FREEBUF | 企业安全 俱乐部

等保2.0的实践之旅

何斌第 携程安全合规团队负责人

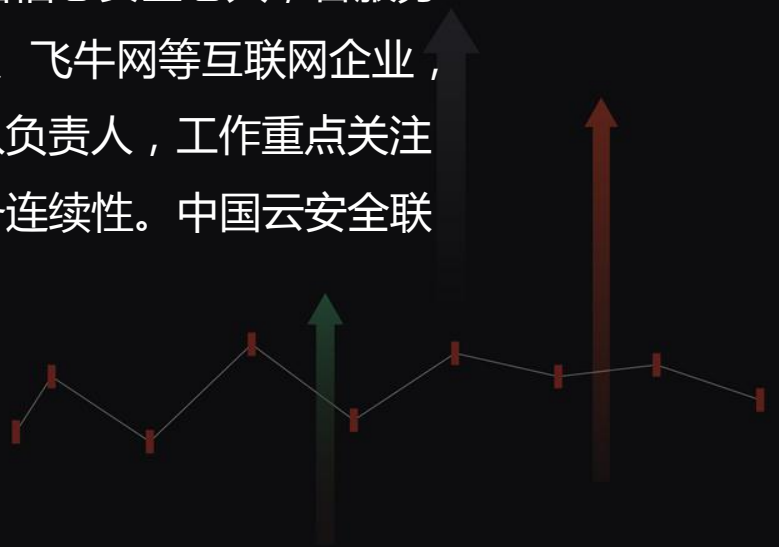
2019企业安全俱乐部 等保专场

等保2.0的实践之旅

个人简介

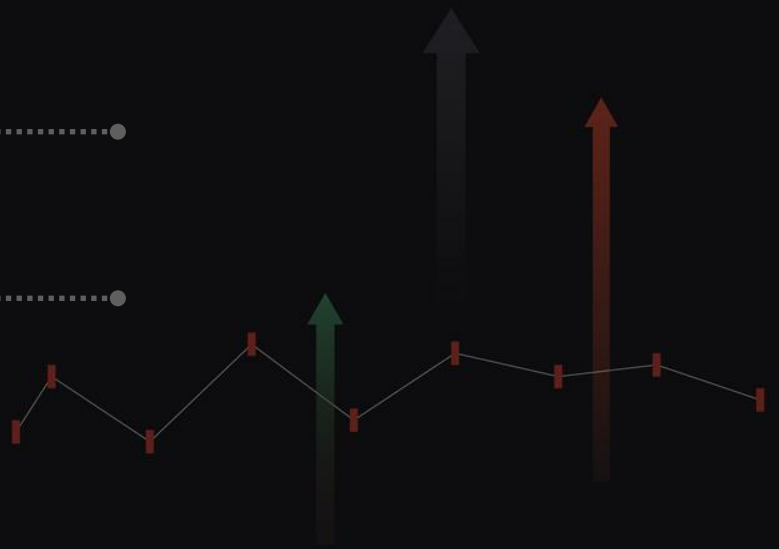
网络ID：上海de老五

工作经历：从事信息安全工作超过15年的一名信息安全老兵，曾服务于中科网威、天融信等乙方安全公司和1号店、飞牛网等互联网企业，现在担任携程旅行网信息安全部安全合规团队负责人，工作重点关注领域是隐私保护、云计算等新技术合规和业务连续性。中国云安全联盟（C-CSA）专家组成员。



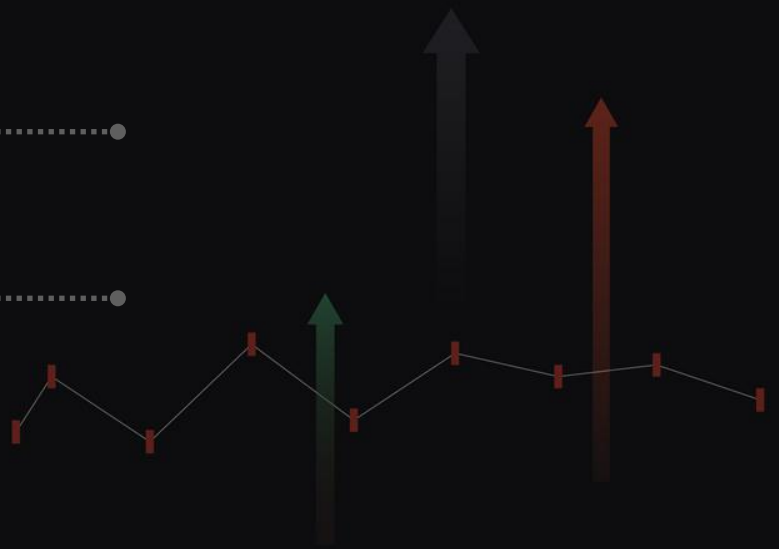
等保2.0的实践之旅

1. 等保的发展历程
2. 等保2.0的主要变化
3. 携程的等保2.0实践
4. 践行等保2.0的疑惑



等保2.0的实践之旅

1. 等保的发展历程
2. 等保2.0的主要变化
3. 携程的等保2.0实践
4. 践行等保2.0的疑惑



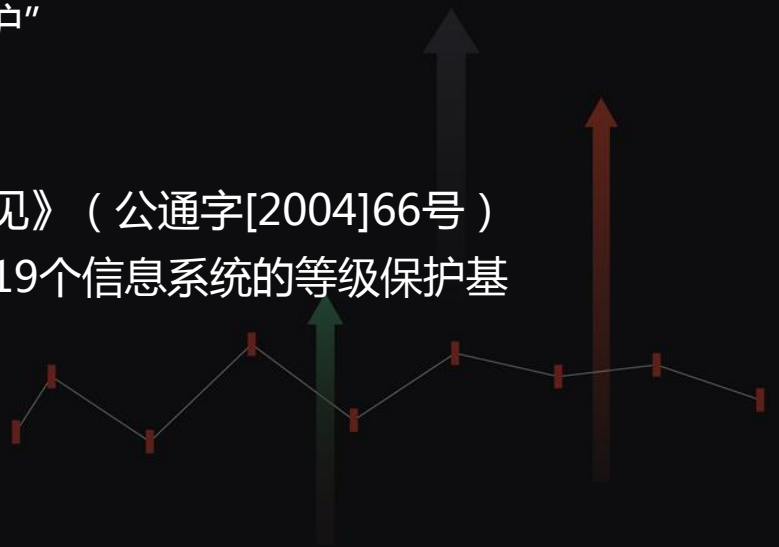
等保2.0的实践之旅

政策准备期（1994-2003）

- 1994年，《中华人民共和国计算机信息系统安全保护条例》规定计算机信息系统实行安全等级保护
- 2003年，《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）明确指出“实行信息安全等级保护”

规模试点期（2004-2006）

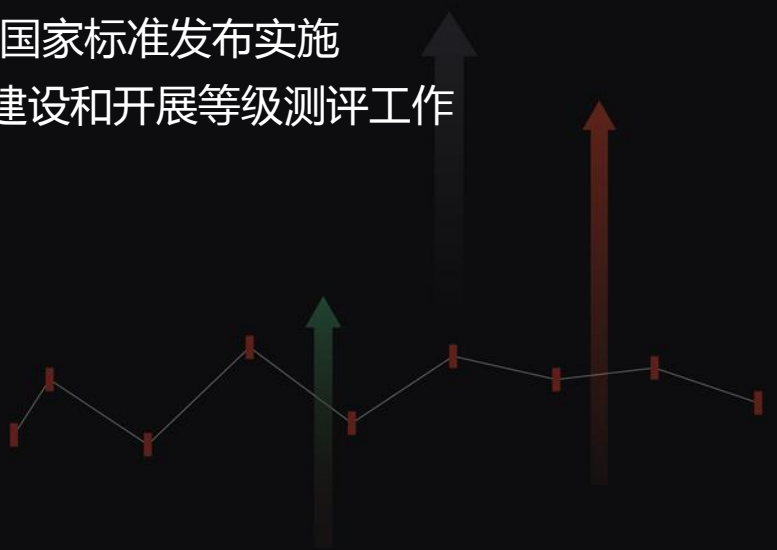
- 2004年，《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）
- 2004-2006年，开展涉及65117家单位，共115319个信息系统的等级保护基础调查和等级保护试点工作



等保2.0的实践之旅

等保1.0时代（2007-2016）

- 2007年，《信息安全等级保护管理办法》（公通字[2007]43号）
- 2007年，召开全国重要信息系统安全等级保护定级工作部署专题电视电话会议，标志着信息安全等级保护制度正式开始实施
- 2008年，GB/T 22239-2008和GB/T 25058-2010国家标准发布实施
- 2010年，《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）



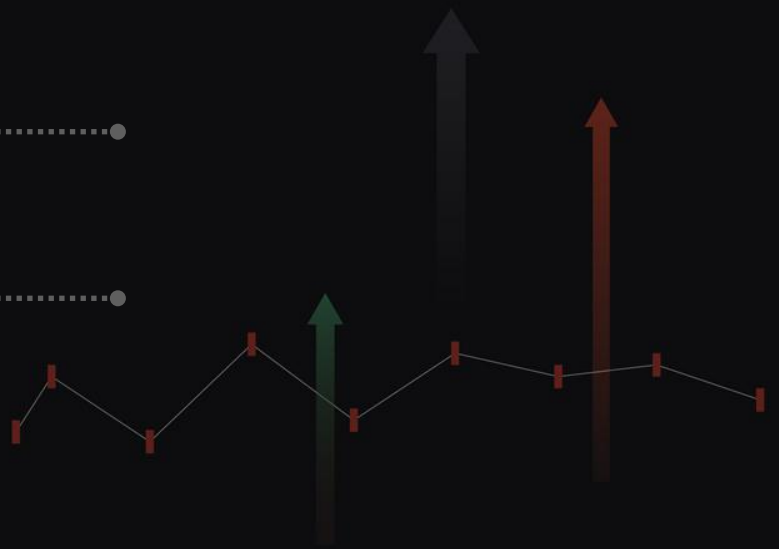
等保2.0的实践之旅

走进新时代（2016-2019）

- 2016年10月10日，第五届全国信息安全等级保护技术大会召开，公安部网络安全保卫局郭启全总工指出“国家对网络安全等级保护制度提出了新的要求，等级保护制度已进入2.0时代”
- 2016年11月7日，《中华人民共和国网络安全法》正式颁布，第二十一条明确“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改……”
- 2019年5月13日，网络安全等级保护基本要求（ GB/T 22239-2019）、网络安全等级保护设计技术要求（ GB/T 25070-2019）和网络安全等级保护测评要求（ GB/T 28448-2019）国家标准发布

等保2.0的实践之旅

1. 等保的发展历程
2. 等保2.0的主要变化
3. 携程的等保2.0实践
4. 践行等保2.0的疑惑



等保2.0的实践之旅

等保2.0的主要标准

- 网络安全等级保护条例（总要求/上位文件）
- 计算机信息系统安全保护等级划分准则（ GB 17859-1999）（上位标准）
- 网络安全等级保护实施指南（ GB/T 25058）（正在修订）
- 网络安全等级保护定级指南（ GB/T 22240）（正在修订）
- 网络安全等级保护基本要求（ GB/T 22239-2019）
- 网络安全等级保护设计技术要求（ GB/T 25070-2019）
- 网络安全等级保护测评要求（ GB/T 28448-2019）
- 网络安全等级保护测评过程指南（ GB/T 28449-2018）

等保2.0的实践之旅

变化一

地位提升——等级保护上升为法律（《网络安全法》第二十一条和第三十一条）

变化二

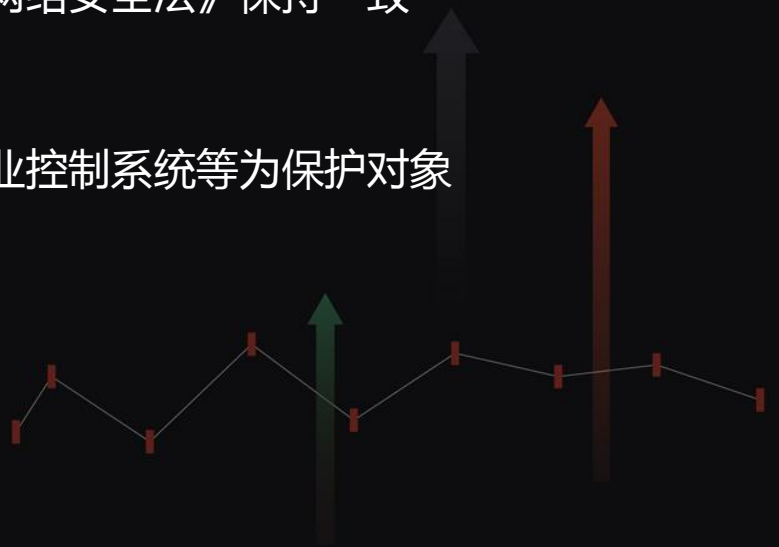
名称变化——变更为“网络安全等级保护”，与《网络安全法》保持一致

变化三

对象变化——增加云计算、移动互联、物联网和工业控制系统等为保护对象

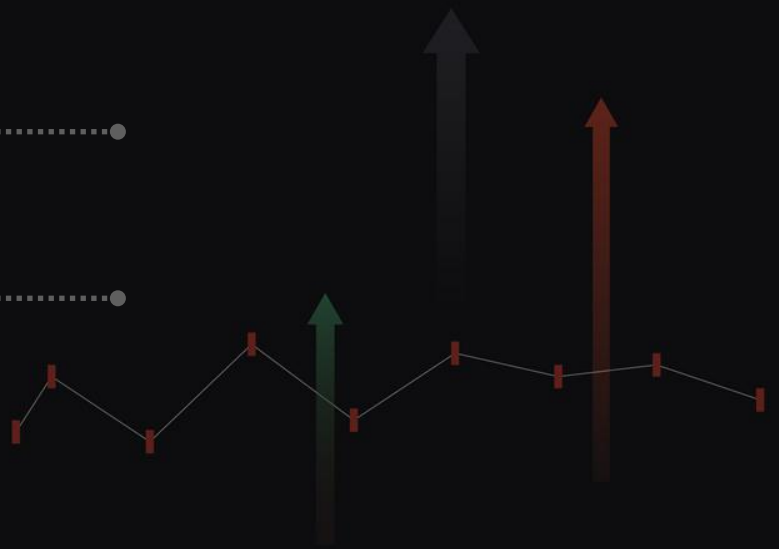
变化四

要求变化——安全通用要求和安全扩展要求



等保2.0的实践之旅

1. 等保的发展历程
2. 等保2.0的主要变化
3. 携程的等保2.0实践
4. 践行等保2.0的疑惑



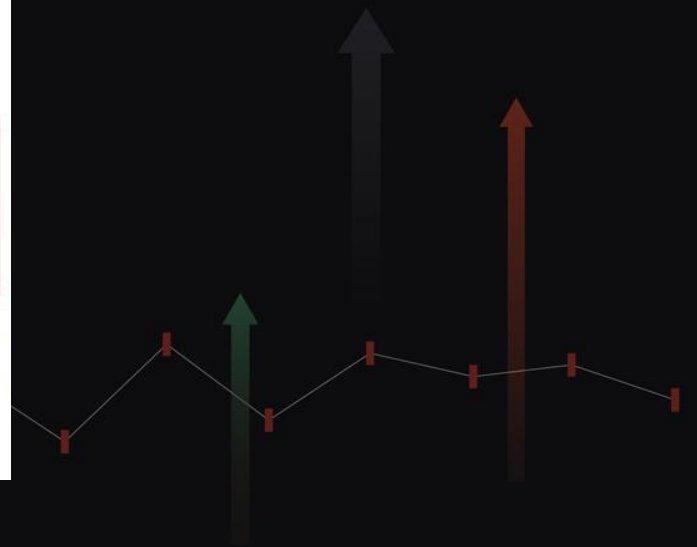
等保2.0的实践之旅

网络安全等级保护条例

（征求意见稿）

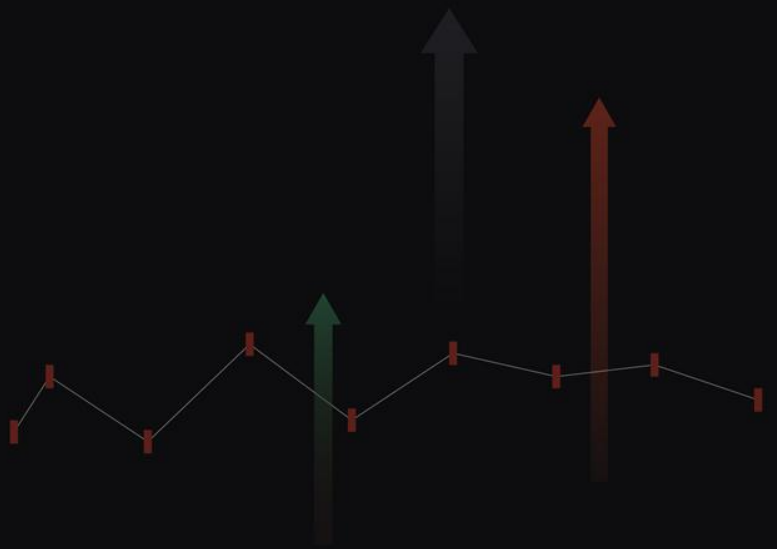
第四十七条【非涉密网络密码保护】非涉密网络应当按照国家密码管理法律法规和标准的要求，使用密码技术、产品和服务。第三级以上网络应当采用密码保护，并使用国家密码管理部门认可的密码技术、产品和服务。

第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。密码应用安全性评估结果应当报受理备案的公安机关和所在地设区市的密码管理部门备案。



等保2.0的实践之旅

- 密码应用安全性评估试点（2018年11月）
- 密码应用安全性评估备案（2019年2月）



等保2.0的实践之旅

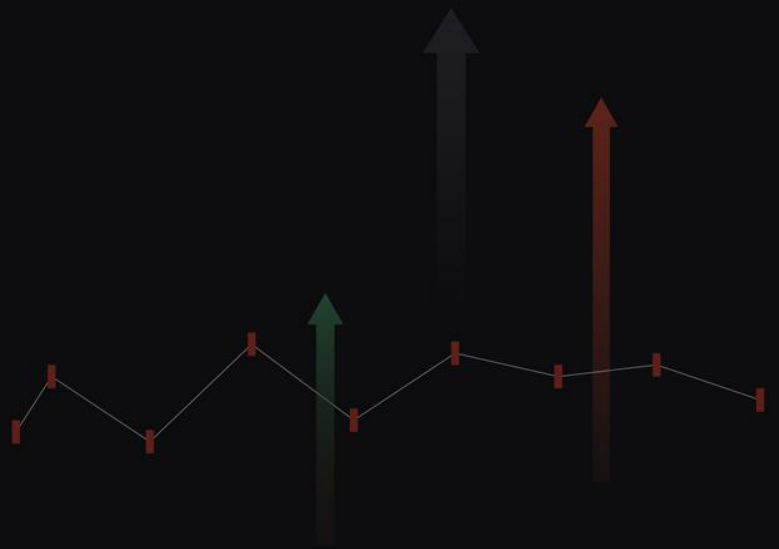
测评准备

- 测评依据
  - 《商用密码应用安全性评估管理办法》
  - 《GM/T 0054 信息系统密码应用基本要求》
  - 《信息系统密码测评要求（试行）》
- 测评内容
  - 总体要求测评包括对信息系统中采用的密码算法、密码技术、密码产品和密码服务的合规性进行测评。
  - 密码应用测评包括对物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个层面的密码应用进行测评。
  - 密钥管理测评包括对信息系统密钥管理全过程进行测评。
  - 安全管理测评包括对信息系统密码应用所涉及的制度、人员、实施和应急等密码应用安全管理过程进行测评。

等保2.0的实践之旅

系统调研

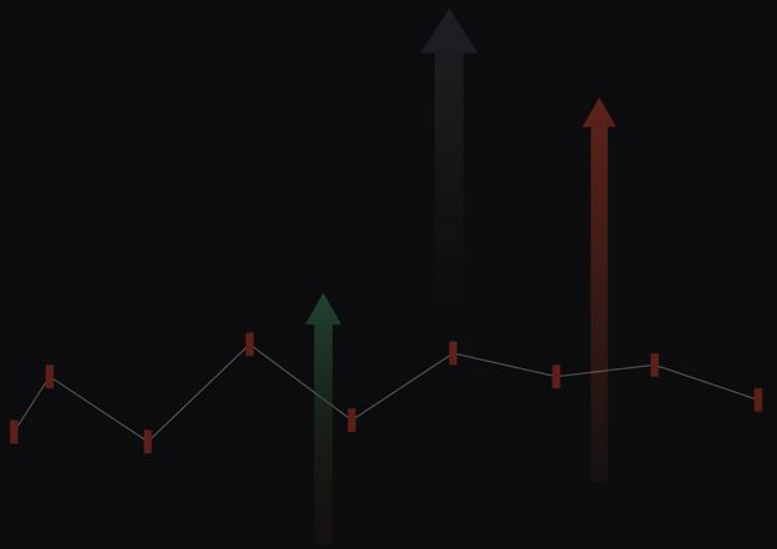
- 《信息系统基本情况调查表》
- 《单位基本情况表》
- 《信息系统密码产品应用情况调查表》



等保2.0的实践之旅

方案编制

- 项目概况
- 被测系统概述
- 密码应用的整体描述
- 测评对象
- 测评指标
- 测评工具
- 测评内容

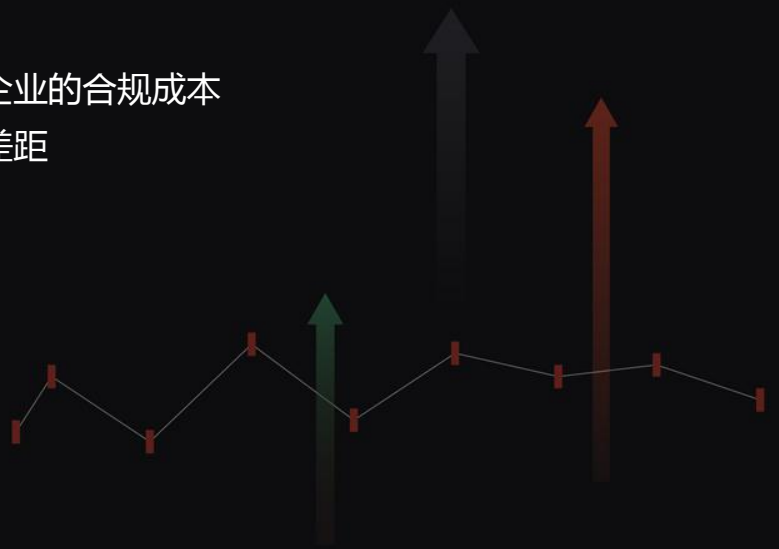


现场测评

物理和环境	1. 身份鉴别	电子门禁系统
	2. 门禁数据完整性	电子门禁系统
	3. 视频数据完整性	视频监控系统
网络和通信	1. 身份鉴别	SSLVPN、SLB、堡垒机
	2. 访问控制信息完整性	SSLVPN、SLB、堡垒机
	3. 通信数据完整性	SSLVPN、SLB
	4. 通信数据机密性	SSLVPN、SLB
	5. 集中管理通道安全	SSLVPN、堡垒机
设备和计算	1. 身份鉴别	WINDOWS SERVER2012、LINUX、加/解密系统、数据库、日志服务器
	2. 设备远程管理鉴别信息机密性	SSLVPN、堡垒机
	3. 访问控制信息完整性。	WINDOWS SERVER2012、LINUX、加/解密系统、数据库、日志服务器
	4. 敏感标记完整性。	WINDOWS SERVER2012、LINUX、数据库（无敏感标记）
	5. 设备重要文件完整性。	WINDOWS SERVER2012、LINUX
	6. 日志记录完整性	WINDOWS SERVER2012、LINUX、加/解密系统、数据库、日志服务器
应用和数据	1. 身份鉴别	注册/登录系统、个人中心、订单查询系统
	2. 访问控制信息和敏感标记完整性	注册/登录系统、个人中心、订单查询系统
	3. 数据传输机密性	无（复用网络层检测）
	4. 数据存储机密性	注册/登录系统、个人中心、订单查询系统、数据库
	5. 数据传输完整性	无（复用网络层检测）
	6. 数据存储完整性	注册/登录系统、个人中心、订单查询系统、数据库
	7. 日志记录完整性	日志服务器
	8. 重要应用程序的加载和卸载	不适用。

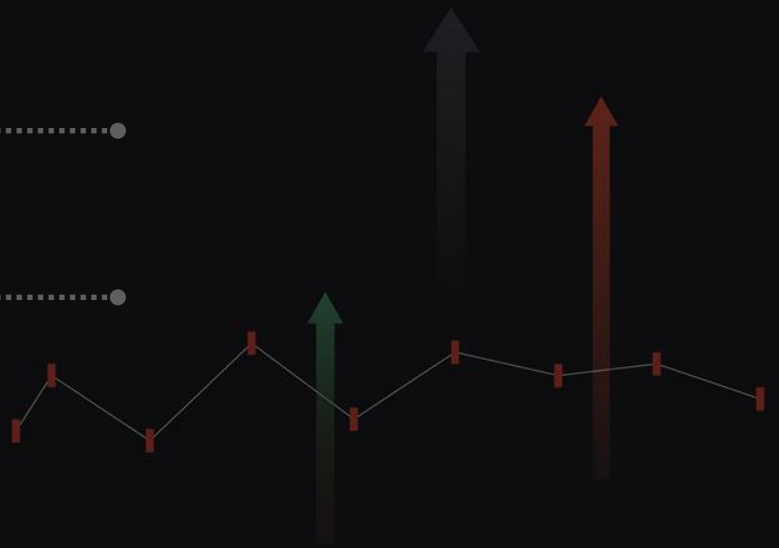
试点成果

- 主要问题
  - 数据完整性问题
  - 密码算法非商密算法
- 试点体会
  - 密码应用安全性评估如果具有一票否决权则会大大增加企业的合规成本
  - 测评依据的标准要求与互联网企业的实际情况存在较大差距



等保2.0的实践之旅

1. 等保的发展历程
2. 等保2.0的主要变化
3. 携程的等保2.0实践
4. 践行等保2.0的疑惑



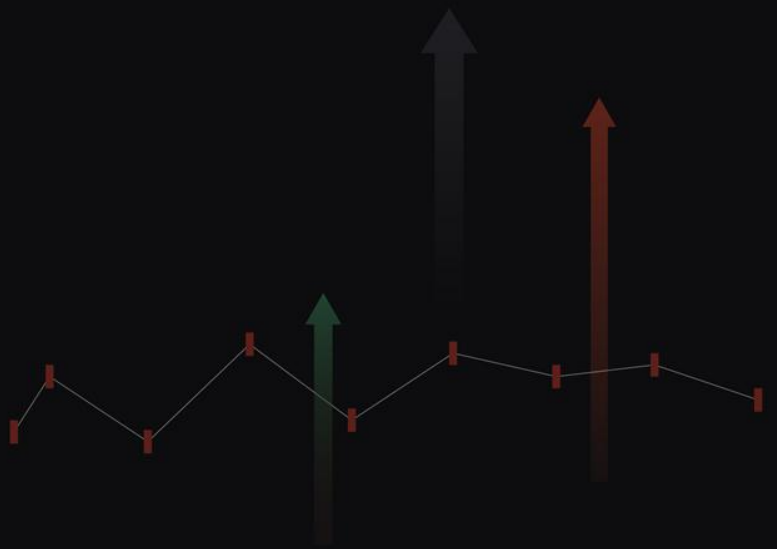
等保2.0的实践之旅

疑惑一

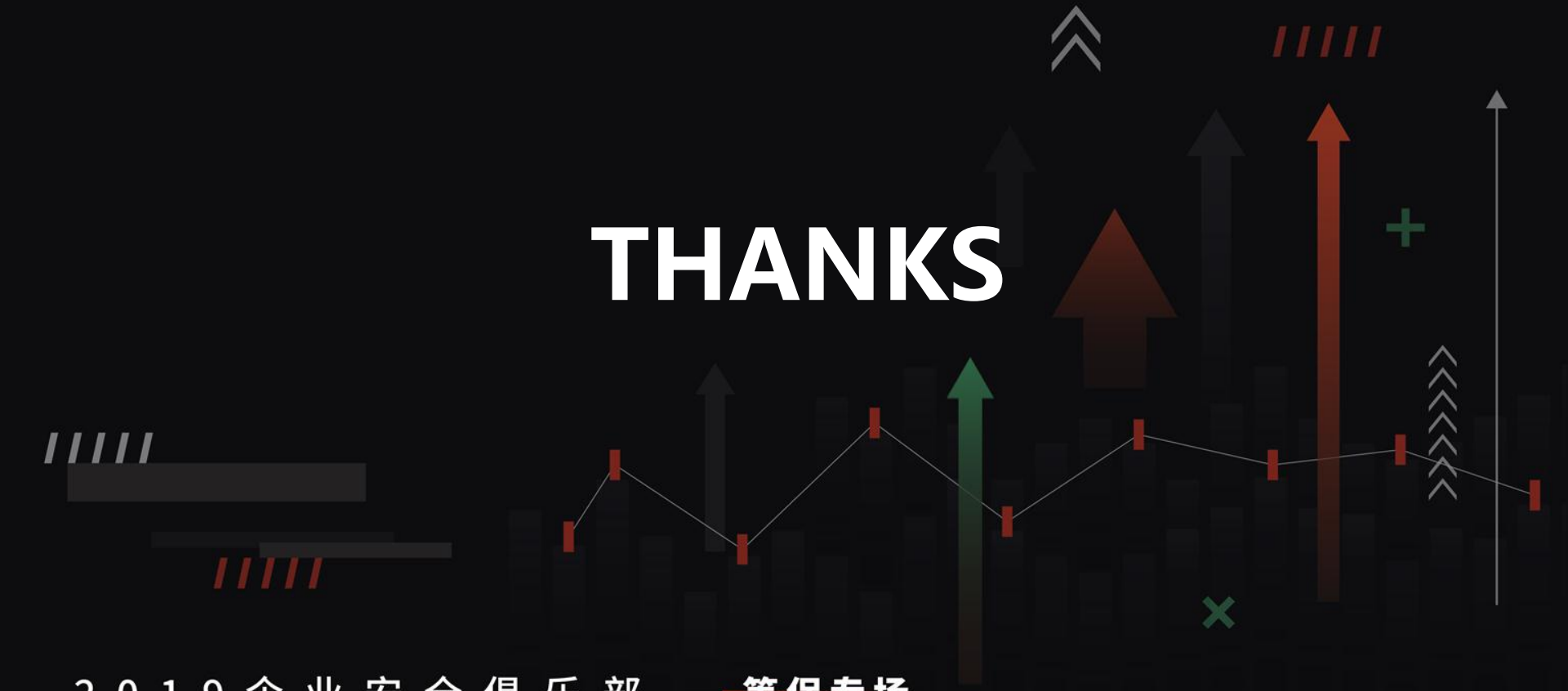
报批稿中的大数据扩展安全要求为何在等保2.0正式标准中被放到附录H？

疑惑二

可信计算在等保2.0中如何实践落地？



FREEBUF | 企业安全 俱乐部



2019企业安全俱乐部 等保专场