



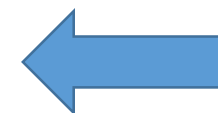
# 情报驱动的 网络安全新生态环境

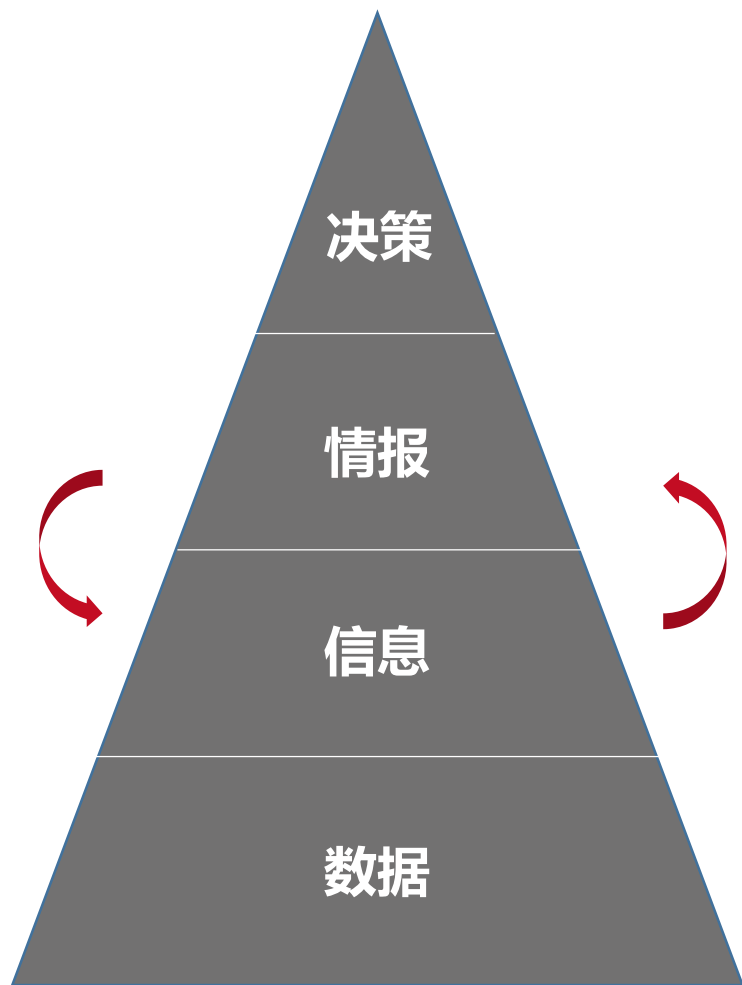
刘广坤

天际友盟 技术总监

## 目录

- 威胁情报简介
- 威胁情报相关标准及应用
- 威胁情报共享生态研究





## 网络安全信息的四个应用维度

**决策维度：**多维结合，最终判断，处置策略，需实际落地，容错率极低

**情报维度：**深度加工，准确性高，时效性强，与场景贴合，应用频次高

**信息维度：**基于数据，初步加工，准确性差，时敏性不高，多作为参考

**数据维度：**原始数据，未做加工，数据量大，利用难度大、应用频次低





## 概念起源

- 最早源于军事情报领域，概念与技术成熟后被引入网络与信息安全领域，与网络安全态势感知理论密切相关。

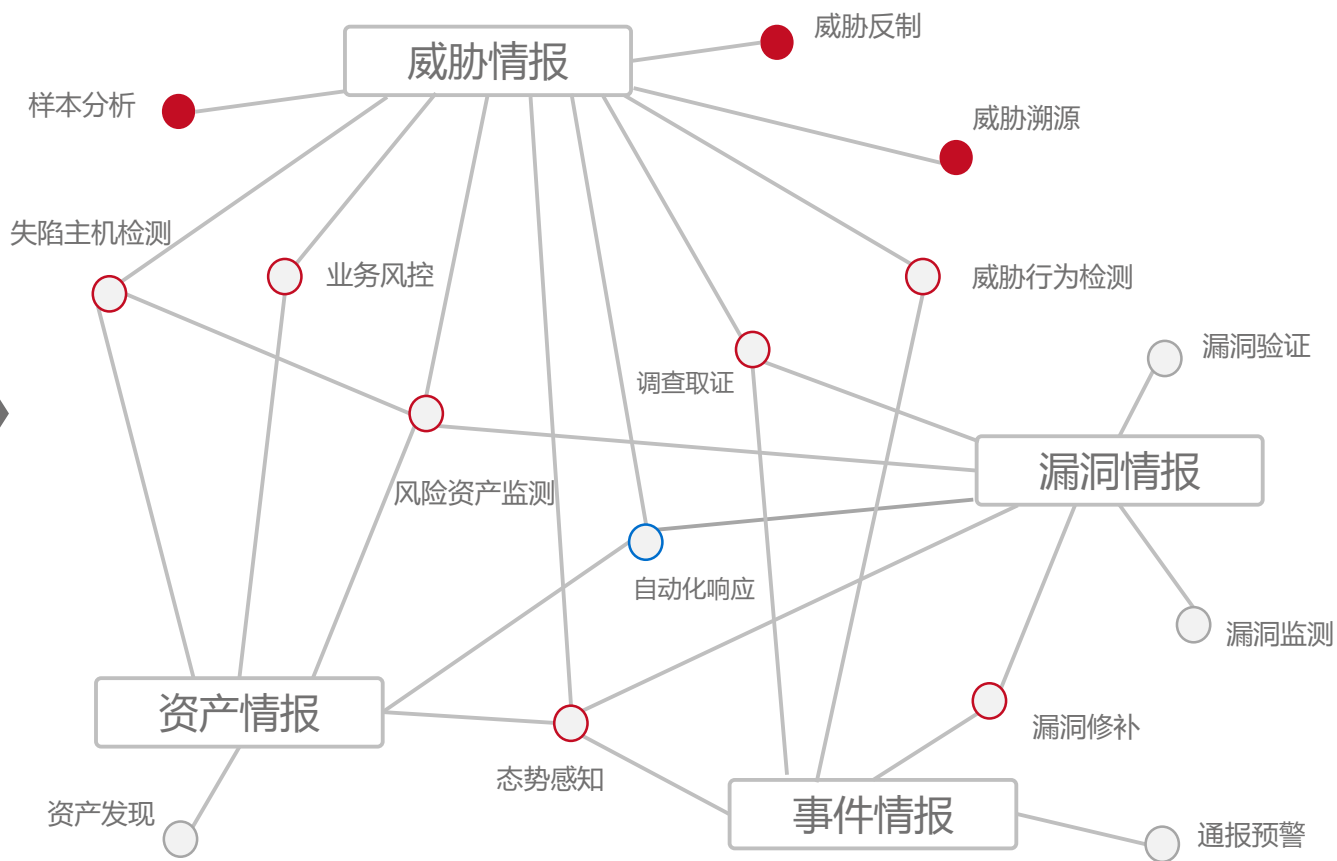
## 概念定义

- “威胁情报是**基于证据的知识**，包括场景、机制、指标、含义和可操作的建议。这些知识是关于现存的、或者是即将出现的针对资产的威胁或危险的，可为主体响应相关威胁或危险提供决策信息。” ---- Gartner, 2013年。
- 安全情报是**包含漏洞、资产、威胁、风险、运行和事件等维度的安全知识集合**。

## 概念理解与延伸

- 威胁情报是信息对抗的产物，是出于掌握对手动态的需求，对威胁的具现化描述。可简单理解为“知彼”。
- 安全情报是威胁情报概念的延伸，是运用威胁情报的理念与技术，对网络安全态势感知OODA过程所需要的各类安全知识的综合运用，以支撑组织内部的所有安全活动。

## 国外主流安全厂商在安全情报推广和应用方面的举措



## 基础信息



IP地理位置  
IDC节点  
移动网IP  
教育网IP



IP信誉  
域名信誉  
URL信誉



IP Whois信息  
域名Whois信息  
Whois信息

## 资产

资产发现



风险资产



资产变更



## 漏洞

CNVD  
www.cnvd.org.cn



CNNVD  
国家信息安全漏洞库  
China National Vulnerability Database of Information Security

IBM

RAPID7

## 恶意威胁

恶意软件威胁



木马软件  
蠕虫软件  
病毒软件  
勒索软件  
其他恶意软件

恶意站点威胁



钓鱼网站  
色情站点  
赌博站点  
DGA域名



Tor节点  
僵尸网络  
C&C节点  
扫描器节点

黑客团伙威胁



APT攻击  
被黑网站  
垃圾邮件  
恶意邮件

恶意攻击威胁

## 事件信息



数据泄露事件



病毒木马事件



DDoS攻击事件



Web攻击事件



失陷主机事件

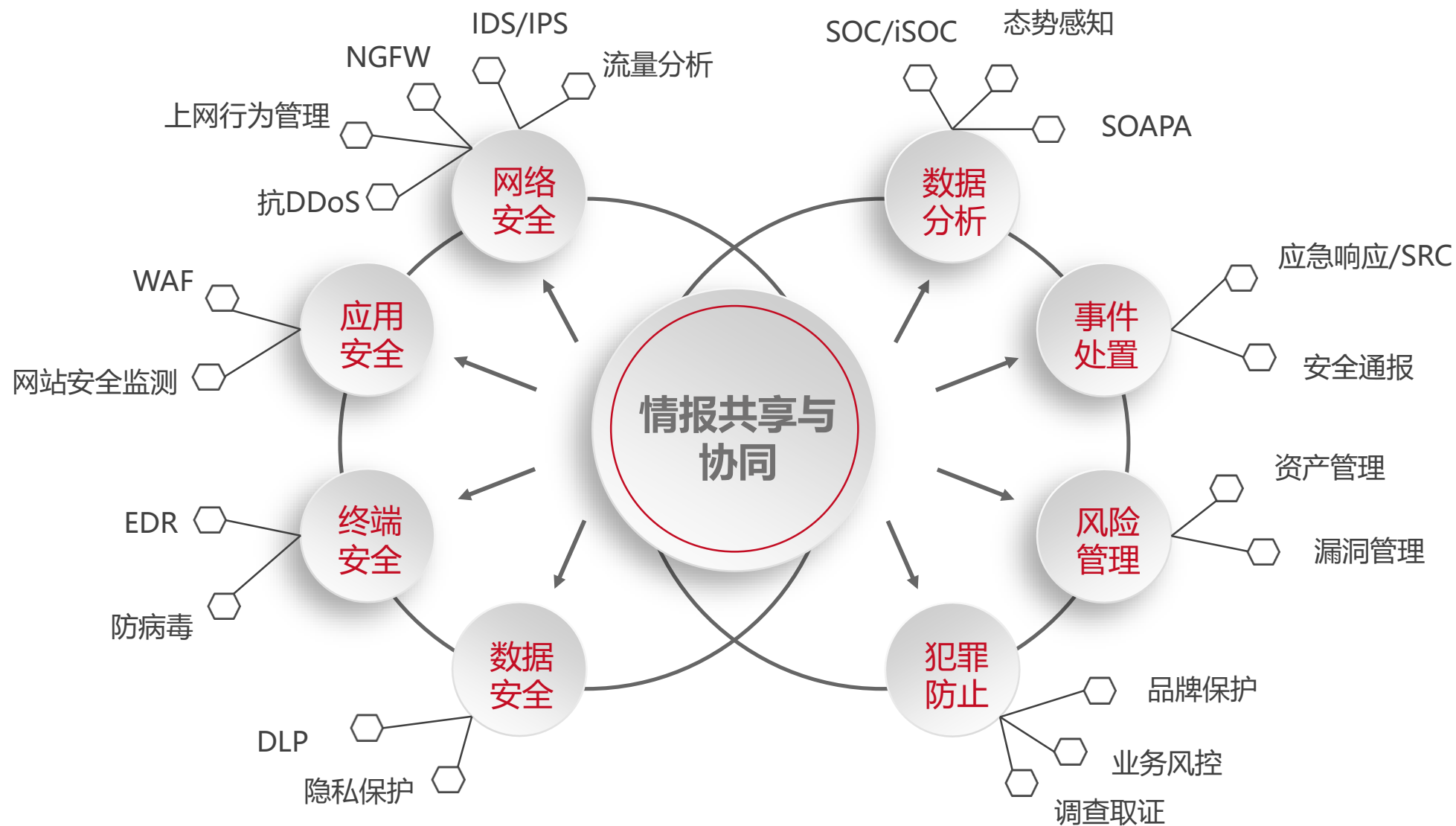


漏洞利用事件

## 其它信息



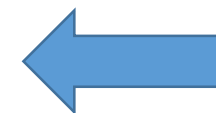
社会舆情  
安全资讯  
其他安全信息





## 目录

- 威胁情报简介
- 威胁情报相关标准及应用
- 威胁情报共享生态研究

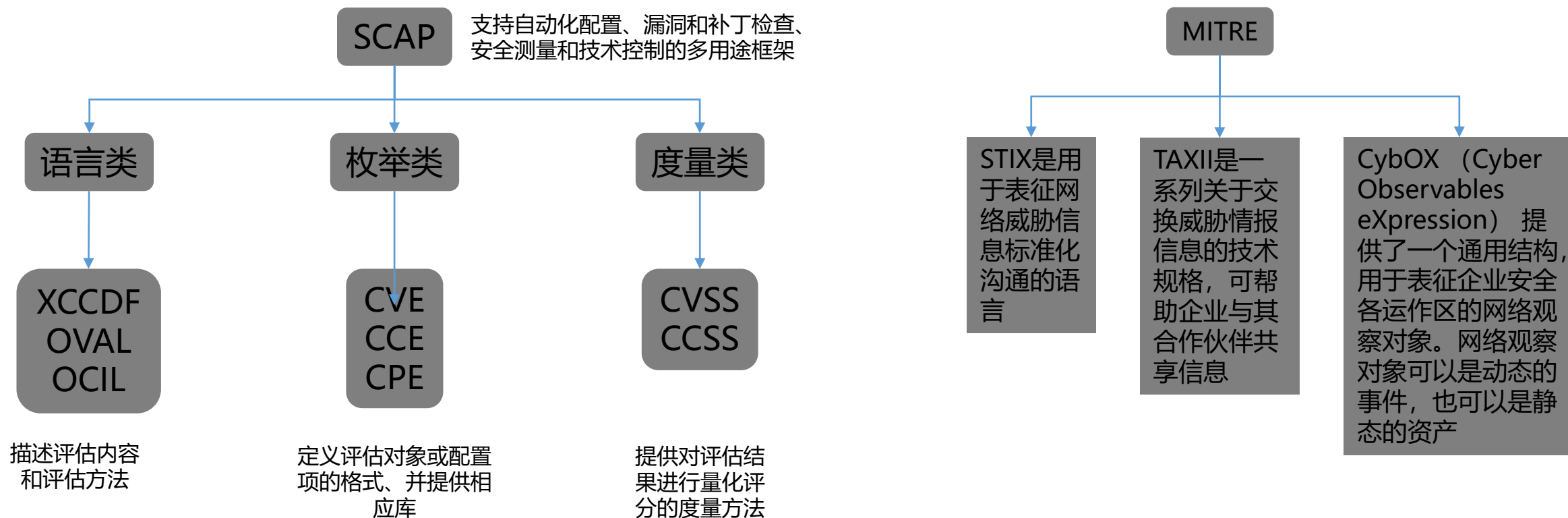




NIST提出了SCAP系列标准，全称为Security Content Automation Protocol

MITRE致力于标准与框架技术研究，提出了知识库模型和框架ATT&CK，语言标准CAPEC、CCE与CWE，结构化命令标准CPE与CVE，结构化语言标准STIX、CybOX与MEAC，开放语言标准OVAL，以及应用层协议标准TAXII等。

标准的目的：1、共享，2计算机自动化操作



## 网络攻击生命期

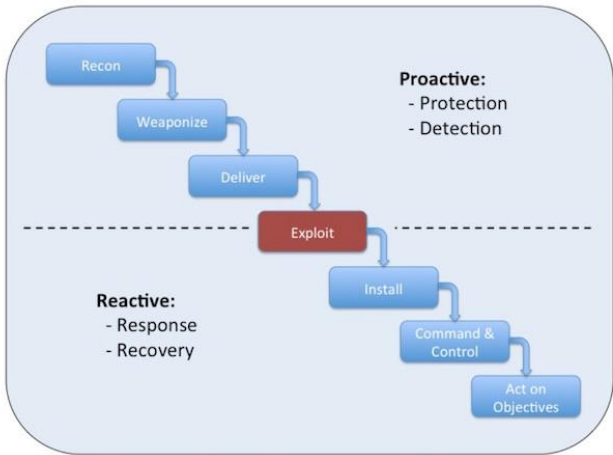


Figure 2-1: Cyber Kill Chain<sup>10</sup>

## 事件响应全生命期

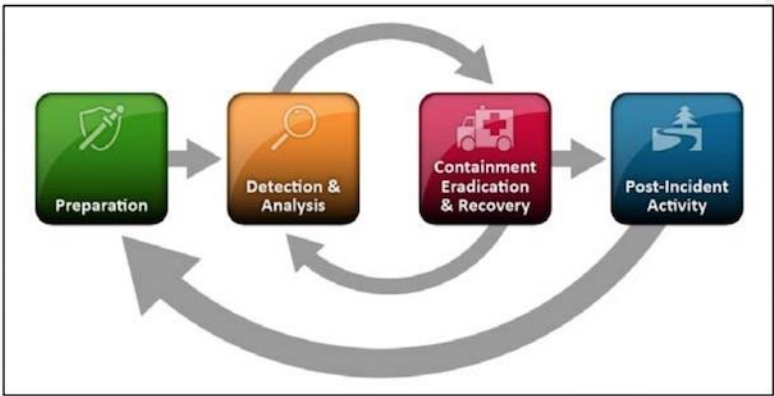


Figure 4-1: Incident Response Life Cycle

## 星型分层级的事件报告机制

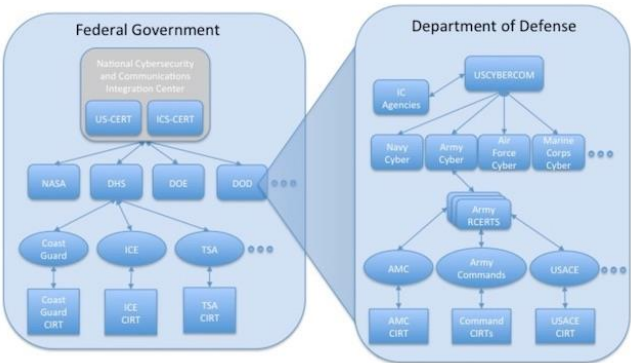


Figure 2-3: Notional Federal Government Hub-and-Spoke Hierarchical Incident Reporting

## 信息共享流程

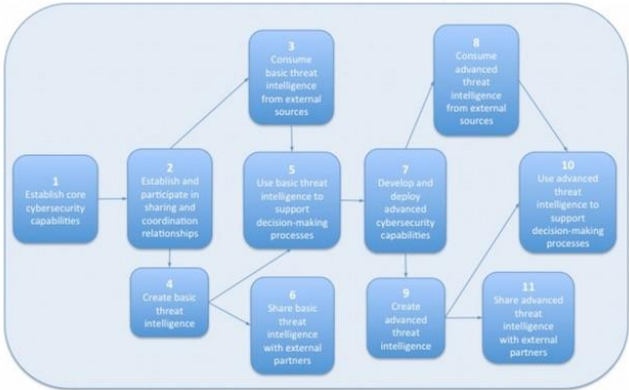
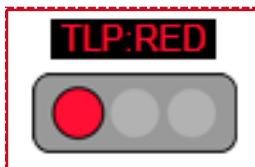
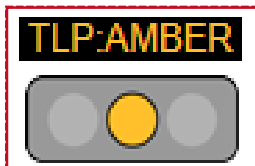


Figure 3-1: Notional Information Sharing Process

TLP是一组确保敏感信息和合适受众共享的标记。TLP借鉴了交通灯信号，以红、黄、绿、白四种颜色来指示接收者对应信息的预期共享边界，每条信息对应的颜色一般会以标签形式随信息传输



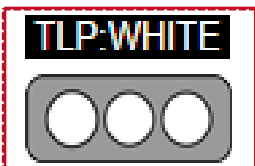
红色：对应的信息内容只允许定向共享和传递至指定的唯一用户，且该用户不应对外再次共享该信息



黄色：对应的信息内容允许向平台和体系内指定的用户组共享和传递，且允许在该用户组内部进行共享，但不应对用户组之外的对象再次共享

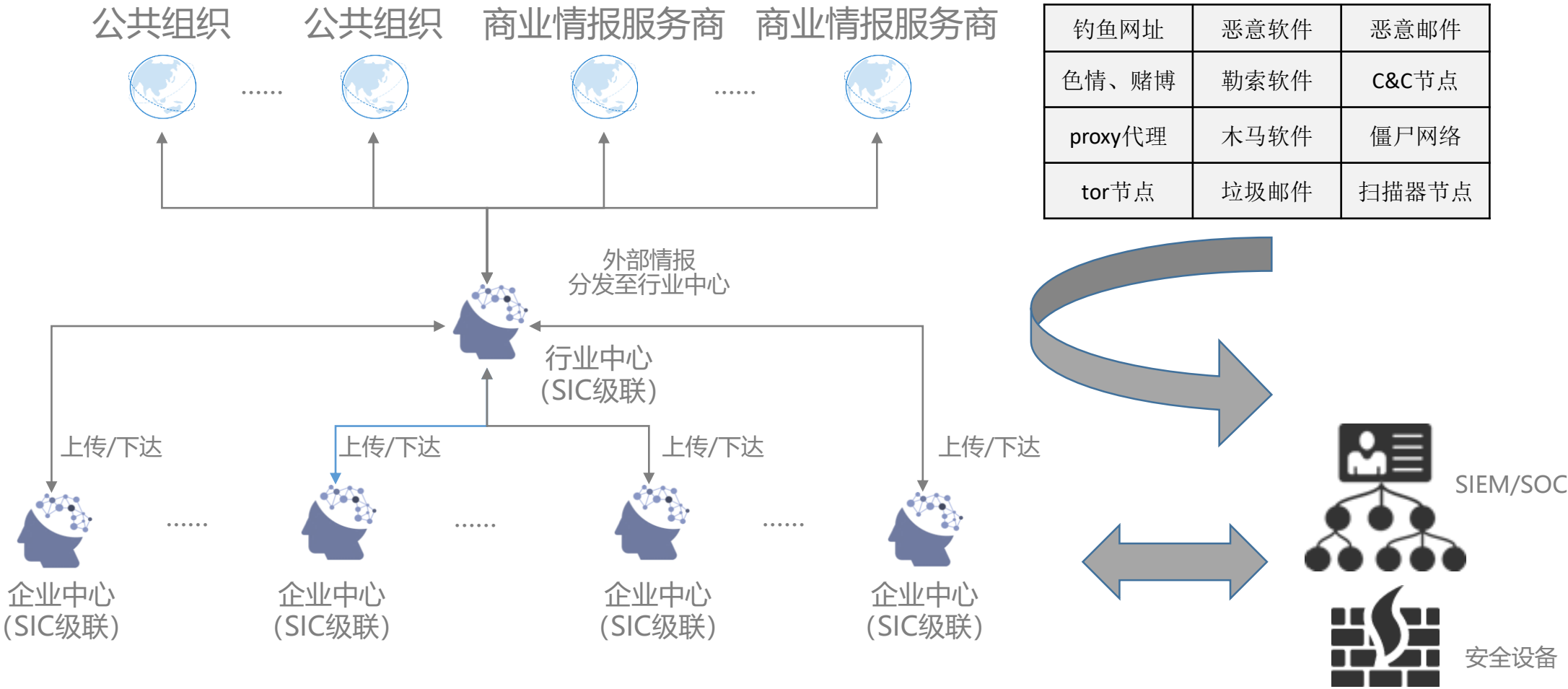


绿色：对应的信息内容允许向平台和体系内的所有用户共享和传递，并且允许用户再次向更广泛的关联平台或组织共享



白色：对应的信息内容在共享和传递上不受任何限制，对所有人或组织完全开放

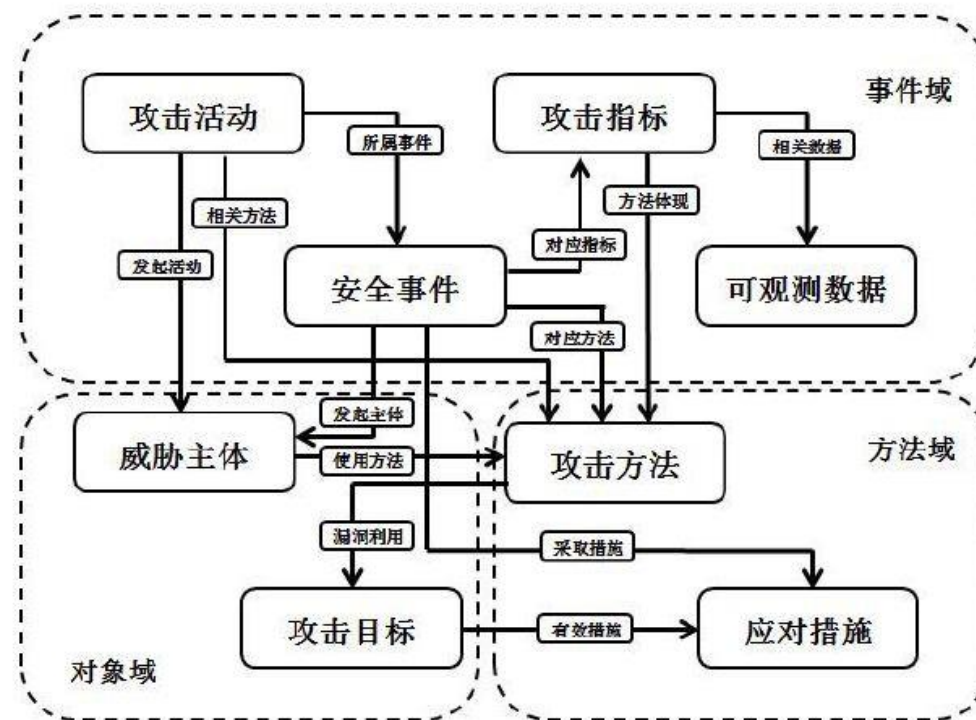




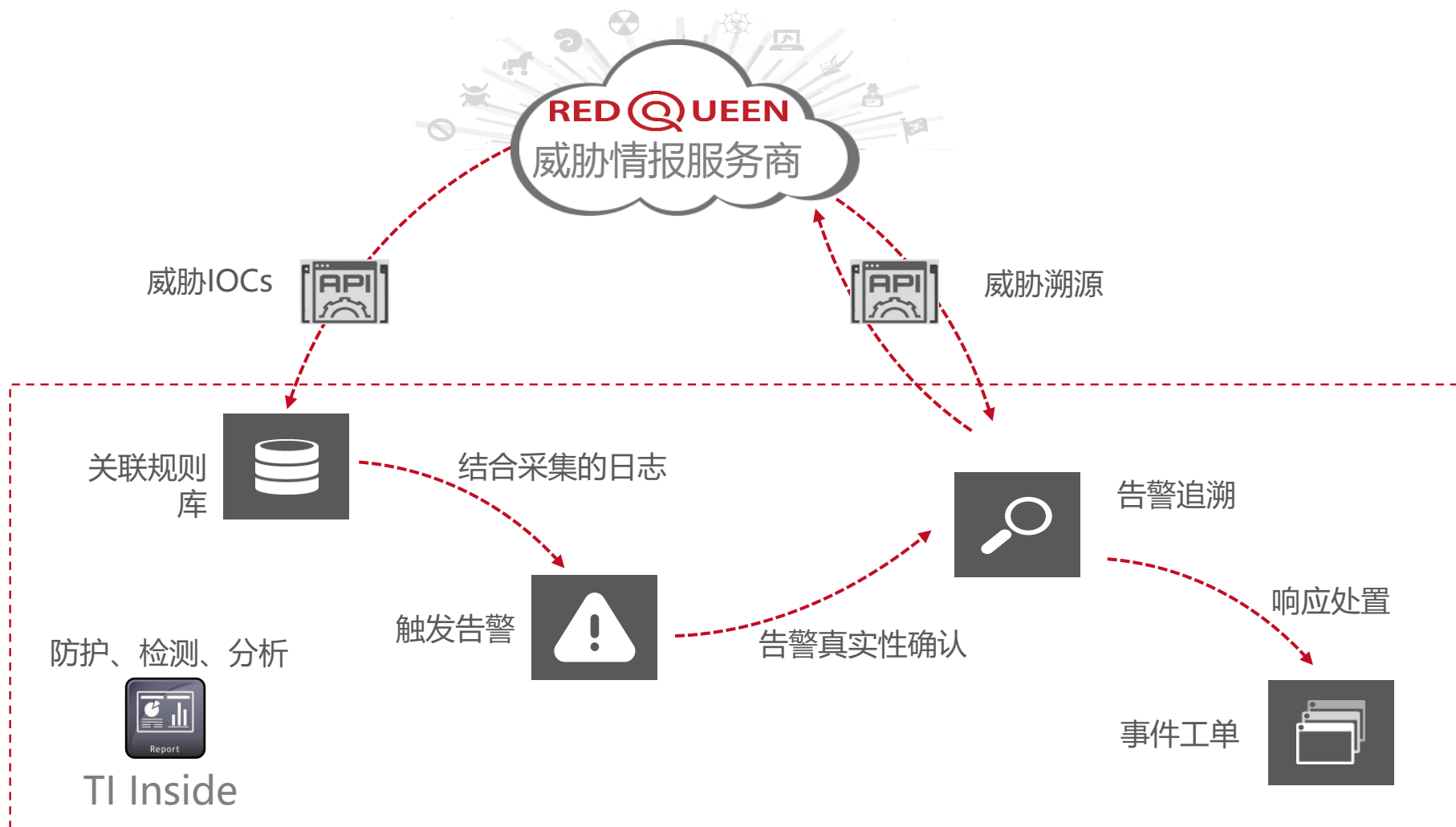
GB/T36643-2018《信息安全技术 网络安全威胁信息格式规范》的发布和施行，标志着我国威胁情报共享进入标准化、规范化的时代

GB/T36643-2018  
《信息安全技术 网络安全威胁信息格式规范》

- 2018 年 10 月 10 日，《信息安全技术 网络安全威胁信息格式规范》GB/T36643-2018发布
- 2018年12月28日，《信息安全技术 网络攻击定义及描述规范》GB/T 37027-2018相继发布
- 网络安全威胁信息交换相关标准，已经在编制
- 规范讲威胁情报分为三个域：对象、方法和事件
- 模型细分为八个组件：可观测数据、攻击指标、安全事件、攻击活动、威胁主体、攻击目标、攻击方法、应对措施



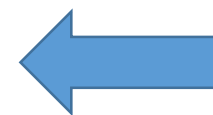
随着GB/T36643-2018的发布和施行，先知先觉的安全厂商已经开始利用Inside机制向最终客户提供服务，并完成了符合国标的接口方式的验证工作





## 目录

- 威胁情报简介
- 威胁情报相关标准及应用
- 威胁情报共享生态研究



在国外，威胁情报共享已经形成专业性、行业性的紧密合作。ISAC已经成为行业内威胁情报交换的重要渠道。

美国FS-ISAC（金融业）目前横跨银行、证券、保险、票券、期货等各业别金融业总计加入业者，约7000金融机构。

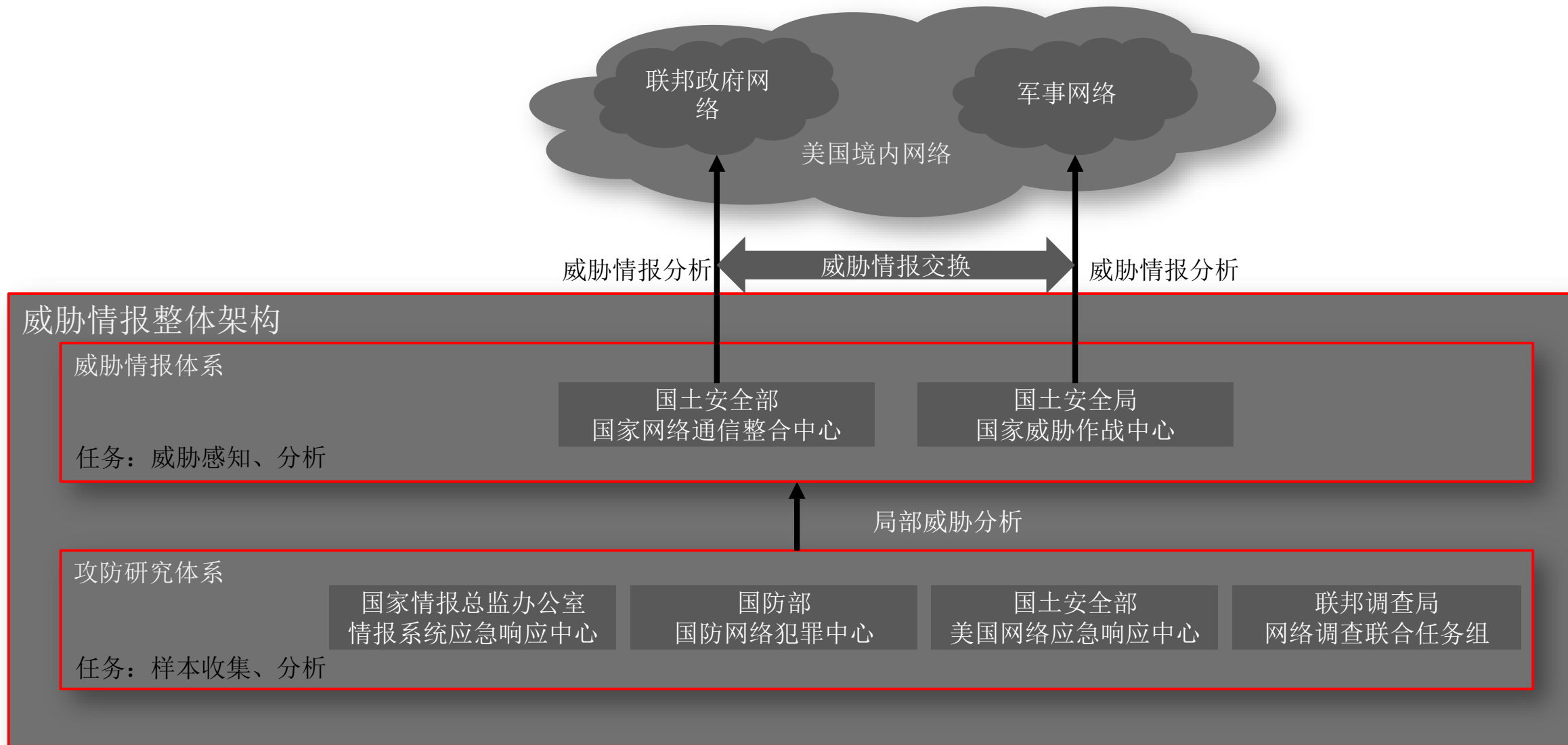
美国目前已具有约20个行业ISAC。主要分布在金融、交通、电力、通信、航空、卫生、能源、水利等拥有大量关键信息基础设施的重点行业。

欧盟:FI-ISAC

韩国:KS-ISA

日本:F-ISAC

FS-ISAC, 1999年成立美国  
IT-ISAC, 2001年成立于日本





**DHS推  
动的态  
势感知  
体系技  
术能力**

核心系统：Einstein（爱因斯坦）系统

关键技术：

- 1) 公网接入点捆绑；
- 2) 攻击流量特征分析、提取；
- 3) 特征全网同步技术；
- 4) 可机读数据共享技术；
- 5) 海量日志智能分析技术；

辅助技术：

全球DNS数据库、Whois信息库、亲缘性分析技术等

**NSA推  
动的态  
势感知  
体系技  
术能力**

核心系统：Tutelage系统

辅助系统：Turmoil、Turbine等

关键技术：

- 1) 截网信号情报获取，攻击特征分析；
- 2) 特征提取技术；
- 3) 特征全网同步技术；
- 4) 可机读数据共享技术；
- 5) 海量日志智能分析技术；

辅助技术：

全球DNS数据库、Whois信息库、非法监控数据、亲缘性分析技术等

共性关键技术：特征分析；特征提取技；特征全网同步技术；可机读数据共享技术；海量日志智能分析技术

共性辅助技术：全球DNS数据库、Whois信息库、亲缘性分析技术等

## 欧盟：“PROTECTIVE”项目

“PROTECTIVE”项目旨在设计一套基于态势感知的主动风险管理体系框架，并在欧盟内部的科研教育网中进行部署实践和效果验证。该计划的特色之处在于：态势感知与主动风险管理的结合；

◆ 运用“知识交互”理念促进威胁情报的共享。



Figure 5: Processes involved in generating TI. Image courtesy CERT-UK (CERT-UK, 2015)

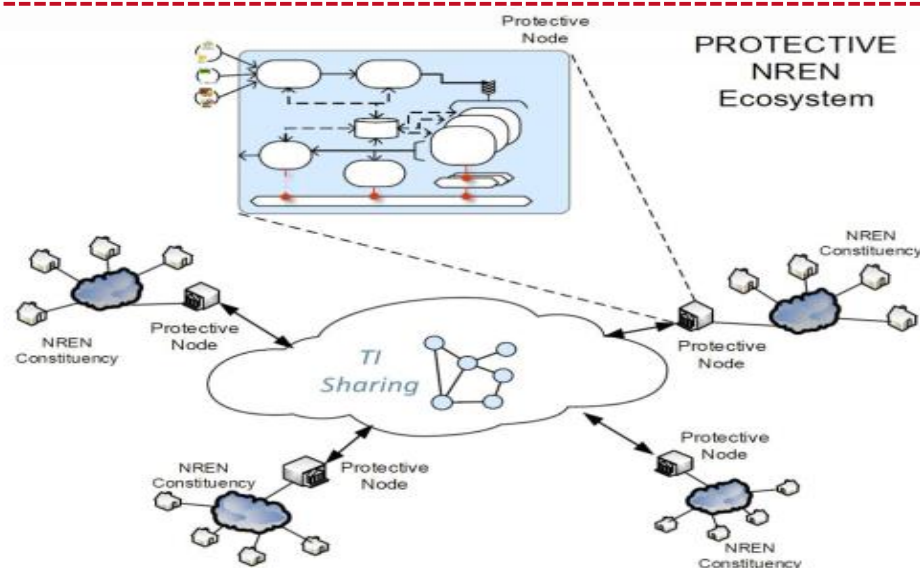


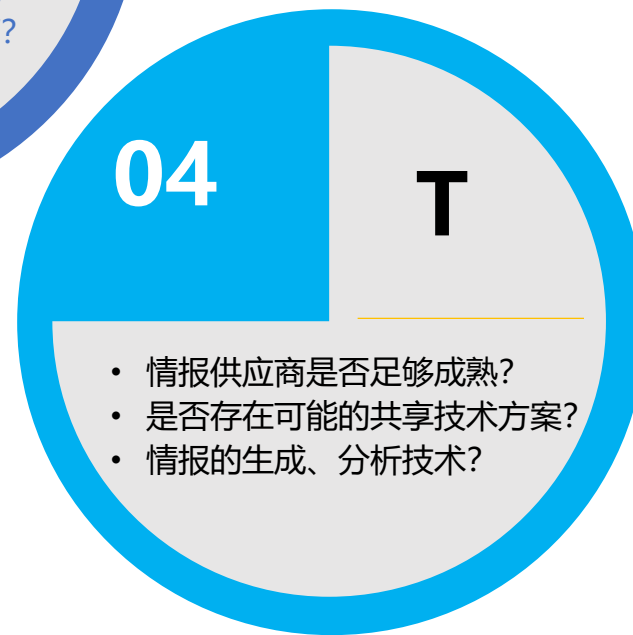
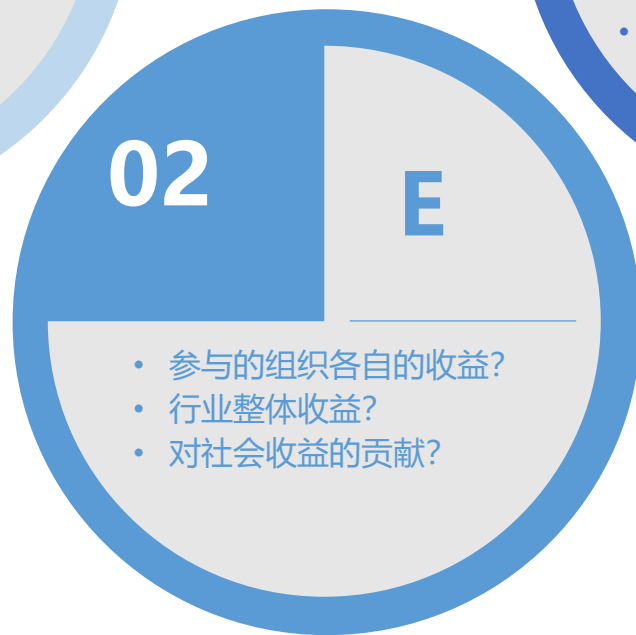
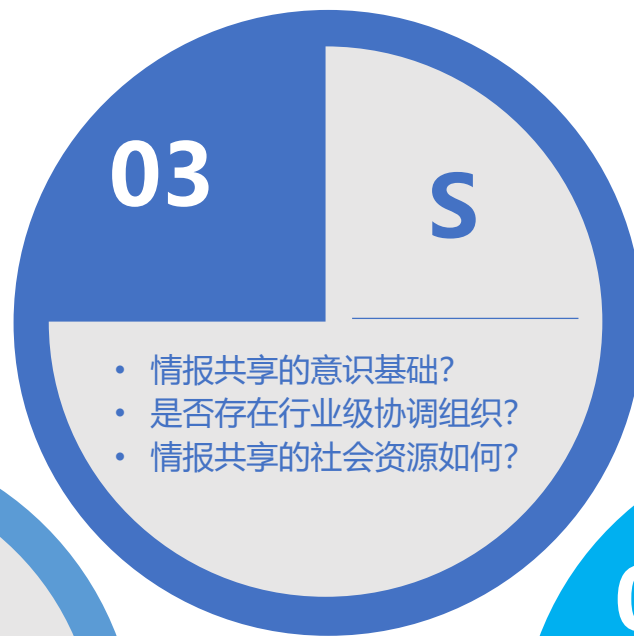
Figure 17: The PROTECTIVE System


我国威胁情报共享的紧密合作已经出现，但广泛的全面、紧密、专业化合作仍待发展



- 2015年10月，烽火台安全威胁情报联盟创立，旨在以安全威胁情报为核心，打造平等互惠的新生态圈模式，共谋共策，推进威胁情报的标准制定及应用推广。
- 2017年9月，威胁情报交换联盟成立于由ISC互联网安全大会发起成立，旨在推动威胁数据交换共享。
- 2018年4月，国家互联网应急中心成立威胁情报共享工作组，工作组包括30多家成员单位。
- 2019年3月，上海市信息安全行业协会发起成立了由互联网、金融科技等覆盖全行业企业组成的“威胁数据共享联盟”。





The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid-like structure, possibly representing a network or data flow. The pattern is more dense in some areas and more sparse in others, creating a sense of depth and movement.

# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE