Как оценить актуальность индикаторов компрометации

Р.С. Ларичев

Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия

Обоснование. Тема оценки актуальности индикаторов компрометации (IoC) играет важную роль в современном мире кибербезопасности. Количество кибератак продолжает расти, а их методы становятся все более изощренными. Злоумышленники постоянно меняют свои тактики и техники, чтобы обойти системы защиты. Например, вредоносное ПО может быть модифицировано в течение нескольких часов, а все данные о злоумышленниках изменены или стерты. Компрометация информационной сети может привести к утечке важной информации, финансовым потерям и другим негативным последствиям. В таких условиях использование устаревших или неактуальных индикаторов компрометации (IoC) может привести к пропуску реальных угроз или к ложным срабатываниям, что снижает эффективность защиты.

Цель — рассмотреть способы оценки актуальности индикаторов компрометации (IoC).

Методы. Так как все новые IoC добавляются в базу данных с указанием их источников и даты добавления, то мы можем автоматически сравнивать с их первоначальным источником и датой создания, чтобы определить, соответствуют ли они актуальным критериям оценки. Этот метод контроля срока жизни индикаторов компрометации можно описать с помощью функции, которая отражает скорость устаревания IoC с течением времени:

$$scorea = basescorea \times \left(1 - \left(\frac{t}{t(\alpha)}\right)^{\frac{1}{\delta\alpha}}\right),$$

где $t = T(t) - T(t-1) > 0$. Каждому индикатору присваивается базовая оценка (base_score(a)), находящаяся в диапазоне от 0 до 100. Эта оценка зависит от надежности источника, предоставившего IoC. При повторном обнаружении индикатора базовая оценка может быть скорректирована. Также определяется скорость устаревания индикатора (decay_rate), которая характеризует, насколько быстро снижается его общая оценка с течением времени. Для учета временных изменений используются временные метки $T(t)$ и $T(t-1)$, где $T(t)$ обозначает текущее время, а $T(t-1)$ — момент последнего обнаружения индикатора.

Оценке актуальности индикаторов компрометации помогают SIEM-системы (Security Information and Event Management), позволяя автоматизировать процессы анализа и реагирования. Они могут обнаружить IoC в реальном времени, оценить их актуальность на основе текущих данных и принять решение о реагировании на угрозы. Преимуществами является: оперативное реагирование, автоматизация процессов и интеграция с Threat Intelligence.

Проводя мониторинг сетевой активности, можно воспользоваться внешними источниками активного поиска Threat Intelligence, чтобы получить информацию об известных угрозах и индикаторах компрометации. Рейтинг индикаторов компрометации позволяет выделить из общей массы индикаторов только те, анализ которых действительно поможет в борьбе с внешними угрозами. При расчете рейтинга учитываются различные метрики, например:

1) обширность (отражает степень связанности индикатора компрометации с дополнительным контекстом, в том числе Geo-привязкой, данными об открытых портах;
2) оперативность (показатель определяется частотой обновления конкретного фида по сравнению с другими источниками);
3) полнота (параметр отражает условный «вклад» фида в общий объем данных об индикаторах, поступающих из всех доступных фидов).

Опираясь на данные методы, для автоматизации был написан скрипт расчета срока жизни IoC. С его помощью можно вовремя обнаруживать активные угрозы и снижать время реагирования на инциденты. А использование современных инструментов, таких как SIEM-системы и платформы Threat Intelligence, позволяет автоматически улучшить защиту и минимизировать риски для организаций.

Результаты. В результате работы был написан скрипт, который позволяет автоматизировать процесс расчета актуальности индикаторов компрометации. На выходе программа выдает расчет срока жизни индикатора, время, прошедшее с первого обнаружения индикатора, и его вес на момент обнаружения.

Выводы. Оценка актуальности индикаторов компрометации — это важный процесс, который позволяет эффективно использовать ресурсы для защиты от киберугроз. Предложенный подход оценки актуальности IoC позволяет не только оперативно среагировать на угрозы, но и предположить их дальнейшие развитие.

Ключевые слова: индикаторы компрометации; IoC; SIEM-системы; компрометация информационных систем; уязвимости; Threat Intelligence.

Сведения об авторе:

Роберт Сергеевич Ларичев — студент, группа ИБТС-21, факультет № 1; Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: la-robin@yandex.ru

Сведения о научном руководителе:

Ирина Сергеевна Поздняк — доцент кафедры информационной безопасности; Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: i.pozdnyak@psuti.ru