SCADA Hacking for Dummies

Piotr Linke
Security Engineer for EE

Who doesn’t like these conferences!? my wife…

SOURCEfire
daptive Intrusion Detection and Prevention Systems
Snort®-based rules
Zero-day threat protectior
99% event reduction
Centralised management
24/7 passive network disco
Automated IPS tuning
Real-time policy complianc
Security for virtual environn
ConfidEncE

Agenda

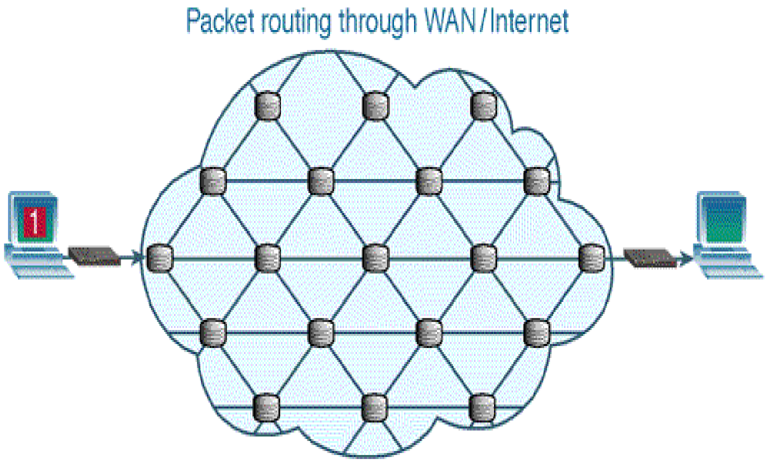
- Snort and Sourcefire
- What we should know about SCADA
- SCADA model for our demo
- Live presentation
- Two words about the NextGen IPS

About Sourcefire

- Founded in 2001 by Snort Creator, **Martin Roesch**, CTO
- Polska: Krzysztof Rocki, Michał Ceklarz
- FY2010 Revenue: $130.6M
- 12 offices worldwide, 380 employees
- Over 4000 commercial/enterprise/government customers
- #1 in IPS Detection by NSS Labs (96.7% default)
- Recognized by Forbes as Fastest-Growing company in Security (2011)
- NASDAQ: FIRE

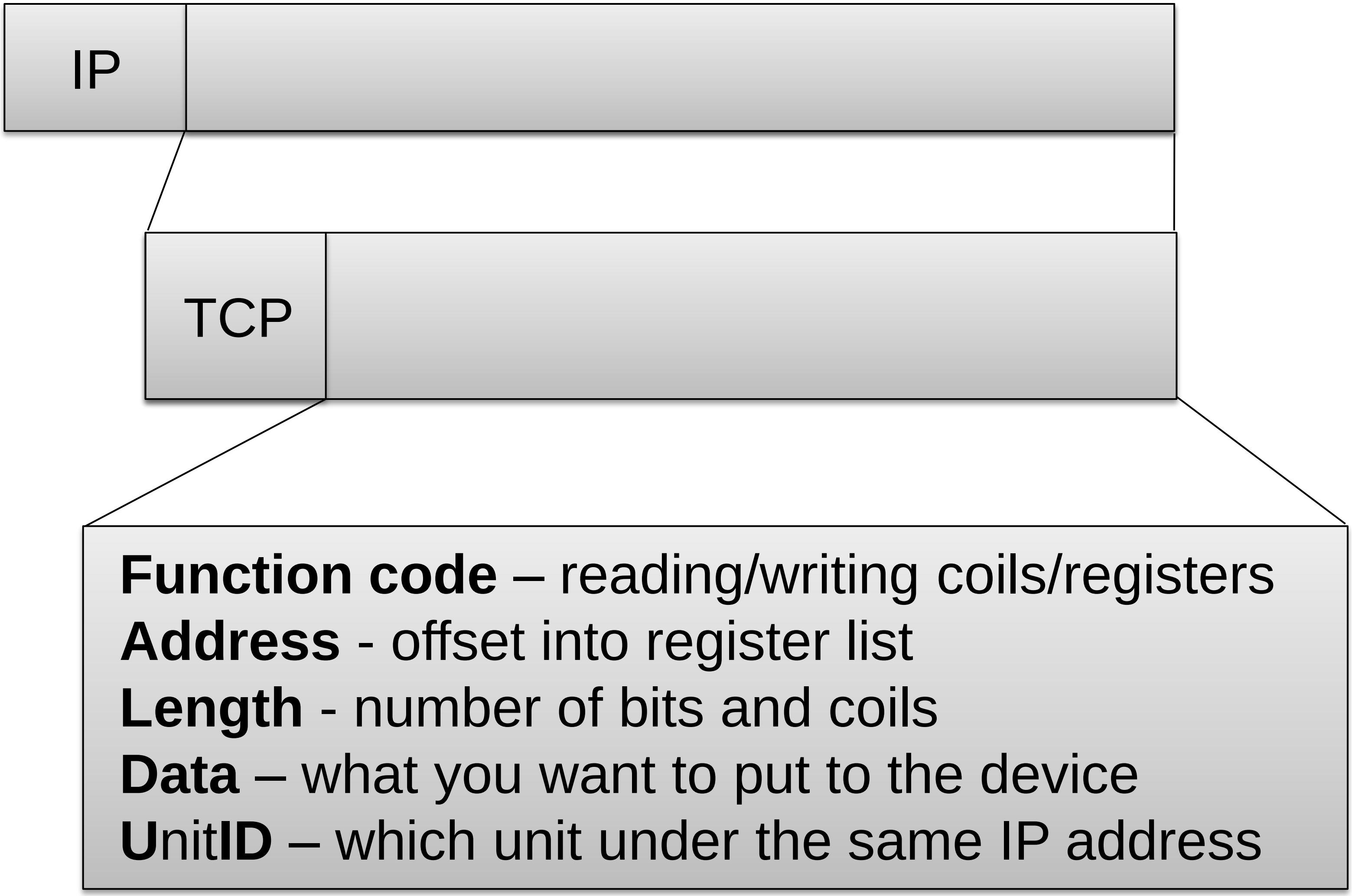
SCADA

- **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition
  - Evolved from analog signaling from the past into TCP/IP based signaling:
    - Human maintained
    - Leased telephone line
    - Circuit switched lines
    - Packet Switched lines



SCADA’s connectivity

- **Modbus TCP**



IP

TCP

Function code – reading/writing coils/registers
Address - offset into register list
Length - number of bits and coils
Data – what you want to put to the device
Unit**ID** – which unit under the same IP address

SCADA

- Functions and elements
  - Data Acquisition:
    - **sensors** (digital ‘on’ and ‘off’ or analog ‘how much?’)
    - **relays**
  - Data Communication:
    - Comm. Networks
  - Data Presentation:
    - Remote Terminal Unit – **RTU**
    - **Historian** used for storage
  - Control:
    - Programmable Logic Controller – **PLC**
    - Human-Machine Interface – **HMI**
    - Supervisory Computer System - **SCS**

SCADA model

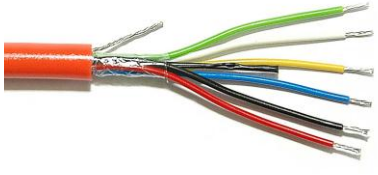
Data Control

PLC/HMI/SCS

Data Presentation

RTU/Historian

Data Comm.

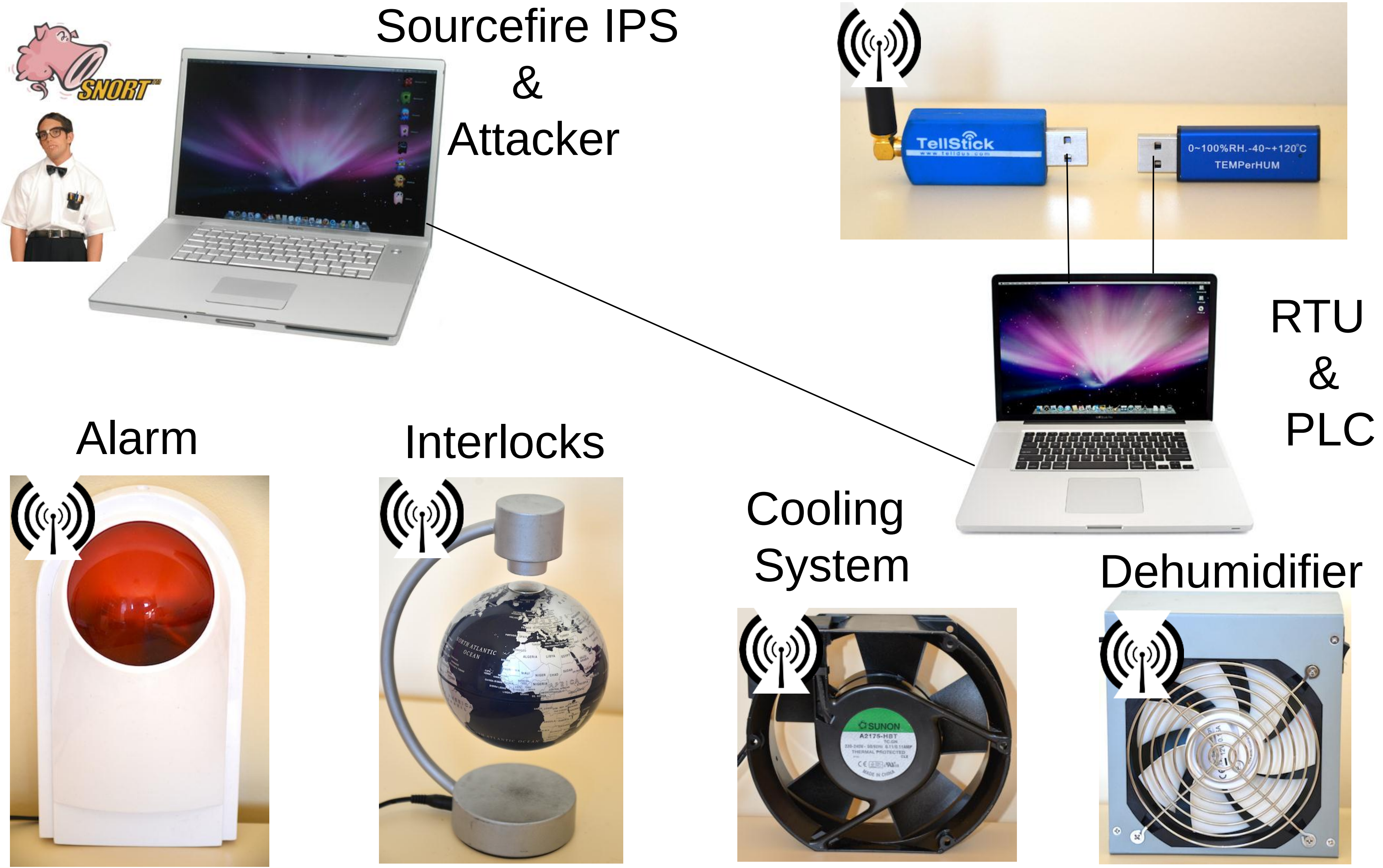


Cables/Radio

Data Acquisition

Sensors/Relays

Our SCADA model



Sourcefire IPS
&
Attacker

RTU
&
PLC

Alarm

Interlocks

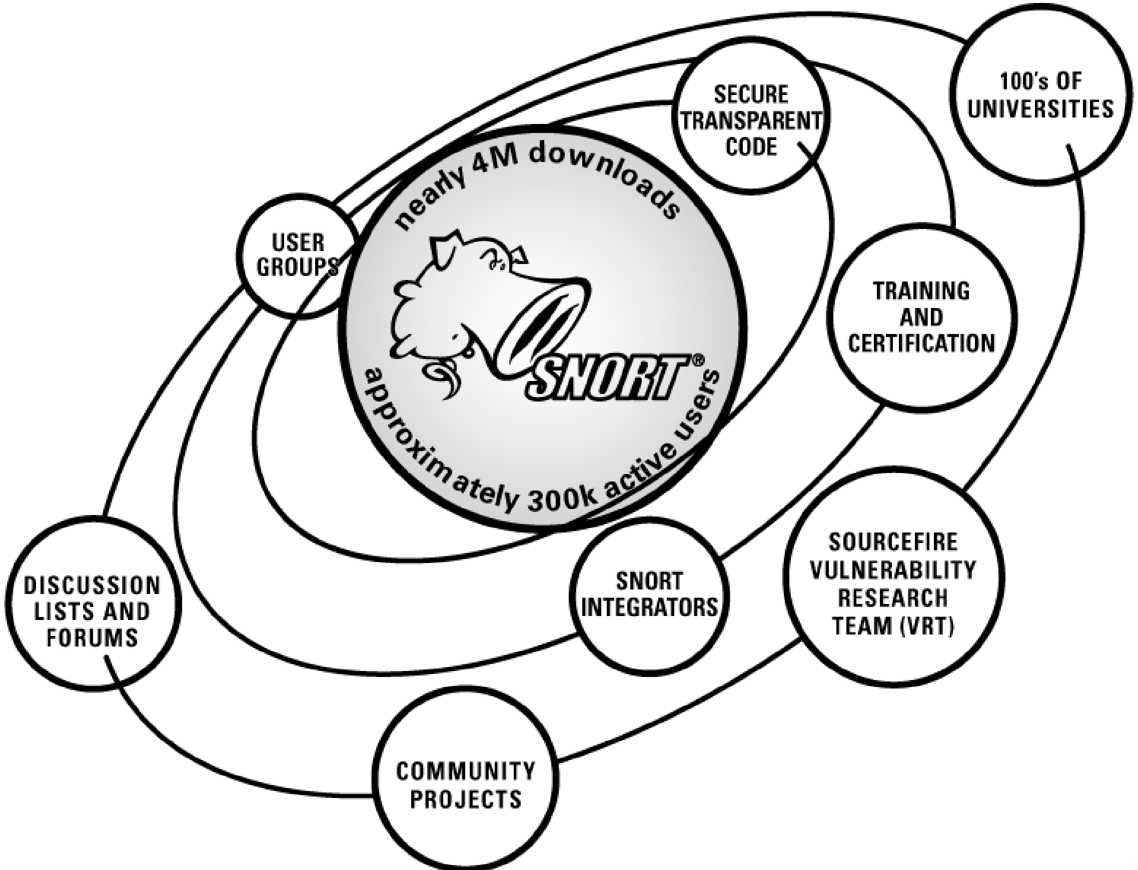
Cooling System

Dehumidifier

Demonstration Time!

Real world example

Open Source Snort



nearly 4M downloads
SNORT®
approximately 300k active users
SECURE TRANSPARENT CODE
100's OF UNIVERSITIES
USER GROUPS
TRAINING AND CERTIFICATION
SOURCEFIRE VULNERABILITY RESEARCH TEAM (VRT)
SNORT INTEGRATORS
DISCUSSION LISTS AND FORUMS
COMMUNITY PROJECTS

- Global IDS/IPS standard
- Largest community contributing to atack detection rules
- Easy to integrate
- Ran in parallel with Sourcefire
- Global Portal www.snort.org

Snort For Dummies
Snort & IDS Tools
Intrusion Detection with Snort
Intrusion Detection und Prevention mit Snort 2 & Co.
Snort IDS and IPS Toolkit
Snort et les IDS
Snort入侵检测 实用解决方案
IDS入門

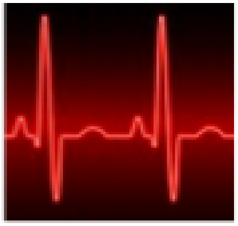
Next-Gen IPS – The Power of Awareness

Network

Know what’s there, what’s vulnerable,
and what’s under attack

Application

Identify change and enforce policy
on hundreds of applications



Behavior

Detect anomalies in configuration,
connections and data flow

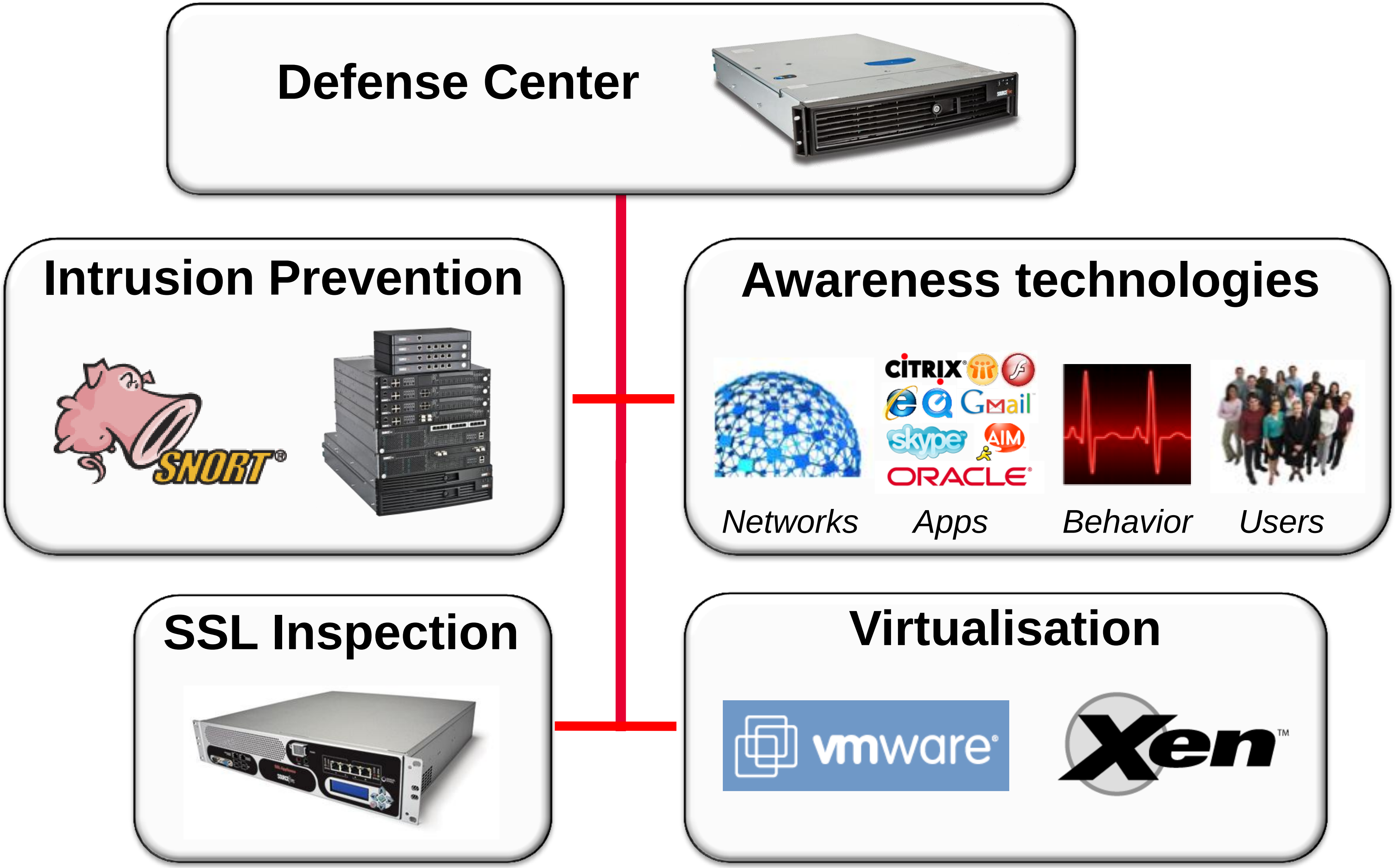
Identity

Know who is doing what,
with what, and where

Next-Generation IPS

NSS Labs TESTED

ICSA labs CERTIFIED NETWORK IPS



Defense Center

Intrusion Prevention

Awareness technologies

Networks

Apps

Behavior

Users

SSL Inspection

Virtualisation

NSS Labs report May 2011

As part of this test, Sourcefire submitted the **3D8260 IPS Appliance**

NSS Labs' Rating: Recommend

Product	Effectiveness	Throughput
Sourcefire 3D8260	97.6%	27,600 Mbps

Configuration	Total Number of Exploits Run	Total Number Blocked	Block Percentage
Default Configuration	1,179	1138	96.5%
Tuned Configuration	1,179	1151	97.6%

www.linkedin.com

Chrumkarnia – Snort PL