении угроз и управления ими;
- статистика использования для измерения эффективности используемых потоков данных;

- поиск индикаторов по запросу (контрольные суммы, IP-адреса, домены, URL-адреса) для углубленного исследования угроз;
- пользовательский веб-интерфейс с визуализацией данных, доступом к конфигурации, управлением потоками, правилами парсинга логов, черными и белыми списками;
- расширенная фильтрация потоков (на основе контекста, предоставляемого каждым из индикаторов, включая тип угрозы, географическое положение, популярность, метки времени и др.) и логов (на основе пользовательских условий);
- экспорт результатов поиска по индикаторам, содержащихся в потоках данных, в формат CSV для интеграции с другими системами (сетевые экраны, системы предотвращения вторжений (IDS) на уровне сети и хоста, другие инструменты);
- массовое сканирование логов и файлов;
- интерфейс командной строки для платформ Windows и Linux;
- автономный режим, в котором Kaspersky CyberTrace не интегрируется с SIEM-системой, а получает и анализирует логи различных систем, например, логи сетевых устройств;
- возможность установки в DMZ, когда требуется изоляция от интернета.

Этот продукт использует внутренний процесс анализа и сопоставления поступающих данных, что существенно снижает рабочую нагрузку на SIEM-систему. Kaspersky CyberTrace анализирует поступающие данные, быстро сопоставляет их с потоками и генерирует собственные оповещения при обнаружении угроз. На рисунке ниже показана высокоуровневая архитектура интеграции решения:

Рис. 9:
Схема интеграции Kaspersky CyberTrace

«Лаборатория Касперского» также предлагает набор постоянно обновляемых потоков данных об угрозах, которые могут интегрироваться с Kaspersky CyberTrace, обеспечивая глобальное представление об угрозах, их своевременное обнаружение, приоритизацию оповещений систем защиты и эффективное реагирование на инциденты:

- Данные о репутации IP-адресов – список IP-адресов с контекстной информацией, сообщающий о подозрительных и вредоносных узлах.
- URL-адреса вредоносных и фишинговых ссылок — список URL-адресов, соответствующих опасным ссылкам и веб-сайтам. Доступны записи с масками и без масок.
- URL-адреса командных серверов ботнетов – список URL-адресов командных серверов ботнетов и связанных с ними вредоносных объектов.
- URL-адреса командных серверов ботнетов для мобильных устройств – список URL-адресов командных серверов ботнетов для мобильных устройств. Идентификация зараженных устройств, обменивающихся данными с командными серверами.
- URL-адреса программ-вымогателей – ссылки на страницы, где размещены программы-вымогатели (ransomware) или к которым обращаются такие программы.
- Индикаторы заражения APT – вредоносные домены, хосты, IP-адреса и файлы, используемые злоумышленниками для осуществления APT-атак.
- Passive DNS (pDNS) – набор записей, содержащий результаты DNS разрешений доменов в соответствующие IP-адреса.
- URL-адреса IoT-угроз – веб-сайты, которые использовались для загрузки вредоносного ПО, заражающего устройства интернета вещей

- Хеши вредоносных объектов – список файловых хешей, охватывающий наиболее опасные и распространенные, а также самые новые вредоносные программы.
- Хеши вредоносных объектов для мобильных устройств – список файловых хэшей для обнаружения вредоносных объектов, заражающих мобильные устройства на базе Android и iOS.
- Данные о троянцах P-SMS – список хэшей троянцев с контекстной информацией для обнаружения SMS-троянцев, которые звонят с мобильных телефонов на платные номера, а также позволяют злоумышленнику перехватывать SMS-сообщения, отвечать на них и удалять их.

Потоки данных составляются из множества разнообразных надежных источников, включая сеть Kaspersky Security Network, более ста миллионов пользователей которой по всему миру добровольно предоставляют нам данные о киберугрозах, наши собственные поисковые роботы, сервис мониторинга ботнет-угроз (круглосуточное слежение за ботнетами и их мишенями), ловушки для спама, данные исследовательских групп и партнеров.

Вся собранная информация тщательно проверяется и очищается в режиме реального времени при помощи различных методов предварительной обработки: статистических методов, инструментов экспертных систем «Лаборатории Касперского» (таких как песочницы и средства эвристического анализа, мультисканеры, определения сходства и профилирования моделей поведения), проверки аналитиками и сопоставления с белыми списками.

Каждая запись в каждом потоке содержит обширные контекстные данные (оценки угроз, географическое положение, имена угроз, метки времени, установленные IP-адреса зараженных веб-ресурсов, хеши, популярность и т. п.).

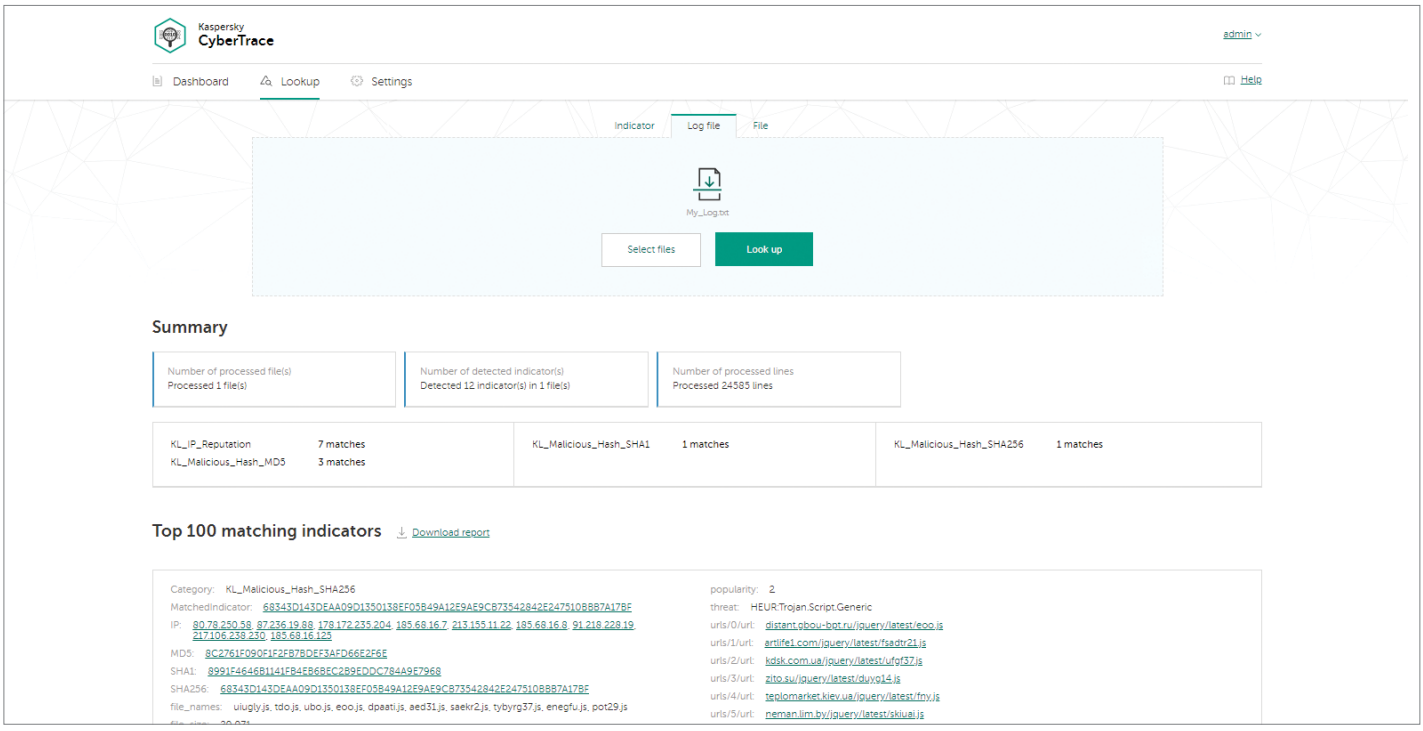


Рис. 10:
Контекст потоков данных об угрозах

Эти данные можно использовать, например, чтобы составить общее представление о ситуации или провести дополнительные проверки. Они помогут найти ответы на вопросы «кто?», «что?», «где?» и «когда?», чтобы выявить источники атак и принять своевременные решения.

Хотя Kaspersky CyberTrace и потоки данных «Лаборатории Касперского» об угрозах можно использовать по отдельности, при совместном использовании они существенно расширяют возможности обнаружения угроз, предоставляя специалистам по обеспечению безопасности их полную картину. Kaspersky CyberTrace и потоки данных «Лаборатории Касперского» об угрозах позволяют аналитикам центра обеспечения безопасности:

- эффективно фильтровать и приоритизировать оповещения систем безопасности; оптимизировать и ускорять процессы классификации и первоначального реагирования;
- быстро определять наиболее критичные из оповещений и принимать более взвешенные решения об их дальнейшей передаче группам реагирования на инциденты;
- создать проактивную систему защиты на основе глобальных аналитических данных

Предложение «Лаборатории Касперского»: портал Kaspersky Threat Intelligence (проверка угроз и облачная песочница)

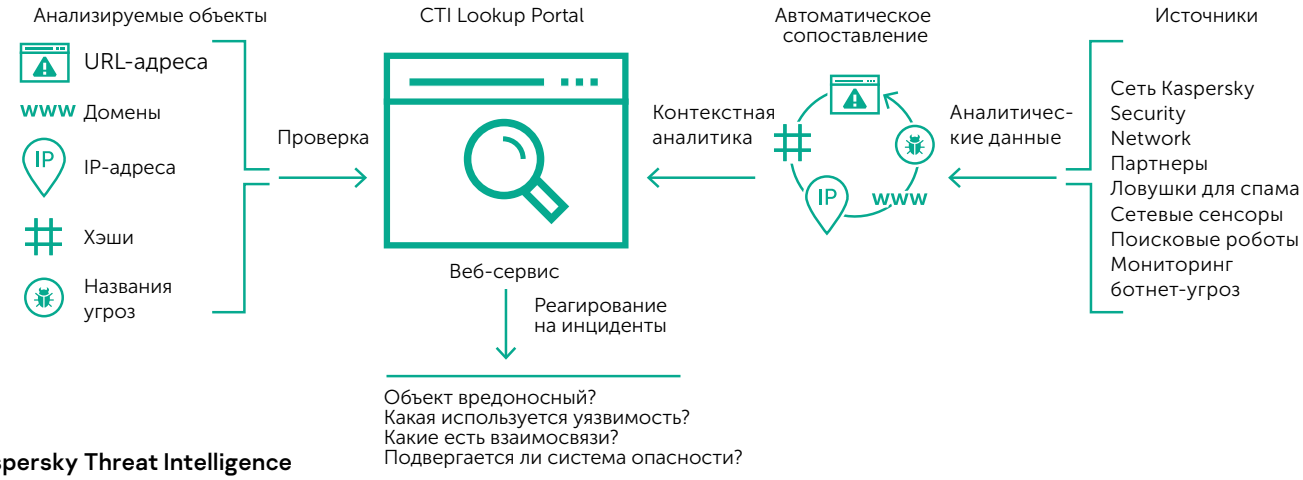


Рис. 11:
Портал Kaspersky Threat Intelligence

Особенности сервиса

- **Надежные данные об угрозах**. Ключевая особенность портала Kaspersky Threat Intelligence – надежность данных об угрозах с практическими контекстными рекомендациями по их нейтрализации. Продукты «Лаборатории Касперского» показывают наилучшие результаты при тестировании решений для защиты от вредоносных программ[3]. Непревзойденное качество аналитических данных подтверждается самым высоким уровнем обнаружения практически без ложных срабатываний.
- **Активный поиск угроз.** Проактивное выявление и предотвращение атак позволяет минимизировать их воздействие и сократить частоту. Вы сможете отслеживать и устранять атаки на самых ранних этапах. Чем раньше будет обнаружена атака, тем меньший будет нанесен ущерб и тем быстрее будет восстановлена работоспособность ресурсов и сети.
- **Анализ в песочнице.** Для выявления неизвестных угроз подозрительные объекты можно запускать в безопасной среде, получая понятные отчеты с полной информацией об их поведении и артефактах.
- **Разнообразие форматов экспорта.** Поддерживается экспорт индикаторов компрометации (IoC) и практических контекстных рекомендаций в популярные машиночитаемые форматы, такие как STIX, OpenIOC, JSON, YARA, Snort и даже CSV. Это позволяет применять данные об угрозах с максимальной пользой, автоматизируя рабочие процессы и интегрируя эти данные в структуры управления безопасность, такие как SIEM-системы.

Портал Kaspersky Threat Intelligence – это онлайн-платформа, которая предоставляет удобный доступ ко всем накопленным «Лабораторией Касперского» знаниям об угрозах и их взаимосвязях. Сервис предоставляет вашим специалистам SOC максимум информации для предотвращения кибератак до того, как организации будет нанесен вред. Портал собирает подробные актуальные сведения об угрозах: URL-адреса, домены, IP-адреса, контрольные суммы файлов, названия угроз, статистику и информацию об активности, данные WHOIS/DNS, атрибуты файлов, данные геолокации, цепочки загрузок, метки времени и т. п. Облачная песочница позволяет связать эти знания с индикаторами компрометации, сгенерированными анализируемым образцом. В результате вы получаете глобальное представление о новых и развивающихся угрозах, что помогает вам обеспечить защиту вашей организации и повысить эффективность мер реагирования на инциденты.

Аналитические данные об угрозах, предоставляемые порталом Kaspersky Threat Intelligence, генерируются и отслеживаются в реальном времени мощной отказоустойчивой инфраструктурой, которая обеспечивает постоянную доступность и бесперебойную работу сервиса. В подготовке аналитических данных участвуют сотни экспертов, включая аналитиков безопасности со всего мира, специалистов центра глобальных исследований и анализа угроз (GReAT), и ведущие научно-исследовательские коллективы.

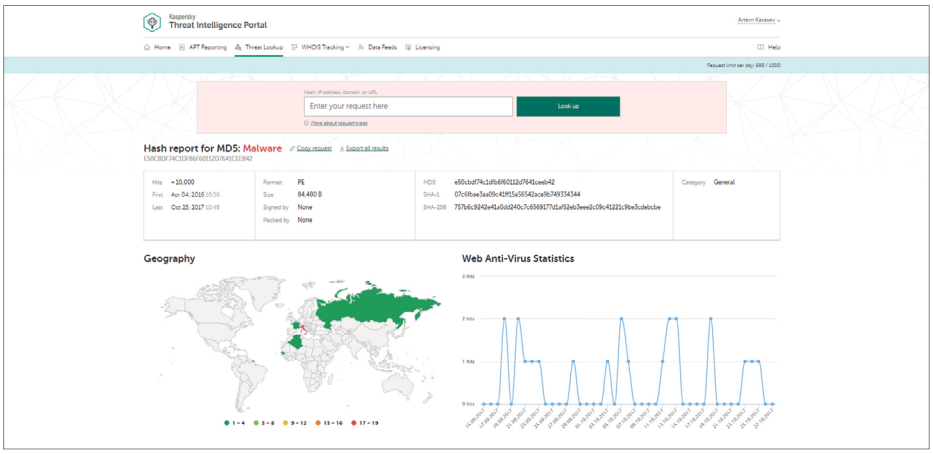


Рис. 12:
Портал Kaspersky Threat Intelligence

Предложение «Лаборатории Касперского»: аналитические отчеты об APT-угрозах

Новости об обнаружении комплексных таргетированных угроз (APT-угроз) не всегда сообщаются сразу, а во многих случаях такая информация вообще не объявляется публично. Наши подробные отчеты позволят вам в числе первых получать эксклюзивную, глубокую и актуальную информацию об APT-угрозах.

Наши исследования APT-угроз

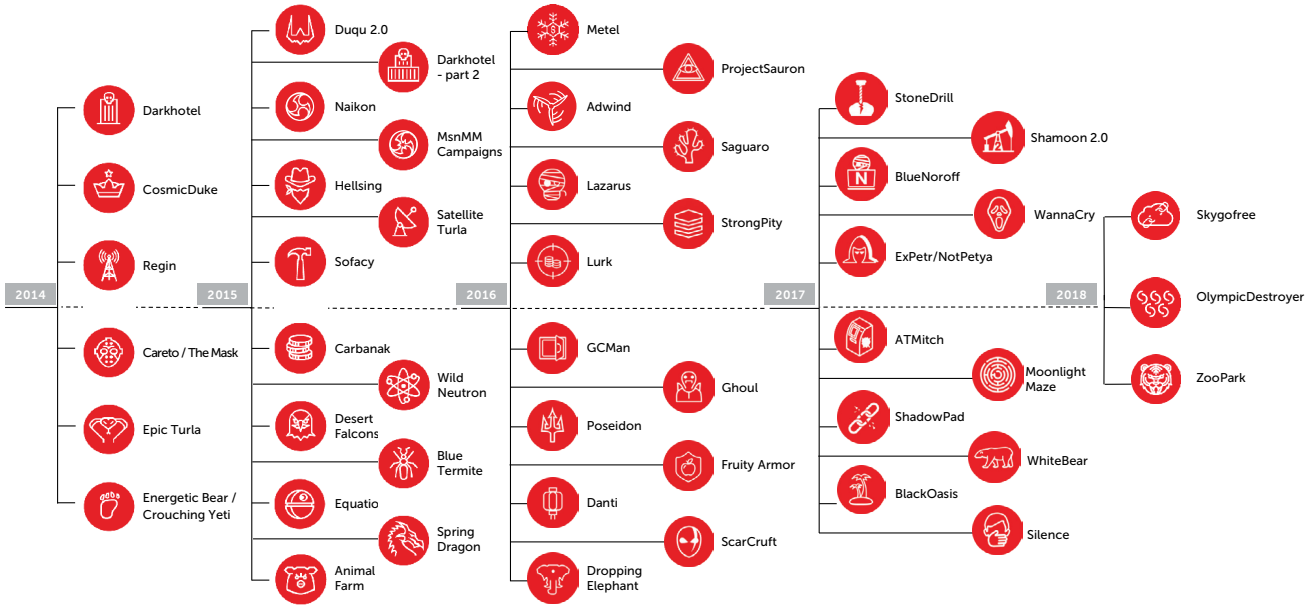


Рис. 13:
Расследования APT-атак, проведенные «Лабораторией Касперского»

Особенности сервиса

- Эксклюзивный доступ к техническим описаниям новейших угроз уже в ходе расследования, до публичного объявления. В 2017 году было составлено более 100 отчетов об APT-атаках.
- Данные о закрытых APT-угрозах. Не обо всех масштабных угрозах сообщается публично. Некоторые угрозы так и остаются тайной из-за специфики жертв, особой конфиденциальности данных, особенностей процесса устранения уязвимости или привлечения правоохранительных органов. Однако наши клиенты получают доступ к таким отчетам.
- Подробные технические данные, образцы и инструменты, в том числе расширенный список индикаторов компрометации (IoC), доступный в формате openIOC, а также доступ к нашим YARA-правилам.
- Непрерывный мониторинг APT-кампаний. Доступ к ценным аналитическим данным в ходе расследования (информация о распространении APT-угрозы, индикаторы заражения, инфраструктура командных центров).

Подписчики на отчеты «Лаборатории Касперского» об APT-угрозах получают уникальный доступ к результатам расследования и техническим данным в различных форматах по каждой APT-угрозе сразу после появления этих данных, даже если они так никогда и не будут опубликованы. Наши эксперты – это наиболее подготовленные и самые успешные «охотники» на APT-угрозы. Они немедленно оповестят вас о любых обнаруженных изменениях в тактике киберпреступников. Вы также получите доступ к полной базе отчетов «Лаборатории Касперского» о комплексных таргетированных угрозах. Она станет ценным аналитическим дополнением к вашей корпоративной системе безопасности.

С практической точки зрения для экспертов SOC самыми информативными являются данные об индикаторах компрометации. Эта структурированная информация предназначена для использования со специальными автоматическими инструментами, которые помогают проверить инфраструктуру на наличие признаков заражения.

Все отчеты доступны через веб-интерфейс или через API на основе REST.

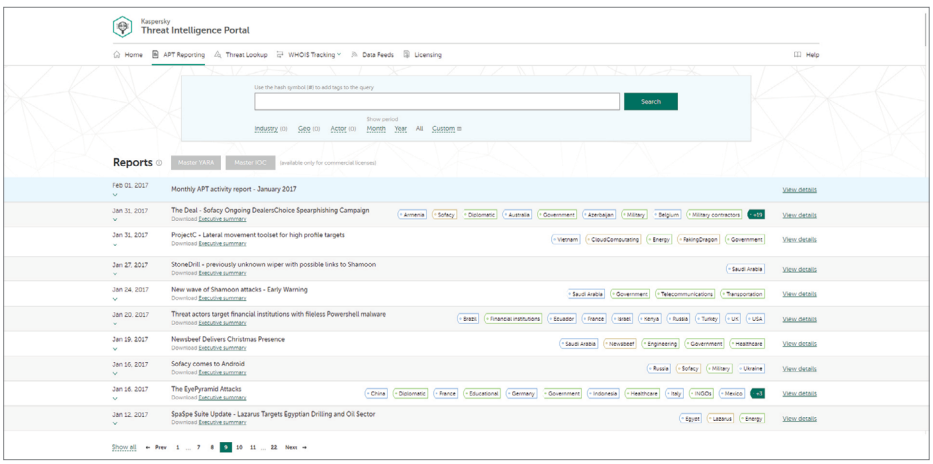


Рис 14:
Аналитические отчеты об APT-угрозах

Предложение «Лаборатории Касперского»: подготовка персонализированных отчетов об угрозах

Аналитические отчеты об угрозах для конкретных клиентов

Как лучше всего организовать атаку на вашу организацию? Какие векторы атаки и какие сведения доступны злоумышленнику, который решит атаковать вашу компанию? Возможно, атака уже организована или начнется в ближайшем будущем?

Специально подготавливаемые отчеты «Лаборатории Касперского» для конкретных клиентов отвечают на эти и другие вопросы. Наши эксперты выстраивают полную картину текущей ситуации с угрозами, выявляют уязвимые места в вашей защите и обнаруживают признаки прошедших, текущих и планируемых атак.

Эти уникальные аналитические данные позволят вам сосредоточиться на уязвимостях, которые больше всего интересуют киберпреступников, чтобы быстро и точно отражать вторжения и свести к минимуму риск успешной атаки.

Эти отчеты составляются с использованием общедоступных источников информации (OSINT), мощных экспертных систем и баз «Лаборатории Касперского» и наших данных о подпольных преступных сетях. В отчетах рассматриваются следующие вопросы:

- Определение векторов угроз: выявление и анализ состояния критических компонентов вашей сети, доступных извне – включая банкоматы, системы видеонаблюдения, телекоммуникационное оборудование и другие виды систем, а также профили сотрудников в социальных сетях и личные учетные записи электронной почты. Любой из этих компонентов может стать целью для атаки.
- Анализ отслеживания вредоносных программ и кибератак: выявление, мониторинг и анализ любых активных и неактивных образцов вредоносных программ, нацеленных на вашу организацию, текущей и зафиксированной ранее активности ботнетов, а также любой другой подозрительной сетевой активности.
- Атаки на третьи стороны: выявление признаков угроз и активности ботнетов, направленных на ваших клиентов, партнеров и абонентов. Их зараженные системы могут стать источником последующей атаки на вашу компанию.
- Утечки информации. Ведя скрытое наблюдение за подпольными интернет-форумами и сообществами, мы можем обнаружить планы атаки на вашу компанию, если злоумышленники обсуждают их, а также выявить нечистоплотных сотрудников, торгующих ценной информацией.
- Текущая подверженность атакам. APT-угрозы могут оставаться незамеченными в течение многих лет. Если мы обнаружим, что вашу инфраструктуру уже атакуют, то дадим рекомендации по эффективному реагированию на атаку.

Быстро. Удобно. Без дополнительных ресурсов

Определив параметры персонализированных отчетов и предпочтительные форматы данных, вы сможете пользоваться этим сервисом «Лаборатории Касперского», не прибегая к созданию дополнительной инфраструктуры.

Для подготовки аналитических отчетов «Лаборатории Касперского» не используются активные методы анализа, поэтому сервис не влияет на целостность и доступность ресурсов исследуемой компании.

Аналитические отчеты об угрозах для конкретных стран

Кибербезопасность страны подразумевает защиту всех ее ключевых структур и крупных организаций. Комплексные таргетированные угрозы (APT), направленные на органы государственного управления, могут подрывать национальную безопасность; кибератаки, нацеленные на производство, транспортную сеть, систему телекоммуникаций, банковскую сферу и другие важнейшие отрасли экономики, способны причинить значительный ущерб на уровне государства, вызывая финансовые потери, аварии на производстве, перебои в работе сетей связи, общественное недовольство и другие негативные последствия

Отчеты об угрозах для конкретных стран составляются при помощи широкого ряда средств – от общедоступных источников информации (OSINT) до мощных экспертных систем и баз «Лаборатории Касперского», а также наших данных о подпольных преступных сетях. В отчетах рассматриваются следующие вопросы:

- **Определение векторов угроз:** выявление и анализ состояния критических IT-ресурсов страны, доступных извне, включая уязвимые правительственные приложения, телекоммуникационное оборудование, компоненты промышленных систем управления.

- **Анализ вредоносных программ и кибератак:** выявление и анализ APT- кампаний, активных и неактивных образцов вредоносных программ, текущей и зафиксированной ранее активности ботнетов, а также других крупных угроз, направленных на вашу страну, на основе данных внутреннего мониторинга из наших уникальных источников.

- **Утечки информации:** ведя скрытое наблюдение за подпольными форумами и интернет-сообществами, мы можем обнаружить планы атак на определенные организации, если злоумышленники обсуждают их. Мы также выявляем компрометацию ценных учетных записей, которая может нести в себе риск для затронутых организаций и структур (например, учетных записей, принадлежащих сотрудникам правительственных учреждений и полученных злоумышленниками при взломе сайта Ashley Madison, которые могли быть использованы для шантажа).

Сервис подготовки аналитических отчетов «Лаборатории Касперского» не влияет на целостность и доступность исследуемых сетевых ресурсов, так как он основан на неинтрузивных методах сканирования сети, а также анализе информации, доступной из открытых источников и источников с ограниченным доступом.

По результатам работы сервиса вы получите отчет, содержащий описание крупных угроз для различных отраслей и государственных структур, а также дополнительные подробные данные технического анализа. Отчеты доставляются посредством зашифрованных сообщений электронной почты.

Сервис может предоставляться единовременно или по подписке, например ежеквартально.

Подробнее об источниках данных Kaspersky Threat Intelligence

Данные об угрозах собираются из множества гетерогенных высоконадежных источников, включая сеть Kaspersky Security Network (KSN) и наши собственные поисковые роботы, наш сервис мониторинга ботнет-угроз (круглосуточное слежение за ботнетами и их мишенями) и ловушки для спама; мы получаем информацию от исследовательских групп и партнеров, используются также исторические данные о вредоносных объектах, собранные «Лабораторией Касперского» почти за два десятилетия работы. Вся собранная информация тщательно проверяется и очищается в режиме реального времени при помощи различных методов предварительной обработки: статистических критериев, инструментов экспертных систем «Лаборатории Касперского» (таких как «песочницы» и средства эвристического анализа, определения сходства и профилирования моделей поведения), проверки аналитиками и сопоставления с белыми списками.

После того как вы набрали высококвалифицированных сотрудников и наладили получение аналитических данных об угрозах и их интеграцию с используемыми вами средствами обеспечения безопасности, можно переходить собственно к реагированию на инциденты.

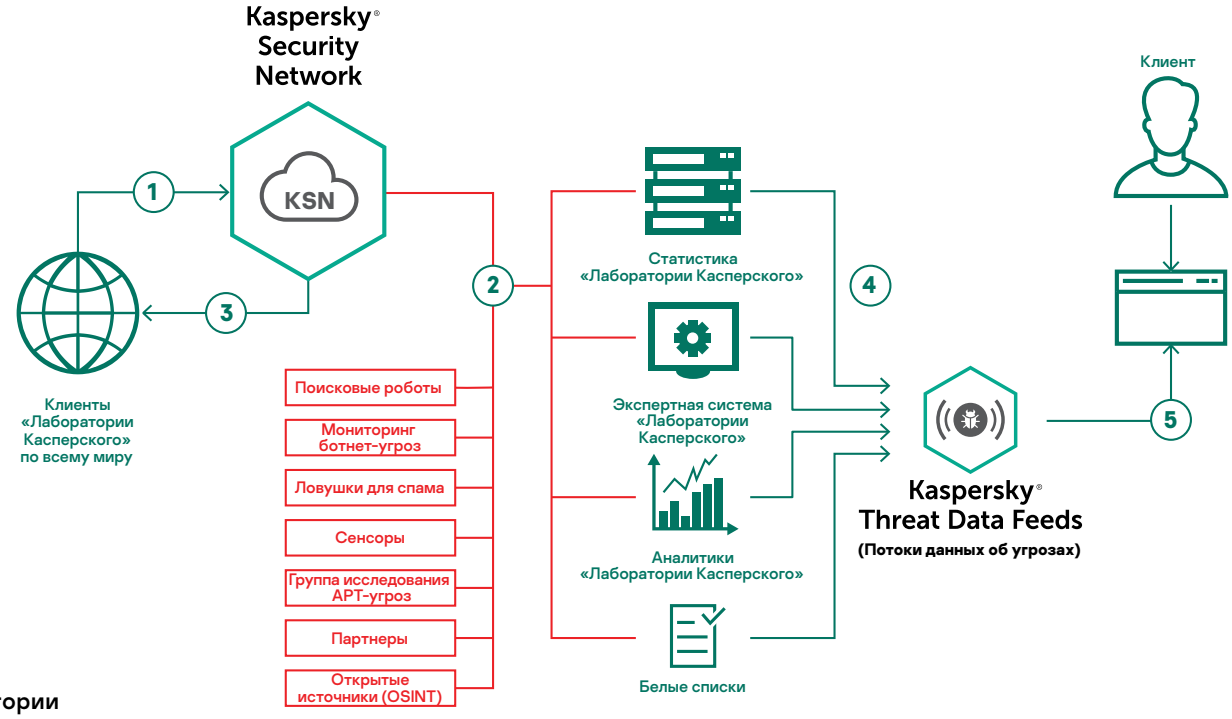


Рис. 15: Источники аналитических данных «Лаборатории Касперского» об угрозах

Активный поиск угроз (Threat Hunting)

Активный поиск угроз – важная часть ежедневной работы SOC. Сама идея обнаружения неизвестных и продвинутых угроз усилиями специалистов по безопасности, а не с использованием автоматических правил или механизмов обнаружения на основе сигнатур, не нова.

Современные атаки учитывают возможности защитных систем, находящихся в распоряжении их жертв, поэтому вредоносное ПО разрабатывается с учетом этих особенностей, чтобы обходить механизмы автоматического обнаружения и предотвращения атак. Атаки такого рода зачастую осуществляются вообще без использования какого-либо ПО, а действия атакующих практически не отличаются от действий специалистов службы IT-безопасности и информационной безопасности. Ниже перечислены лишь некоторые из методов осуществления современных атак:

- Использование методов, затрудняющих криминалистический анализ, например безвозвратного удаления артефактов с жесткого диска или осуществления атаки исключительно в памяти компьютера.
- Использование легитимных инструментов, которые обычно применяются в IT-отделах и службах информационной безопасности.
- Многоэтапные атаки, когда следы ранее осуществленных действий безвозвратно удаляются.
- Интерактивная работа команды профессионалов (аналогичная тестированию на проникновение).

Автоматическими средствами подобные атаки могут быть выявлены только после того, как целевой ресурс будет скомпрометирован, поскольку подозрительное поведение, указывающее на вредоносную активность, может быть обнаружено только тогда. Активный поиск угроз позволяет обнаруживать атаки еще до того, как произойдет первичная компрометация. Здесь ключевым элементом является участие профессионального аналитика на финальном этапе принятия решений. Присутствие человека в цепочке анализа событий компенсирует слабости логики автоматического обнаружения угроз. Более того, когда в атаке, подобной тестированию на проникновение, задействован человек, в противостоянии автоматическим технологиям преимущество, несомненно, будет на его стороне, поэтому участие аналитика является единственным способом противодействовать таким атакам.

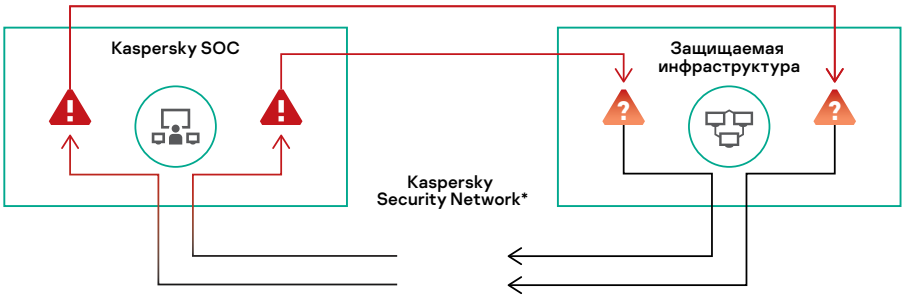
Однако нужно понимать, что ни автоматизированное обнаружение, ни активный поиск сами по себе не являются панацеей от всего спектра современных киберугроз. Только сочетание традиционных инструментов обнаружения и предотвращения угроз, активных до компрометации, с последующим итеративным процессом поиска новых угроз, пропущенных автоматизированными инструментами, может быть достаточно эффективно.

Особенности сервиса

- Высокий уровень непрерывной защиты от целевых атак и вредоносного ПО, круглосуточный мониторинг и поддержка, предоставляемые вашей персональной специализированной командой экспертов «Лаборатории Касперского», богатый выбор специалистов, обладающих множеством специальных навыков, и постоянный сбор аналитических данных об угрозах.
- Своевременное и точное обнаружение атак, не использующих вредоносное ПО, атак, использующих ранее неизвестные инструменты, и атак, эксплуатирующих уязвимости «нулевого дня».
- Обеспечение немедленной защиты от любых обнаруженных угроз за счет автоматического обновления антивирусных баз.
- Ретроспективный анализ инцидентов и активный поиск угроз, включая методы и технологии, использованные злоумышленниками против вашей организации.
- Интегрированный подход: линейка решений «Лаборатории Касперского»

Предложение «Лаборатории Касперского»: Kaspersky Managed Protection

Сервис Kaspersky Managed Protection позволяет поднять признанную эффективность решений Kaspersky Security для бизнеса и Kaspersky Anti Targeted Attack Platform на новый уровень и обеспечить противодействие самым сложным и уникальным угрозам. Сервис включает в себя круглосуточный анализ событий ИБ экспертами «Лаборатории Касперского» и непрерывный анализ данных о киберугрозах для обнаружения в реальном времени как известных, так и новых киберпреступных и шпионских кампаний, нацеленных на ваши информационные системы.



*Kaspersky Private Security Network для изолированных инфраструктур

Рис. 16:
Kaspersky Managed Protection

Преимущества для клиентов

- Быстрое и эффективное обнаружение, обеспечивающее более оперативное и эффективное устранение последствий инцидентов.
- Отсутствие ложноположительных срабатываний благодаря четкому немедленному обнаружению и классификации любой подозрительной активности.
- Сокращение расходов на безопасность. Отсутствие необходимости найма и обучения штатных сотрудников разных профилей.
- Уверенность в том, что вы находитесь под постоянной защитой даже от самых сложных и изощренных угроз, не использующих вредоносное ПО.
- Получение информации об атакующих, их мотивах, используемых методах и инструментах и потенциальном ущербе от их действий способствует разработке информированной и эффективной стратегии защиты.

Примечание

Настоящий документ не является публичной офертой и предназначен для использования только в ознакомительных целях.

Предоставляемые услуги могут варьироваться в зависимости от доступности в конкретных географических регионах. Для пользования некоторыми описанными в настоящем документе сервисами требуется заключение дополнительного соглашения с «Лабораторией Касперского».

www.kaspersky.ru