МЕХАНИЗМЫ ВИЗУАЛИЗАЦИИ В SIEM-СИСТЕМАХ

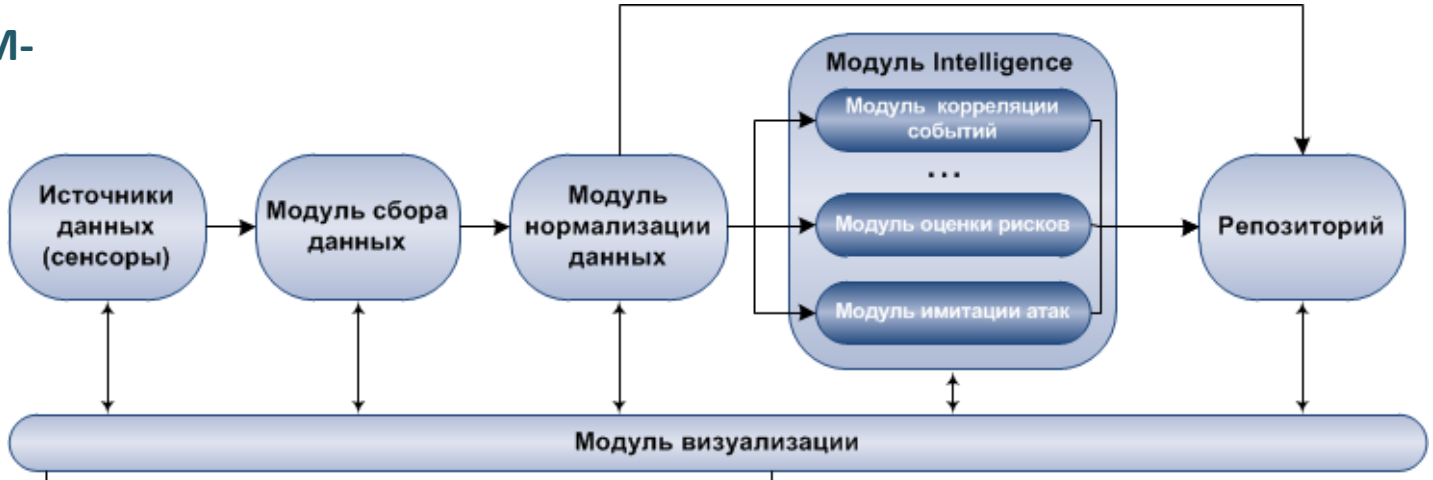
Новикова Е.С.
Санкт-Петербургский Государственный Электротехнический Университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Санкт-Петербург, Россия

Лаборатория проблем компьютерной безопасности Санкт-Петербургского Института Информатики и Автоматизации РАН
Санкт-Петербург, Россия

РусКрипто'2012, 28-31 марта 2012 г.

Модуль визуализации в SIEM-системы

Архитектура SIEM-системы



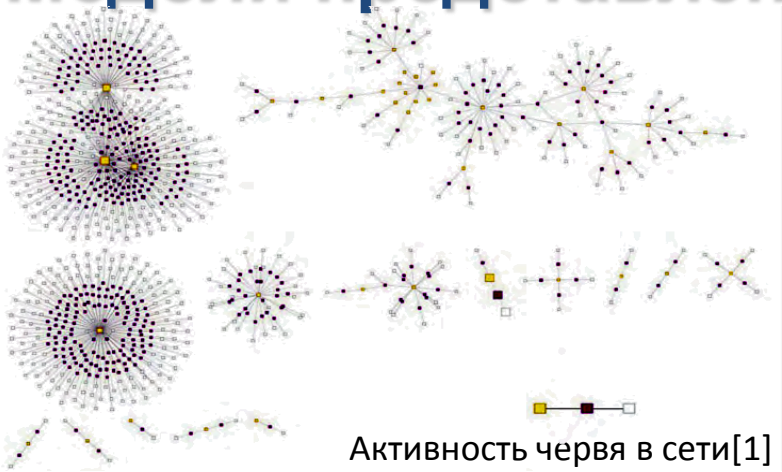
Задачи модуля визуализации

- Формирование отчетов
- Исторический анализ данных
- Мониторинг событий
- Визуализация результатов анализа, оценки рисков, моделирования атак
- Настройка параметров модулей анализа, оценки рисков,имитации атак
- Управление пользователями конфигурацией SIEM -системы
- Управление ресурсами сети
- Управление источниками данных (сенсорами)

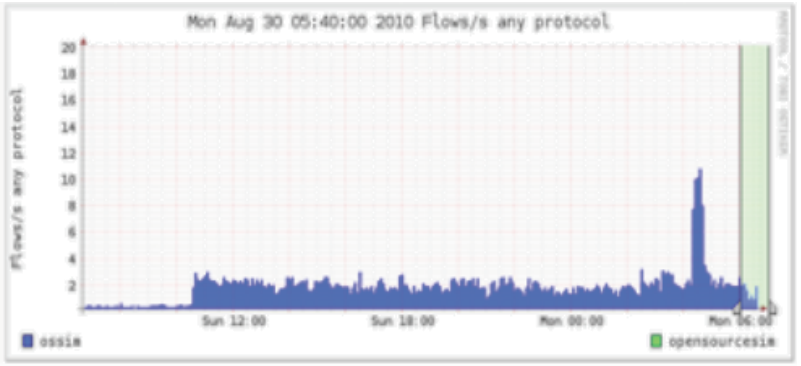
Модели представления данных и их применение

- Мониторинг периметра сети :
  - круговая диаграмма, представляющая наиболее активных хостов-приемников и хостов-получателей
  - гистограмма наиболее часто используемых сервисов
  - граф коммуникаций, отражающих потоки между хостами
  - карта деревьев (treemap), отражающая частоту использования портов различными хостами
  - связные графы вида «отправитель-сообщение-получатель» и т.д.
- Контроль деятельности пользователей:
  - связные графы вида «пользователь-деятельность» и «пользователь-сервер»
  - гистограмма, отражающая число документов, просмотренных пользователям
- Отображение уровня безопасности и рисков :
  - круговая диаграмма, отражающая наиболее уязвимые хосты
  - карты деревьев, отражающие наиболее уязвимые хосты
  - географические карты, отражающие расположение хостов с указанием оценок рисков, доступности и уязвимости хостов

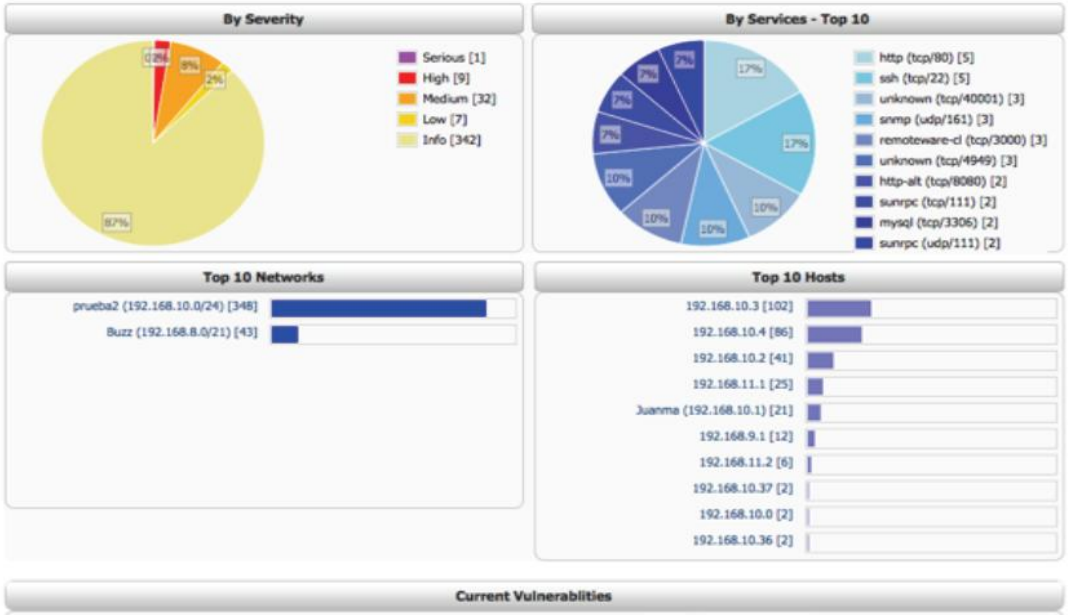
Модели представления данных



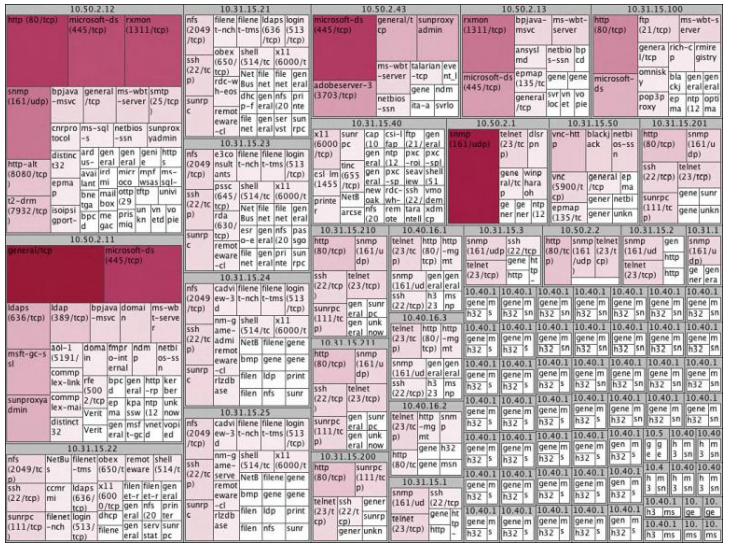
Активность червя в сети[1]



Визуализация трафика Open Source SIEM [2]



Отчет о выявленных уязвимостях в Open Source SIEM [2]

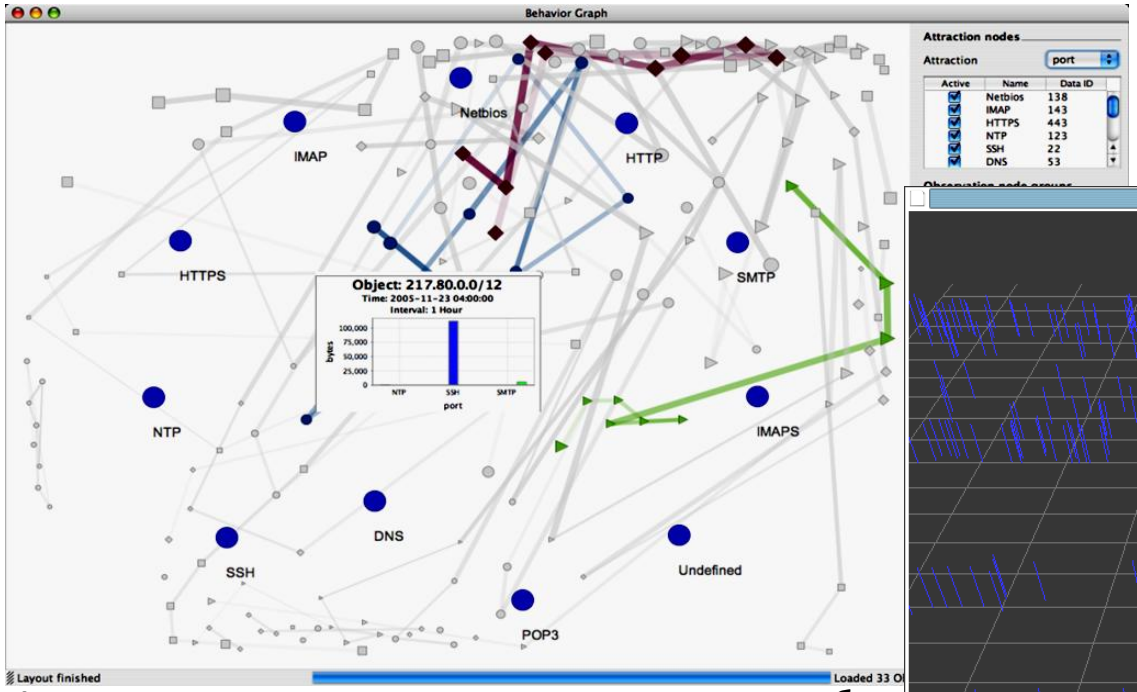


Анализ уязвимостей с помощью карт деревьев[1]

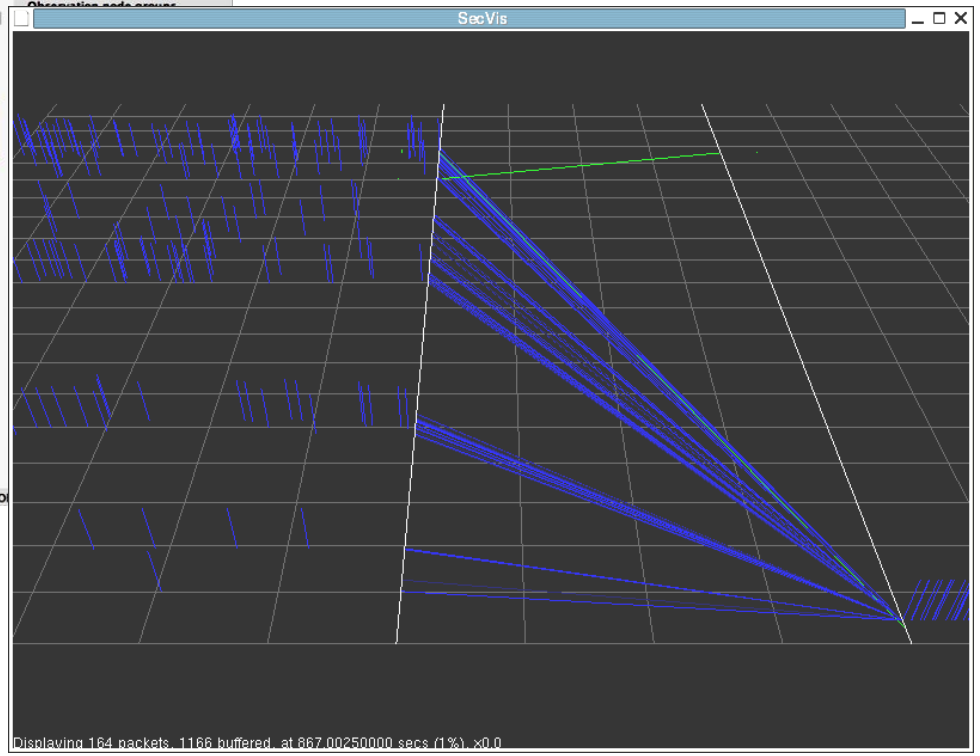
[1] R. Marty Applied Security Visualization. NY, Addison Wesley , 2008.

[2] http://communities.alienvault.com/community/reporting

Модели представления данных



Активность хоста в зависимости от того, какие службы от используются [1]

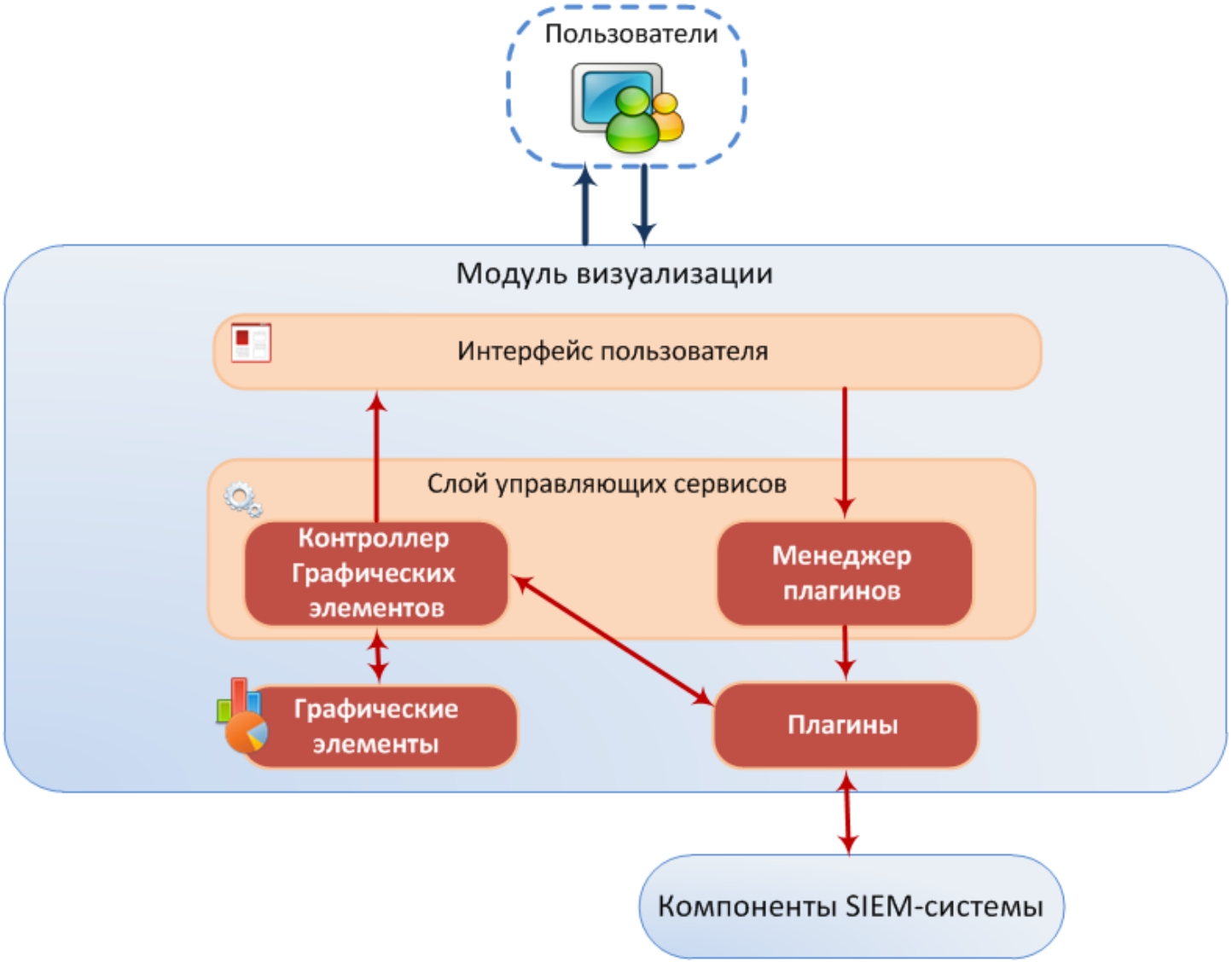


Сетевой трафик во время атаки червя, отслеживаемый в течение 640 сек [2]

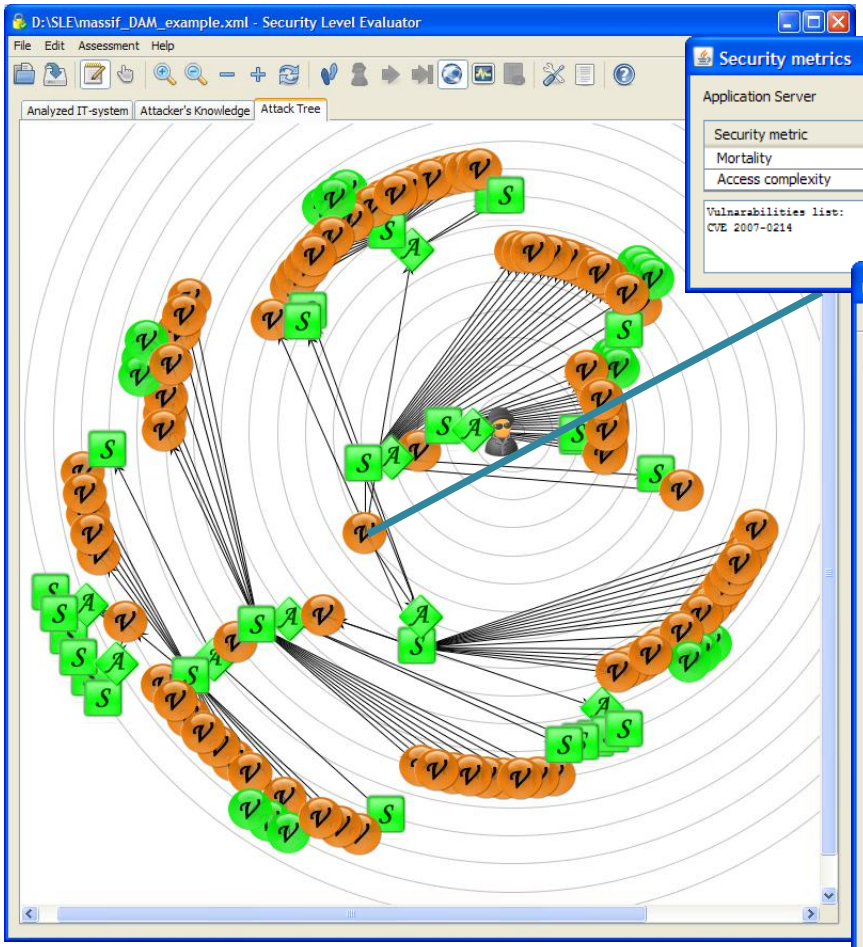
[1] Mansmann F., Meier L., Keim D. A. Visualization of Host Behavior for Network Security. In Proceeding SecViz 2007

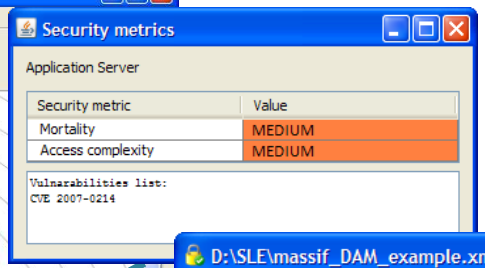
[2] Krasser, S., Conti, G., Grizzard, J., Gribshaw, J., Owen, H. Real-time and forensic network data analysis using animated and coordinated visualization. In 2005 IEEE Workshop on Information Assurance (2005), IEEE Press.

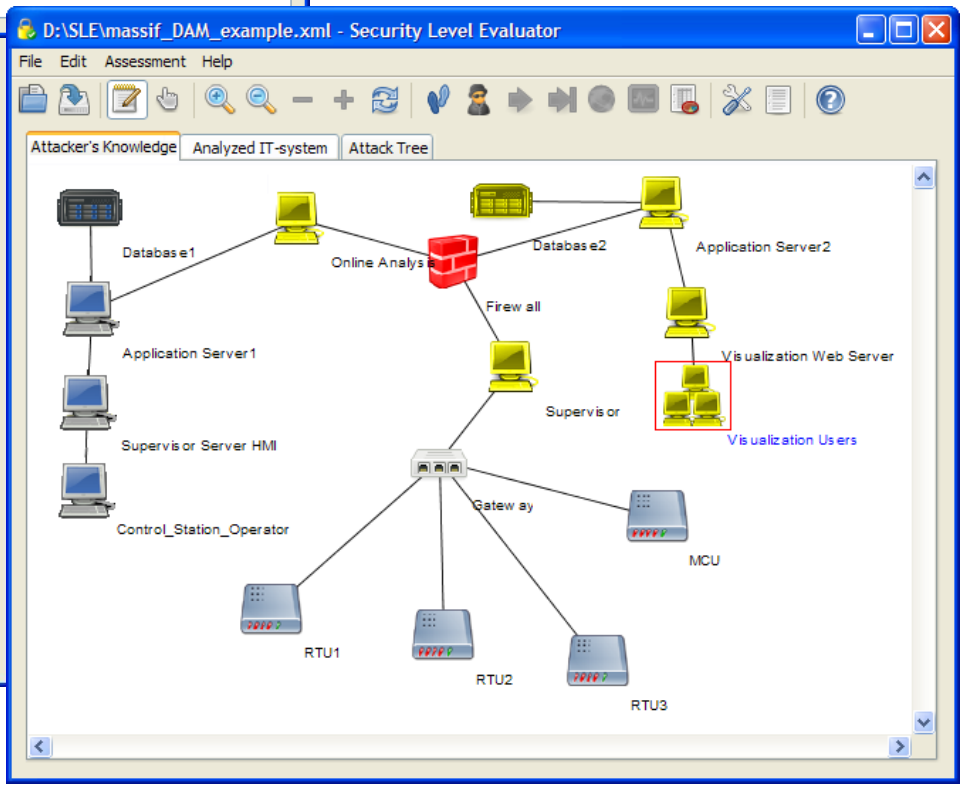
Архитектура модуля визуализации



Прототип модуля визуализации







Граф действий атакующего, отражающий сложность их выполнения

Граф знаний злоумышленника, цветом указана критичность узлов

Заключение

Полученные результаты

- Проанализированы способы графического представления информации о событиях безопасности
- Разработана архитектура модуля визуализации
- Разработан прототип модуля визуализации
- Проведены первоначальные эксперименты

Дальнейшие исследования

- Развитие библиотеки графических компонент
- Проработка вопросов, связанных с *масштабируемостью* и *интерактивностью* отображаемых данных
- Развитие прототипа модуля визуализации
- Проведение экспериментов

Контактная информация

Новикова Евгения Сергеевна
novikova@comsec.spb.ru

Благодарности

Работа выполняется при финансовой поддержке РФФИ (проект №10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект № 3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.