Kaspersky Managed Protection

Круглосуточная служба анализа событий безопасности, созданная «Лабораторией Касперского» — признанным лидером в области исследований целевых атак.

Обычно отделы IT-безопасности реагируют на инциденты только после получения соответствующих оповещений систем безопасности.

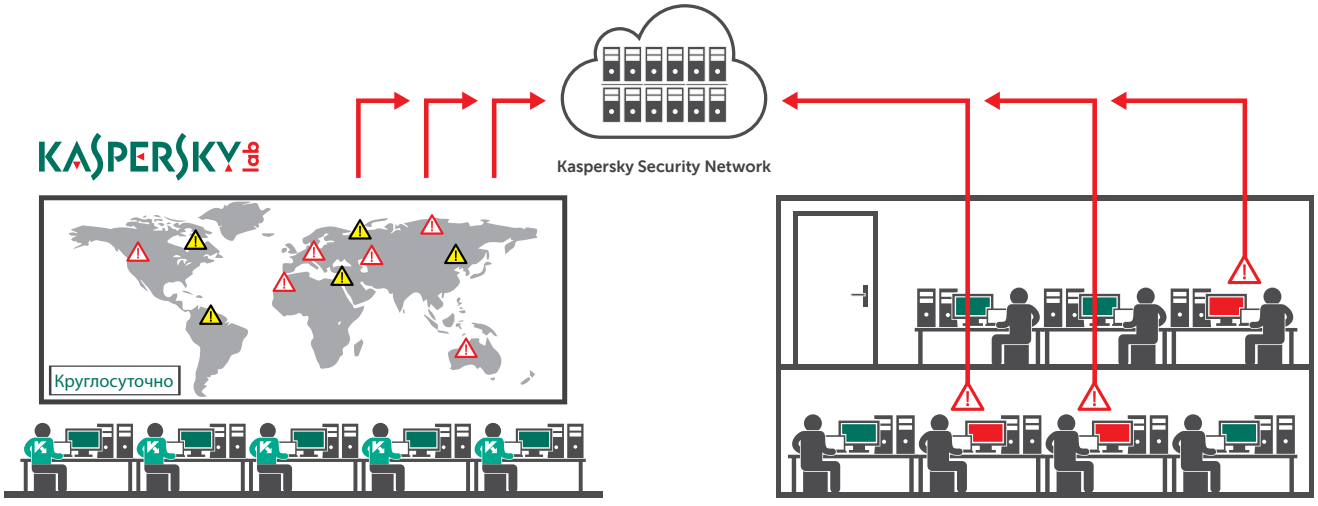
По этой причине новые угрозы, для которых производителем защитных решений пока не предложена методика обнаружения, могут ускользать из поля зрения, что создает ложное чувство защищенности.

Компании все чаще осознают потребность в проактивном выявлении угроз (Cyber Threat Hunting) для корпоративных инфраструктур – такой подход позволяет обнаружить незамеченные действующие атаки, а также помогает противодействовать угрозам, для которых еще не разработаны решающие правила.

На протяжении многих лет «Лаборатория Касперского» проводит исследования, направленные на выявление самых сложных кибератак. Высокое качество этих исследований подтверждается многочисленными успешными результатами тестов наших продуктов. Однако с появлением целевых атак подобные исследования необходимо перенести в инфраструктуру конкретного предприятия. Kaspersky Managed Protection – операционный сервис активного поиска киберугроз, направленных на вашу организацию.

Ключевые преимущества

- Комплексный подход к противодействию угрозам: предотвращение атак с использованием признанной системы защиты рабочих мест Kaspersky Security для бизнеса, обнаружение и расследование – там, где автоматическое предотвращение технически невозможно, и активный поиск угроз высококвалифицированным аналитиком в случае скрытых целевых атак, требующих глубокого исследования.
- Обнаружение бесфайлового вредоносного ПО (file-less), атак, выполняемых без применения вредоносного ПО (malware-less attacks) или с применением неизвестных ранее инструментов проведения атак.
- Моментальное противодействие атаке через используемую систему защиты рабочих мест.



Дополнительные преимущества

- В качестве сенсоров используются уже развернутые продукты (Kaspersky Security для бизнеса и Kaspersky Anti Targeted Attack Platform) – не надо разворачивать и конфигурировать дополнительные агенты и сервера управления
- Снижение совокупных затрат на обеспечение безопасности — не нужно нанимать и обучать штатных специалистов
- Минимальное количество ложных срабатываний благодаря тому, что последнее слово в цепи принятия решения остается за высококвалифицированным аналитиком
- Уверенность от осознания того, что вы защищены даже от самых сложных и инновационных атак, подтвержденная многолетней успешной практикой «Лаборатории Касперского» по выявлению сложнейших угроз
- Сведения об атакующих вас злоумышленниках, их мотивации, методах и средствах, а также потенциальном ущербе, который они могли бы причинить, ложатся в основу разработки эффективной стратегии защиты.

Как работает Kaspersky Managed Protection

В рамках оказания сервиса эксперты Центра мониторинга кибербезопасности «Лаборатории Касперского» осуществляют анализ расширенной телеметрии с установленных в сетях заказчика продуктов Kaspersky Security для бизнеса и Kaspersky Anti Targeted Attack, выступающих в качестве сенсоров. Это достигается, в частности, за счет проактивного сбора метаданных сетевой и системной активности. Полученная информация агрегируется с использованием Kaspersky Security Network и исследуется аналитиками на основе данных об угрозах (Threat intelligence), собранных «Лабораторией Касперского» за все время деятельности, что позволяет обнаружить актуальные тактики, техники и процедуры злоумышленников.

Круглосуточная служба анализа событий безопасности:

- оперативно выявляет инциденты информационной безопасности посредством многоэтапного анализа расширенной телеметрии сенсоров, размещенных в инфраструктуре заказчика;
- собирает информацию, достаточную для классификации выявленных инцидентов (ложное или корректное срабатывание);
- инициирует процесс реагирования на выявленные инциденты;
- при наличии технической возможности, инициирует обновление баз средств защиты, чтобы заблокировать угрозу;
- проводит ретроспективный анализ системной и сетевой активности процессов и приложений с целью расследования инцидентов.

Опыт мирового уровня

Чтобы противостоять целевым атакам, необходимы большой опыт их выявления и постоянное изучение механизмов их распространения. В 2008 году «Лаборатория Касперского» стала первой IT-компанией, создавшей специальный центр для исследования комплексных угроз. Именно поэтому она раскрыла больше сложных целенаправленных атак (включая ряд самых крупных), чем любой другой поставщик защитных решений. Когда становится известно о новой целенаправленной угрозе, велика вероятность, что ее обнаружил глобальный центр исследований и анализа угроз «Лаборатории Касперского» (GReAT). Полученные в результате анализа угроз знания находят прямое применение в разработке продуктов, а облачная репутационная база Kaspersky Security Network использует аналитические данные, получаемые в режиме реального времени от более чем 80 миллионов узлов по всему миру.

Все эти знания и многолетний опыт «Лаборатория Касперского» готова предложить для защиты вашей IT-инфраструктуры в рамках сервиса Kaspersky Managed Protection.

www.kaspersky.ru

#ИстиннаяБезопасность