ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССОВ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ф.Т. Борботько

При построении систем защиты информации важным аспектом является обеспечение мониторинга информационных систем [1], сущность которого заключается в обнаружении и реагировании на инциденты информационной безопасности. Практическая реализация мониторинга возможна с использованием соответствующих программно-технических средств, например, Incident Response Platform.

Incident Response Platform компании R-Vision [2] представляет собой программное обеспечение, предназначенное для агрегации данных об инцидентах из различных источников, их обработки, реагирования на них и координации действий подразделения, которое обеспечивает информационную безопасность в организации. Указанное программное обеспечение позволяет выполнить инвентаризацию активов организации, реализовать объединение в единой базе данных информации от различных средств информационной безопасности (сканеры уязвимостей, антивирусные средства защиты, SIEM системы и т.д.). Ее применение совместно

с программным обеспечением Threat Intelligence Platform которая используется для получения данных о моделях нарушителя (данные кибербразведки), позволяет разработать сценарии реагирования (playbook) на действия нарушителя. Сокращение времени реагирования обеспечивается за счет того, что отдельные этапы в рамках предварительно разработанного сценария реагирования, могут быть выполнены в автоматическом режиме без участия оператора системы. Это в свою очередь, позволяет оптимизировать штат сотрудников, деятельность которых направлена на обнаружение и реагирование на инциденты информационной безопасности.

Литература

1. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны. М.: ДМК Пресс, 2020. 326 с.

2. R-Vision IRP / R-Vision [Электронный ресурс]. – 2022. – Режим доступа: https://rvision.ru/products/irp. – Дата доступа: 02.05.2022.