Полина ПЕРЛОВА
менеджер по продуктовому маркетингу R-Vision

Валерий ГОРБАЧЁВ
руководитель направления внедрения СЗИ АО «ДиалогНаука»

ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ ДАННЫМИ THREAT INTELLIGENCE

ОПЫТ ВЫБОРА ПЛАТФОРМЫ ДЛЯ АНАЛИЗА УГРОЗ

Информационная безопасность уже давно сводится не только к выстраиванию процесса реагирования на уже произошедшие инциденты: современный подход к ИБ включает в себя как реактивные, так и проактивные меры, а умение предугадать и распознать атаку по самым ранним признакам становится одним из ключевых факторов защиты бизнеса от киберугроз. Одним из инструментов, позволяющим снизить вероятность возникновения инцидентов, а также получить дополнительный контекст для их расследования, является использование данных Threat Intelligence (TI).

ЧТО ТАКОЕ THREAT INTELLIGENCE И ДЛЯ ЧЕГО НУЖНА КИБЕРРАЗВЕДКА?

Между понятиями TI и киберразведки часто ставят знак равенства, однако следует разделять эти термины на совокупность данных и собственно процесс их получения и использования. Если кратко, TI — это любые знания, позволяющие сделать выводы об актуальных угрозах в отношении конкретной организации или целой отрасли, спланировать защитные меры, а также повысить эффективность обнаружения и реагирования на них. Наряду с этим процесс получения данных TI напоминает классическую разведку: ИБ-специалисты собирают информацию, обрабатывают её, ищут недостающий контекст, преобразовывают всё в единый вид и передают лицу, принимающему решения, для оценки рисков и принятия защитных мер. При этом качество данных TI напрямую влияет на скорость и эффективность решений.

Проактивный подход к защите особенно актуален для банковской сферы, где утечки конфиденциальных данных и денежных средств не только могут ударить по репутации организации, но и напрямую влияют на деятельность остальных участников финансового рынка. Одним из инициаторов такого подхода выступил ЦБ РФ, сформировавший в своей структуре специальный Центр мониторинга и реагирования на компьютерные атаки — ФинЦЕРТ. Система АСОИ ФинЦЕРТ[1], созданная на базе подразделения, аккумулирует всю информацию об угрозах в кредитно-финансовой сфере и позволяет обмениваться ею между всеми участниками системы: банками, правоохранительными органами, провайдерами связи, ИБ-организациями, а также получать рекомендации ФинЦЕРТ по реагированию на угрозы. Создаётся своеобразный эффект «коллективного иммунитета».

[1] Автоматизированная система обработки инцидентов ФинЦЕРТ.

ПРОБЛЕМА ОБРАБОТКИ ДАННЫХ TI

Чаще всего организация процесса киберразведки начинается с использования открытых источников, содержащих индикаторы компрометации: хеши вредоносных файлов, домены, IP-адреса и прочие артефакты, связанные с деятельностью киберпреступников. Основные проблемы на данном этапе происходят при попытке добыть максимум «разведданных» путём подписки на всевозможные доступные источники. Получается палка о двух концах: чрезмерный поток разрозненных данных неизбежно приводит к невозможности их обработать.

При этом важно понимать, как полученные индикаторы связаны с конкретными группировками, например ведущими свою деятельность в отношении банковской отрасли или действующими против конкретной страны. Таким образом, для принятия эффективных контрмер против киберпреступников необходимо не только использовать уже имеющиеся в наличии данные, но и быстро находить недостающий и актуальный контекст.

ЗАДАЧИ, КОТОРЫЕ РЕШАЮТ TI-ПЛАТФОРМЫ

По мере расширения инфраструктуры организации назревает потребность

в автоматизации работы со сведениями об угрозах. На помощь приходят специализированные платформы кибербразведки, которые агрегируют всю доступную информацию в единой базе, автоматизируют ключевые процессы, связанные с обработкой данных TI и, наконец, позволяют экономить временны́е и человеческие ресурсы. В качестве проактивной защиты платформы позволяют автоматически экспортировать индикаторы компрометации на СЗИ.

Помимо этого, TI-платформы используются в различных рабочих сценариях, самый распространённый из которых — реактивное реагирование на угрозы путём поиска индикаторов компрометации в инфраструктуре, а именно в событиях SIEM-систем. Также платформа кибербразведки может участвовать в процессе реагирования на инциденты как своеобразная база знаний, предоставляя полный контекст по индикаторам, содержащимся в инцидентах.

Использование подобных платформ упрощает работу с данными TI в целом, позволяет быстро выявить скрытые угрозы в инфраструктуре, минимизирует ущерб благодаря своевременной блокировке угроз, а также ускоряет все ИБ-процессы организации.

ВЫБОР ПЛАТФОРМЫ АНАЛИЗА УГРОЗ

Компания «ДиалогНаука» долгое время поставляла заказчикам решения как российских, так и зарубежных вендоров. Когда компания Anomali, один из ведущих поставщиков платформ Threat Intelligence, ушла с российского рынка, было необходимо найти среди отечественных систем аналог, не уступающий в качестве западному продукту, который уже не один год был в портфеле решений компании.

При выборе подходящей системы компания концентрировалась на нескольких аспектах — архитектуре, модульности и интеграционных возможностях платформы. В ходе реализуемых проектов «ДиалогНаука» работает с разными типами инфраструктур заказчиков: территориально распределённые, гибридные, инфраструктуры с высокой нагрузкой и другие. Таким образом, одним из основных требований были

В R-Vision TIP реализована встроенная интеграция с ключевыми источниками данных TI, при этом поддерживается более 20 сервисов обогащения

масштабируемость решения и возможность архитектурно поддерживать инфраструктуры любого типа.

Заказчики «ДиалогНауки» неоднократно отмечали важность гибкости платформы, а именно возможность подключения различных поставщиков фидов. Кроме того, учитывая существующие сценарии применения систем кибербразведки, одним из ключевых параметров при выборе была открытость платформы. Крайне важно встроить работу TI-платформы в текущие процессы информационной безопасности конкретной организации, такие как реагирование на инциденты, обнаружение событий ИБ, распространение информации об индикаторах компрометации на средства защиты информации и сетевые устройства организации.

Прежде чем предлагать заказчику решение какого-либо вендора, компания всегда проводит его предварительную проверку в своей тестовой лаборатории. R-Vision, в свою очередь, придерживается схожего подхода: сначала продукты проходят процесс тестирования в рамках инфраструктуры вендора, затем пилотирование в инфраструктурах заказчиков, а финальный процесс внедрения всегда индивидуален и проходит под контролем команды экспертов.

ПЛАТФОРМА R-VISION TIP

При проведении тестирования R-Vision Threat Intelligence Platform (TIP) «ДиалогНаука» отметила изобилие как коммерческих, так и открытых фидов, с которыми поддерживается работа. В их число входит АСОИ ФинЦЕРТ, а также R-Vision Threat Feed, который входит в состав платформы.

Помимо встроенных интеграций, возможно подключение других источников, при этом платформа поддерживает более 20 сервисов обогащения. За счёт ретроспективного и проактивного поиска релевантных индикаторов в потоке событий данное решение снимает нагрузку с SIEM-систем и сокращает ресурсы на её настройку. Также R-Vision TIP поддерживает автоматическую выгрузку индикаторов для немедленной блокировки на такие средства защиты, как антивирусы, межсетевые экраны и решения класса EDR.

Поскольку ручной процесс обработки данных может занимать существенное время, для решения этой задачи в TI-платформах используются инструменты оценки качества источников и индикаторов, что позволяет аналитикам концентрироваться только на важных и актуальных вопросах. Эта функциональность также реализована в системе R-Vision TIP.

На более продвинутом уровне кибербразведки R-Vision TIP позволяет формировать собственную базу данных: например, создавать уникальные IoCs и отчёты об угрозах, связывая при этом сущности друг с другом. Для получения целостной картины происходящего и проведения подробного анализа взаимосвязи между объектами можно отобразить в виде схемы. Кроме того, платформа позволяет осуществлять обмен данными между различными подразделениями организации путём создания бюллетеней о существующих в инфраструктуре угрозах и уязвимостях.

* * *

Тренд на импортозамещение коснулся и платформ Threat Intelligence — компании активно интересуются отечественными аналогами западных систем, при этом становясь всё требовательней в вопросе качества получаемых данных. По итогам сравнения различных TI-платформ система R-Vision TIP показала полное соответствие всем необходимым требованиям и уже получила положительные отзывы со стороны заказчиков в ходе ряда пилотов и полноценных внедрений.