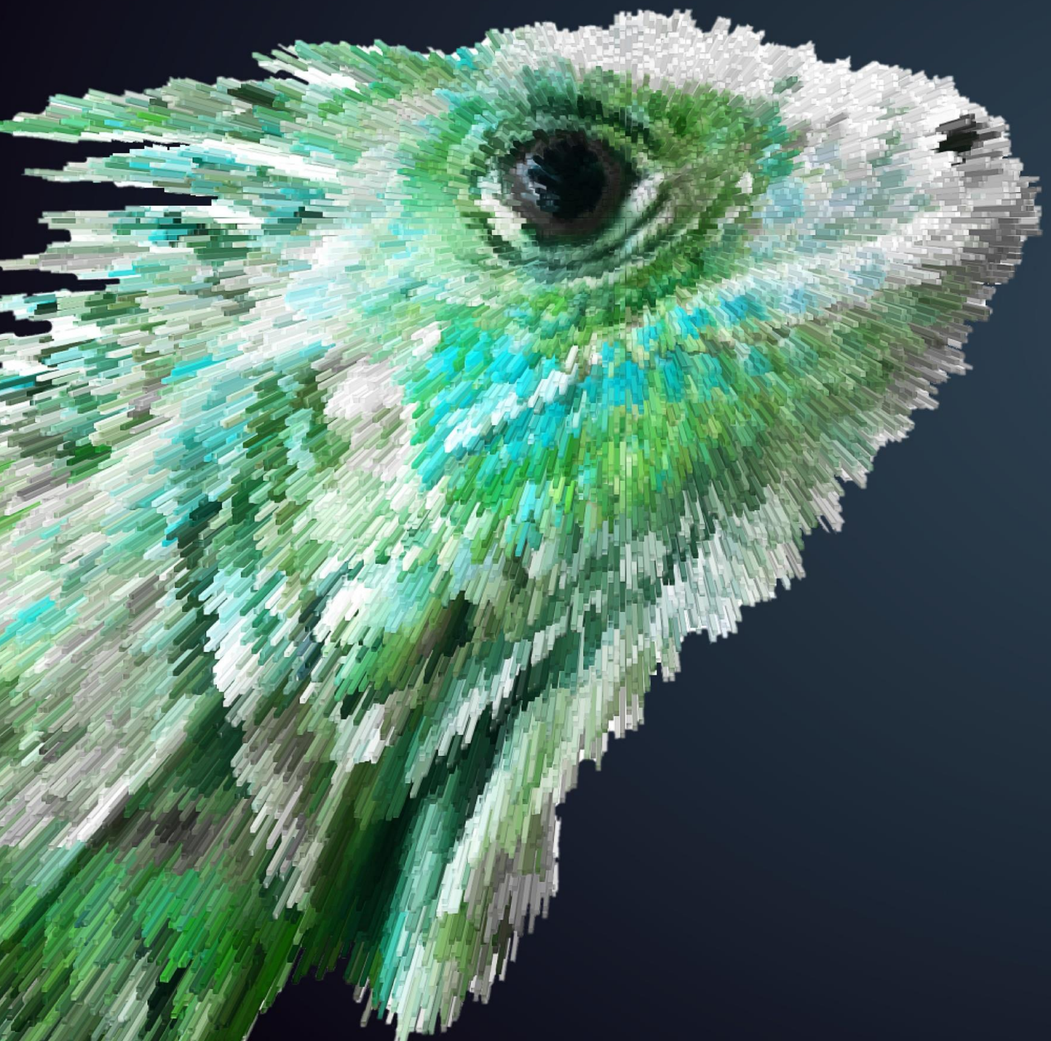
「融合·CONVERGENCY」

TECHWORLD 2021

绿 盟 科 技 技 术 嘉 年 华



理想汽车车联网安全挑战与思考

理想汽车 董威

NSFOCUS TECHWORLD | NSFOCUS

目录
CONTENTS

1 车联网安全挑战
2 车企网络安全能力建设难点
3 理想汽车车联网安全实践
4 安全工作建议

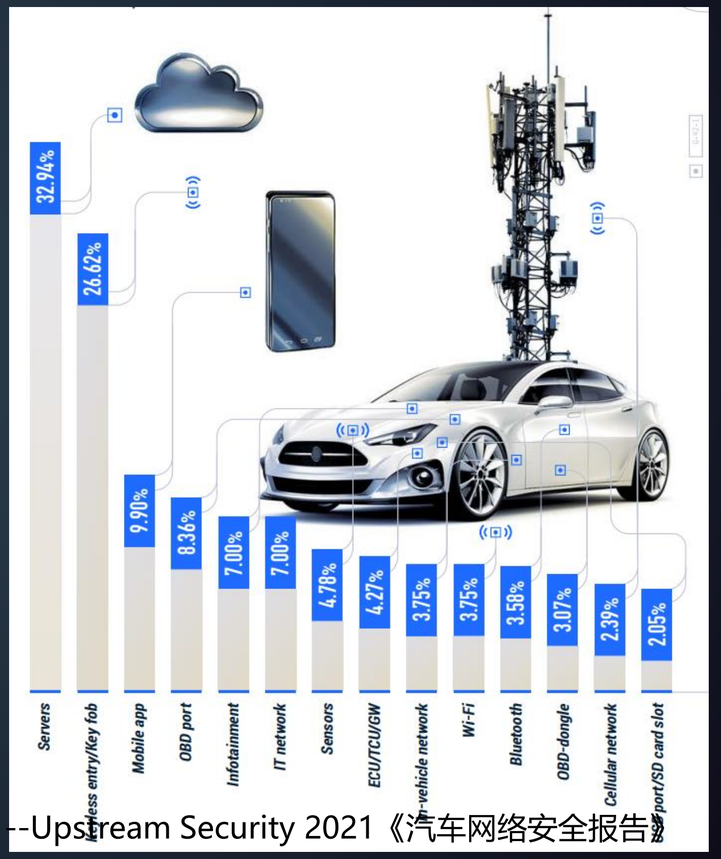
1 车联网安全挑战

1.车联网安全挑战

◆智能网联汽车攻击面扩大，整体安全形势严峻

外部安全形势

- 智能网联汽车成为互联网重要入口
- 全球范围内汽车信息安全事件频发，自2016年增加605%
  --Upstream Security 2020《汽车网络安全报告》
- 国内外汽车信息安全政策法规纷纷出台



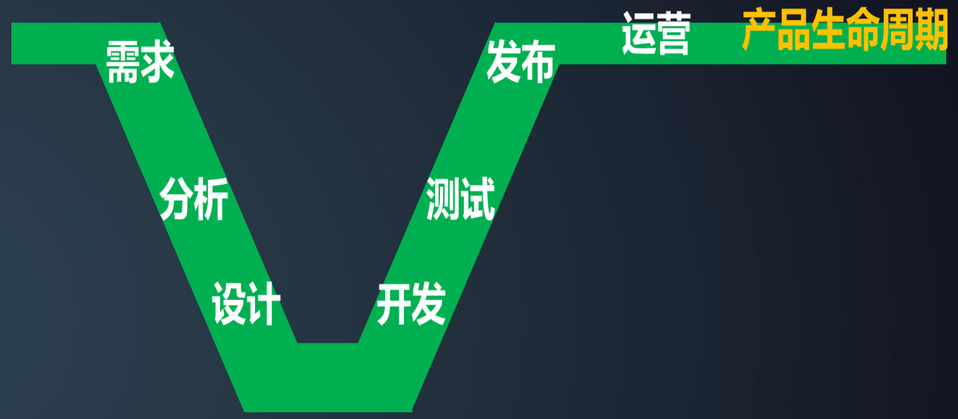
--Upstream Security 2021《汽车网络安全报告》

1.车联网安全挑战

◆智能网联汽车攻击面扩大，整体安全形势严峻

内部安全影响

- 网联功能需求涌现，安全防护急需前置设计
- 基于自主安全团队进行设计开发、验证及运营
- 安全合规成为企业市场开拓的重要前提条件



1.车联网安全挑战

◆数据安全问题成为国家、社会及汽车行业的重点关注问题

头部出行服务公司海外上市
接受有关部门**网络安全**审查

上海车展上演维权事件
引发**数据权利和真实性**争议

37	房产超市	房超科技有限公司	7.0.8	未公开收集使用规则；未经用户同意收集使用个人信息；存在引起个人信息泄露的安全漏洞等。
38	[redacted]汽车	[redacted]新能源汽车有限公司	3.8.0	未明示收集使用个人信息的目的、方式和范围；未经用户同意收集使用个人信息；存在引起个人信息泄露的安全漏洞等。
39	e家安	浙江瑞客佳科技有限公司	4.2.3	未明示收集使用个人信息的目的、方式和范围；未经用户同意收集使用个人信息；存在引起个人信息泄露的安全漏洞等。

车企APP受到公开通报批评
涉及**个人信息数据违规采集**

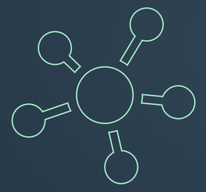
2 车企网络安全能力建设难点

2.车企网络安全能力建设难点

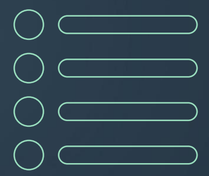
安全能力维度

产品信息安全生命周期

人员能力



组织建设



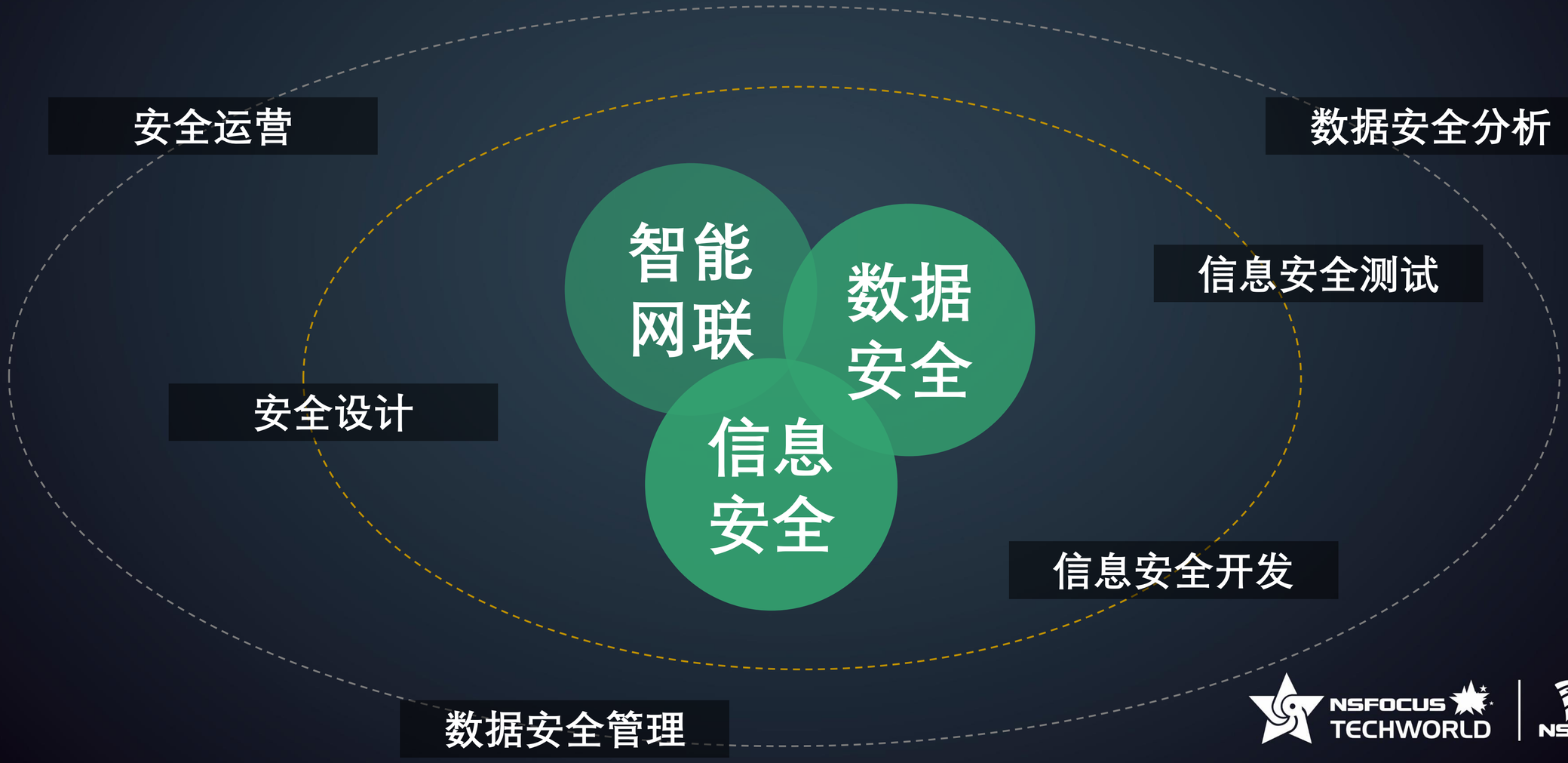
制度流程

技术工具

产品数据安全生命周期

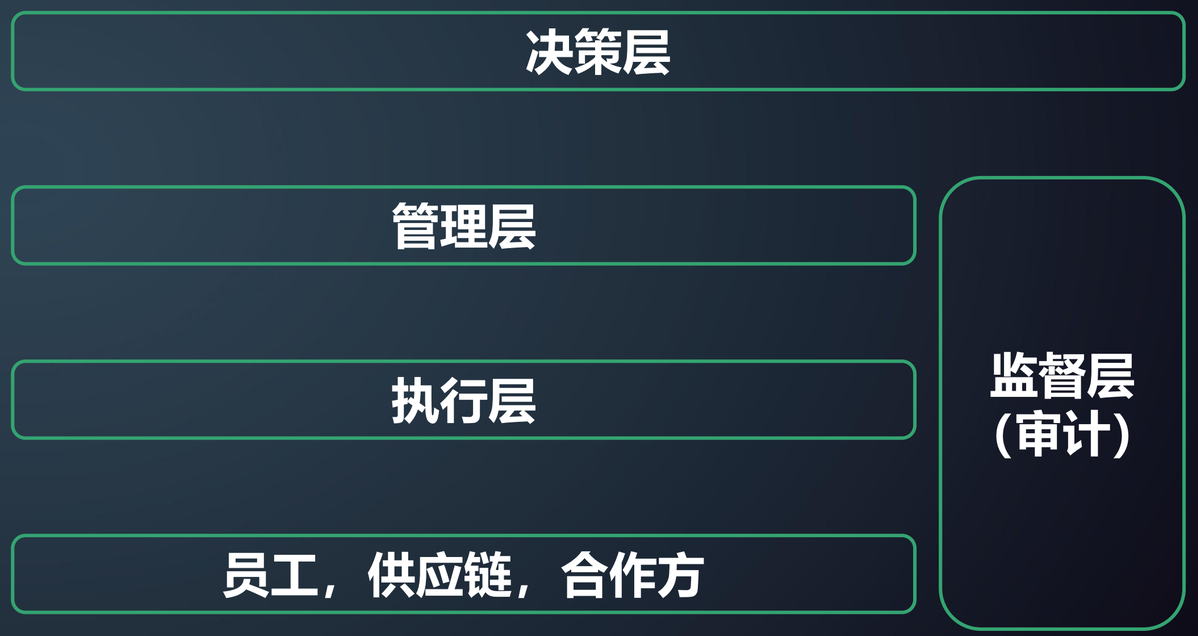
2.车企网络安全能力建设难点

◆汽车行业信息安全人才稀缺，安全团队难组建



2.车企网络安全能力建设难点

◆ **车企业务体系复杂，涉及众多的岗位层级与职能角色，难以建立统一的信息安全管理组织架构。**



2.车企网络安全能力建设难点

◆行业缺乏相关实践积累，车企尚在各自艰难摸索，制度流程难落实

信息安全

- ☑《ISO21434 道路车辆-汽车网络安全工程》
- ☑《WP29 R155法规》
- ☑《智能网联汽车生产企业及产品准入管理指南》

行业指导规范

数据安全

- ☑《汽车数据安全管理若干规定》

企业体系建设面临相同的问题

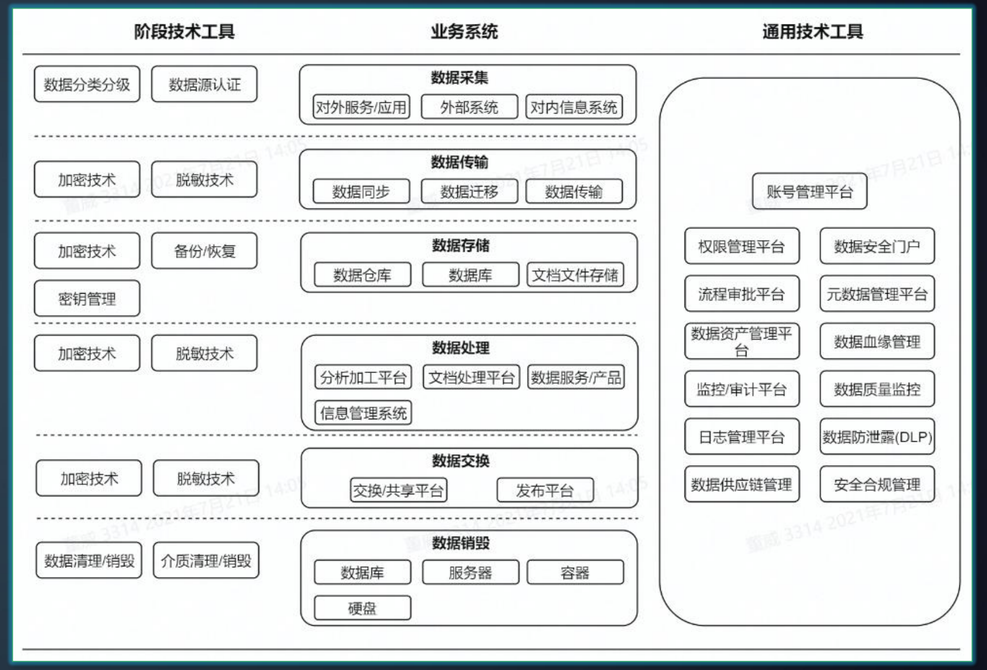
车辆信息安全&数据安全生命周期管理体系

- 网络安全责任制度
- 网络安全技术措施
- 网络安全防护制度
- 网络安全监测预警机制
- 网络安全应急响应机制
- 网络安全漏洞管理机制
- 供应链网络安全保障机制
- ……

- 数据资产管理
- 数据分类分级管理
- 数据风险评估
- 数据风险检测
- 数据安全事件响应机制
- 数据生命周期管理要求
- 数据生命周期技术要求
- 供应链数据安全保障机制
- ……

2.车企网络安全能力建设难点

◆ 数据安全技术及平台工具应用条件受限，安全管控难成体系



- 数据资产散乱不清
- 数据资产管理，权责不明
- 敏感数据信息，分布情况不清楚
- 多数据库接口未统一管理，数据动态监控难实施


APP


小程序


网页


车辆


配套设备/产品


线下门店

3 理想汽车车联网安全实践

3.理想汽车车联网安全实践

云端
安全

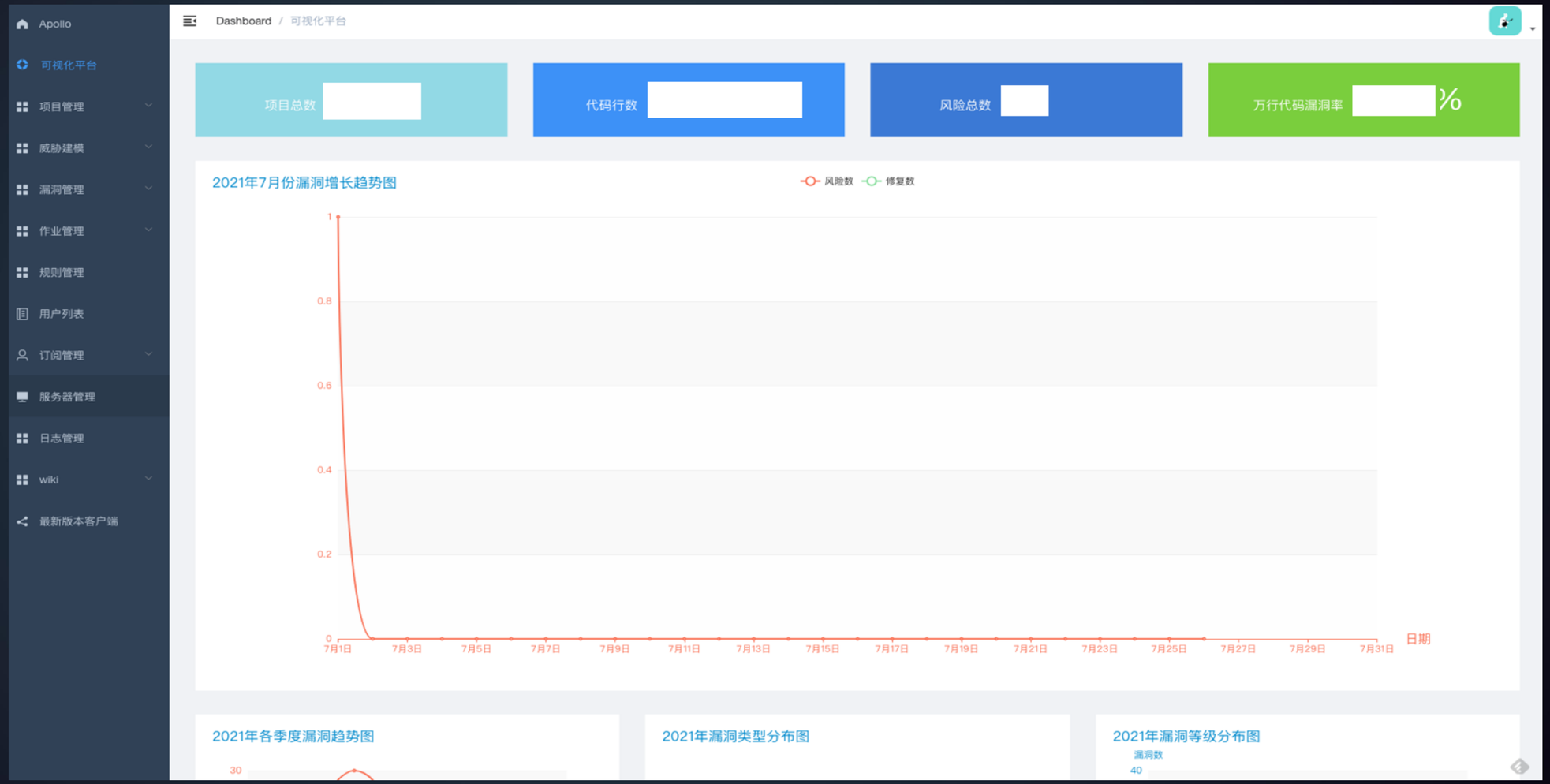
车端
安全

数据
安全

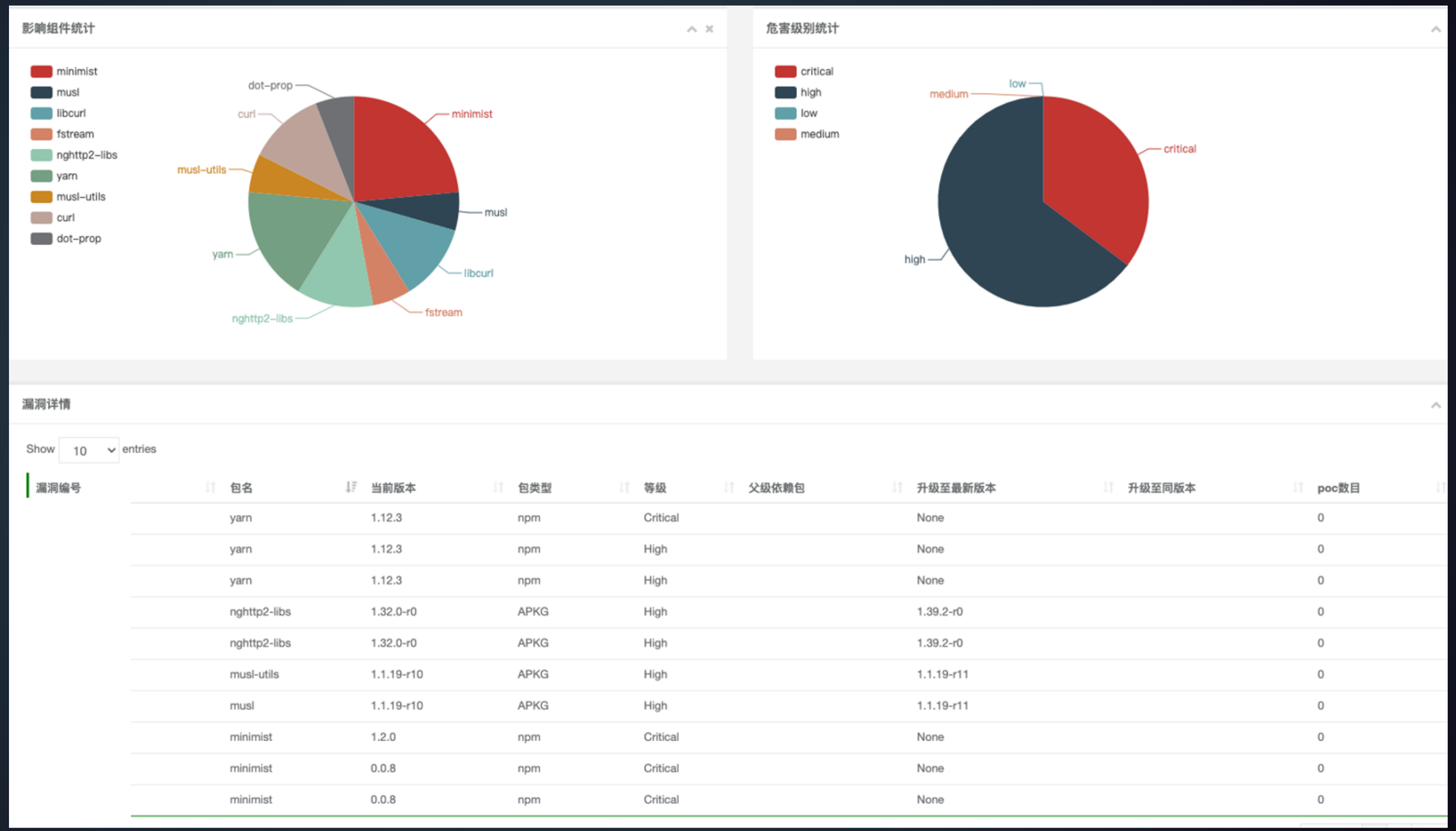
合规
建设

3.1 云端安全---DevSecOps

- 威胁建模
- 白盒检测
- SCA检测
- 灰盒检测
- 黑盒检测



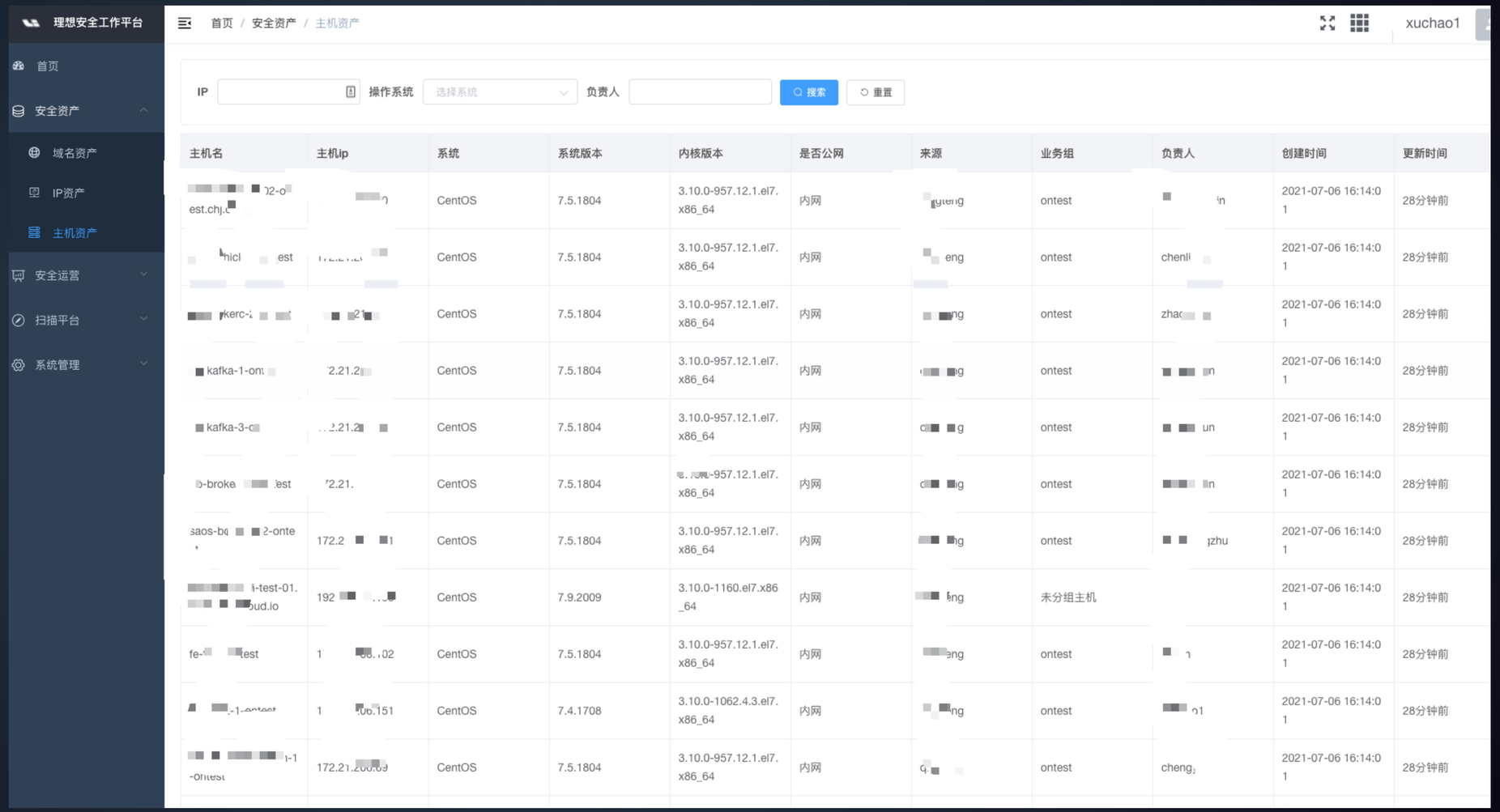
3.1 云端安全---容器安全


影响组件统计
minimist
musl
libcurl
fstream
nghttp2-libs
yarn
musl-utils
curl
dot-prop
危害级别统计
critical
high
low
medium
漏洞详情
Show 10 entries
漏洞编号
包名
当前版本
包类型
等级
父级依赖包
升级至最新版本
升级至同版本
poc数目
yarn 1.12.3 npm Critical None 0
yarn 1.12.3 npm High None 0
yarn 1.12.3 npm High None 0
nghttp2-libs 1.32.0-r0 APKG High 1.39.2-r0 0
nghttp2-libs 1.32.0-r0 APKG High 1.39.2-r0 0
musl-utils 1.1.19-r10 APKG High 1.1.19-r11 0
musl 1.1.19-r10 APKG High 1.1.19-r11 0
minimist 1.2.0 npm Critical None 0
minimist 0.0.8 npm Critical None 0
minimist 0.0.8 npm Critical None 0

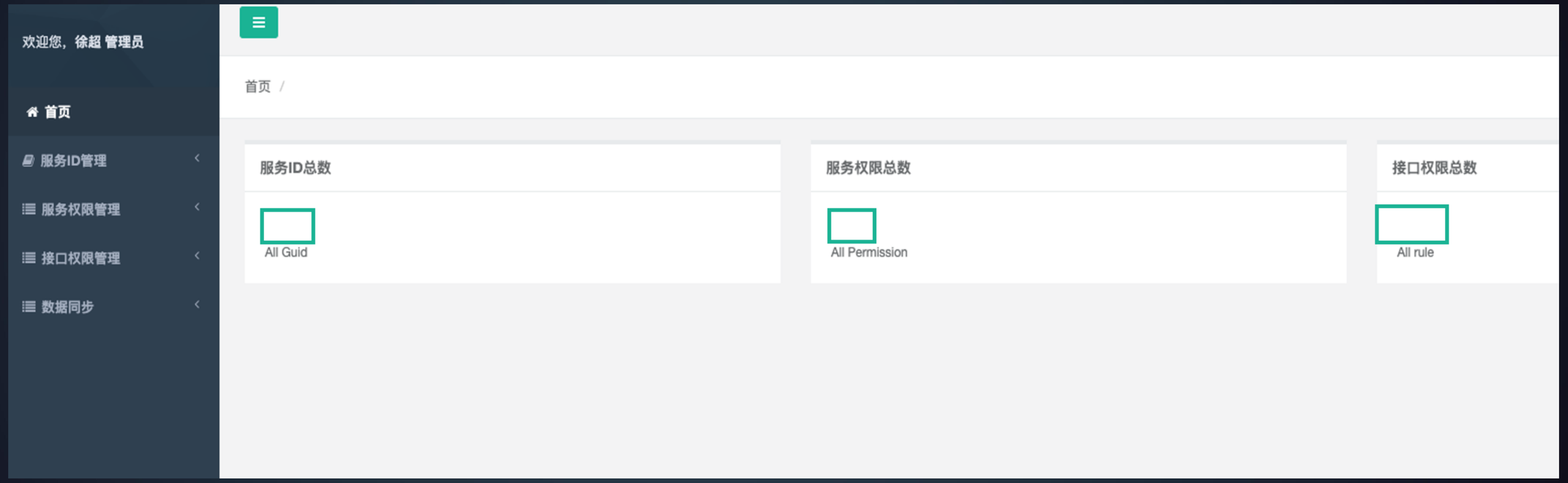
3.1 云端安全---自动化风险评估系统

资产管理

风险管理



3.1 云端安全---API接口管理



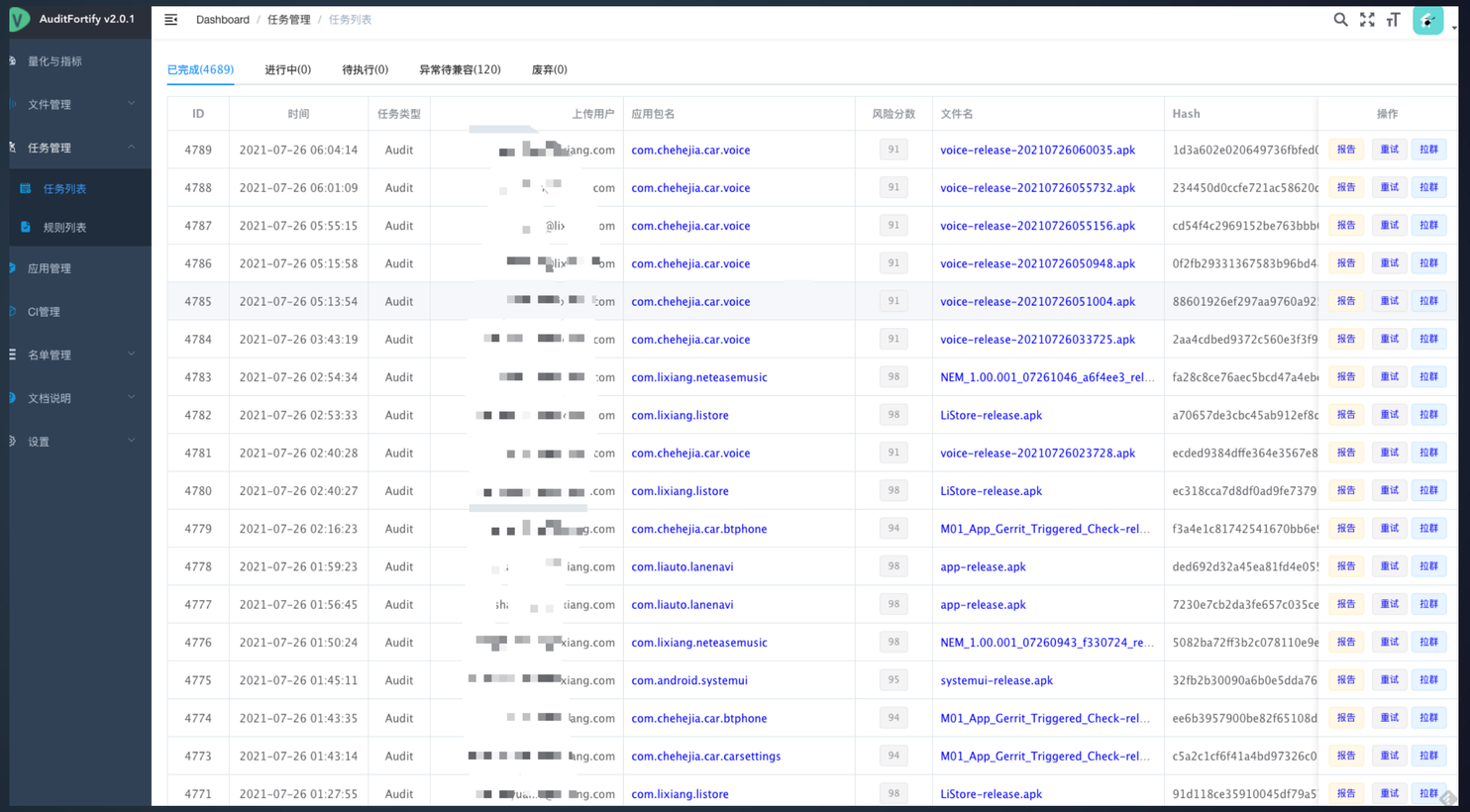
3.2 车端安全---安全防护部署

整车安全	零部件安全	功能系统安全
硬件层安全	网络层安全	HU FOTA
系统层安全	框架层安全	XCU FOTA
网络层安全	内核安全	HOA FOTA
访问层安全	APP安全	

3.2 车端安全---自动化资产风险评估系统

资产管理

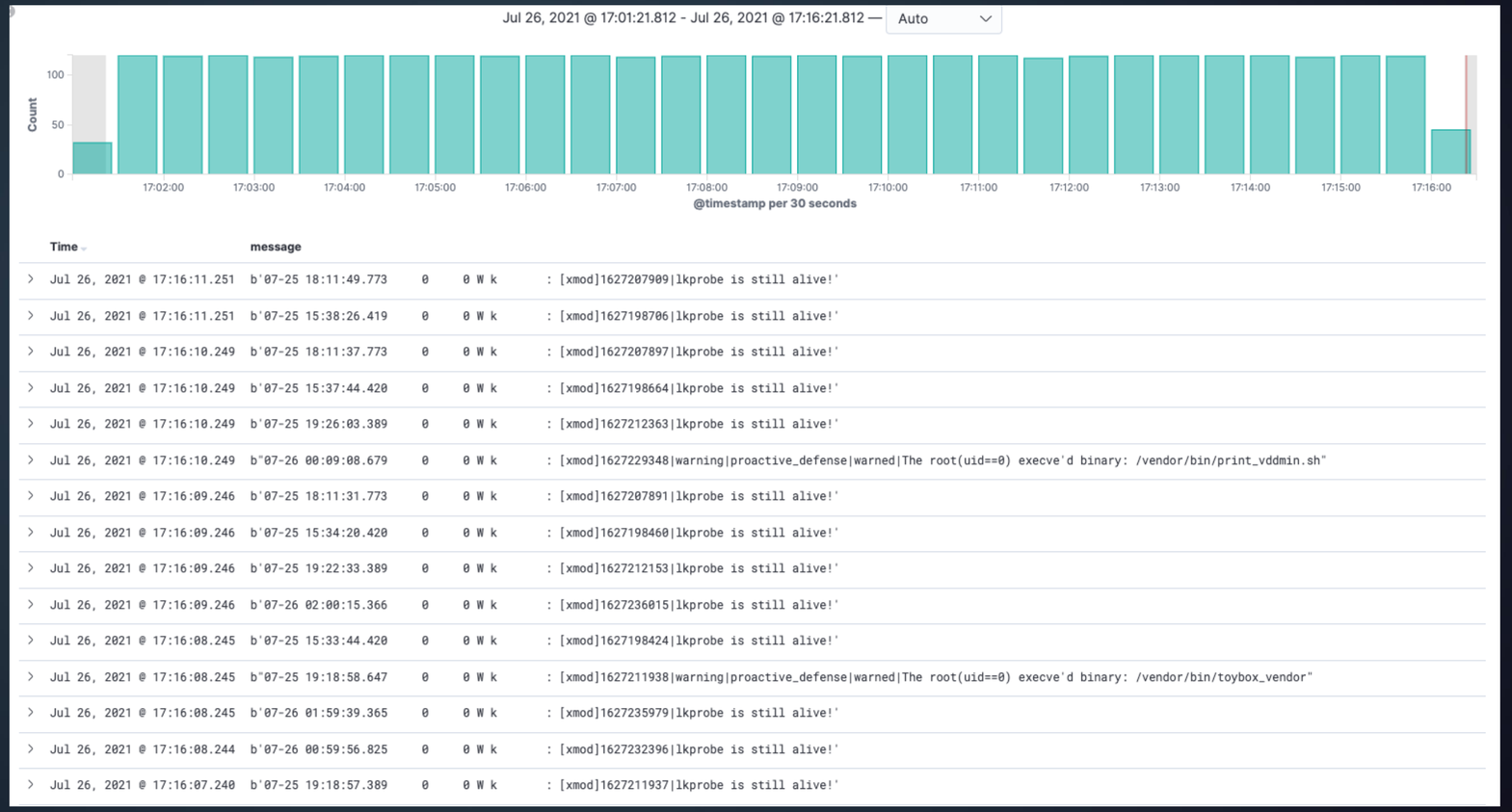
风险管理



ID	时间	任务类型	上传用户	应用包名	风险分数	文件名	Hash	操作
4789	2021-07-26 06:04:14	Audit	[redacted]	com.chehejia.car.voice	91	voice-release-20210726060035.apk	1d3a602e020649736fbfed0	报告 重试 拉群
4788	2021-07-26 06:01:09	Audit	[redacted]	com.chehejia.car.voice	91	voice-release-20210726055732.apk	234450d0ccfe721ac58620c	报告 重试 拉群
4787	2021-07-26 05:55:15	Audit	[redacted]	com.chehejia.car.voice	91	voice-release-20210726055156.apk	cd54f4c2969152be763bbb	报告 重试 拉群
4786	2021-07-26 05:15:58	Audit	[redacted]	com.chehejia.car.voice	91	voice-release-20210726050948.apk	0f2fb29331367583b96bd4	报告 重试 拉群
4785	2021-07-26 05:13:54	Audit	[redacted]	com.chehejia.car.voice	91	voice-release-20210726051004.apk	88601926ef297aa9760a92	报告 重试 拉群
4784	2021-07-26 03:43:19	Audit	[redacted]	com.chehejia.car.voice	91	voice-release-20210726033725.apk	2aa4cdbed9372c560e3f3f9	报告 重试 拉群
4783	2021-07-26 02:54:34	Audit	[redacted]	com.lixiang.neteasemusic	98	NEM_1.00.001_07261046_a6f4ee3_rel...	fa28c8ce76aec5bcd47a4eb	报告 重试 拉群
4782	2021-07-26 02:53:33	Audit	[redacted]	com.lixiang.listore	98	LiStore-release.apk	a70657de3cbc45ab912ef8c	报告 重试 拉群
4781	2021-07-26 02:40:28	Audit	[redacted]	com.chehejia.car.voice	91	voice-release-20210726023728.apk	ecded9384dffe364e3567e8	报告 重试 拉群
4780	2021-07-26 02:40:27	Audit	[redacted]	com.lixiang.listore	98	LiStore-release.apk	ec318cca7d8df0ad9fe7379	报告 重试 拉群
4779	2021-07-26 02:16:23	Audit	[redacted]	com.chehejia.car.btphone	94	M01_App_Gerrit_Triggered_Check-rel...	f3a4e1c81742541670bb6e5	报告 重试 拉群
4778	2021-07-26 01:59:23	Audit	[redacted]	com.liauto.lanenavi	98	app-release.apk	ded692d32a45ea81fd4e05	报告 重试 拉群
4777	2021-07-26 01:56:45	Audit	[redacted]	com.liauto.lanenavi	98	app-release.apk	7230e7cb2da3fe657c035ce	报告 重试 拉群
4776	2021-07-26 01:50:24	Audit	[redacted]	com.lixiang.neteasemusic	98	NEM_1.00.001_07260943_f330724_re...	5082ba72ff3b2c078110e9e	报告 重试 拉群
4775	2021-07-26 01:45:11	Audit	[redacted]	com.android.systemui	95	systemui-release.apk	32fb2b30090a6b0e5dda76	报告 重试 拉群
4774	2021-07-26 01:43:35	Audit	[redacted]	com.chehejia.car.btphone	94	M01_App_Gerrit_Triggered_Check-rel...	ee6b3957900be82f65108d	报告 重试 拉群
4773	2021-07-26 01:43:14	Audit	[redacted]	com.chehejia.car.carsettings	94	M01_App_Gerrit_Triggered_Check-rel...	c5a2c1cf6f41a4bd97326c0	报告 重试 拉群
4771	2021-07-26 01:27:55	Audit	[redacted]	com.lixiang.listore	98	LiStore-release.apk	91d118ce35910045df79a5	报告 重试 拉群

3.2 车端安全---入侵检测

- 主机IDS
- 网络IDS
- 车端系统IDS
- 车载通信IDS

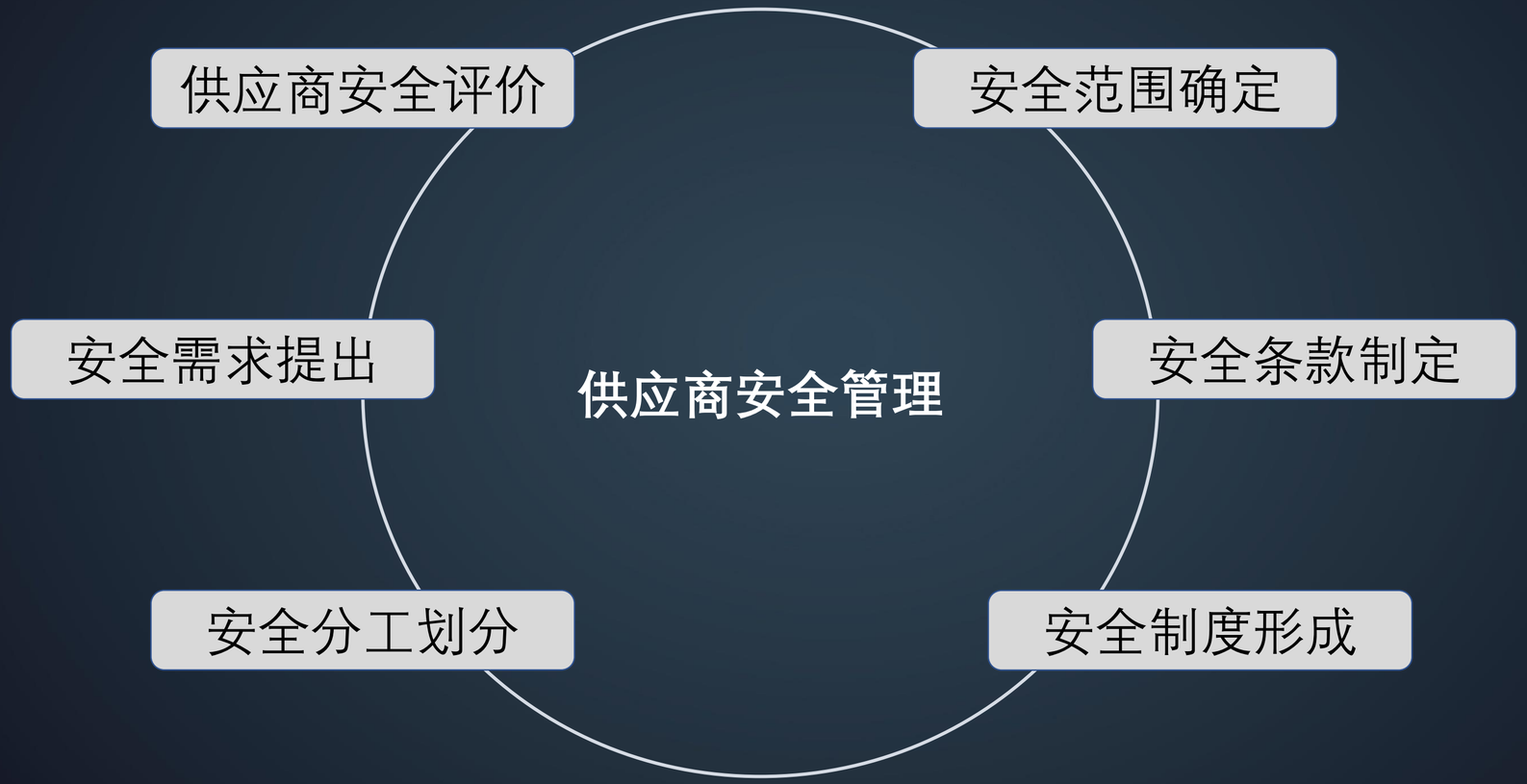


Time	message
Jul 26, 2021 @ 17:16:11.251	b'07-25 18:11:49.773 0 0 W k : [xmod]1627207909|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:11.251	b'07-25 15:38:26.419 0 0 W k : [xmod]1627198706|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:10.249	b'07-25 18:11:37.773 0 0 W k : [xmod]1627207897|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:10.249	b'07-25 15:37:44.420 0 0 W k : [xmod]1627198664|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:10.249	b'07-25 19:26:03.389 0 0 W k : [xmod]1627212363|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:10.249	b"07-26 00:09:08.679 0 0 W k : [xmod]1627229348|warning|proactive_defense|warned|The root(uid==0) execve'd binary: /vendor/bin/print_vddmin.sh"
Jul 26, 2021 @ 17:16:09.246	b'07-25 18:11:31.773 0 0 W k : [xmod]1627207891|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:09.246	b'07-25 15:34:20.420 0 0 W k : [xmod]1627198460|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:09.246	b'07-25 19:22:33.389 0 0 W k : [xmod]1627212153|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:09.246	b'07-26 02:00:15.366 0 0 W k : [xmod]1627236015|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:08.245	b'07-25 15:33:44.420 0 0 W k : [xmod]1627198424|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:08.245	b"07-25 19:18:58.647 0 0 W k : [xmod]1627211938|warning|proactive_defense|warned|The root(uid==0) execve'd binary: /vendor/bin/toybox_vendor"
Jul 26, 2021 @ 17:16:08.245	b'07-26 01:59:39.365 0 0 W k : [xmod]1627235979|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:08.244	b'07-26 00:59:56.825 0 0 W k : [xmod]1627232396|lkprobe is still alive!'
Jul 26, 2021 @ 17:16:07.240	b'07-25 19:18:57.389 0 0 W k : [xmod]1627211937|lkprobe is still alive!'

3.3 数据安全

- 数据分类分级
- 数据风险评估
- 数据风险检测

3.4 合规建设---供应商管理



4 安全工作建议

4.1 信息安全管理建议

- **整车企业：**
  安全技术的量产应用需谨慎推进
- **零部件供应商：**
  安全开发能力已成为竞争力
- **安全服务供应商：**
  关注完整解决方案及场景考虑

4.2 数据安全管理建议

1. 细化行业监督管理要求

希望监管机构能够推进行业细则的出台，减少监管和规范多单位并行推进的情况，使车企能够聚焦能力体系的建设及问题的解决。

2. 制定数据安全建设实施指南

由行业监管机构牵头，整车企业、互联网代表企业、安全公司参与，围绕过程阶段、技术应用、系统/工具编订数据安全建设实施指南。

3. 同步定位关键标准规范需求

基于实施指南同步构建智能网联汽车数据安全管理体系及技术架构，针对重要紧急缺失环节展开标准规范的制定。

4. 制定行业数据安全过程审查评价规则

基于规范要求及实践反馈制定完善、可执行的数据安全过程审查评价规则，提出更为规范的约束提升行业安全能力水平。

NSFOCUS TECHWORLD | NSFOCUS

THANKS

欢迎关注绿盟科技
了解更多安全资讯

微信公众号

新浪微博