信息安全从运维到运营

吕毅

中国人民银行金融信息中心信息安全部副主任

ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原“中国互联网安全大会”）

现状

运维到运营

注意事项

现状1.埋头拉车和选择性忽视

低头拉车VS抬头看路

埋头拉磨 蒙眼狂奔 抬头看路 逐渐提升

风险：

没出事儿时候你没什么大用

出事儿了证明你真没什么大用

信任：

既然你只能干这个

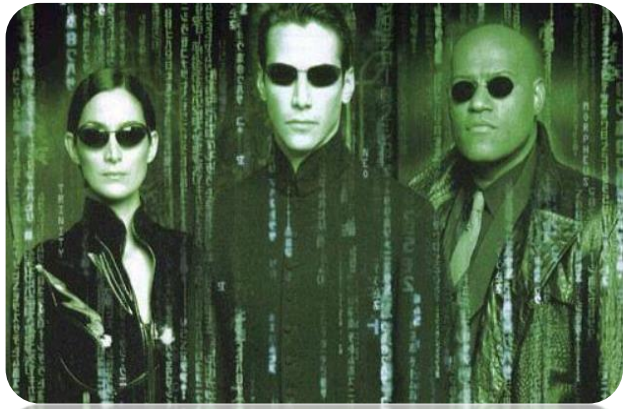
你就继续干这个

现状2.安全协同效应

无法协同的安全=孤军奋战

现状3.理想丰满，现实骨感

理想中的我们



VS

实际的我

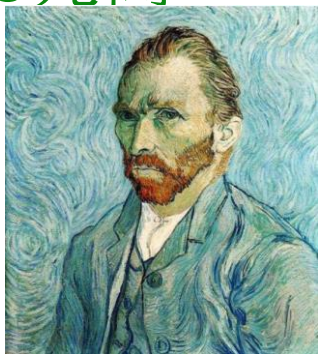
理想中的黑客

VS

实际的黑客

现状4.安全价值的认可

宋徽宗VS梵高



运维 VS 运营

现状

运维到运营

注意事项

活着→活得好 从运维到运营（从ITOM和Gartner启发）

运维

被动维持	主动经营
基础设施	业务用户
稳定可靠	体验效益
监管控	数据态势
保值	保值增值
自行车	汽车

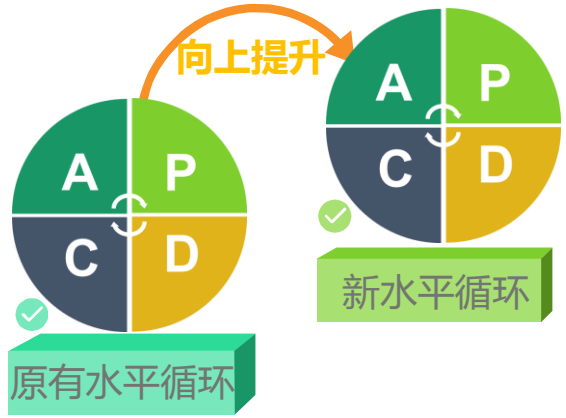
运营

ZERO TRUST SECURITY

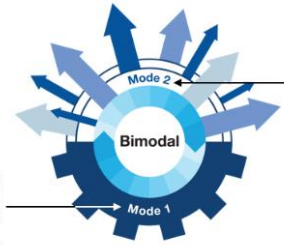
参考陈傲寒《IT：从运维到运营》

安全运营PDCA模型及Bimodal

从运维到运营



Bimodal is the practice of managing two separate but coherent styles of work — one focused on predictability and the other on exploration.



Mode 2 is exploratory, experimenting to solve new problems.

Mode 1 is predictable, improving and renovating in more well-understood areas.

运营

ZERO TRUST SECURITY

Gartner I&O Maturity Model

从运维到运营

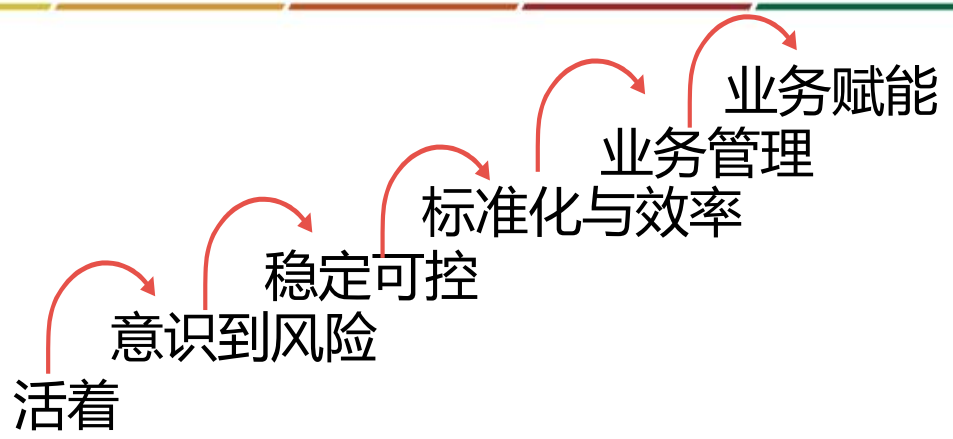


Figure 1. The Components of Gartner's I&O Maturity Model

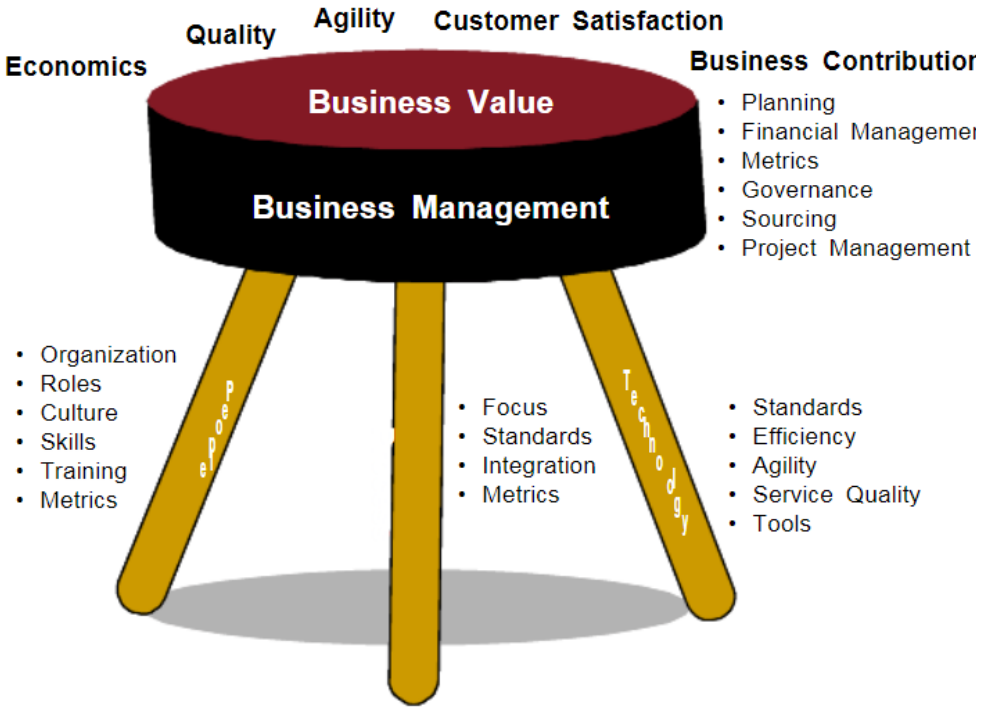


Figure 2. The Levels of Gartner's I&O Maturity Model

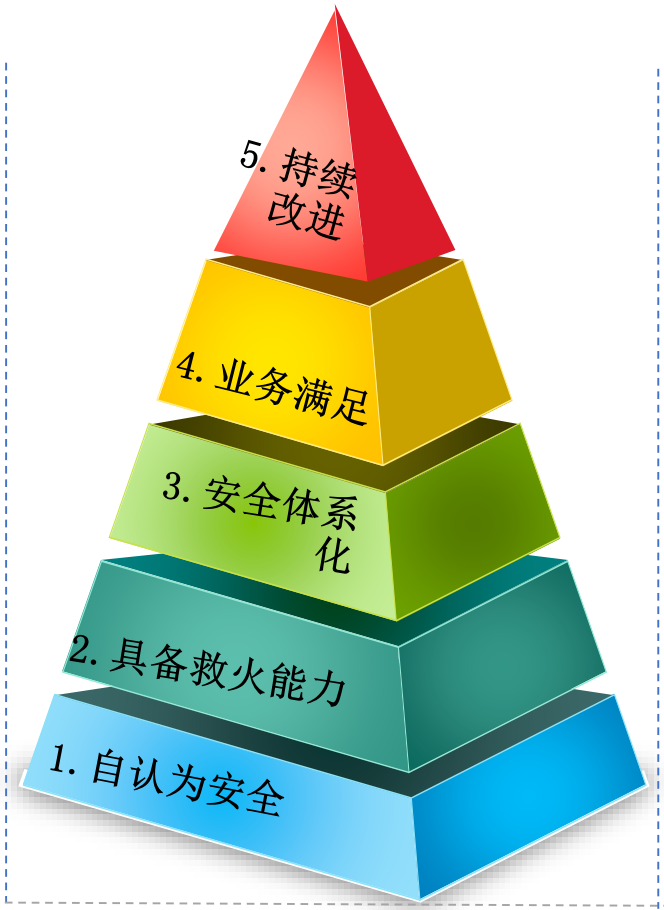
	Survival	Awareness	Committed	Proactive	Service-Aligned	Business Partnership
People 人	No organizational focus on IT infrastructure and operations	Defined, technology-centric organization for IT infrastructure and operations	Technology-centric organization; investment in IT service desk function and staff	Process-centric organization, defined governance structure	Customer- and business-focused, IT service and delivery centric organization, formal governance	Business optimization and entrepreneurial focused culture
Process 流程	No formal IT processes for IT infrastructure and operations	Ad hoc, but aware that processes are necessary; dependent on tools to implement de facto processes	Defined processes for IT service support and project management	Repeatable and individually automated; focus on IT service delivery-related IT processes	Integrated, automated and extended beyond I&O; focus on all service and business management processes	Dynamic optimization of IT services, implement processes fostering business innovation
Technology 技术	No formal strategy or execution on technology investments	Basic management tools; no formal infrastructure hardware or software standards	IT support and project-related management tools; desktop hardware/ software standards defined; begin infrastructure standardization/ rationalization	Formal infrastructure standards and policies; process and domain-centric management tools; virtualization foundation in place	Formal IT management process/tools architecture; shared services; aggregated capacity management	Proactively promoting new technologies and impact to business; real-time infrastructure
Business Management 管理	No formal IT business management functions	Very little outside of budgeting	Project management office	Financial management, formal key performance indicators	IT service cost metrics, competitiveness	Business contribution metrics
Level:	0	1	2	3	4	5

Source: Gartner (October 2007)

成熟度模型

从运维到运营

实现	优化级	震慑	天网级	运营
情感	可管理	情报	智能级	
社交	已定义	主动	自动化级	
安全	可重复	被动	基础级	运维
生理	初始	架构	自发级	

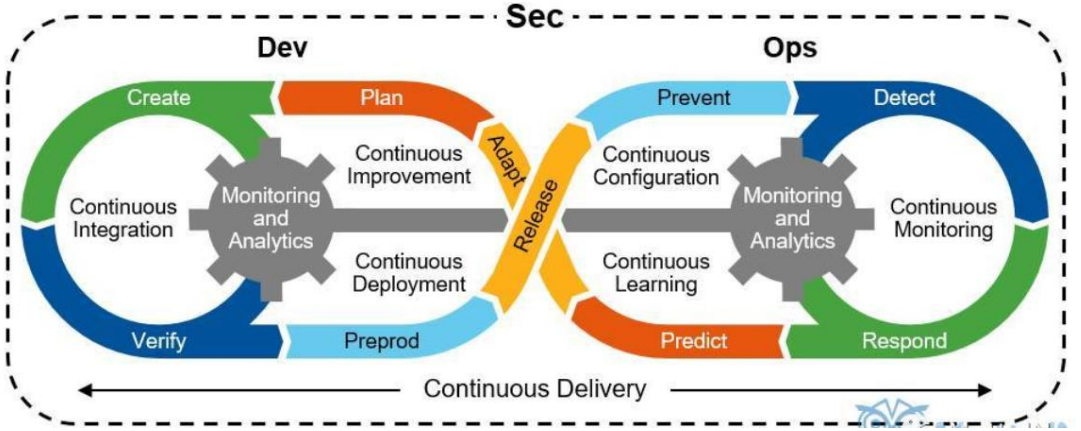


马斯洛	CMM	SANS	赵彦	聂君
1954	1991	2015	2016	2016

甲方安全运营模式

从运维到运营

范围经济 对抗复杂性



Gartner

Adaptive SecurityArchitecture

ZERO TRUST SECURITY

乙方安全运营模式

从运维到运营

乙方安全运营

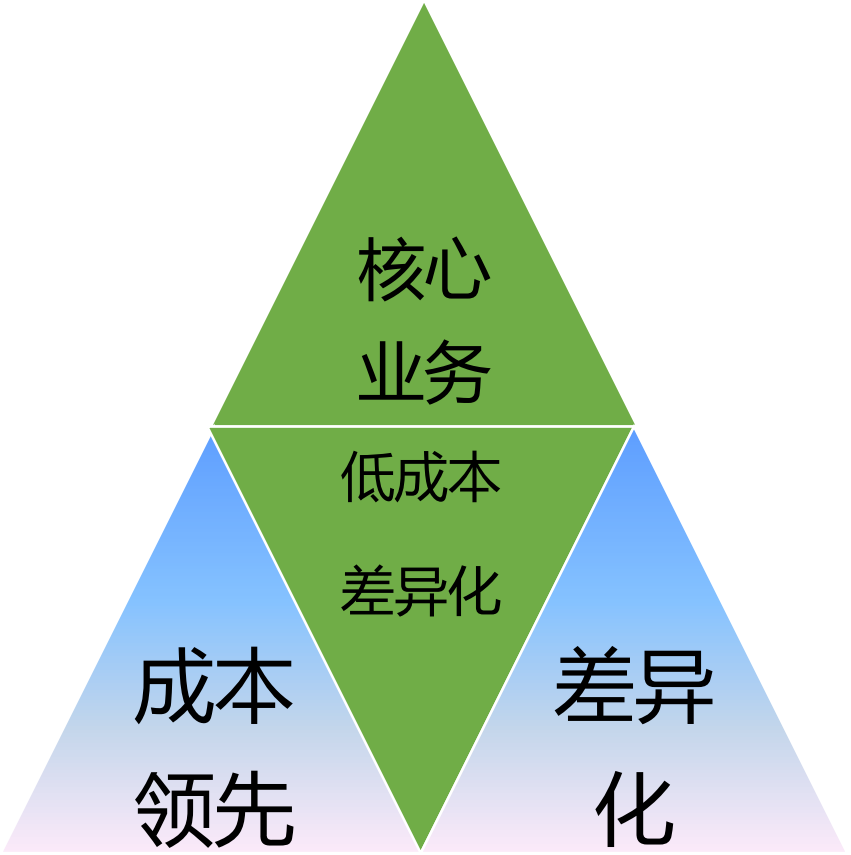
平台

＋

资本

＋

服务



创新优势（熊彼特）

海底捞服务

ZERO TRUST SECURITY

近几十年来全球科技创新的一个突出特征是“科技创新始于技术，成于资本”

互联网安全运营模式

从运维到运营

大型互联网企业安全建设

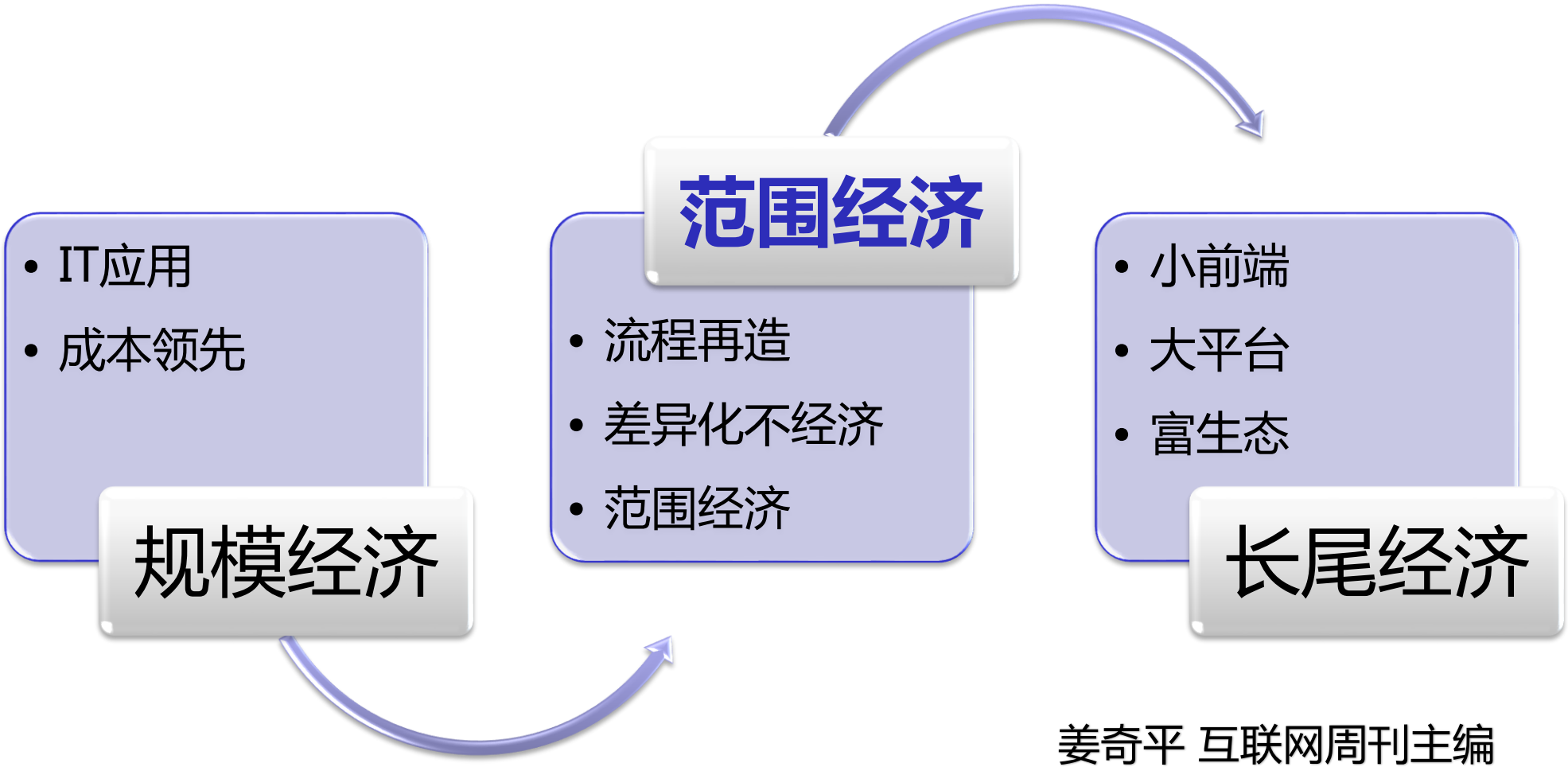
规模经济 平台优势

		完全竞争	垄断竞争	结合状态
实践		平台 （大规模分享）	APP （定制分成）	平台+APP （大规模定制）
理论范式		无差异 同质性，Q	差异 异质性，N	复杂性范式 网络，图
资源配置理论（新古典）	均衡点	P=MC	P=AC	AC-MC（广义均衡）
	理论方法	边际方法	平均方法	新综合
	利润	零利润	正利润	双层经营
	市场结构	垄断（竞争）	竞争（“垄断”）	新垄断竞争
	竞争战略	成本领先 （降价竞争）	差异化 （提价竞争）	低成本差异化 （免费赚钱）
利益相互作用理论（古典）	产权	拥有	使用	两权分离 （云：XaaS）
	交易费用	0	正值（租）	差异租：AC-MC
	租值	耗散	集聚	分成

姜奇平 互联网周刊主编

互联网安全运营增值

从运维到运营



姜奇平 互联网周刊主编

运维 VS 运营

现状

运维到运营

注意事项

几个陷阱---从运维到运营

陷阱一：采取集中化规划与执行方式　　安全运营中，事务可以外包，但责任不可以外包

陷阱二：将安全运营中心的任务与责任外包出去

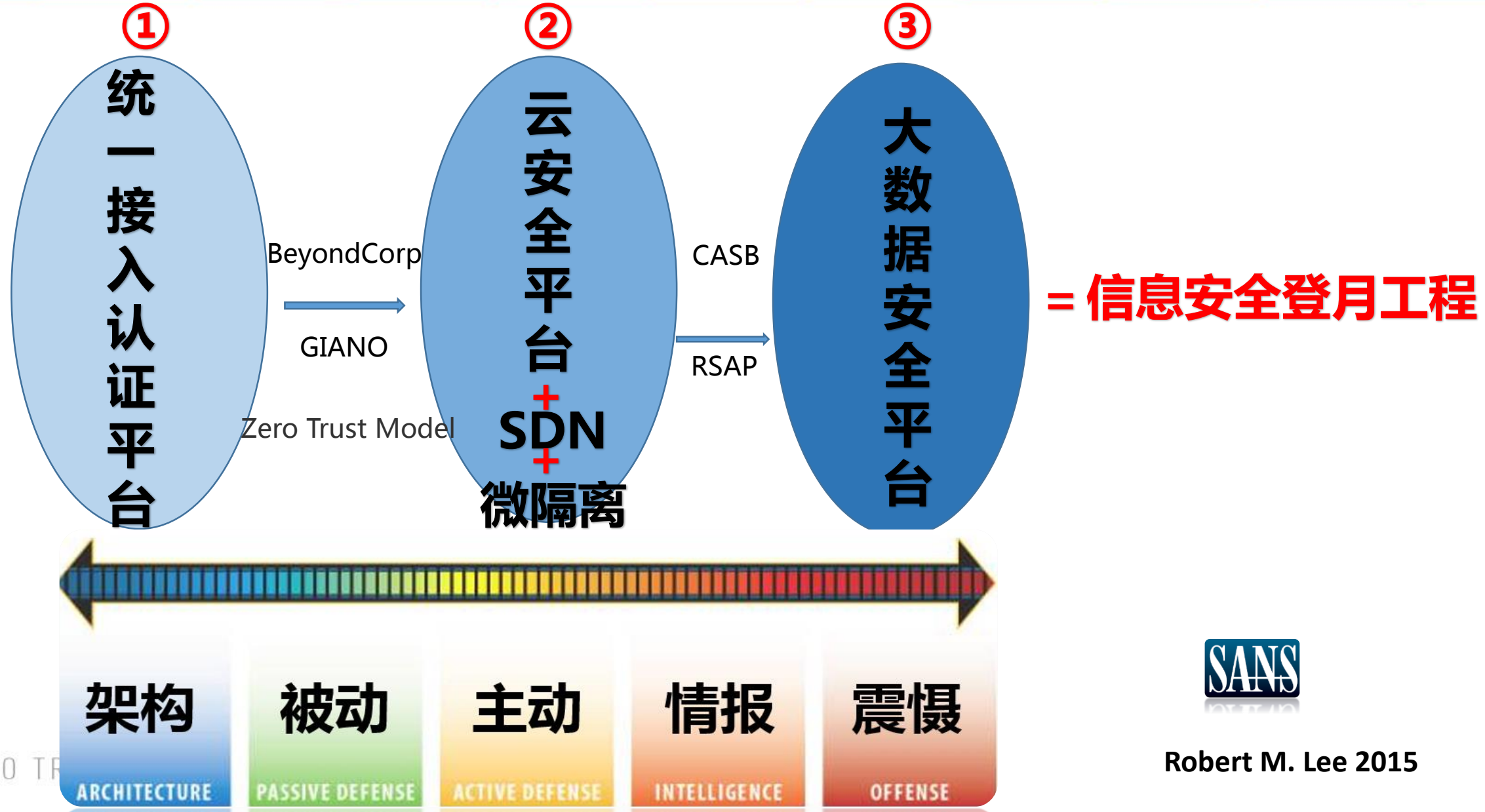
陷阱三：坚信单靠技术本身已经足以提供有效的安全保障

陷阱四：把事件管理与问题管理混为一谈

陷阱五：对一切对象加以保护(在多数情况下，保护一切意味着毫无保护)

来源：前任美国陆军网络司令部安全运营中心

安全运营基础设施---从运维到运营



安全运营价值体系---从运维到运营

高尔定律（Gall’s Law）：任何一个成功的复杂系统永远源于一个成功的简单系统

价值源自信息系统（OF）
运行服务信息系统（BY）
为业务保值和增值 (FOR)

内因：风险防御能力 RISK

外因：信任感 TRUST

CARTA, Continuous Adaptive Risk and Trust Assessment

持续自适应风险与信任评估战略 Gartner

安全运营目标---从运维到运营

从农业经济到工业经济到范式转移信息经济的

简单性范式（同质化假定）向复杂性范式（个性化、多样化现实）

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原“中国互联网安全大会”）

吕毅 18510331933