协同安全能力 共建情报生态

威胁情报生态大会

Enhance enterprise threat intelligence capability and promote intelligence sharing

提升企业威胁情报能力，推动情报共享

中国华电集团有限公司

演讲人：罗建东

日期：2019年1月

01

中国华电简介

China huadian introduction

02

企业威胁情报的应用

Application of corporate threat intelligence

03

威胁情报的共享共用

The sharing of threat intelligence

中国华电男建东

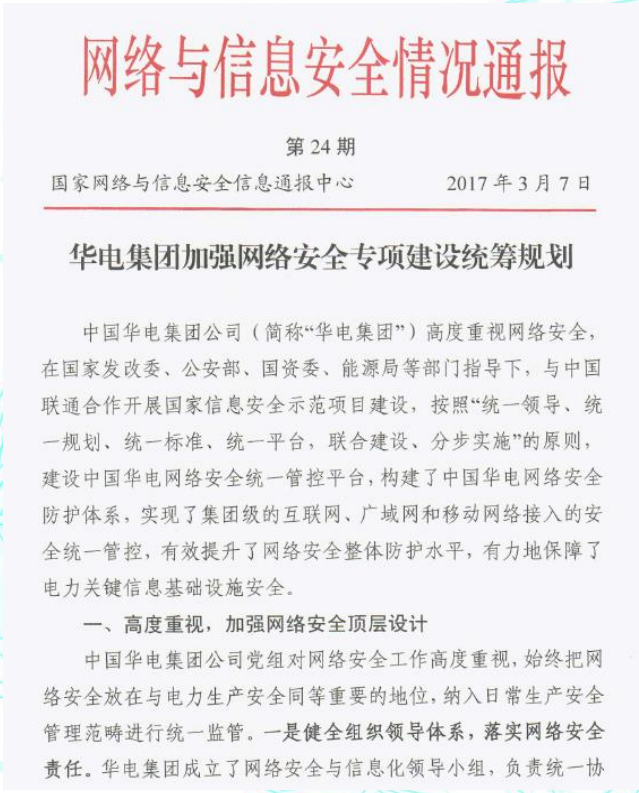
PART 01

中国华电简介

China huadian introduction

14827万千瓦	5123亿千瓦时	7984亿元	2006亿元
装机容量	发电量	资产总额	营业收入

中国华电集团有限公司是2002年底国家电力体制改革组建的国有独资发电企业，属于国务院国资委监管的特大型中央企业，主营业务为：电力生产、热力生产和供应；与电力相关的煤炭等一次能源开发以及相关专业技术服务。近年来，公司深入贯彻落实党中央、国务院各项决策部署和国家能源战略，加快结构调整，着力提质增效，深化改革创新，加强党的建设，综合实力不断增强，行业地位明显提升。2017年在世界500强排名382位。



网络与信息安全情况通报

第 24 期

国家网络与信息安全信息通报中心　　2017 年 3 月 7 日

华电集团加强网络安全专项建设统筹规划

中国华电集团公司（简称“华电集团”）高度重视网络安全，在国家发改委、公安部、国资委、能源局等部门指导下，与中国联通合作开展国家信息安全示范项目建设，按照“统一领导、统一规划、统一标准、统一平台，联合建设、分步实施”的原则，建设中国华电网络安全统一管控平台，构建了中国华电网络安全防护体系，实现了集团级的互联网、广域网和移动网络接入的安全统一管控，有效提升了网络安全整体防护水平，有力地保障了电力关键信息基础设施安全。

一、高度重视，加强网络安全顶层设计

中国华电集团公司党组对网络安全工作高度重视，始终把网络安全放在与电力生产安全同等重要的地位，纳入日常生产安全管理范畴进行统一监管。**一是健全组织领导体系，落实网络安全责任。**华电集团成立了网络安全与信息化领导小组，负责统一协

中国华电一贯高度重视网络安全工作，坚持做好顶层设计，不断健全完善网络安全体系和网络安全保障与信息通报机制。国家网络与信息安全信息通报中心曾发专报，宣传中国华电网络安全工作。

为了贯彻落实中央网络安全和信息化领导小组的有关要求，在国家发改委、公安部、国资委、国家能源局等相关部委的指导下，中国华电承担了国家发改委国家信息安全专项-网络安全统一管控项目。

针对央企集团面临的主要网络安全风险和威胁，采用安全可控的技术、产品和服务，开展发电电力行业信息系统网络安全试点示范工作，探索建立关键信息基础设施网络安全联动保障机制，提高了关键信息基础设施网络安全综合保障能力和水平。

- 关闭了华电300余家系统单位的本地互联网出口，将分散在各地的互联网出口统一汇聚至北京总部互联网出口，实现了华电系统单位近100000人的互联网统一管控；
- 开通300余家系统单位的广域网，实现ERP和燃料等核心业务系统使用单位的双线广域网全覆盖；
- 提供集团级移动网络接入平台，支撑200余家系统单位的数万个移动办公用户接入。


集中的安全管控


分散的安全部署


实时的监控预警


归一化的网络服务


冗余化的网络安全设计

在中央企业首家全面实现了集团级的互联网、广域网和移动网络接入的安全统一管控，实现了用户统一认证、设备统一管理、流量统一控制、数据统一收集和综合安全态势感知，集团公司网络安全管控能力得到大幅提升。

PART 02

企业威胁情报的应用

Application of corporate threat intelligence

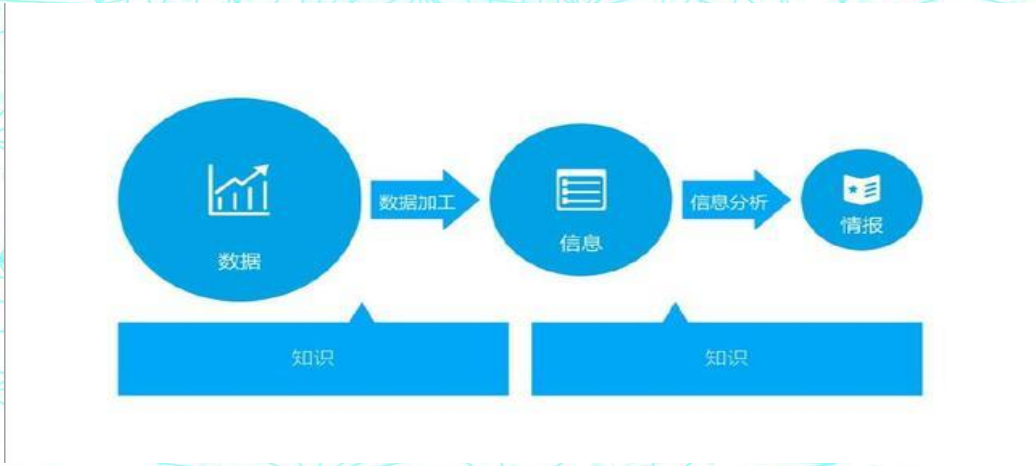
企业的威胁情报应用需求

网络攻击呈现多样化、复杂化、专业化的趋势，传统方法难以检测并阻断这些新式攻击。

攻防的不对等使得企业在网络安全这场没有硝烟的“战争”中处于被动挨打的位置。

企业亟需在自身的网络安全体系中应用威胁情报，改变被动态势。

Gartner 在 2014 年发表的《安全威胁情报服务市场指南》(Market Guide for Security Threat Intelligence Service) 中提出的定义：威胁情报是关于IT或信息资产所面临的现有或潜在威胁的循证知识，包括情境、机制、指标、推论与可行建议，这些知识可为威胁响应提供决策依据。



企业的威胁情报是什么

是什么？

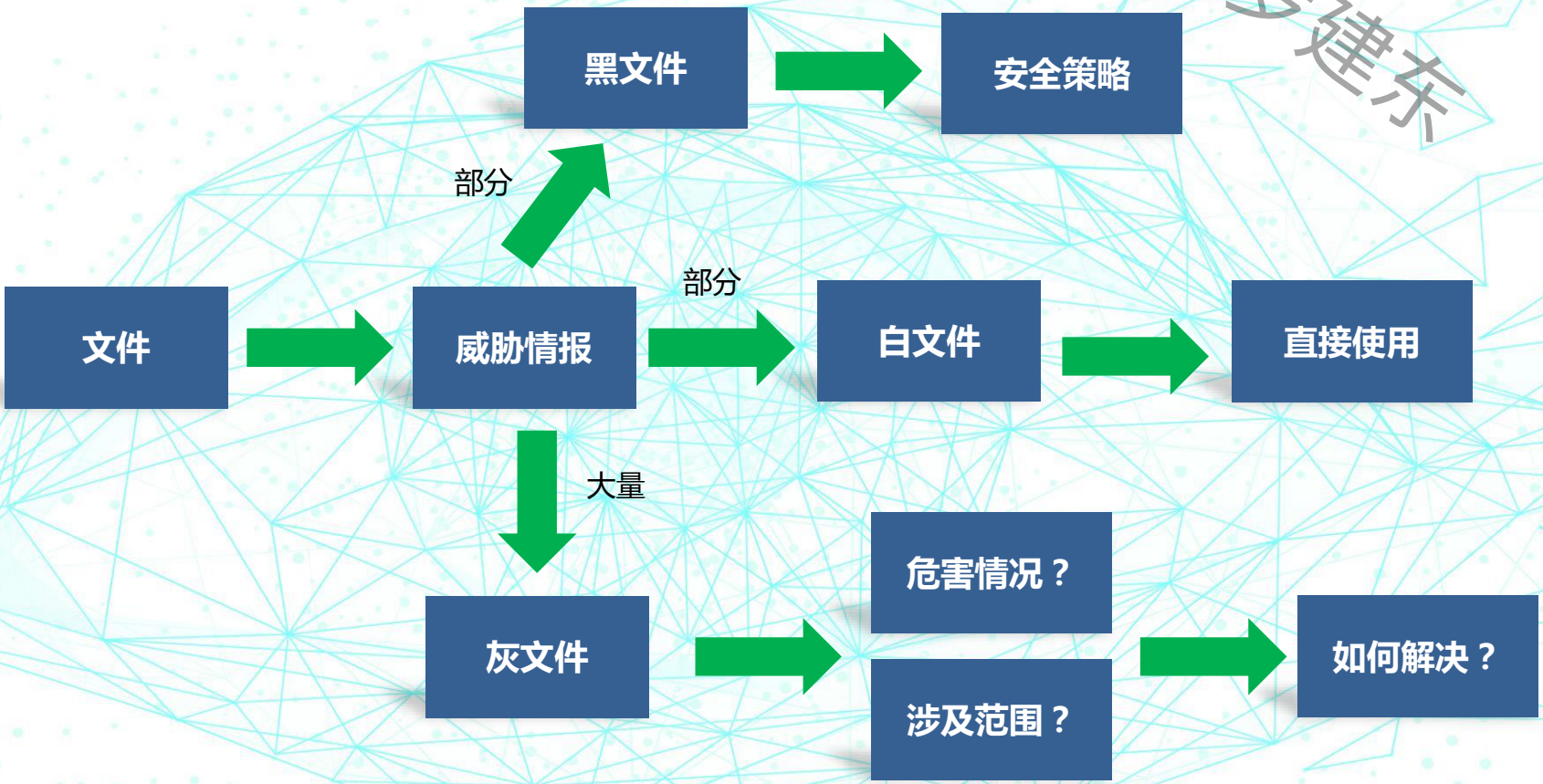
《孙子·谋攻篇》有云：“知彼知己，百战不殆；不知彼而知己，一胜一负；不知彼，不知己，每战必殆。”

知彼：调用外部开源或付费的威胁情报接口，获取最新的外部威胁情报，形成对外的感知能力。

知己：借助自身的安全基础设施和分析能力（资产识别、沙箱、漏洞扫描、NTA）产生与企业相关的自身威胁情报，形成对自身的感知能力。

怎么用？

将内外部威胁情报相关联，通过安全分析平台，让企业对于攻击有更清晰全面的认识，从而能够更好的应对安全威胁和攻击。



威胁情报的应用需求

终端电脑

- ✓ Windows 7/8/10
- ✓ Windows XP
- ✓ MAC OS
- ✓ ……

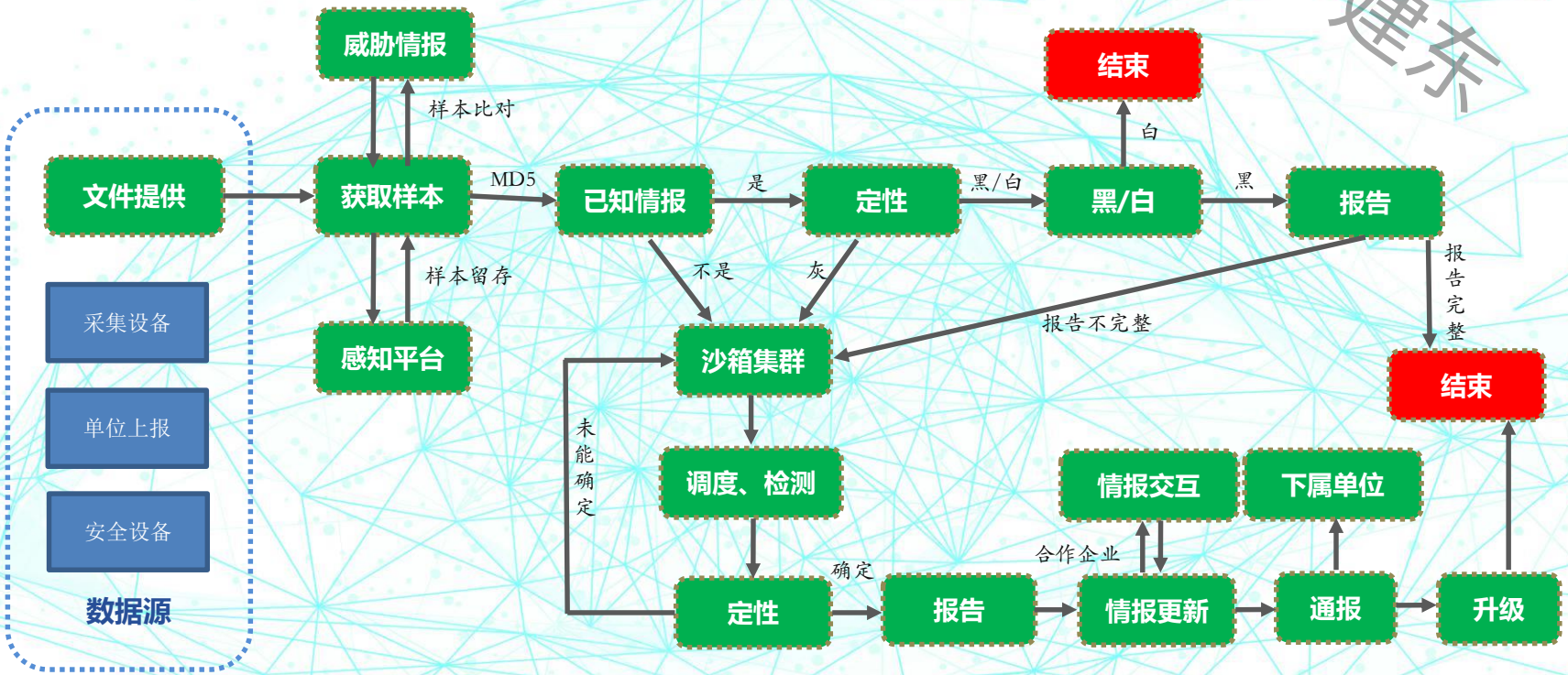
服务器

- ✓ server 2003/2008
- ✓ Linux
- ✓ ……

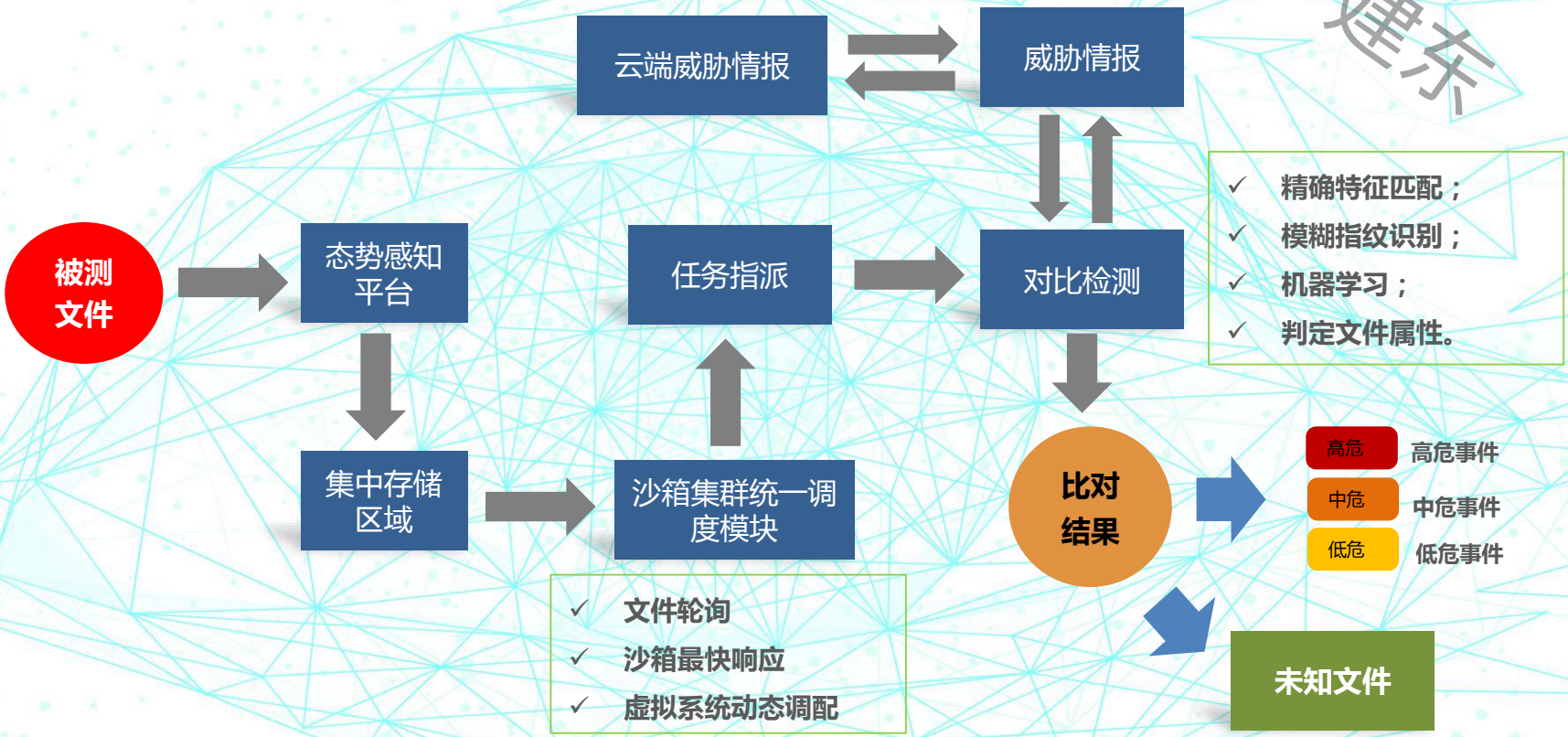
BYOD设备

- ✓ Andriod
- ✓ IOS
- ✓ Windows
- ✓ ……

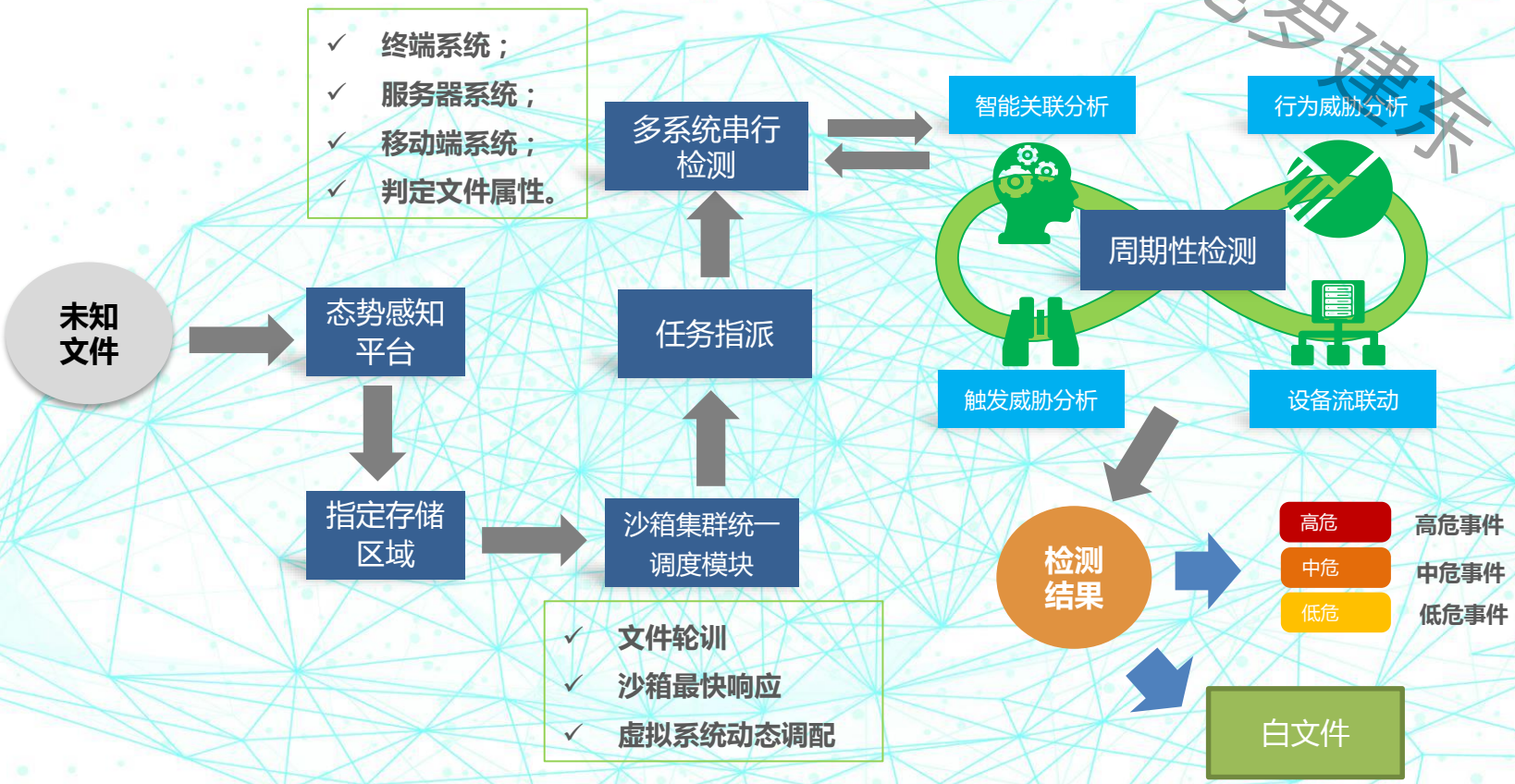
企业威胁情报衍进流程图

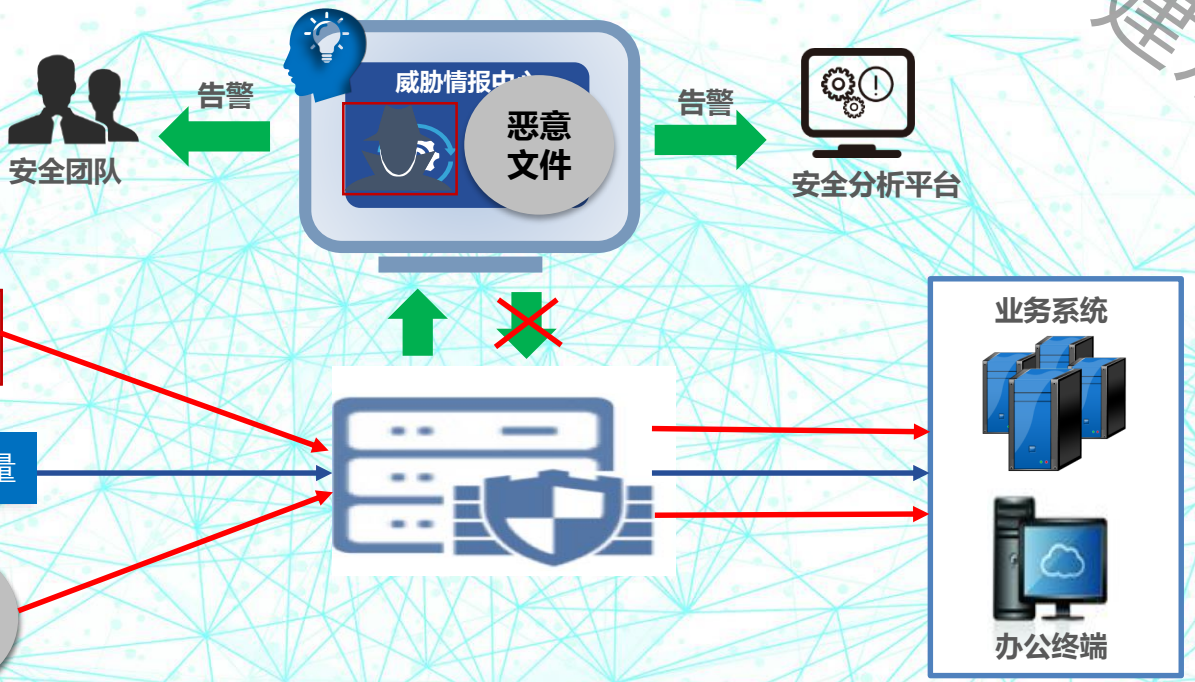


威胁情报应用-静态比对

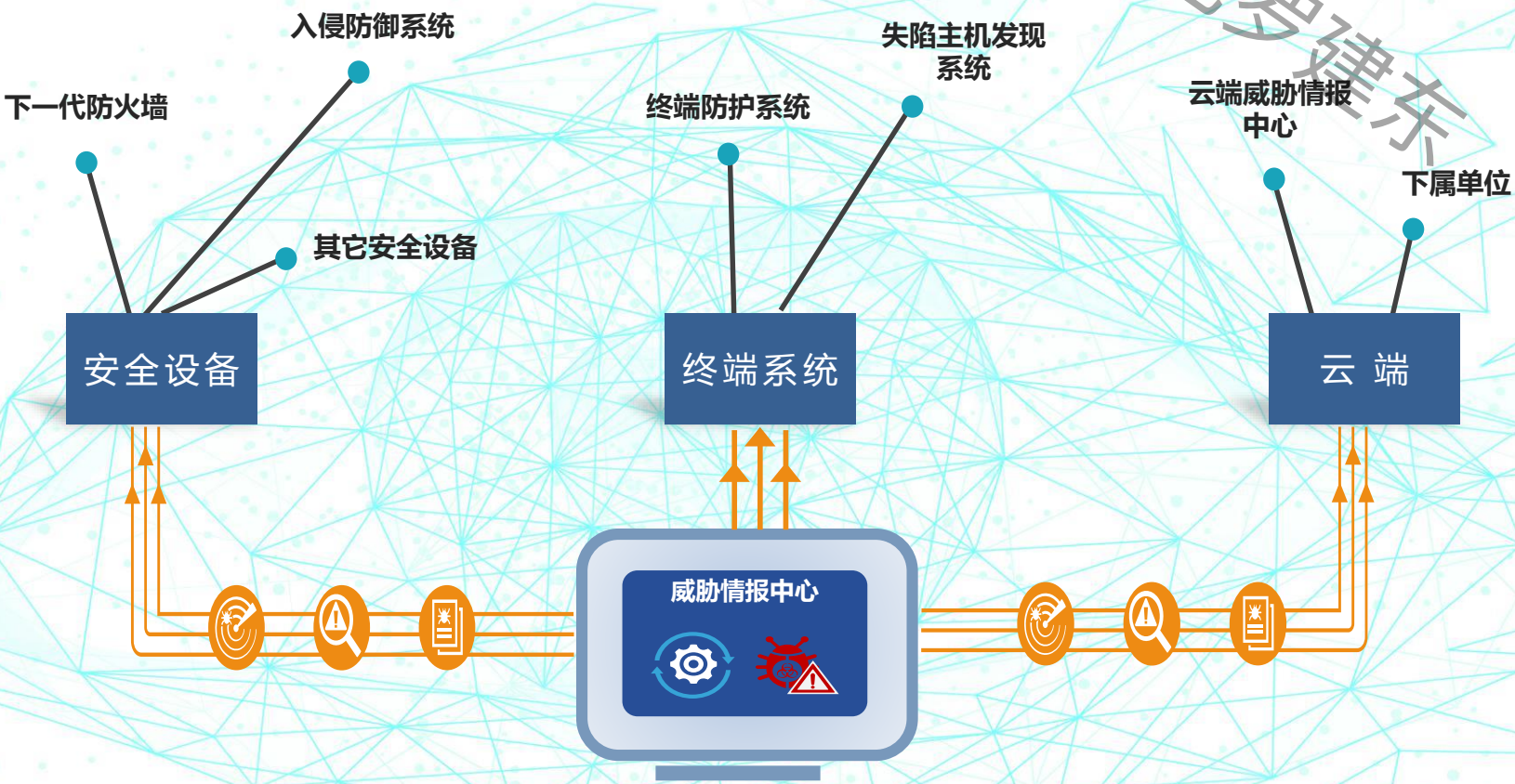


文件仲载，内生威胁情报

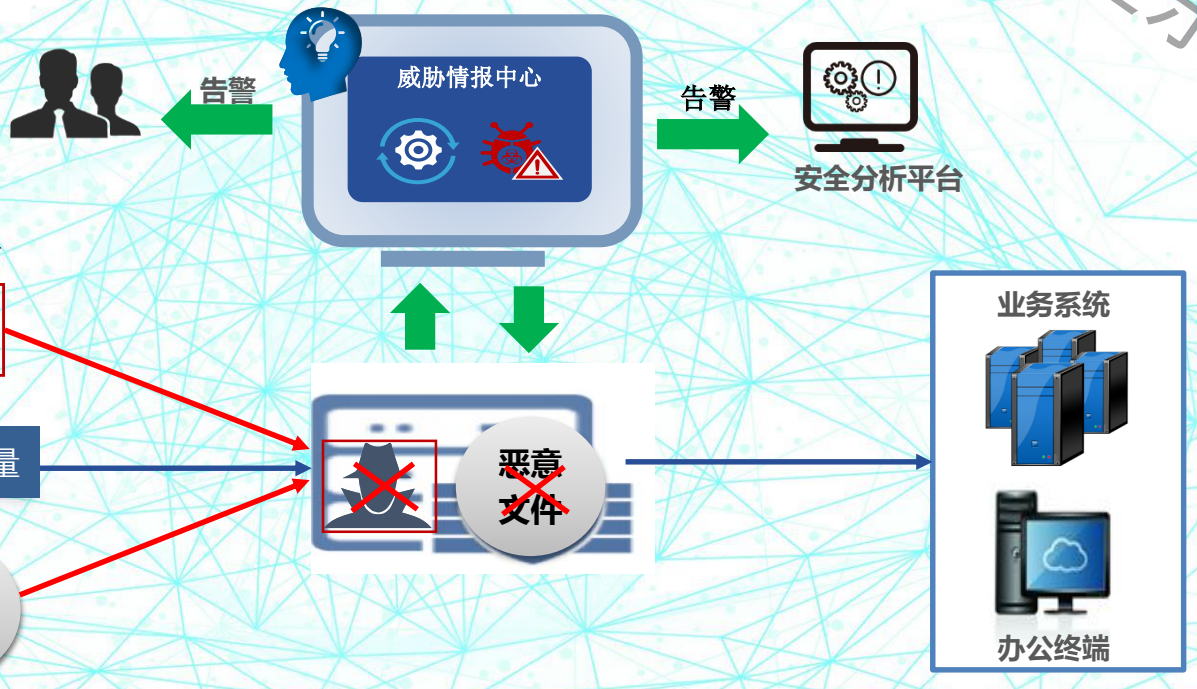




威胁情报的落地

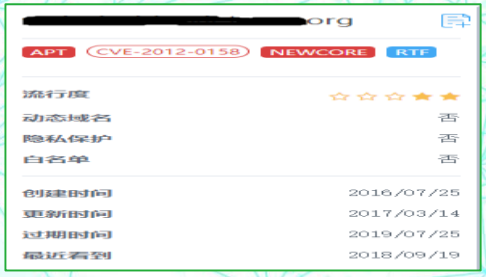


威胁情报的智慧应用（自动化）



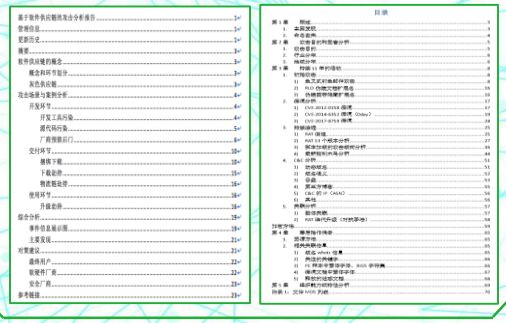
作战情报

丰富的情报上下文，帮助轻松研判事件优先级



安全论坛爆出某种针对央企的最新变种威胁样本。

战略情报



APT报告中给出针对央企的APT组织名单及常用的武器样本。

内网威胁狩猎流程

1

威胁情报中心

2

态势感知平台通过自动查询存储区的流量数据及各类安全日志，以方便调查

威胁情报
您对这些可观测量（IP，Hash，URL等）了解多少？

论坛、网站发布

威胁情报

暗网信息

ooo

威胁调查
我们看过这些攻击吗？
哪些终端与这些威胁相关？

终端

DNS

邮件

网络数据

安全设备

1

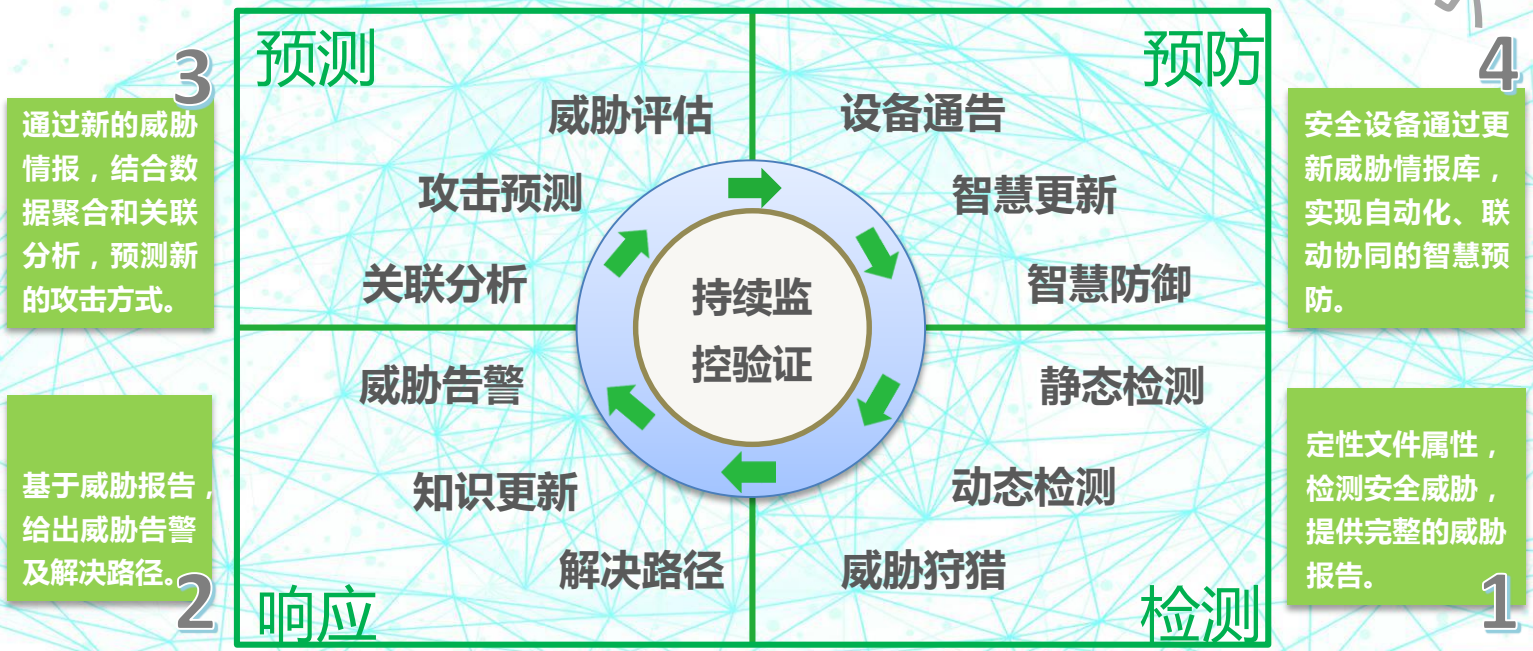
定 义---威胁狩猎是主动搜索自身网络的过程，以检测和隔离逃避现有安全防御措施的高级威胁。

2

目 标

- 回答一个简单的问题：“我受到攻击了吗？"
- 识别网络或终端系统中存在攻击的证据
- 评估现有的安全工具并找出差距以减少攻击面
- 通过寻找新的检测方法来查找攻击者，从而缩短黑客存在的时间

威胁情报贯穿于企业安全运营管理的每个环节，才能真正提升企业的威胁情报能力



企业如何用好威胁情报

1. 网络安全要有顶层设计，整体体系架构要能够联动协同
2. 威胁情报标准化、应用自动化
3. 内外部情报要结合使用
4. 与安全分析平台（ SIEM/SOC/态势感知平台）结合使用
5. 具备基本的网络安全团队（安全分析人员）
6. 选择威胁情报应关注针对性、时效性、威胁报告的可读可用性、是否支持或兼容国家标准和STIX、TAXII等国际标准

PART 03

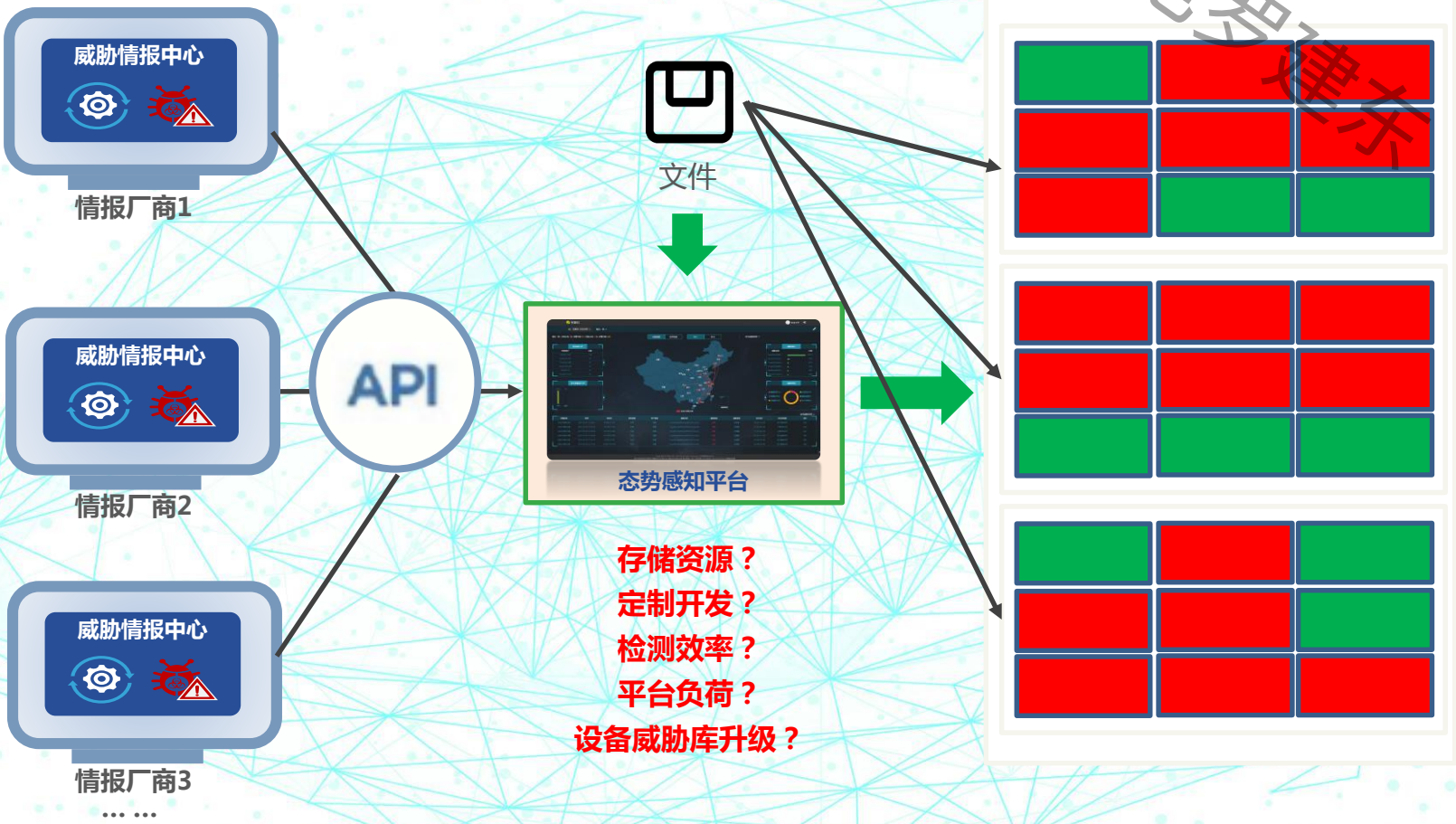
威胁情报的共享共用

The sharing of threat intelligence

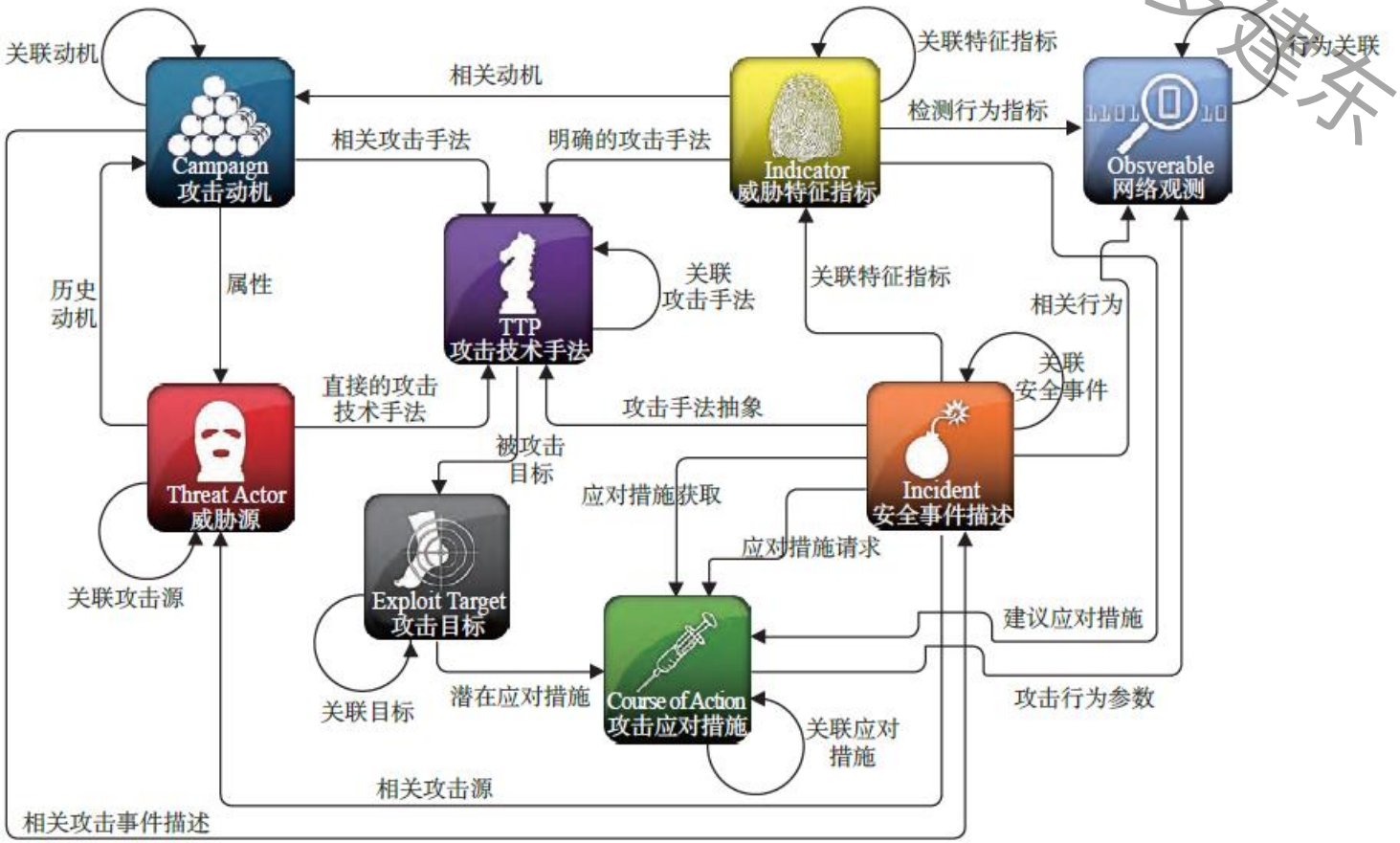
习近平总书记指出

- 没有网络安全就没有国家安全。
- 要建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。
- 要建立政府和企业网络安全信息共享机制，把企业掌握的大量网络安全信息用起来。网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。

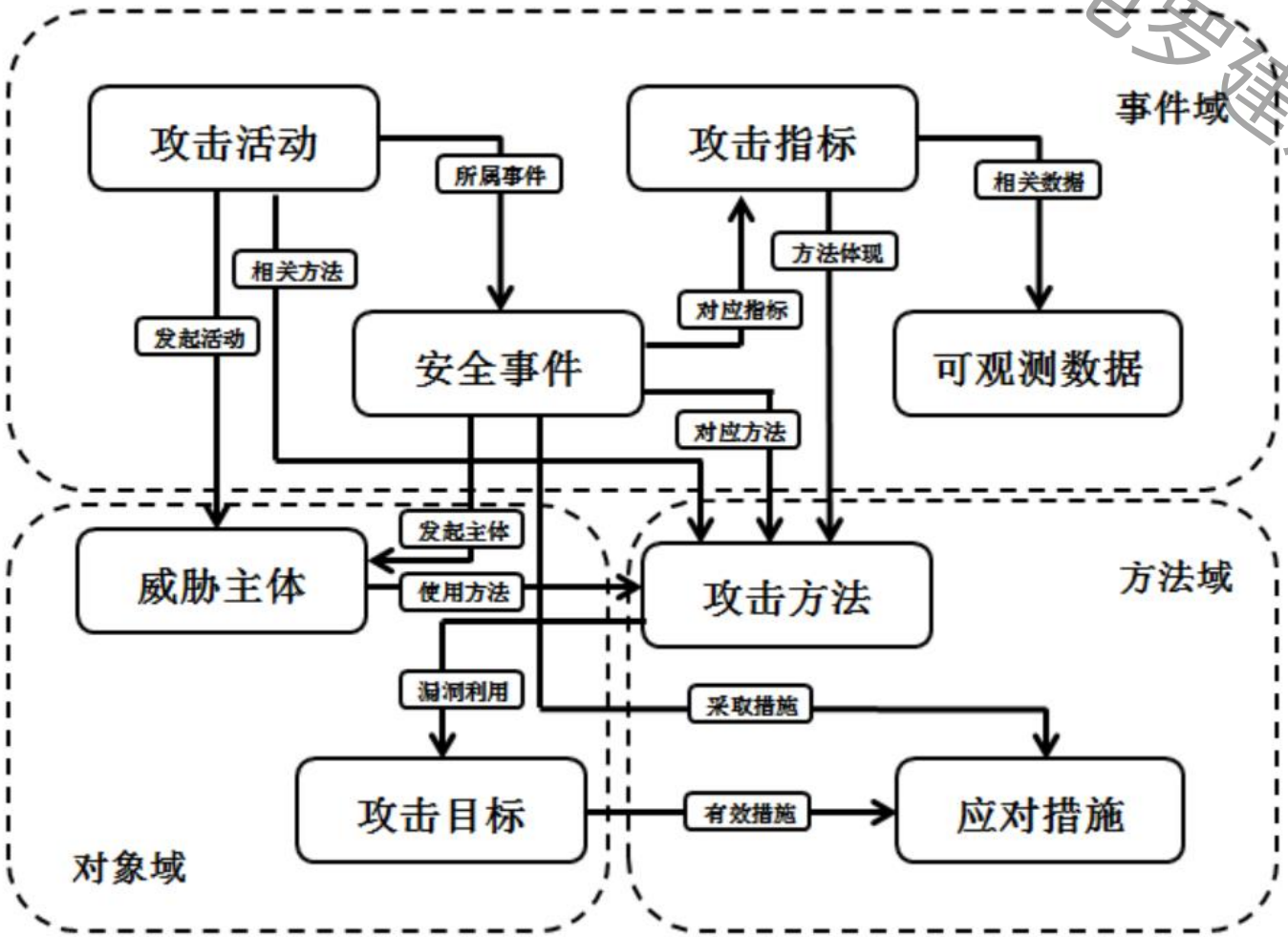
威胁情报应用的壁垒



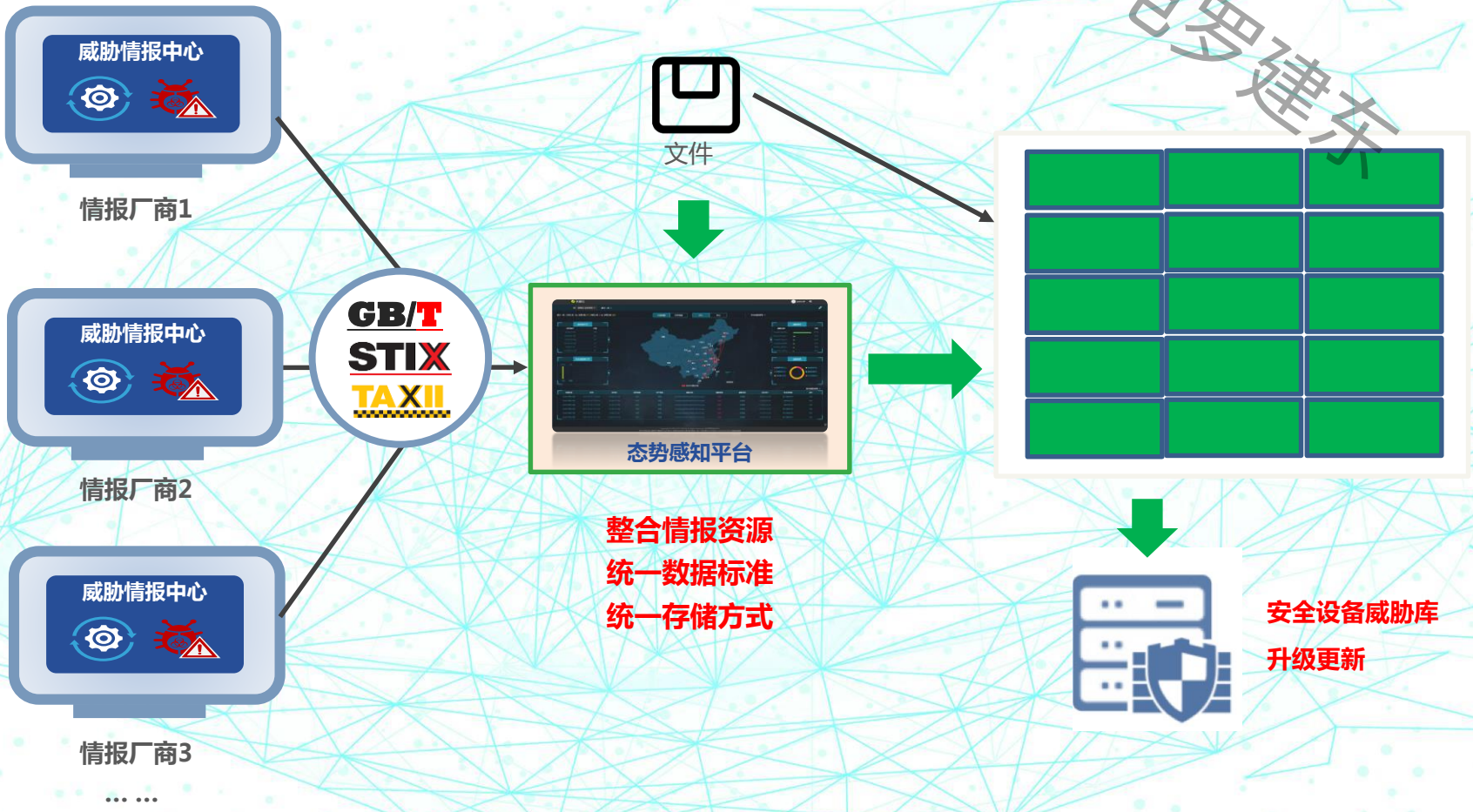
（STIX）


关联动机
Campaign
攻击动机
相关动机
关联特征指标
Indicator
威胁特征指标
检测行为指标
行为关联
Obsverable
网络观测
相关攻击手法
明确的攻击手法
历史
动机
属性
TTP
攻击技术手法
关联
攻击手法
关联特征指标
相关行为
关联
安全事件
直接的攻击
技术手法
攻击手法抽象
Threat Actor
威胁源
被攻击
目标
应对措施获取
Incident
安全事件描述
应对措施请求
关联攻击源
Exploit Target
攻击目标
建议应对措施
关联目标
潜在应对措施
Course of Action
攻击应对措施
攻击行为参数
关联应对
措施
相关攻击源
相关攻击事件描述

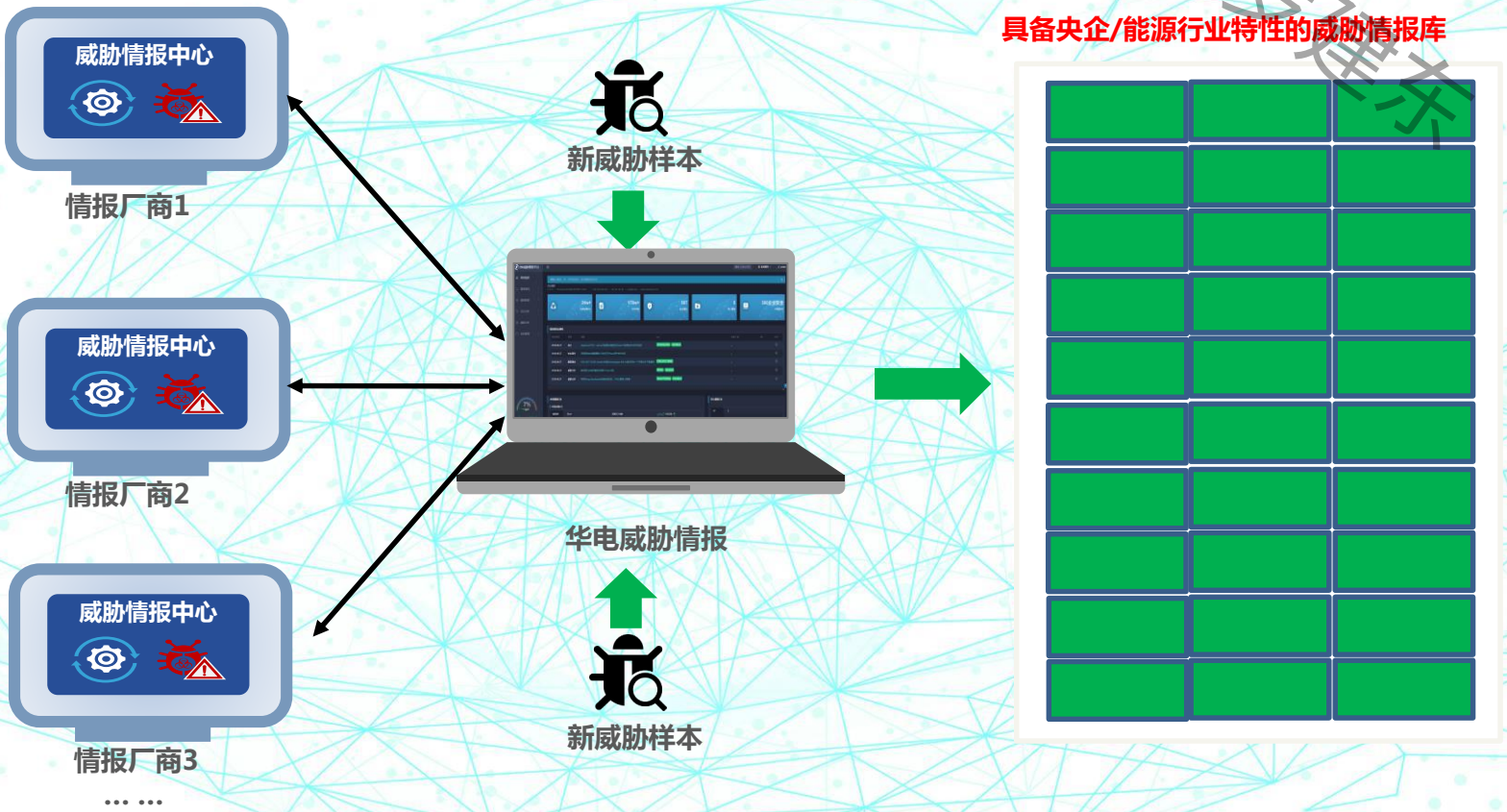
网络安全威胁信息表达模型GB/T 36643-2018



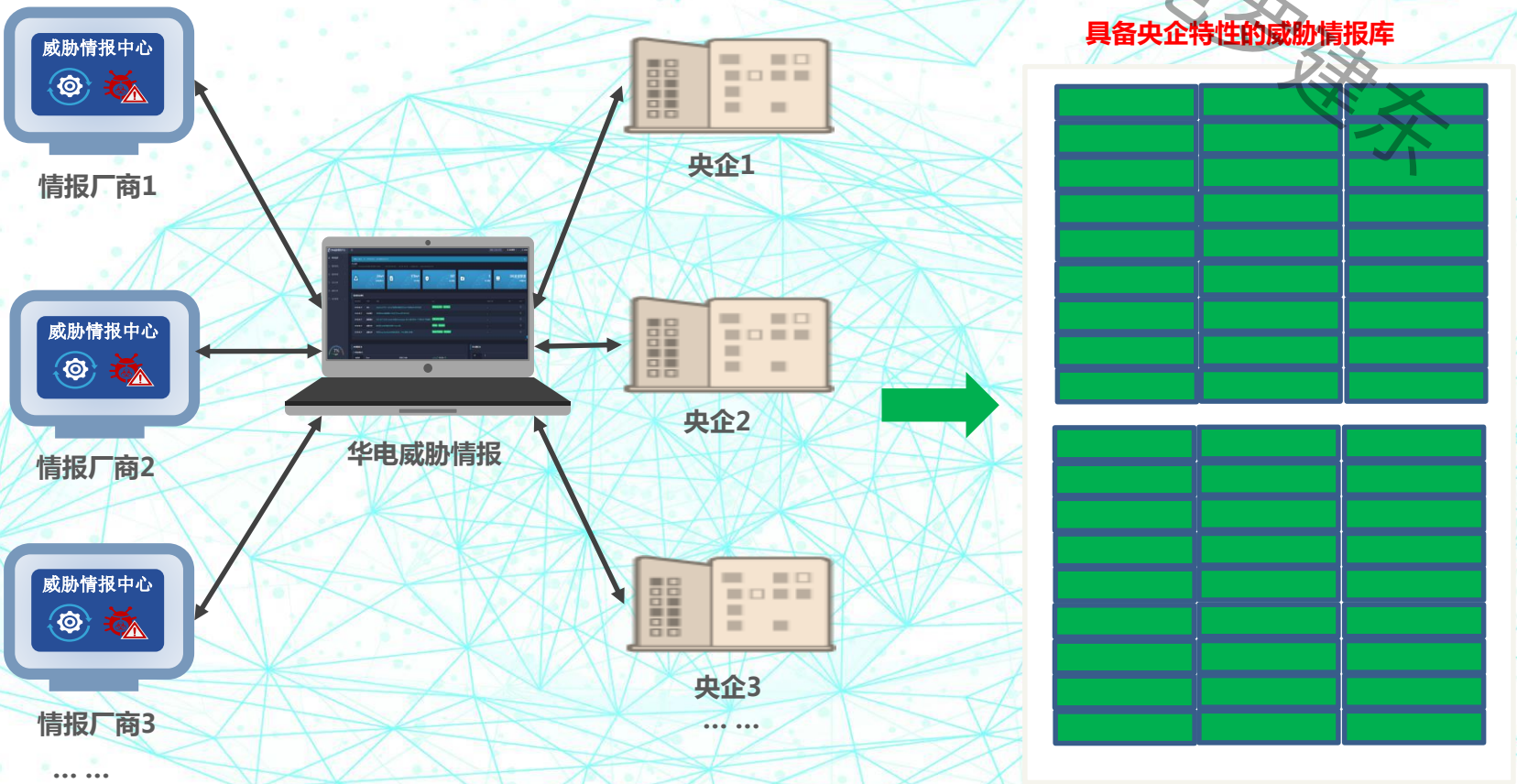
威胁情报需要整合



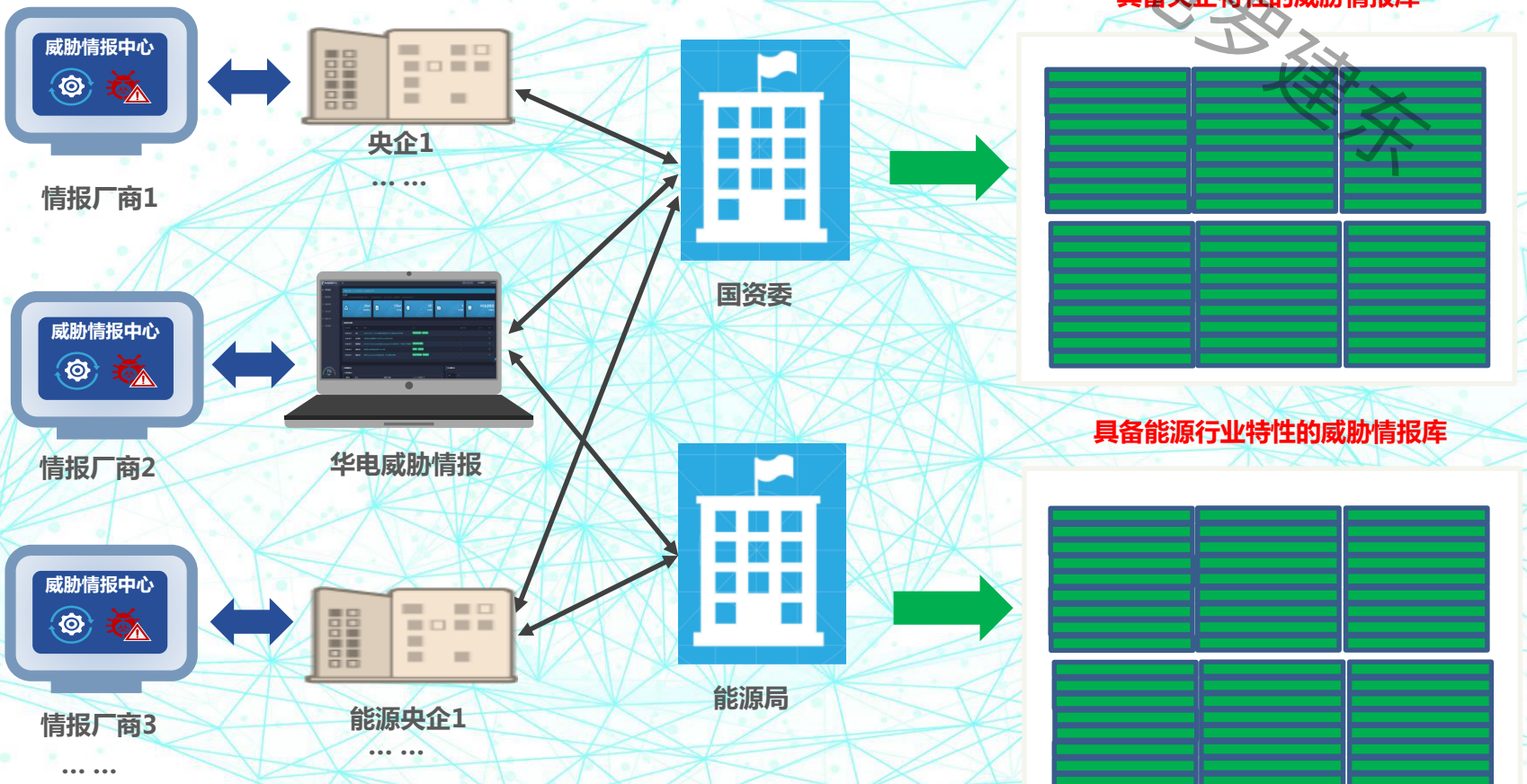
威胁情报需要合作



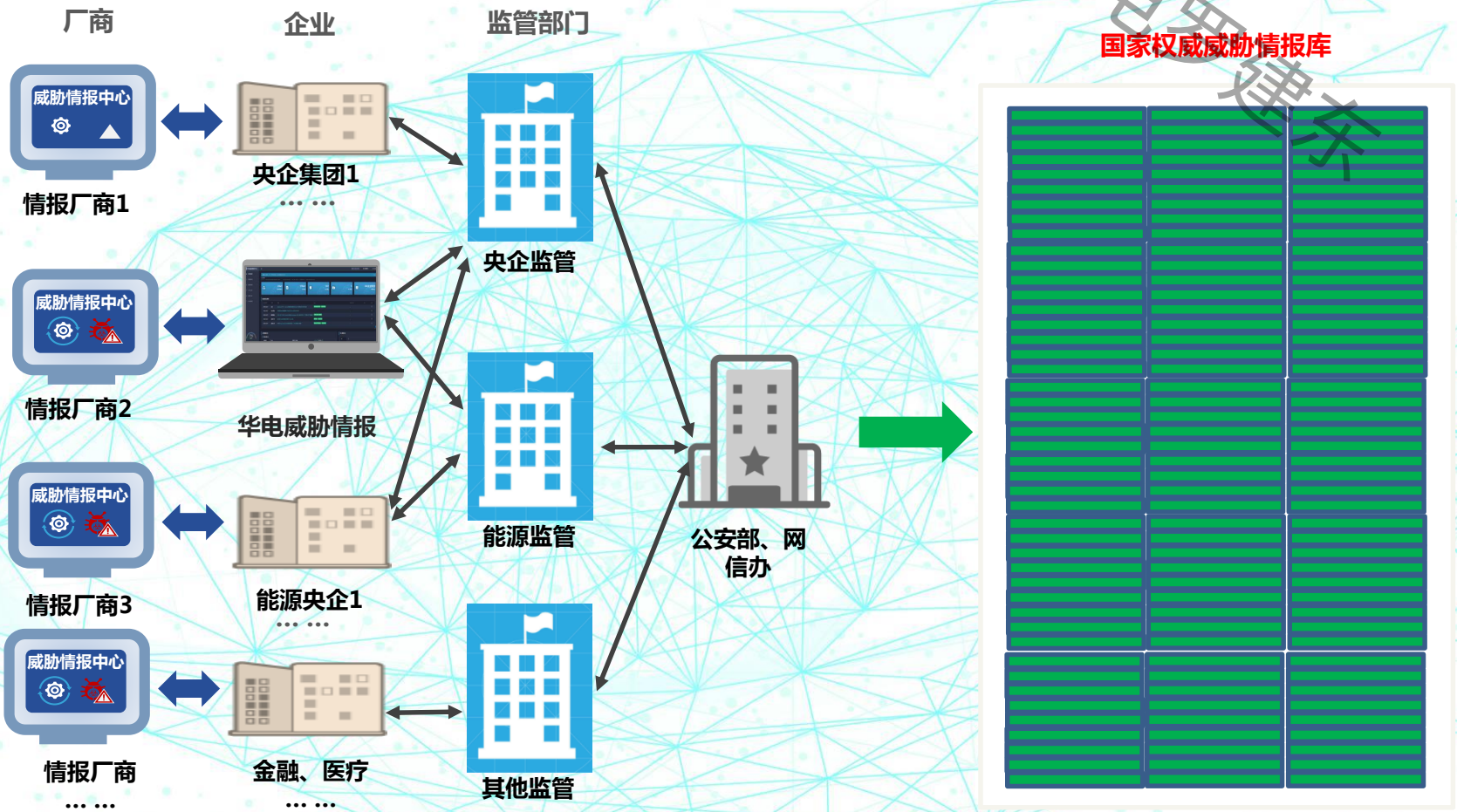
威胁情报需要更为广泛的合作



威胁情报需要更为广泛的合作



威胁情报需要更为广泛的合作



推动情报共享的建议

1. 加快威胁情报的标准化和自动化落地
2. 建立统一的威胁情报平台，汇聚各个主流安全厂商的威胁情报，有偿对外提供服务，并建立情报的评估和反馈机制
3. 情报厂商不一定只做产品卖给最终用户，还可以与安全设备厂商合作，相互赋能，实现情报的共享共用和共赢
4. 威胁情报能否按照行业、地域等特征进行细分，使得情报更加有的放矢

网络安全永远在路上

威胁情报领域经过几年的探索、积淀和实践，已经洗去浮华，正在企业的网络安全体系和应急响应中逐渐发挥出真正的价值。中国华电愿意与各个有意愿、有能力的用户企业、安全厂商、安全联盟携手合作，共同推动威胁情报在企业、在行业、乃至在国内的共享共用，为筑牢企业、行业乃至国家网络安全防线贡献力量。


THANK YOU
谢谢