股票代码：002439

启明星辰

2016阿里安全峰会——网络安全情报在企业侧的落地与实践

叶蓬　　启明星辰 泰合本部

2016-7-14

网络与信息安全面临的挑战

- 攻击无法避免，重要地是检测和响应
- 响应太不及时，留给对手太多自由攻击时间
- 检测力度不够，难以识别未知威胁
- 缺乏主动安全，处处落后于对手
- 各自为战，缺乏协同，知识难于传递
- 人才有限，分布不均，企业侧安全人员匮乏

RSA：当APT成为主流


Report based on discussions with the
Security for Business Innovation Council
RSA
WHEN ADVANCED PERSISTENT THREATS GO MAINSTREAM
Building Information-Security Strategies to Combat Escalating Threats
RECOMMENDATIONS FROM GLOBAL 1000 EXECUTIVES
INSIDE THIS REPORT:
Key characteristics of APTs
How enterprises are making themselves vulnerable
New approaches to information security
Seven defensive measures against escalating threats

RSA报告：2011年

构建一个情报引领的新型安全体系架构

1. **进行高级情报收集与分析** – 让情报成为战略的基石
2. **建立智能监测机制** – 知道要寻找什么，并建立信息安全与网络监控机制，以寻找所要寻找之物
3. **重新分配访问控制权** – 控制特权用户的访问
4. **认真开展有实效的用户培训** – 培训用户以识别社会工程攻击，并迫使用户承担保证企业信息安全的个人责任
5. **管理高管预期** – 确保最高管理层认识到，抗击高级持续性攻击的本质是与数字军备竞赛战斗
6. **重新设计IT架构** – 从扁平式网络转变为分隔式网络，使攻击者难以在网络中四处游荡，从而难以发现最宝贵的信息
7. **参与情报交换** – 分享信息安全威胁情报，利用其他企业积累的知识

威胁情报的定义

Gartner

威胁情报是一种基于证据的知识，包括了情境、机制、指标、隐含和实际可行的建议。威胁情报描述了现存的、或者是即将出现的针对资产的威胁或危险，并可以用于通知主体针对相关威胁或危险采取某种响应。

FORRESTER

威胁情报是针对内部和外部威胁源的动机、意图和能力的详细叙述，包括了这些敌对方的战技过程（TTP）的描述。

SANS

威胁情报是一个为了对安全威胁、恶意攻击者、漏洞利用者、恶意代码、漏洞和失陷指标进行阐释而进行收集、评估和应用的数据集。

美国《国家情报战略》（2014）指出，网络空间情报（cyber intelligence）包括有关外国活动者的网络计划、意图、能力、行动等，他们对本国国家安全、信息系统、基础设施、数据资料的影响，以及外国信息系统网络特征、组件、结构、使用、漏洞等情况。

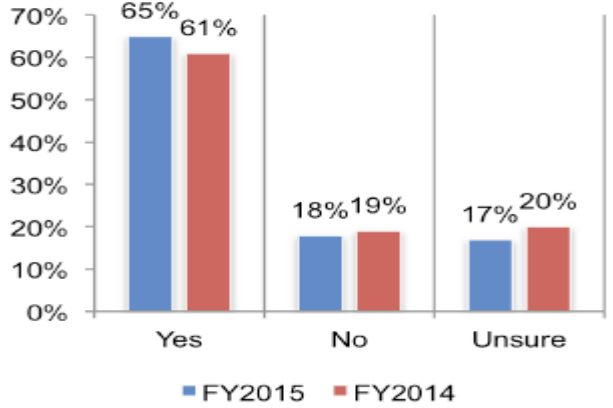
《孙子兵法》：知己知彼，百战不殆

威胁情报正在得到客户认可

Ponemon INSTITUTE

Second Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way

Figure 1. Do you believe threat intelligence could have prevented or minimized the consequences of the attack on your organization?



《第二次关于网络空间威胁情报交换的年度调查报告》*

2015年有65%的受访者表示威胁情报能够阻止或减轻攻击造成的后果

* 该报告基于对692位企业和组织的专业IT人士进行的有效问卷调查得出。

从威胁情报到安全情报/安全智能

- 威胁情报不是漏洞情报！

从防御者的角度来看，获取**威胁**情报是为**知彼**，而获取**漏洞**情报是为**知己**

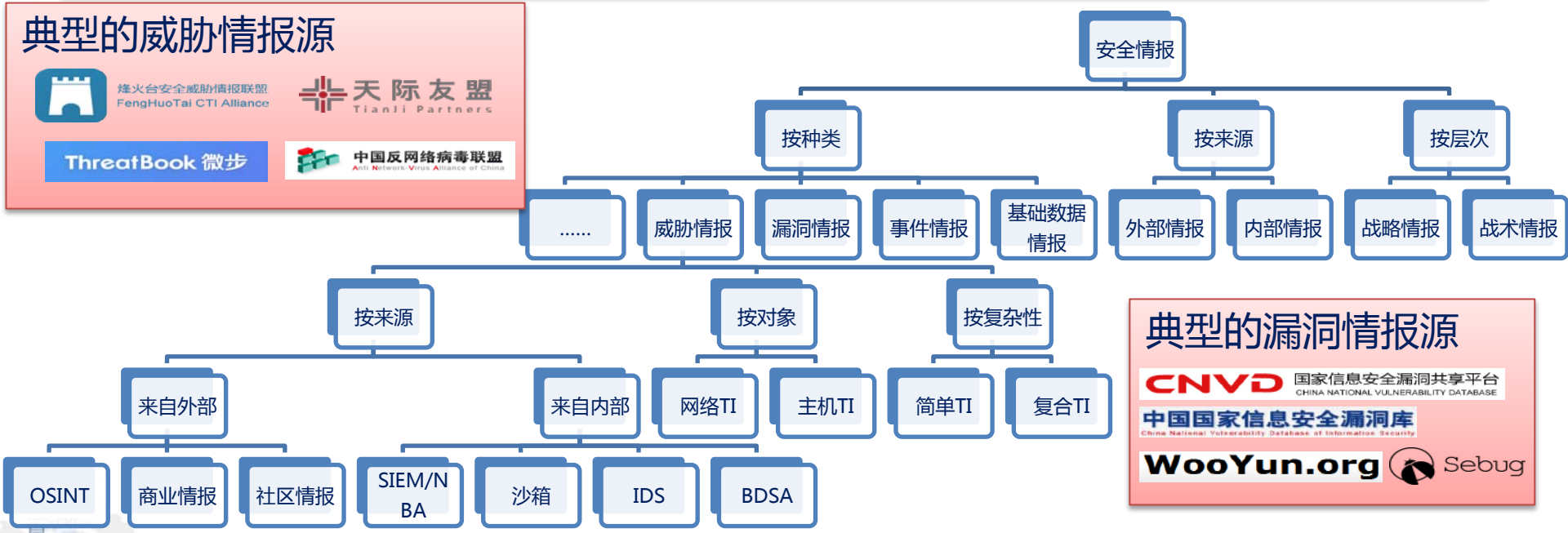
典型的威胁情报源

烽火台安全威胁情报联盟 FengHuoTai CTI Alliance

天际友盟 TianJi Partners

ThreatBook 微步

中国反网络病毒联盟 Anti Network-Virus Alliance of China



典型的漏洞情报源

CNVD 国家信息安全漏洞共享平台 CHINA NATIONAL VULNERABILITY DATABASE

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

WooYun.org

Sebug

安全情报分为提供者和消费者

- 现在国内的视线大都聚焦到安全情报的生产者（提供者）身上了
- 对于如何消费情报谈之甚少

只讲情报本身而不讲情报的使用都是空谈

对于政企客户，情报只有使用起来才有价值！

情报的使用过程就是将情报与企业自身的安全要素信息和安全机制相结合的过程

企业侧如何消费安全情报？

漏洞预警、威胁预警

设备情报升级、系统协同与自动化响应

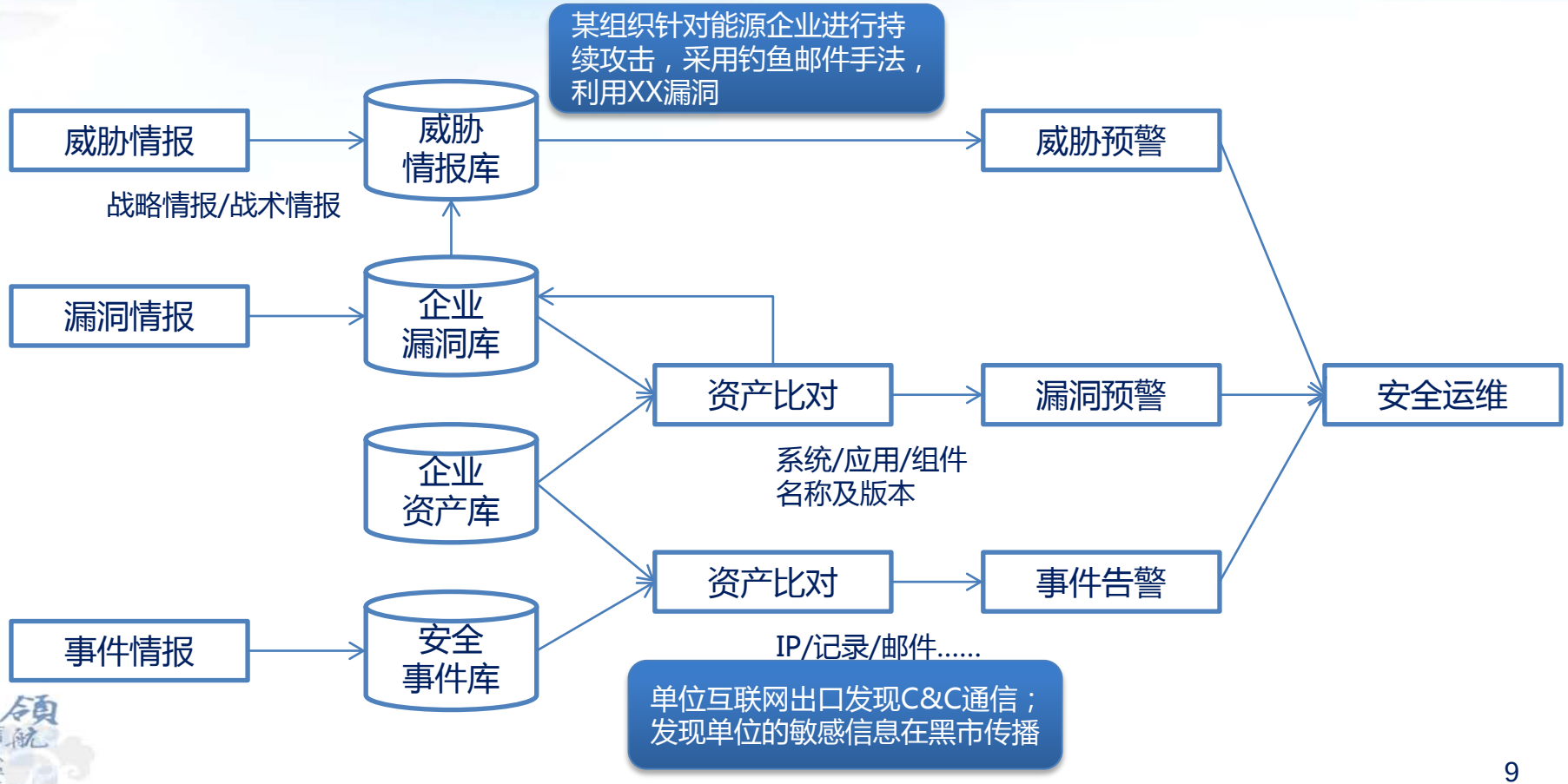
内部数据与外部情报实时比对

内部情报产生与分享

内部历史数据与外部情报批式比对分析

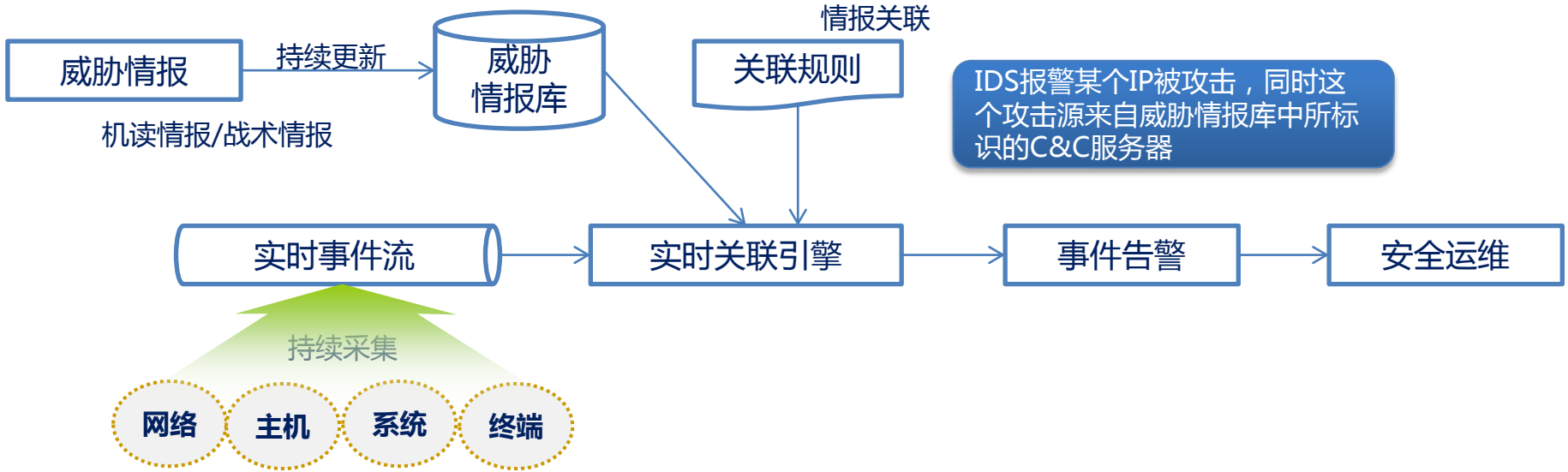
交互式分析、威胁追踪与猎捕、攻击链分析

用例1：安全预警

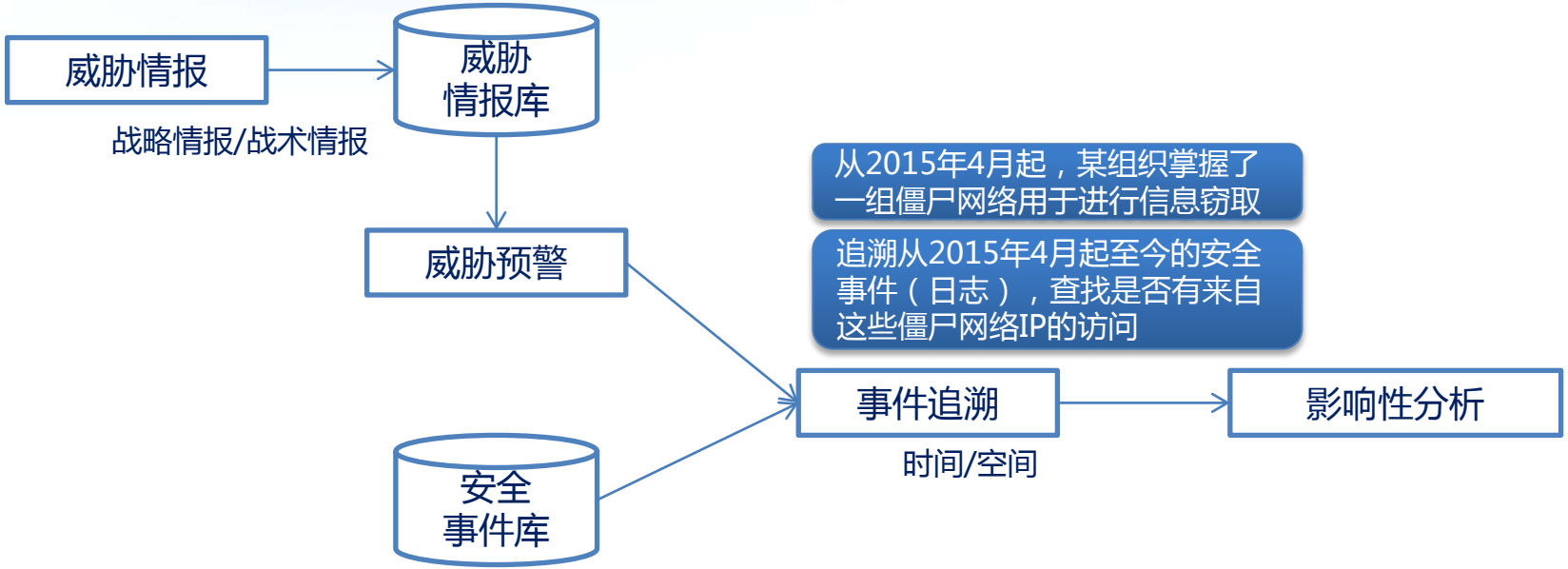

某组织针对能源企业进行持续攻击，采用钓鱼邮件手法，利用XX漏洞
威胁情报
威胁情报库
威胁预警
战略情报/战术情报
漏洞情报
企业漏洞库
资产比对
漏洞预警
安全运维
企业资产库
系统/应用/组件名称及版本
资产比对
事件告警
事件情报
安全事件库
IP/记录/邮件……
单位互联网出口发现C&C通信；发现单位的敏感信息在黑市传播

用例2：实时比对

通过威胁情报增强安全事件关联分析质量



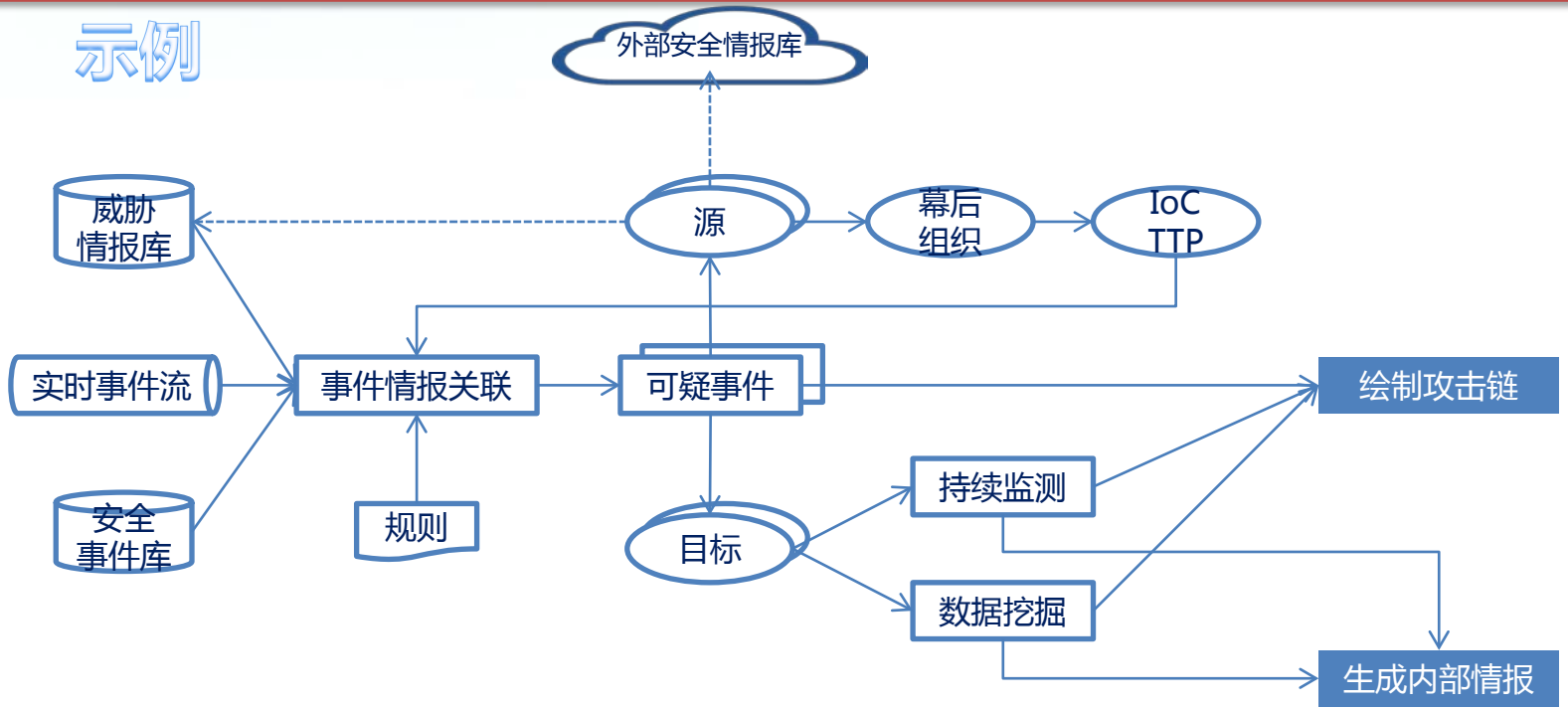
用例3：历史追溯


威胁情报
战略情报/战术情报
威胁
情报库
威胁预警
从2015年4月起，某组织掌握了一组僵尸网络用于进行信息窃取
追溯从2015年4月起至今的安全事件（日志），查找是否有来自这些僵尸网络IP的访问
事件追溯
时间/空间
影响性分析
安全
事件库

用例4：威胁猎捕(Threat Hunting)

威胁猎捕是一个交互式安全分析过程，威胁情报为威胁猎捕提供线索

示例



用例5：情报生成与分享

内部情报更重要！

SANS

Incident Response Capabilities in 2016:
The 2016 SANS Incident Response Survey

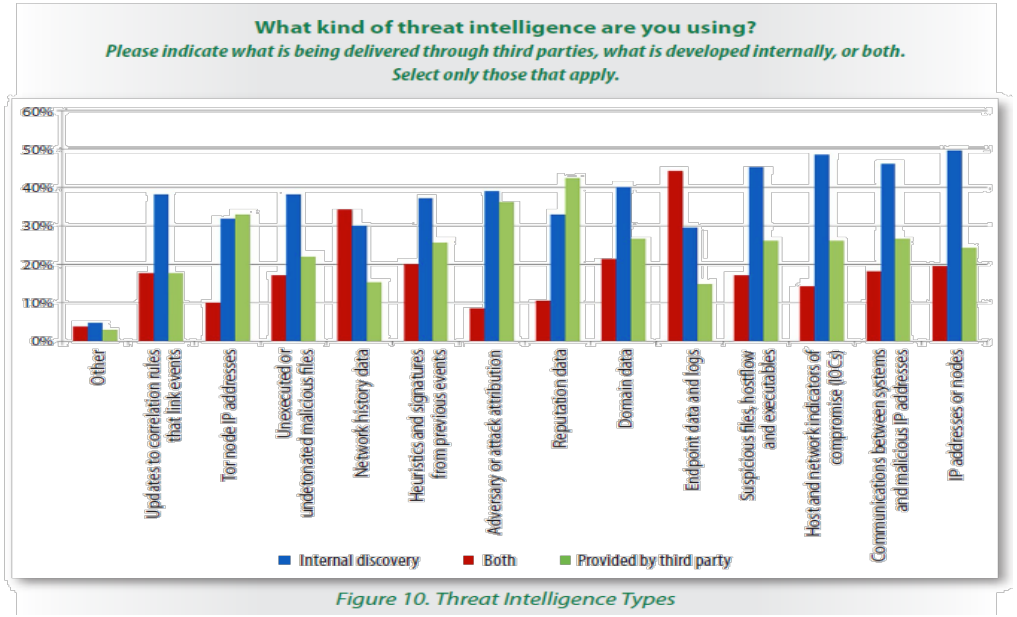
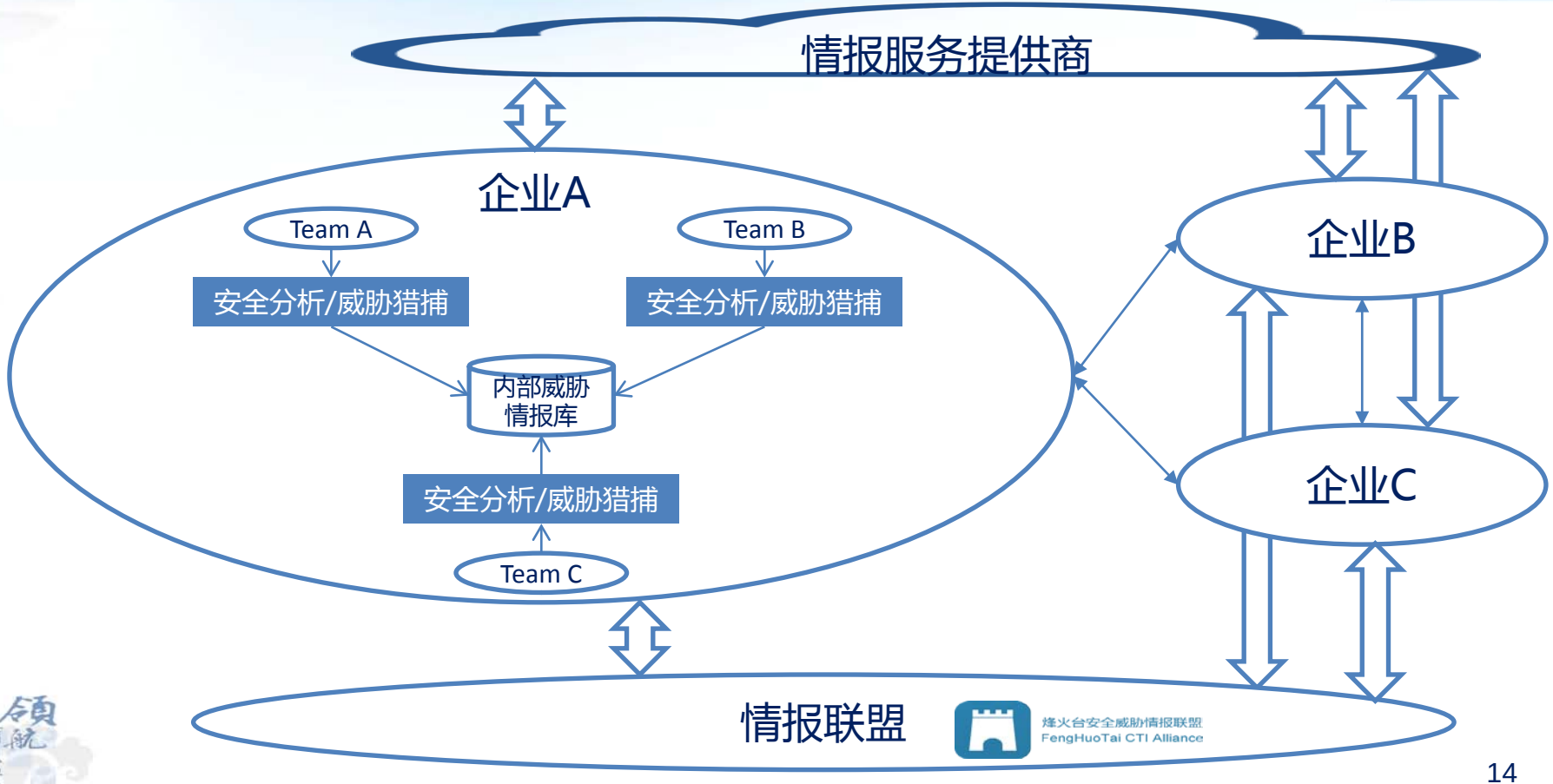
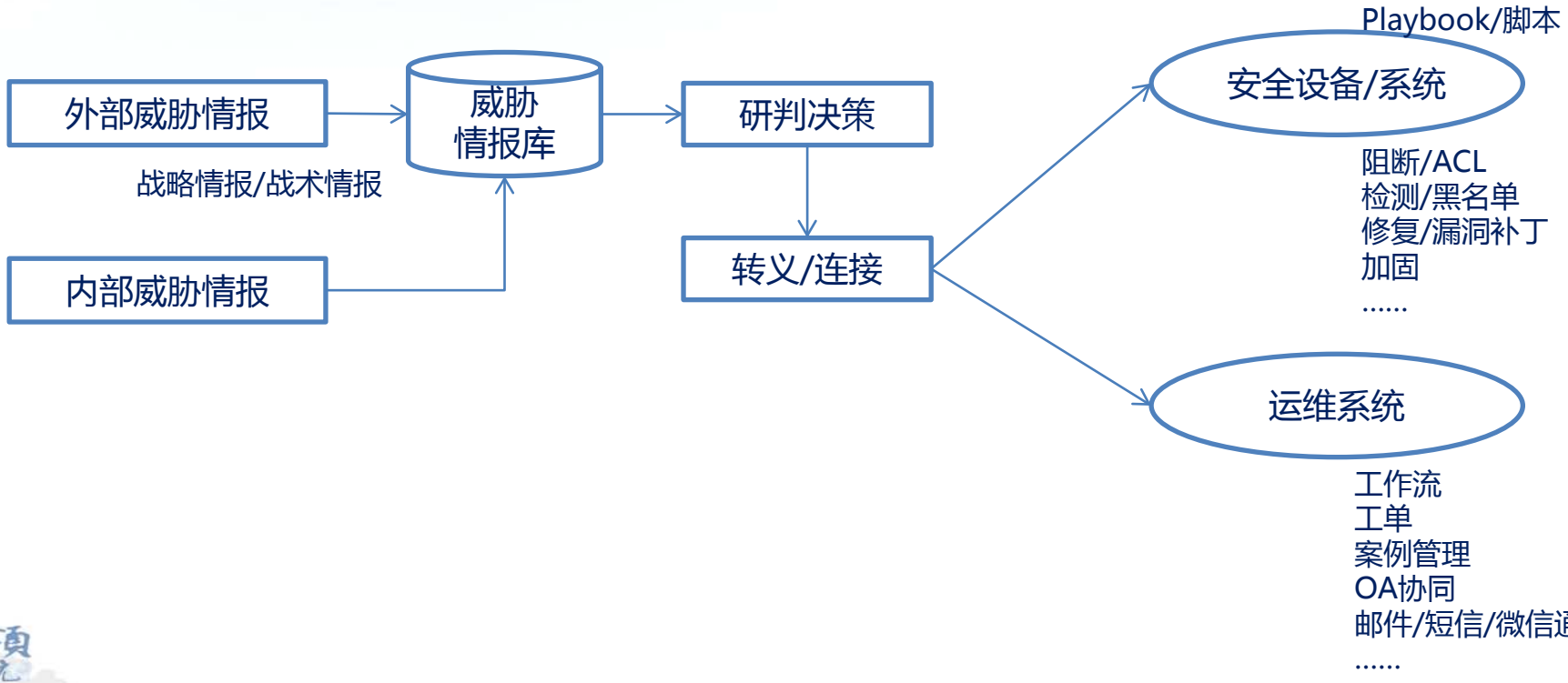


Figure 10. Threat Intelligence Types

用例5：情报生成与分享


情报服务提供商
企业A
Team A
Team B
安全分析/威胁猎捕
安全分析/威胁猎捕
内部威胁
情报库
安全分析/威胁猎捕
Team C
企业B
企业C
情报联盟
烽火台安全威胁情报联盟
FengHuoTai CTI Alliance

用例6：协同响应


外部威胁情报
战略情报/战术情报
内部威胁情报
威胁
情报库
研判决策
转义/连接
安全设备/系统
Playbook/脚本
阻断/ACL
检测/黑名单
修复/漏洞补丁
加固
……
运维系统
工作流
工单
案例管理
OA协同
邮件/短信/微信通知
……

企业侧如何落地安全情报？

企业安全情报平台+SOC/SIEM

SOC/SIEM是承载机读威胁情报的最优选择

Gartner

G00259304

Technology Overview for Machine-Readable Threat Intelligence

Published: 9 January 2014

Analyst(s): Craig Lawson, Rob McMillan

Machine-readable threat intelligence is a capability that allows SIEM and other security controls to make operational security decisions based on information about the prevailing threat landscape. Security leaders should understand how MRTI operates, and how it can be used to mitigate threats.

Recommendations

CISOs, CTOs and security leaders should:

- Enable or add MRTI capabilities to security controls such as SIEM, NGFW and IPS if they are available from their existing providers.
- Leverage MRTI content to make "threat context"-based decisions for SIEM, NGFW and NGIPS.
- Exploit the benefits of MRTI at each layer, stretching from endpoint to network.

Use SIEM as the most effective tool at ingesting multiple sources of MRTI to provide maximum advantage to give visibility to a broad range of threats.

SOC需要借助威胁情报来提升自身的价值

Gartner

The Five Characteristics of an Intelligence-Driven Security Operations Center

2 November 2015 ID:G00271231

Analyst(s): Oliver Rochford, Neil MacDonald

Recommendations

Security leaders building or maturing a SOC must:

Adapt a mindset that is based on the assumption that they have already been compromised.

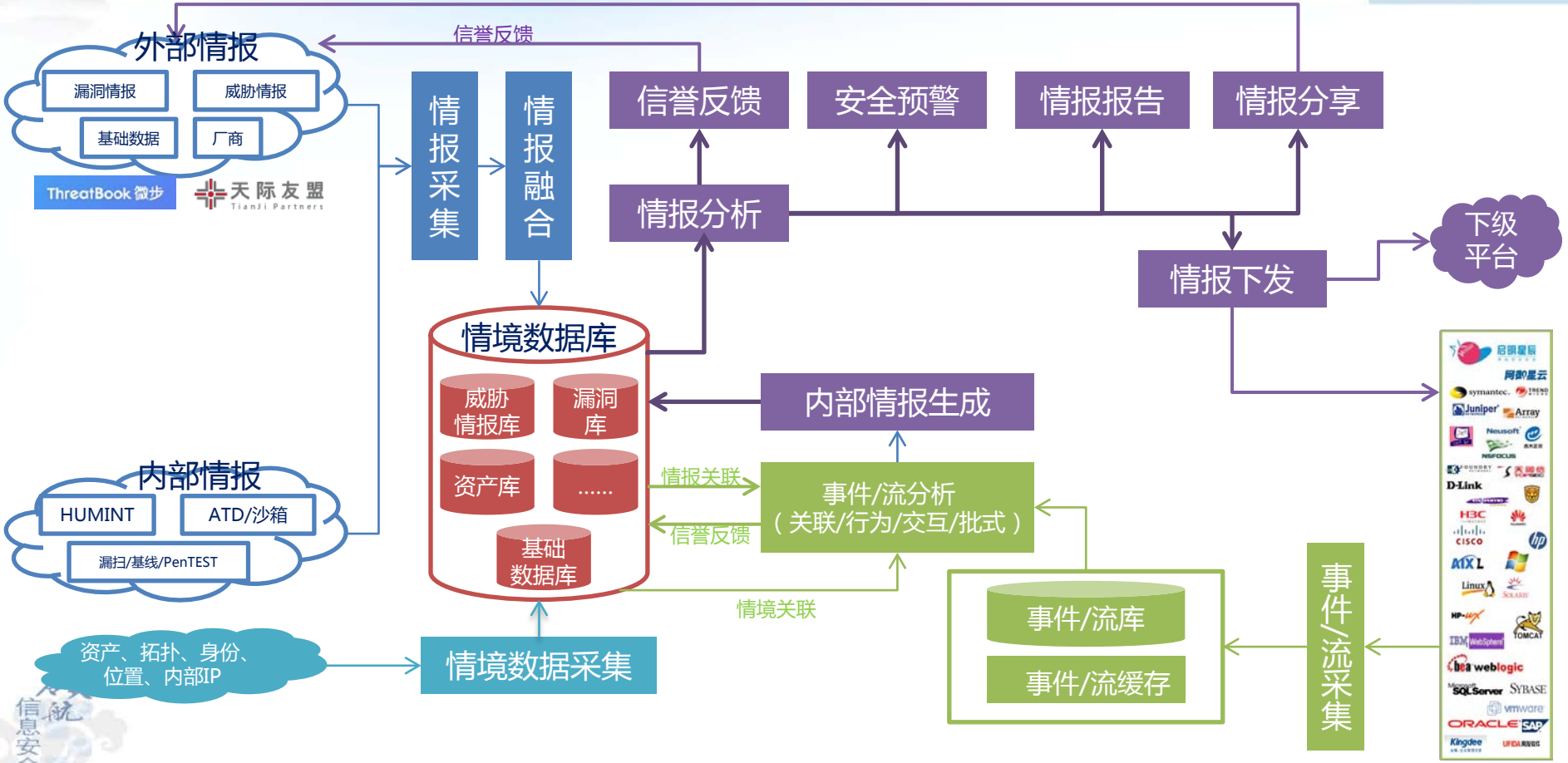
Instrument their SOC for comprehensive visibility.

Follow an intelligence-driven SOC approach with these five characteristics: use multisourced threat intelligence strategically and tactically; use advanced analytics to operationalize security intelligence; automate whenever feasible; adopt an adaptive security architecture; and proactively hunt and investigate.

未来SOC发展趋势：

① 在战略和战术上集成威胁情报
② 通过高级分析将安全智能落地
③ 尽可能地安全自动化
④ 主动的威胁猎捕与调查
⑤ 部署自适应安全架构

企业安全情报平台eSIP+SIEM/SOC



企业安全情报平台的价值

启明星辰如何将安全情报落地？

泰合计划

泰合

ThreatBook 微步

天际友盟 TianJi Partners

启明星辰泰合™
安全管理平台+企业安全情报平台

国内最专业的
独立威胁情报服务提供商

泰合计划的宗旨是：**平等协作、互利共赢**
以泰合安管平台为依托，**连接**业界优秀的安全威胁分析能力，共同为政企客户交付安全价值

情报利用能力成熟度

Level	Capability	Sources	Usage and Tools	Processes
1.	N/A — Feed into system OOB	Security vendors	NIPS, firewall —Blocking	Consumption
2.	TI tasks	Security vendors, OSS, some TI vendors	NIPS, SIEM — Detection	Aggregation
3.	Part time TI role	Tactical TI vendors, government, and so on	SIEM, NFT, some ETDR — Detection, triage	Aggregation and some validation
4.	TI person/team in SOC/CIRT	Tactical, strategic TI vendor, government community	TMC/TIM platform (SaaS?), SIEM, NFT, ETDR — Detection, triage, fusion	Fusion, multitool usage
5.	Fusion center, TMC/TIM (a peer to SOC and CIRT), custom intelligence	Internal (I), tactical/strategic TI vendors, community, private, and so on	Custom TMC/TIM fusion platform, indicator management, reversing lab	Fusion, creation, sharing

Gartner

建议和结论

- 对于政企客户而言，需要知道
  - 利用安全情报是大势所趋
  - 正确厘清安全情报的内涵和外延
  - 了解情报服务提供商的类型和内容分类
  - 了解消费情报的6种style
  - 大型客户需要考虑搭建安全情报平台
  - 情报的消费要跟自身实际相匹配