Анализ ландшафта угроз по индивидуальному заказу

Проблема

Планирование и организация эффективной киберзащиты предприятия, отрасли и страны требует глубокого погружения в специфику – учета локальных особенностей ландшафта угроз, особенностей цепочек поставок, партнерских связей и других аспектов. Успешное реагирование на вызовы информационной безопасности невозможно без знания актуального ландшафта угроз.

Решение

Анализ ландшафта угроз, выполненный по заказу клиента: угрозы, атаки и уязвимости, разбор релевантных инцидентов.

Для кого

Службы информационной безопасности промышленных предприятий, поставщики услуг по управлению кибербезопасностью (MSSP), центры реагирования на компьютерные инциденты (CERT), государственные регуляторы.

Проблематика

Многолетние наблюдения за ландшафтом угроз для систем АСУ подтверждают наличие региональной и отраслевой специфики. Эта специфика отражается в статистике: даже незначительная разница в показателях может указывать на существенные проблемы и вызовы безопасности, требующие анализа.

Различия в производственной культуре и культурных традициях, законодательной базе, моделях и способах организации бизнеса, процессах и процедурах, техническом оснащении и уровне осведомленности персонала об угрозах делают предприятия различных отраслей, регионов и стран по-разному уязвимыми.

Не менее важную роль играет организация цепочек поставок и структура партнерских связей предприятия, отрасли, ведь это еще один из каналов распространения угроз.

Понимание угроз, актуальных для конкретного предприятия, отрасли, страны и региона, критически важно для организации эффективной защиты.

Что мы предлагаем

Два типа отчетов, подготовленных индивидуально с учетом запросов клиента: квартальный и годовой. Отчеты отличаются подходами к сбору и анализу данных и служат разным целям. Первый полезен при решении оперативно-тактических задач, второй – при стратегическом планировании. Оба отчета содержат рекомендации по устранению текущих и потенциальных угроз.

Квартальный отчет: оперативно-тактический взгляд и рекомендации

Отчет содержит краткий обзор 5–10 наиболее актуальных киберугроз за квартал, а также подробную техническую информацию по каждой из них. Он помогает выявлять и предотвращать текущие угрозы для критически важных ресурсов и тем самым обеспечивать непрерывность технологических процессов.

> Сопоставление любой подозрительной активности в системах организации с выводами экспертов Kaspersky ICS CERT упрощает обнаружение угрозы и помогает принять незамедлительные меры.

Представленные в отчете данные также помогают организациям усиливать свои меры кибербезопасности и средства контроля, чтобы эффективно реагировать на современные угрозы и вызовы.

Годовой отчет: стратегический взгляд и рекомендации

Отчет содержит углубленный анализ актуальных угроз и уязвимостей, а также подробные рекомендации по принятию решений по кибербезопасности на всех уровнях. Представленная информация помогает принимать обоснованные стратегические решения в отношении кибербезопасности организации, разрабатывать и внедрять изменения в соответствующие политики, способствующие снижению потенциальных рисков, обеспечению кибербезопасности и непрерывности технологических процессов. Кроме того, она помогает сформировать дорожную карту усиления кибербезопасности и рационально подходить к расходам на ее обеспечение.

Как мы работаем

Процесс

1. Помогаем клиенту определить фокус и период исследования.

2. Собираем данные – с использованием автоматизации и дополнительно (для годового отчета) вручную.

3. Анализируем все данные с привлечением экспертов Kaspersky ICS CERT, специализирующихся на противодействии киберугрозам для промышленных организаций.

4. Предоставляем отчет (в формате PDF) с анализом угроз и рисков, а также подробными рекомендациями.

5. Даем пояснения. Вместе с годовым отчетом клиент получает персональную консультацию экспертов Kaspersky ICS CERT – они объясняют, как максимально информативно интерпретировать результаты исследования, и отвечают на вопросы.

Источники информации

Квартальный отчет

При подготовке отчета мы используем информацию, полученную через Kaspersky Security Network (KSN) с компьютеров АСУ, защищаемых продуктами Kaspersky по всему миру. Это:

- серверы управления и сбора данных (SCADA);
- серверы хранения данных (Historian);
- шлюзы данных (OPC);
- стационарные рабочие станции инженеров и операторов;
- мобильные рабочие станции инженеров и операторов;
- человеко-машинный интерфейс (HMI);
- компьютеры администраторов технологических сетей и разработчиков ПО для систем промышленной автоматизации.

Все полученные данные верифицируются и обогащаются с помощью множества технологий и техник, предполагающих анализ на основе статистических критериев, анализ экспертными системами «Лаборатории Касперского» (песочницы, эвристический анализ, анализ подобия, профилирование поведения и т. д.), проверка аналитиками и проверка по списку разрешенного ПО.

Годовой отчет

В ходе подготовки эксперты Kaspersky ICS CERT собирают и анализируют информацию из различных источников, ориентируясь на специфические требования клиента (география, отрасль, инфраструктура),

Анализ инцидентов и атак проводится с использованием следующих источников и методик:

- собственные источники «Лаборатории Касперского», в частности данные телеметрии, автоматизированный и ручной анализ;
- результаты реагирования на инциденты*, их анализ;
- информация, полученная в рамках сотрудничества с местными и международными проектами, инициативами и группами по обмену информацией в области кибербезопасности, организациями и поставщиками продуктов, пострадавшими в результате инцидентов, а также с компаниями по обеспечению кибербезопасности, независимыми исследователями кибербезопасности, частными лицами и т. д.*
- информация из открытых источников (интернет, публикации), дополненная собственным экспертным анализом Kaspersky ICS CERT.

Анализ уязвимостей проводится с использованием следующих источников и методик:

- информация из открытых источников (веб-сайты поставщиков OT-продуктов, общедоступные базы данных уязвимостей) с последующими проверкой и экспертным анализом;
- результаты собственных исследований уязвимостей «Лаборатории Касперского» и скоординированной работы по ответственному раскрытию уязвимостей.**

Что получает клиент

Итоговый отчет в формате PDF. При заказе годового отчета еще и консультацию экспертов Kaspersky ICS CERT, которые комментируют итоговый документ и отвечают на вопросы.

Выбор формата отчета зависит от потребностей клиента.

- Квартальный отчет помогает определить, какие важные изменения необходимо внести в средства информационной безопасности.

---

* При условии, что это не ограничено внутренними политиками «Лаборатории Касперского», соглашениями о конфиденциальности, условиями контрактов или законодательством.
** При условии подтверждения клиентом законной необходимости получения этой информации (например, в качестве лицензированного пользователя соответствующего продукта), а также в соответствии с Политикой раскрытия уязвимостей конкретного поставщика и условиями контракта.

- Годовой отчет помогает сформировать долгосрочную стратегию кибербезопасности и пересмотреть методы ее обеспечения.

Эти отчеты дополняют друг друга, поэтому многие клиенты предпочитают использовать оба, чтобы получить наиболее полное представление о ландшафте угроз.

Основные различия отчетов

	Квартальный отчет	**Годовой отчет**
Задача	Оперативно-тактическая	Стратегическая
Формат	Обзор 5–10 ключевых угроз с базовым техническим анализом	Подробный обзор релевантных угроз, атак, инцидентов и уязвимостей с экспертным анализом
Ландшафт угроз		
Зафиксированные целенаправленные атаки	Только для заданной инфраструктуры	Все потенциально опасные для инфраструктуры
Обнаруженные APT	Только для заданной инфраструктуры	Все потенциально опасные для инфраструктуры
Фишинг и социальная инженерия	Только для заданной инфраструктуры	Все потенциально опасные для инфраструктуры
Вредоносное ПО, техники, тактики и процедуры злоумышленников	✓	✓
Основные первоначальные источники заражения (векторы атаки)	✓	✓
Индикаторы компрометации	✓	
Методы кибератак		Наиболее опасные из возможных
Инциденты кибербезопасности за отчетный период		Все потенциально значимые / релевантные
Актуализация сведений по ранее произошедшим инцидентам кибербезопасности		По предварительному согласованию
Информация об уязвимостях в OT-продуктах и технологиях		✓

Сбор данных	Автоматизированный	Автоматизированный и ручной
Источники информации		
Собственные данные «Лаборатории Касперского»	✓	✓
Сторонние источники		✓
Открытые источники		✓
Анализ	Автоматизированный и ручной	Автоматизированный и ручной
Рекомендации экспертов Kaspersky ICS CERT	✓	Рекомендации по устранению текущих угроз и предотвращению аналогичных атак в будущем
Результат	Отчет в формате PDF, индикаторы компрометации	Отчет в формате PDF, последующая консультация (онлайн или офлайн – по желанию клиента)
Объем	3–10 страниц	30–150 страниц

Подробное содержание отчетов

Квартальный отчет

1. **Краткое описание ландшафта угроз и статистический анализ** обезличенных данных об угрозах, заблокированных продуктами Kaspersky на компьютерах в заданных регионе и отрасли, за отчетный период.

   - Общая статистика атак: сравнение с глобальными и/или региональными показателями.
   - Анализ источников угроз для OT-инфраструктуры.
   - Динамика ландшафта угроз: сравнение с предыдущим отчетными периодами.

2. **Ландшафт угроз**, представляющий собой анализ 5–10 наиболее опасных и/или распространенных кампаний или типов угроз, затронувших компьютеры OT-инфраструктуры в заданных отраслях и регионах. Каждый тип угроз сопровождается анализом тактик, техник и процедур (TTP) злоумышленников.

- Начальные векторы атаки, используемые для проникновения в инфраструктуру жертвы.
- Разведка и распространение внутри инфраструктуры жертвы (если доступно).
- Взаимодействие с инфраструктурой, контролируемой злоумышленниками: C&C-сервер, хостинг вредоносных программ и т. д. (если применимо).
- Ключевые функции/возможности вредоносного инструментария.
- Цели атаки (при наличии).
- Связь с известными группами (при наличии).
- Потенциальное воздействие: определение последствий для OT/АСУ и безопасности/непрерывности процессов.
- Наиболее распространенные первоначальные источники заражения (векторы атаки).

3. **Индикаторы компрометации** (IoC) для вредоносного инструментария, включая хеши, URL, YARA-правила и STIX.
4. **Рекомендации** по устранению текущих угроз и предотвращению аналогичных атак в будущем.

Годовой отчет

1. **Краткое изложение отчета**, позволяющее быстро оценить риски, связанные с описанными угрозами, и определить необходимые действия для планирования и реализации мер по снижению рисков.
2. **Ландшафт угроз** с учетом специфики и запроса (отрасли, регионы, период времени) клиента. Формируется на основе данных об угрозах, заблокированных продуктами Kaspersky в инфраструктурах, схожих с инфраструктурой клиента и, соответственно, релевантных. Ландшафт угроз описывает:

   - Целенаправленные атаки и APT, которые затронули заданные промышленные инфраструктуры.
   - 5–10 наиболее значимых угроз, обнаруженных в АСУ ТП, и их потенциальное воздействие, анализ тактик, техник и процедур (TTP), рекомендуемые меры по устранению последствий.
   - Наиболее распространенные первоначальные источники заражения (векторы атак).
   - Другие факторы, которые повлияли на ландшафт угроз для указанных инфраструктур.

> Если выявленная угроза требует срочного реагирования со стороны клиента, мы незамедлительно сообщаем ему об этом и предоставляем всю имеющуюся на тот момент информацию.

3. **Изучение методов кибератак**, направленных на заданные цели, отрасли или регионы, в том числе методов, которые используются или могут быть использованы при атаках на заданные OT-инфраструктуры.
4. **Обзор киберинцидентов**, которые затронули промышленную инфраструктуру (как ИТ-, так и OT-системы) в отчетном периоде. Обзор также может включать новую информацию о ранее произошедших киберинцидентах, если стали известны новые важные детали. Подробная информация об инцидентах включает:

   - Дату, время и место инцидента.
   - Обзор затронутых инфраструктур и ИТ-систем.
   - Описание инцидента.
   - Анализ тактик, техник и процедур (TTP), используемых злоумышленниками.
   - Информация о состоянии кибербезопасности затронутой инфраструктуры на момент атаки/инцидента (оценка подверженности инфраструктуры киберугрозам и действующих мер кибербезопасности).
   - Общий обзор, мотивы и намерения злоумышленников.
   - Уровень сложности атаки и оценка возможностей и квалификации злоумышленников.
   - Проблемные области, выявленные в результате инцидента, и рекомендуемые меры для защиты указанных инфраструктур от подобных ситуаций в будущем.

5. Обзор нескольких ранее произошедших киберинцидентов по выбору клиента, включающий ту же информацию, что и в п. 4.

6. Подробная информация об уязвимостях в OT-продуктах и технологиях, используемых в заданных инфраструктурах (в соответствии с перечнем продуктов, выбранных клиентом), которые были выявлены и/или устранены разработчиками в течение отчетного периода.

Информация об уязвимостях представляется в формате бюллетеня об уязвимости и обычно содержит:

- Тип уязвимости.
- Краткое описание.
- Ссылку на рекомендации по устранению уязвимости, предоставленные поставщиком.
- Ссылку на отчет об уязвимости CVE.
- Список уязвимых продуктов (линеек, версий), согласно данным «Лаборатории Касперского».
- Информацию о доступности эксплойта в общедоступных и/или приватных источниках.
- Степень критичности (в соответствии с CVSS v3.0 и другими показателями, если применимо).

- Признаки эксплуатации уязвимости (или аналогичной уязвимости в том же или аналогичных продуктах) в реальных кибератаках.
- Информацию о результатах эксплуатации уязвимостей в отработке Red Team и Blue Team, соревнованиях по спортивному хакингу CTF, тестах защитных продуктов АСУ и др. (если таковая имеется).
- IDS-правила (если таковые имеются) для выявления попыток эксплуатации уязвимостей.
- Меры по снижению влияния уязвимостей, рекомендованные Kaspersky ICS CERT.

Запросить консультацию специалиста

Рекомендуем дополнительно

- Поток данных об угрозах для систем промышленной автоматизации
- Kaspersky Threat Intelligence: информация об уязвимостях и угрозах для АСУ ТП
- Аналитика известных уязвимостей АСУ для принятия критически важных решений в части информационной безопасности
- Расследование киберинцидентов на промышленных предприятиях
- Цифровая криминалистика и расследование инцидентов в АСУ ТП. Тренинг
- Разработка руководства и обучение реагированию на инциденты

Запросить консультацию специалиста

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com