**AlphaSEC**

**Цель и задачи проекта:**

**Цель:** разработать систему помогающую принимать решения оператору ИБ или принимающую решения за оператора ИБ.

**Задачи:**

* Сбор информации с разных систем (событий, здоровья систем и т.п.);
* Разработка искусственного интеллекта(AI), который на основе поступающих данных будет способен принимать решения;
* Разработка аналитики по данным находящимся в системе (Отчет, прогнозирование и т.п.);
* Разработка алгоритмов атаки и контрмер, на основе команд от оператора и/или AI;
* Разработка автоматизированного аудита(Стандарты, политики организации и т.п.);
* Разработка автоматизированной оценки защищенности и рисков защищаемой среды;
* Разработка компонентов управления подконтрольных систем;
* Разработка GUI.

**Алгоритмы:**

**Принятие решения:**

1. 1)Поступление события(alert);
2. 2)Определение alert-а (В чем смысл alert-а(какое направление, например: подбор пароля, посещение вредоносного сайта и т.п.);
3. 3)Сбор информации по alert-у(IP, Hostname, Username, Системы которые могут быть задействованы (сбор информации с них) и т.п.);
4. 4)Подтверждение на основе полученной информации, что произошел или нет инцидент ИБ (подтверждение на основе не менее 3 – 5 факторов);
5. 5)Если произошел инцидент принятие решения по нейтрализации последствий;
6. 6)Корректировка системы (превентивные меры для того чтобы в будущем инцидент нанес меньший ущерб или не наступил вообще).

**Модули:**

**Сбор:**

1. 1)Сбор осуществляется по агентской (Программа или скрипт установленный на контролируемой системе) и без агентской схеме (На основе: syslog или подобной системе отправки событий; с помощью технологический пользователей, который на основе автоматизированных команд будут собирать информацию о контролируемой системе);
2. 2)Агент отправляет информацию на коллектор (коллектор может обрабатывать n количество агентов).
3. 3)Коллектор структурирует поступающую информации от Агентов и отправляет на хранение в БД.
4. Коллектор принимает информацию от модуля проверки на действия в рамках аудита и отправляет на исполнение Агенту.

**АI:**

1. Подгружает информацию о событии из БД и на основе алгоритмов(Нейронные сети(обучение) и экспертная система(БД знаний экспертов)) осуществляет анализ;
2. Результат анализа AI предоставляет оператору или AI принимает решение самостоятельно;

**Аналитика:**

1. На основе алгоритмов обработки данных(OLAP, статистика, риски и т.п.) осуществлять анализ данных на основе выбранных критериев оператором и AI.
2. Вывод отчета в интерактивной форме оператору.

**Проверка (атака и аудит):**

1. Осуществляет атаки на системы (подконтрольные и нет) по алгоритмам на основе команд от оператора или AI.
2. Проверяет на наличие критериев определенных оператором или стандартами ИБ.
3. Проводит аудит подконтрольных систем на основе отправки запроса коллектору.
4. Загружает собранную информацию в БД.

**Хранение:**

1. Агент: хранит информацию по политикам и правилам. Осуществляет хранение информации при отключении от системы AlphaSEC и отправку на коллектор при включении.
2. Коллектор: временно осуществляет хранение поступающей информации до отправки в БД.
3. AI: Осуществляет хранение информации в БД(Экспертная БД) в которой находиться информация по экспертным решениям от оператора и на основе обучения AI.
4. Проверка: Хранит промежуточную информации по аудиту, стандартам и запросам от AI до помещения в Основную БД или передачи в AI.
5. Основная БД: Осуществляет хранение данных собранных системой AlphaSEC.
6. Управление: Хранит информацию по сбору здоровья систем в реальном времени и отправляет в GUI.
7. GUI: хранит поступающую информацию от систем в реальном времени.

**Управление:**

1. Осуществляет управление(конфигурирование систем и/или подконтрольными системами через прямые обращения(Системы информационной безопасности) и с помощью коллекторов(Системы которые генерируют события).
2. Осуществляет слежение за здоровьем систем информационной безопасности.

**GUI:**

1. WEB интерфейс осуществляющий управление подсистемами AlphaSEC, на основе команд от оператора.
2. Интерфейс должен находиться в одном окне (выплывающие окна, вкладки без перехода).
3. Выводить инциденты после обработки AI и подробную информацию о инциденте.
4. Настройка правил для AI и обработки логов (на основе логических операторов).
5. Управление(настройка) AI (Необработанные решения (когда AI не может принять решения), настройка экспертной БД(на основе правил) и т.п.) и подконтрольными системами.
6. Отображение состояния здоровья систем.
7. Запрос и отображение отчетов из модуля аналитики и прямых запросов к основной БД.
8. Настройка векторов атаки и систем участвующих в атаке.
9. Отображение подобранной информации (собранной со всех систем в одном окне) по атакуемым и подконтрольным системам собранных в процессе аудита/атаки.
10. Определение критичных систем на основе экспертного решения оператора.
11. Отправка уведомлений оператору(инциденты, состояние системы и т.п.).