Kaspersky®
Threat Intelligence

Применение стратегических данных об угрозах

Сегодня наша жизнь во многом зависит от интернета. Благодаря дешевизне и высокой скорости онлайн-коммуникаций он стал значимым фактором успеха для частных компаний и государственных учреждений. Динамичные и взаимосвязанные среды открывают доступ ко множеству важных возможностей, которые позволяют повышать эффективность коммуникаций, защищать персональные, конфиденциальные и другие данные, контролировать ключевые системы и бизнес-процессы и одновременно поощряют конкуренцию между компаниями. Однако с углублением взаимосвязи между участниками интернет-пространства расширяется и поле для потенциальных атак, и злоумышленники активно выискивают уязвимости на всех уровнях, чтобы воспользоваться ими при первой возможности.

За последние пару лет границы между различными типами угроз и профилями киберпреступников размылись. Вспомним хакерскую группировку The Shadow Brokers, которая выкладывала в открытый доступ сложные эксплойты, якобы разработанные Агентством национальной безопасности США – если бы не она, столь нетривиальный код вряд ли попал бы в руки злоумышленников. Еще один пример – распространение комплексных целенаправленных угроз (APT), ориентированных не на кибершпионаж, а на кражу денег с целью финансирования различных видов преступной деятельности.

Иными словами, мотивация злоумышленников может быть самой разной – от хищения денежных средств до подрыва авторитета конкурентов, кражи персональных данных и мошенничества. Более того, каждая отрасль и каждая организация имеют свои собственные уникальные конфиденциальные данные, уникальный набор приложений, используемых технологий и многое другое. Это приводит к тому, что с каждым днем разновидностей атак и методов их проведения становится все больше.

На фоне постоянно меняющегося ландшафта угроз цифровая трансформация бизнеса, столь необходимая для его роста, становится непростой задачей, и руководству компаний приходится внедрять стратегический подход, подразумевающий непрерывное взвешивание киберрисков и их сопоставление с задачами предприятия.

Четкое понимание таких рисков необходимо для принятия взвешенных решений о запуске новых инициатив, об открытии региональных офисов, инвестировании в технологии и т. д. Также оно помогает разработать проактивные стратегии минимизации убытков и соответствующим образом адаптировать бюджетную и кадровую политики.

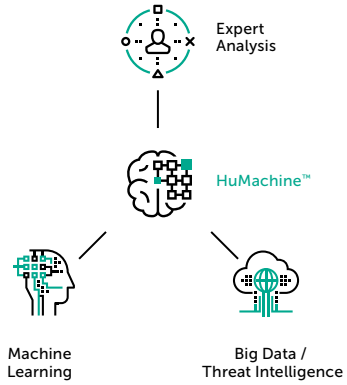
Стратегический анализ угроз предоставляет подробную информацию о распространенных видах атак, о технологиях и методах, используемых злоумышленниками, об их мотивации и характеристиках и помогает ответить на ряд важных вопросов:

- Кто ваши противники? Что им нужно?
- Какие преступные группировки промышляют в вашей отрасли или в вашем регионе?
- Какие векторы атак они используют?
- Как удобнее всего организовать атаку на вашу организацию?
- Какие сведения доступны злоумышленнику, который решит вас атаковать?
- Была ли проведена атака? Или, возможно, преступники только готовятся на вас напасть?
- Как снизить уровень риска вашей компании?

Когда вы вникнете в ответы на эти вопросы и поймете, как они затрагивают ваши критически важные активы, системы и бизнес-процессы, вы сможете осуществить детальный анализ рисков и предоставить руководству четкие и понятные сценарии возможных атак, что, в свою очередь, повлияет на инвестиции в конкретные программы, технологии и кадровую политику. Имея в распоряжении такие аналитические данные, компания может сосредоточиться на уязвимостях, наиболее привлекательных для киберпреступников, чтобы быстро и точно отражать вторжения и свести к минимуму риск успешной атаки.

Предложение «Лаборатории Касперского»:

Тип отчета	Предоставляемые данные	Варианты использования
Аналитические отчеты об APT-угрозах	• Описание тактик и методов, которые используют организаторы кампаний кибершпионажа, направленных на вашу и смежные отрасли • Профили преступников и сведения об используемых ими тактиках, методах и процедурах (Tactics, Techniques and Procedures, TTP) • Сопоставление TTP с MITRE ATT&CK – базой данных о методах преступников, опирающейся на реальные наблюдения	• Анализ профилей преступников в вашей отрасли или регионе и используемых ими методов • Выявление информационных активов и систем, находящихся под угрозой, оценка потенциального ущерба от компрометации данных и расстановка приоритетов • Адаптация стратегии информационной безопасности, планирование и обоснование инвестиций в технологии, пересмотр кадровой политики и программ противодействия потенциальным векторам атак
Аналитические отчеты об угрозах для финансовых организаций	• Описания тактик и методов злоумышленников, атакующих финансовый сектор • Информация об атаках на специфичные инфраструктуры, такие как банкоматы и платежные терминалы • Сведения о конкретных инструментах для атак на финансовые сети, используемых, разрабатываемых и распространяемых киберпреступниками в теневом интернете по всему миру	• Идентификация злоумышленников, атакующих финансовые организации в разных странах, и используемых ими методов • Выявление информационных активов и систем, находящихся под угрозой, оценка потенциального ущерба от компрометации данных и расстановка приоритетов. • Адаптация стратегии информационной безопасности, планирование и обоснование инвестиций в технологии, пересмотр кадровой политики и программ противодействия потенциальным векторам атак
Аналитические отчеты об угрозах для конкретных компаний	• Пассивная идентификация сетевого периметра, доступных сервисов и имеющихся уязвимостей • Персонализированный анализ уязвимостей и возможностей для их эксплуатации • Идентификация, мониторинг и анализ всех активных и неактивных вредоносных программ, нацеленных на вашу организацию • Сведения об утечках информации и идентификационных данных • Информация о фишинговых угрозах, нацеленных на ваши бренды и веб-ресурсы • Отслеживание угроз и активности ботнетов, направленных против клиентов, партнеров и поставщиков компании • Анализ угроз и киберпреступных методов, используемых злоумышленниками в конкретной индустрии	• Обеспечение доступности и грамотного распределения ресурсов для устранения обнаруженных проблем безопасности • Принятие более взвешенных решений по сотрудничеству с партнерами, поставщиками и клиентами для противодействия возможным атакам на цепи поставок • Адаптация политик и контрольных мер для минимизации потенциальных внутренних угроз • Повышение осведомленности сотрудников о кибербезопасности путем разработки персонализированной программы, основанной на данных отчета (например, компрометация корпоративных учётных данных при использовании сторонних сервисов) • Минимизация потенциального репутационного ущерба путем отслеживания незаконного использования брендов компании в целях фишинга • Планирование и обоснование инвестиций в определенные технологии, кадровую политику и программы противодействия актуальным векторам атак



www.kaspersky.ru

#ИстиннаяБезопасность