



Realization of Security Events Management System via OPENSTF

Lance Yoo

www.antpower.org





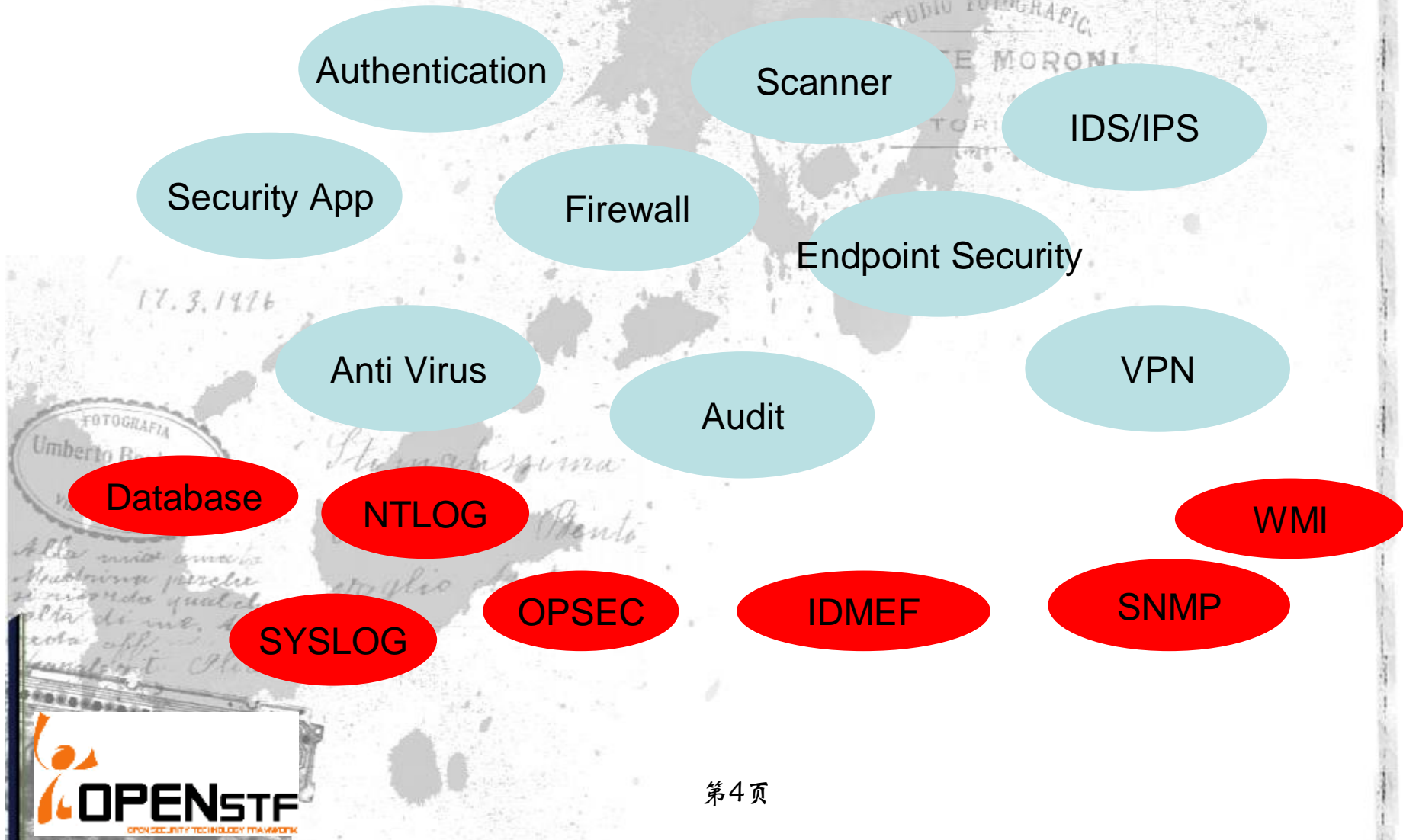
Requirements Analysis of Security Event Management



- We could not qualify the impact of so many heterogeneous security products
- It is useless to view a mass of security events with a mount of trustless information included
- The policy constitute could not acquire the whole view on security state
- There are no valid correlations with security decision and security application.
- An Open Loop System, which is consisted of Early Warning, Defending, Responding sub-systems, has no strong ability to desist the strikes.



Heterogeneous security solution leads to risks



Enterprise Network EPS: Peak vs. Average

Typical Medium/Heavy Workload of 55 Devices

Devices: 18 Router, 8 Firewalls, 11 LAN Switches, 6 VPN's, 12 IDS Sensors

Company: 35M Annual Revenue, 1700 Employees

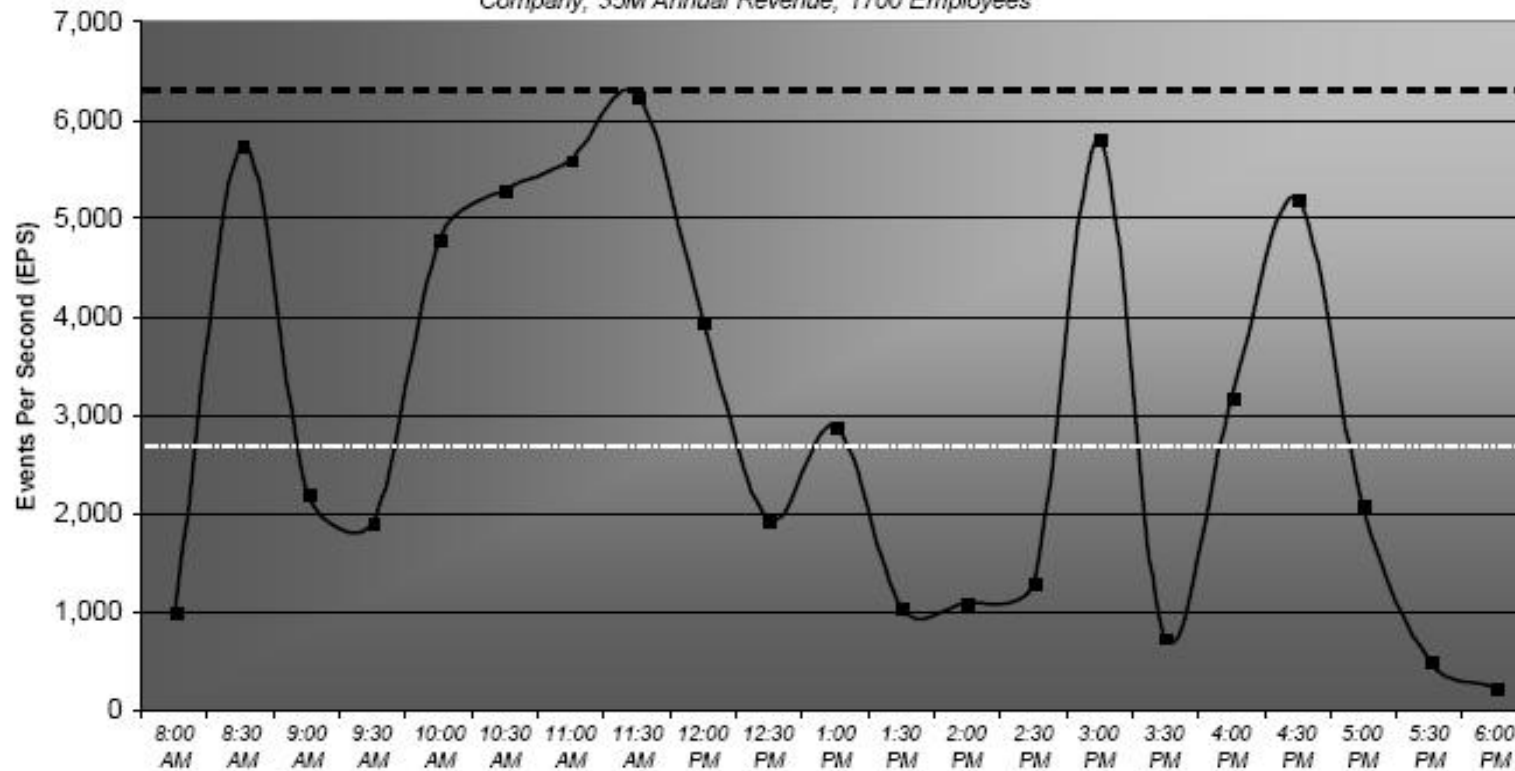


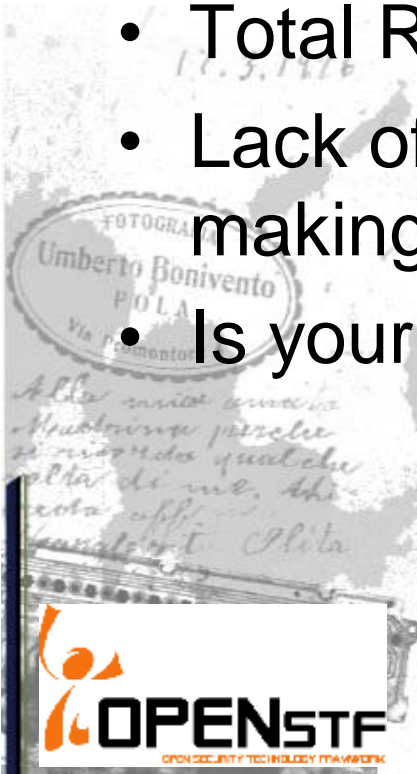
Chart 1: Sample Comparison of Peak and Average EPS Loads



- Sensibility And Reliability are conflict
- IDS acquirement and analysis of information is limited according to its network level and performance (Context-Free)
- IDS SNR enhancement lies on Efficiency of event management



- Current solution is elementary and partial
- No effective way to show whole security tendency
- Total Risks have to obey “Bucket Principle”
- Lack of practical data when leader or manager making security policy
- Is your security system an closed loop system?



- How to dynamic evaluate real asset value in security solution
- How to manage risk assessment in security application
- For users, “Business Application” is the goal, not “Security”
- Find hidden threat in time

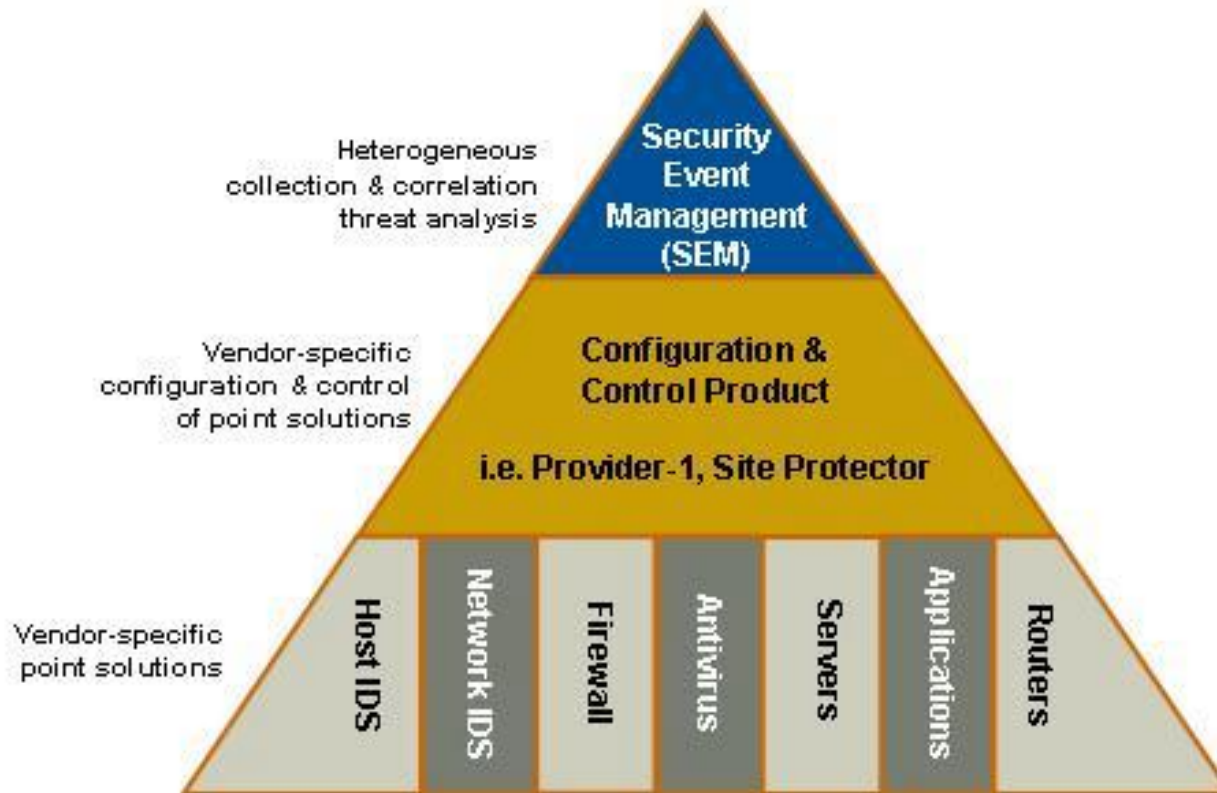


It is so creative to analyze the security events real time collected from Computer, Network, Storage and Security devices. The SEM helps us to find the true security risk via the correlations on security events with different places, different layers and different types. In fact, we could not only assess the current security state and risk, but also make emergency responding with pre-defined policies automatically.

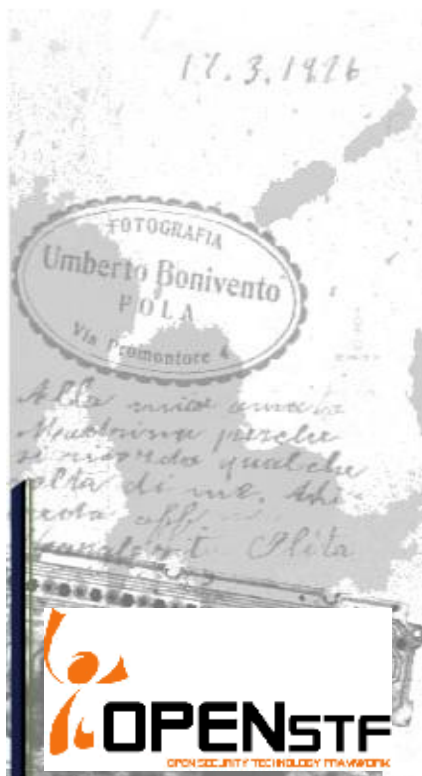
Dynamic security system Model is the major body of intelligent system



Security Event Management – SEM Core of risk management



- Correlation and Aggregation of security events
- The risk quantization and visualization
- Closed Loop System, Response in time



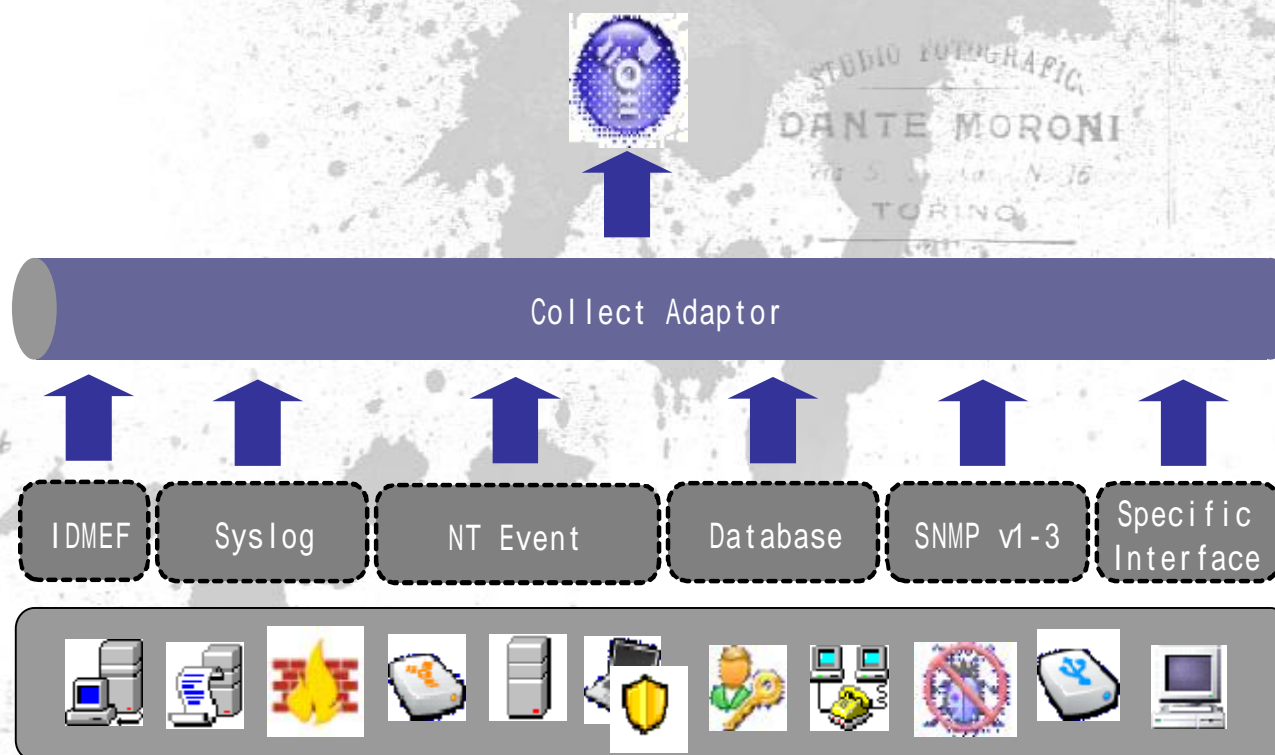


Technologies in security event management



- Normalization
- Aggregation
- Correlation
- Visualization



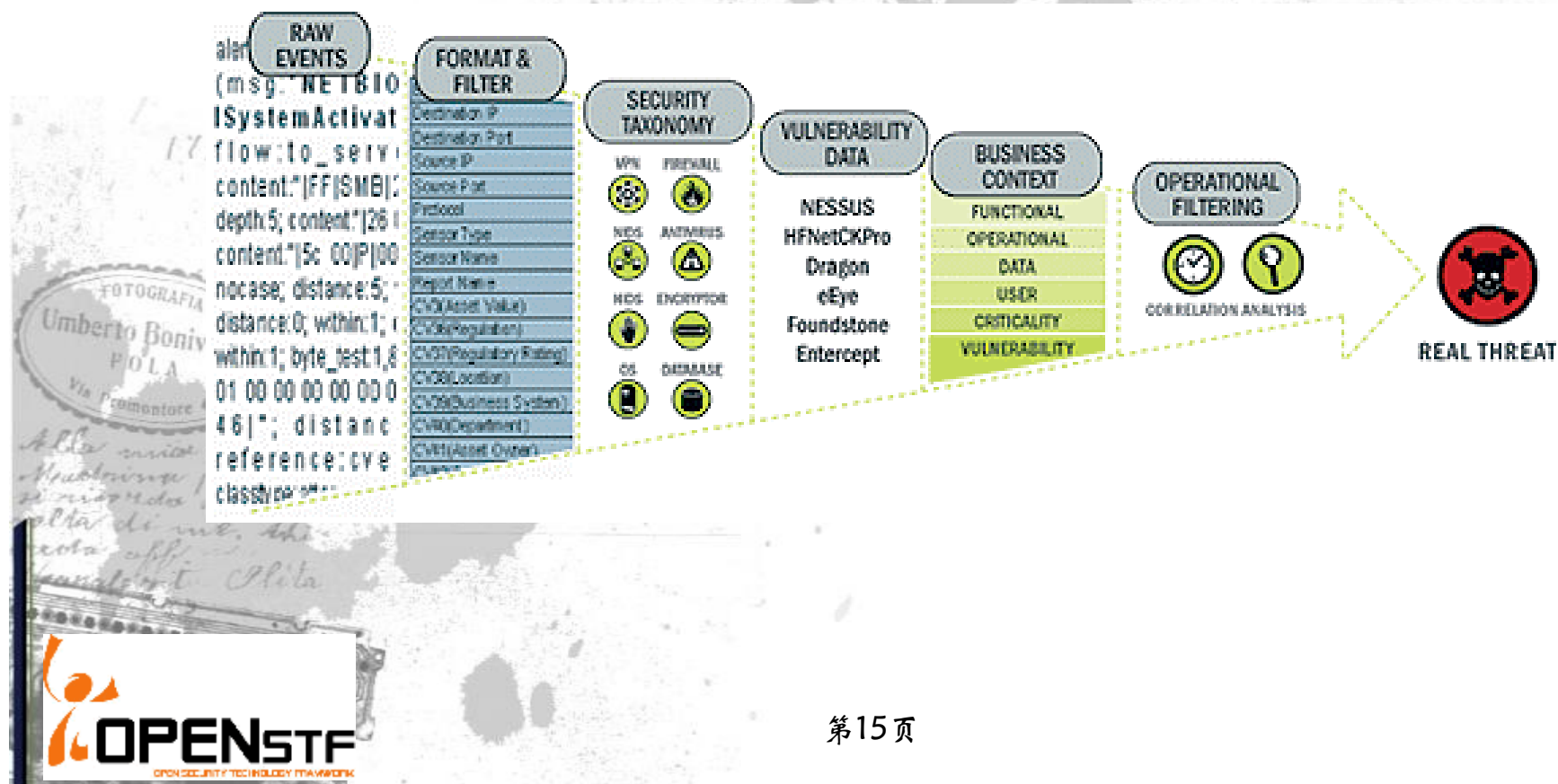


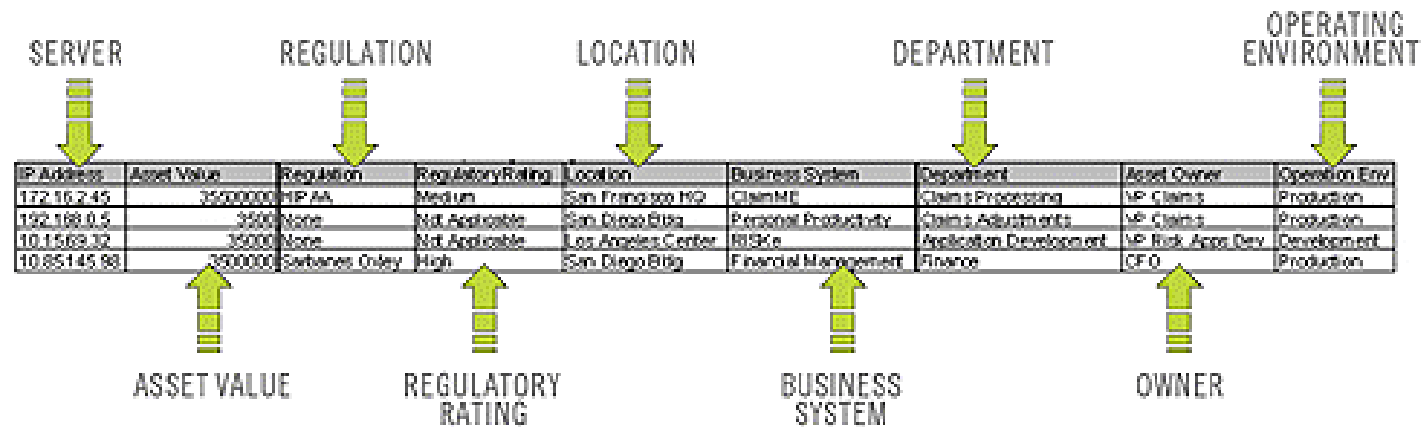
Alta carica...
Maurizio...
si ricorda qualche
volta di me. Ah
nota off...
lavoratori. Rita

vo glio...



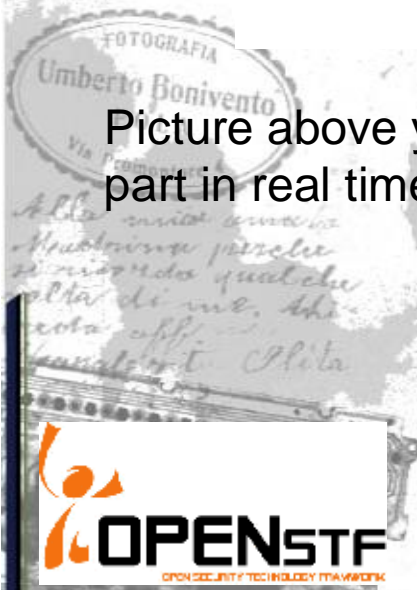
- filtrate
- eliminate the redundant data
- classify
- Bind context



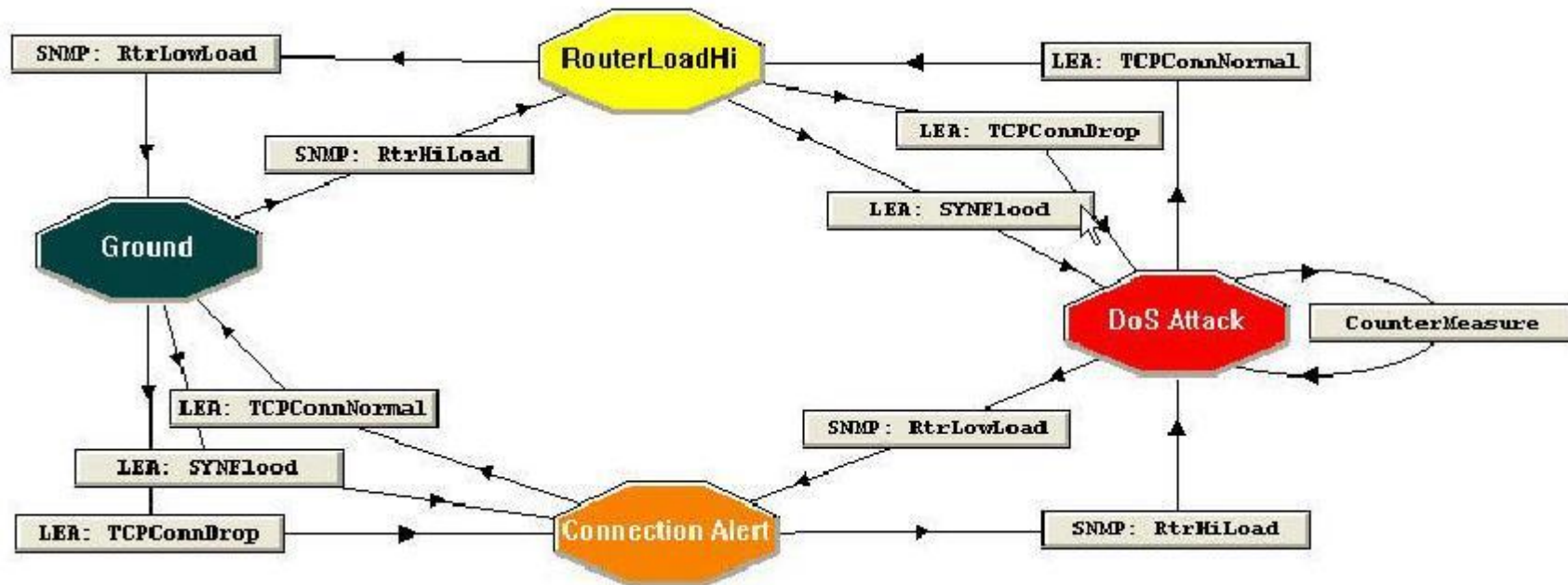


SERVER	REGULATION	LOCATION	DEPARTMENT	OPERATING ENVIRONMENT				
IP Address	Asset Value	Regulation	Regulatory Rating	Location	Business System	Department	Asset Owner	Operation Env
172.16.2.45	3500000	HIP AA	Medium	San Francisco HQ	Claim Mgt	Claims Processing	MP Claims	Production
192.168.0.5	3500	None	Not Applicable	San Diego Bldg	Personal Productivity	Claims Adjustments	MP Claims	Production
10.1569.32	35000	None	Not Applicable	Los Angeles Center	RISKe	Application Development	MP Risk Apps Dev	Development
10.85.145.98	3500000	Services Only	High	San Diego Bldg	Financial Management	Finance	CFO	Production

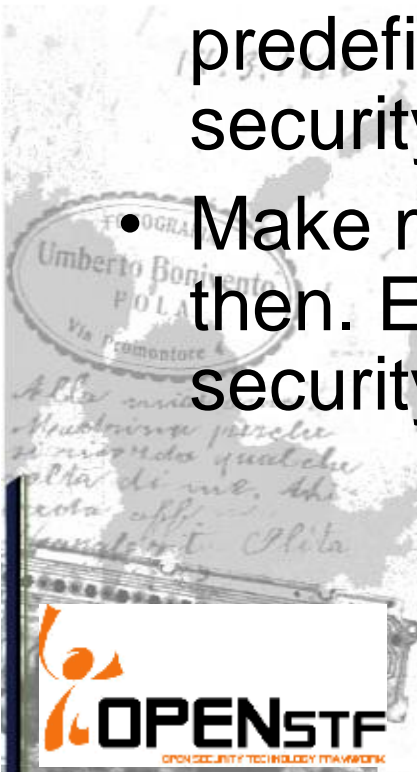
Picture above you can see security attributes of asset which will be an important part in real time risk calculation.

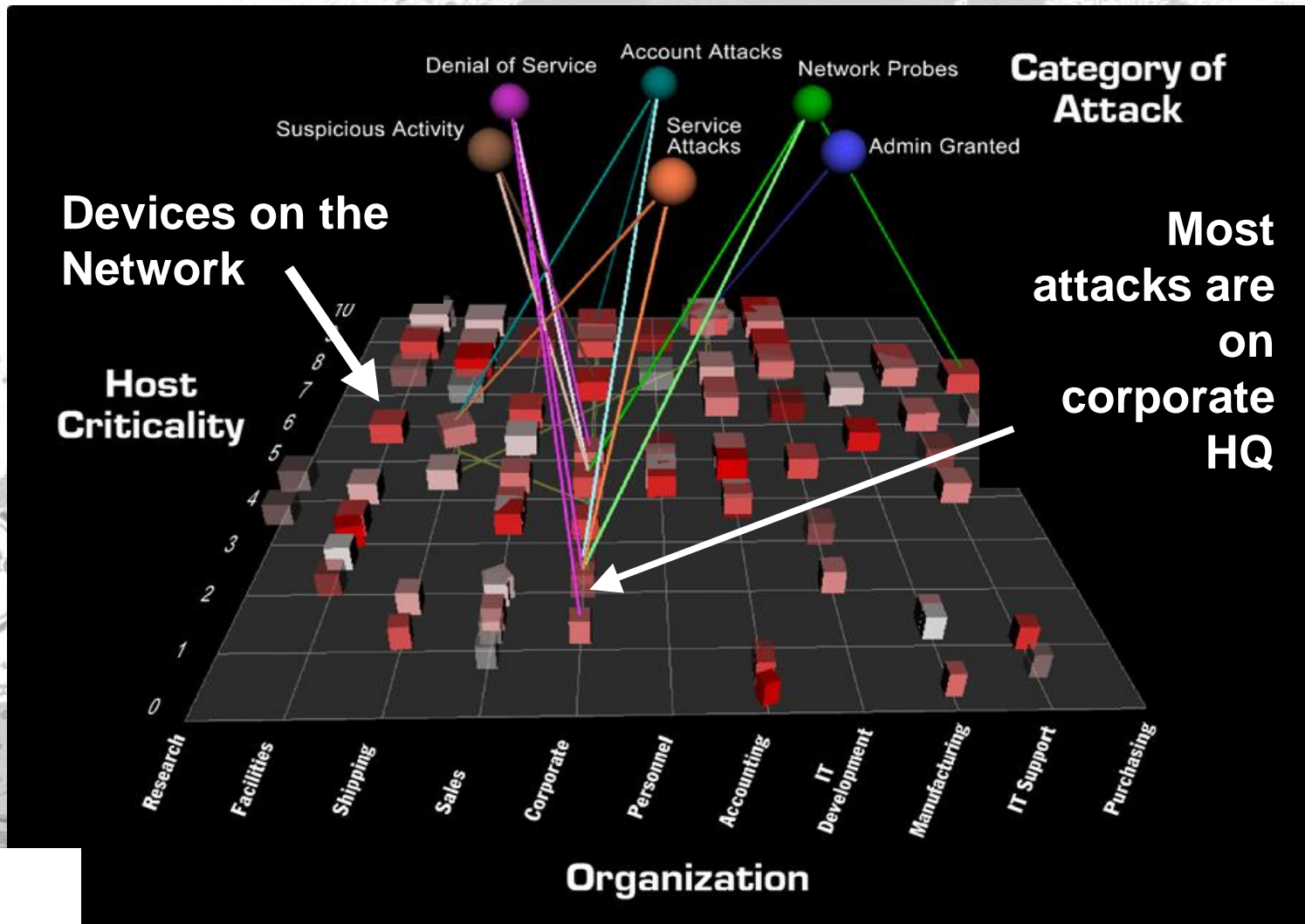


- Correlate event by predefined policy to make accurate security alarm. Strong real-time analysis ability based on small time windows as you should define correlation rule first.



- Consolidate a certain time event, refer to a threshold, and make a security tendency estimation finally. Based on large time windows, less real-time analysis ability, not necessary predefined rule, reflect system the whole system security attributes.
- Make major categories first, classify the events then. Evaluate the attack according to the event security level and quantity.





- To mitigate the burden of processing security alarms involving human
- To reduce the false positives of security events
- To avoid the potential risk under the mass volume of events
- To quicken the response of incidents
- To Manage events from IDS, Firewall, OS, Antivirus, Web server, Database





Implementing of SEM with OpenSTF



- Not only the technical problems, but also the people and operation
- A extendable basic system plus different modules and solutions for different application environment
- Usually need 2nd development to form the final management system
- From the view of design & development method, it's similar to ERP system for enterprise management



Fred Brooks – Father of IBM 360 System

“The Mythical Man-Month”, he brought us 4 root causes of the difficulty in software system development:

- complexity
- conformity
- changability
- invisibility

No Silver Bullet !?

**Same in SIM/SEM
development!**



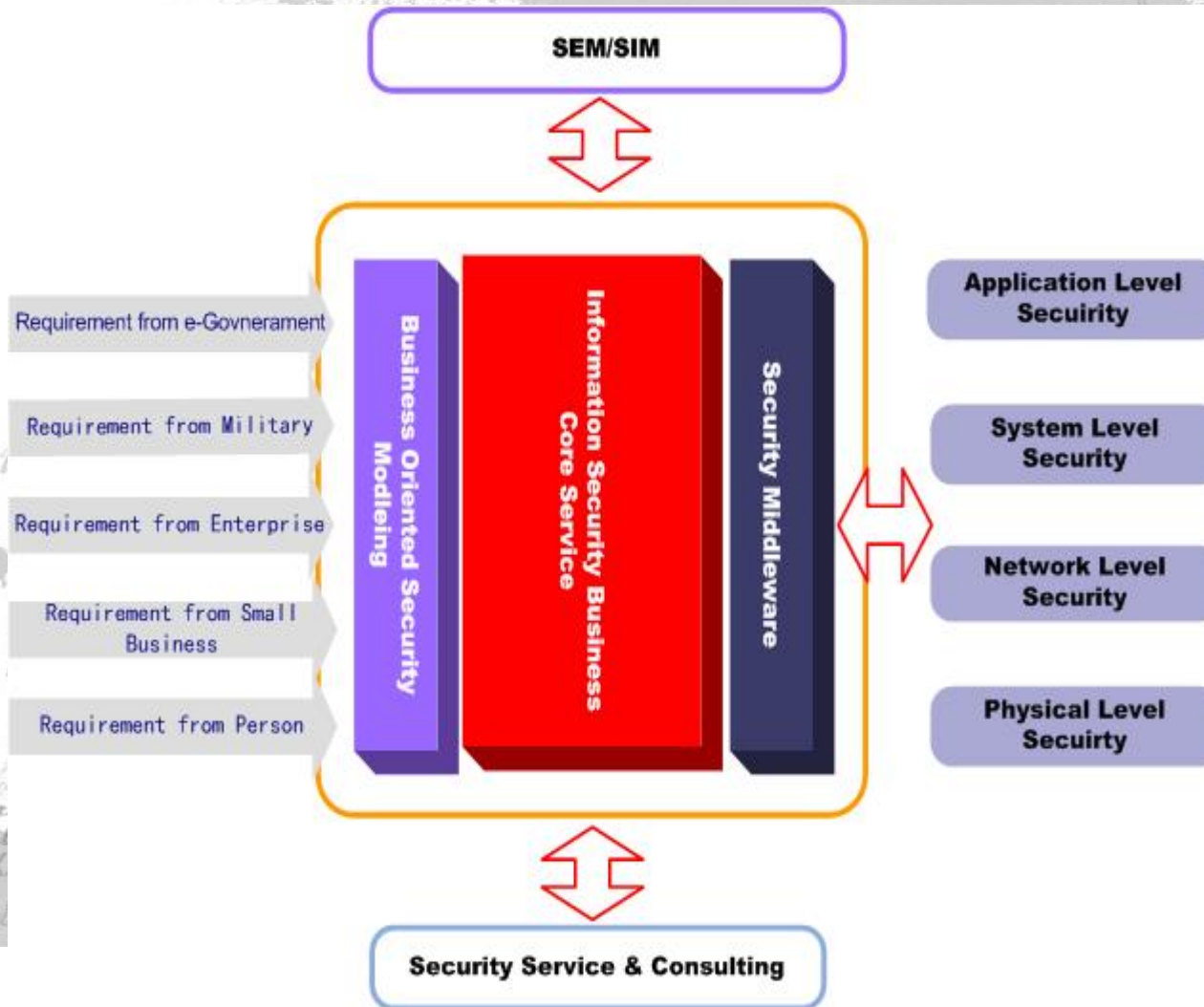
The evolution of software development vs. info-sec system development

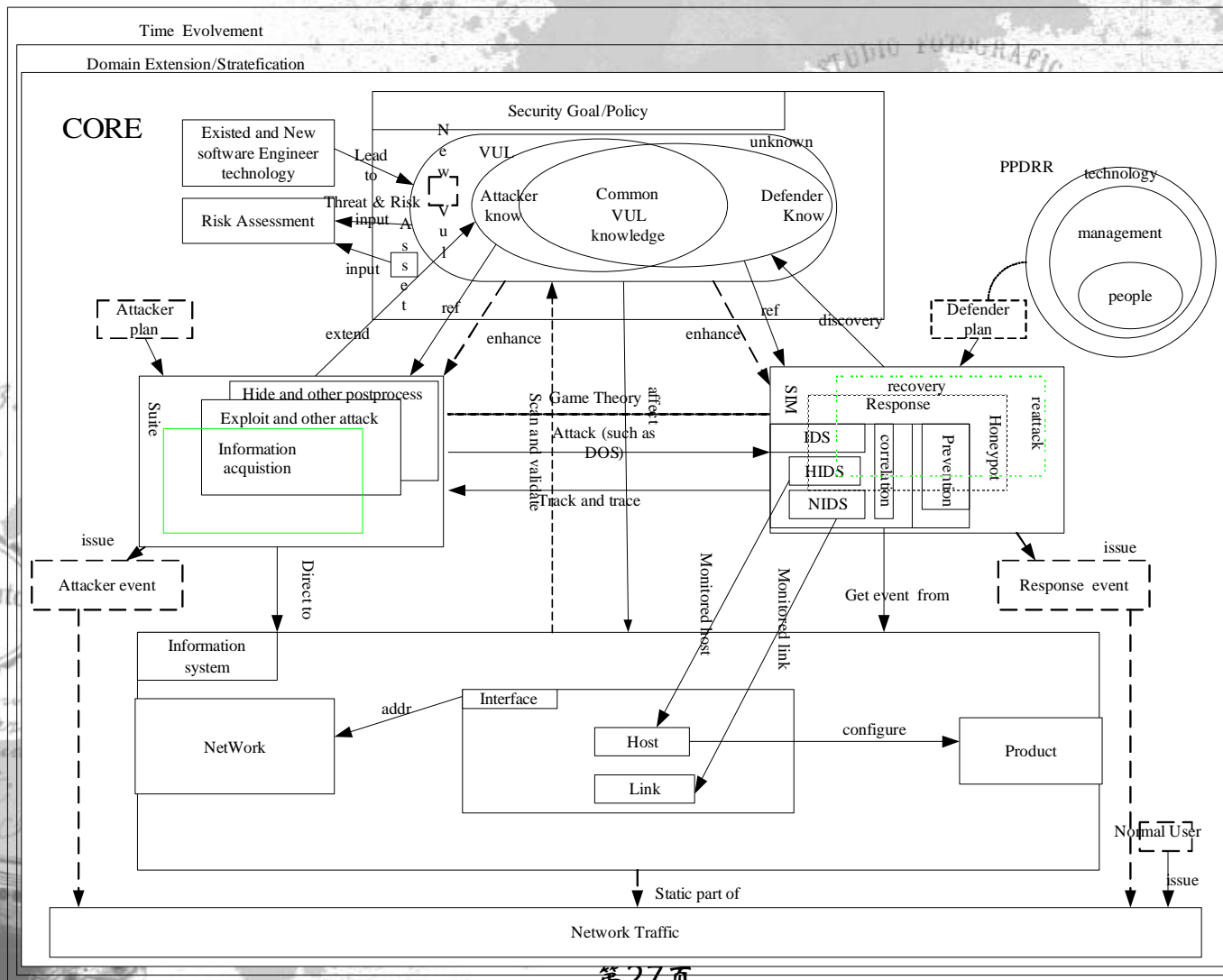
- Software Engineering(RUP, XP, CMM ...)
- OO(MDA, UML, Design Pattern ...)
- Platform(software platform, business application platform)
- Middleware
- Info-sec engineering (ISSE/SSE-CMM)
- Standard of Security Managment (ISO17799/BSI7799)
- IATF
- PKI/PMI
- Security Middleware
- Info Sec Application Oriented Platform



Security Application Oriented Platform

Business application oriented, to solve the problems of integration, interaction, extension, management of different security sub system, to reduce the total cost of own finally!



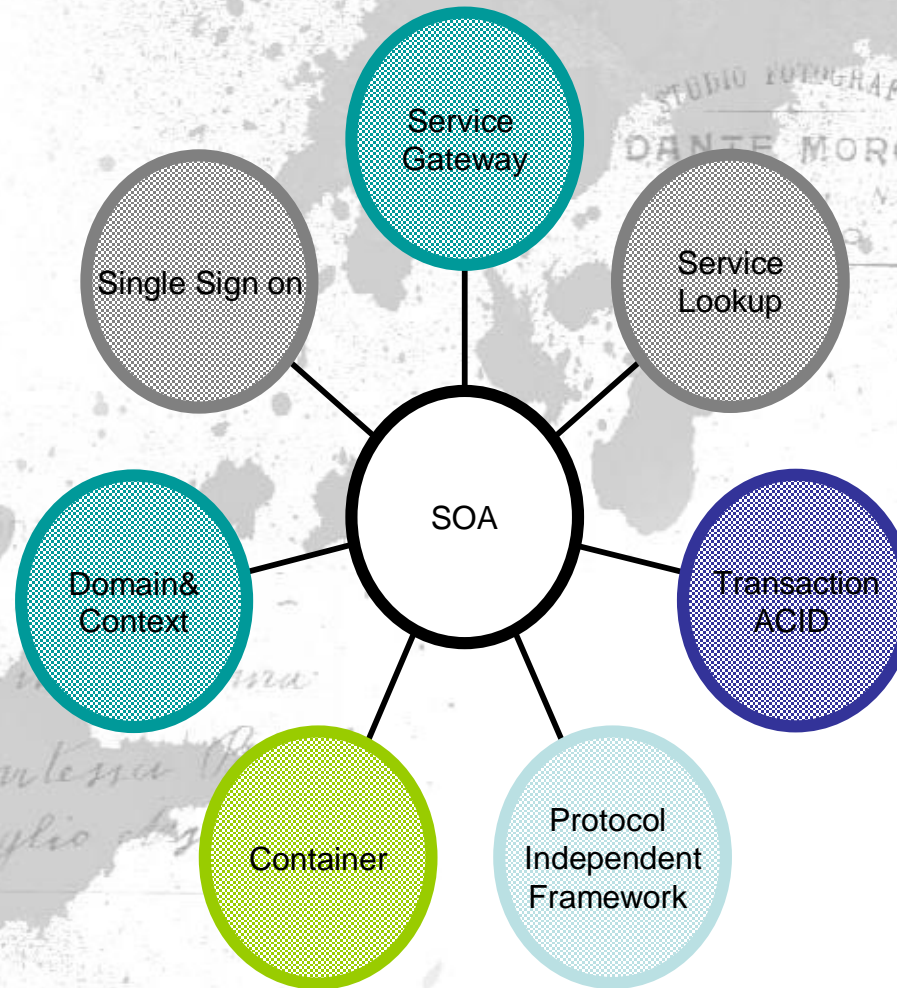


- Information System/ Asset
- Attacker
- Defender
- Security Goal/ Policy & Vulnerability

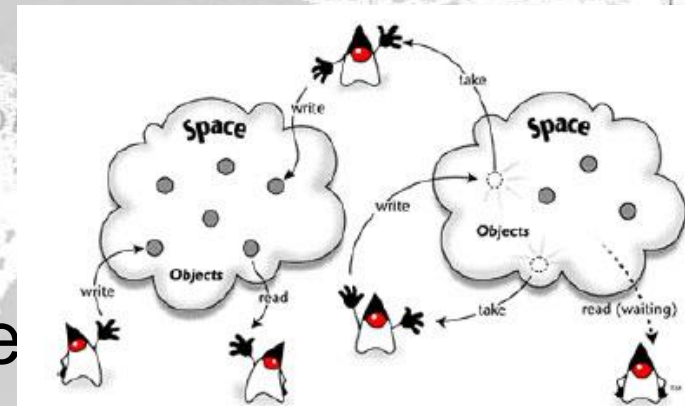


- Service Oriented Design Model is a revolution after OOD, which born in context of distributed computing
- Service Oriented Programming (SOP) is based on OOP

Service is a predefined contract implemented by component and used by other components. The providing and using of the service are connected by contract which is interface in computer programming knowledge scope.



- Component Service
- Domain Service (Context)
- Policy Service
- Message and Transaction Service
- Internal Security Service (Authentication & Authorization)
- Universal UI Framework (GUIStarter)



- Middleware is a kind of reusable software
- Middleware's goal is resource sharing in distributed system
- Middleware not only implements connection but also inter-operation
- Middleware's application must be based on platform

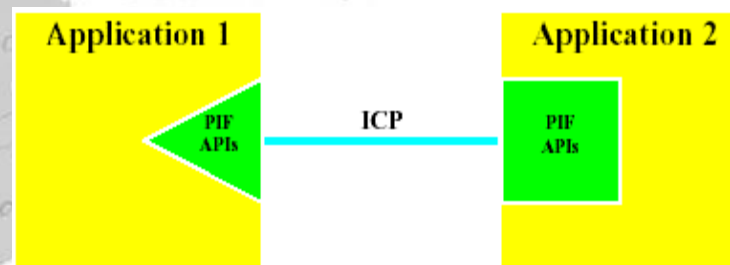


- Middleware is the collection of components which implement a certain type security function through collaboration
- The collaboration between them and other middleware assured and supported by services of OpenSTF core
- Middleware is the format of distribution, which has many properties: uuid, vendor, version, features, list of compontes
- The management of middleware and inside components is reached by OpenSTF core's Component Service



- To solve the problem of multi-protocol in event collection with PIF provided by OpenSTF Core

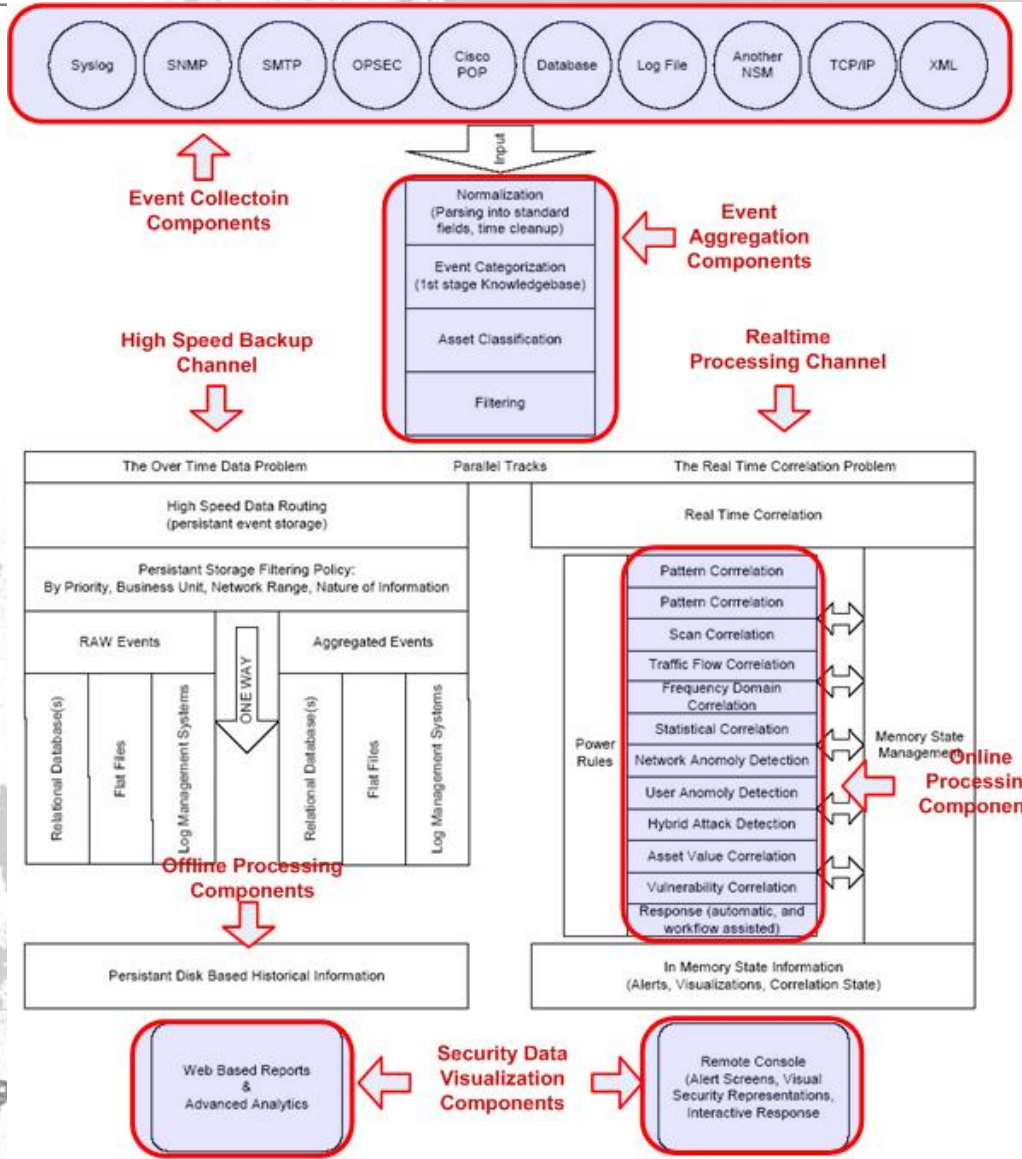
SNMP、SYSLOG、NTLOG、OPSEC、Database、XML



Protocol Independent Framework — PIF

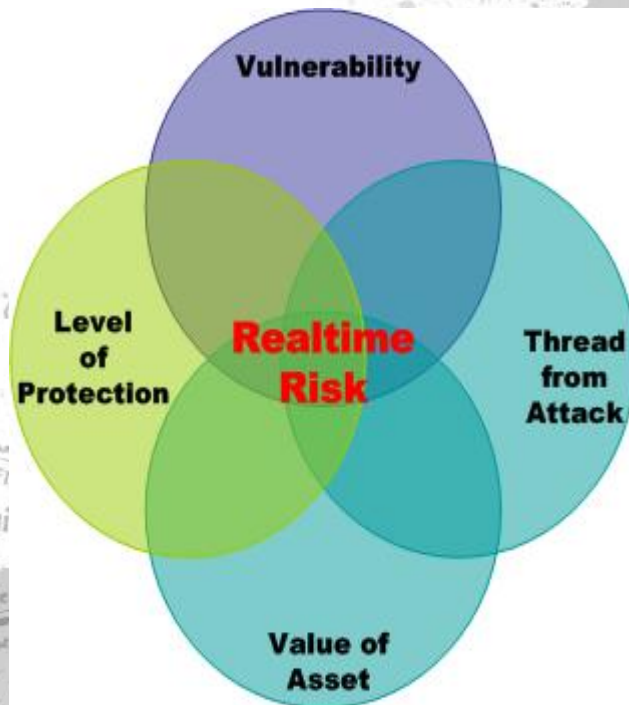


Components in Event Processing Flow



- Dynamic loading event collecting component according to event source's protocol
- Dynamic deploying online event processing component according to the event routing and processing policy
- Dynamic distributing visualization or UI component according the type of console





- Value of Asset, which is static, imported from asset evaluation by service & consulting
- Vulnerability found by scanner or penetration tester
- Thread presented by security events
- Protection refer to the level of countermeasures



- Collaboration between SEM and 3rd-party System or Device through Message Service provided by OpenSTF core
- Collaboration among peoples with role based workflow which begins with Transaction Service provided by OpenSTF Core



POST CARD

STUDIO FOTOGRAFIC
DANTE MORONI
Via S. ... N. 16
TORINO



17.3.1976

FOTOGRAFIA
Umberto Bonivento
PIOLA
Via Promontore

Stimabilissima
Contessa Monto
voglio dire

Atta mia amica
Non mi pare
si ricorda qualche
volta di me. Ah
ciao aff.
Umberto Piola

