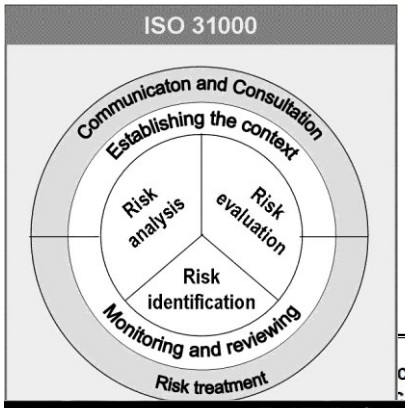
Объективизация оценки рисков сложных информационных систем

Что нам стоит дом построить!

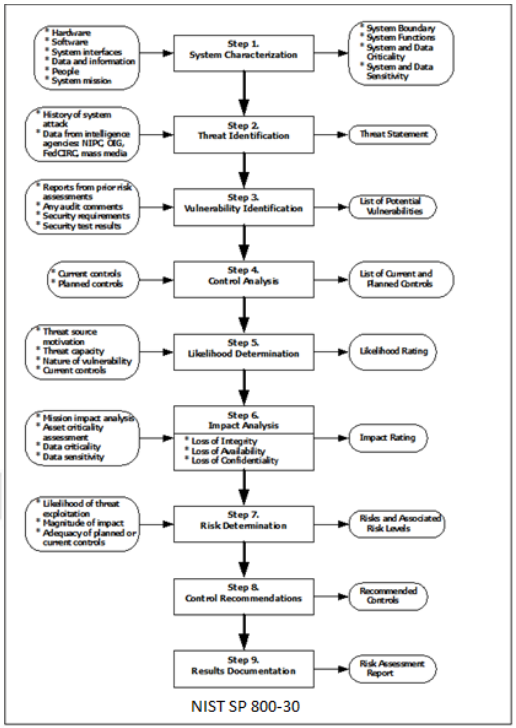
Оценка рисков является неотъемлемой частью практически всех современных стандартов по ИБ

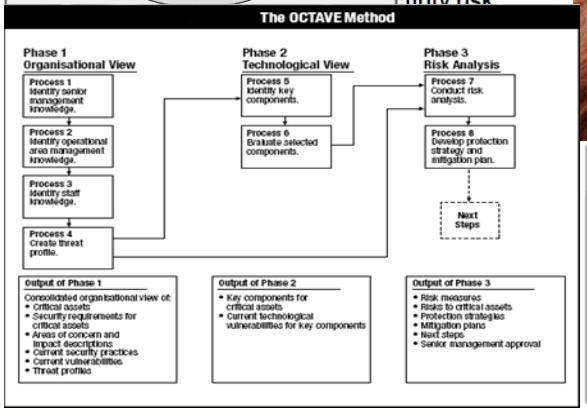


ISO/IEC 27005

Second edition
2011-06-01

curity
curity risk





Однако от это она **не стала объективнее** и чаще всего её результаты **НЕ несут существенной информационной новизны**

Вечная дилемма моделирования

Мало деталей

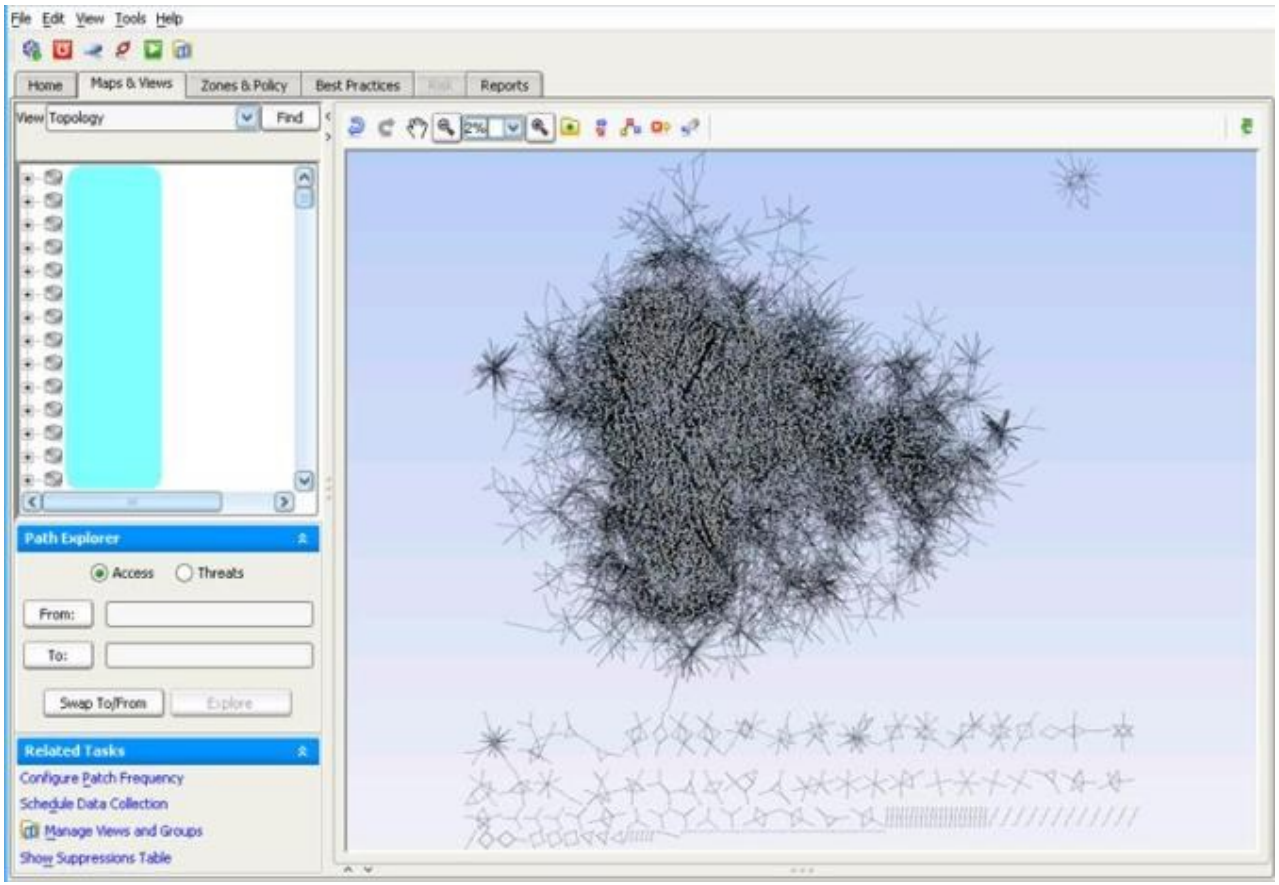
“Высокоуровневый” анализ рисков практически не даёт результатов обладающих информационной новизной

Очень подробно

“Детальный” анализ рисков либо не завершается никогда, либо занимает слишком много времени и усилий, соответственно оценка рисков производится очень редко

Результаты анализа рисков практически **никогда не применяются** для **принятия решений по оперативным вопросам ИБ**.

Есть ли понимание состояния ИБ?

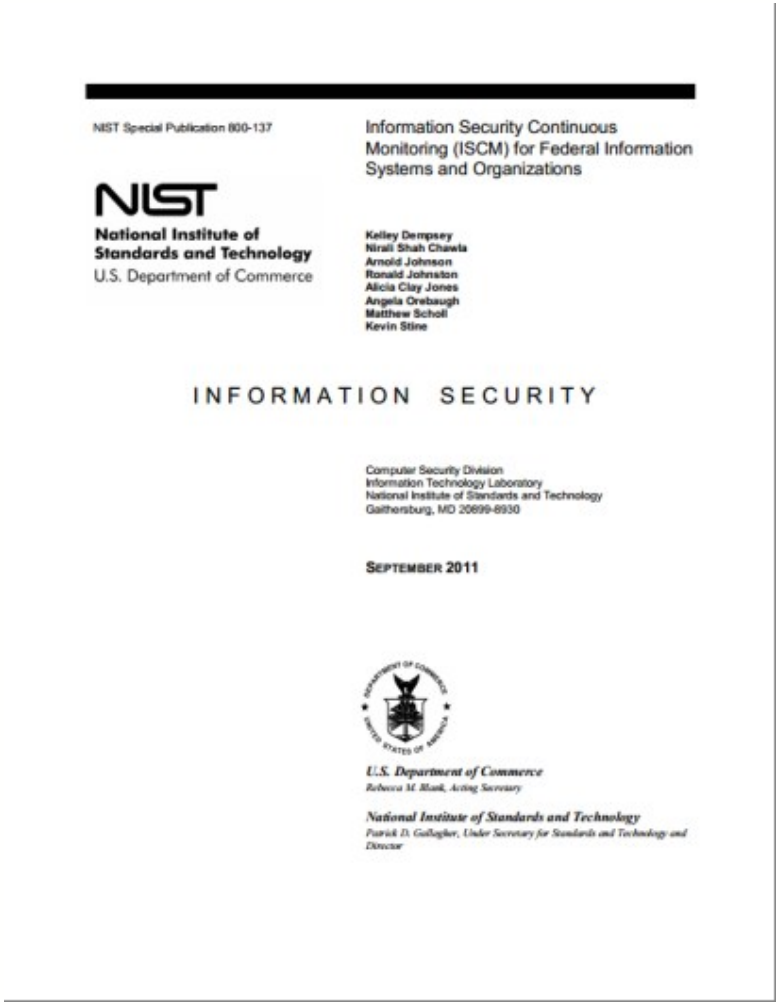


В крупных организациях практически нет людей осознающих полную картину работы информационной системы. Эта картина зачастую слишком сложна для восприятия одним человеком.

Эффективна ли оценка рисков на основе “лучших практик”?

*В **больших** организациях сложность и изменчивость ИТ-инфраструктуры и бизнес-процессов делают любые **статичные требования** и **периодические мероприятия** по обеспечению ИБ практически **бесполезными***

Мировые тенденции



NIST Special Publication 800-137

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Kelley Dempsey
Nirali Shah Chawla
Arnold Johnson
Ronald Johnston
Alicia Clay Jones
Angela Orebaugh
Matthew Scholl
Kevin Stine

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

SEPTEMBER 2011

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

Американский институт стандартов – NIST в 2011 принял кардинально новый для всей отрасли ИБ стандарт по Системам Непрерывного Мониторинга Состояния ИБ - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST SP 800-137)

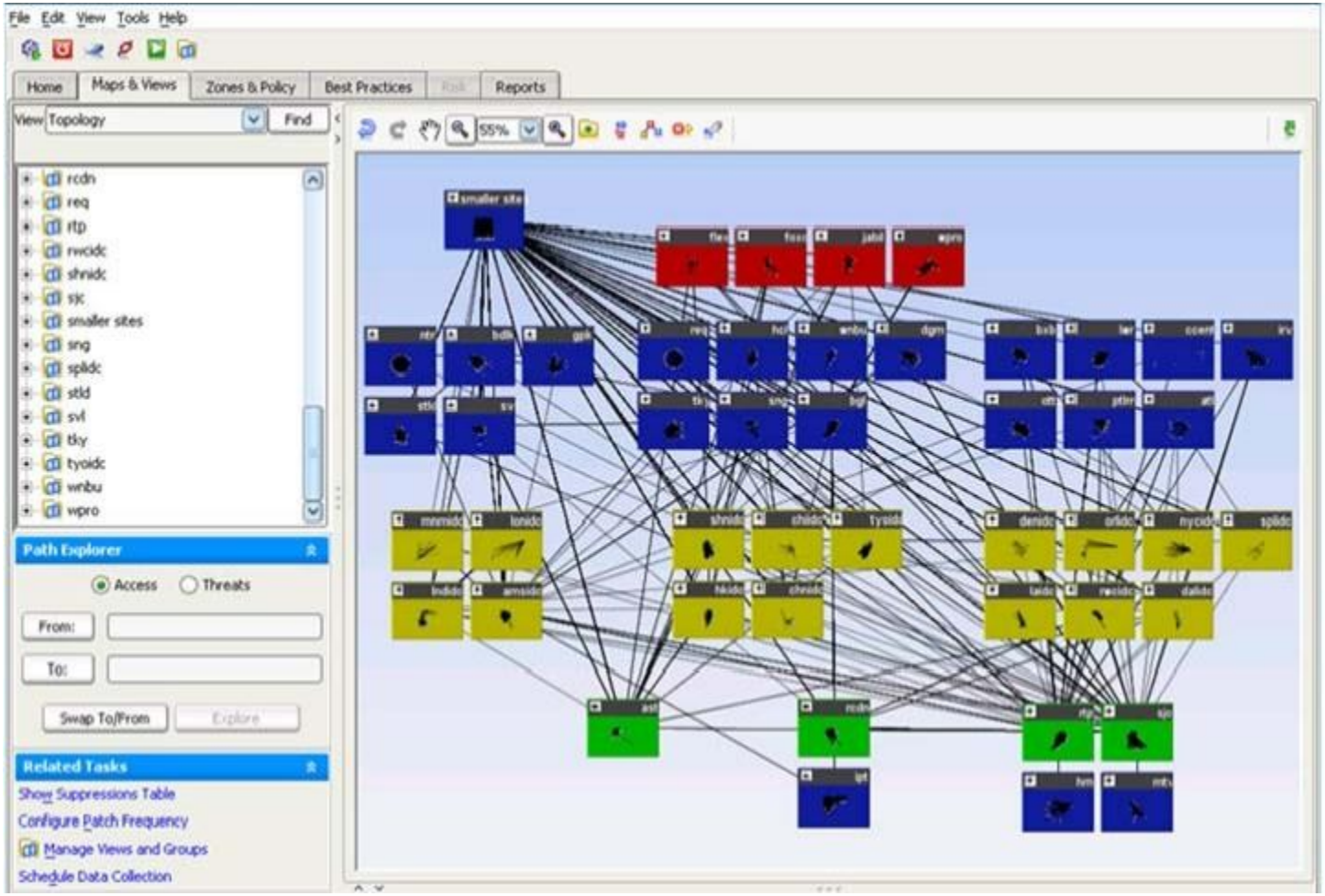
Мировые тенденции

Основной новизной стандарта является требование создания единой системы решающей следующие задачи:

- **Ведение и разбор всех угроз и потенциально опасной деятельности;**
- **Оценка работы всех защитных мер;**
- **Сбор, сопоставление и анализ всей связанной с обеспечением безопасности информации;**
- **Поддержание ситуационной осведомленности всех уровней управления в масштабе всей организации;**
- **Активное участие в процессе управления рисками высших должностных лиц.**

Эффективная система должна работать в режиме реального времени

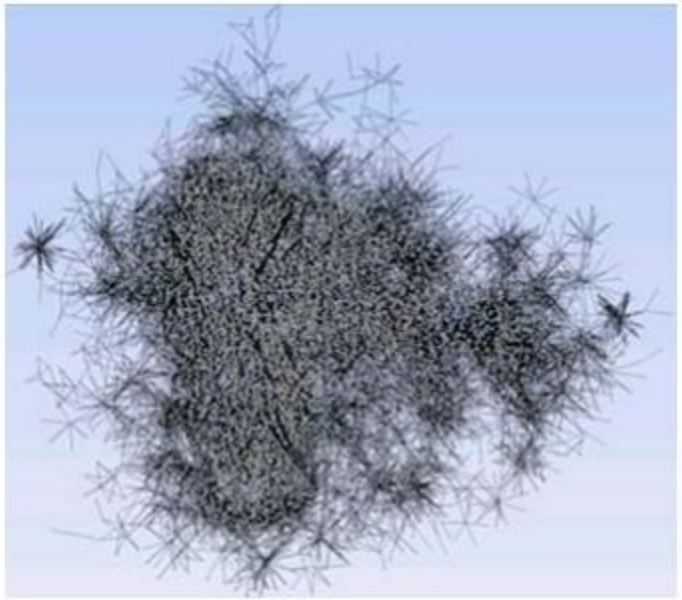
Что хочется получить:
Вид сети –
после обработки в RedSeal



В итоге получаем:

Сегментация сети с учетом фактического расположения ее элементов и взаимосвязей между ними.

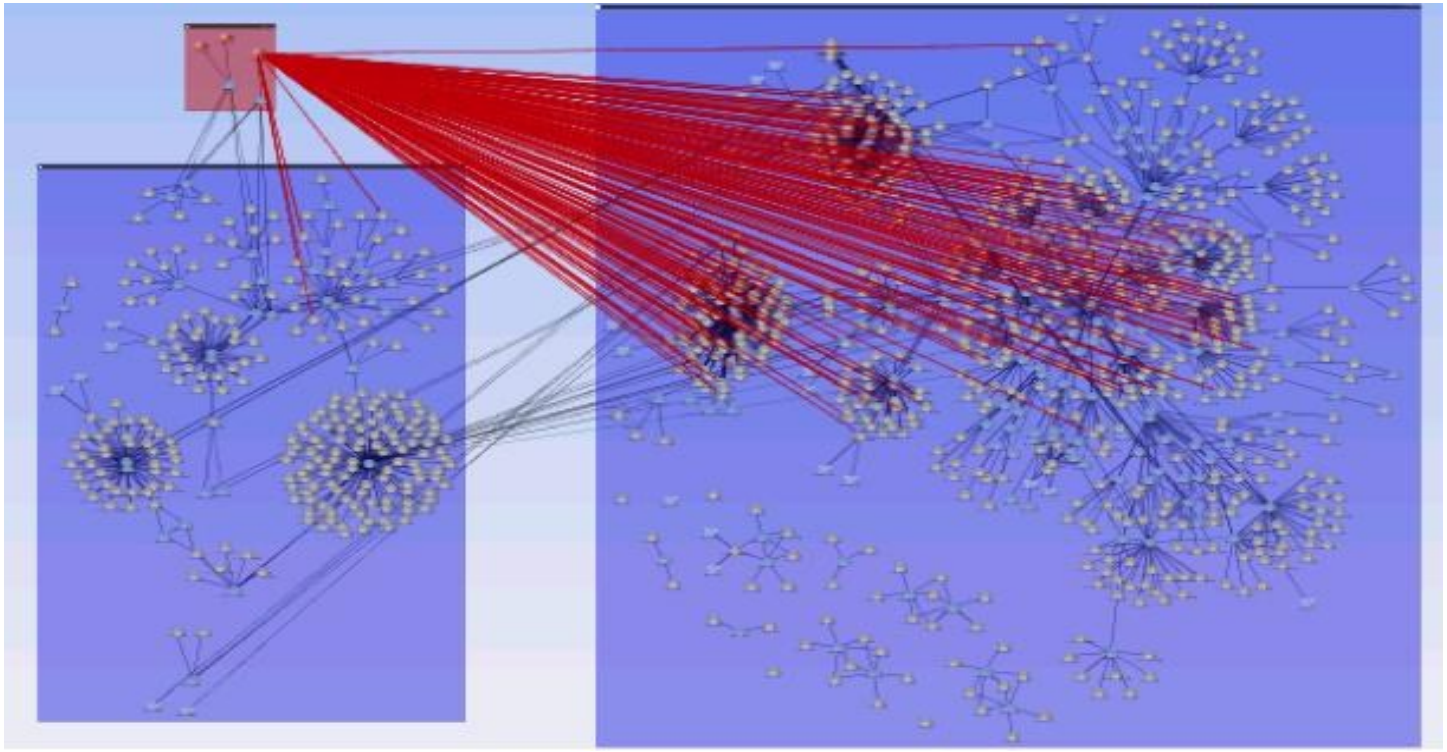
Before:



After:

Моделирование векторов атак

RedSeal позволяет провести моделирование векторов атак, исходящих из конкретных подсетей и направленных на конкретные серверы, использующих реально обнаруженные уязвимости, учитывая сетевую топологию и правила фильтрации трафика.



Моделирование векторов атак формирует критерии для обнаружения свидетельств существования реальных атак

"сырые" данные/логи

Критерии атак

splunk>

RedSeal Analytics Engine

Коннекторы к устройствам и узлам

Сетевые устройства

Juniper Networks
CITRIX
F5
Check Point Software Technologies
Cisco
Brocade

Сканеры

Rapid7
nCircle
McAfee
Qualys
Tenable Network Security
Nessus
MaxPatrol

CMDB

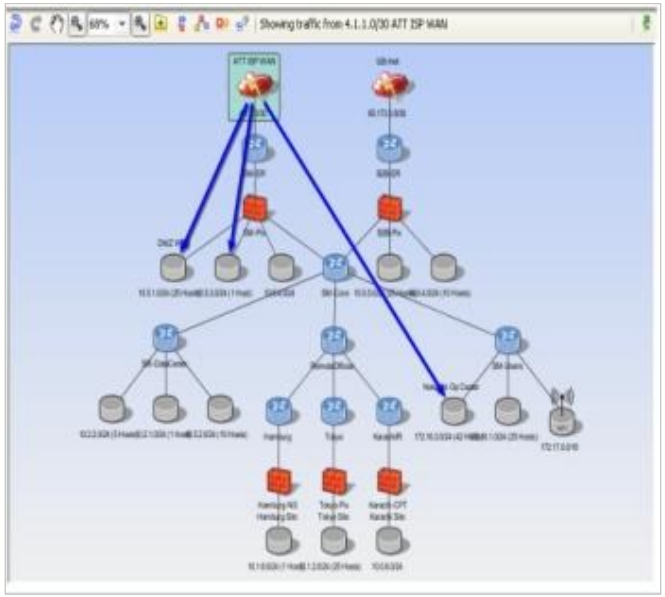
Cisco
HP
solarwinds
tripwire

Что достигаем

Использование технологии SPM позволяет достичь баланса затрат усилий/времени на оценку рисков, объективности и своевременности

Что достигаем

- ✓ Наличия достоверных данных о практически реализуемых векторах атак;
- ✓ Свидетельств того, что события атак уже происходили;
- ✓ Прозрачности картины возникновения и развития атаки в сети;
- ✓ Объективной оценки уровня опасности конкретных векторов атак и уязвимостей;
- ✓ Чёткого прогноза последствий внесения конкретных изменений в правила сетевого доступа;
- ✓ Повышение прозрачности и видимости инфраструктуры ИБ и всей информационной системы в целом;
- ✓ Объективизации результатов оценки рисков.



Внимание!

Презентация уже закончилась!