Group-IB

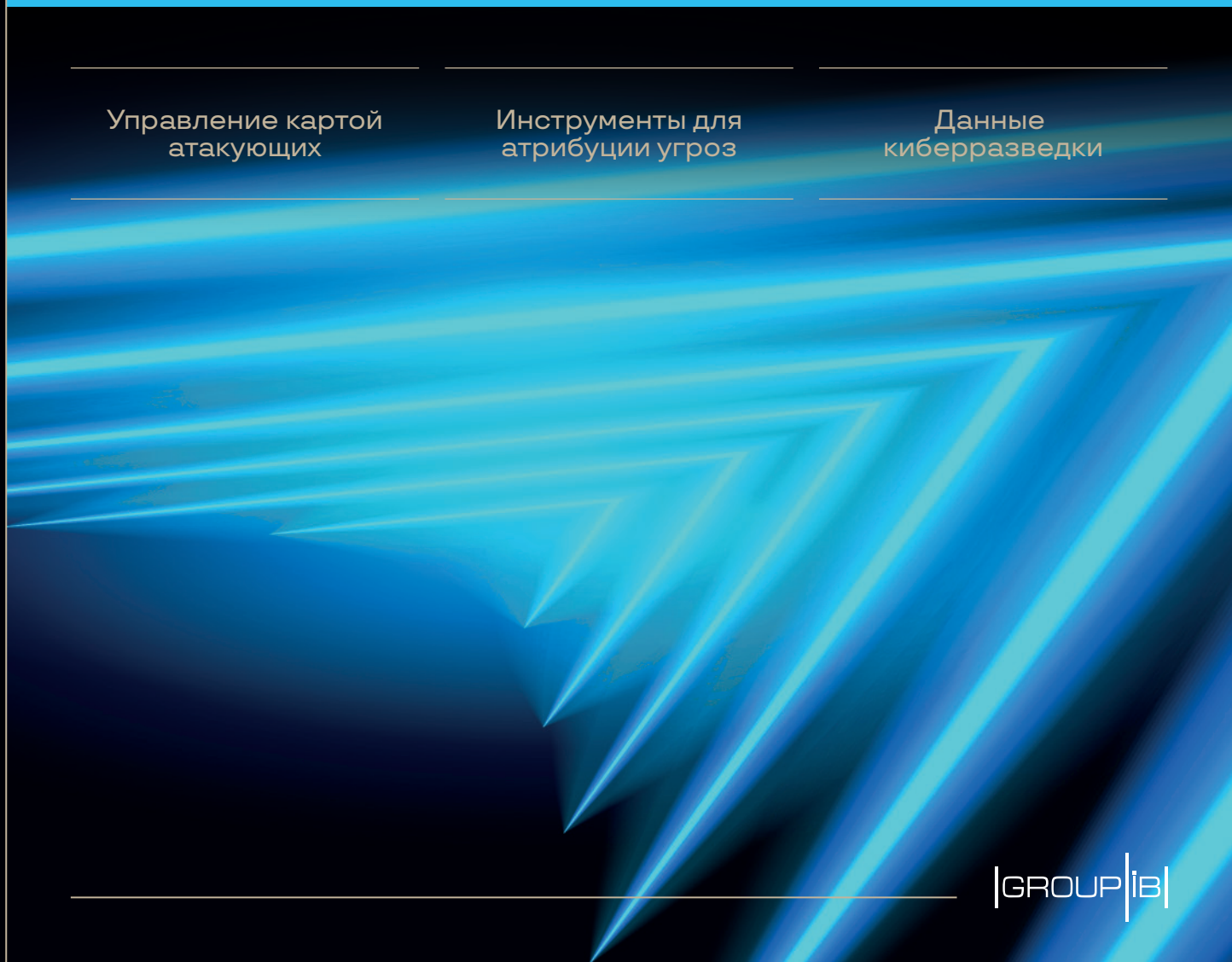
THREAT INTELLIGENCE

Атрибуция угроз, основанная на данных киберразведки

Управление картой атакующих

Инструменты для атрибуции угроз

Данные киберразведки



GROUP IB

Эволюция подхода к выявлению угроз

Без знаний о том, кто представляет для вас угрозу, невозможно защититься от хорошо подготовленных атак.
Поэтому современную систему защиты необходимо строить не на управлении индикаторами, которые в большинстве случаев нерелевантны для вашей организации, а на информации о том, кто стоит за каждой конкретной атакой.

Threat Intelligence

От управления индикаторами к управлению атакующими

Threat Intelligence — решение для исследования и управления атакующими и угрозами, релевантными для определенной организации и отрасли.

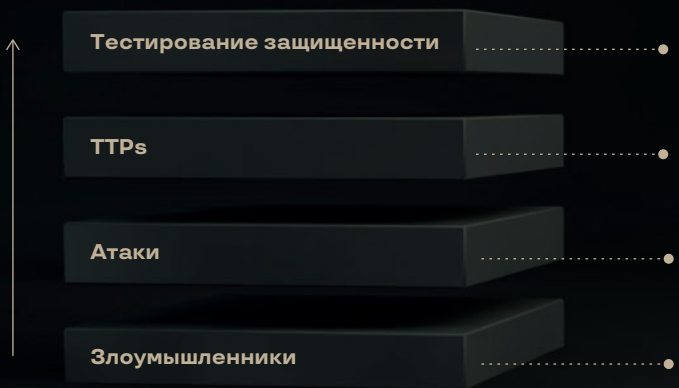
Отвечает на ключевые вопросы:

- Кого и что детектируют ваши системы безопасности?
- Кто еще представляет для вас угрозу?
- Как и с помощью каких инструментов вас будут атаковать?
- Выдержит ли ваша система безопасности кибератаку?
- Какие меры безопасности необходимо применить для адекватной работы?

Широкий спектр возможностей позволяет:

1. Атрибутировать угрозы, с которыми сталкивается компания
2. Изучать релевантные для организации и отрасли атаки
3. Исследовать тактику и изменяющиеся инструменты атакующих
4. Тестировать и улучшать существующую систему безопасности для защиты от реальных угроз

Новый подход



- **Тестирование защищенности** — Тестирование среды командой Red team против тактик, методов и процедур релевантных для вас преступных группировок.
- **TTPs** — Глубокий анализ тактических приемов, методов и процедур злоумышленников, в соответствии с матрицей MITRE ATT&CK.
- **Атаки** — Таймлайн релевантных атак, целенаправленное исследование угроз и хантинг.
- **Злоумышленники** — Матрица злоумышленников, атакующих вашу организацию, индустрию, партнеров, о которых важно знать.

Как работает Threat Intelligence

1 Обнаружение угроз

- Ваши системы безопасности постоянно детектируют различные угрозы.
- Threat Intelligence позволяет увидеть то, что пропустили текущие решения.
- Все обнаруженные угрозы проходят процесс атрибуции.

2 Атрибуция и обогащение

- Сырые данные об интернет-серверах и вредоносных программах поступают в систему.
- Благодаря корреляции сырых данных с информацией из Threat Intelligence, система сопоставляет атаки с известными угрозами.
- Инструменты для исследования вредоносных программ и поиска неявных связей позволяют атрибутировать неизвестные угрозы.
- Обогащенные индикаторы загружаются в системы безопасности для более эффективного детектирования угроз.

3 Ранжирование угроз

- Атакующие ранжируются по релевантности и критичности.
- По этим атакующим выстраивается процесс хантинга.
- Данные об атакующих трансформируются в их TTPs для будущих проверок.

4 Тестирование защищенности

- Новые и релевантные техники используются для тестирования системы безопасности.
- Тестирование проводится локальной командой или Group-IB Red Team.

Ключевые преимущества

- Встроенные инструменты для атрибуции
- Интеграция с внедренными решениями по безопасности с поддержкой STIX/TAXII, API/JSON
- Глубокая аналитика данных
- Персонализированная и максимально релевантная информация Threat Intelligence
- Совместная работа с экспертами из разных областей
- Автоматизация процессов Threat Hunting, Incident Response и Malware Research

Group-IB входит в число лучших мировых поставщиков решений класса Threat Intelligence по версии Gartner, IDC, Forrester, Cyber Defense Magazine и SC Media.

group-ib.ru ↗

Group-IB один из ведущих мировых разработчиков решений для детектирования и реагирования на кибератаки, предотвращения мошенничества и защиты интеллектуальной собственности в сети

Group-IB входит в число лучших мировых поставщиков решения класса Threat Intelligence по версии Gartner, IDC, Forrester, SC Media и Cyber Defenses Magazine.

Эксперты Group-IB проводили тренинги по кибербезопасности для специалистов Europol, INTERPOL, правоохранительных органов, корпоративных команд и преподавателей университетов в Европе и Азии.

INTERPOL EUROPOL

Официальный партнер

16 лет	60 000+	1 000+	360+
практического опыта	часов опыта реагирования	расследований по всему миру	специалистов и разработчиков

→

Узнайте больше о возможностях Threat Intelligence

group-ib.ru

→

Свяжитесь с нами, чтобы провести тест-драйв Threat Intelligence

info@group-ib.com

→

Познакомтесь с Group-IB

group-ib.ru
facebook.com/GroupIB

Сервисы Group-IB

Укрепите кибербезопасность с помощью специалистов с практическим опытом реагирования и расследования сложных атак, использующих одну из самых продвинутых систем слежения за киберугрозами в мире.

Аудит и оценка рисков

- Тестирование на проникновение
- Анализ исходного кода
- Выявление следов компрометации сети
- Киберобучения в формате Red Teaming
- Проверка готовности к реагированию на инциденты
- Оценка соответствия

Обучающие программмы

- Реагирование на инциденты
- Анализ вредоносного кода
- Проактивный поиск угроз

Threat Hunting и реагирование

- 24/7 Центр реагирования CERT-GIB
- Проактивный хантинг угроз
- Выездное реагирование на сложные кибератаки
- Реагирование на инциденты «по подписке»

Криминалистика и расследования

- Компьютерная криминалистика
- Расследование финансовых и корпоративных киберпреступлений, атак на объекты КИИ