Кибербезопасность крупного бизнеса

KASPERSKY lab

Сервисы «Лаборатории Касперского» для SOC

www.kaspersky.ru

#ИстиннаяБезопасность

Сервисы «Лаборатории Касперского» для SOC

Корпоративная защита от киберугроз становится все лучше – поэтому злоумышленники изобретают все более изощренные методы проникновения за периметр безопасности. Возможность завладеть огромными средствами при помощи кибератак привлекает все больше любителей наживы, которые непрерывно отыскивают и эксплуатируют еще не обнаруженные недостатки защиты.

В ответ на это компании все чаще создают специальные центры обеспечения безопасности (SOC), которые борются с угрозами по мере их возникновения, а также помогают быстро реагировать на инциденты и устранять их.

Работа центров обеспечения безопасности должна основываться на сборе, анализе и сопоставлении данных из множества различных источников. Архитектура таких центров, с точки зрения организационных процессов и технологий, должна быть адаптивной, чтобы эффективно реагировать на постоянно меняющиеся угрозы. Руководители служб безопасности должны понимать, как SOC, опирающиеся на комплексный анализ данных, используют инструменты, процессы и стратегии для борьбы с современными угрозами.

Gartner, The Five Characteristics of an Intelligence-Driven Security Operations Center, ноябрь 2015 г.

Согласно модели адаптивной архитектуры безопасности, предложенной компанией Gartner, для успешной борьбы с киберугрозами в современных условиях сотрудники SOC должны располагать следующими возможностями:

- ПРОГНОЗИРОВАНИЕ
- ОБНАРУЖЕНИЕ
- ПРЕДОТВРАЩЕНИЕ
- РЕАГИРОВАНИЕ

Gartner, «Разработка адаптивной архитектуры безопасности для защиты от комплексных атак» (Designing an Adaptive Security Architecture for Protection From Advanced Attacks), февраль 2014 г., обновление – январь 2016 г.

SOC – централизованная функция для постоянного мониторинга и анализа угроз, а также предотвращения и устранения последствий инцидентов кибербезопасности

Опрос, в 2016 году проведенный исследователями B2B International среди 4000 компаний в 25 странах, показал:

- **38%** респондентов в течение предыдущих 12 месяцев столкнулись с серьезными **инцидентами, вызванными вирусами и вредоносными программами,** что повлекло за собой снижение производительности;
- **21%** компаний пострадали от **утечки/раскрытия данных в результате целевых атак;**
- около 40% опрошенных выделяют эти события как отдельную проблему;
- **17%** компаний пострадали от **DDoS-атак** в предыдущие 12 месяцев, и многие – больше одного раза;
- **42%** всех респондентов, столкнувшихся с **фишинговыми атаками**, – предприятия;
- **26%** всех нарушений безопасности **оставались необнаруженными** в течение нескольких недель и дольше до проведения внешних аудитов безопасности;
- в среднем для одного предприятия одна утечка данных **обходится, в финансовом выражении, в 891 тыс. долл. США** (в эту сумму входят зарплаты для дополнительных штатных сотрудников, потери средств в результате падения кредитного рейтинга и повышения страховых премий, ущерб от упущенных сделок, затраты на дополнительные PR-мероприятия для восстановления репутации бренда и расходы на услуги внешних консультантов);
- сумма общего ущерба для отдельных предприятий в результате **утечки данных составила от 393 тыс. до 1,1 млн долл. США**, в зависимости от срока обнаружения инцидента (чем короче срок, тем меньше ущерб для компании);
- общее количество скомпрометированных конфиденциальных записей о сотрудниках и клиентах также зависит от срока обнаружения и составляет от 9 тыс. при почти мгновенном обнаружении (при наличии системы обнаружения) до 240 тыс. в случаях, когда инцидент не обнаруживают дольше года.

Четыре ключевых элемента

Чтобы обеспечить такой подход, признанный эталонным в отрасли, необходимо использовать четыре ключевых элемента, а также четко определенные процессы и актуальные технологии. Необходимые элементы – следующие:

- **УПРАВЛЕНИЕ ЗНАНИЯМИ.** Сотрудники (специалисты SOC) должны быть хорошо обучены в области цифровой криминалистики, анализа вредоносных программ и реагирования на инциденты, чтобы предотвращать все более сложные атаки и эффективно реагировать на них.
- **АНАЛИЗ УГРОЗ** на основе данных, собранных из множества различных источников (чем больше, тем лучше), необходим для того, чтобы своевременно обнаруживать возникающие угрозы. Необходимо использовать:
  1. внутренние данные об угрозах;
  2. аналитику из общедоступных источников информации (OSINT);
  3. информацию подразделений CERT в отрасли;
  4. сведения от поставщиков защиты от вредоносных программ во всем мире.
- **АКТИВНЫЙ ПОИСК УГРОЗ** позволяет заблаговременно узнавать об угрозах, не обнаруживаемых традиционными системами безопасности, такими как сетевые экраны, системы обнаружения и предотвращения вторжений (IPS/IDS), SIEM и т. д.
- **ПРАВИЛЬНО ВЫСТРОЕННЫЙ ПРОЦЕСС РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ** позволяет ограничить ущерб и снизить затраты на устранение инцидентов. Все эти элементы одинаково важны, и каждый из них требует отдельного рассмотрения.

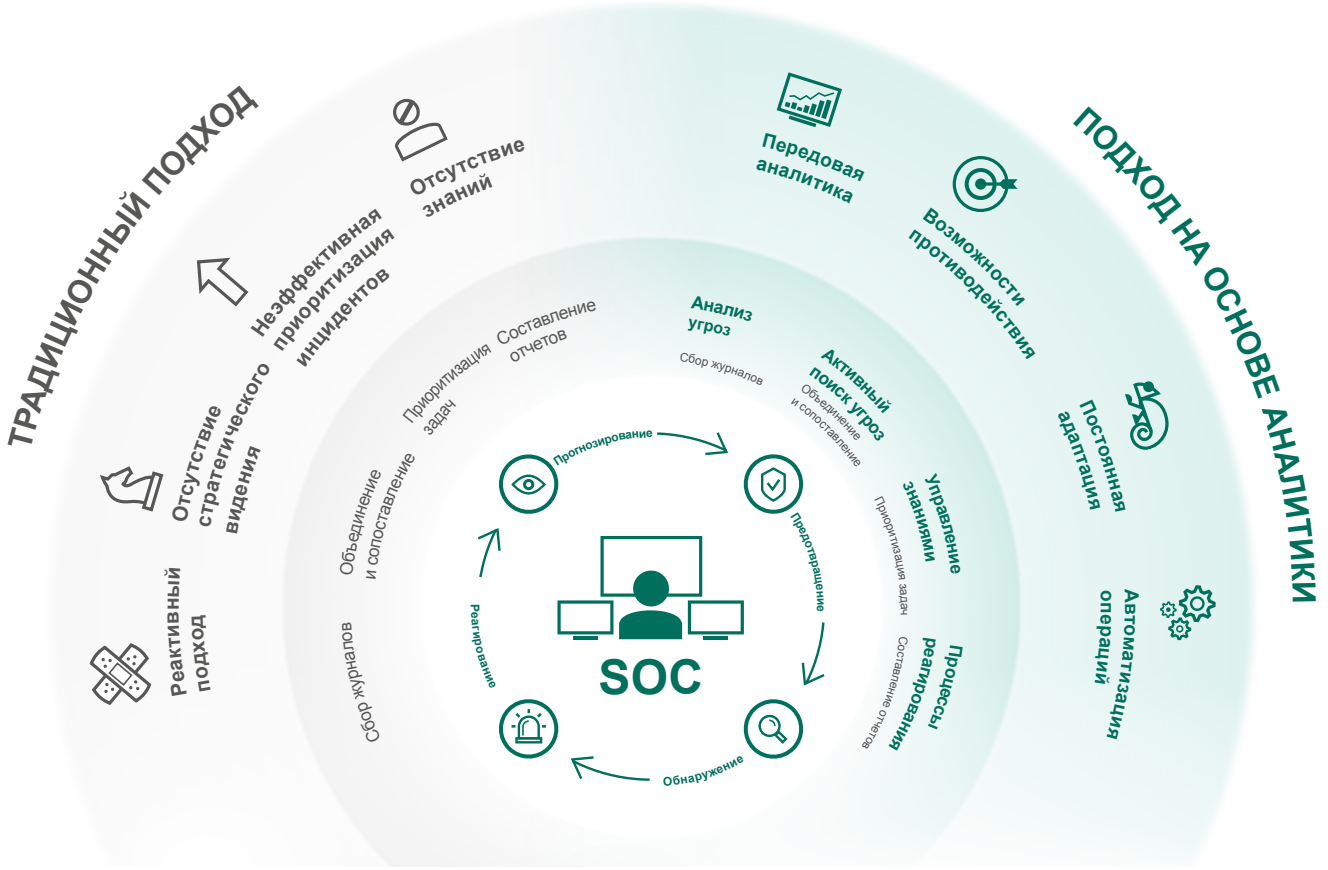


Рисунок 1. Четыре ключевых элемента SOC

Управление знаниями

SOC должен представлять собой источник практических знаний и опыта, позволяющих анализировать огромный объем данных и определять необходимость дальнейшего расследования.

В то же время ограниченные бюджеты затрудняют комплектование SOC первоклассными сотрудниками.

Сегодня рынок испытывает нехватку хорошо обученных специалистов по кибербезопасности, из-за чего возрастают затраты на набор таких сотрудников и оплату их труда.

Эффективный специалист SOC должен обладать следующими компетенциями:

- аналитический склад ума, позволяющий составлять общую картину путем сопоставления разрозненной информации;
- способность сохранять непрерывную концентрацию и выдерживать высокий уровень стресса;
- глубокие общие знания в области IT и кибербезопасности, предпочтительно дополненные богатым практическим опытом.

Кандидаты, уже обладающие нужными навыками для работы в SOC, встречаются редко – и внутри компаний, и на открытом рынке. Потребуется непрерывное обучение – не только чтобы развить нужные навыки на основе имеющихся, но и чтобы вооружать специалистов знаниями о постоянно меняющихся технологиях безопасности и развивающихся угрозах.

Навыки в области реагирования на инциденты, цифровой криминалистики и анализа вредоносных программ – обязательны для специалистов SOC.

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ И ЦИФРОВАЯ КРИМИНАЛИСТИКА

- Своевременный и точный ответ на инцидент
- Анализ улик (образы жестких дисков, дампы памяти, трассировки сети), а также восстановление истории и логики инцидентов
- Определение источников атаки и того, какие еще системы могли подвергнуться компрометации (если возможно)
- Выявление корневых причин инцидента для предотвращения подобных нарушений в будущем

АНАЛИЗ ВРЕДОНОСНЫХ ПРОГРАММ

- Изучение подозрительного образца и его возможностей
- Определение того, является ли этот образец вредоносной программой
- Выявление возможностей воздействия образца на скомпрометированные системы организации
- Составление комплексного плана устранения последствий, учитывающего изученное поведение вредоносной программы

Развитие навыков в области кибербезопасности

«Лаборатория Касперского» уже 20 лет постоянно расширяет и совершенствует свои экспертные знания в области кибербезопасности, будь то обнаружение угроз, исследование вредоносного ПО, обратная разработка или цифровая криминалистика. Наши эксперты знают, как лучше всего справиться с угрозами, представление о которых дают ежедневно обнаруживаемые ими 310 000 образцов вредоносных программ, и как передать эти знания и практический опыт организациям, сталкивающимся с новыми опасностями современного цифрового мира.

Консультационные услуги с участием экспертов «Лаборатории Касперского», включают как теоретические, так и практические (лабораторные) элементы и задания. После завершения программы консультаций участники могут проверить свои знания путем сертификации.

Консультационные услуги ориентированы на IT-специалистов, обладающих общими или экспертными навыками системного администрирования и программирования. Все консультации проводятся в региональных офисах «Лаборатории Касперского» либо на территории заказчика.

Описание программы

Темы	Продолжительность	Навыки
Цифровая криминалистика		
• Введение в цифровую криминалистику • Оперативное реагирование и сбор цифровых улик • Внутренняя структура реестра Windows • Анализ артефактов в Windows • Криминалистический анализ браузера • Анализ электронной почты	5 дней	• Организация лаборатории цифровой криминалистики • Сбор цифровых улик и порядок обращения с ними • Воссоздание хронологической картины инцидента с помощью временных меток • Выявление следов вторжения посредством анализа артефактов в ОС Windows • Анализ истории браузера и электронной почты • Эффективное применение средств и методов цифровой аналитики
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 скриптов и программ, отличных от исполняемых файлов (пакетные файлы, Autolt, 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

Темы	Продолжительность	Навыки
Цифровая криминалистика (экспертный уровень)		
• Экспертная криминалистика в ОС Windows • Восстановление данных • Сетевая и облачная криминалистика • Криминалистический анализ дампов памяти • Хронологический анализ • Практическая криминалистика реальных целевых атак	5 дней	• Глубокий анализ файловой системы • Восстановление удаленных файлов • Анализ сетевого трафика • Обнаружение вредоносной активности по дампам памяти • Восстановление хронологии инцидента
Анализ и обратная разработка вредоносного по (экспертный уровень)		
• Методы расширенного статического и динамического анализа (статический анализ шелл-кода, синтаксический анализ заголовка исполняемого файла, блоки переменных окружения потока (TEB) и окружения процесса (PEB), загрузка функций на основе различных алгоритмов хэширования) • Методы расширенного динамического анализа (структура исполняемого файла, ручная и экспертная распаковка, распаковка вредоносных архивов, содержащих полный исполняемый файл в зашифрованной форме) • Обратная разработка APT-угроз (полная проработка сценария APT-атаки, начиная с фишингового сообщения электронной почты и заканчивая как можно более глубоким анализом) • Анализ протоколов (анализ зашифрованных коммуникаций по протоколу C2, методы расшифровки трафика) • Анализ руткитов и буткитов (отладка загрузочного сектора при помощи IDA и VMWare, отладка ядра при помощи двух виртуальных машин, анализ образцов руткитов)	5 дней	• Использование передовых методов обратной разработки и распознавание методов защиты от обратной разработки (обфускация, защита от отладки) • Расширенный анализ руткитов и буткитов • Анализ шелл-кода эксплойтов, внедренного в различные виды файлов, а также вредоносных программ для сред, отличных от Windows
Реагирование на инциденты		
• Общие сведения о реагировании на инциденты • Обнаружение и первичный анализ • Цифровой анализ • Создание правил обнаружения (YARA, Snort, Bro)	5 дней	• Отделение APT от других типов угроз • Понимание различных методов атаки и анатомии целевых атак • Применение специальных методов мониторинга и обнаружения • Выполнение процедуры реагирования на инциденты • Восстановление хронологической картины и логики инцидента • Создание правил обнаружения и подготовка отчетов

Инструменты со временем меняются, но основные принципы и методы работы остаются прежними. Участники не только получат набор инструментов с инструкциями, но и освоят фундаментальные принципы и ключевые функции. Все практические задания основаны на реальных случаях (если их можно использовать без нарушения конфиденциальности клиентов).

Анализ и активный поиск угроз

Центры SOC создавались, чтобы обеспечить, в частности, следующее:

- управление устройствами защиты, поддержание безопасности периметра и управление превентивными технологиями борьбы с угрозами (IPS/IDS, сетевые экраны, прокси-серверы и т. д.);
- мониторинг событий безопасности при помощи системы управления информацией и событиями информационной безопасности безопасности (SIEM);
- реагирование на инциденты и устранение их последствий;
- контроль соответствия внутренним и нормативным требованиям (например, стандарту PCI-DSS).

Многие организации планируют развернуть собственные SOC, чтобы повысить свою осведомленность об угрозах. В то же время некоторые компании, уже использующие центры обеспечения безопасности, по-прежнему сталкиваются со старыми проблемами.

Это происходит по ряду причин:

- неправильная приоритизация, в результате которой настоящие угрозы «теряются» среди тысяч оповещений о незначительных событиях, получаемых и анализируемых ежедневно;
- устранение последствий инцидентов без надлежащего понимания тактики, методов и процедур, применяемых злоумышленниками, в результате чего комплексные атаки не обнаруживаются;
- ложные срабатывания из-за отсутствия данных о соответствующих угрозах;
- реактивный подход к защите вместо проактивного поиска угроз, не обнаруженных, но вредящих организации;
- отсутствие полной картины существующих угроз или осведомленности об атаках на похожие предприятия и доступных мерах противодействия;

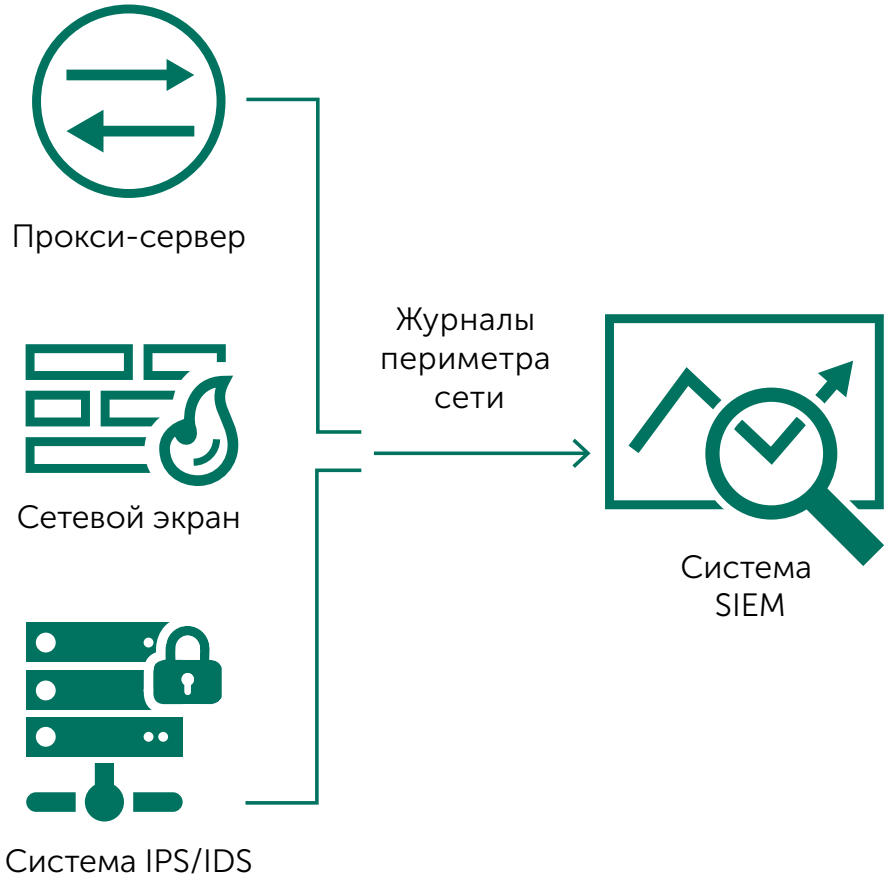


Рисунок 2. Традиционная организация SOC

- трудности привлечения достаточного финансирования на конкретные технологии безопасности из-за непонимания руководителями возможных рисков для бизнес-процессов вследствие нарушений безопасности.

Gartner определяет аналитику угроз следующим образом:

«Основанные на фактах знания (включая контекст, механизмы, индикаторы, последствия и практические шаги) о существующей или возникающей угрозе или опасности для активов, на основании которых субъект может принимать решения о реагировании на эту угрозу или опасность».

Gartner, «Аналитика угроз в понимании Gartner» (How Gartner Defines Threat Intelligence), февраль 2016 г.

Чтобы эффективно бороться с угрозами, SOC должен постоянно внедрять новые технологии и средства защиты, в соответсвии с быстро меняющимся ландшафтом угроз.

Используя внутренние данные об угрозах и информацию, собранную из многочисленных источников (например, OSINT или от поставщиков защиты от вредоносных программ во всем мире), компания узнает о методах и возможных признаках атак. Это, в свою очередь, позволяет вырабатывать эффективные стратегии защиты от обычных и комплексных атак, направленных на компанию.

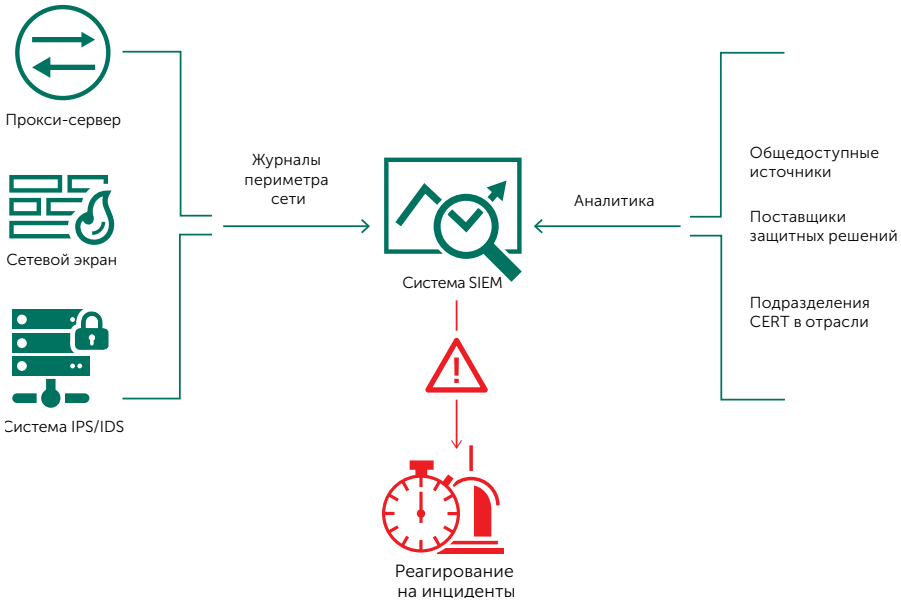


Рисунок 3. Подход к организации SOC на основе аналитики

Источники данных необходимо выбирать тщательно. От качества используемых данных напрямую зависит эффективность принимаемых на их основе решений. Если вы полагаетесь на неактуальную, неточную или не соответствующую целям вашей отрасли или бизнес-целям аналитику, качество корпоративных решений может сильно снижаться. То же справедливо, если информация поступает несвоевременно.

Использование «сырых» данных без контекстной информации не позволит SOC достичь нужной эффективности. Одно дело – обнаружить, что URL-адрес вредоносен, и совсем другое – знать, что он используется для хранения эксплойта или вредоносной программы конкретного типа. Аналитика такого уровня помогает специалистам по безопасности понять, что следует искать при исследовании зараженной машины.

Требования к внешним источникам аналитики угроз:

- глобальный охват данных, обеспечивающий максимальный обзор существующих атак
- поставщик обладает подтвержденной способностью быстро обнаруживать признаки новых угроз;
- результаты анализа содержат контекст и дают возможность действовать незамедлительно;
- форматы и методы доставки данных позволяют просто интегрироваться с существующей системой безопасности.

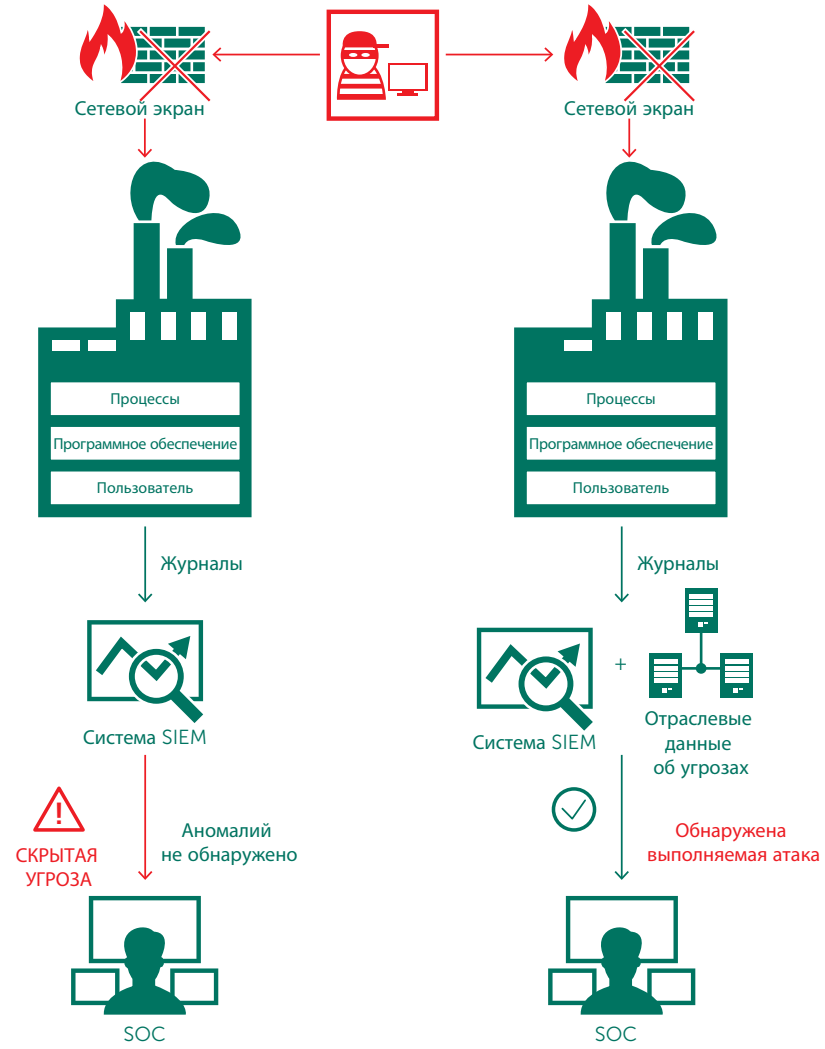


Рисунок 4. Модель анализа угроз

Активный поиск угроз является еще одним важным элементом повседневной работы SOC. Эта концепция не нова. Для обнаружения неизвестных и комплексных угроз требуется тщательная проактивная работа аналитиков по безопасности: здесь не всегда могут помочь автоматические правила и сигнатурные механизмы обнаружения.

Этот процесс предполагает подбор различных методов (таких как статический анализ, машинное обучение и визуализация) и применение их ко всем доступным данным, полученным с рабочих мест, из сетей, применяемых средств защиты, систем аутентификации и т. д. Цель этой работы – проверка существующей гипотезы о возможном нарушении безопасности. Для активного поиска угроз аналитики могут использовать уже упомянутые технологии: SIEM, OSINT, платформы анализа угроз и другие источники данных.

Аналитики, занимающиеся поиском угроз, опираются на индикаторы компрометации (IOC), полученные из внешних источников, и применяют специализированные инструменты для обнаружения таких артефактов (в форме IP- и URL-адресов, хэшей файлов и т. д.) на узлах организации. При обнаружении очевидного признака нарушения безопасности инициируются процедуры реагирования на инцидент.

Поиск в огромных массивах данных для выявления артефактов, не обнаруженных автоматическими средствами, могут выполнять только высококвалифицированные, опытные специалисты.

Потоки данных об угрозах

«Лаборатория Касперского» предлагает клиентам постоянно обновляемые потоки данных об угрозах: используя их, специалисты SOC могут могут своевременно узнавать о существующих атак и эффективнее противодействовать атакам.

Описание потоков данных

Данные о репутации IP-адресов – набор IP-адресов с контекстной информацией, сообщающий о подозрительных и вредоносных узлах.

URL-адреса вредоносных ссылок – набор URL-адресов, соответствующих опасным ссылкам и веб-сайтам. Доступны записи с масками и без масок.

URL-адреса фишинговых ссылок – набор 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.

Белые списки – систематизированный набор хэшей надежных файлов, доступный для использования решениями и сервисами третьих сторон.

Хэши вредоносных объектов – набор файловых хэшей, охватывающий наиболее опасные и распространенные, а также самые новые вредоносные программы.

Хэши вредоносных объектов для мобильных устройств – набор файловых хэшей для обнаружения вредоносных объектов, заражающих мобильные устройства.

Данные о троянцах P-SMS – набор 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.

Хэши вредоносных объектов для мобильных устройств – набор файловых хэшей для обнаружения вредоносных объектов, заражающих мобильные устройства.

URL-адреса командных серверов ботнетов для мобильных устройств – набор URL-адресов с контекстной информацией для выявления командных серверов ботнетов, использующих мобильные устройства.

Преимущества сервиса

- Потоки данных об угрозах 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 большое количество обнаруженных угроз и точность обнаружения.
- Каждая запись в каждом потоке данных содержит контекст, позволяющий действовать (названия угроз, временные метки, географическое местоположение, IP-адреса зараженных веб-ресурсов, хэши, популярность и т. д.). Информация о контексте помогает увидеть общую картину, оправдывая широкое использование данных в настоящем и в дальнейшем. Данные в контексте легче использовать, чтобы ответить на вопросы «Кто?», «Что?», «Где?», «Когда?», которые позволяют выявить источники атак, а также помогают принять своевременные решения и выполнить действия, которые защитят именно вашу организацию.
- Простые форматы для распространения данных (JSON, CSV, OpenIoC, STIX) через HTTPS и методы доставки для конкретных случаев позволяют без затруднений интегрировать потоки данных в решения безопасности.
- Аналитические данные об угрозах генерируются и отслеживаются мощной отказоустойчивой инфраструктурой, что обеспечивает постоянную доступность и непрерывную работу.
- Обеспечена мгновенная интеграция с HP ArcSight, IBM QRadar, Splunk и др.

Сервис Threat Lookup

Kaspersky Threat Lookup – это мощная единая платформа, открывающая доступ ко всем накопленным «Лабораторией Касперского» знаниям о киберугрозах и их взаимосвязях. Сервис предоставляет вашим специалистам по безопасности максимум информации для предотвращения кибератак до того, как организации будет нанесен вред. Платформа собирает подробные актуальные сведения об угрозах: URL-адреса, домены, IP-адреса, контрольные суммы файлов, названия угроз, статистику и поведенческие данные, данные WHOIS/DNS и т. д. Это обеспечивает глобальную видимость новых и возникающих угроз, помогает ускорить реагирование и повысить его эффективность.

Преимущества сервиса

- Надежные данные об угрозах. «Лаборатория Касперского» предоставляет надежные данные об угрозах с практическими контекстными рекомендациями по их нейтрализации. Продукты «Лаборатории Касперского» показывают наилучшие результаты при тестировании решений для защиты от вредоносных программ[1]. Непревзойденное качество аналитических данных подтверждается самым высоким уровнем обнаружения практически без ложных срабатываний.
- Широкий охват в реальном времени. Аналитика угроз генерируется автоматически в режиме реального времени на основе данных, собираемых по всему миру сетью Kaspersky Security Network.
- Активный поиск угроз. Проактивное выявление и предотвращение атак позволяют 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.
- Разнообразие данных. Сервис проверки угроз собирает об угрозах данные самых разнообразных типов, в том числе контрольные суммы, URL- и IP-адреса, данные whois, pDNS и GeoIP, атрибуты файлов, статистику и сведения об активности, цепочки загрузки, временные метки и многое другое. Вооружившись этой информацией, вы сможете оценить все разнообразие угроз, которым подвергаетесь.
- Постоянная доступность. Аналитические данные об угрозах генерируются и отслеживаются мощной отказоустойчивой инфраструктурой, что обеспечивает постоянную доступность и непрерывную работу.
- Постоянное сотрудничество с экспертами по безопасности. В подготовке аналитических данных участвуют сотни экспертов, включая аналитиков по безопасности со всего мира, специалистов глобального центра исследования и анализа угроз и лучшие научно-исследовательские коллективы.

1 http://www.kaspersky.ru/top3

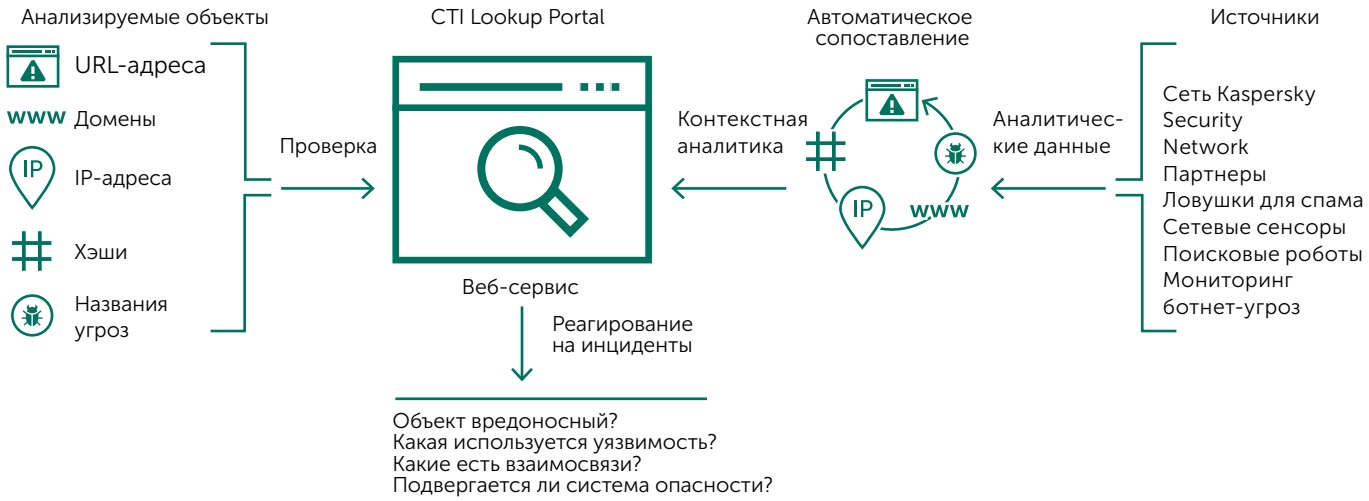
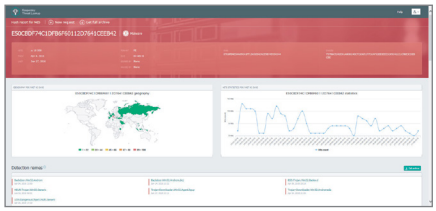
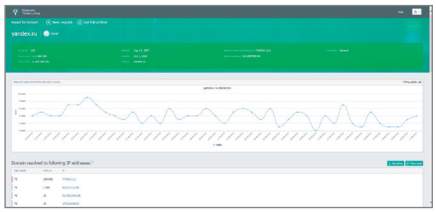


Рисунок 5. Архитектура Kaspersky Threat Lookup





- 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 безопасностью, такие как системы SIEM.
- Простота использования через веб-интерфейс или API на основе REST. К сервису можно обращаться в ручном режиме через веб-интерфейс (открывается в браузере) или через простой API на основе REST.

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 информацию об APT-угрозах и действовать.

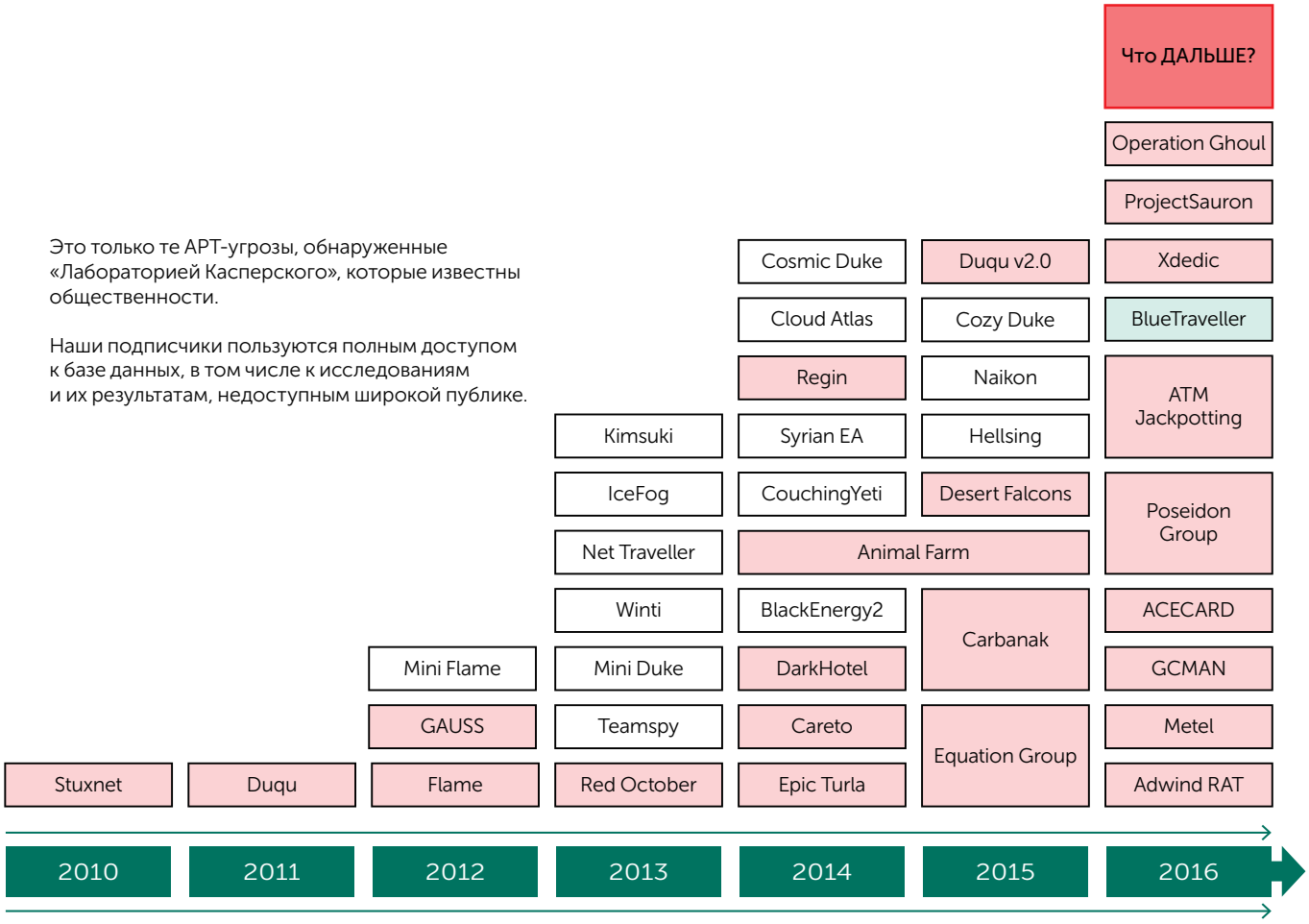


Рисунок 6. APT-угрозы, обнаруженные «Лабораторией Касперского»

Подписчики на такие отчеты получают уникальный доступ к результатам расследования и техническим данным в различных форматах по каждой обнаруженной APT-угрозе, даже если эти данные 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. Более того, вы получите доступ к полной базе отчетов «Лаборатории Касперского» о комплексных целевых угрозах. Она станет ценным аналитическим дополнением к вашей корпоративной системе безопасности.

Преимущества сервиса

- Эксклюзивный доступ к техническим описаниям новейших угроз уже в ходе расследования, до публичного объявления.
- Непубличные данные об APT-угрозах. Не обо всех масштабных угрозах сообщается публично. Некоторые угрозы так и остаются тайной из-за специфики своих жертв, особой конфиденциальности данных, самой природы устранения уязвимости или привлечения правоохранительных органов. Однако наши клиенты получают доступ к таким отчетам.
- Подробные технические данные, 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).
- Ретроспективный анализ. В течение периода подписки предоставляется доступ ко всем ранее выпущенным закрытым отчетам.

С практической точки зрения, индикаторы компрометации – наиболее полезная часть отчетов для специалистов SOC. Эта структурированная информация предназначена для использования вместе со специальными автоматическими инструментами, которые помогают проверить инфраструктуру на наличие признаков заражения. Все отчеты доставляются через специальный портал аналитических отчетов об APT-угрозах (см. рис. ниже).

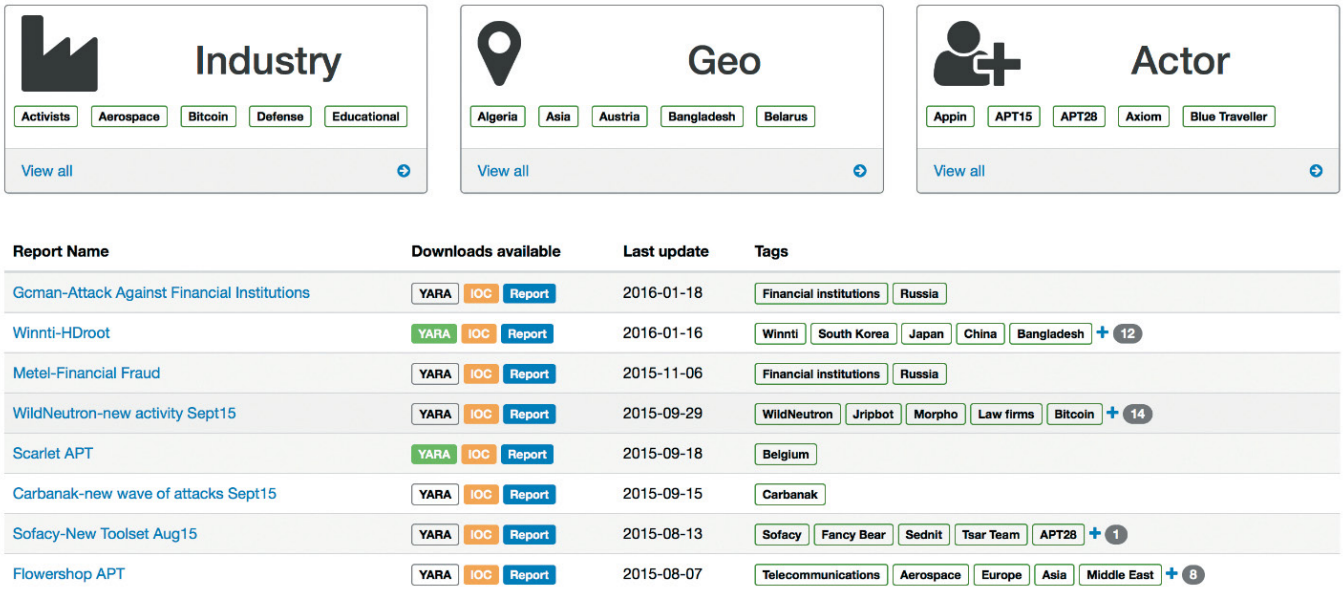


Рисунок 7. Портал аналитических отчетов об APT-угрозах

Кастомизированные отчеты об угрозах

Отчеты об угрозах для конкретных организаций

Как удобнее 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?

Кастомизированные отчеты «Лаборатории Касперского» для конкретных организаций 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. Отчёты содержат следующую информацию:

- **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 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.
- **Утечка 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 отчетов для конкретных клиентов 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.

Отчеты об угрозах для конкретных стран

Кибербезопасность страны важна для защиты 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.

Имея представление о поверхности атаки на данный момент, а также о текущих тенденциях распространения вредоносных программ и кибератак против вашей страны, вы сможете сосредоточиться на уязвимостях, которые больше всего интересуют киберпреступников, чтобы быстро и точно отражать вторжения и свести к минимуму риск успешной атаки.

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. Отчеты содержат следующую информацию:

- **Определение векторов угроз.** Выявление и анализ состояния критически важных IT-ресурсов страны, доступных извне, включая уязвимые правительственные приложения, телекоммуникационное оборудование, компоненты промышленных систем управления (системы SCADA, программируемые контроллеры и др.), банкоматы и т. д.
- **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.
- **Утечка 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 существующих 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.

Kaspersky Managed Protection

Kaspersky Managed Protection — круглосуточная служба мониторинга и реагирования на инциденты. Внутри «Лаборатории Касперского» специально для вашей компании формируется команда экспертов, обладающих специализированными навыками и богатым опытом в области анализа угроз. Эти специалисты предоставляют полностью управляемый, индивидуально подобранный сервис непрерывного обнаружения, защиты и анализа, а вы получаете максимальную отдачу от данных, получаемых от установленных в вашей инфраструктуре решений «Лаборатории Касперского».

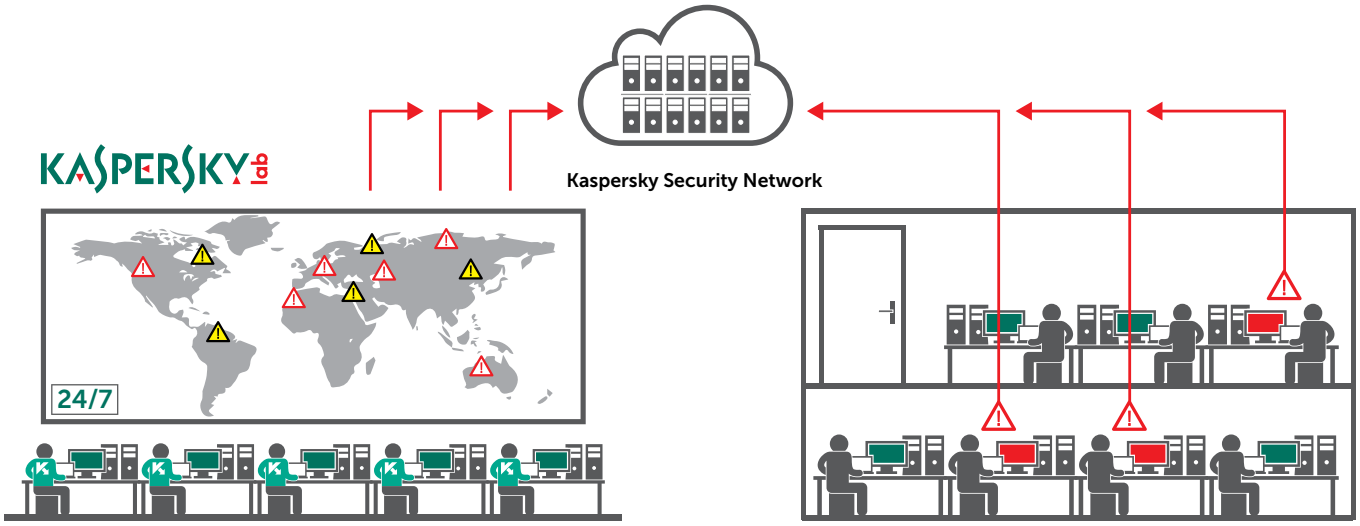


Рисунок 8. Защита силами «Лаборатории Касперского»

Ключевые преимущества

- Высокий уровень защищенности от целевых атак и вредоносного ПО при поддержке аналитиков «Лаборатории Касперского».
- Обнаружение атак, выполняемых без применения вредоносного ПО (non-malware attacks) или с применением неизвестных ранее инструментов, а также эксплуатирующих уязвимости нулевого дня.
- Мгновенная защита от только что обнаруженных угроз путем автоматического обновления баз данных угроз в режиме реального времени.
- Ретроспективный анализ инцидентов, в том числе с помощью методов и технологий, использованных против вас злоумышленниками.
- Комплексный подход: наличие у «Лаборатории Касперского» технологических и сервисных продуктов для организации полного цикла организации защиты от целевых атак: Подготовка – обнаружение и расследование – анализ данных – автоматизированная защита.

Круглосуточная служба мониторинга:

- оперативно выявляет инциденты
- собирает информацию, достаточную для их классификации (ложное или корректное срабатывание)
- устанавливает насколько распространены собранные артефакты, определяя степень уникальности данной атаки
- инициирует процесс реагирования на инцидент информационной безопасности
- при необходимости инициирует обновление баз знаний средств защиты, чтобы заблокировать угрозу
- проводит ретроспективный анализ системной и сетевой активности процессов и приложений с целью расследования инцидентов.

Дополнительно об источниках, используемых «Лабораторией Касперского» для анализа угроз

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.

Итак, ваши специалисты обладают необходимыми навыками и хорошо обучены. Аналитические данные об угрозах поступают из надежных источников в ваши системы безопасности. Остается правильно организовать процесс реагирования на инциденты.

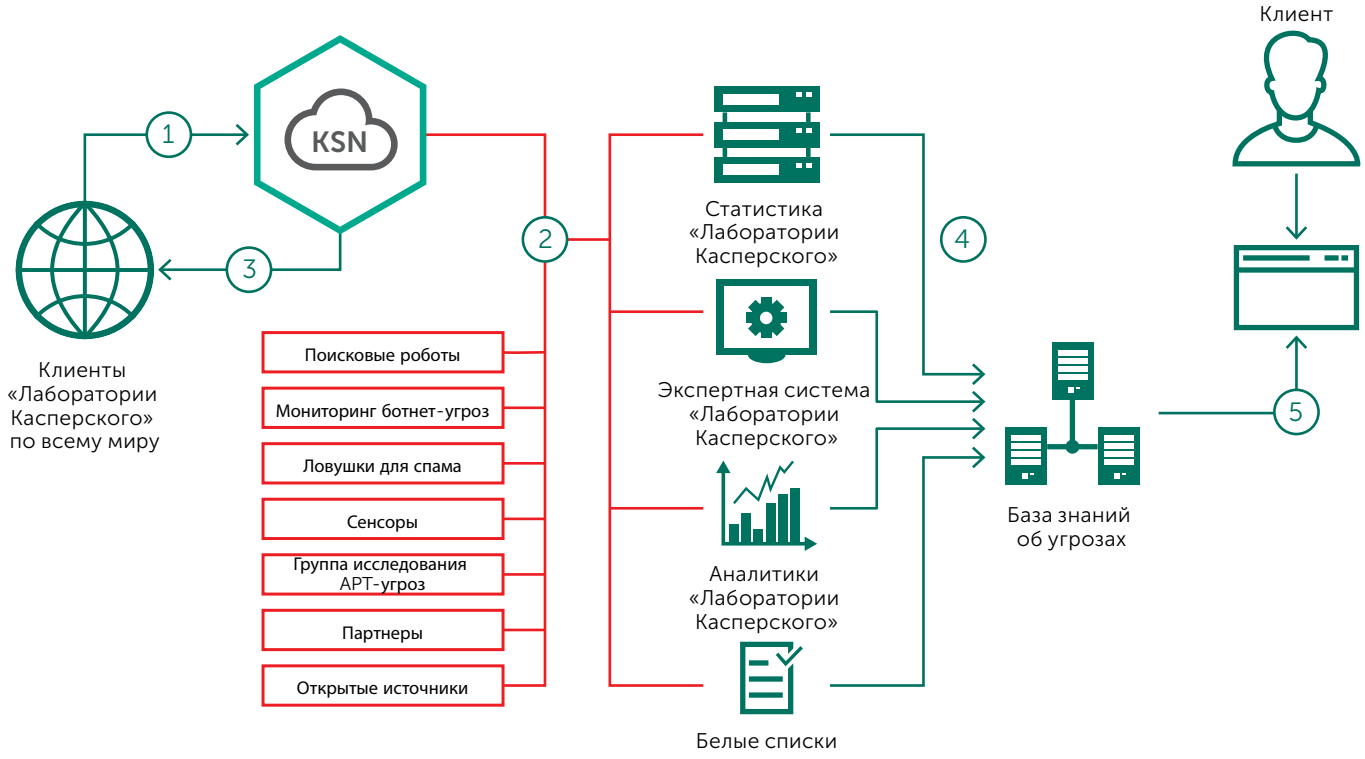


Рисунок 9. Источники, используемые «Лабораторией Касперского» для анализа угроз

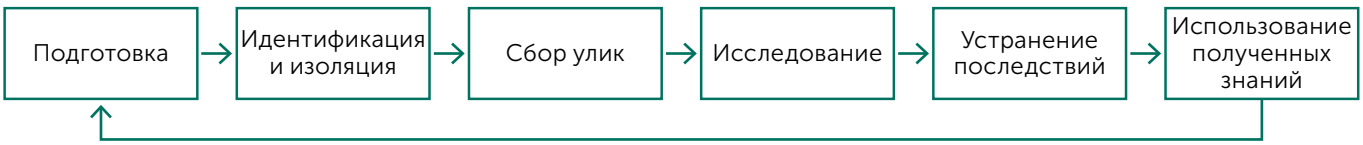
Реагирование на инциденты информационной безопасности

Цифровая криминалистика и реагирование на инциденты требуют выделения значительных внутренних ресурсов, причем в крайне короткое время или даже мгновенно. Для решения этих задач нужны компетентные специалисты, обладающие обширным практическим опытом борьбы с киберугрозами, способные оперативно идентифицировать, изолировать и блокировать вредоносное действие. Скорость имеет здесь первостепенное значение: чем быстрее реакция на угрозу, тем меньше последствий и ниже затраты на их устранение.

Такая срочная «мобилизация» возможна далеко не всегда, даже для хорошо организованного SOC, – редкие компании обладают достаточными внутренними ресурсами, чтобы незамедлительно останавливать атаки. А в некоторых случаях – например, если предприятие подверглось комплексной атаке, организованной каким-либо государством, или пострадало от APT-кампании – специалисты SOC просто не обладают экспертными знаниями о специфичных подходах и тактиках, используемых противником.

В таких случаях лучше прибегнуть к помощи стороннего поставщика услуг или консультаций по реагированию на инциденты, способного быстро и компетентно ответить на угрозу: это более экономично и эффективно. Правильно выстроенный процесс реагирования на инциденты должен содержать следующие шаги:

- **Идентификация инцидента**
  Первоначальный анализ инцидента и изоляция зараженных систем.
- **Сбор улик**
  Исследование различных источников (в зависимости от типа инцидента) для получения необходимых доказательств.
- **Цифровая криминалистика (если требуется)**
  Составление подробной картины инцидента.
- **Анализ вредоносной программы (если требуется)**
  Анализ для выявления возможностей вредоносной программы.
- **План устранения последствий**
  Составление плана для устранения корневой причины инцидента и всех следов вредоносного кода.
- **Использование полученных знаний**
  Пересмотр и обновление существующих мер безопасности для предотвращения подобных инцидентов.



Процесс реагирования на инциденты

Рисунок 10. Процесс реагирования на инциденты

Сервис реагирования на инциденты

Сервис реагирования на инциденты предоставляет наилучшие возможности защиты. Он включает весь цикл расследования инцидента, от сбора улик на месте до выявления дополнительных индикаторов компрометации, подготовки плана борьбы с последствиями и полного устранения угрозы для вашей организации. Работы по реагированию на инциденты ведут опытные аналитики и специалисты по обнаружению проникновения в информационные системы. На разрешение возникшего у вас нарушения безопасности будет направлена вся мощь нашего глобального опыта в цифровой криминалистике и анализе вредоносных программ.

В ходе предоставления сервиса мы выполняем следующие действия:

- выявляем скомпрометированные ресурсы;
- изолируем угрозу;
- останавливаем распространение атаки;
- находим и собираем улики;
- анализируем улики, а также восстанавливаем хронологическую картину и логику развития инцидента;
- анализируем вредоносные программы, использованные для атаки (если такие программы обнаружены);
- по возможности выявляем источники атаки и определяем, какие еще системы могли подвергнуться компрометации;
- проверяем вашу IT-инфраструктуру на возможные признаки компрометации;
- анализируем исходящие соединения вашей сети с внешними ресурсами для выявления подозрительных объектов (например, командных серверов);
- устраняем угрозу;
- рекомендуем вам дальнейшие действия по устранению последствий.

В зависимости от наличия у вас собственной группы реагирования на инциденты наши эксперты могут провести расследование полного цикла, либо только выявить и изолировать скомпрометированные машины и предотвратить распространение угрозы, либо выполнить анализ вредоносных программ или цифровую криминалистическую экспертизу.

Анализ вредоносного ПО

Анализ вредоносного ПО позволяет получить полное представление о поведении конкретных вредоносных программ, использованных для атаки на вашу организацию, а также о целях, преследуемых злоумышленниками. Эксперты «Лаборатории Касперского» осуществляют всесторонний анализ образца вредоносного ПО, предоставленного вашей организацией, и составляют подробный отчет, содержащий следующую информацию:

- свойства образца – краткое описание и вердикт согласно классификации «Лаборатории Касперского»;
- подробное описание вредоносной программы – углубленный анализ функций, поведения и целей вредоносной программы, включая индикаторы компрометации, дающий вам информацию, необходимую для нейтрализации угрозы;
- сценарий устранения последствий – в отчете будут предложены шаги по обеспечению эффективной защиты вашей организации от угроз данного типа.

Цифровая криминалистика

Цифровой криминалистический анализ может включать в себя анализ вредоносного ПО, если оно будет обнаружено в ходе расследования. Эксперты «Лаборатории Касперского» используют различные источники, например образы жестких дисков, дампы памяти, трассировки сети и др., чтобы воссоздать полную картину инцидента. Расследование начинается с того, что клиент собирает улики и предоставляет описание инцидента. Эксперты «Лаборатории Касперского» исследуют симптомы инцидента, идентифицируют исполняемый файл вредоносной программы (если он есть) и проводят ее анализ. Клиенту предоставляется подробный отчет с указанием мер, необходимых для устранения последствий инцидента.

ВАРИАНТЫ ПРЕДОСТАВЛЕНИЯ СЕРВИСА

Сервис реагирования на инциденты, предлагаемый «Лабораторией Касперского», доступен:

- на основе подписки;
- для устранения единичного инцидента.

В обоих случаях наши эксперты могут уделять устранению инцидента различное количество времени. Этот вопрос обсуждается с клиентом до подписания контракта. Клиент может включать в контракт столько рабочих часов, сколько считает необходимым, или прислушаться к рекомендациям наших экспертов в каждом конкретном случае.

В чем преимущества «Лаборатории Касперского»?

Мы обладаем следующими возможностями:

- с нами сотрудничают международные правоохранительные организации, включая Интерпол и подразделения CERT;
- мы используем средства облачной защиты, отслеживающие миллионы киберугроз по всему миру в режиме реального времени;
- наша международная команда экспертов исследует и анализирует все виды интернет-угроз.

«Лаборатория Касперского» – это:

- крупнейшая в мире независимая компания – производитель ПО для обеспечения IT-безопасности, ориентированная на глубокое изучение угроз и технологическое лидерство;
- безоговорочный лидер среди всех производителей защитного ПО по числу наград, завоеванных в независимых тестах;
- лидер по версиям Gartner, Forrester и IDC.

О «Лаборатории Касперского»

«Лаборатория Касперского» – крупнейшая в мире частная компания, поставляющая решения для защиты рабочих мест. Компания входит в список четырех лидирующих мировых поставщиков решений для обеспечения безопасности рабочих мест. На протяжении своей 20-летней истории «Лаборатория Касперского» постоянно внедряет новые разработки в сфере IT-безопасности и предлагает эффективные решения для обеспечения компьютерной безопасности предприятиям крупного, среднего и малого бизнеса, а также частным пользователям. Технологии и решения «Лаборатории Касперского» защищают более 350 миллионов пользователей почти в 200 странах и регионах мира.

Информация о сервисах

Настоящий документ не является публичным предложением и предназначен исключительно для ознакомительных целей.

Типы предоставляемых сервисов могут различаться в зависимости от их доступности в конкретном географическом регионе

Использование ряда сервисов, описанных в документе, требует дополнительных соглашений с «Лабораторией Касперского».

Для получения более подробной информации обратитесь к региональному представителю «Лаборатории Касперского» или отправьте запрос по адресу intelligence@kaspersky.com.

www.kaspersky.ru

#ИстиннаяБезопасность