用OpenSTF实现安全事件管理系统

郁朗 小蚁雄心团队

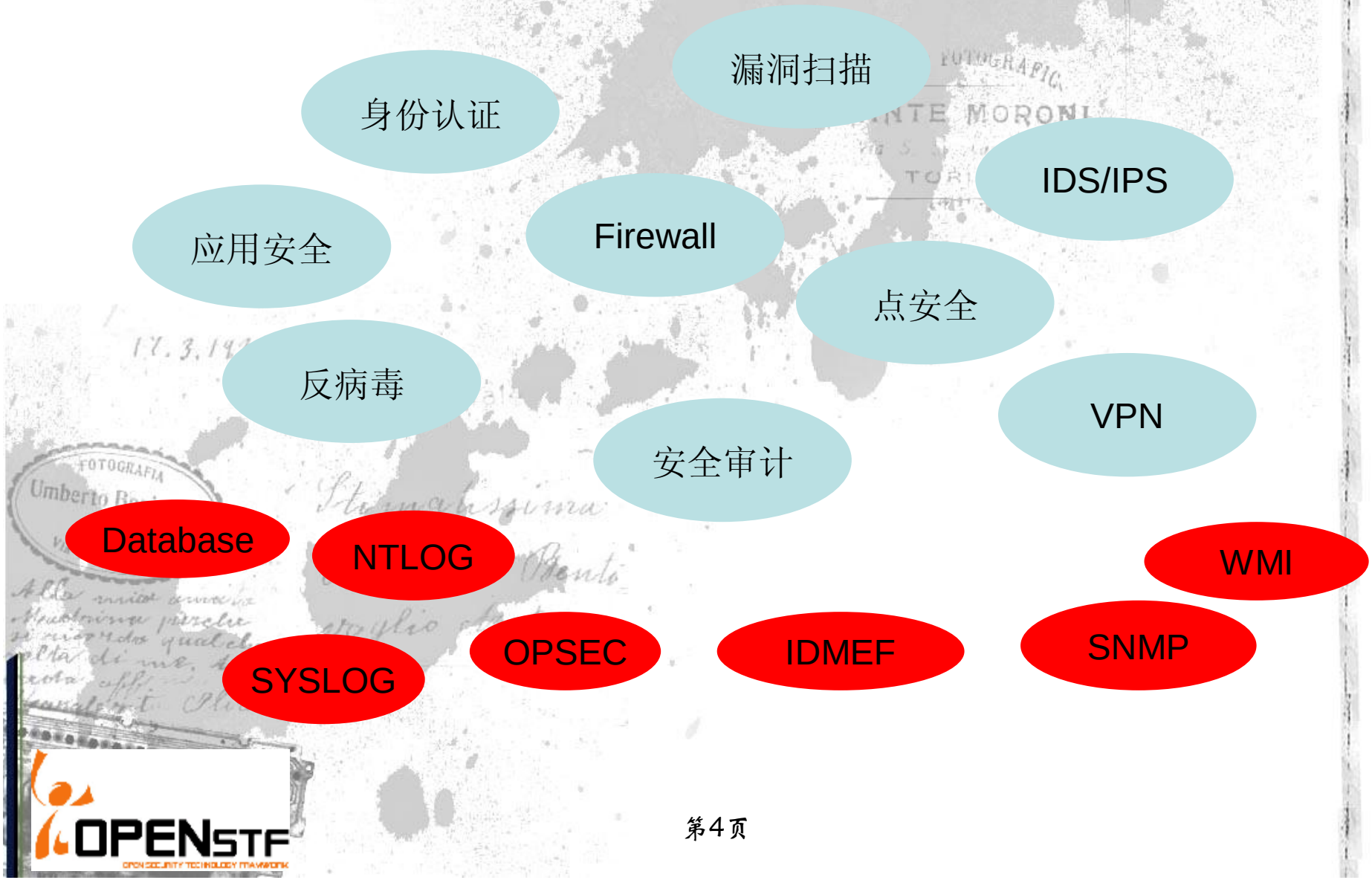
www.antpower.org

安全事件管理的需求分析

安全事件管理需求产生的背景

- 初步的建设引入了众多异构的安全技术，它们的运行效果无从量化
- 海量的安全事件充斥着大量不可靠的信息，从而变的毫无价值
- 制定安全策略的高层管理人员无法获得对安全态势的全局观
- 安全措施与它所保障的实际业务没有有效的关联
- 安全预警、安全防护、应急响应各子系统没有形成高效的闭环系统，导致安全体系的抗打击能力弱

异构的安全措施导致风险



海量安全事件不可人为管理

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

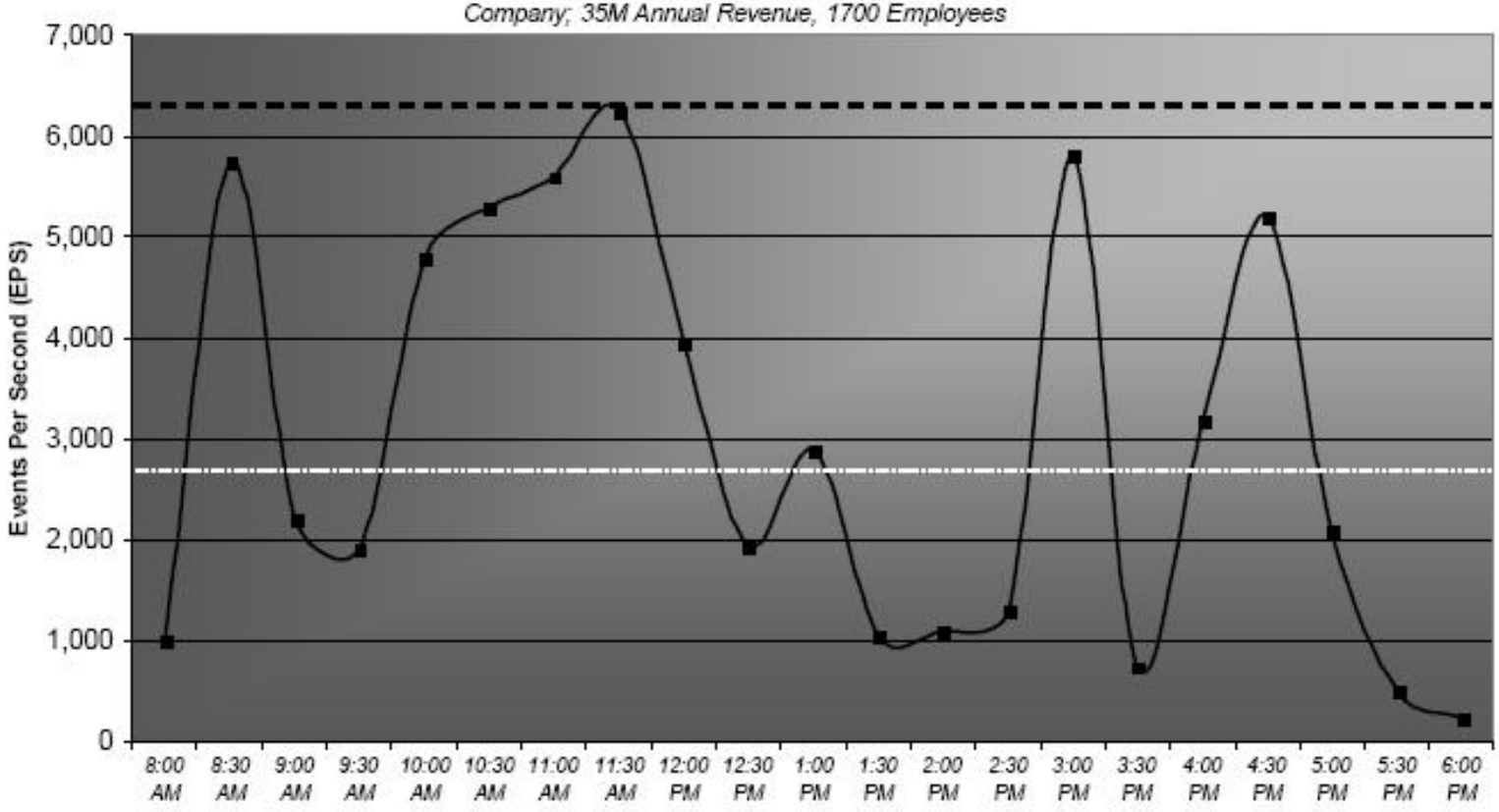


Chart 1: Sample Comparison of Peak and Average EPS Loads

IDS的漏报/误报现象

- 灵敏度和可靠度是IDS难以解决的一对矛盾
- IDS所处的网络层次和性能问题决定了其所获取和分析信息的局限性（Context-Free）
- IDS的信噪比的提高在于有效的事件管理

安全策略的制定缺乏全局观

- 目前的安全措施是初步的、局部的
- 没有有效的整体安全态势的表示方法
- 安全系统的总体风险不得不遵循水桶原理
- 领导和高层管理人员制定和修改安全策略时缺乏来源于实践的依据
- 你的安全系统是闭环的自反馈系统吗?

风险与实际价值的对应

- 资产的实际价值如何动态的体现到安全措施中
- 风险评估的结果如何在安全系统中充分体现
- 在用户的眼中“安全“不是目的，“业务应用”才是
- 实时的发掘潜藏的威胁

安全事件管理需求产生的背景

- 初步的建设引入了众多异构的安全技术，它们的运行效果无从量化
- 海量的安全事件充斥着大量不可靠的信息，从而变的毫无价值
- 制定安全策略的高层管理人员无法获得对安全态势的全局观
- 安全措施与它所保障的实际业务没有有效的关联
- 安全预警、安全防护、应急响应各子系统没有形成高效的闭环系统，导致安全体系的抗打击能力弱

我们对安全事件管理的定义

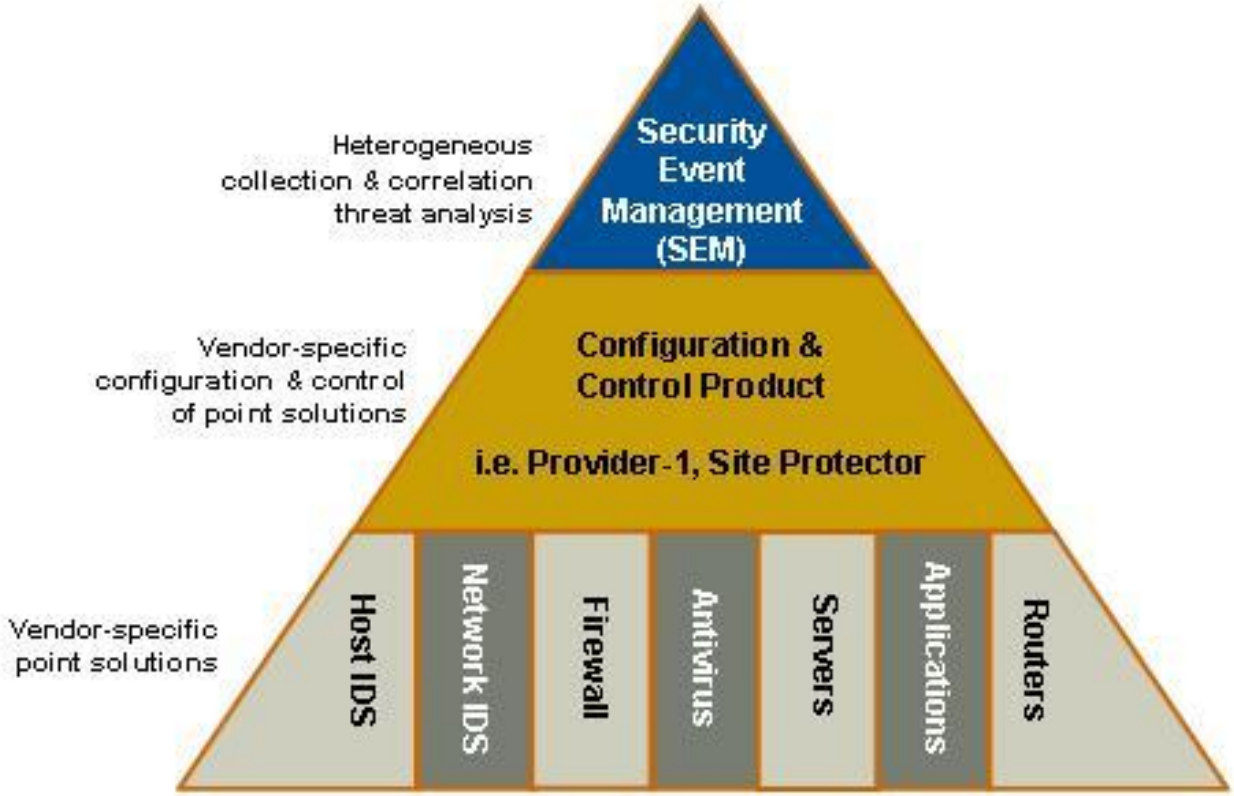
安全事件管理技术的创新在于能够实时的分析来自于计算/网络/存储/安全等设备的与安全相关的事件，其优势在于信息来源的广泛。通过关联来自于不同地点、不同层次、不同类型的安全事件，发现真正的安全风险，提高安全报警的信噪比，从而可以准确的、实时的评估当前的安全态势和风险，并根据预先制定策略作出快速的响应。

安全事件管理则代表了安全系统的动态模型，是系统智能的主要体现

SEM在安全体系中的层层次

Security Event Management – SEM

风险管理的核心部分



SEM的主要目标

- 安全事件整合和关联
- 风险的量化和风险的可视
- 形成闭环，及时响应

安全事件管理的底层技术手段

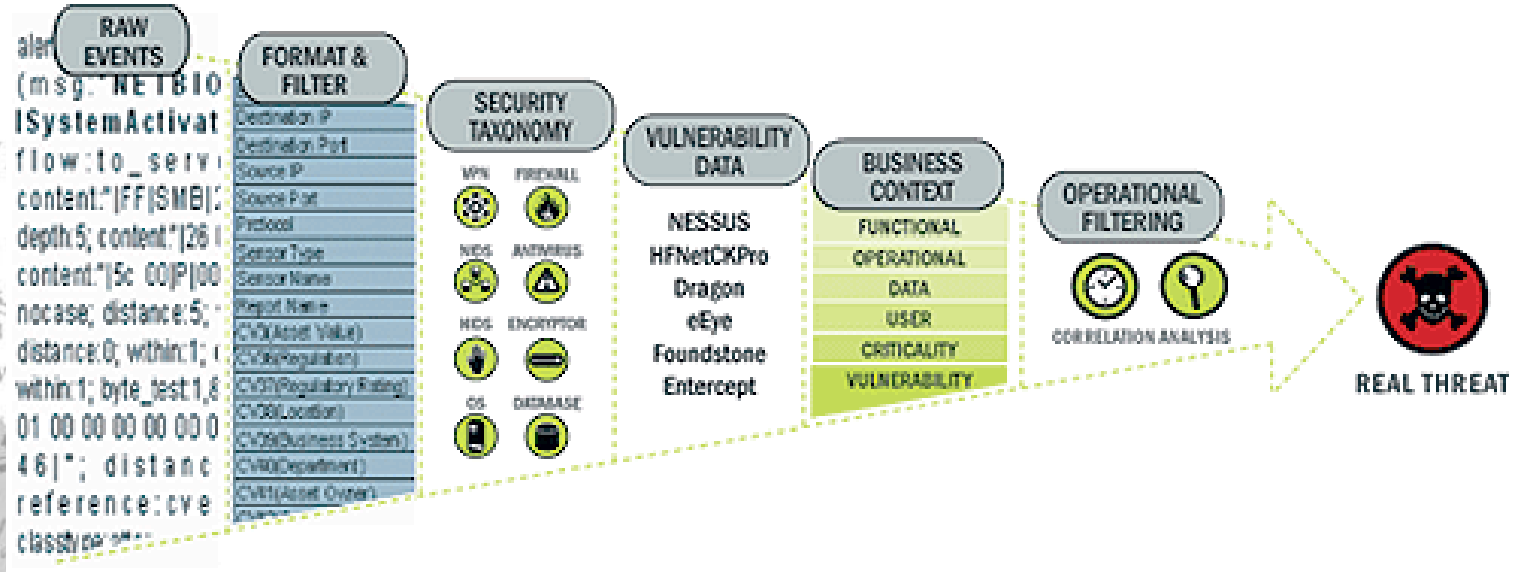
SEM要实现四化

- 统一化（Normalization）
- 整合化（Aggregation）
- 关联化（Correlation）
- 可视化（Visualization）

安全事件统一化采集？

安全事件如何整合

- 过滤
  - 冗余处理
  - 归纳分类
  - 绑定环境



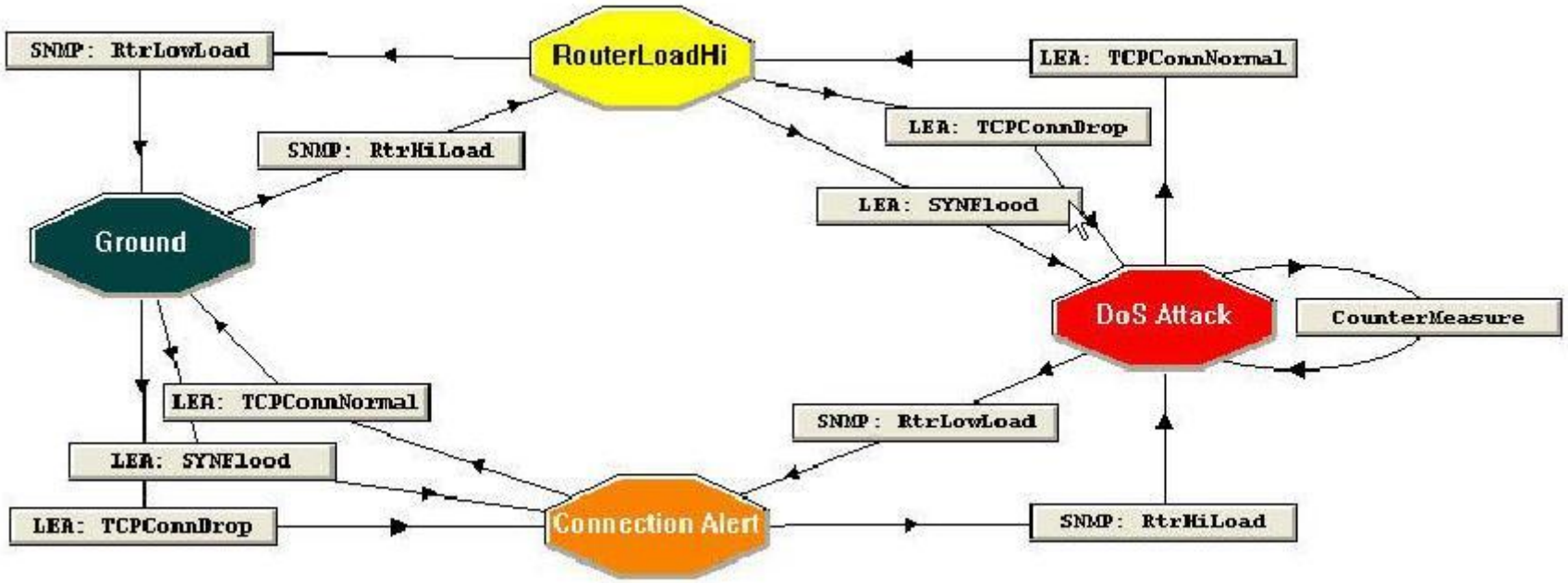
资产评估的结果促使事件的环境化

IP地址	资产价值	安全标准	安全等级	物理位置	业务	部门	所有者	操作环境
172.162.4.5	3000000	ISO7799	高	上海	项目申请服务	项目管理部	王明	SCO+MySQL
192.168.0.5	3500	商密标准	中	北京	门户网站	市场部	李艳	MSIIS 6.0
10.15.69.22	300200	无	低	大连	在线销售	销售部	赵卫红	Linux+MySQL
10.85.145.98	600000	无	无	南京	技术交流	技术部	刘海	RedhatLinux 9.0

图反映了资产的安全属性设置，这些属性在风险的实时计算中将发挥重要的作用

安全事件如何关联-基于规则

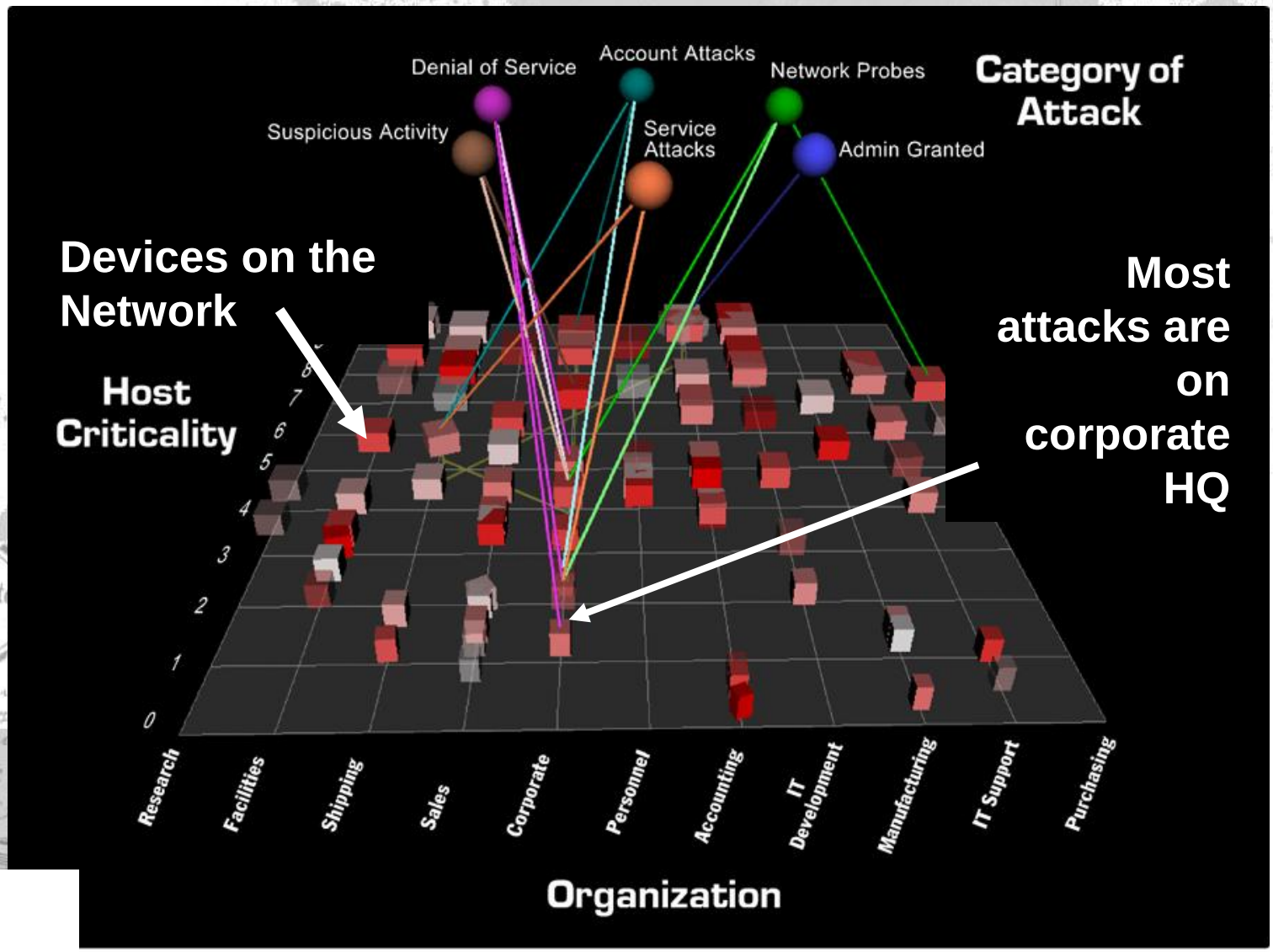
- 基于规则的事件关联，是由厂商、用户预先制定的规则对两个或两个以上的事件进行关联，以得出安全事件是否发生的准确判断。它基于较小的时间窗，实时性较强，但需要预先设定模式。



安全事件如何关联-基于统计

- 基于统计学的事件关联，是将系统在某一时间段内的信息进行统一，并参照一个阀值进行判断，最终得出对安全态势的一种判断。基于大时间窗，实时性较差，但不需要预先设定模式，较完整地反映系统的安全性。
- 定义一些大的安全事件类别，将出现的事件先归类，然后再根据大类出现的事件的安全级别和数量来估计发生的攻击。

数据挖掘-3维风险的可视化



SEM解决的实际问题

- 控制须人为处理的安全报警的规模和复杂度
- 减少安全事件的误报率
- 最大程度减轻潜在安全问题所带来的风险
- 加快应急响应速度
- 管理来自于入侵监测系统、防火墙、操作系统、反病毒、应用服务器、数据库的安全事件。

安全事件管理系统的实现

安全事件管理系统开发的特点

- 不只是技术层面的问题，还衔接了人和操作
- 应该是一种具备高度可扩展性的基础系统+一系列适应不同环境的解决方案
- 要经过二次开发形成最终管理系统
- 在设计开发手段上类似与用于企业管理的ERP系统

软件系统开发VS信息安全系统开发

Fred Brooks – IBM 360系统之父

《人月神话》中提出软件开发的根本性困难：

- 复杂性(complexity)
- 一致性(conformity)
- 易变性(changability)
- 不可见性(invisibility)

没有银弹！？

软件开发VS信息安全系统开发

- 软件工程（RUP、XP、CMM …）
- OO技术的迅速发展（MDA、UML、设计模式 …）
- 平台技术（系统平台、软件基础平台、业务基础平台）
- 中间件技术（消息中间件、交易中间件、对象中间件、数据访问中间件、应用服务器、安全中间件）

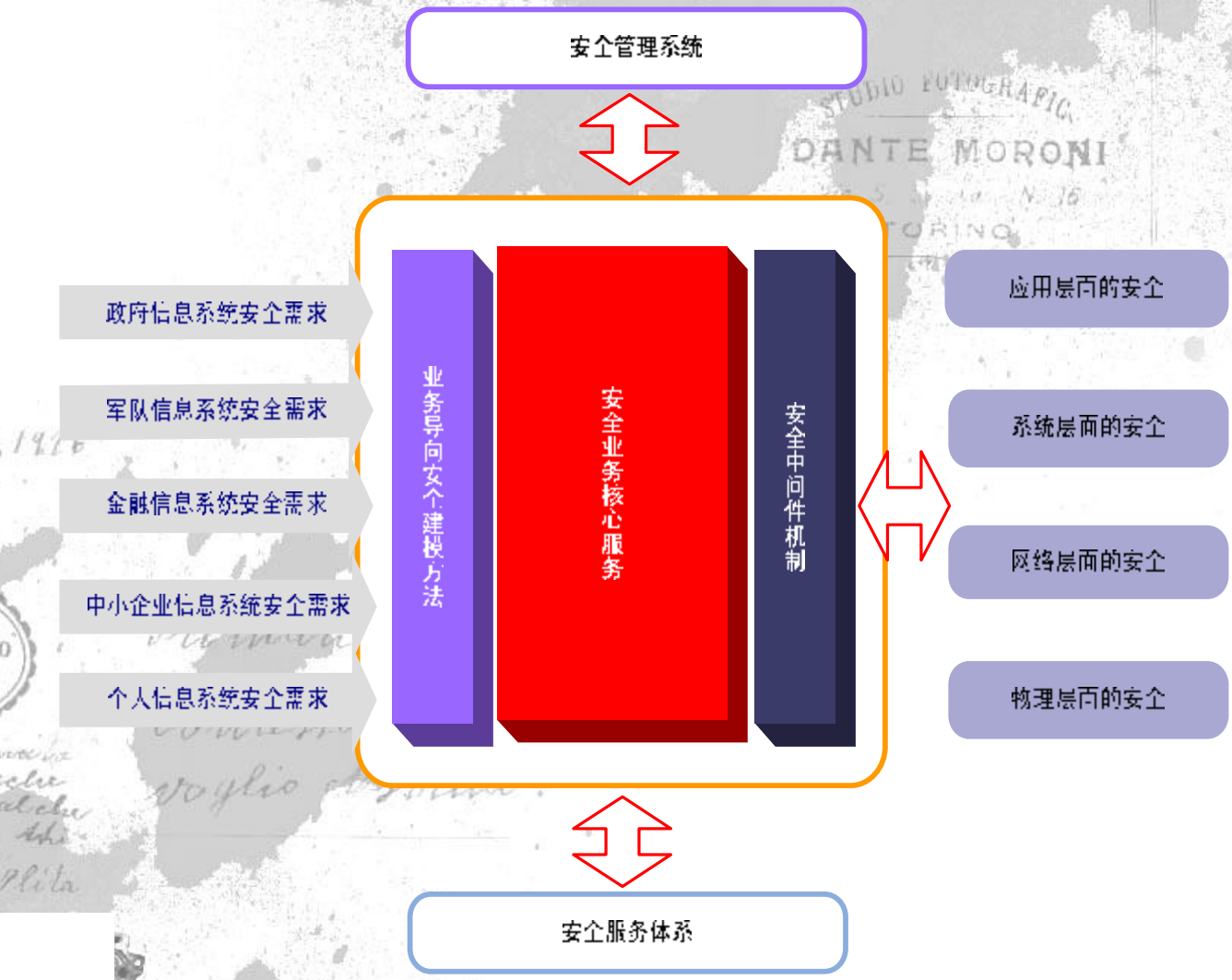
- 信息安全工程(ISSE/SSE-CMM)
- 安全管理（ISO17799/BSI7799)
- PKI/PMI
- 安全中间件
- 信息安全基础业务平台

总体目标

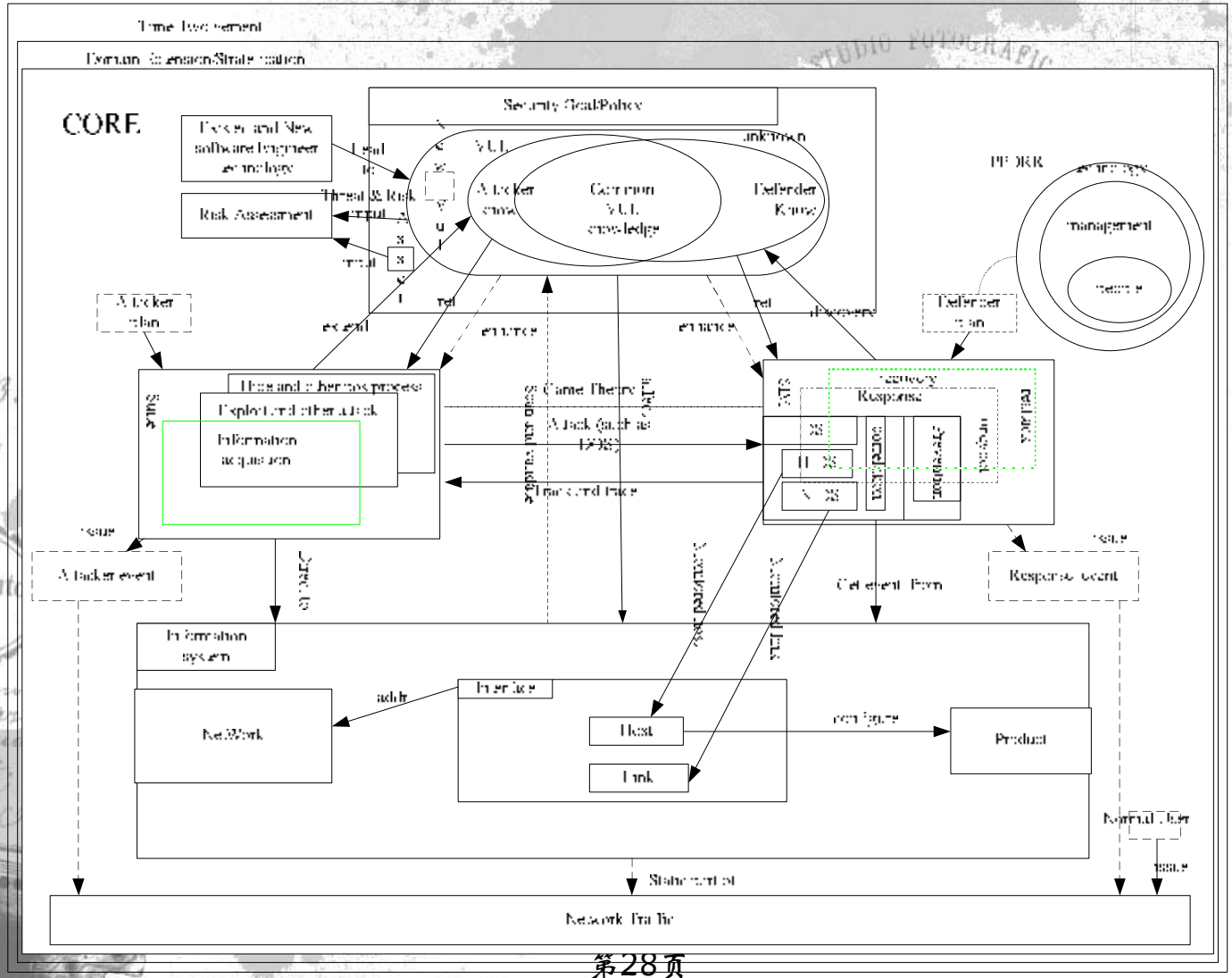
信息安全业务的平台

面向应用，解决信息系统安全子系统的互操作性、可扩展性、可管理性、并最终降低信息安全系统的总体拥有成本（TCO）！

信息安全业务的基础平台



攻防模型


CORE
Security Goal/Policy
Risk Assessment
Attacker Plan
Defender Plan
Information acquisition
Attacker event
Response event
Information system
Network
Host
Link
Product
Network Traffic

攻防模型

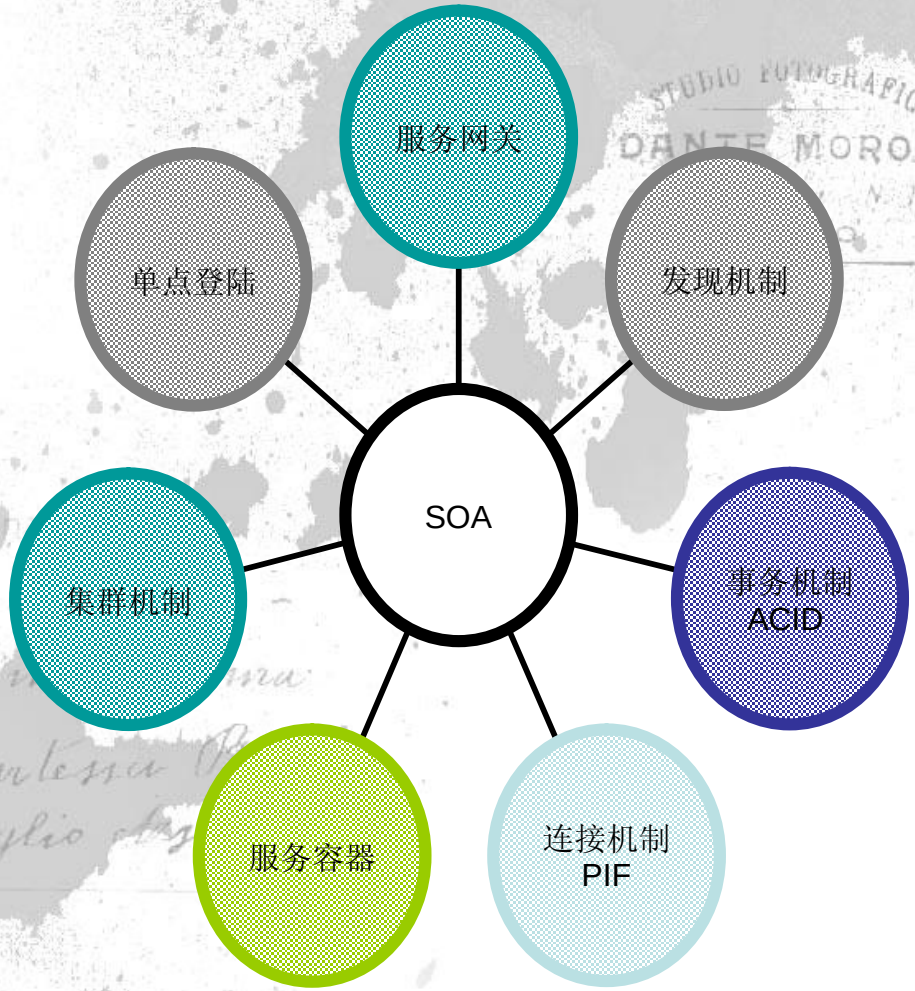
- 信息系统/资产（“Information System/ Asset”）
- 攻击方（“Attacker”）
- 防守方（“Defender ”）
- 安全目标/策略与脆弱性（“Security Goal/ Policy & VUL”）

基于SOA的核心

- 面向服务的设计模型是继面向对象的设计模型之后，又一次令人振奋的软件革命，它是随着分布式计算的日益发展而产生的
- Service Oriented Programming（SOP）是建立在OOP的基础之上的

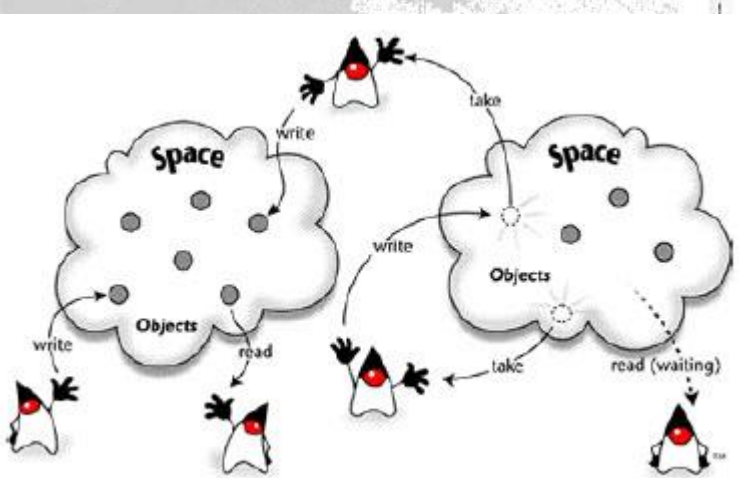
服务是一种预先由契约（**Contract**）定义好的行为，它由组件实现并对外提供，由其他组件访问和使用，这种服务的提供和使用的关系是靠契约（**Contract**）维系的，契约（**Contract**）在计算机程序的语境下就是接口（**Interface**）

SOA的一些基本概念



OpenSTF核心服务

- 组件服务
- 空间服务（域服务）
- 策略服务
- 消息与事务服务
- 内部安全服务（身份认证、
- 统一界面框架服务（GUIStarter）



中间件的基本概念

- 中间件（Middleware）是基础软件的一大类，属于可复用软件的范畴。IDC对其的定义是：中间件是一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源，中间件位于客户机服务器的操作系统之上，管理计算资源和网络通信
- 中间件不仅仅实现互连，还要实现应用之间的互操作；中间件是基于分布式处理平台的软件

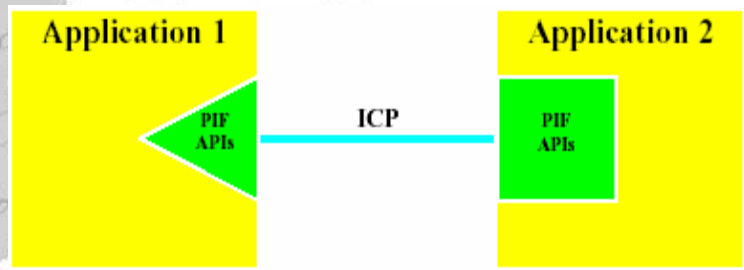
OpenSTF安全中间件

- 中间件是组件的集合，这些组件共同完成某一种类的安全功能；
- 中间件中的各个组件通过OpenSTF核心服务互联与协作；
- 中间件是产品发布的形态，即发行包，其属性包括唯一标识、厂商、版本、安全特性、组件列表；
- OpenSTF通过组件服务管理中间件及其组件

安全事件的数据交换

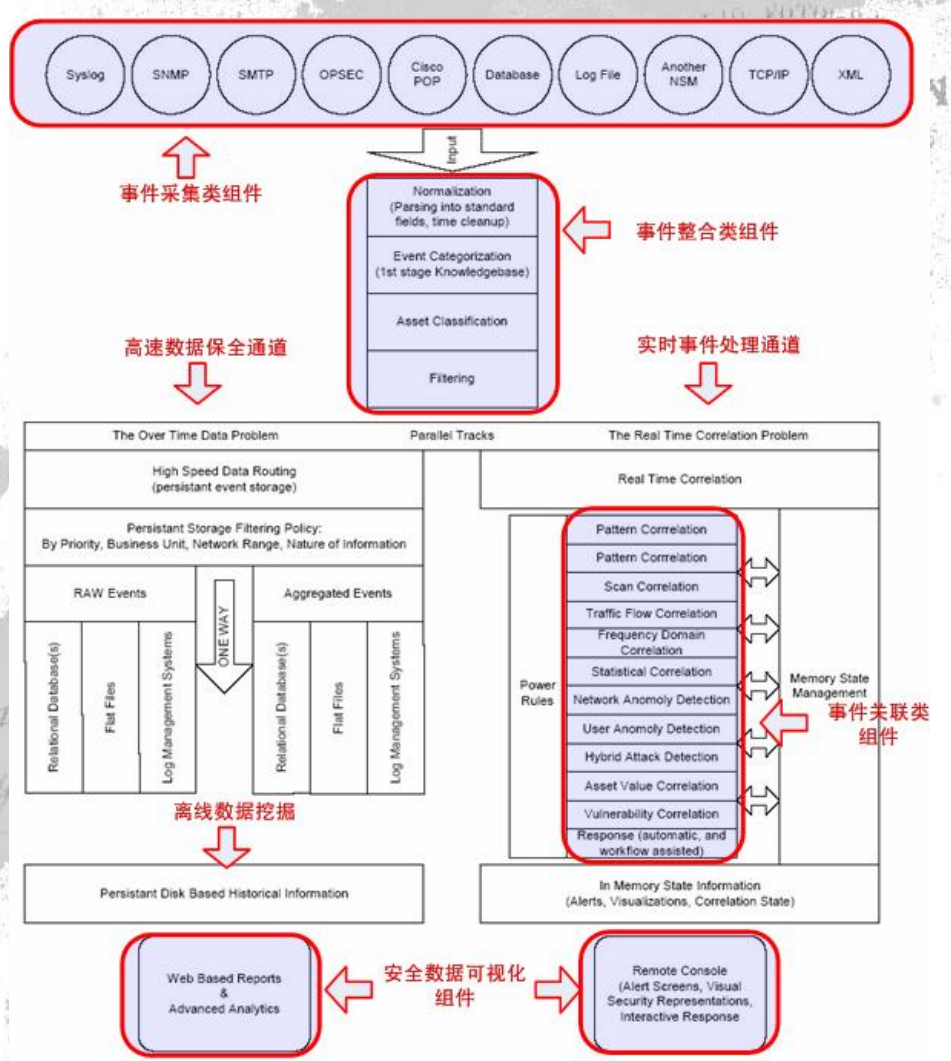
- 解决了安全事件在各个处理组件的数据交换问题

SNMP、SYSLOG、NTLOG、OPSEC、Database、XML



Protocol Independent Framework—PIF

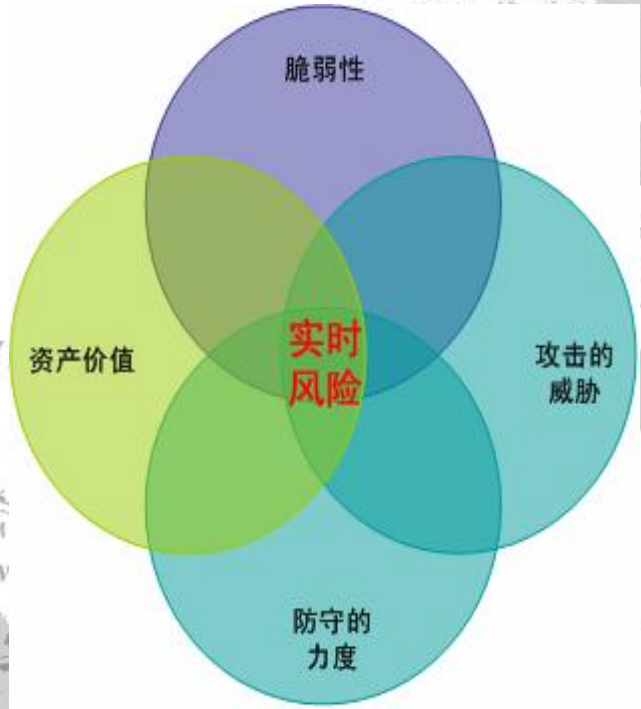
安全事件处理流的组件化



OpenSTF组件VS安全事件管理

- 事件采集组件根据应用环境动态分发和加载
- 事件处理组件根据事件路由和处理策略动态分发和加载
- 事件可视化组件根据用户终端的类型动态分发和加载

基于攻防模型的实时风险分析



- Value（资产价值）是静态的，可以由安全服务资产评估的过程引入系统；
- Vulnerability（脆弱性）可以由漏洞扫描软件或者人为的去评估；
- Thread主要有各类安全事件所代表；
- Protection则表示防守方针对潜在的威胁所作的防护措施。

安全事故的应急响应

- 基于OpenSTF的消息服务实现安全设备与系统的联动
- 基于OpenSTF的事务机制实现工作流

X'con 2004

OPENSTF

OPEN SECURITY TECHNOLOGY FRAMWORK