等保2.0时代
保险行业信息安全趋势

中科软科技股份有限公司 李鑫

中科软科技

- 中国科学院软件所实施的知识创新试点工程
- 注册资金4.24亿元，目前拥有17000多名员工
- 致力于软件开发、系统集成等领域，涵盖国内众多行业

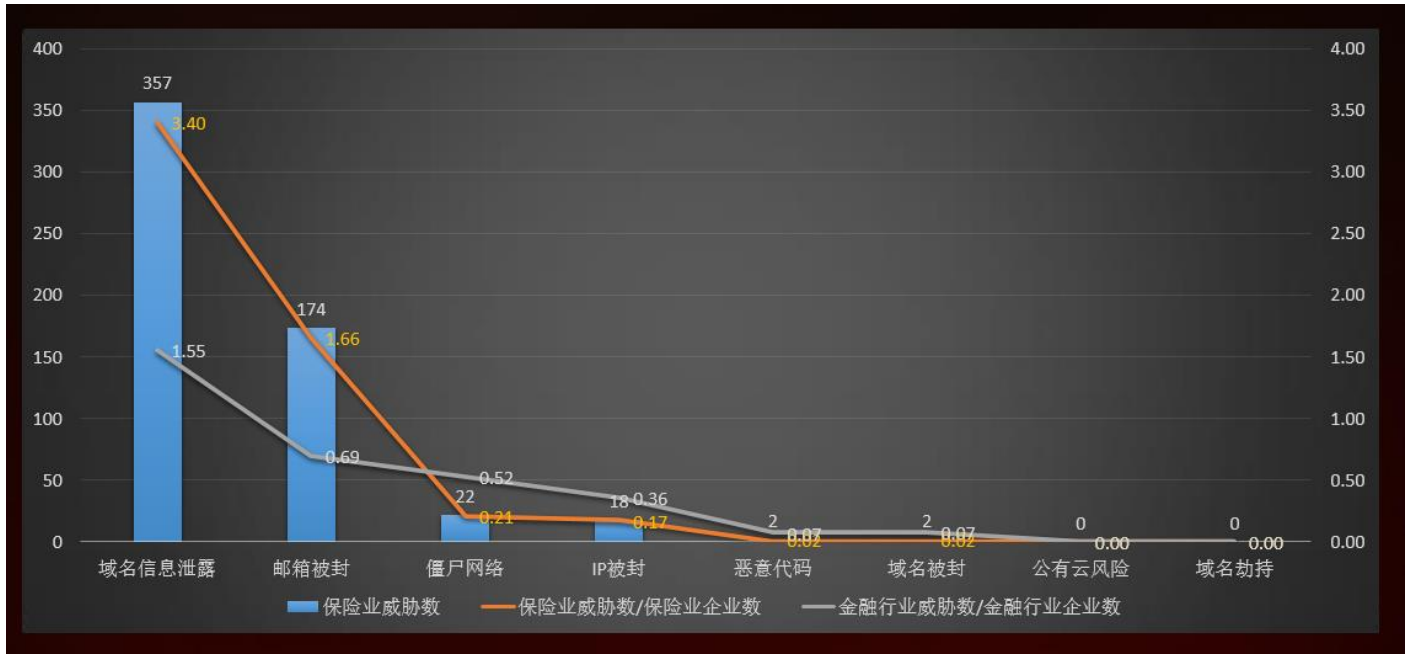
主要股东

- 中科院软件研究所
- 海淀国资委
- ……

目录

Sinosoft

保险行业安全问题-外部威胁

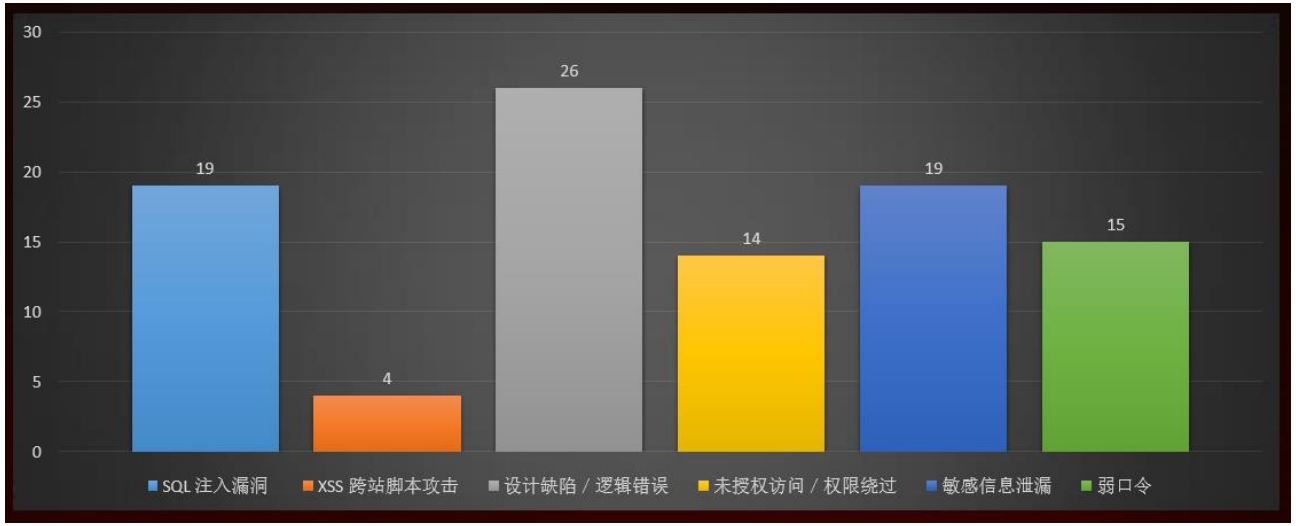


外部威胁调研8类威胁指标中发现最多的3个问题依次是

- 域名信息泄 露
- 僵尸网络
- IP被封

Sinosoft

保险行业安全问题-安全漏洞情况



保险行业的漏洞数量最多的三类漏洞依次是

- 设计缺陷 / 逻辑错误
- SQL 注入漏洞
- 敏感 信息泄漏

Sinosoft

保险行业安全问题-信息安全内部管控现状

- 信息泄露、业务欺诈是互联网金融最关注的风险。
- 导致安全问题的因素。
  - ✓ 投入不足
  - ✓ 人员缺乏
  - ✓ 安全意识薄弱
  - ✓ 制度流程不规范
  - ✓ 安全需求 不明确
- 新技术：大数据和威胁情报技术是比较受关注的信息安全技术。

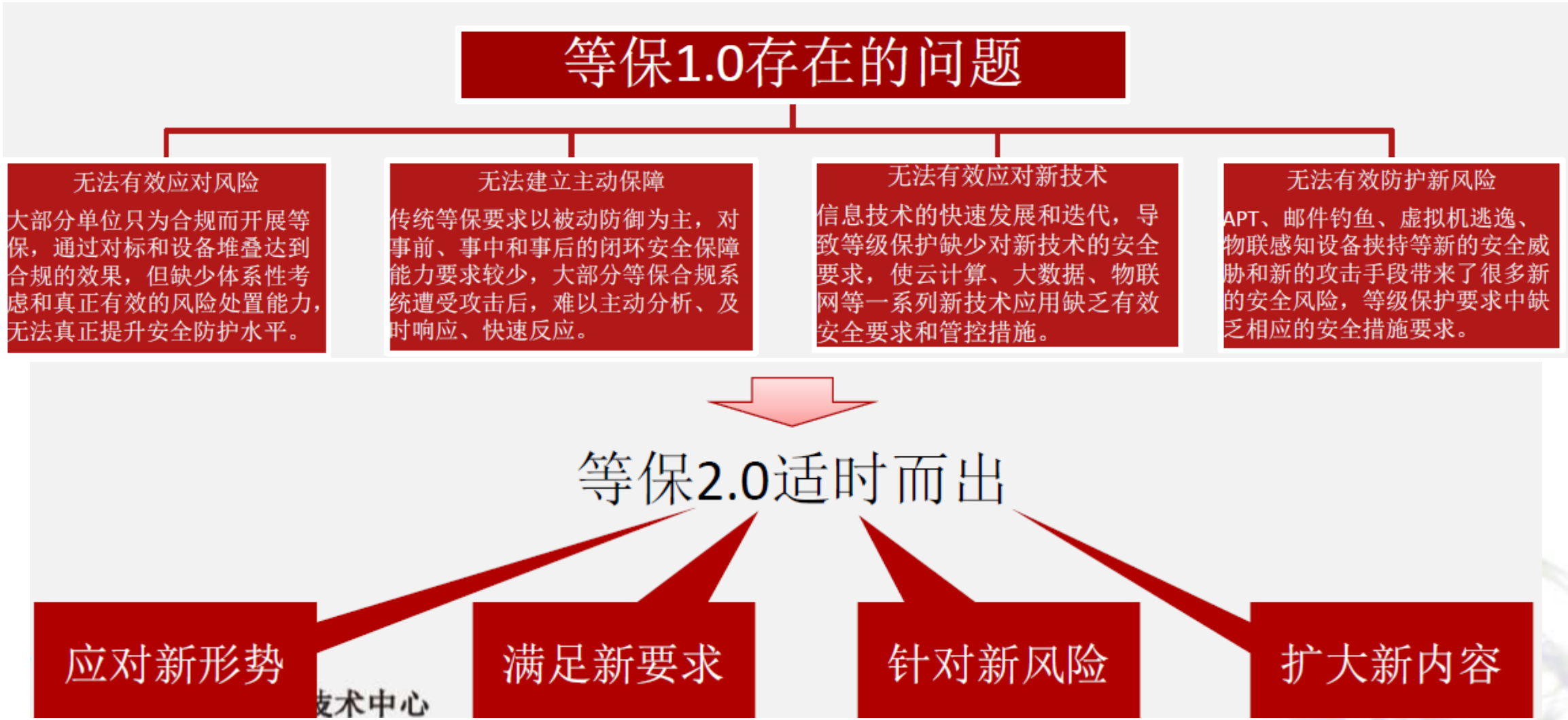
保险行业安全问题-信息安全管控趋势

- 监管政策的完善会促进互联网金融行业整体信息安全现状的提升
- 各保险公司建立和完善信息安全管理体系将会变得越来越重要
  重系统建设→重运维管理
- 行业成熟度的提升将促进对安全投入的增加
- 安全岗位人员需求继续旺盛
- 防数据泄露、防业务欺诈将继续成为安全管控的重点内容
- 大数据在安全领域的应用将会越来越普遍-新技术

目录

Sinosoft

等保1.0向2.0发展的背景



等级保护2.0安全体系的变化

Sinosoft

	等保1.0	等保2.0
测评周期	第三级系统每年一次 第四级系统每半年一次	第三级以上系统每年一次
测评结果	60分以上基本符合	优良中差，70-80中

2.0标准的变化

1.对象范围扩大：新标准将云计算、移动互联、物联网、工业控制系统等列入标准范围，构成了“安全通用要求+新型应用安全扩展要求”的要求内容

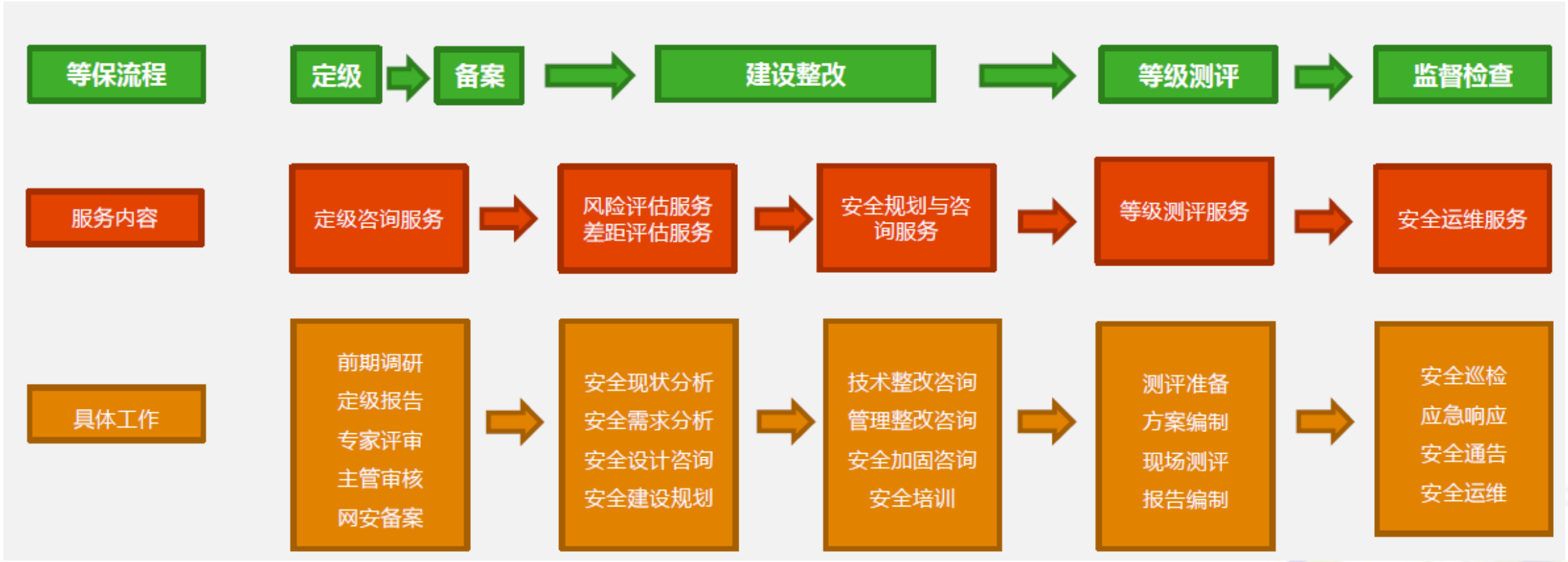
2. 分类结构统一：新标准“基本要求、设计要求和测评要求” 分类框架统一， 形成了“安全通信网络” 、“安全区域边界” 、“安全计算环境”和“安全管理中心” 支持下的三重防护体系架构

3. 强化可信计算：新标准强化了可信计算技术使用的要求，把可信验证列入各个级别并逐级提出各个环节的主要可信验证要求

4. 名称变化：网络安全

5. 对密码、个人信息保护、内部防护、审计的重视

等保项目实施流程



Sinosoft

目录

Sinosoft

保险等保建设主要差距技术点

- 数据库安全审计
- 存储保密性
- 传输过程保密性
- 异地备份
- 日志审计

数据库安全审计

等保要求

应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

解决方案

增加数据库安全审计流量镜像旁挂方式，或者堡垒机，进行对管理用户行为的审计，降低风险级别；

存储保密性

等保要求

应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

解决方案

确认敏感数据范围，可用软件应用层实现加密服务、数据库加密、机密机等方式进行加密处理，如果技术实施难度较大，可采取区域隔离、部署数据库安全审计等降低风险。

传输过程保密性

等保要求

应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

解决方案

系统采用HTTPS，运维管理使用SSH、堡垒机、VPN等技术措施

异地备份

等保要求

应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

解决方案

异地实时备份有难度的话可以考虑实际可接受数据损失程度进行策略配置。

日志审计

等保要求

应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求（一般是180天）。

解决方案

建议增加集中日志审计设备（安全管理中心系统），统一收集各设备的审计数据，进行集中分析。

THANKS