УДК 004.056

Разработка методики использования технологии введения в заблуждение в защите от атак на информационные системы

Евсеева Т.А. (ИТМО)
Научный руководитель – кандидат технических наук, доцент Левко И.В.
(ИТМО)

Введение. Современные процессы мониторинга в SOC опираются на корреляцию событий SIEM и телеметрию EDR/IDS, при этом малошумные действия злоумышленника на стадиях разведки и закрепления могут оставаться незамеченными. Практика применения honeypot-технологий показывает, что обращение к заранее подготовленным приманкам формирует высокосигнальные события, не характерные для легитимной активности [1]. Подходы к систематизации deception-технологий и их роли в активной защите рассматриваются в работах [2, 3].

Основная часть. Методика построена на сопоставлении целевых техник MITRE ATT&CK с типами deception-активов [4]. В качестве приоритетных выбраны техники разведки и перемещения: System Information Discovery (T1082), Account Discovery (T1087), Network Service Scanning (T1046), File and Directory Discovery (T1083), Remote System Discovery (T1018). Указанные техники выполняются штатными средствами ОС (PowerShell, net, wmic, arp) и часто не вызывают срабатываний сигнатурных механизмов.

Методика включает четыре этапа.

1. Формирование набора приманок. Для каждой техники определяется тип события, которое должно быть зафиксировано (например, попытка аутентификации, обращение к файлу, сетевое подключение). Далее выполняется сопоставление с типом приманки:
   - honeytokens (учетные записи, пароли, ключи доступа) – для техник Credential Access и Account Discovery;
   - сервисные ловушки (эмуляция RDP/SMB/SSH) – для Network Service Scanning и Remote Access;
   - decoy-хосты и директории – для File and Directory Discovery и Lateral Movement. Отбор производится с учетом изоляции, недопустимости pivot-сценариев и правдоподобия размещения в сегменте.
2. Размещение и интеграция. Приманки размещаются в рабочих, серверных и административных сегментах. Каждому объекту присваивается уникальный идентификатор (decoy_id). События нормализуются в формате SIEM и обогащаются контекстом (сегмент, критичность, пользователь, источник).
3. Корреляция и приоритизация. В SIEM реализуются правила трех типов:
   - hard-trigger – любое обращение к honeytoken;
   - rate-trigger – превышение порога попыток подключения к сервисной ловушке;
   - chain-trigger – последовательность «сканирование → попытка доступа». Событию присваивается приоритет на основе типа действия и критичности сегмента. Маппинг на техники ATT&CK обеспечивает единый язык описания инцидента [4].
4. Автоматизированное реагирование. При формировании алерта запускается playbook в SOAR: сбор артефактов (логи аутентификации, сетевые соединения, контекст узла), изоляция хоста или блокировка учетной записи при достижении заданного уровня критичности. Подход к интеграции deception в защитный контур соответствует принципам, описанным в [3]. Эксперимент проведен в двух контурах: базовом и экспериментальном с deception-слоем. Для каждого сценария атаки выполнено не менее пяти повторений. Получены следующие показатели:
   - MTTD сокращено с 12 до 4 минут;
   - MTTR сокращено с 25 до 15 минут;

- Precision увеличено с 0,85 до 0,95;
- FPR снижено с 0,12 до 0,03;
- увеличено покрытие техник ATT&CK;
- доля автоматических действий выросла с 30% до 60%. Снижение MTTD обусловлено тем, что обращение к приманке формирует событие на ранней стадии атаки, до развития lateral movement. Повышение точности связано с тем, что события deception практически не пересекаются с легитимной активностью, что подтверждается выводами обзора [2].

Выводы. Разработанная методика демонстрирует, что интеграция deception-активов в контур SIEM/SOAR повышает скорость обнаружения и реагирования на атаки, увеличивает точность детектирования и снижает операционную нагрузку SOC. Практическая применимость методики определяется ее адаптируемостью к различным сегментам инфраструктуры и согласованием с моделью угроз организации.

Список использованных источников:

1. Spitzner L. Honeypots: Tracking Hackers. – Boston: Addison-Wesley, 2003.
2. Fraunholz D., Duque Antón S., Lipps C., et al. Demystifying Deception Technology: A Survey // IEEE Communications Surveys & Tutorials. 2019. Vol. 21(1).
3. Almeshekah M., Spafford E. Planning and Integrating Deception into Computer Security Defenses // HICSS. 2016.
4. MITRE Corporation. MITRE ATT&CK Framework. URL: https://attack.mitre.org/

Автор _____ Евсеева Т.А.
Научный руководитель _____Левко И.В.