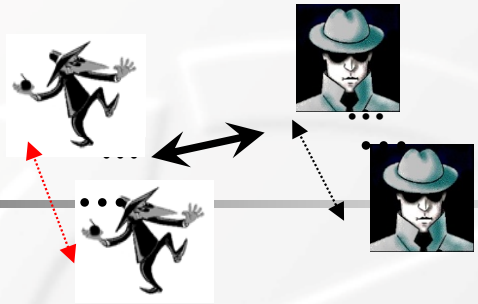


Модели и методики визуального анализа данных для решения задач компьютерной безопасности

И.В. Котенко

СПИИРАН

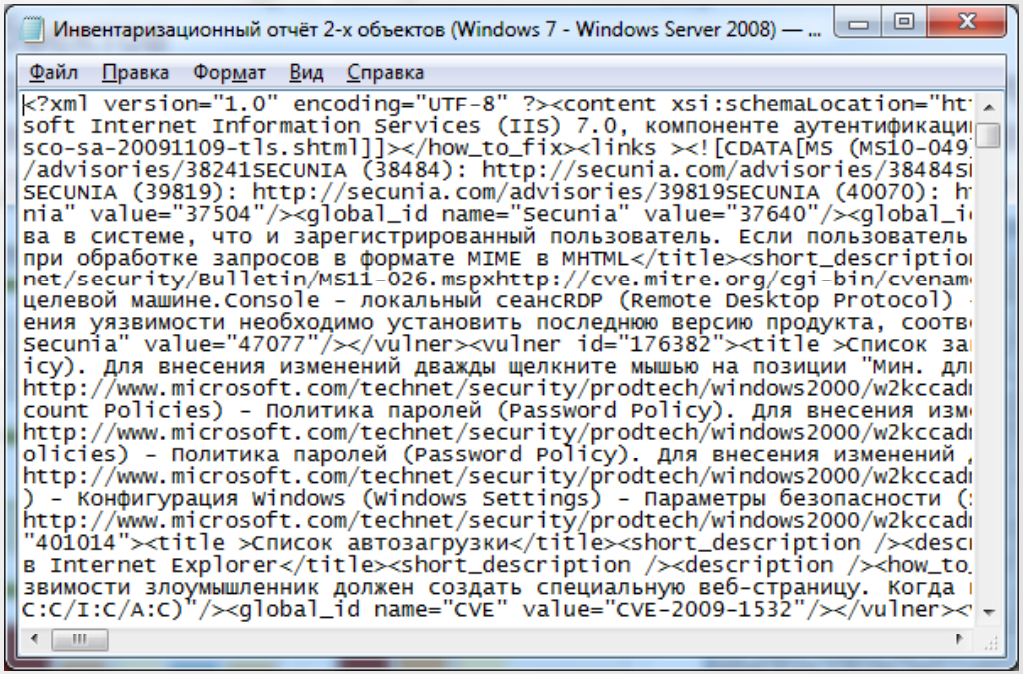
Е.С. Новикова

СПбГЭТУ «ЛЭТИ»

РусКрипто'2014, 25-28 марта 2014 г.

Визуальный анализ данных

Отчет о выявленных уязвимостях системы OSSIM



Отчет о выявленных уязвимостях сканера уязвимостей MAXPatrol

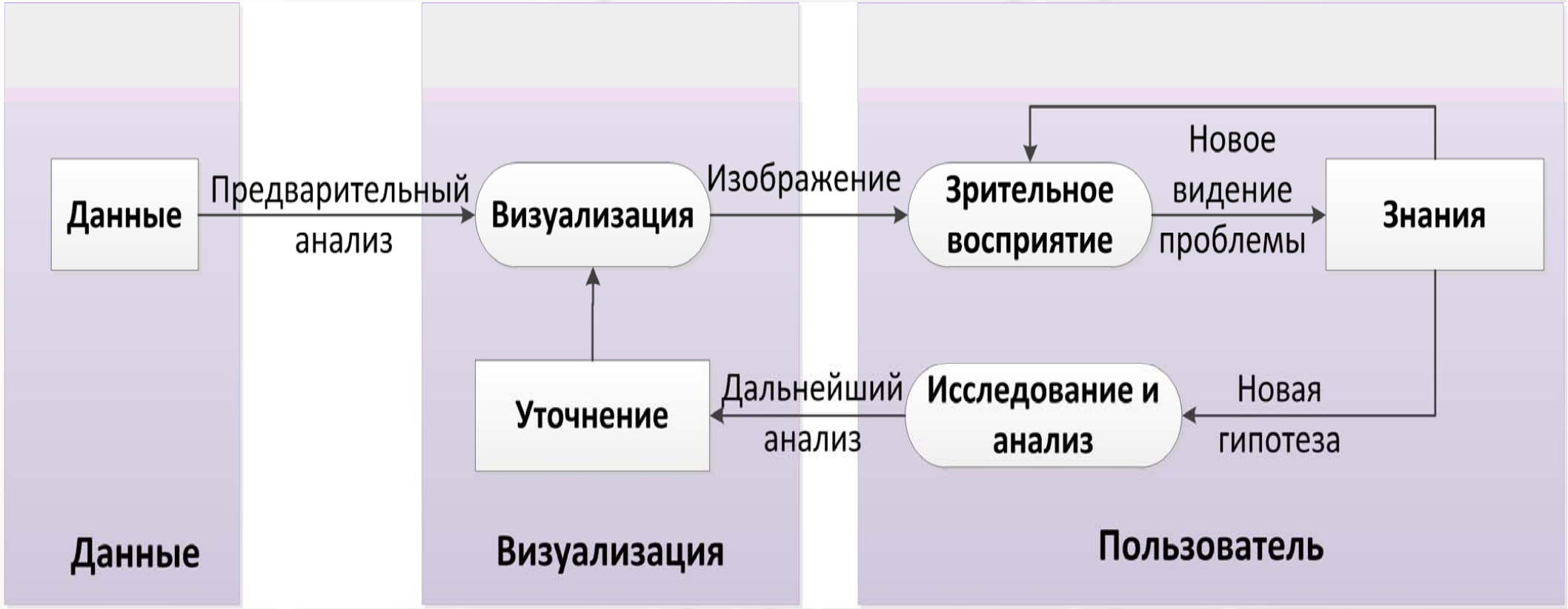
План доклада

- Введение
- Методы, модели и методики визуализации
- Визуализация в SIEM-системах
- Представление сетевого трафика
- Представление политик безопасности и правил сенсоров безопасности
- Представление уязвимостей и событий безопасности
- Визуализация графов атак
- Подсистема визуализации для моделирования атак и оценки защищенности
- Заключение

Объект и предмет исследования

- В настоящей работе анализируются различные модели визуализации, используемые для решения задач информационной безопасности, и представляется ряд моделей, предложенных для аналитической обработки в разрабатываемой SIEM-системе
- В многих ситуациях использование простых способов графического представления данных, таких как гистограммы, линейные графики, предпочтительнее, поскольку они способны мгновенно передать информацию пользователю, указать на возможные аномалии
- Однако они не позволяют исследовать причины их появления, поэтому будут рассмотрены сложные и достаточно необычные модели визуализации многомерных данных, описывающих состояние безопасности информационной системы

Схема процесса визуального анализа данных [Keim et al., 2008]



Классы моделей, методик и методов графического представления данных

1. **Научная визуализация (scientific visualization)** - методики визуализации характеризуются использованием реалистичных 3D-моделей, сложных текстур и поверхностей, механизмов анимации для отражения динамики изменения объекта во времени [Keim et al., 2008; Spencer, 2001]

2. **Инфографика (визуализация информации, information visualization)** - графическое представление абстрактных данных в интуитивно понятном виде. Оно позволяет отобразить данные следующих типов [Andrews, 2011; Plaisant, 2005; Harris, 1999]

Типы данных, используемые в инфографике

- простые, стандартные 2-х и 3-х мерные модели (гистограммы, линейные графики, секторные диаграммы и т.д.)
- геометрические преобразования (графики рассеивания, графы на параллельных координатах и т.д.), позволяющие отобразить многомерные данные в двухмерном пространстве
- пиктограммы (лица Чернова [Chernoff, 1973], глифы, пиктограммы в виде звезд, цифровых приборов и др.), в основе которых лежит преобразование свойств объектов в свойства пиктограмм
- пиксельное представление, в котором каждый пиксель используется для кодирования значения определенного свойства объекта. Особенностью данных моделей визуализации заключается в способности графически представлять большие массивы данных
- иерархические графические модели (карты деревьев, [Inselberg&Dimsdale, 1990]

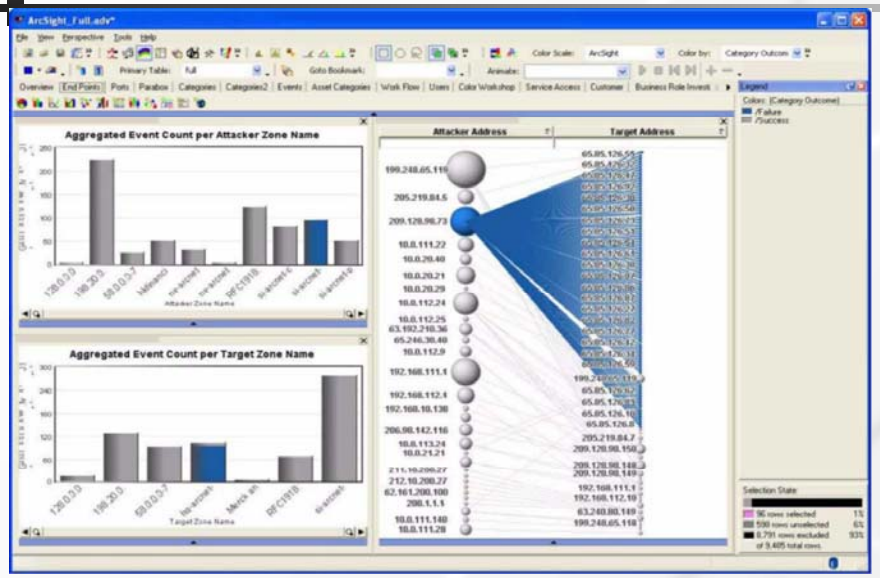
Примеры моделей представления данных в информационной безопасности

- **Мониторинг периметра сети:**
  - круговая диаграмма, представляющая наиболее активные хосты-приемники и хосты-получатели
  - гистограмма наиболее часто используемых сервисов
  - граф коммуникаций, отражающих потоки между хостами
  - карта деревьев (treemap), отражающая частоту использования портов различными хостами
  - графы вида «отправитель-сообщение-получатель» и т.д.
- **Контроль деятельности пользователей:**
  - графы вида «пользователь-деятельность» и «пользователь-сервер»
  - гистограмма, отражающая число документов, просмотренных пользователям
- **Отображение уровня защищенности:**
  - 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

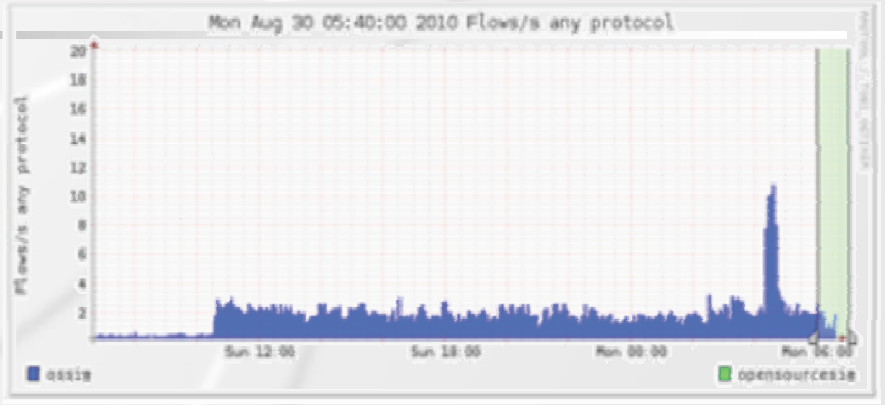
План доклада

- Введение
- Методы, модели и методики визуализации
- **Визуализация в SIEM-системах**
- Представление сетевого трафика
- Представление политик безопасности и правил сенсоров безопасности
- Представление уязвимостей и событий безопасности
- Визуализация графов атак
- Подсистема визуализации для моделирования атак и оценки защищенности
- Заключение

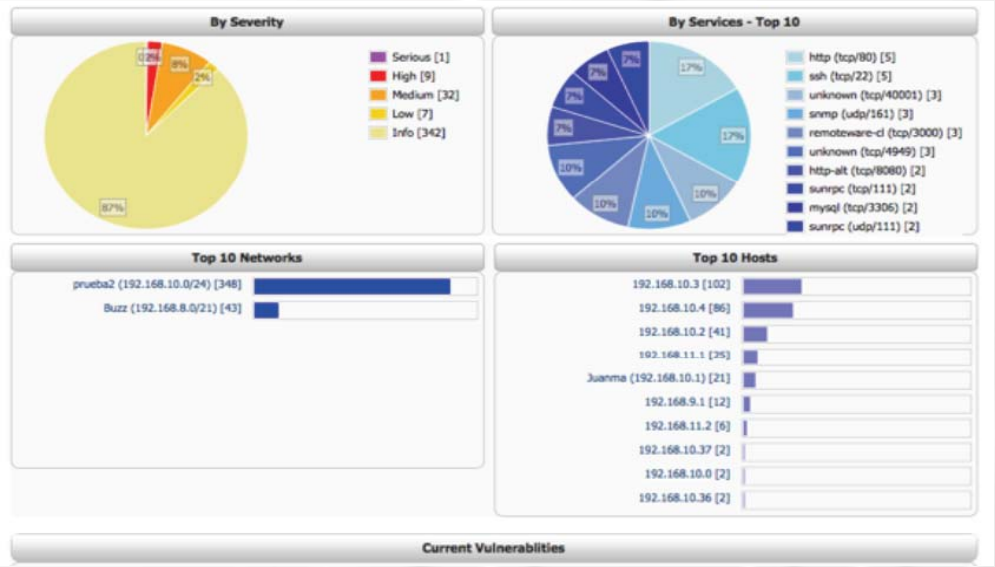
Визуализация в SIEM-системах



Arcsight: обнаружение атак



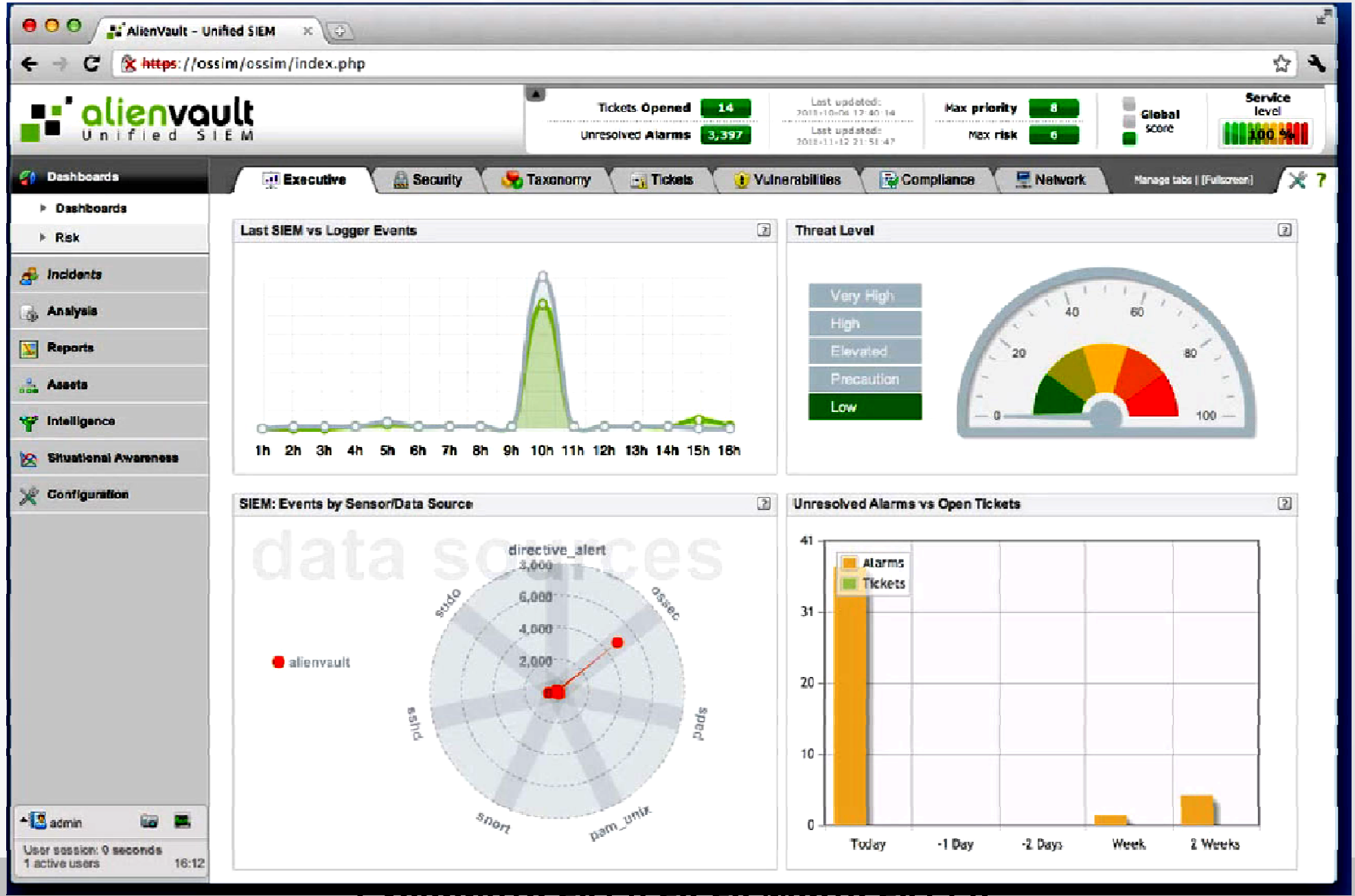
OSSIM: визуализация сетевого трафика



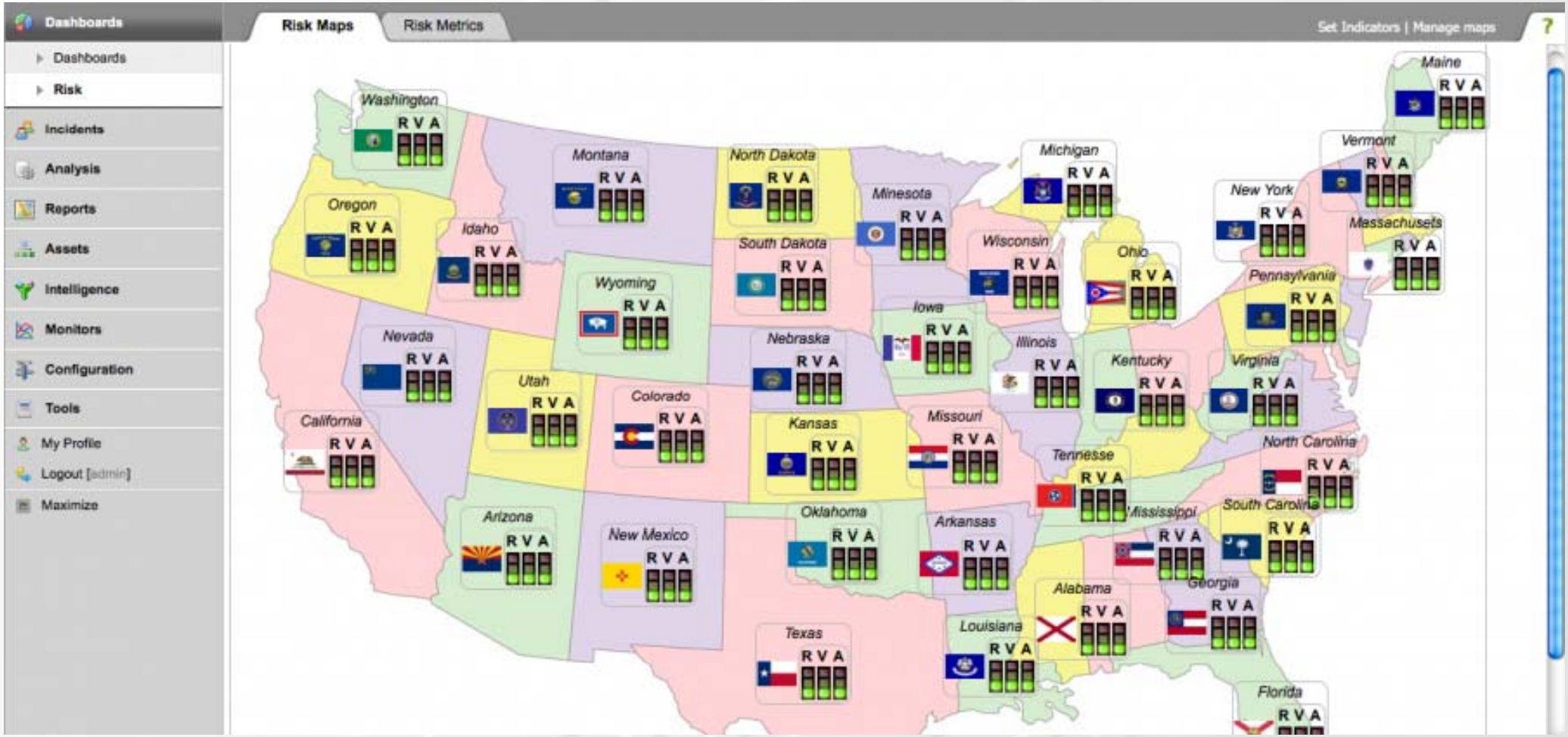
OSSIM: отчет об уязвимостях

TSIEM: представление правил доступа

OSSIM: панель управления



OSSIM: карта рисков

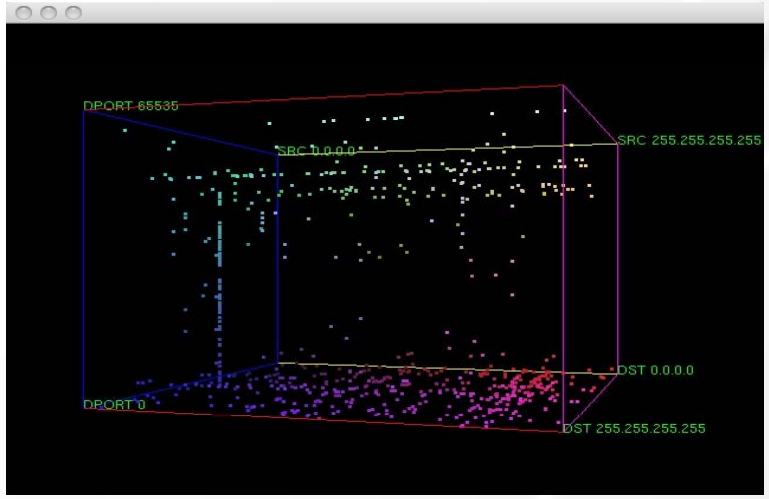


План доклада

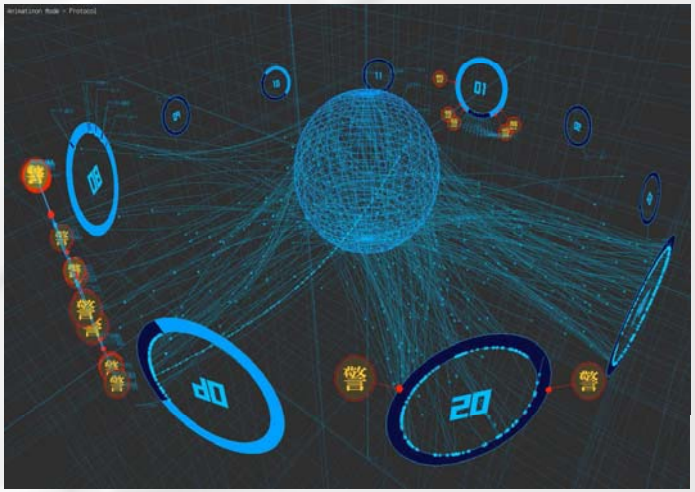
- Введение
- Методы, модели и методики визуализации
- Визуализация в SIEM-системах
- **Представление сетевого трафика**
- Представление политик безопасности и правил сенсоров безопасности
- Представление уязвимостей и событий безопасности
- Визуализация графов атак
- Подсистема визуализации для моделирования атак и оценки защищенности
- Заключение

Модели представления сетевого трафика

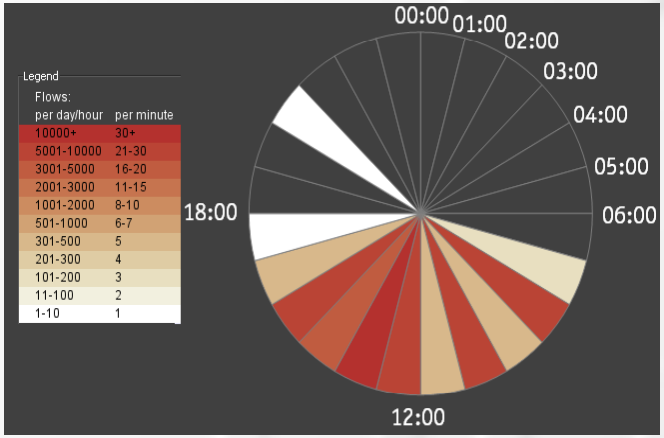
3D-график рассеивания [1]



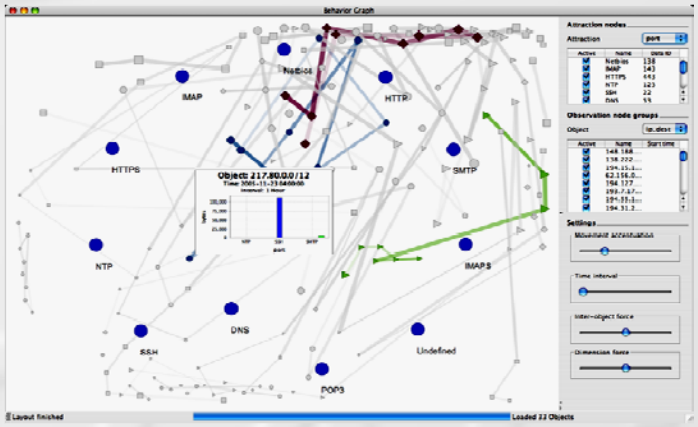
3D-визуализация системы Deadalus-Viz [2]



ClockView [3]



Граф, отражающий поведение хостов [4]



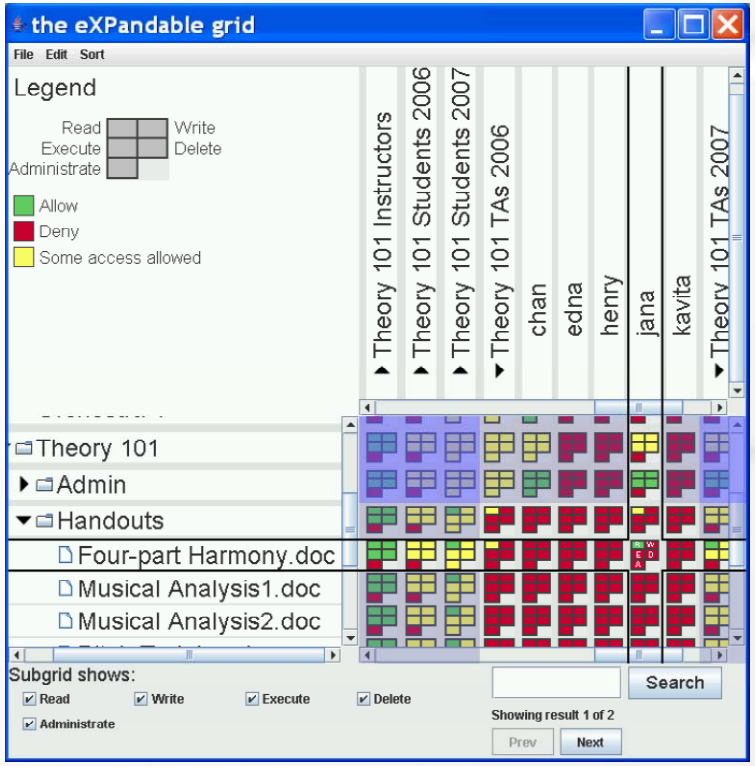
[1] Lau S. The spinning cube of potential doom. Communications of the ACM, vol. 47(6), 2004. P.24-26.
[2] Inoue D., Eto M., Suzuki K., Suzuki M., Nakao K.. DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System". VizSec '12, October 15, Seattle, WA, USA , 2012.
[3] Kintzel C., Fuchs J., Mansmann F. Monitoring Large IP Spaces with ClockView". VizSec'11, 2011.
[4] Mansmann F., Meier L., Keim D.A. Visualization of Host Behavior for Network Security. VizSEC'07, Sacramento, USA. 2007.

План доклада

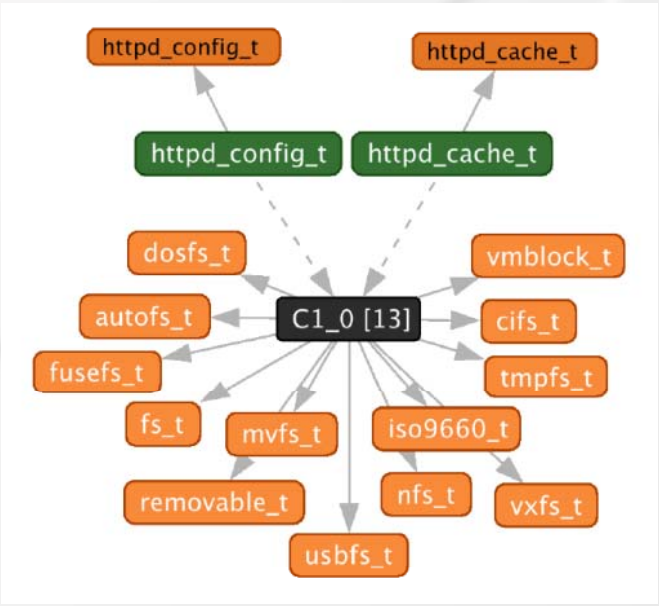
- Введение
- Методы, модели и методики визуализации
- Визуализация в SIEM-системах
- Представление сетевого трафика
- **Представление политик безопасности и правил сенсоров безопасности**
- Представление уязвимостей и событий безопасности
- Визуализация графов атак
- Подсистема визуализации для моделирования атак и оценки защищенности
- Заключение

Представление политик безопасности и правил сенсоров безопасности

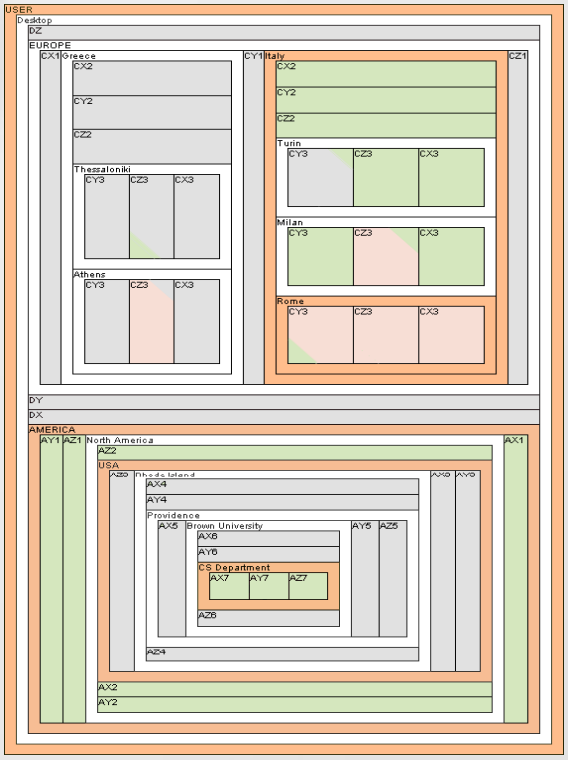
Матричное представление прав доступа к ресурсам [1]



Представление прав доступа к ресурсам в виде графа [2]



Представление прав доступа к ресурсам в виде карты деревьев [3]



[1] Reeder R. W., Bauer L., Cranor L. F., et al. Expandable grids for visualizing and authoring computer security policies. *SIGCHI Conference on Human Factors in Computing Systems* (CHI '08). ACM, New York, NY, USA, 2008.

[2] Marouf S., Shehab M. SEGrapher: Visualization-based SELinux PolicyAnalysis. 4th Symposium on Configuration Analytics and Automation (SAFECONFIG), 2011.

[3] Heitzmann A., Palazzi B., Papamanthou C., Tamassia R. Effective Visualisation of File System Access-Control. 5th international workshop on Visualisation for Computer Security (VizSec'08), LNCS, Vol.5210, Springer-Verlag, Berlin, Heidelberg, 2008.

Представление правил межсетевых экранов

Визуализация в виде "солнечные лучи" (Sunburst) [1]

PolicyViz [2]

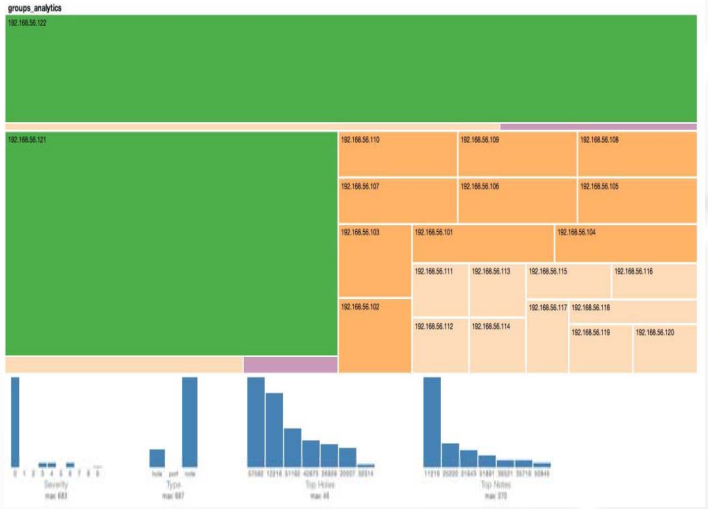
[1] Mansmann F., Göbel T., Cheswick W. Visual Analysis of Complex Firewall Configurations. VizSec'12, October 15, 2012, Seattle, WA, USA, 2012.

[2] Tran T., Al-Shaer E., Boutaba R. PolicyVis: Firewall Security Policy Visualisation and Inspection. 21st Conference on Large Installation System Administration Conference (LISA'07), USENIX Association, Berkeley, CA, USA, 2007.

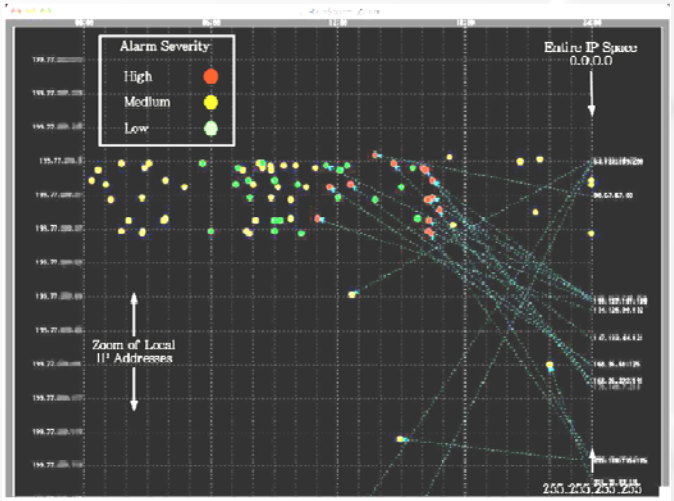
План доклада

- Введение
- Методы, модели и методики визуализации
- Визуализация в SIEM-системах
- Представление сетевого трафика
- Представление политик безопасности и правил сенсоров безопасности
- **Представление уязвимостей и событий безопасности**
- Визуализация графов атак
- Подсистема визуализации для моделирования атак и оценки защищенности
- Заключение

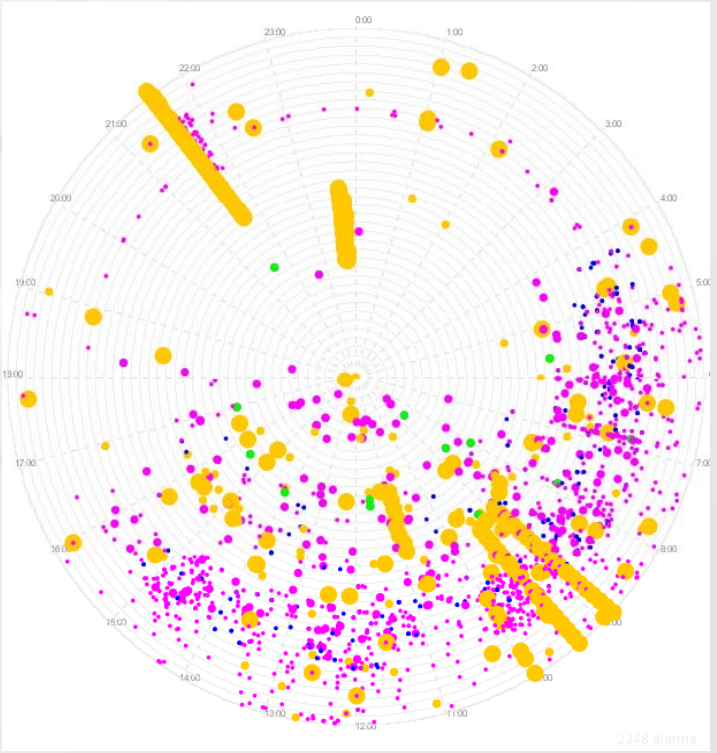
Представление уязвимостей и событий безопасности



Nv Tool [1]



IDS Rainstorm [2]



Спиральное представление событий безопасности [3]

[1] Harrison, L., Spahn, R., Iannacone, M., Downing, E., Goodall, J.R.: NV: Nessus Vulnerability Visualisation for the Web. Proc. of the VizSec'12, October 15 2012, Seattle, WA, USA (2012)

[2] Abdullah K., Lee C., et al. IDS Rainstorm: Visualizing ids alarms. IEEE Workshops on Visualization for Computer Security, 2005.

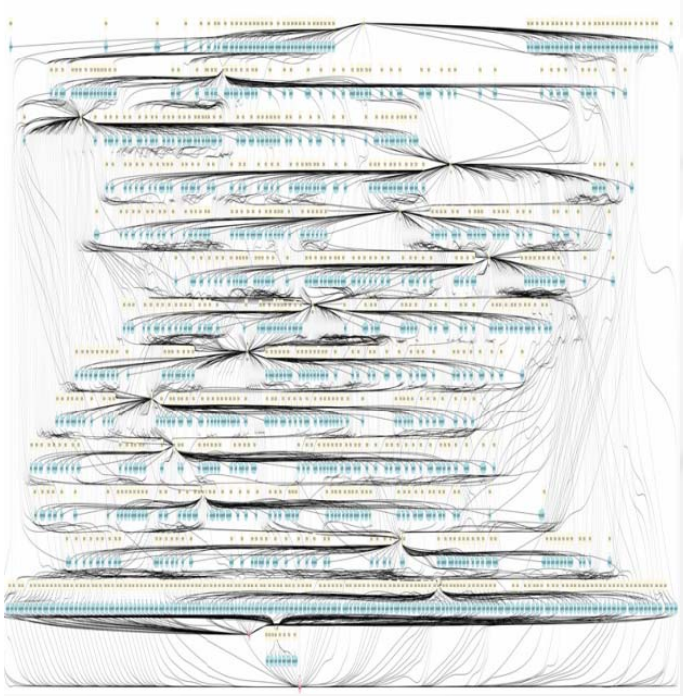
[3] Bertini E., Hertzog P., Lalanne D. SpiralView: Towards Security Policies Assessment through Visual Correlation of Network Resources with Evolution of Alarms. IEEE Symposium on Visual Analytics Science and Technology (VAST) 2007.

План доклада

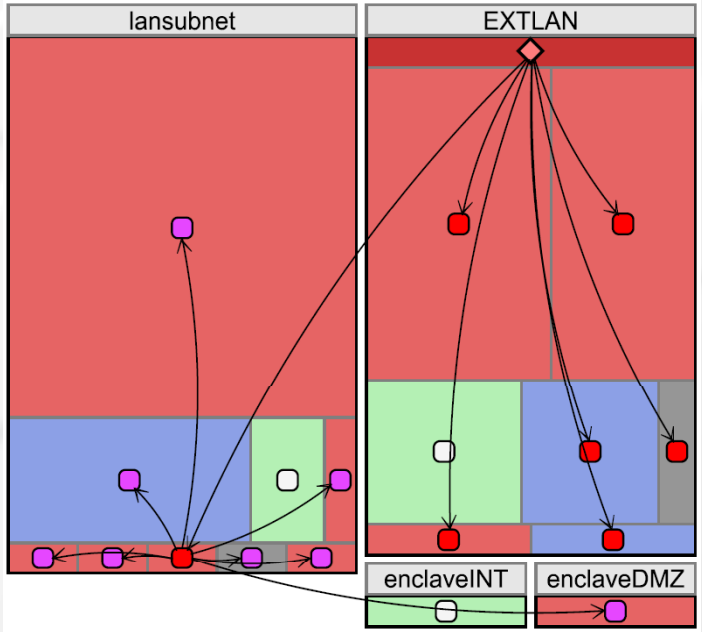
- Введение
- Методы, модели и методики визуализации
- Визуализация в SIEM-системах
- Представление сетевого трафика
- Представление политик безопасности и правил сенсоров безопасности
- Представление уязвимостей и событий безопасности
- **Визуализация графов атак**
- Подсистема визуализации для моделирования атак и оценки защищенности
- Заключение

Визуализация графов атак

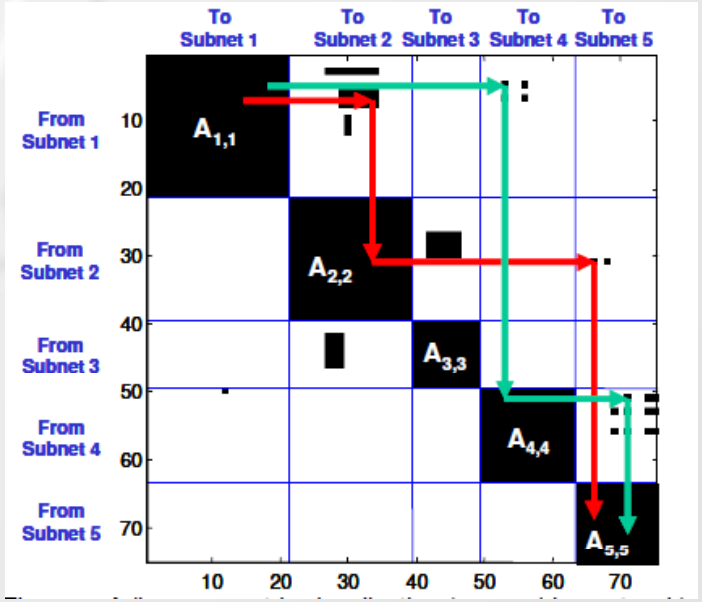
Использование графов [1]



Использование карт деревьев [2]



Использование матричного представления [3]



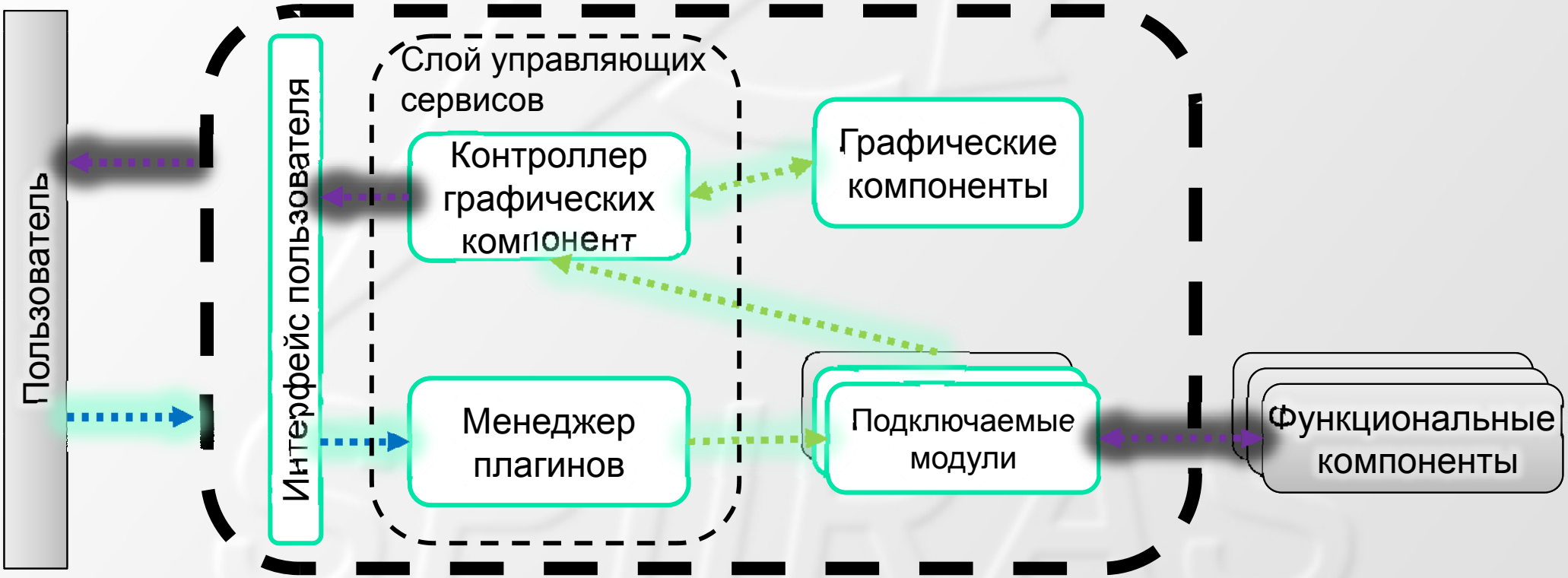
[1] Noel S., Jacobs M., Kalapa P., Jajodia S. Multiple Coordinated Views for Network Attack Graphs. IEEE Workshops on Visualisation for Computer Security, IEEE Computer Society, 2005.
[2] Williams L., Lippmann R., Ingols K. GARNET: A Graphical Attack Graph and Reachability Network Evaluation Tool. 5th International Workshop on Visualisation for Computer Security (VizSec'08), LNCS, Vol.5210, Springer-Verlag, 2008.
[3] Noel S., Jajodia S. Understanding Complex Network Attack Graphs through Clustered Adjacency Matrices. 21st Annual Computer Security Applications Conference (ACSAC'05). IEEE Computer Society, 2005.

План доклада

- Введение
- Методы, модели и методики визуализации
- Визуализация в SIEM-системах
- Представление сетевого трафика
- Представление политик безопасности и правил сенсоров безопасности
- Представление уязвимостей и событий безопасности
- Визуализация графов атак
- **Подсистема визуализации для моделирования атак и оценки защищенности**
- Заключение

Архитектура подсистемы визуализации

- Функциональная расширяемость
- Гибкая связь между компонентами
- Независимая разработка модулей



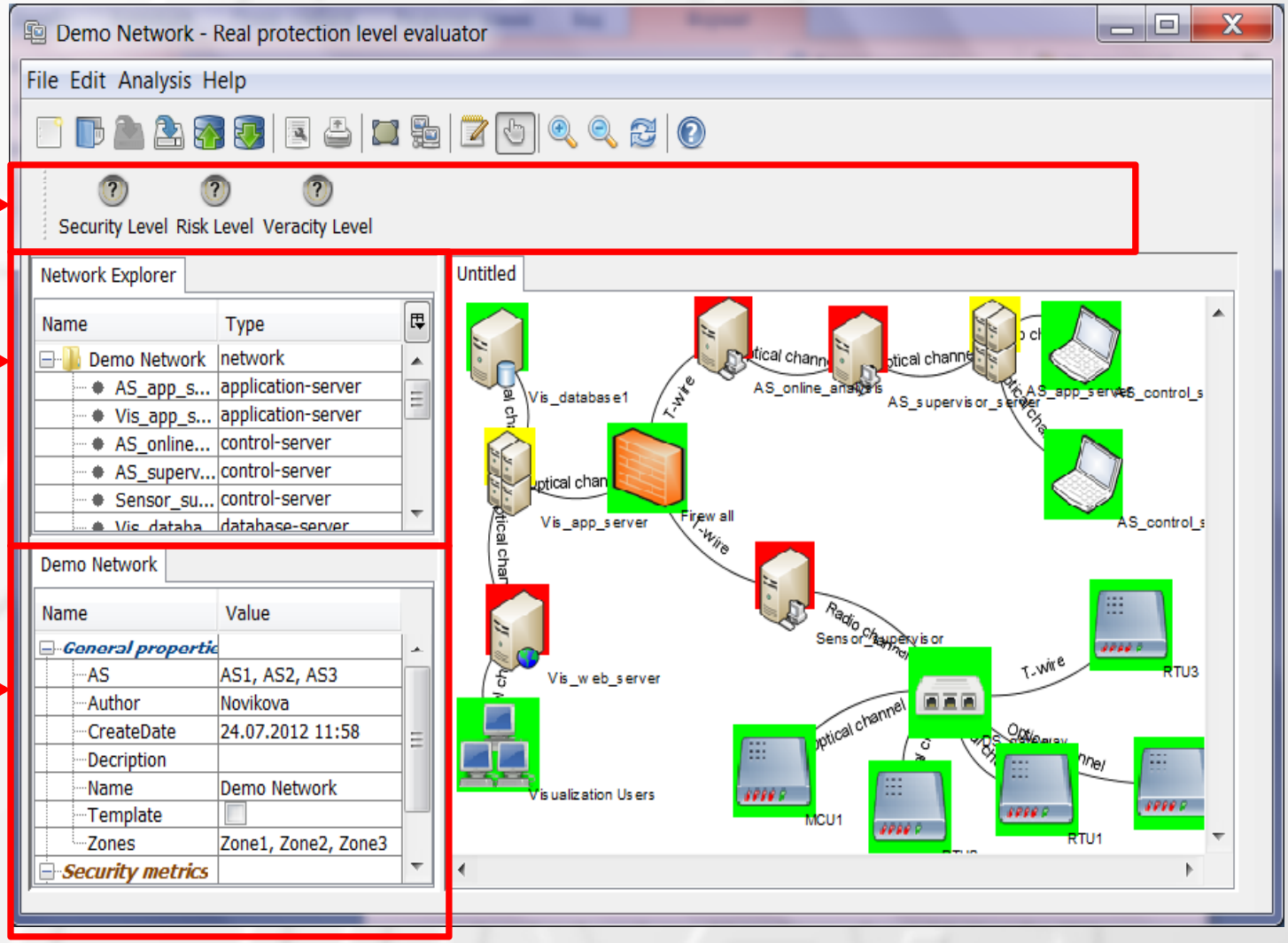
Графический интерфейс модуля моделирования атак и оценки защищенности

Главное окно

Основные метрики

Редактор структуры сети

Редактор свойств объектов сети



Элементы графического интерфейса компонента

Метрики безопасности – семафор

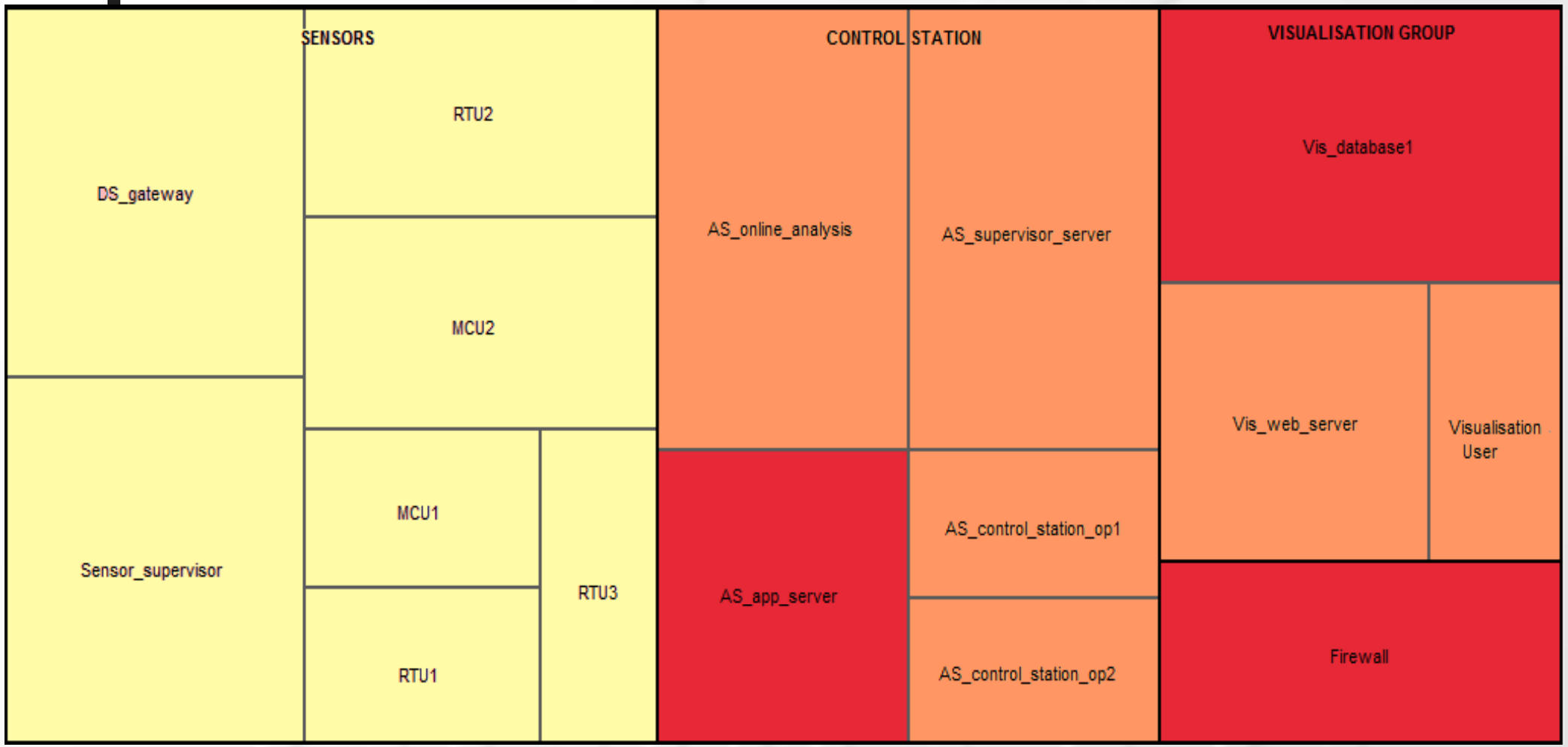
Security Level

- Not defined
- Green (Network is secured)
- Yellow (Low Criticality)
- Orange (Medium Criticality)
- Red (High Criticality)

Пиктограммы, использующие для отображения графа атак

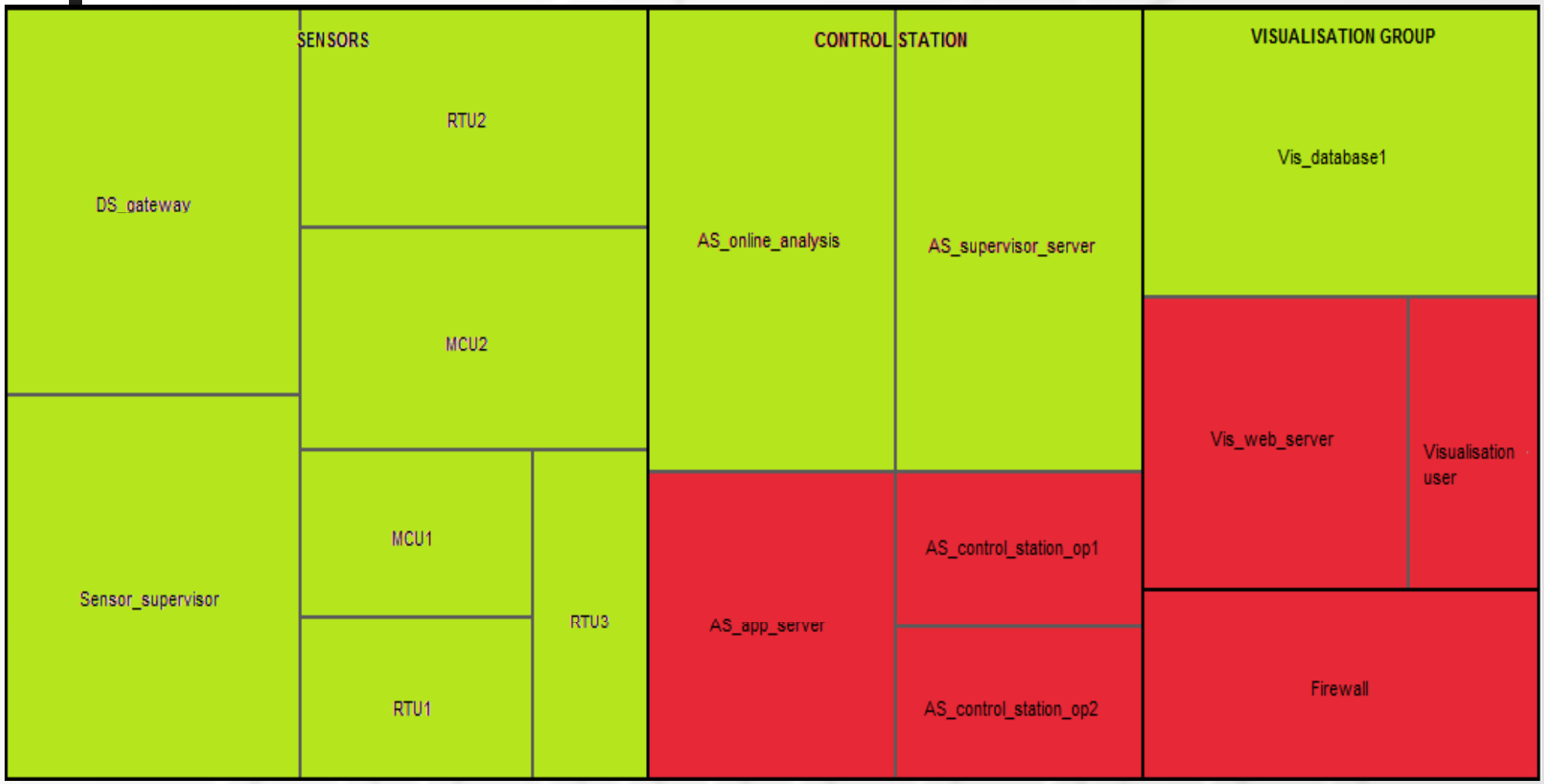
- Исходное положение нарушителя
- Применение атомарного действия
- Применение сценария без использования уязвимости
- Эксплуатация уязвимости

Отчет об уязвимостях на основе карт деревьев



Каждый вложенный прямоугольник отображает хост. Размер прямоугольника определяется задаваемой пользователем критичностью хоста. Цвет используется для обозначения серьезности уязвимости, обнаруженной на данном хосте.

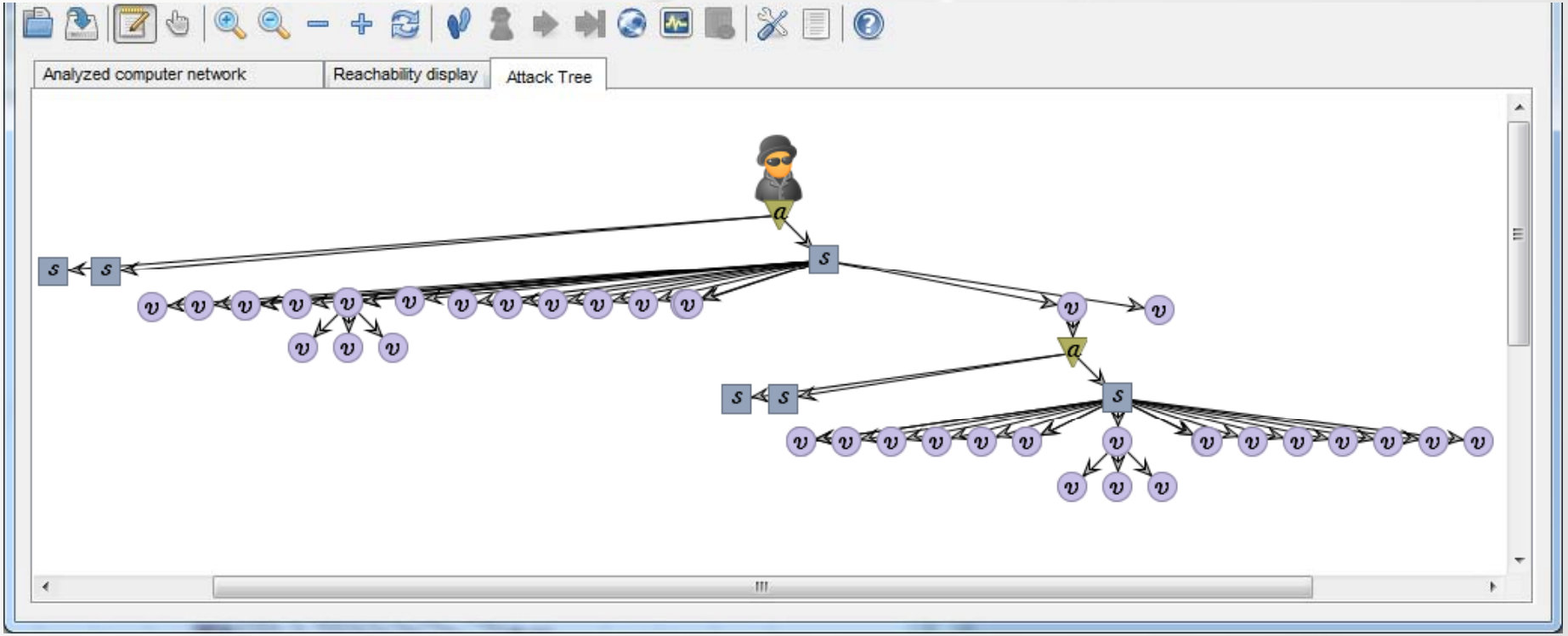
Анализ достижимости атаки на основе карт деревьев



Размер вложенных прямоугольников соответствует уровню критичности, а цвет отражает состояние хоста (красный - хост достигаем нарушителем, зеленый - нарушитель не может получить доступ к хосту.

Представление графов атак (1/2)

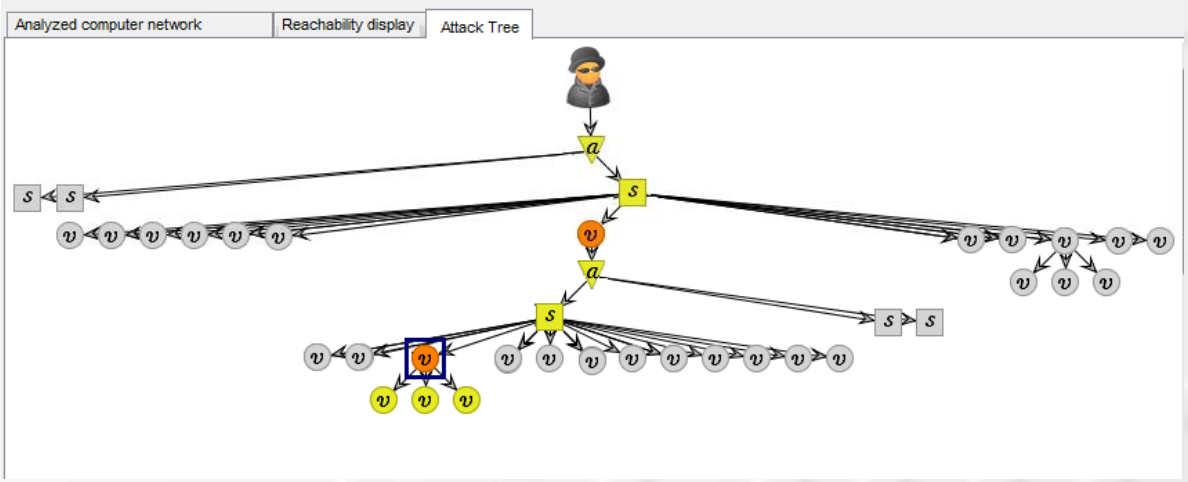
Обозначение	Описание
	Исходное положение нарушителя
	Специфическое атакующее действие
	Сценарий, не использующий уязвимости
	Атакующее действие, использующее уязвимость



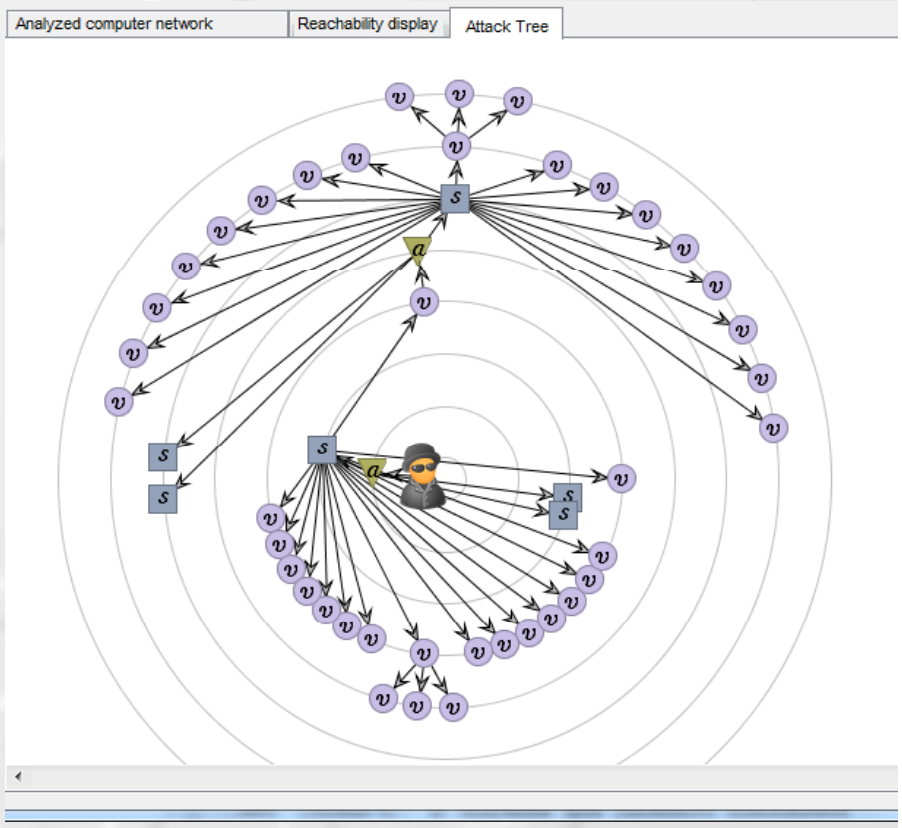
Представление графов атак (2/2)

Способы взаимодействия с графическим представлением графов атак:

- Управление представлением графа (древовидное и радиальное)
- Геометрическое масштабирование
- Семантическое масштабирование (агрегирование узлов графа)
- Детали по требованию
- Подсветка и связывание



Древовидное представление и эффект подсветки и связывания



Радиальное представление

План доклада

- Введение
- Методы, модели и методики визуализации
- Визуализация в SIEM-системах
- Представление сетевого трафика
- Представление политик безопасности и правил сенсоров безопасности
- Представление уязвимостей и событий безопасности
- Визуализация графов атак
- Подсистема визуализации для моделирования атак и оценки защищенности
- **Заключение**

Основные результаты работы

- Представлены результаты исследования механизмов визуализации информации о безопасности компьютерных систем. Выявлены основные тенденции в графическом представлении данных для решения различных задач по обеспечению информационной безопасности.
- Предложена архитектура компонента визуализации, учитывающая результаты проведенного исследования и позволяющая легко расширять функциональность приложения. Данная архитектура позволяет использовать различные технологии для графического отображения данных.
- Описан программный компонент визуализации, предоставляющий графический интерфейс для моделирования атак и оценки защищенности.

Направления дальнейших исследований

- Расширение функциональности компонента визуализации за счет проектирования панели управления, предоставляющей общую информацию о результатах моделирования, развития механизмов масштабируемости генерируемых графических изображений, а также реализации новых форм визуализации данных.

Контактная информация

Котенко Игорь Витальевич (СПИИРАН)
ivkote@comsec.spb.ru
http://comsec.spb.ru/kotenko/

Благодарности

- Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт №2.2) и проекта ENGENSEC программы Европейского Сообщества TEMPUS.

РОССИЙСКАЯ АКАДЕМИЯ НАУК