skybox® security

Unequaled Visibility and Productivity

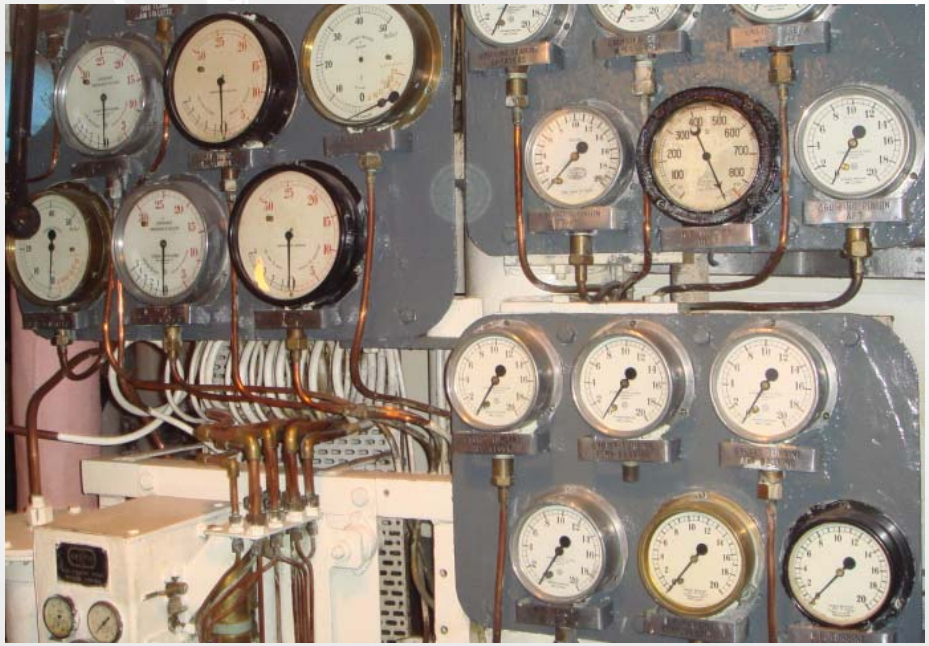
Model Based Metrics

Amnon Lotem

April 2008

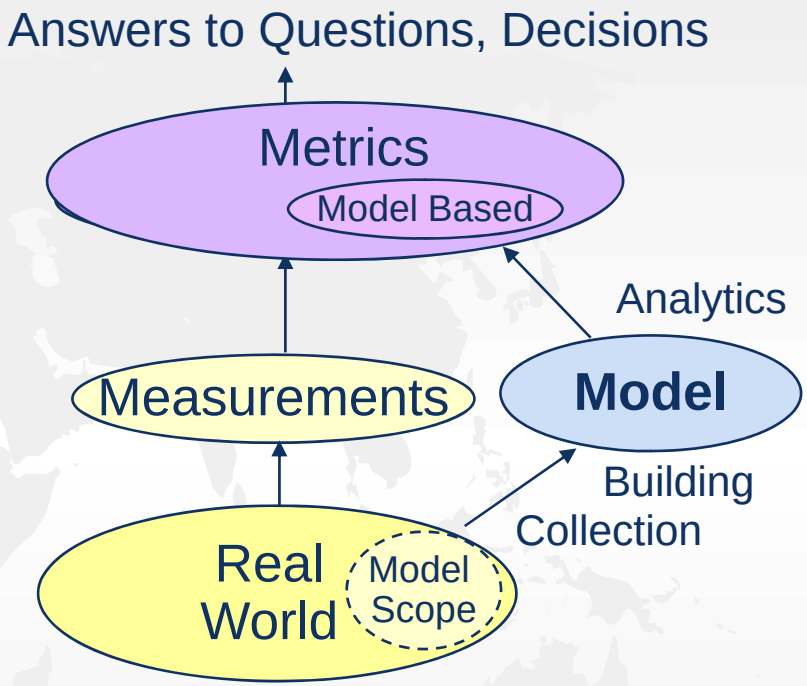
Agenda

- What are Model Based Metrics?
- Why do we need them?
- Examples
- Field experience
- The Security Model
- Advantages
- Challenges
- Conclusions



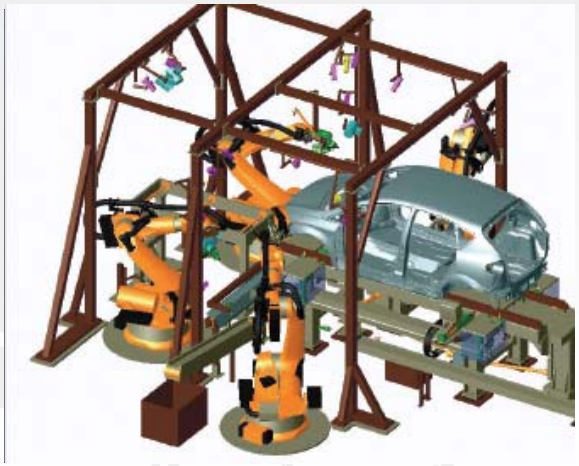
Model Based Metrics

- Metrics which are based on the analysis of a model
- Model
  - A representation of some aspects of the real world (scope)
  - Enables understand and predict behavior
- Required Capabilities
  - Data collection
  - Model building
  - Model analytics



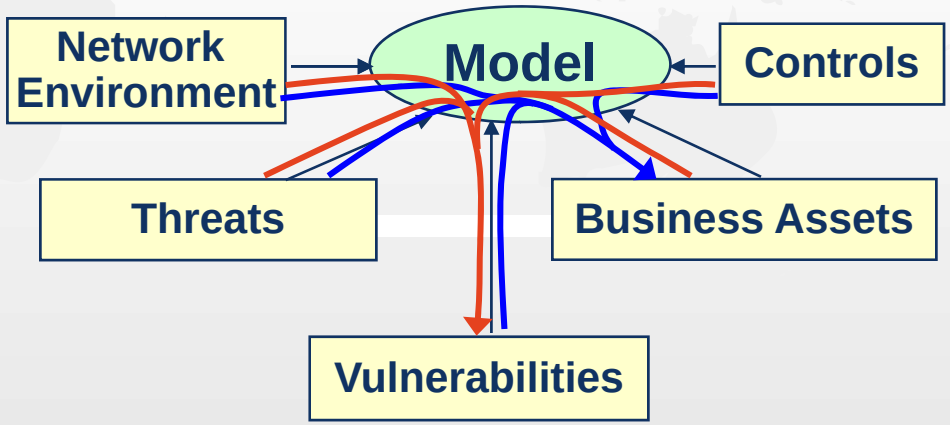
Do We Need Model Based Metrics?

- Models are widely and reliably used in other fields



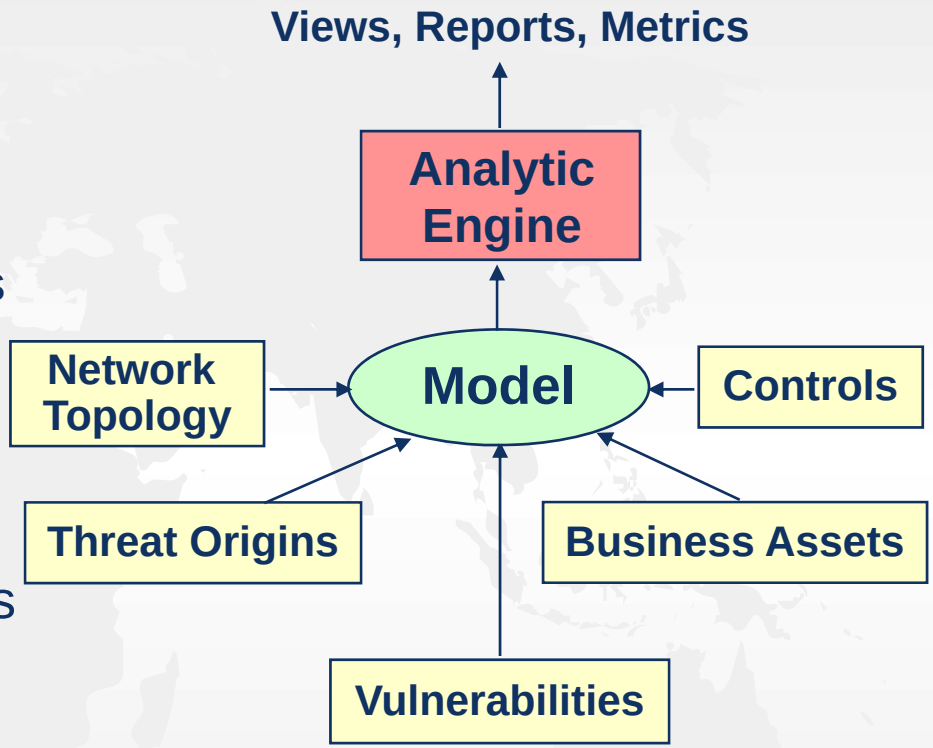
- They enable to associate between several disciplines and simulate behavior

- Security involves many disciplines
- Associating between them is essential for answering security questions:
  - Is our current security environment strong enough? or,
  - What is our current risk level?
  - What are the most urgent vulnerabilities we need to fix?

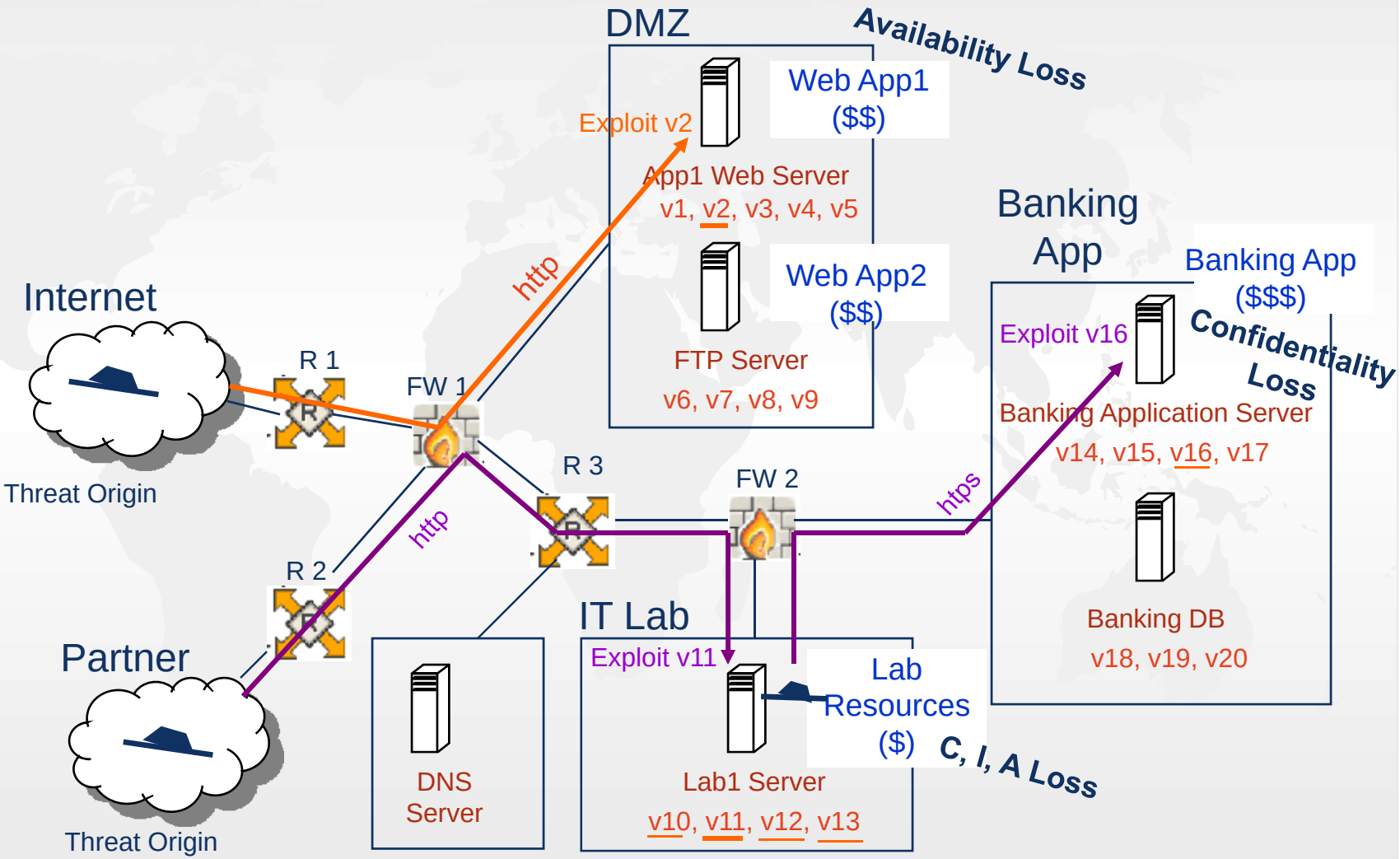


Our Approach

- Represent in one model:
  - Network topology and hosts
  - Vulnerabilities
  - Controls (Firewalls, IPS, …)
  - Business Assets and Threat Origins
- Use Analytic engine for predicting capabilities and behavior
- Extract Views, Reports, and Metrics
- Applicable for:
  - Enterprise vulnerability management
  - Risk management
  - Policy Compliance of firewalls
  - Change Management



A Network Example

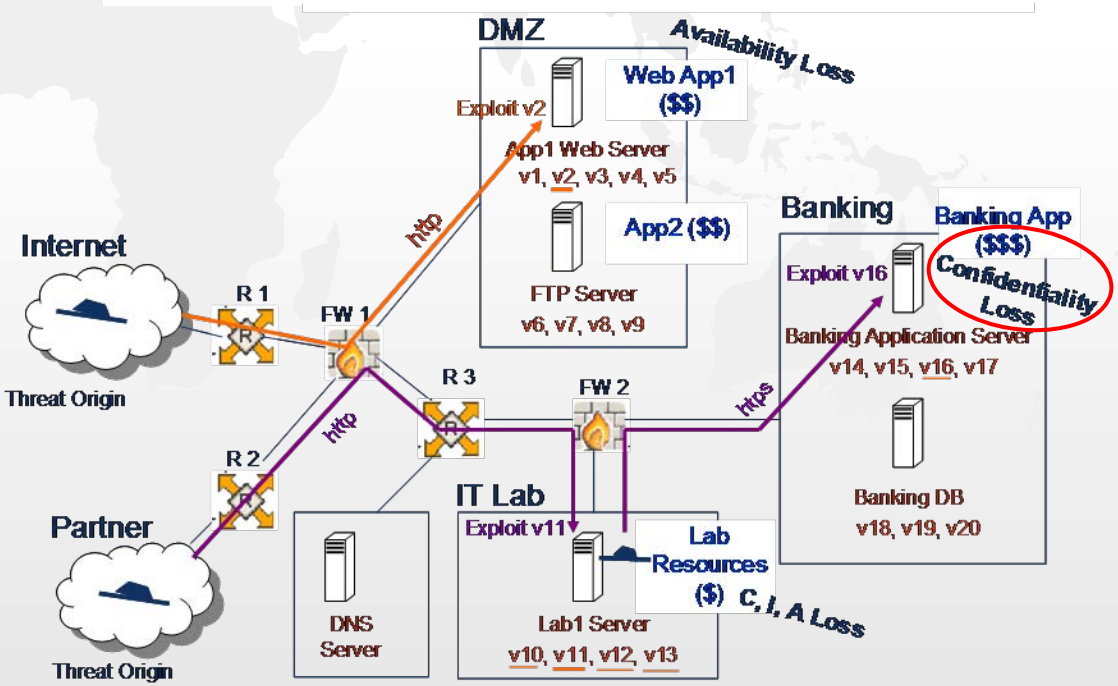


Extracted Metrics – Business Assets Risk

- Assigning risks to business assets
- e.g., Banking App:
  - Business Asset Classification:
    - Confidentiality loss => Very High damage
  - Attack analysis:
    - Possible
    - Likelihood: Medium
  - Risk:
    - Likelihood * Impact
    - => High
- Basis for:
  - Effort prioritization
  - Overview of Risks and Trends

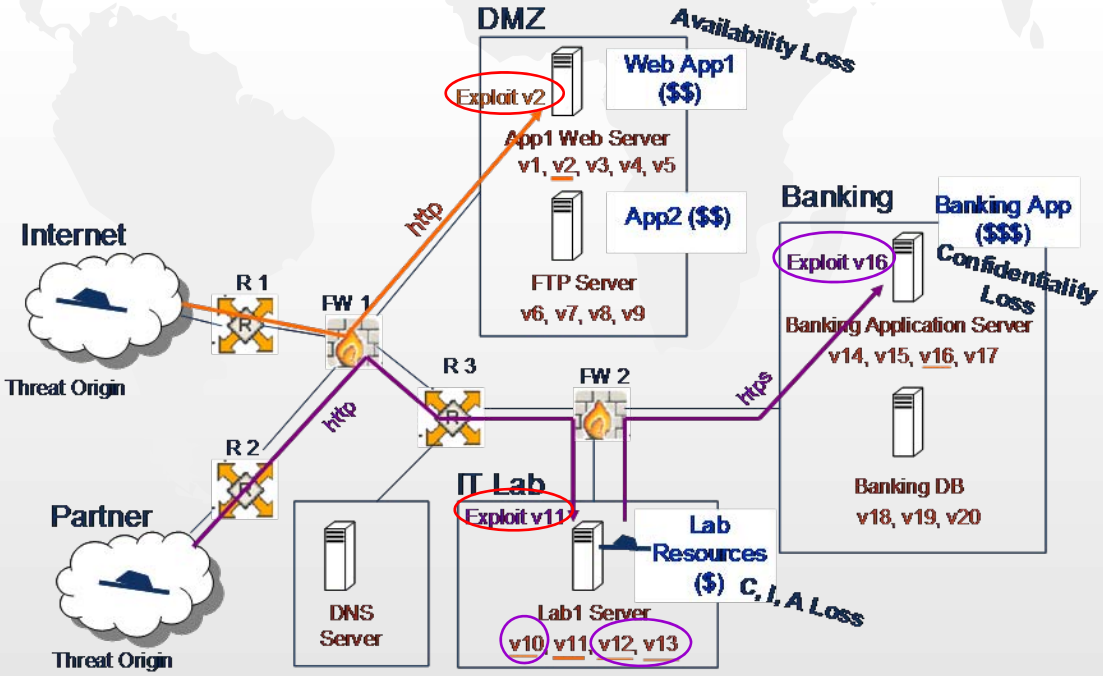
Business Assets Analysis: Business Assets by Risk

Name	Risk
Banking App	
Web App1	
Lab Resources	
Web App2	



Extracted Metrics – Vulnerability Exposure

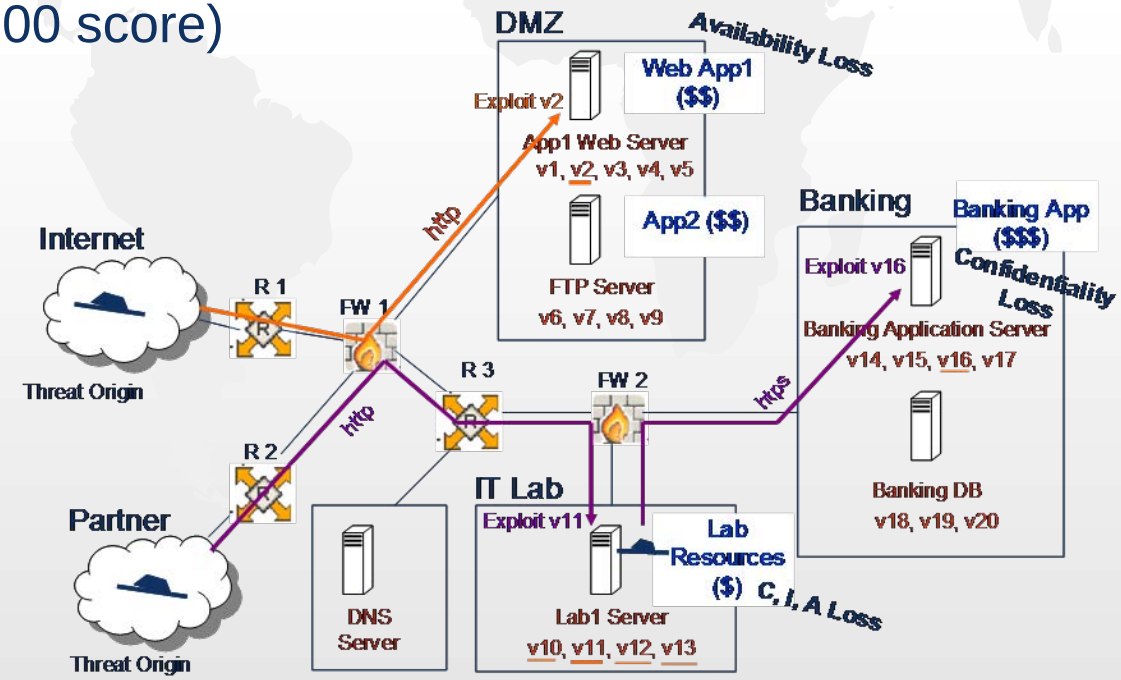
- Exposure
  - Q: Is the vulnerability exploitable from the threat origins? How may attack steps are required?
    - **Direct** - one attack step is sufficient (an entry point)
    - **Indirect** – at least two attack steps
    - **Inaccessible** – no attack is possible



Vul.	Exposure
v1	Inaccessible
v2	**Direct**
v3	Inaccessible
v4	Inaccessible
v5	Inaccessible
v6	Inaccessible
v7	Inaccessible
v8	Inaccessible
v9	Inaccessible
v10	**Indirect**
v11	**Direct**
v12	**Indirect**
v13	**Indirect**
v14	Inaccessible
v15	Inaccessible
v16	**Indirect**
v17	Inaccessible
v18	Inaccessible
v19	Inaccessible
v20	Inaccessible

Extracted Metrics – Vulnerability Imposed Risk

- Imposed Risk
  - The damage expectancy of the vulnerability
  - Based on attack paths in which the vulnerability instance is exploited
  - Numeric Value (likelihood * damage)
  - Can be translated into a scale (e.g., a 5-level scale or 0-100 score)



Vul.	Imposed Risk
v1	
v2	**High**
v3	
v4	
v5	
v6	
v7	
v8	
v9	
v10	Low
v11	**Critical**
v12	Low
v13	Medium
v14	
v15	
v16	**Critical**
v17	
v18	
v19	
v20	

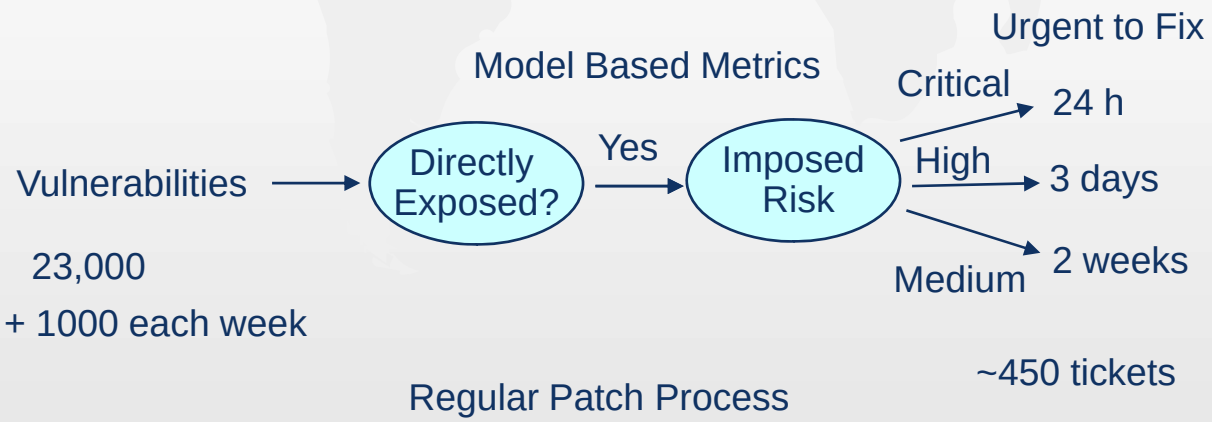
A Strong Mechanism for Ranking Vulnerabilities

- Identifying the relatively small group of vulnerabilities that enable attacks from external threat origins
- Usually less than 1-2% of the total vulnerabilities (feasible to fix in a reasonable time)
- Daily or alert-based process of fixing new risky and directly exposed vulnerabilities that are identified
- At the management level interesting metrics are:
  - What is the current number / rate of directly exposed vulnerabilities
  - How many of them are at high risk
  - What is the trend?

Vul.	Exposure	Imposed Risk
v1	Inaccessible	
v2	**Direct**	**High**
v3	Inaccessible	
v4	Inaccessible	
v5	Inaccessible	
v6	Inaccessible	
v7	Inaccessible	
v8	Inaccessible	
v9	Inaccessible	
v10	**Indirect**	Low
v11	**Direct**	**Critical**
v12	**Indirect**	Low
v13	**Indirect**	Medium
v14	Inaccessible	
v15	Inaccessible	
v16	**Indirect**	**Critical**
v17	Inaccessible	
v18	Inaccessible	
v19	Inaccessible	
v20	Inaccessible	

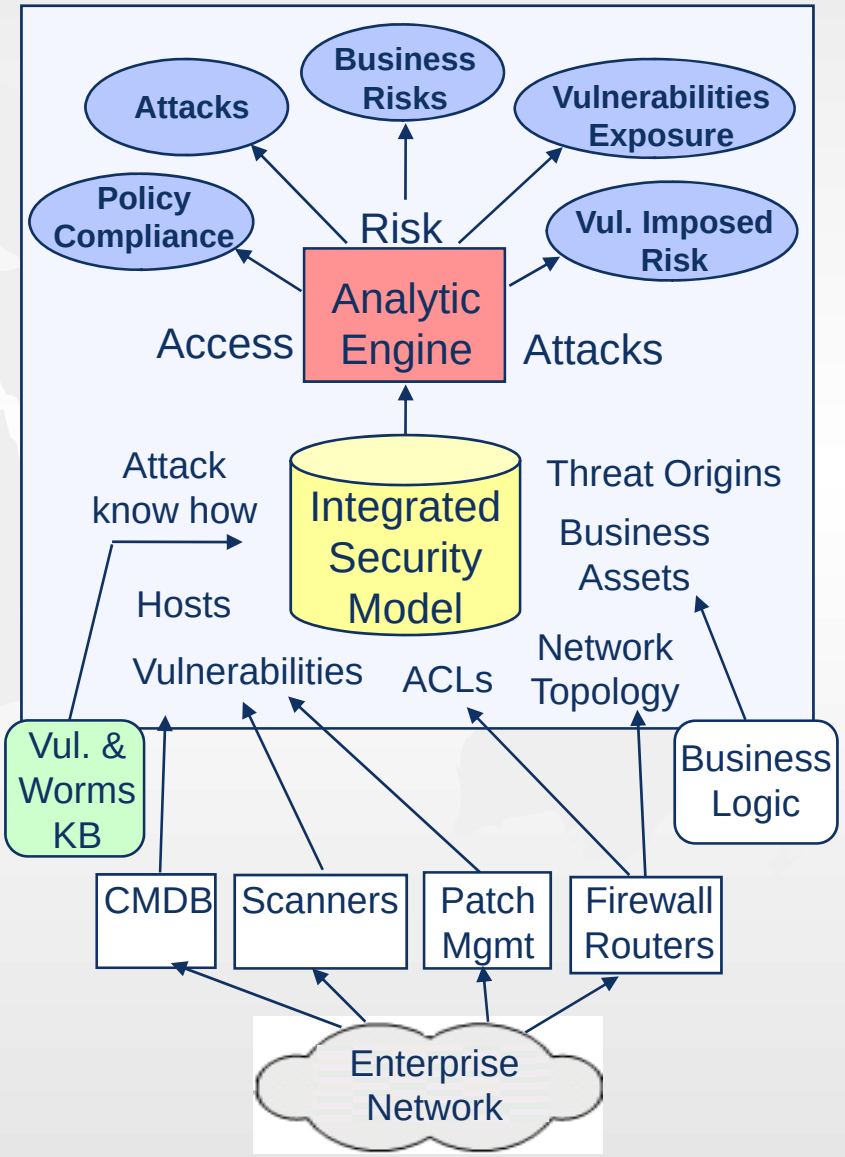
Field Experience – An Example

- Medium size organization
- Uses our product for vulnerability management on a daily basis
- 1,500 Servers
- 10 External threats: Internet, Partners
- ~100 Business Assets
- 23,000 Vulnerabilities; 1,000 new vulnerabilities each week
- A daily process of fixing **directly exposed** vulnerabilities
  - SLA is based on imposed risk: 24h, 3 days, two weeks
- ~450 tickets with relatively high priority



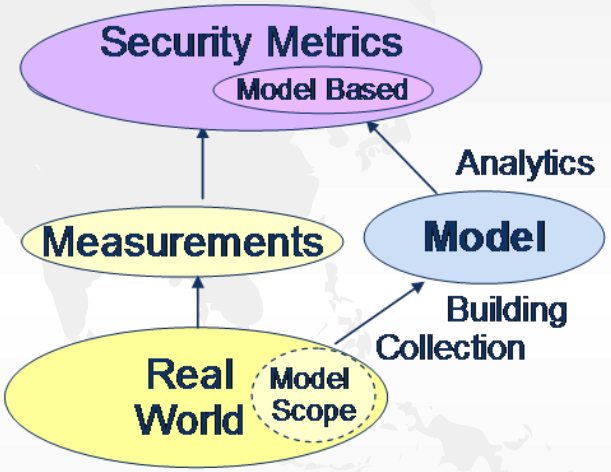
The Security Model and its Environment

- Represents the enterprise network and related security data
- Assembled from a wide variety of data sources
- Refreshed regularly
  - e.g., every night
  - Using automated tasks
- The Analytic Engine is invoked for computing access, attacks, and risk
- Extraction of Metrics and Views



Model Based Metrics - Advantages

- Extend the set of security metrics that can be maintained
  - Adding metrics that are too complex to compute or measure
- Can relate to predicted behavior (possible, impossible, likely to happen, …)
- What-if mode – examine what will be the effect of a proposed change on the security
- Enable root cause analysis
- Filter noise in raw data
  - As the model merges and correlates data from various sources
- Continuous extraction of the metrics



Model Based Metrics - Challenges

- The model must be accurate enough for the metrics to be trustworthy
  - How this can be measured?
  - How do we assure that?
  - How do we calibrate the computations?
- How do we represent and consider unknown factors?
  - Unknown threat origins, non-reported vulnerabilities, …
- Can we combine model-based metrics with traditional metrics?
- Best practices and standards:
  - Model based metrics are not there yet. Should be

Conclusions

- Model based metrics increase our insight on security status and required actions
- They are already in use in some security management processes (vulnerability management, access compliance)
- As metrics experts, we should:
  - Explore the new opportunities for measuring and assessing the security status based on security models
  - Develop the metrics and measurements required for tuning the models and assuring their accuracy

Thank You