Виктор СЕРДЮК
генеральный директор
АО «ДиалогНаука»

Роман ВАНЕРКЕ
технический директор
АО «ДиалогНаука»

ЦИФРОВАЯ КИБЕРРАЗВЕДКА

ПЛАТФОРМА TIP ВЫЯВЛЯЕТ И РАССЛЕДУЕТ

Сейчас уже невозможно гарантировать, что внутри корпоративной сети всё благополучно. Даже если антивирусы молчат, межсетевые экраны отражают все нападения, а система установки обновлений работает быстро и оперативно, всё равно остаётся вероятность успешных целенаправленных атак злоумышленников, которые часто используют уязвимости «нулевого дня», ворованные учётные данные и методы социальной инженерии. При этом нарушители реализуют атаку в течение длительного временного промежутка, что также существенно затрудняет её обнаружение. Злоумышленники долго изучают защитные системы объекта атаки и наносят точные и стремительные удары в наиболее уязвимые места, вследствие чего средства защиты не всегда успевают их зафиксировать. Для выявления вредоносной активности нападающих необходимо использовать комплекс мер и инструментов, которые выявляют признаки присутствия в системе злоумышленника. Одним из таких инструментов являются специализированные платформы для управления данными киберразведки (Threat Intelligence).

БАЗА TIP

Ключевым элементом платформы цифровой киберразведки (Threat Intelligence Platform, TIP) являются индикаторы компрометации или Indicators of compromise (IoC). Это набор признаков, по которым можно идентифицировать активность злоумышленников. В качестве таких признаков могут выступать хэши вредоносных файлов, IP-адреса и домены, связанные с преступной активностью. IoC может содержать, в том числе, и регулярные выражения для выявления записей в системных журналах, которые соответствуют действиям тех или иных хакерских группировок. Понятие IoC впервые было введено компанией Mandiant (сейчас является частью FireEye), которая использовала их в процессе расследования инцидентов безопасности.

Чем IoC отличается от антивирусной сигнатуры? Индикатор компрометации содержит сведения о действиях программы, а не о её коде. Это позволяет описывать не только вредоносные программы, но и потенциально опасное проведение вполне легитимных программ и даже конкретных пользователей. Как правило, индикаторы компрометации составляют производители средств защиты информации — антивирусные лаборатории, разработчики межсетевых экранов, песочниц и др. Также в качестве поставщиков IoC могут выступать центры реагирования на инциденты, например, ФинЦЕРТ или ГосСОПКА в России или US-CERT в США. В частности, US-CERT начал публиковать индикаторы компрометации для хакерских группировок, атакующих ведомственные ресурсы США, в серии документов под названием Malware Analysis Report (MAR), то есть отчёты по анализу вредоносов.

IoC содержит сведения о действиях программы, а не о её коде. Это позволяет описывать не только вредоносные программы, но и потенциально опасное проведение вполне легитимных программ и даже конкретных пользователей

Последовательности IoC из одного источника принято называть фидами — от английского слова feed, то есть подписка на серию IoC. Среди поставщиков фидов можно выделить такие компании, как Group-IB, Palo Alto, ESET, Kaspersky Lab, FireEye. Фиды бывают бесплатными, как в случае с MAR, так и платными — обычно такими продажами как раз и занимаются вендоры.

Платформы киберразведки предназначены для автоматического сбора, нормализации и хранения индикаторов компрометации (фидов). В состав поставки платформы Threat Intelligence, как правило, входит и набор фидов, как платных, так и бесплатных, которые в большой мере и определяют функциональные возможности платформы.

В состав платформы TIP также может входить модуль, который собирает информацию из различных системных журналов, средств защиты и операционных систем и анализирует их на наличие индикаторов компрометации, которые содержатся в платформе. В качестве источников таких исходных данных может выступать SIEM-система, которая уже содержит все необходимые события.

Если система находит тот или иной IoC в журналах аудита, то она выдаёт рекомендации по предотвращению вредоносной деятельности и проведению расследования. Качество рекомендаций сильно зависит от источника IoC — платные фиды могут содержать инструкции для конкретных межсетевых экранов или антивирусов, в то время как с рекомендациями от бесплатных придётся разбираться самостоятельно, что потребует дополнительных расходов на зарплату соответствующего компетентного персонала.

Таким образом, платформа TIP может использоваться как для выявления новых, так и для расследования уже случившихся инцидентов. Расследование потребует анализа с помощью платформы данных истории (действий/событий), которые должны быть собраны. В качестве источника таких данных также может выступать SIEM-система. По этим данным с помощью индикаторов компрометации можно обнаружить, где и когда произошла атака, которая впоследствии привела к расследуемому инциденту. Эти сведения помогают обнаружить виновных и выяснить реальный ход событий, что и является основной целью расследования. Если корпоративная сеть является распределённой, то поиск срабатывания IoC по данным истории (действий/событий) по всем филиалам позволяет оценить качество работы службы безопасности в них.

РЫНОК TIP

Одним из пионеров рынка платформ Threat Intelligence является компания Anomali, которая выпускает свои продукты с 2013 года. Возглавляет компанию Хью Ньеманзе (Hugh Njemanze), бывший соучредитель, CTO и исполнительный вице-президент по разработке производителя SIEM-инструмента ArcSight, который в июле 2014 года занимал пост генерального директора. Собственно, рынок TIP является продолжением SIEM, которые просто собирали и обрабатывали сведения из различных средств защиты.

В портфеле компании 3 продукта:

- Anomali STAXX — бесплатная платформа, позволяющая получать фиды в открытых стандартах обмена информацией о киберугрозах;
- Anomali ThreatStream — коммерческая платформа, осуществляющая сбор индикаторов компрометации более чем из 130 возможных источников в различных форматах;
- Anomali Enterprise — корпоративная платформа проактивного поиска угроз в сети, которая способна хранить события с глубиной поиска по архиву за последние 5 лет.

При этом в STAXX интеграция может быть организована только в открытых форматах STIX (Structured Threat Information eXpression) и TAXII (Trusted Automated Exchange of Intelligence Information), а с другими источниками взаимодействие не предусмотрено. В то же время Anomali ThreatStream интегрируется с другими системами защиты и позволяет реализовать весь цикл киберразведки. Anomali Enterprise позволяет осуществлять автоматический поиск индикаторов компрометации по всему архиву событий, что особенно важно для проведения расследований по данным истории (действий/событий) крупных корпоративных сетей.

Впрочем, есть и российские продукты для цифровой киберразведки. В частности, одним из них является платформа R-Vision Threat Intelligence Platform (RTIP), которая представляет собой специализированную платформу управления данными киберразведки. Она обеспечивает автоматический сбор, нормализацию и обогащение индикаторов компрометации, передачу обработанных данных напрямую на внутренние средства защиты, а также поиск и обнаружение индикаторов во внутренней инфраструктуре организации с помощью сенсоров.

RTIP упрощает работу с индикаторами компрометации, осуществляя непрерывный сбор, нормализацию и хранение данных из различных источников в единой базе. Продукт облегчает выявление скрытых угроз, обеспечивая автоматический мониторинг релевантных индикаторов в сторонних SIEM, записях системных журналов syslog и DNS-запросах с помощью сенсоров. Собираемые сведения позволяют вовремя блокировать угрозы и минимизировать возможный ущерб благодаря автоматической выгрузке обработанных данных напрямую на внутренние средства защиты, такие как межсетевые экраны Cisco, PaloAlto Networks, Check Point и другие.

Есть разработки и с открытыми исходными кодами, лидером среди которых является Malware Information Sharing Platform (MISP). Платформа была выпущена более 6 лет назад и собрала вокруг себя множество профессионалов по всему миру. MISP интегрируется с IRP-системой TheHive, в связке, с которой способна реализовать гибкий механизм реагирования на инциденты ИБ, обнаруженные в рамках процесса киберразведки. Среди достоинств данной TIP можно отметить поддержку всех известных и используемых форматов импорта и экспорта индикаторов компрометации, обогащение и классификацию инцидентов, а также ежемесячные обновления и поддержку разработчиков.

* * *

Платформы киберразведки TIP в перспективе могут стать неотъемлемой частью ситуационных центров по информационной безопасности (SOC). Хотя платформа TIP сама по себе и не является средством защиты, но она позволяет оперативно обнаружить признаки начавшейся атаки и оперативно на неё среагировать. Кроме этого, платформа киберразведки может использоваться как эффективный инструмент для расследования инцидентов информационной безопасности.