АССОЦИАЦИЯ БАНКОВ РОССИИ

BI.ZONE
Cybersecurity

Платформа обмена данными об актуальных киберугрозах

Версия 2.0

АССОЦИАЦИЯ БАНКОВ РОССИИ

BI.ZONE
Cybersecurity

Оглавление

Введение

В условиях четвертой промышленной революции кибератаки становятся одним из основных глобальных рисков. По данным Всемирного экономического форума, общие потери от кибератак в 2017 году составили $1 трлн — при текущем развитии событий эта цифра восьмикратно возрастет в ближайшие годы.

Компании и целые страны не успевают технологически адаптироваться к новым киберугрозам. Нехватка актуальной информации, отсутствие единой доверенной платформы для обмена ею значительно затрудняют процесс реагирования на инциденты и сокращают возможности минимизации потенциального ущерба от атаки. Участники рынка вынуждены рассчитывать только на себя, в то время как кибергруппировки с разветвленной сетью структур на разных континентах оперативно реагируют на появление новых уязвимостей и все время оказываются на шаг впереди.

Наибольший удар приходится на кредитно-финансовый сектор: как и обычные злоумышленники, киберпреступники в первую очередь заинтересованы в деньгах. Если раньше вектор атак был в основном направлен на клиентов, теперь группировки все чаще целятся непосредственно на финансовые организации. Взлом банкоматов, атаки на системы дистанционного банковского обслуживания фишинговые рассылки становятся все изощренней, а между обнаружением уязвимости и ее использованием проходит порой не более нескольких часов.

Чтобы противостоять киберпреступности, финансовому сектору необходимы открытый диалог и постоянный обмен информацией. Беспрецедентные условия для этого созданы в рамках Ассоциации банков России, объединяющей более 450 участников рынка. Для практической реализации данной уникальной возможности компания BI.ZONE разработала технологическое решение — платформу для доверенного обмена данными о киберугрозах.

Пилотный проект помогает защищать инфраструктуру российской банковской отрасли с 18 июня 2018 года. Внедрение Платформы уже позволило Участникам обмена избежать многомиллионных потерь за счет своевременного получения актуальной информации.

На основе обратной связи от членов проекта Платформа постоянно обновляется — предоставляет Участникам больше возможностей и гибко подстраивается под их нужды. Платформа 2.0, где реализовано множество предложенных идей, уже готова для подключения новых пользователей. Расширение числа Участников из кредитно-финансового сектора и интенсификация доверенного обмена проверенными и релевантными данными позволит сделать большой шаг вперед на пути к повышению уровня защищенности отрасли.

Описание платформы

Платформа обмена данными — сервис доверенного обмена информацией об актуальных киберугрозах внутри банковской отрасли, включающий обширные базы индикаторов компрометации. Платформа не просто агрегирует данные и предоставляет возможность поиска по ним — это полноценная система, которая позволяет Участникам обмена автоматически и в режиме реального времени:

- получать верифицированную и релевантную для них информацию о киберугрозах;
- безопасно делиться собственной информацией с другими Участниками.

Дополнительным преимуществом сервиса является его механизм комплексной обработки предоставленной информации: Платформа анализирует, группирует, приводит в единый формат и обогащает данные, проверяет их достоверность и учитывает уровень доверия источнику. В результате Участники обмена получают доступ к наиболее актуальной, верифицированной информации с соответствующим контекстом.

С помощью специальных инструментов Платформы Участникам удобно:

- расширять потенциал средств защиты и эффективно настраивать правила корреляции SIEM-систем;
- отбирать наиболее релевантные данные, чтобы регулярно отслеживать приоритетные угрозы;
- визуализировать связи между объектами для успешного расследования инцидентов;
- наглядно представлять тренды в актуальных методах и направлениях атак на отрасль и обоснованно формировать стратегию противодействия.

Внедрение Платформы в ежедневную практику специалистов по кибербезопасности позволяет повысить надежность средств защиты и эффективность расследований, скорость реагирования и устранения последствий инцидентов, а также снизить ущерб от действий злоумышленников.

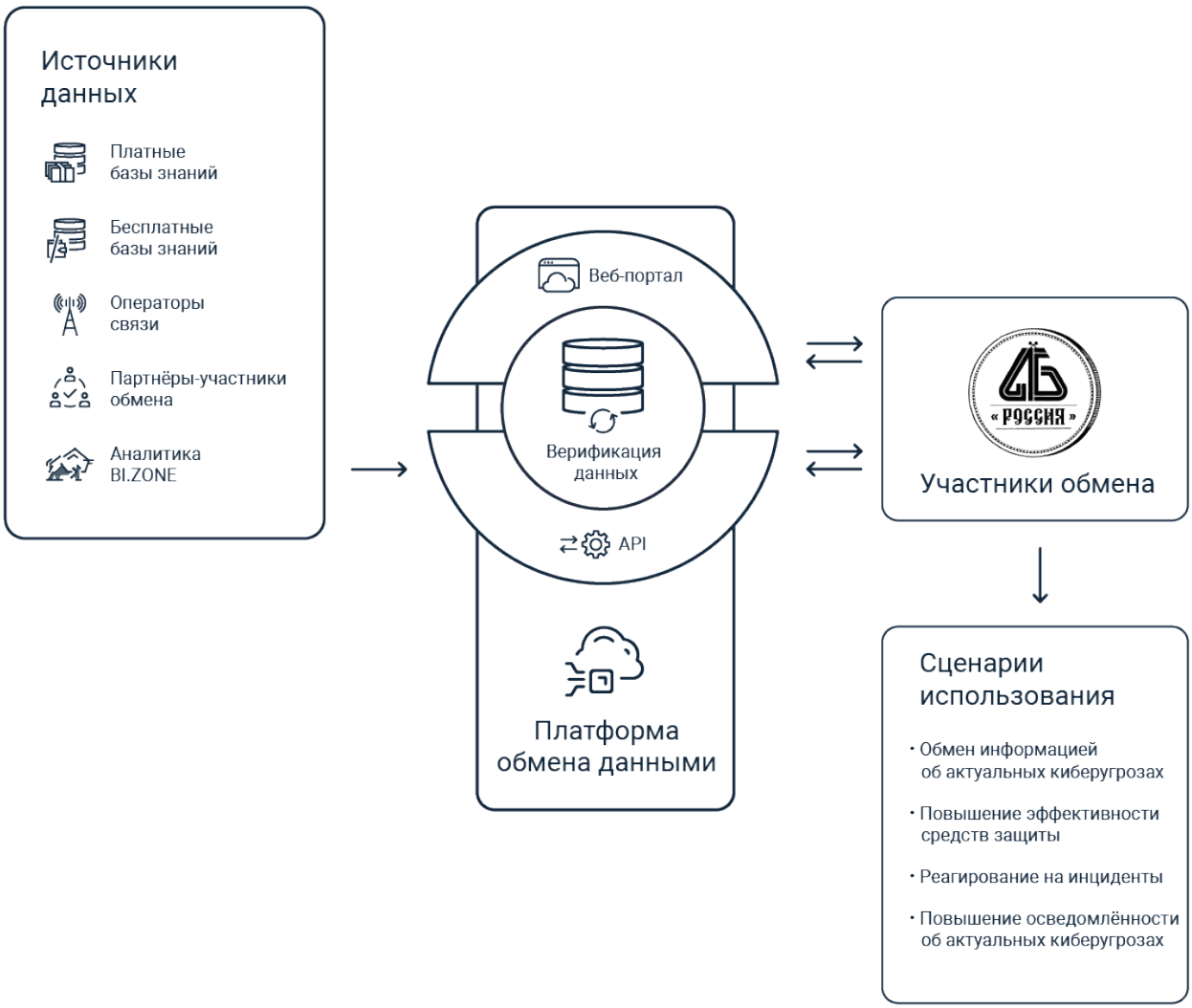

Рис. 1. Платформа обмена данными

Сценарии использования Платформы

Платформа эффективно действует как центр накопления и обмена TI-информацией. При интеграции Платформы со средствами защиты она позволяет повысить эффективность выявления потенциальных киберугроз, оперативно реагировать на инциденты и выстраивать надежную стратегию противодействия. Обогащение Платформы опытом Участников обмена поможет раскрыть и усилить ее потенциал как мощного инструмента в арсенале специалистов по кибербезопасности финансового сектора и страны в целом.

Обмен информацией об актуальных киберугрозах

Обычно лишь малая часть информации о киберпреступлениях попадает в открытый доступ. В этих условиях Платформа становится не только удобной базой знаний, но и уникальным инструментом для доверенного обмена новой важной информацией между представителями банковской отрасли.

- **Актуальный опыт Участников обмена**. Платформа позволяет каждому Участнику как получать, так и загружать информацию об инцидентах, вредоносных рассылках, обнаруженных индикаторах компрометации.

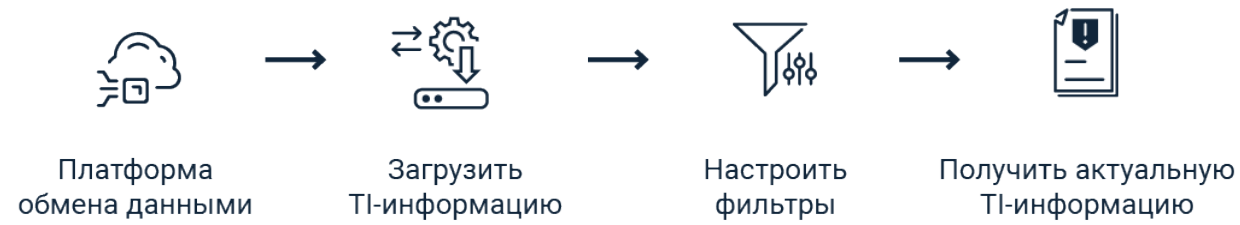

Рис. 2. Получение актуальной TI-информации

- **Агрегация и верификация загруженных данных**. Платформа автоматически обрабатывает данные от источников TI-информации: приводит к единому формату и исключает непроверенные или противоречивые сведения.

- **Оценка уровня доверия источникам TI-информации.** Платформа реализует механизм проверки данных, загружаемых источниками TI-информации, по результатам анализа источники ранжируются по уровню доверия. Рейтинг может быть пересчитан позднее — например, если качество данных изменится.
- **Автоматический и ручной режимы обмена**. Платформа оптимизирована для автоматического обмена данными (через REST API), но ее можно использовать для самостоятельного поиска и загрузки индикаторов компрометации через веб-портал.

Повышение эффективности средств защиты

Загрузка и оперативное обновление TI-информации расширяет потенциал средств защиты Участника обмена. Благодаря актуальным данным о киберугрозах средства защиты быстрее обнаруживают компрометацию инфраструктуры, надежнее предотвращают вторжения.

- **Интеграция со средствами защиты через API**. Платформа включает ряд стандартных модулей для автоматической интеграции со средствами защиты и предусматривает возможность создания новых модулей по запросам Участников. Если необходимо индивидуальное решение, специалисты поддержки помогут разработать собственный модуль интеграции через REST API.
- **Группировка индикаторов компрометации для последующего построения цепочек корреляции в SIEM-системах**. Платформа организует добавленные в нее данные, сохраняя детали контекста и связи между объектами. Модель данных Платформы позволяет настраивать соответствующие правила корреляции SIEM-систем, снижая количество ложных срабатываний.

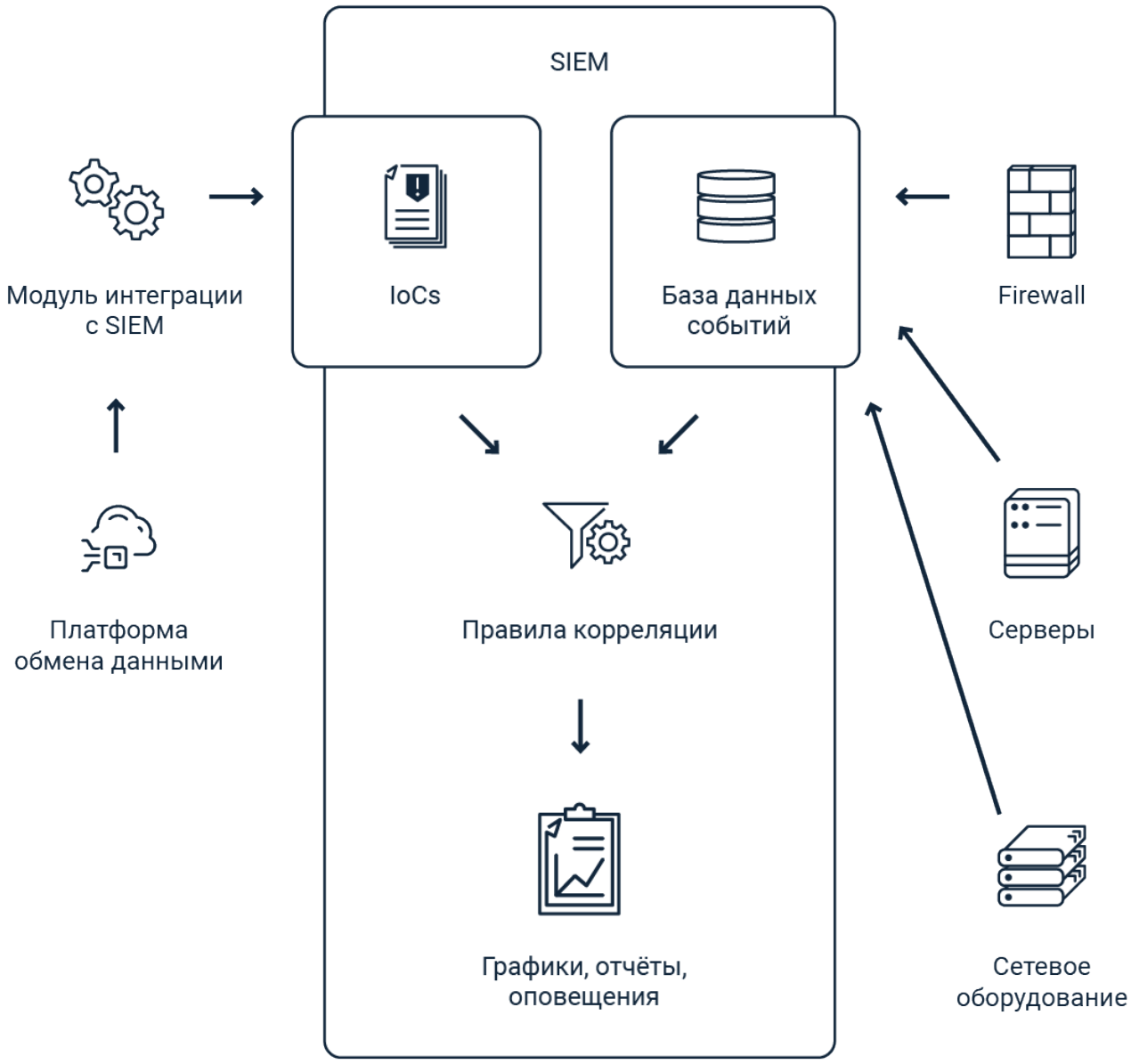

Рис. 3. Пример интеграции с SIEM-системой

Использование данных и возможностей платформы при реагировании на инциденты

Платформа — удобный инструмент для специалиста по расследованию инцидентов. База точной, подробной и актуальной информации об индикаторах компрометации и известных уязвимостях с расширенным поиском помогает повысить скорость и эффективность реагирования на инциденты, а за счет этого минимизировать возможные потери от атак.

- **Визуализация связи между объектами.** Платформа отображает в виде графов связанные индикаторы компрометации и контекстную информацию, нужную для формулирования гипотез и определения следующего шага расследования.
- **Рекомендации по предотвращению и устранению последствий инцидентов.** При расследовании инцидентов через веб-портал Платформа не только обеспечивает доступ к исчерпывающей информации об угрозах, но и позволяет получить рекомендации по противодействию угрозам на основе собранных данных.

Рис. 4. Роль Платформы в расследовании инцидентов

Повышение осведомленности об актуальных киберугрозах

Модели угроз, характерные типы атак и цели киберпреступников различаются по секторам экономики. Платформа отслеживает и агрегирует TI-информацию, релевантную конкретной отрасли, что помогает организациям видеть цифровой контекст и принимать более взвешенные решения о необходимых мерах безопасности.

- **Настройка фильтра по релевантным угрозам**. Платформа позволяет фильтровать TI-информацию по отрасли, конкретному типу угрозы, определенному уровню опасности и так далее. Когда в Платформе появляются новые данные об угрозах, подходящих под заданные Участником фильтры, она оперативно извещает об этом.
- **Создание собственной базы знаний по угрозам**. При локальной установке Платформы Участник может составить внутреннюю базу знаний, которая поддерживает большинство возможностей облачного сервиса, сохраняет возможность синхронизации с ним, а также предоставляет дополнительную функциональность.
- **Визуализация трендов по угрозам**. Встроенные инструменты Платформы наглядно представляют возникновение и угасание трендов в атаках, чтобы Участникам было удобнее учитывать актуальные угрозы при планировании стратегии кибербезопасности.
- **Ретроспективный поиск по архивному хранилищу**. Платформа хранит историю изменений по всей записанной в нее TI-информации — данные по эволюции и взаимосвязанности угроз помогают не только расследовать инциденты, но и изучать потенциал и актуальность угроз при планировании мер безопасности.

Рис. 5. Средства повышения осведомленности об актуальных киберугрозах

Техническое описание

Основная функциональность Платформы

Подключение любых TI-источников

К Платформе можно подключить любой TI-источник. С технической стороны процесс выглядит следующим образом:

1. Сопоставляются модели данных TI-источника и Платформы.
2. Создается модуль для загрузки данных из TI-источника в Платформу.
3. Информация из TI-источника проходит тестирование. К тестированию могут подключаться сами Участники обмена.
4. По результатам тестирования принимается решение, использовать ли данные из TI-источника — и если да, то нужно ли их обогащать. При положительном решении данные из TI-источника становятся доступными для загрузки из Платформы.

Механизмы оценки уровня доверия TI-источникам

Платформа позволяет назначить уровень доверия каждому TI-источнику.

- Уровень доверия назначается по результатам тестирования TI-источника.
- Уровень доверия может изменяться в зависимости от качества информации и отзывов Участников обмена.

Нормализация, агрегация и дедупликация TI-информации

Платформа приводит все загружаемые данные к единому формату, сохраняя максимальное количество контекста.

Платформа решает проблему наличия дубликатов: при загрузке уже существующего в базе индикатора компрометации она автоматически обновляет его данные и не позволяет создать копию.

Платформа систематизирует информацию из TI-источников по индикаторам: если один и тот же индикатор пришел от нескольких источников, Платформа сохранит все сведения в рамках одной записи и отметит, какая информация из какого источника поступила.

Верификация индикаторов компрометации

Платформа проверяет индикаторы компрометации в несколько этапов.

- Все индикаторы проходят предварительную проверку при загрузке. Если индикатор не проходит верификацию, он не загружается в Платформу.
- После загрузки индикаторы периодически проверяются — как в автоматическом режиме, так и вручную аналитиками провайдера Платформы. Если индикатор не проходит периодическую проверку, он изменяется или удаляется из базы.

Обогащение индикаторов компрометации

Платформа поддерживает настройку механизма обогащения информации. Дополнительный контекст к индикаторам компрометации добавляется с помощью запросов к открытым и платным источникам.

Группировка индикаторов, сохранение их связности и контекста

Платформа сохраняет связи между индикаторами компрометации и позволяет группировать их — например, в рамках инцидентов или атак.

Отследить связи можно и у сложных объектов — инцидентов, кибергруппировок, уязвимостей и так далее.

Категоризация и тегирование информации

Вся TI-информация в платформе разбивается на категории, а при необходимости дополнительно тегируется.

- Один объект можно отнести к нескольким категориям (например, угроза для мобильных устройств может попасть одновременно в категории Malware и Mobile).

- Категории определены провайдером Платформы, но список расширяется при необходимости.
- Теги выставляются на основе информации от TI-источника, предоставившего соответствующие данные.

Динамическая актуализация с возможностью устаревания информации

Платформа поддерживает базу индикаторов компрометации в актуальном состоянии с помощью механизмов устаревания и обновления.

- Механизм устаревания позволяет удалять неактуальные индикаторы, а механизм обновления – сохранять актуальные.
- Актуальность каждого индикатора определяется его временем жизни и частотой обновления.

Архивное хранилище

Все удаленные объекты Платформы помещаются в архивное хранилище. Здесь сохраняется не только сам удаленный объект, но и объекты, связанные с ним на момент удаления. Такой срез позволяет в любой момент получить информацию по последнему актуальному состоянию группы или индикатора компрометации.

Механизм обратной связи

Платформа позволяет оставлять обратную связь по использованным индикаторам компрометации: Участники обмена могут выставить им положительный (like) и отрицательный (dislike) рейтинг.

Локальная инсталляция с дополнительными опциями

Платформу можно установить в инфраструктуре Участника обмена. Локальный экземпляр удобен для формирования собственной базы знаний по угрозам.

В отличие от облачного сервиса, локальный экземпляр Платформы позволяет:

- подключать дополнительные TI-источники;
- самостоятельно назначать рейтинги источников;

- заводить собственные индикаторы компрометации, информацию об инцидентах, уязвимостях и т. д.;
- использовать дополнительные сервисы обогащения TI-информации;
- настраивать индивидуальные механизмы фильтрации;
- управлять пользователями и их правами (т. е. определять, какая информация кому доступна, кто может ее получать или загружать, и т. д.);
- настраивать по собственным параметрам динамическую приоритизацию угроз.

Локальный экземпляр Платформы поддерживают синхронизацию с другими локальными экземплярами, установленными у Участника, а также с облачным сервисом — в одностороннем и двустороннем режиме.

Обширные возможности для интеграции

При работе как с облачным сервисом, так и с локальной инсталляцией Платформы через интерфейс REST API Участники обмена могут:

- получать, изменять и загружать TI-информацию;
- гибко настраивать фильтрацию и поиск;
- давать обратную связь;
- обогащать информацию;
- выполнять поиск по архивному хранилищу;
- подключать новые TI-источники (только в локальном экземпляре);
- управлять пользователями и ролями — наборами прав для групп пользователей (только в локальном экземпляре).

Веб-портал с возможностью визуализации и работы с TI-информацией

При работе как с облачным сервисом, так и с локальной инсталляцией Платформы через веб-интерфейс Участники обмена могут:

- искать и просматривать любую доступную пользователю TI-информацию;
- гибко настраивать фильтрацию и поиск;

- давать обратную связь;
- выполнять поиск по архивному хранилищу;
- управлять пользователями и ролями — наборами прав для групп пользователей (только в локальном экземпляре).

Помимо этого, веб-портал имеет Dashboard для просмотра актуальных трендов и статистики по TI-информации, графовый интерфейс для расследования инцидентов и визуализации связей между объектами, а также содержит исчерпывающую документацию по самой Платформе и интеграции с ней.

Модель данных

TI-информация в Платформе разделена на два типа:

- **Индикаторы компрометации** — объекты, которые описывают характерные признаки компрометации IT-инфраструктуры, а также включают контекстную информацию и релевантные метаданные потенциальной атаки.
- **Группы** — информация по ВПО, злоумышленникам, инцидентам и т. д.

Группы используются для построения целостной картины (например, по конкретным угрозам, инцидентам, атакам) путем объединения индикаторов и других групп между собой.

Индикаторы компрометации

Платформа позволяет работать с индикаторами компрометации, указанными в табл. 1.

Табл. 1. Индикаторы компрометации, поддерживаемые Платформой

№	Индикатор	Описание
1	Bank card	Банковская карта *Пример: номер банковской карты, используемой злоумышленниками для мошенничества*
2	Certificate	Цифровой сертификат X.509 *Пример: поддельный SSL-сертификат*
3	Device	Информация об устройстве *Пример: IMEI скомпрометированного мобильного телефона*

4	Email	Сообщение электронной почты *Пример: шаблон сообщения из фишинговой рассылки*
5	File	Информация о вредоносном файле *Пример: SHA-256 хеш ВПО*
6	FQDN	Домен *Пример: скомпрометированный домен, используемый для рассылки ВПО*
7	IPv4/IPv6	IP-адрес *Пример: IP-адрес сервера управления ВПО*
8	Message	Шаблон сообщения *Пример: SMS-сообщение, содержащее ссылку на ВПО*
9	Process	Процесс в операционной системе *Пример: процесс ВПО, маскирующийся под легитимный процесс операционной системы*
10	Registry key	Ключ реестра *Пример: ключ реестра, используемый ВПО*

11	Subscriber	Абонент *Пример: зараженный или потенциально зараженный абонент мобильного оператора*
12	URL	URL *Пример: фишинговый URL*

Группы

Платформа позволяет работать с группами, указанными в табл. 2.

Табл. 2. Группы, поддерживаемые Платформой

№	Группа	Описание
1	Adversary	Злоумышленник или преступная группировка, характерные методы и инструменты проведения атак, целевой сектор и т. д.
2	Attack	Последовательность / методология проведения конкретной атаки, использованные инструменты / методы и рекомендуемые способы противодействия
3	General	Группа, предназначенная для отображения связей между индикаторами компрометации
4	Incident	Описание инцидента Помимо общего описания, может включать в себя: • время выявления инцидента; • время, затраченное на устранение; • связанные индикаторы компрометации; • методы и средства, использованные злоумышленником; • последствия и возможные меры по предотвращению / сокращению потерь.

5	Malware	Возможности, поведение и особенности конкретного ВПО Описание может касаться семейства ВПО или конкретной модификации
6	Signature	Правило или сигнатура Содержит правило, его описание и назначение (например, что оно позволяет найти)
7	Vulnerability	Уязвимость, описание уязвимости Может содержать: • информацию относительно источника, места и времени публикации; • ссылки на системы классификации уязвимостей (например, CVE), скоринговые системы (например, CVSS); • рекомендации по предотвращению эксплуатации уязвимости; • другую дополнительную информацию.

Планы

Вектором эволюции Платформы обмена данными о киберугрозах **в краткосрочной перспективе** выбрано улучшение индивидуального опыта взаимодействия с сервисом. Потенциал Платформы будет усилен новыми возможностями по автоматической и персонализированной приоритизации угроз, точечному реагированию на наиболее важную для Участников обмена TI-информацию. Также в ближайшем обновлении Платформы — возможность определить глубину вторжения с помощью представления индикаторов в формате kill chain, отследить тренды для оценки потенциальных рисков в масштабе отрасли, региона.

- **Динамическая приоритизация угроз.** Платформа предложит готовые правила расчёта уровня угрозы, а также позволит создавать собственные правила в рамках локальной инсталляции.
- **Поиск дополнительной TI-информации.** Если необходимых сведений не окажется в Платформе, она обратится к расширенному поиску по внешним открытым и закрытым источникам. Также Платформа сможет запомнить запрос специалиста и прислать уведомление, когда нужная информация появится в базе знаний.
- **Группировка индикаторов компрометации в рамках атаки (kill chain).** Наглядная атрибуция индикаторов к различным этапам последовательной атаки позволит визуализировать цепочку вторжения для удобного расследования инцидентов, повышать приоритет инцидента при обнаружении следующего индикатора из той же цепочки.
- **Поддержка макрокорреляций.** На основе обратной связи от Участников Платформа сможет отследить тенденции в изменении типов атак и техник, используемых злоумышленниками, а также предложить превентивные меры защиты.

В долгосрочной перспективе Платформа будет усилена инструментами, которые позволят ей войти в арсенал директоров, руководителей отделов и должностных лиц, отвечающих за кибербезопасность: она поможет оценить и обосновать финансовые риски, а также, выявив на основе паттернов действия

кибергруппировок, вовремя усилить защитные меры при начале крупных атак на отрасль.

- **Выстраивание инфраструктуры злоумышленников.** Платформу планируется развить до мощного аналитического центра — инструменты сервиса позволят вычислять действия конкретных группировок, целенаправленно атакующих отрасль. Платформа поможет понять вектор деятельности таких киберпреступников и оперативно приоритизировать риски, адаптировать стратегию кибербезопасности компании к изменяющейся цифровой среде.
- **Оценка финансовых рисков.** При локальной инсталляции комплексная обработка актуальной TI-информации и данных об инфраструктуре организации позволит достоверно определять наиболее приоритетные области для модернизации корпоративных средств защиты и обоснованно планировать бюджет на кибербезопасность.

Используемые сокращения

Сокращение	Определение
ВПО	Вредоносное программное обеспечение
API	Application Programming Interface
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
FQDN	Fully Qualified Domain Name
IMEI	International Mobile Equipment Identity
IoC	Indicator of Compromise
SIEM	Security Information and Event Management
SMS	Short Message Service
SSL	Secure Sockets Layer
TI	Threat Intelligence
TLP	Traffic Light Protocol
URL	Uniform Resource Locator