2021-2022学年春季学期

网络空间安全态势感知

Cyber security situation awareness

授课团队：刘宝旭 卢志刚 刘玉岭

助　　教：李　宁

网络空间安全态势感知

Cyber security situation awareness

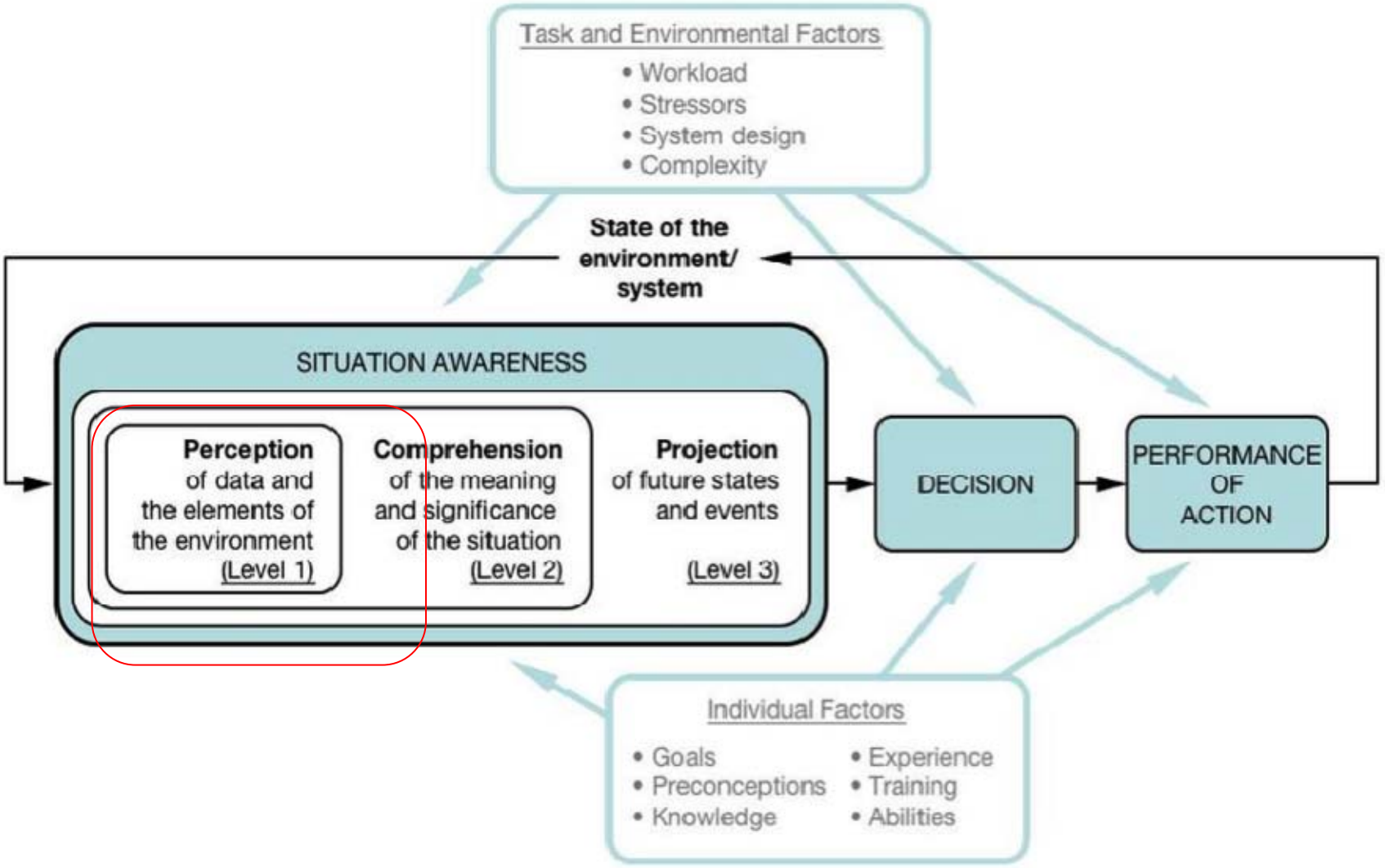
[第5次课] 网络安全态势要素获取技术

授课教师：刘玉岭

授课时间：2022.3.7

内容概要

态势感知技术体系

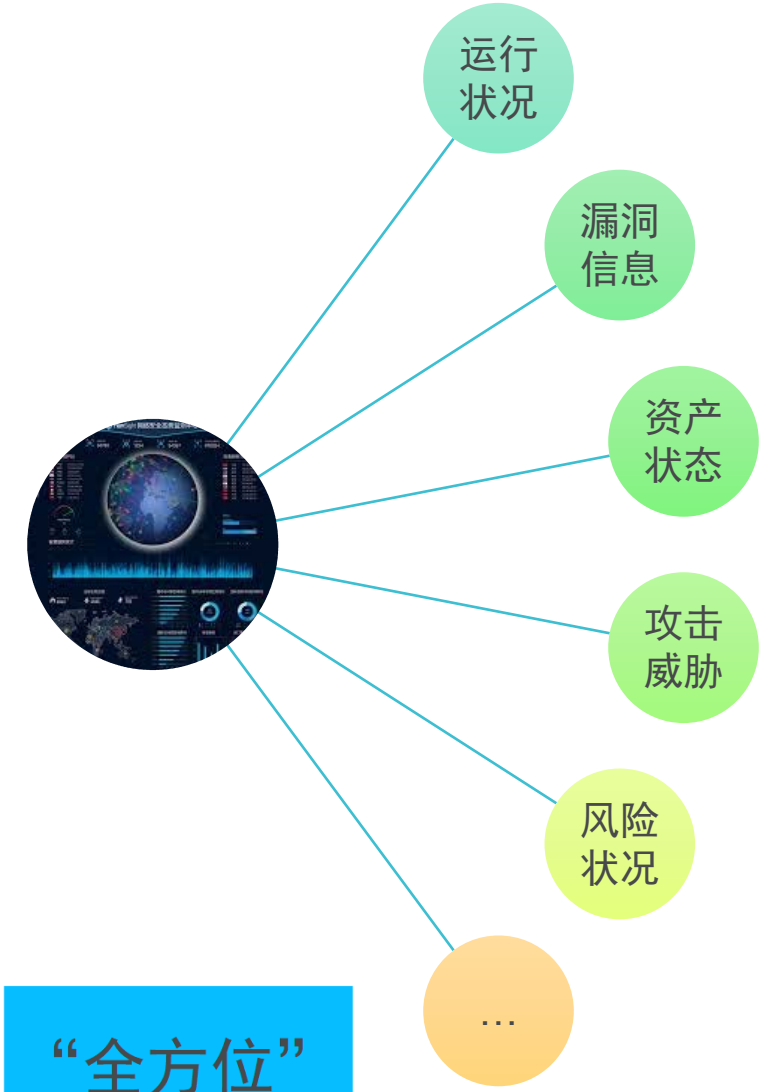

Task and Environmental Factors
• Workload
• Stressors
• System design
• Complexity
State of the environment/ system
SITUATION AWARENESS
Perception of data and the elements of the environment (Level 1)
Comprehension of the meaning and significance of the situation (Level 2)
Projection of future states and events (Level 3)
DECISION
PERFORMANCE OF ACTION
Individual Factors
• Goals
• Preconceptions
• Knowledge
• Experience
• Training
• Abilities

需要思考的问题？

① 网络空间安全态势要素获取中的权衡点在于？取舍原则是？
② 现有态势要素表示方法中最大的问题是？

一、主要态势要素及内涵（1）

- 态势要素分类标准和方式不一
  - 系统配置信息、系统运行信息、…
  - 资产、威胁、脆弱性、…
  - 资产状态、运行状况、漏洞信息、攻击威胁、攻击信息、风险状况，…
  - …



“全天候”

“全方位”

一、主要态势要素及内涵（2）

攻击方态势要素：攻击组织、工具、方法、地点、步骤、…

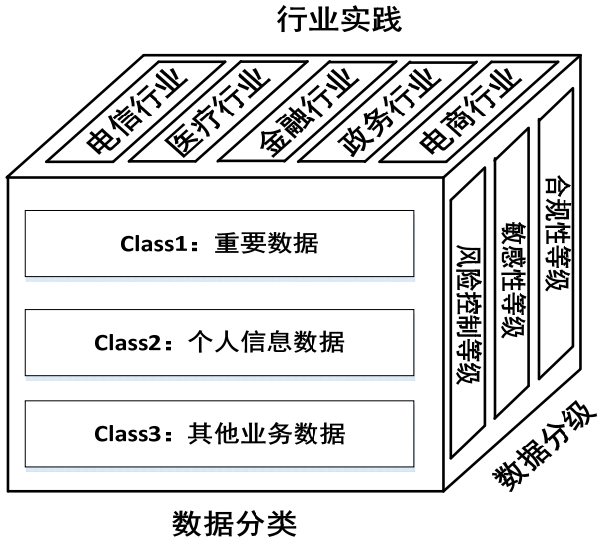
防御方态势要素：脆弱性、防护措施、人员组织、…

攻防环境态势要素：拓扑结构、资产运行情况、补丁修复情况、策略配置情况、风险状况、…

内容概要

二、态势要素获取方法（1）

- 态势要素选取原则
  - 代表性和准确性之间的权衡
- 常用解决方案
  - 数据分类、分级
  - 数据标签、追溯分析
  - 业务导向、绩效评估



- 态势要素选取原则
  - 隐私与效率之间的平衡

类别	子类及范围
（A类）用户身份相关数据	**（A1）用户身份和标识信息**：（A1-1）自然人身份标识、（A1-2）网络身份标识、（A1-3）用户基本资料、（A1-4）实体身份证明、（A1-5）用户私密资料 **（A2）用户网络身份鉴权信息**：（A2-1）密码及关联信息
（B类）用户服务内容数据	**（B1）服务内容和资料数据**：（B1-1）服务内容数据、（B1-2）联系人信息
（C类）用户服务衍生数据	**（C1）用户服务使用数据**：（C1-1）业务订购关系、（C1-2）服务记录和日志、（C1-3）消费信息和账单、（C1-4）位置数据、（C1-5）违规记录数据 **（C2）设备信息**：（C2-1）设备标识、（C2-2）设备资料

二、态势要素获取方法（2）

数据来源

已有网络安全基础设施

合作单位

信息安全企业和互联网企业的威胁情报信息

…

技术手段

流量监测

主动探测

部（端）点监测

蜜罐捕获

边界感知

样本分析鉴定

检查工具

…

存储方式

数据分类存储：基础知识数据、基础资源数据、业务资源数据

数据分级存储

存储架构：结构化、非结构化

…

二、态势要素获取方法（3）

常见要素获取方法

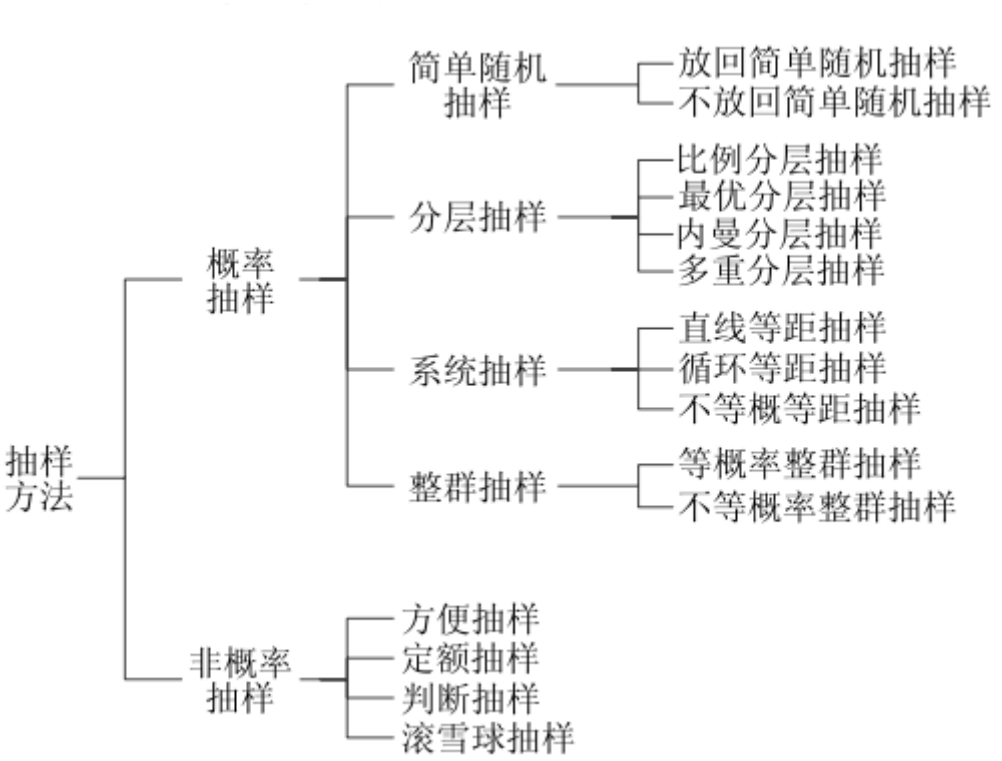
- 抽样
- 分光
- 爬虫
- 监测
- 汇聚
- 订阅
- …

基础类数据

定向类数据

二、态势要素获取方法（4）

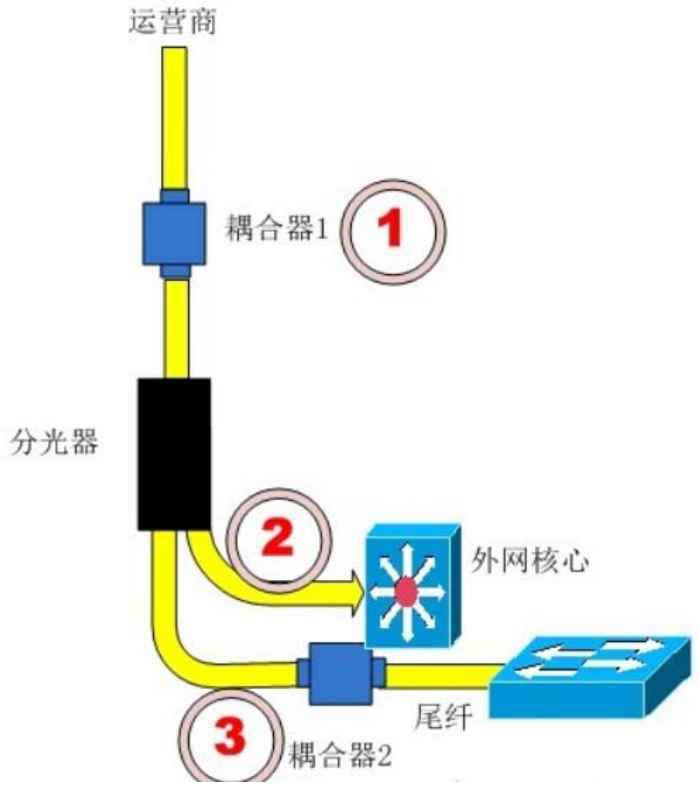
- 数据抽样方法
  - 由统计学而来的方法
  - 适用场景：原始数据量很大，业务承载度受限
  - 基于“过滤器” 的抽取
    - 业务场景-业务规则集



“管中窥豹、可见一斑”，亟需先验知识的辅助

二、态势要素获取方法（5）

- 数据分光方法
  - 一种物理学的方法
  - 类似的方法为“镜像方法”
  - 适用场景
    - 原始数据价值较高或级别较高
    - 关系紧密度高或使用权限高
    - 对抗DDoS攻击的利器
  - 优缺点
    - 优点：可靠性高、采集成本低
    - 缺点：使用场景受限



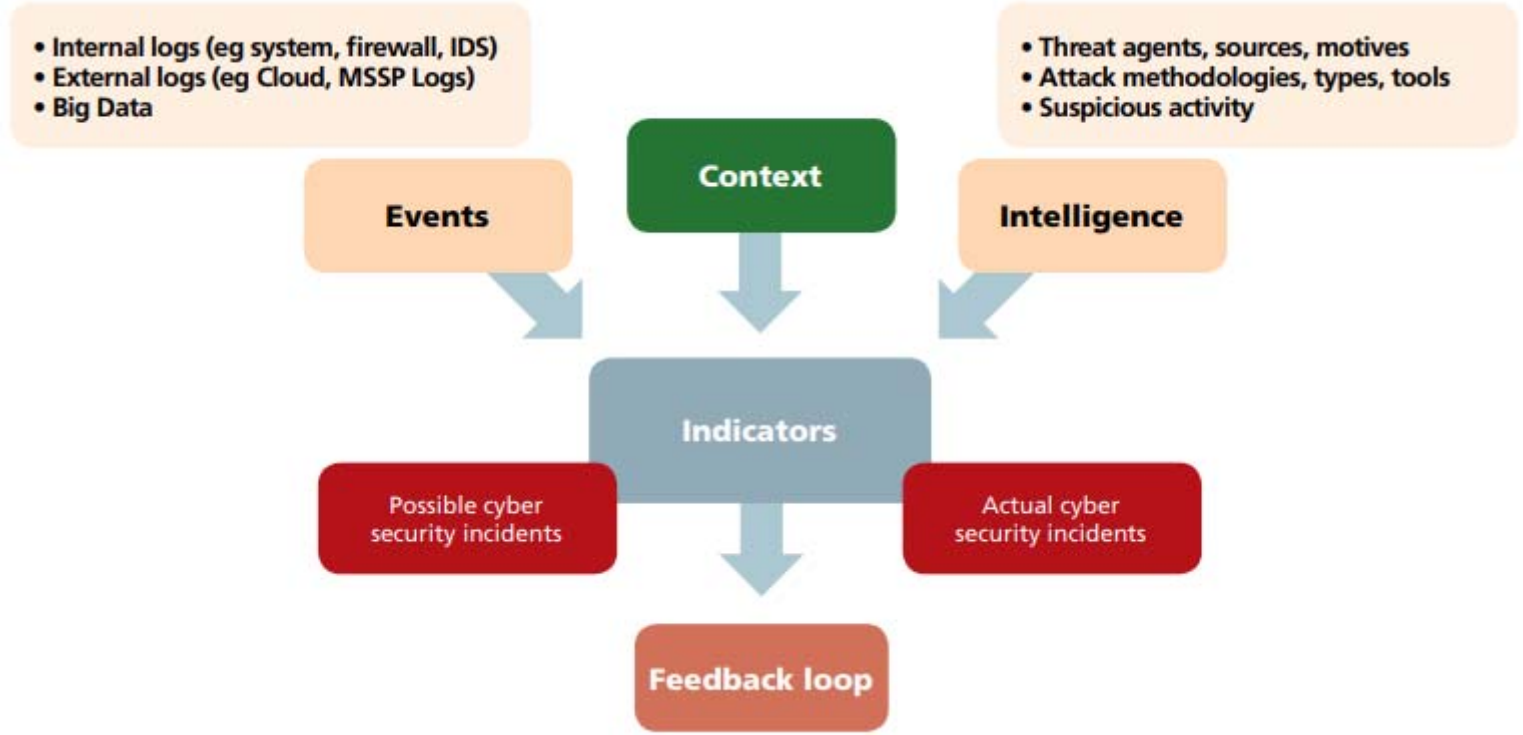
分光器物理连接示意图

二、态势要素获取方法（6）

- 数据爬虫方法
  - 数据采集中常用的方法，但不是安全数据采集中的常用方法
  - 适用场景
    - 社交类网络数据采集：微博、知乎
    - 定向事件的扩展数据采集
    - 网络安全中更为使用嗅探、扫描等
  - 优缺点
    - 优点：技术成熟，工具众多；利于统计分析
    - 缺点：对安全关键数据的采集能力有限：威胁特征、脆弱性信息、…

二、态势要素获取方法（7）

- 数据监测方法
  - 严格来讲不是一种方法，是安全数据采集中的常用方式
  - 一般需要设备、盒子、系统的辅助：IDS、WAF、漏洞检测等



二、态势要素获取方法（8）

- 汇聚和订阅方法
  - 获取外部安全数据的常用方式
  - 汇聚方法
    - 数据可能是原始数据，也可能是加工后的数据
    - 需要制定数据汇聚标准，统一接口规范
  - 订阅方法
    - 一般获取的是高层次信息，需要支持机读
    - 研究热点：订阅信息的动态更新、效益评价
    - 经典案例：Falcon Threat Intelligence、Fireeye、微步在线等

内容概要

三、态势要素获取关键技术（1）

- ✓ 获取方式
  - 流量监测
  - 主动探测
  - 部（端）点监测
  - 蜜罐捕获
  - 边界感知
  - 样本分析鉴定
  - 检查工具
  - …
- ✓ 预处理技术手段
  - 数据去重技术
  - 数据补全技术
  - 数据质量评估技术
  - …

三、态势要素获取关键技术（2）

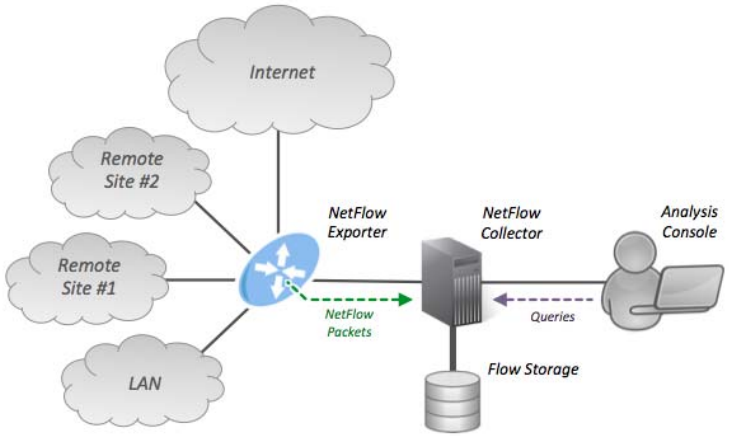
- 态势要素获取技术手段--流量监测
  - 以网络流量为感知对象，部署于IP层之上
  - 分为串行（直路）检测和针对镜像数据（旁路）的检测（BGP路由等）
  - 数据输出：
    - 五元组：源IP地址，源端口，目的IP地址，目的端口，和传输层协议
    - Netflow：收集进入及离开网络界面的IP包的数量及信息，分析Netflow收集到的信息，可获取数据包的来源及目的地、网络服务的种类、以及造成网络拥塞的原因
    - 扫描探测、SQL注入、漏洞利用、后门控制、异常流量等安全信息
    - 定制化内容

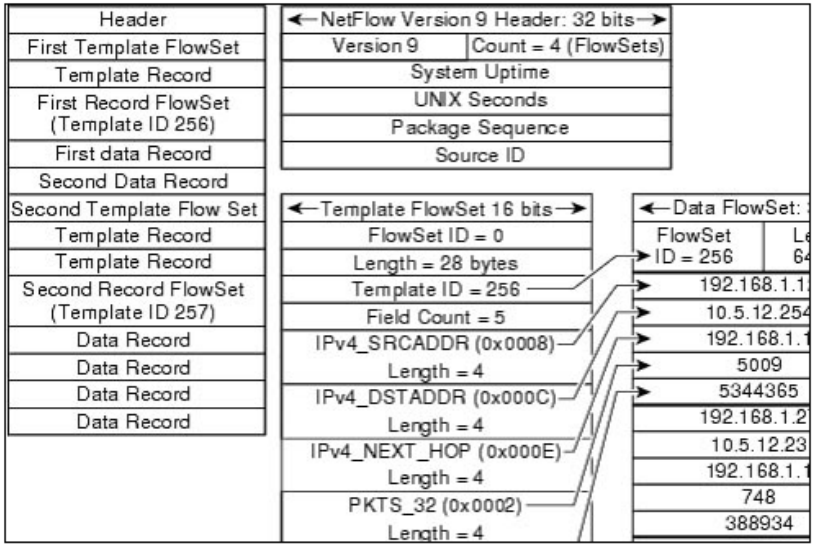
FloCon会议：https://flocon2018.sched.com/

2019年会议：https://resources.sei.cmu.edu/news-events/events/flocon/

三、态势要素获取关键技术（3）

- 态势要素获取技术手段--流量监测--Netflow
  - Cisco公司主导开发，NetFlow V1、NetFlow V5、NetFlow V7、NetFlow V8和NetFlow V9等5个主要的实用版本
  - 涵盖IP数据包的7个基本属性：源IP地址；目标IP地址；源通信端口号；目标通信端口号；第三层协议类型；服务类型（TOS）字节；网络设备输入或输出的逻辑网络端口
  - 支持定制，包括输出流版本、个数、缓冲区大小；流量采集端的汇聚、过滤策略、文件存放目录、格式等
  - 非采样和采样两种使用模式





三、态势要素获取关键技术（4）

- 态势要素获取技术手段--流量监测-常见工具
  - 简单网络管理协议SNMP
  - 网络映射器NMAP
  - 抓包工具：如Sniffer Pro、Wireshark
  - Fiddler：适用于任何平台和任何操作系统
  - Nagios：免费、开源、常用
  - Zenoss：企业级、提供统计分析
  - IDS、IPS、VDS、TDS、Firewall、UTM、NGFW等
  - ...
  - 定制化盒子：业务导向，输出内容导向

三、态势要素获取关键技术（5）

- 态势要素获取技术手段—主动探测
  - 以端为感知对象，但部署于其他端点上，或者是专用设备上
  - 采用主动发送报文，或者获取反馈数据进行判断的方式
  - 具体工作机理分为：扫描、爬取
  - 表现形态：漏洞扫描器、WEB扫描器、网络爬虫
  - 云环境、工业互联网、物联网等的扫描
  - 主动防御的绕过
  - 。。。

三、态势要素获取关键技术（6）

- 态势要素获取技术手段—蜜罐俘获（1）
  - 以端为感知对象，但部署于其他端点上
  - 采用构造或模拟漏洞，以及其他引诱手段，等待攻击方探测发现，以感知攻击方并记录攻击过程
  - 表现形态
    - 虚拟机蜜罐、蜜罐网、分布式蜜罐
    - 高交互蜜罐、低交互蜜罐

三、态势要素获取关键技术（7）

● 态势要素获取技术手段—蜜罐俘获

概念提出

1989年出版的《The Cuckoo’s Egg》给出了商业间谍案追踪的案例

- Cohen研发了专门工具DTK，给出了信息对抗领域中欺骗技术的框架和模型

蜜网技术

早期蜜罐交互程度低、捕获信息有限

- Spitzner 等提出蜜网技术，由多个蜜罐系统加上防火墙、入侵防御、系统行为记录、自动报警与数据分析等辅助机制构成

分布式蜜网

传统蜜罐技术监测范围受限

- 分布式蜜罐、蜜网于 2005 年提出（Kanga 分布式蜜网系统）
- 案例：The
- Kanga 及其后继 GDH 系统、欧洲电信的 Leurre.Com与
- SGNET系统、中国 Matrix 分布式蜜罐系统等

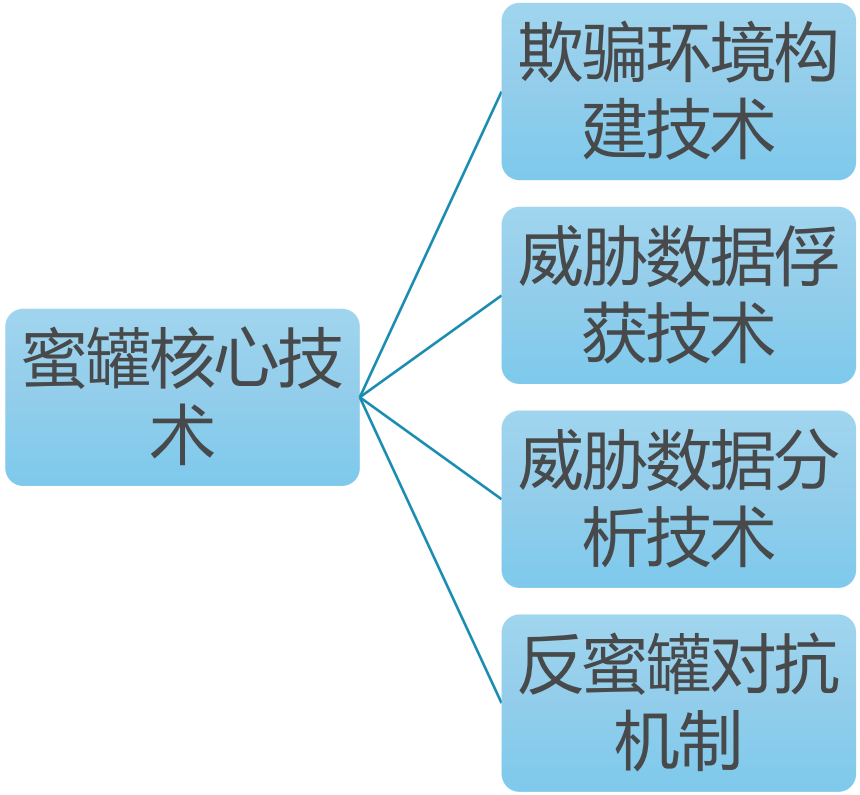
蜜场

分布式蜜网大量的硬件设备、较多的人力成本

- 2003 年Spitzner提出了蜜罐系统部署的新型模式—蜜场
- 基于蜜场技术实现的网络威胁预警与分析系统：Collapsar、Potemkin和Icarus

三、态势要素获取关键技术（8）

- 态势要素获取技术手段—蜜罐俘获（3）



风险控制机制：法律、实施策略等

配置、管理、维护机制

三、态势要素获取关键技术（9）

- 态势要素获取技术手段—分析鉴定（1）
  - 以疑似威胁载荷为对象
  - 采用静态判定、动态沙箱鉴定为手段
  - 可以增强其他环节判定能力，并感知威胁载荷更多关联行为，从而完善事件链
  - 表现形态：独立产品或内嵌入其他产品
- 关键技术
  - 加壳加密混淆技术
  - 动态加载分析技术
  - 分析对抗技术
  - …
- 检测点
  - 文件类API
  - 网络类API
  - 注册表类API
  - 系统调用类API
  - 进程操作类API

三、态势要素获取关键技术（10）

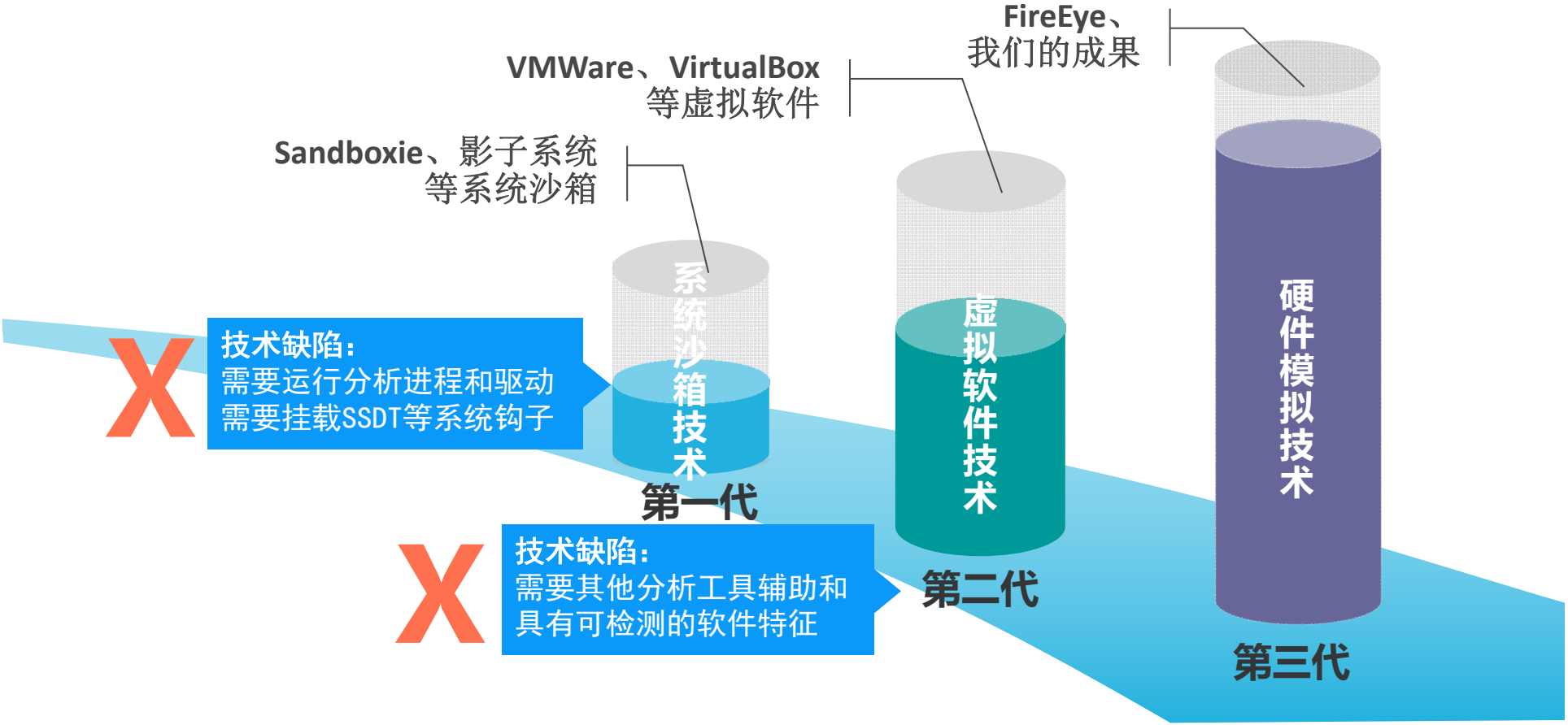
● 态势要素获取技术手段—分析鉴定（2）

防检测
虚拟机系统完全纯净，不做修改

防篡改
从模拟硬件直接提取原始数据

防穿透
所有代码经过模拟器翻译执行

防干扰
数据提取与数据分析相互隔离



三、态势要素获取关键技术（11）

- 态势要素获取技术手段—端点防护（1）
  - 以端为感知对象，部署于端点之上
  - 采用主动防御、实时监测、定时扫描、白名单对比等方式
  - 表现形态：企业反病毒、网站防篡改、内网管理系统、私有云防护等

- 移动化管理
- 国产终端安全
- 虚拟终端安全
- 边界安全
- 内网安全
- 防病毒

● 态势要素获取技术手段—端点防护（2）

网页防篡改技术

外挂轮询技术

用一个网页读取和检测程序，以轮询方式读出要监控的网页，与真实网页相比较，来判断网页内容的完整性，对于被篡改的网页进行报警和恢复

核心内嵌技术

将篡改检测模块内嵌在Web服务器软件里，它在每一个网页流出时都进行完整性检查，对于篡改网页进行实时访问阻断，并予以报警和恢复

事件触发技术

利用操作系统的文件系统或驱动程序接口，在网页文件的被修改时进行合法性检查，对于非法操作进行报警和恢复

三、态势要素获取关键技术（13）

- 态势要素获取技术手段—检查工具（1）
  - 以端为感知对象，部署于便携介质或便携设备上
  - 采用连接（接入）后扫描检测的方式
  - 表现形态：等保检查工具、保密检查工具
  - 合规性检查：法律法规、标准规范

- 等级保护
  - 信息安全等级保护==》网络安全等级保护
  - 信息系统==》信息系统+云系统、大数据、工控系统、移动互联网等

- 态势要素获取技术手段—检查工具（2）
  - 等级保护安全检查工具构成

三、态势要素获取关键技术（15）

- 态势要素获取技术手段—检查工具（3）
  - 等级保护安全检查工具构成
    - Windows主机安全配置分析工具
    - Linux主机安全配置分析工具
    - 病毒检查工具
    - 木马检查工具
    - 网络及安全设备检查工具
    - 网站安全检查工具
    - 网站恶意代码检查工具
    - 弱口令检查工具
    - 数据库安全检查工具
    - ...

三、态势要素获取关键技术（16）

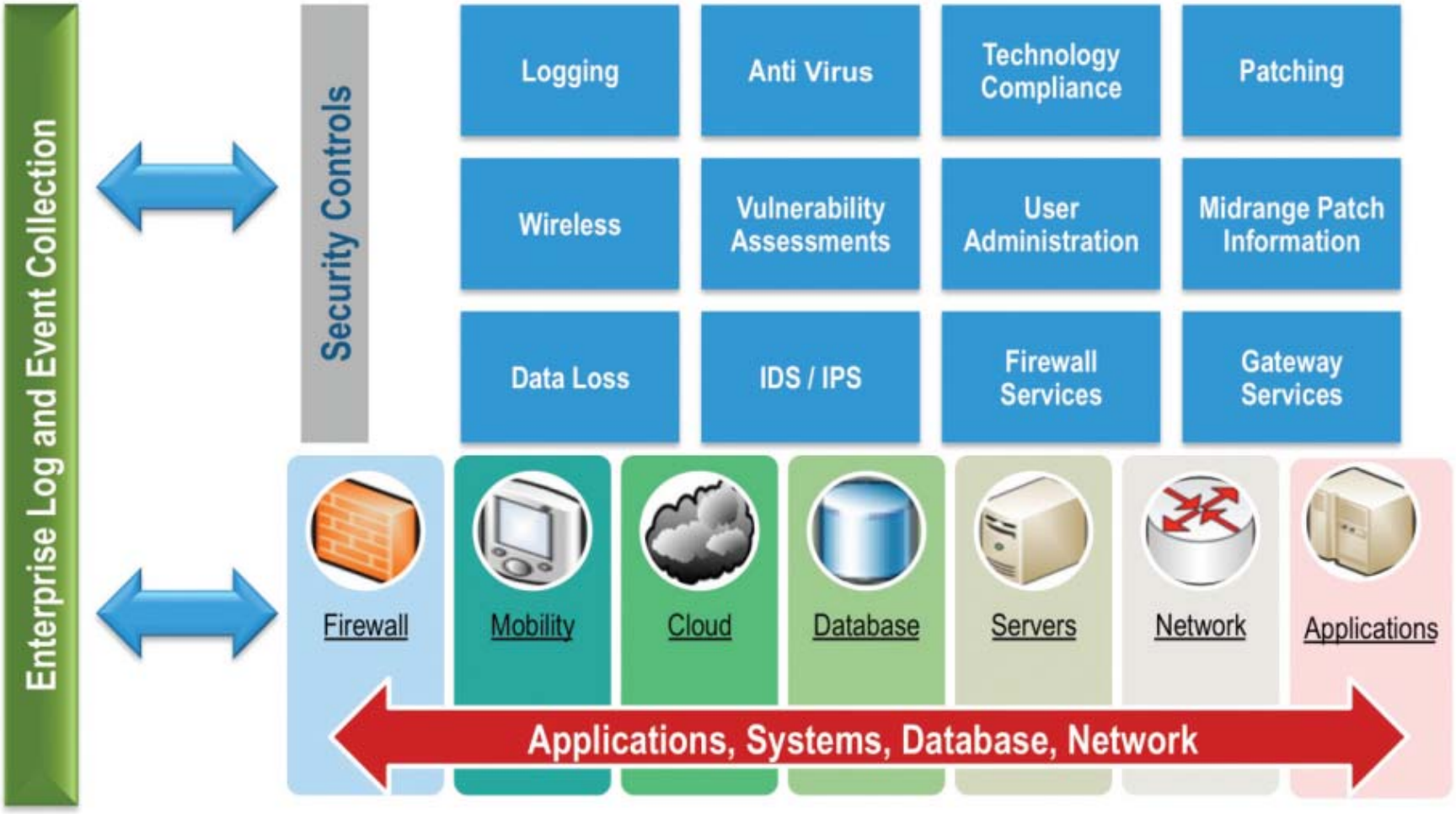
三、态势要素获取关键技术（17）

- 态势要素获取技术手段对比分析

	数据输入	数据输出	接入带宽占用	公网链接需求
流量监测	流量	检测结果及对应的元数据（五元组、收发件人、APP_ID、）、还原威胁载荷样本、被缓存的流量等	无	有
主动探测	地址范围、域名列表	域名、IP地址、URL、事件名称、威胁样本或有害数据等	大	有
蜜罐捕获	扫描攻击流量	检测结果	小	有
分析鉴定	文件样本	检测结果 动静态分析向量和报告	无	可能需要
端点防护	文件对象 内存对象 扇区对象	检测结果	N/A	N/A
检查工具	主机场景	检测结果 分析报告 提取物	无	无

三、态势要素获取关键技术（18）

- 态势要素获取实例—日志获取



三、态势要素获取关键技术（1）

- ✓ 获取方式
  - 流量监测
  - 主动探测
  - 部（端）点监测
  - 蜜罐捕获
  - 边界感知
  - 样本分析鉴定
  - 检查工具
  - …
- ✓ 预处理技术手段
  - 数据去重技术
  - 数据补全技术
  - 数据质量评估技术
  - …

三、态势要素获取关键技术（1）

- 态势要素预处理技术—数据去重技术

- 考虑因素
  - What：对何种数据进行消重?
  - When：何时进行消重?
  - Where：在何处进行消重?
  - How：如何进行消重?

- 技术分类
  - 内容识别：基于散列识别、基于内容识别
  - 数据处理时间：在线重删除、后删除
  - 数据粒度：文件级、数据块级、字节级
  - 数据块分块方法：变长分块重删、定长分块重删
  - 数据处理位置：源端重删、目的端重删

数据来源、信誉及质量是未来关注重点

三、态势要素获取关键技术（2）

- 态势要素预处理技术—数据补全技术
  - 特征匹配型补全技术
    - 典型实例：风险传播
  - 规则推理型补全技术
    - 数据序列推导
    - 贝叶斯方法
    - …

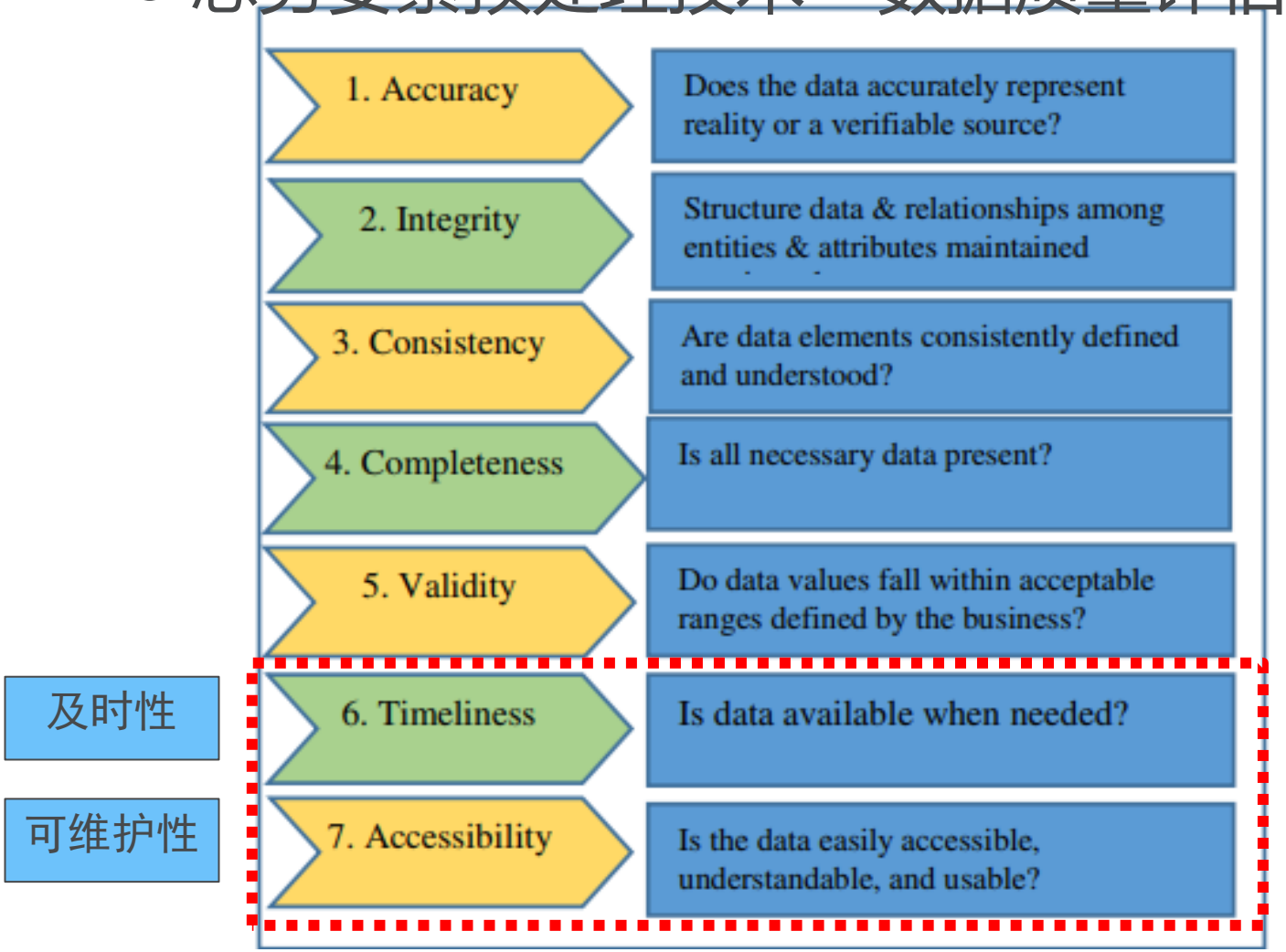
三、态势要素获取关键技术（3）

● 态势要素预处理技术—数据质量评估技术

完整性 Completeness	• 哪些数据丢失了或者哪些数据不可用。
规范性 Conformity	• 哪些数据未按统一格式存储。
一致性 Consistency	• 哪些数据的值在信息含义上是冲突的。
准确性 Accuracy	• 哪些数据和信息是不正确的，或者数据是超期的。
唯一性 Uniqueness	• 哪些数据是重复数据或者数据的哪些属性是重复的。
关联性 Integration	• 哪些关联的数据缺失或者未建立索引

三、态势要素获取关键技术（4）

- 态势要素预处理技术—数据质量评估技术



Hyperdimension	Quality Dimension	Factors to consider
Source	Institutional/Business Environment	Sustainability of the entity-data provider Reliability status Transparency and interpretability
	Privacy and Security	Legislation Data Keeper vs. Data provider Restrictions Perception
Metadata	Complexity	Technical constraints Whether structured or unstructured Readability Presence of hierarchies and nesting
	Completeness	Whether the metadata is available, interpretable and complete
	Usability	Resources required to import and analyse Risk analysis
	Time-related factors	Timeliness Periodicity Changes through time
	Linkability	Presence and quality of linking variables Linking level
	Coherence - consistency	standardisation Metadata available for key variables (classification variables, construct being measured)
	Validity	Transparency of methods and processes Soundness of methods and processes
Data	Accuracy and selectivity	Total survey error approach Reference datasets Selectivity
	Linkability	Quality of linking variables
	Coherence - consistency	Coherence between metadata description and observed data values
	Validity	Coherence between processes and methods and observed data values

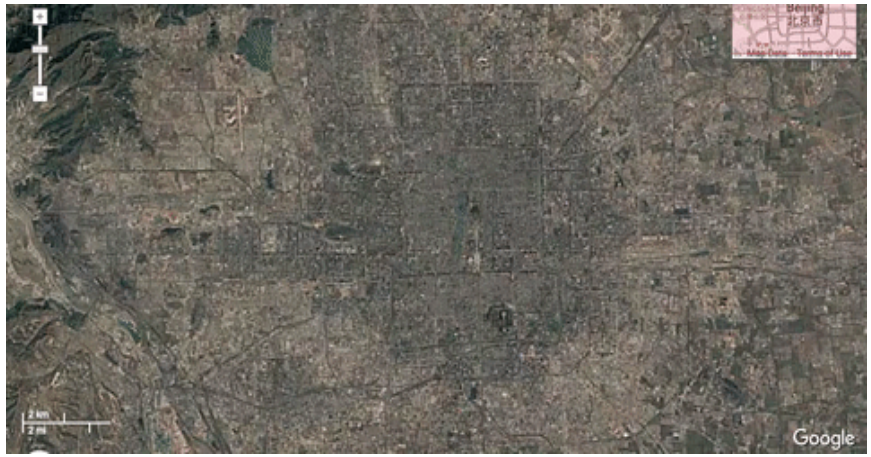
A Suggested Fra eam，2014

内容概要

四、态势要素表示方法（1）

- 态势要素数据结构
  - 时空性
  - 关联性
  - 对抗性
- 态势要素呈现形式
  - 结构化
  - 非结构化
  - 半结构化

Facebook Timeline



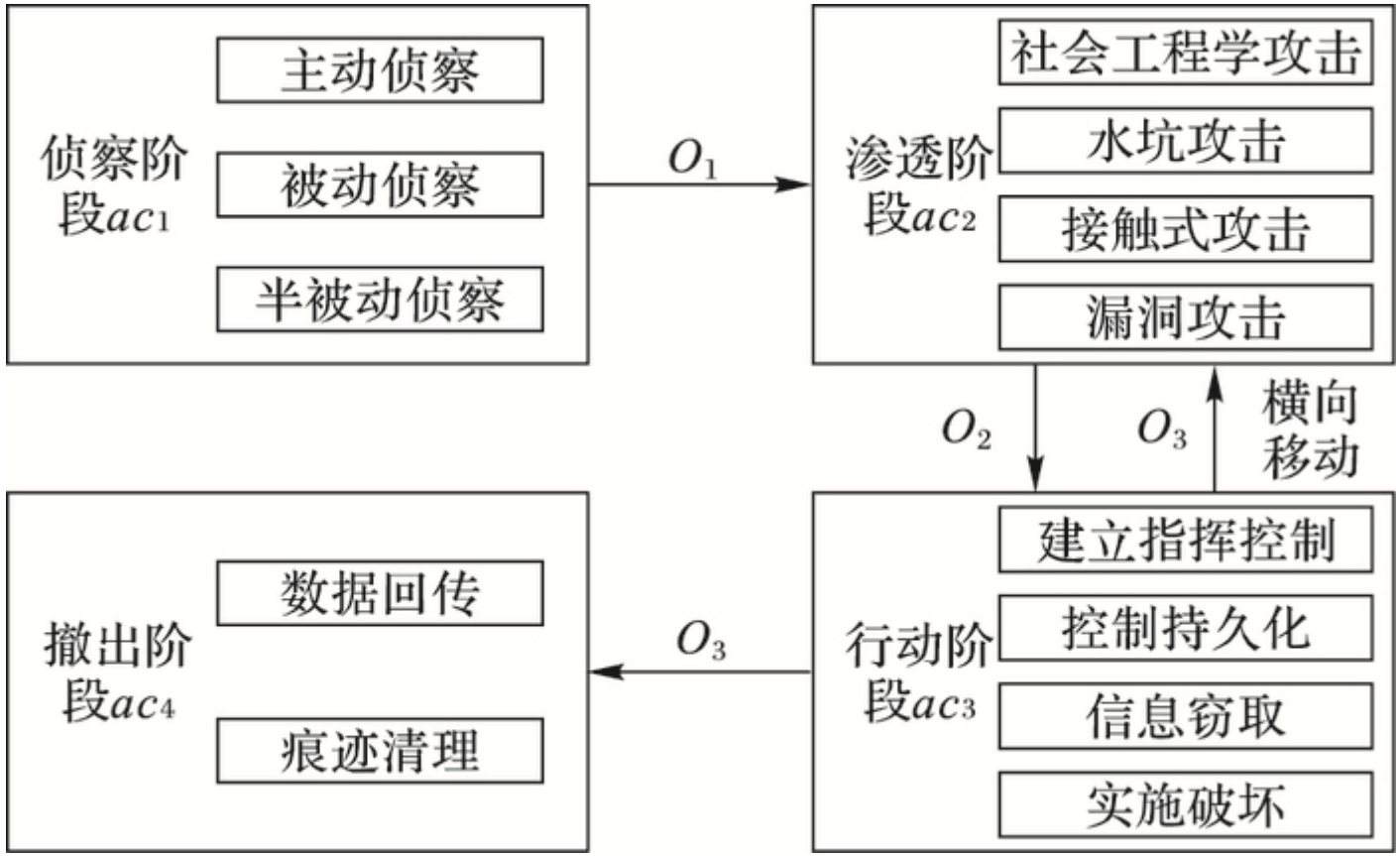
谷歌地图中北京市变化图

四、态势要素表示方法（2）

- 网络安全攻击方的必备元素
  - 人：个人、组织、国家
  - 地：源和目的地点、摆渡点
  - 时：起止时间、关键节点时间
  - 物：攻击工具、攻击资源、攻击知识

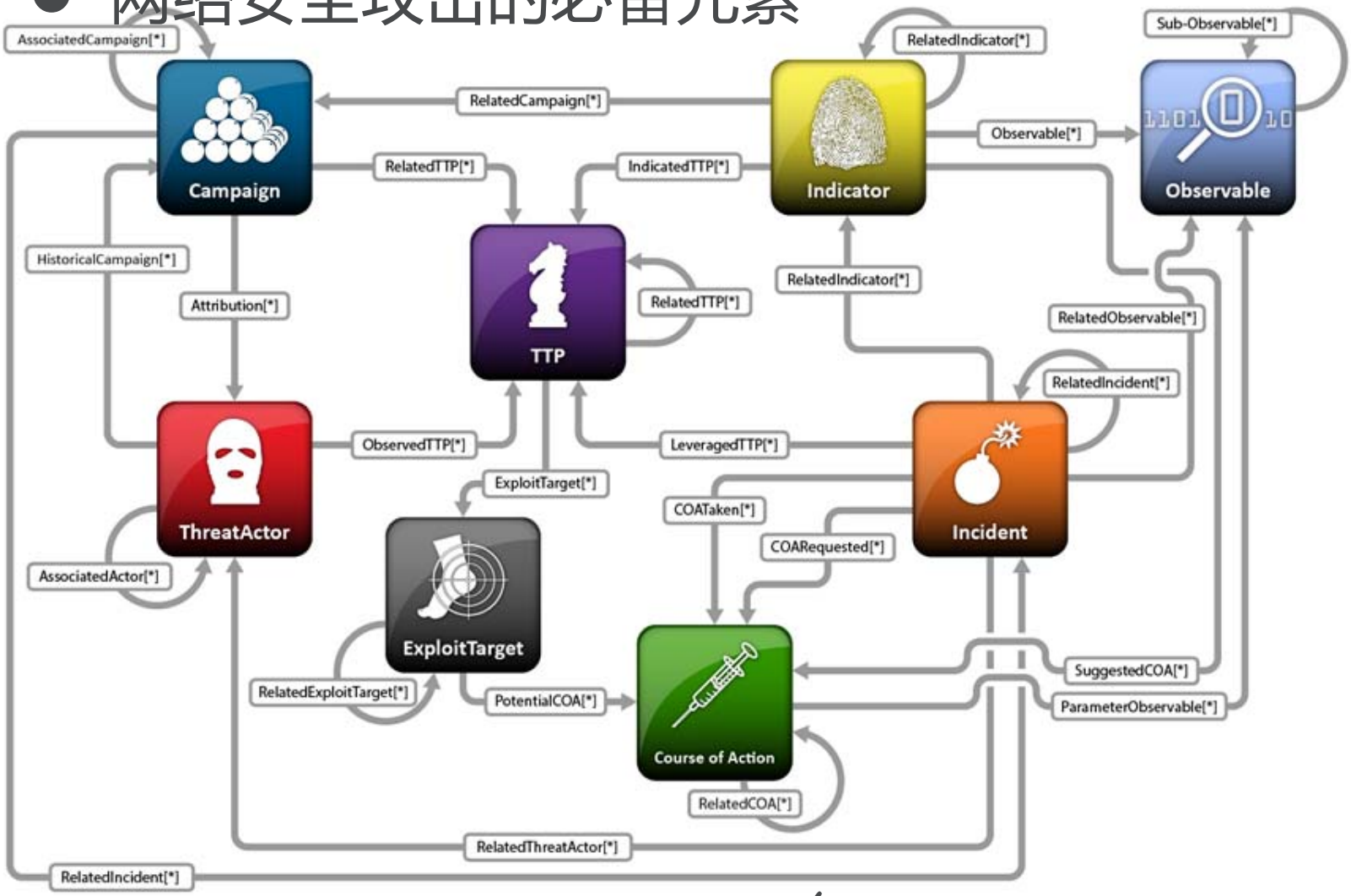
四、态势要素表示方法（3）

- 网络安全攻击的必备元素



四、态势要素表示方法（4）

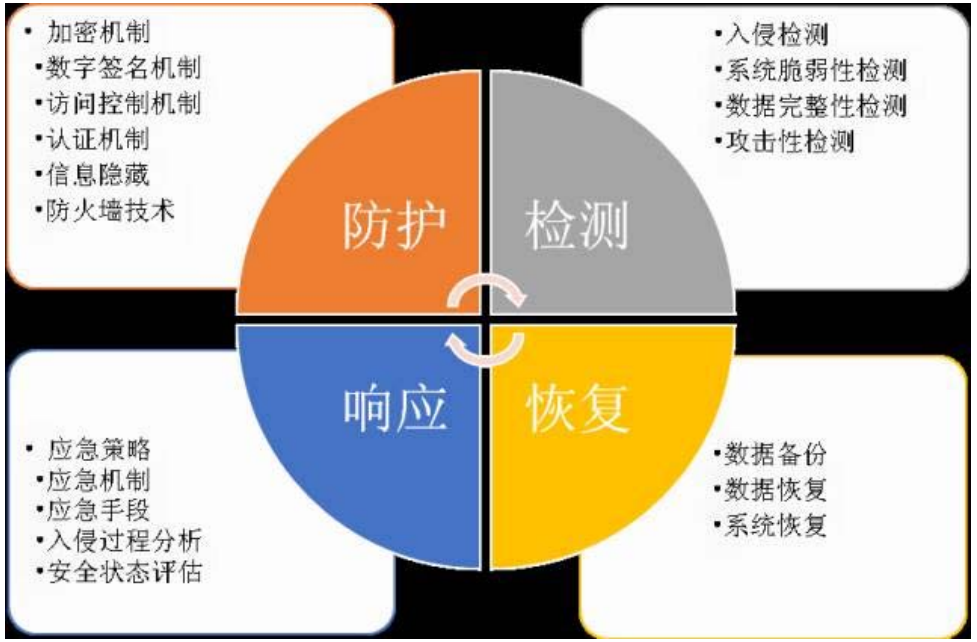
- 网络安全攻击的必备元素



STIX白皮书：http://stixproject.github.io/getting-started/whitepaper/

四、态势要素表示方法（5）

- 网络安全防御方的必备元素
  - 人：个人、组织、国家
  - 地：防御范围
  - 时：策略起止时间、监测预警时间
  - 物：脆弱性、防御工具、防御资源、防御知识（规章制度、专家经验、人员组织）



四、态势要素表示方法（5）

- 网络安全防御方的必备元素-脆弱性元素

CNVD-ID	CNVD-2018-02516
公开日期	2018-03-11

Cisco Web Security Appliance FTP服务器安全漏洞

CNNVD编号：CNNVD-201803-264　　危害等级：

CVE编号：CVE-2018-0087　　漏洞类型：资料不足

发布时间：2018-03-09　　威胁类型：远程

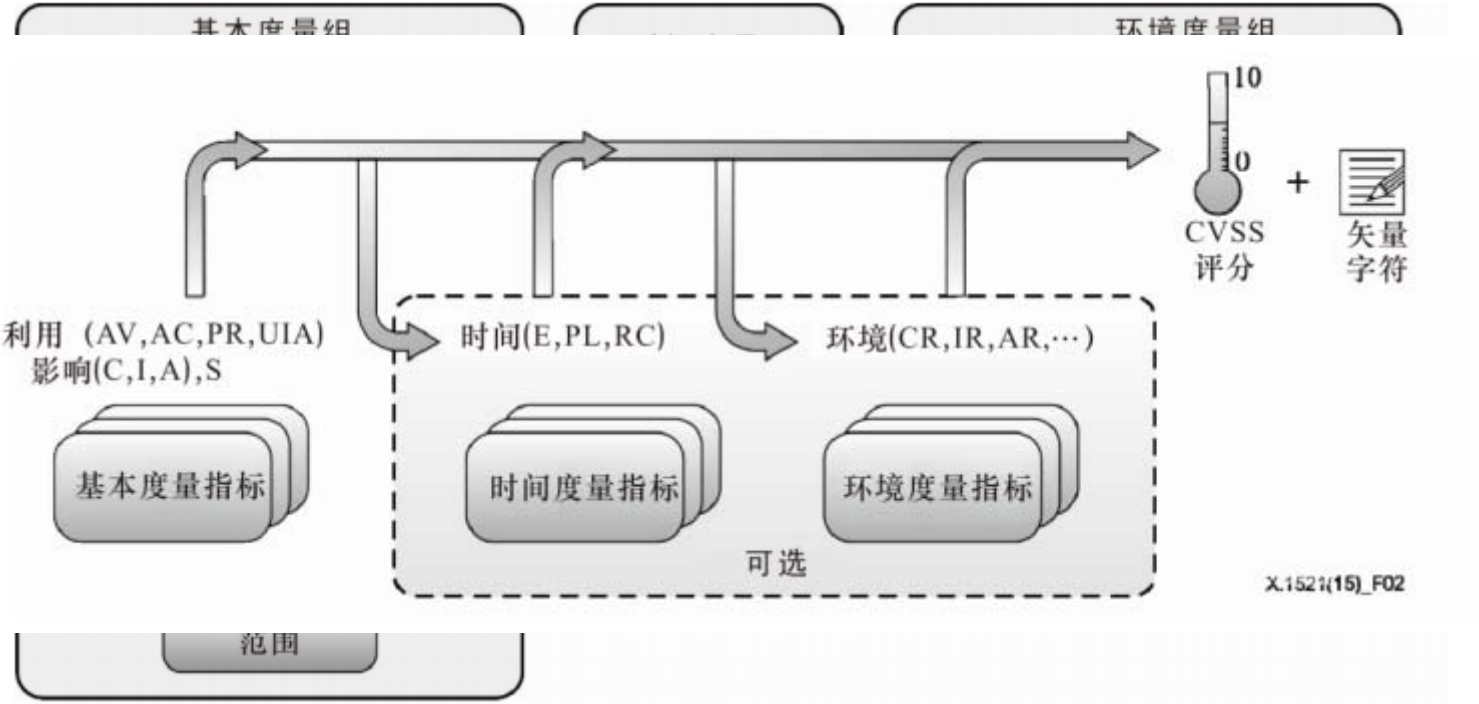
更新时间：2018-03-09　　厂　商：

漏洞来源：

验证信息	已验证
报送时间	2018-01-25
收录时间	2018-02-01
更新时间	2018-03-11
漏洞附件	附件暂不公开

四、态势要素表示方法（6）

- 网络安全防御方的必备元素-脆弱性量化评价
  - 共同漏洞评分系统CVSS



四、态势要素表示方法（7）

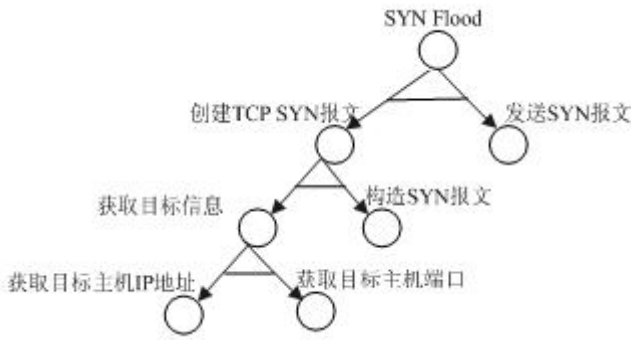
- 典型表示方法
  - 图论
  - 状态空间模型
  - 本体理论
  - XML
  - UML
  - …

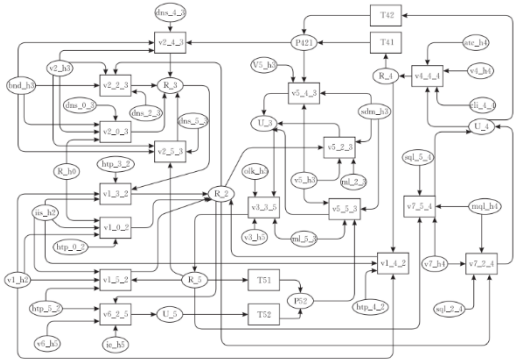
四、态势要素表示方法（8）

- 典型表示方法-图论
  - 直观形象
  - 表示范围有限，图算法亟需研究完善

- 攻击树
  - 一种面向攻击目标的描述系统漏洞的形式化方法

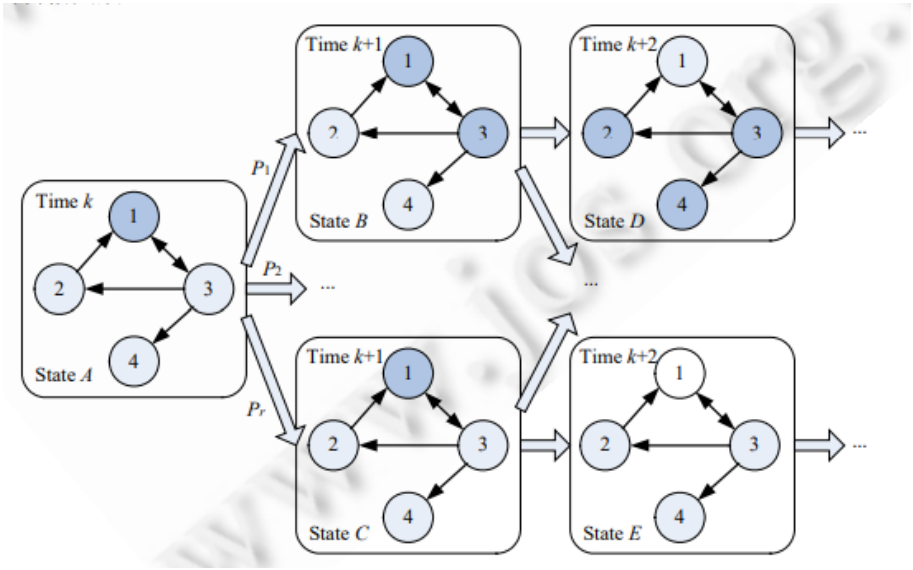
- 攻击图
  - 描述攻击者从攻击起始点到达到其攻击目标的所有路径的方法





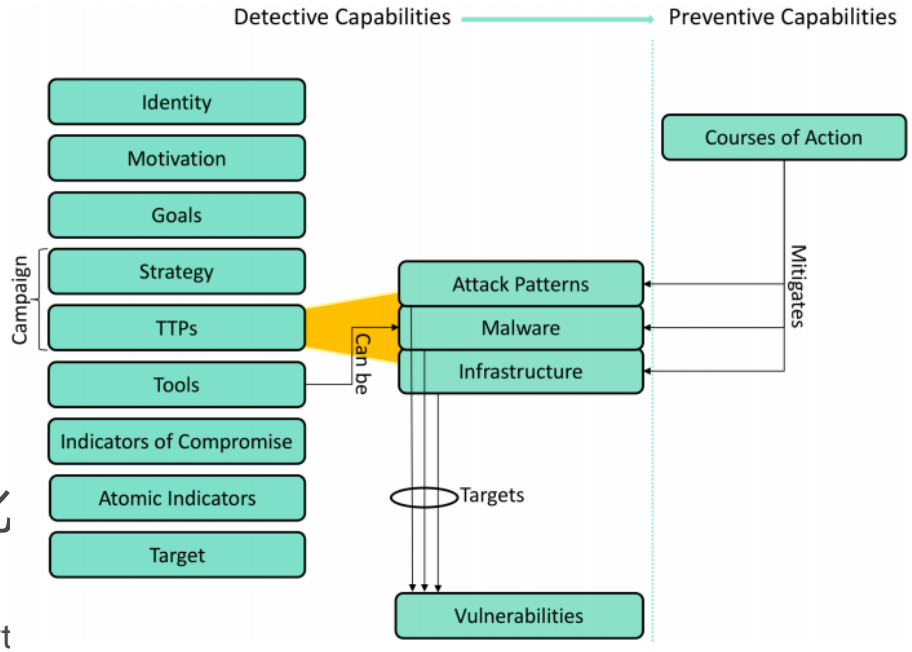
四、态势要素表示方法（9）

- 典型表示方法-状态空间模型
  - 控制学范畴，将物理系统表示为一组输入、输出及状态的数学模式
  - 理论丰富、动态行为的描述更加精准
  - 容易陷入死循环



四、态势要素表示方法（10）

- 典型表示方法-本体理论
  - 对特定领域之中某套概念及其相互之间关系的形式化表达
  - 表示形式丰富，已与知识图谱结合
    - 个体（实例）
    - 类或集合（sets）
    - 属性
    - 关系
    - 函数
    - 约束（限制）
    - 规则
    - 公理
    - 事件：属性或关系的变化



TOCSA: Threat Ontologies for CyberSecurity Analyt

内容概要

五、典型系统和框架-NIST框架（1）

- NIST SP 1800-7电力基础设施态势感知（Situational Awareness for Electric Utilities）
  - 该指南分为三部分：SP1800-7a《执行总结》、SP1800-7b《方法、架构和安全特征》、SP1800-7c《操作指南》
  - 针对电力行业的网络，包括各种工控系统，需要从其中俘获、传输、分析和存储实时或接近实时的数据，从而实现安全异常监测、防御，并与其它能源机构分享结果
  - 提供了一套态势感知的机制

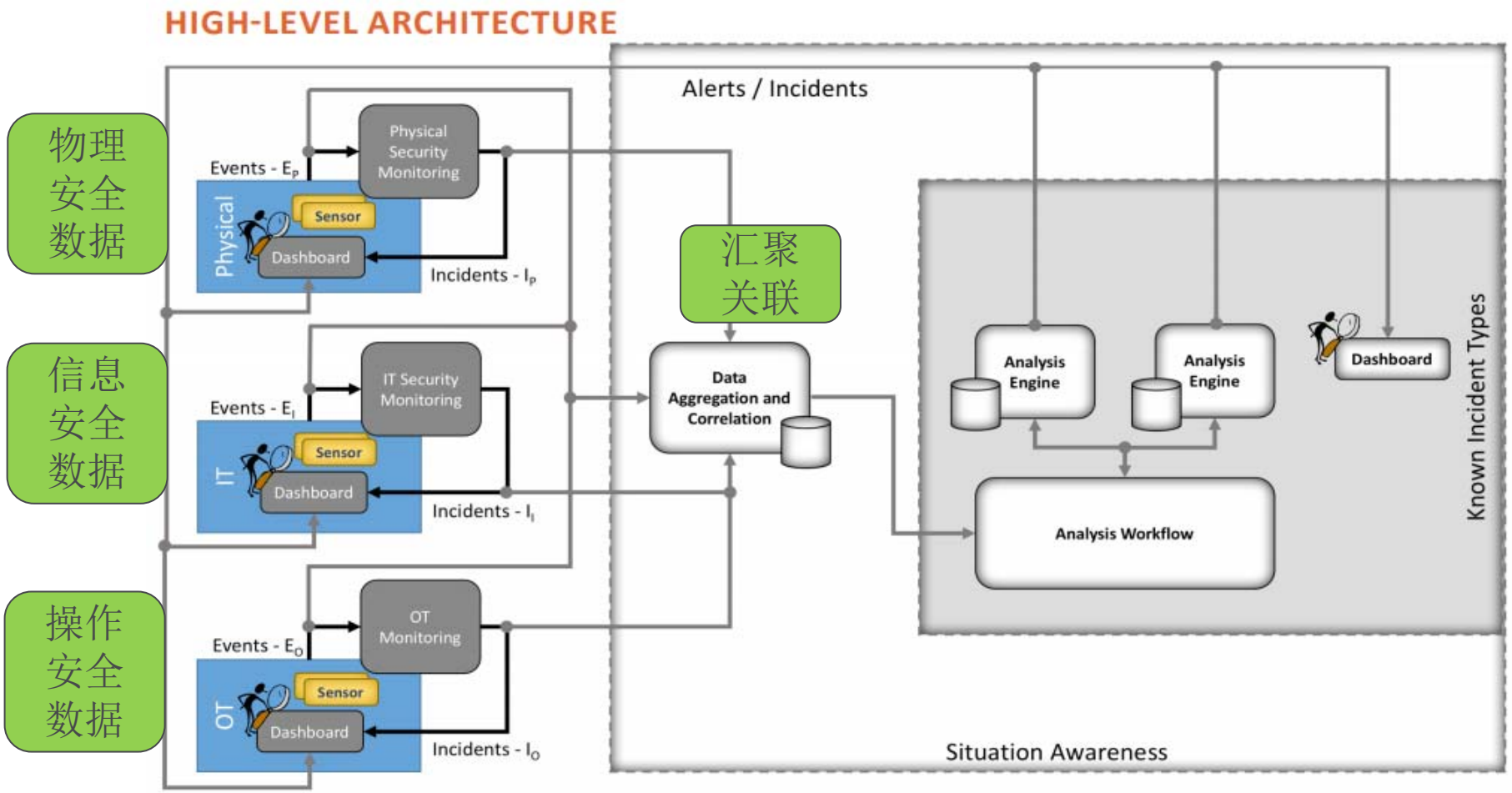
https://nccoe.nist.gov/projects/use-cases/situational-awareness

五、典型系统和框架-NIST框架（2）

- NIST SP标准系列
  - SP800计算机安全（Computer Security）（1990年12月至今），NIST出版计算机、网络和信息安全指南、建议和参考资料的主要模式
  - SP 1800 NIST网络安全实践指南（NIST Cybersecurity Practice Guides）（2015年至今），新创立的子系列用来作为SP800的补充，该系列定位于公有和私有部门中特定网络安全领域的挑战；它提供实用的、用户友好的指南，以更好的利用基于标准的网络安全方法
  - SP 500计算机系统技术（Computer Systems Technology）（1977年1月至今）：NIST信息技术实验室（ITL）广泛使用的一个通用子系列，本报告只列出SP500系列中与NIST计算机安全工作相关的标准。实际上，在SP800系列之前，NIST用SP500系列来出版计算机安全的标准

五、典型系统和框架-NIST框架（3）

- 技术架构



五、典型系统和框架-NIST框架（4）

- 要素数据采集工具及功能（1）

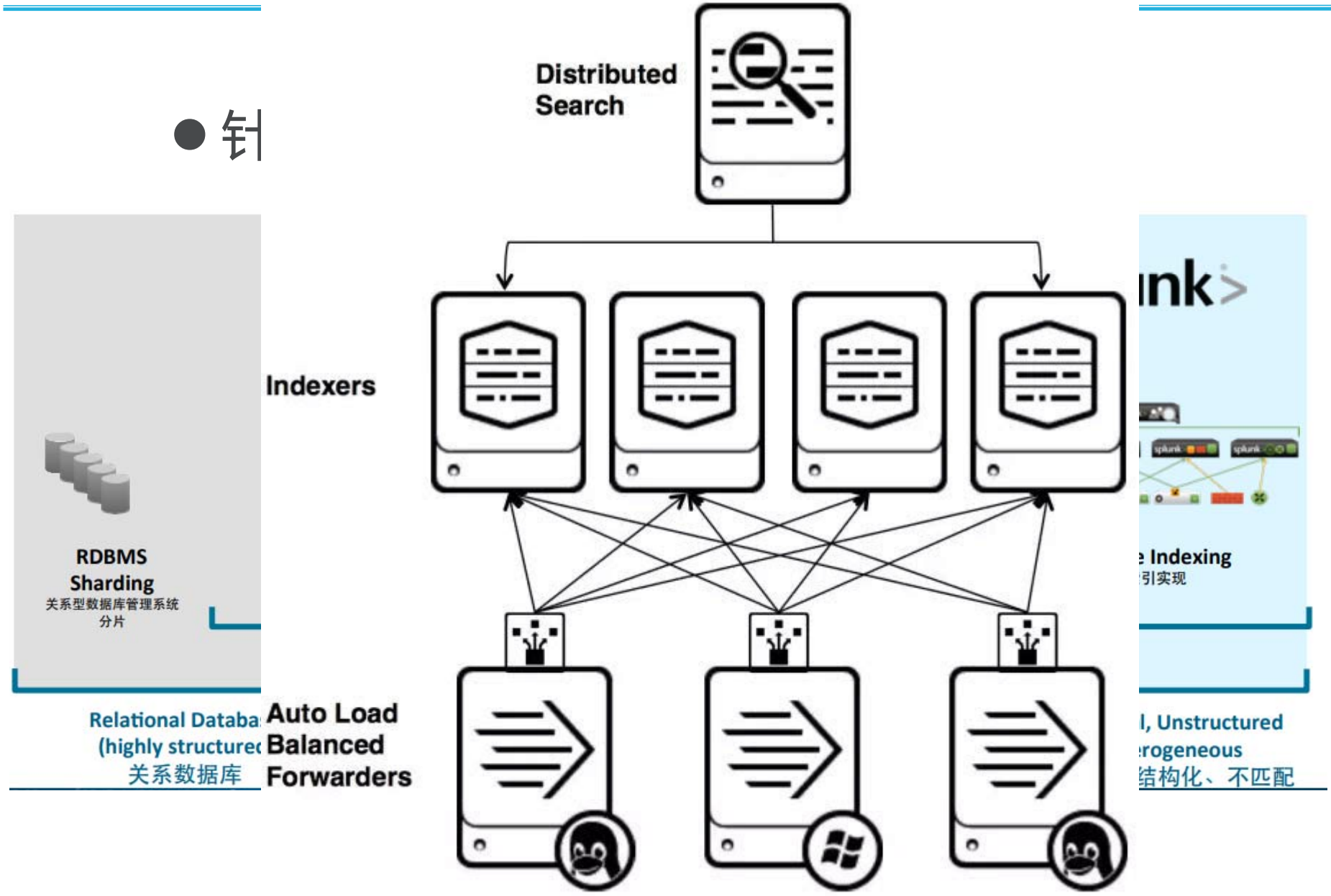
Component	Product	Function
Security Information and Event Management (SIEM)	HPE ArcSight	▪ aggregates all IT, windows, OT (ICS) and physical access monitoring, event, and log data collected by the reference design ▪ acts as a data normalization and correlation point and enables queries to be developed and executed to detect potential security incidents ▪ serves as the central location at which the analyst can access all data collected
Network Tap	IXIA TP-CU3 Tap	▪ collects data from specific locations on the ICS network and send it to the monitoring server via the ICS firewall ▪ the taps are passive, so if they lose power or otherwise fail, they will not adversely affect the ICS network ▪ collects data via monitor ports that are inherently unidirectional (and so do not pose any threat of information leaking from the tap onto the ICS network)

Component	Product	Function
Log Collector/ Aggregator	TDi Technologies ConsoleWorks	■ log collection and aggregation ■ adds a time stamp and integrity seals the log entries ■ log collection in the operations facility protects against potential data loss in the event that the communications channel between the operations and enterprise facilities fails ■ aggregating the log entries of all monitoring components at the operations log collector/aggregator ensures that this log data gets buffered in the operations facility and can be transferred later in the event that network connectivity to the enterprise network is lost
ICS Asset Management System	Dragos Security CyberLens	■ monitors ICS traffic and maintains a database of all ICS assets of which it is aware ■ this enables it to detect new ICS devices, ICS devices that disappear, and changes to known ICS devices
Network Visualization Tool	Dragos Security CyberLens	■ displays a depiction of network devices, connectivity, and traffic flows
Physical Access Control System	RS2 Access It!	■ controls user access to doors ■ detects and reports door open/close events and user identity
Physical Access Sensor	RS2 door controller	■ senses door close/open events ■ generates alerts when door open and close events occur
ICS Network Intrusion Detection System (IDS)	Radiflow iSIM	■ identify, monitor, and report anomalous ICS traffic that might indicate a potential intrusion

Component	Product	Function
Historian	OSIsoft Pi Historian	■ serves as a data repository that essentially replicates the database of collected ICS values on the ICS network's Historian ■ can be configured to generate alerts when changes to certain ICS process values occur
ICS Behavior Monitor	ICS^2 On-Guard	■ monitor ICS process variable values in the Historian to assess application behavior, detect process anomalies, and generate alerts
Application Monitor & Protection	Waratek Runtime Application Protection	■ monitors & protects a running application, analyzes the data it collects, and detects and reports unusual application behavior, e.g., it might generate an alert if it detects a potential SQL injection attack against the SIEM
Analysis Workflow Engine	RSA Archer Security Operations Management	■ automates workflow associated with review and analysis of data that has been collected at the SIEM ■ enables orchestration of various analytic engines
Unidirectional gateway	Waterfall unidirectional security gateway	■ allows data to flow in only one direction
Visualization Tool	RSA Archer Security Operations Management	■ provides data reduction and a dashboard capability for the data in the SIEM, as well as risk analysis

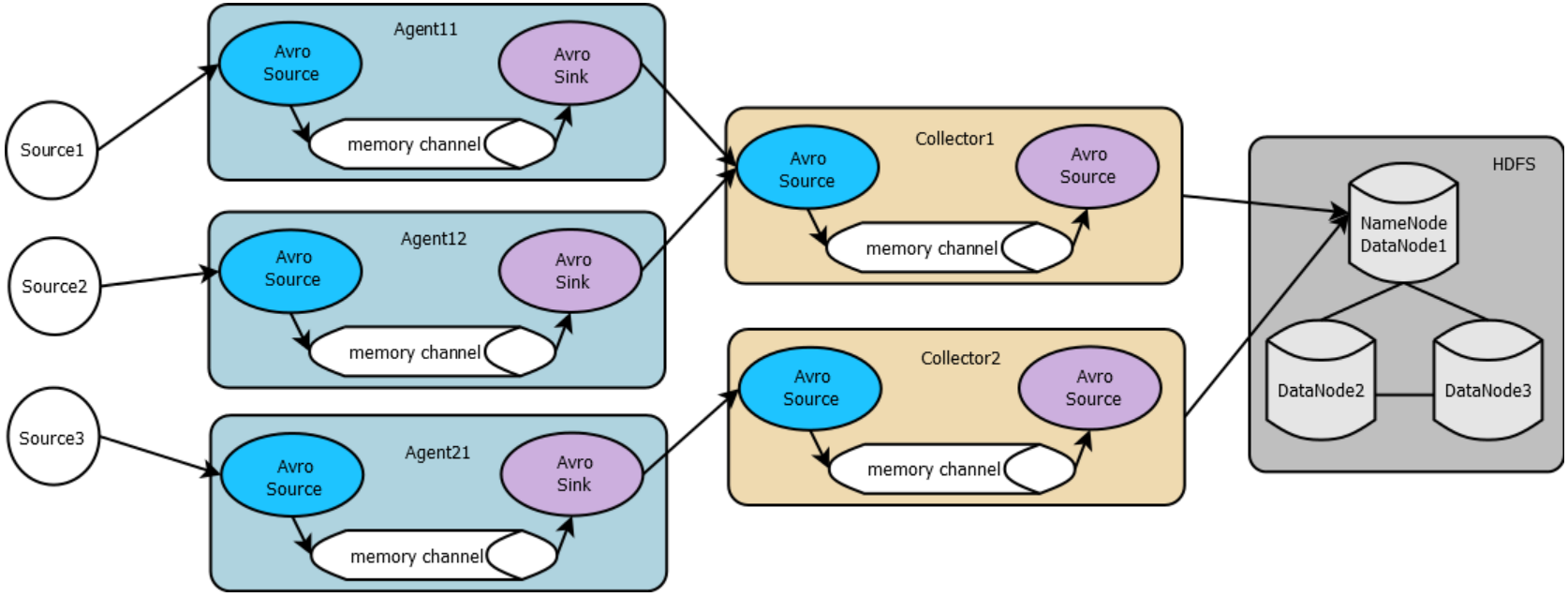
五、典型系统和框架-Splunk

- 针



五、典型系统和框架-Apache Flume

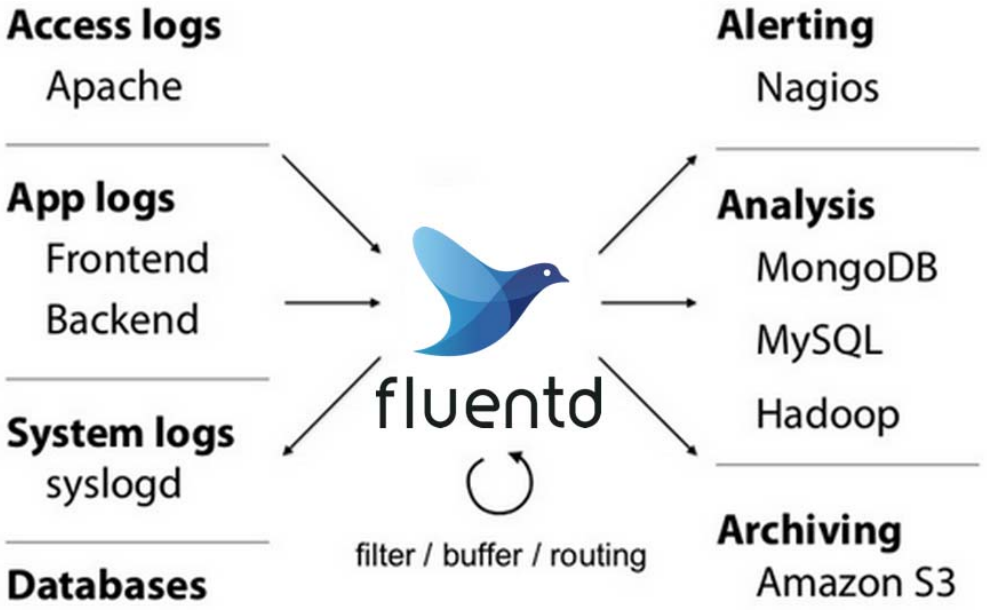
- Apache旗下的一款开源、高可靠、高扩展、容易管理、支持客户扩展的数据采集系统
  - 事件是flume数据传输的基本单元
  - Flume以事件的形式将数据从源头传到目的地
  - 事件由可选的头部和载荷构成



- ELK是著名的开源数据栈
  - ElasticSearch、 Logstash、 Kibana
  - ElasticSearch：承担的搜索功能，分布式多用户能力的全文搜索引擎
  - Logstash：承担的是日志处理功能，它创建一个集中化的管道来储存、搜索和分析日志文件
  - Kibana：承担的分析和展示功能，针对Elasticsearch的开源分析及可视化平台，用来搜索、查看交互存储在Elasticsearch索引中的数据
    - 能集中处理各种类型的数据
    - 能标准化不通模式和格式的数据
    - 能快速的扩展自定义日志的格式
    - 能非常方便的添加插件来自定义数据

五、典型系统和框架-Flunted

- Flunted是著名的开源数据栈
  - 开源的日志收集系统，支持150+个插件
  - 能够将日志收集到MongoDB, Redis, Amazon S3等
  - 能够以json格式来处理日志
  - 具备每天收集5000+台服务器上5T的日志数据，每秒处理50000条消息的性能



需要思考的问题？

① 网络空间安全态势要素获取中的权衡点在于？取舍原则是？
② 现有态势要素表示方法中最大的问题是？


Q&A