华泰证券在金融安全风险运营的实践

姓名 华泰证券 信息安全中心

CIS 网络安全创新大会
Cyber Security Innovation Summit

我们的故事 不是”一个人的安全部”

网络安全创新大会
Cyber Security Innovation Summit

信息安全中心组织架构

- 安全技术运营与攻防
- 安全威胁与事件响应
- 操作风险与数据安全
- 工程效率与应用安全
- 网络安全基础设施

团队到职能精细化分工

- 1、漏洞与资产运营职能
  - 1.1、漏洞运营
    - 1.1.1、内部互联网侧操作系统层漏洞扫描
    - 1.1.2、内部互联网侧web漏洞运营
    - 1.1.3、外部互联网侧操作系统层漏洞运营
    - 1.1.4、外部互联网侧web漏洞运营
    - 1.1.5、外部众测、多源众测、专属SRC
    - 1.1.6、漏洞预警
  - 1.2、资产运营
  - 1.3、补丁运营
    - 1.3.1、操作系统补丁
    - 1.3.2、中间件补丁（weblogic、nginx、tomcat等）
- 2、情报中心职能
  - 2.1、业务情报输出
    - 2.1.1、薅羊毛网站监控
    - 2.1.2、薅羊毛社区监控
  - 2.2、漏洞情报输出
  - 2.3、数据泄露情报输出
    - 2.3.1、github监控
    - 2.3.2、网盘监控
    - 2.3.3、暗网监控
  - 2.4、威胁情报
    - 2.4.1、商业情报
    - 2.4.2、开源情报
    - 2.4.3、自有情报
- 3、主机安全及相关组件标准化职能
  - 3.1、中间件配置基线及其落地与推广
  - 3.2、操作系统配置基线及其落地与推广
  - 3.3、数据库配置基线及其落地与推广
  - 3.4、云主机安全标准化
- 4、安全技术研究与赋能职能
  - 4.1、黑客工具对抗技术研究（CS、冰蝎、隧道等）
  - 4.2、安全算法
    - 4.2.1、DGA检测
    - 4.2.2、DNS隧道检测
    - 4.2.3、EDR行为检测
    - 4.2.4、Webshell检测
    - 4.2.5、网站访问行为检测
    - 4.2.6、数据泄露检测
    - 4.2.7、.....
  - 4.3、样本分析赋能
  - 4.4、NLP
    - 4.4.1、威胁情报采集
    - 4.4.2、API安全检测
    - 4.4.3、.....
  - 4.5、安全大数据分析建模
  - 4.6、安全场景关联分析
- 5、安全运营基础设施建设与运营职能
  - 5.1、漏洞检测系统运营
    - 5.1.1、[redacted]us
    - 5.1.2、[redacted]VS
    - 5.1.3、[redacted]
    - 5.1.4、[redacted]
  - 5.2、防病毒系统运营
    - 5.2.1、[redacted]
  - 5.3、安全监控、数据泄露流量采集点覆盖
  - 5.4、数据库审计运营
  - 5.5、补丁系统运营
    - 5.5.1、YUM源
    - 5.5.2、[redacted]
    - 5.5.3、WSUS
  - 5.6、日志增强类系统
    - 5.5.1、[redacted]n版本迭代
    - 5.5.2、[redacted]y版本迭代
  - 5.7、WAF安全策略调优
  - 5.8、泰坦底层持续迭代
  - 5.9、多源攻击检测建设
    - 5.9.1、[redacted]
    - 5.9.2、[redacted]
    - 5.9.3、[redacted]a
    - 5.9.4、[redacted]
    - 5.9.5、[redacted]
    - 5.9.6、.....
  - 5.10、蜜罐
    - 5.10.1、开源蜜罐
    - 5.10.2、商业蜜罐
  - 5.11、安全检测规则优化
    - 5.11.1、[redacted]
    - 5.11.2、[redacted]y
    - 5.11.3、suricata
    - 5.11.4、yara
    - 5.11.5、[redacted]
- 6、安全日常监控“大运营”职能
  - 6.1、WEB安全
  - 6.2、样本分析
  - 6.3、特殊领域：AD安全、邮件安全
  - 6.4、业务安全
  - 6.5、内网渗透
  - 6.6、威胁hunting
- 7、红蓝对抗职能
  - 7.1、内部蓝军建设
  - 7.2、组织内外部红蓝对抗演练
  - 7.3、基于mitre attack模型的攻防演练平台建设
  - 7.4、演练场景制定

安全技术运营与攻防

单一兵种无法打赢现代环境下网络空间实战

THEN, HOW?

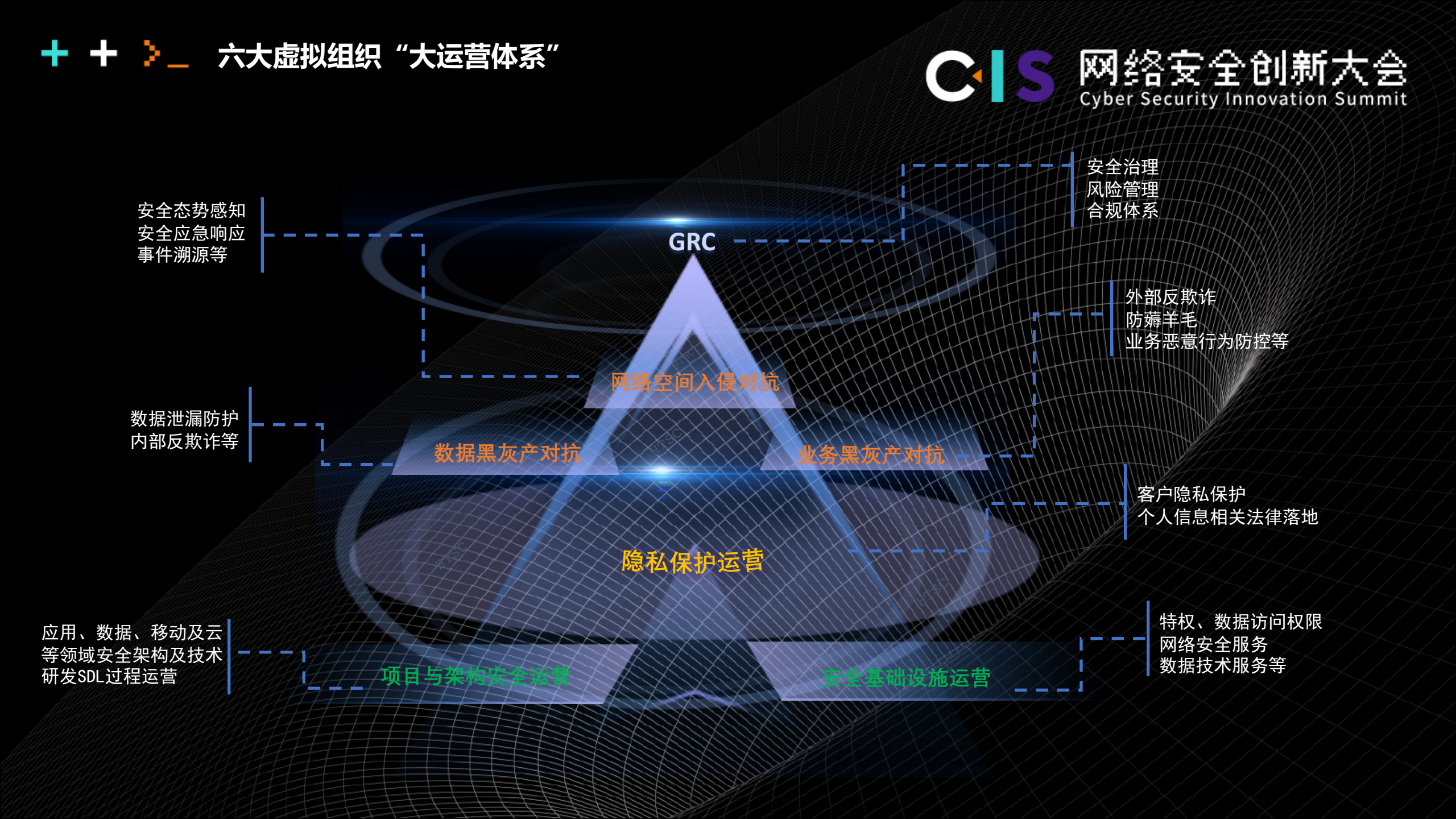
“合成营”

职能精细化带来的挑战

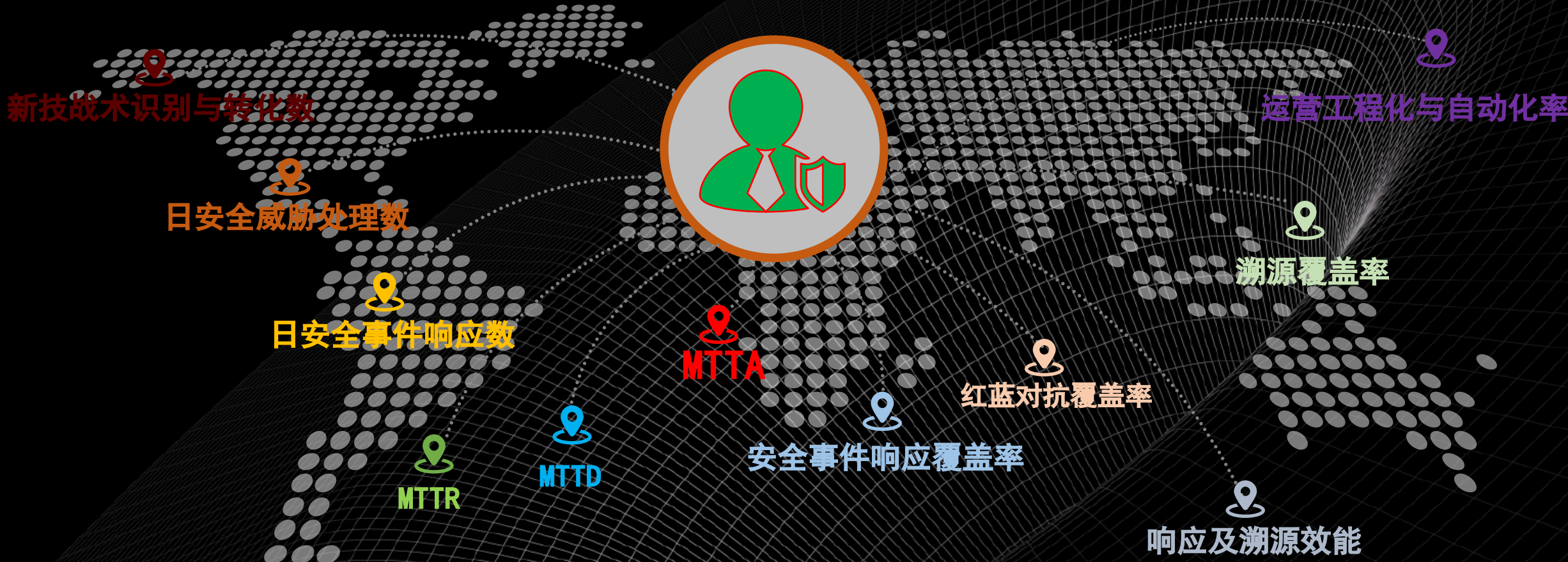
- 安全技术运营与攻防 — 航空兵
- 安全威胁与事件响应 — 装甲兵
- 操作风险与数据安全 — 特种兵
- 工程效率与应用安全 — 电子对抗
- 网络安全基础设施 — 步兵

VS

六大虚拟组织“大运营体系”



网络空间入侵对抗 – 运营指标



数据黑灰产对抗 – 运营指标

1 识别及跟踪外部数据泄露

2 内部数据泄漏

3 内部员工异常行为画像

业务黑灰产对抗 – 运营指标

业务目标

- 能应对千万/年级别的营销活动
- 保障X%的营销资金投放
- 年接入保障业务场景数
- 红蓝对抗业务安全覆盖

安全基础设施 – 运营指标


弹性基础设施
覆盖率
标准化架构
覆盖率
故障MTTD/MTTR
微隔离与访问控
制覆盖率
安全基础服务
工程化自动化率
监控覆盖率
安全基础
自服务数量

项目与架构安全 – 运营指标

01 安全评估覆盖率

02 端到端安全交付效能

03 安全工具链DevOps集成率

04 安全测试能力覆盖率

05 安全漏洞修复率

06 安全漏洞漏出率

07 标准化安全组件数

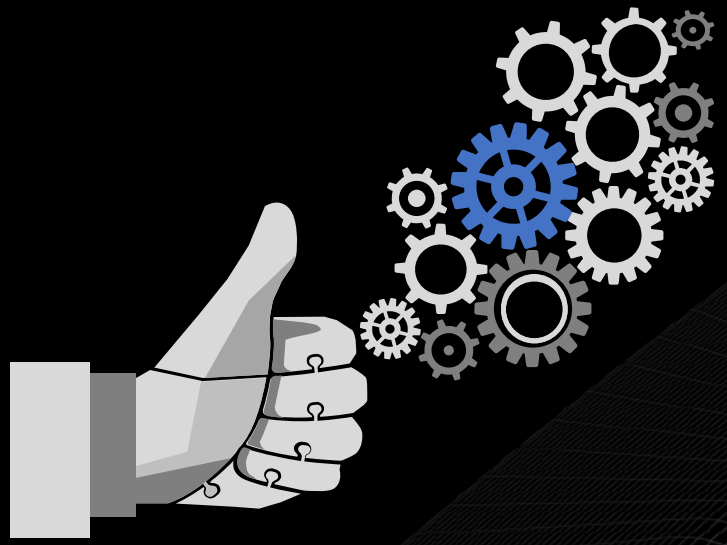
08 软件安全能力成熟度

最小的成本将隐私安全法律法规转落地为控制要求

- 隐私保护措施内建落地数
- 隐私安全评估项目覆盖率
- 业务场景隐私数据Profile成熟度
- 隐私安全问题整改完成率
- 高风险隐私场景标准化数量

GRC

CIS 网络安全创新大会
Cyber Security Innovation Summit



推动公司建立完善的治理机制

1个委员会3个工作组（网安、数安、隐私/客户数据保护）

信息安全风险注册机制

月度风险报告

开展等保2.0合规体系建设

一级 纲领/策略		二级 制度/要求/规范		三级 流程/细则
《中华人民共和国刑法》 《中华人民共和国网络安全法》 《中华人民共和国数据安全法》（征求意见稿） 《中华人民共和国个人信息保护法》（专家建议稿）	**国务院令第147号**：计算机信息系统安全保护条例 **网信办**：《关键信息基础设施安全保护条例》 **网信办**：《数据安全管理办法》 **网信办**：《网络安全威胁信息发布管理办法（征求意见稿）》 **工信部**：《网络安全漏洞管理规定 (征求意见稿)》 **公通43号文**：《计算机信息安全等级保护管理办法》 **公安部**：《网络安全等级保护条例》（征求意见稿）	**国标**：GB/T 35273-2017《信息安全技术 个人信息安全规范》 **国标**：GB/T 22239-2019《信息系统安全等级保护基本要求》（2.0） **国标**：GB/T28448-2012《信息安全技术 信息系统安全等级保护测评要求》 **证券业**：JR/T 证券期货业信息系统安全等级保护基本要求 **证券业**：JR/T 证券期货业信息系统安全等级保护测评要求	**人行**：《金融行业信息系统信息安全等级保护实施指引》 **人行**：《金融行业信息系统信息安全等级保护测评指南》 **人行**：《金融行业信息安全等级保护测评服务安全指引》 **证券业**：《证券期货业数据分类分级指引》（JR/T 0158-2018） **证券业**：《信息系统审计指南》	**等保**：定级、备案、交涉整改、等级测评、监督检查
法律	行政法规 Policy	配套标准（Standard=Control Requirements）	指引/指南	流程/步骤
Charter（章程） 有效期：10年+ 签发：CEO 是否强制：强制	Policy（策略） 有效期：5年+ 签发：CEO 是否强制：强制	Standards（标准/规范） 有效期：2-3年 签发：CIO 是否强制：强制	GuideLines（指南/指引） 有效期：2-3年，签发CIO，是否强制：非强制	Processes and Procedures（流程/步骤） 有效期1-3年，签发：部门经理，是否强制：强制
《华泰证券信息安全章程Charter/ Strategy》/公司章程	《华泰证券网络安全治理条例》（待定）			《华泰证券Risk Register流程》

HOW?

安全产品与平台体系

CIS 网络安全创新大会
Cyber Security Innovation Summit

1 TITANS 泰坦人工智能安全态势感知

泰坦，利用**大数据、智能分析引擎** 和 **可视化**等手段，结合**威胁情报**，对企业面临的网络攻击进行检测，快速、有效地为企业建立威胁检测、分析、处置和全网**安全态势感知**能力，使得企业的信息安全**可知、可见、可控。**

2 PRISM 棱镜UEBA用户行为分析平台

棱镜，通过**机器学习**技术，对用户的行为进行**智能化**分析，建立**用户风险画像**，实时检测异常行为和未知威胁，及时发现**内部用户**违规行为，如违规操作、帐号滥用、内部欺诈、数据泄露等。

3 PANDORA 潘多拉情报中心

潘多拉，基于大数据、NLP技术，实现互联网中企业相关联情报的识别、采集、分析及汇聚，对外提供代码泄露、企业舆情、业务情报等危害企业的情报中心服务。

4 AIYIS 宙斯盾业务反欺诈

宙斯盾，基于**设备指纹**技术以及海量的设备安全数据、威胁情报数据和用户行为数据，利用**流式分析**处理、**数据挖掘**和**机器学习**等关键技术，构建出独有的以设备安全为核心的**智能实时身份反欺诈**模型,精准识别和预防各类互联网身份欺诈风险，检测如恶意注册、薅羊毛等、抢优惠券，提升营销效果。

5 COPHEUS 造父API安全检测平台

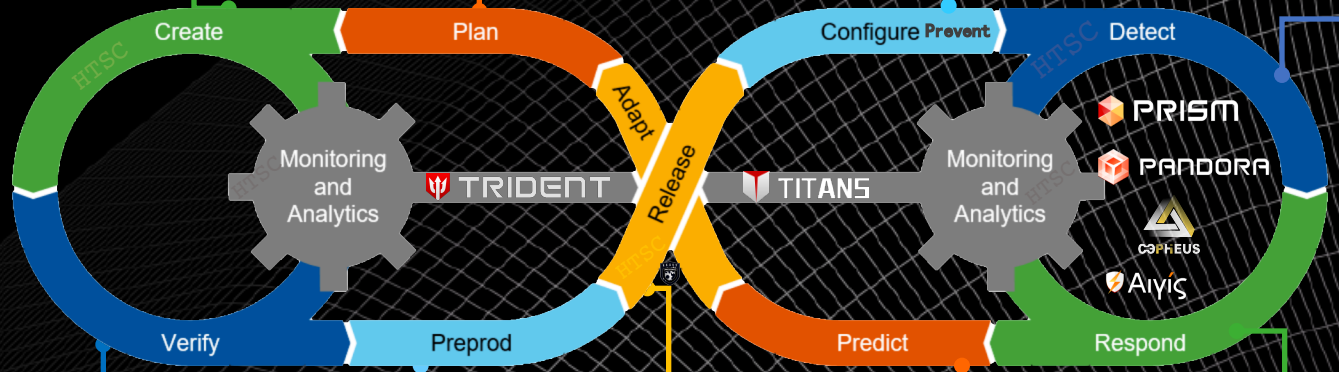
造父，通过流量、网管、标准API文档等，自动发现识别API服务接口，标记敏感数据、登录认证行为、特权行为，记录API变更生命周期；自动发现暴漏在公网的API相关数据、凭证。对重要的API接口进行自动化渗透，发现存在的权限、逻辑漏洞；通过基线和算法模型，自动检测多种攻击，包括Bot攻击、DOS攻击、异常数据访问行为等。

6 TRIDENT 三叉戟安全管理平台

三叉戟，具有SDL全流程管理、应用安全风险画像、漏洞全生命周期管理、 DevSecOps工具链集成、自动化渗透测试工具集等功能，为企业提供应用安全一站式综合管理平台。

安全工具支撑体系

CIS 网络安全创新大会
Cyber Security Innovation Summit



安全编码规范
- Confluence

IDE集成安全工具
- Find Security Bugs (SAST)
- Black Duck (SCA)

安全专家知识库
- WIKI

轻量级威胁建模
- HELIUS安全需求平台

开源组件治理
- Black Duck
- Nexus firewall

WAF
NGFW
宙斯盾反欺诈

主机安全
WEB 安全
NTA
DLP
EDR
蜜罐
沙箱
防病毒
补丁管理
UEBA
- 棱镜PRISM

安全态势感知(NGSOC)
- 泰坦 TITANS

漏洞管理
- 三叉戟TRIDENT

潘多拉情报中心
宙斯盾反欺诈
造父API安全检测

源代码静态扫描(SAST)
- SonarQube(Find Security Bugs)
- Cobra
- Bandit

开源组件安全扫描(SCA)
- Black Duck

Docker安全扫描
- Container Security (Tenable)

黑盒安全测试(DAST/IAST)
- AppScan
- AWVS
- WAS
- OWASP ZAP
- Arachni

移动安全测试(MAST)
- iJIAMI
- MBSF

主机安全扫描:
- Nessus

配置基线安全扫描
- Nessus

渗透测试
- Burp Suite
- SQLMap
- noSQLMap
- Metasploit
- Mitmproxy
- Netcat
- Curl
- Wireshark
- Fiddler
- Apktool
- Dex2jar
- JEB

外部“蓝军”与内部渗透测试

标准化与加固
- CIS Benchmark

主机环境验证测试
- Tenable Nessus

剩余安全风险报告
- JIRA

漏洞修复计划
- JIRA

代码签名
- signtool

APP加固
- iJIAMI

威胁情报(Threat Intelligence)
- 商业情报
- 开源情报

业务情报
数据泄漏情报
潘多拉情报中心
资产管理
- Black Duck
- 三叉戟 TRIDENT

NGFW
WAF
ATP(Terminal)
Incident Response
溯源
- IDA
- OllyDbg

安全响应 | 应用安全 | 移动安全 | 安全攻防

Input from End-Users, Customers, Team and Other Stakeholders

大运营轮值负责人

Product Owner

Team

大运营工作列表

FEATURES

Product Backlog

大运营虚拟团队

How Much To Commit To Do By Sprint's End

Sprint Planning Meeting

(Parts One and Two)

运营计划会

TASKS

Sprint Backlog

任务列表

大运营轮值负责人

ScrumMaster

Product Backlog Refinement

Sprint

1-4 Weeks

1周冲刺

No Changes in Duration or Goal

每日站会

Daily Scrum Meeting and Artifacts Update

Review

运营指标分析

Potentially Shippable Product Increment

Retrospective

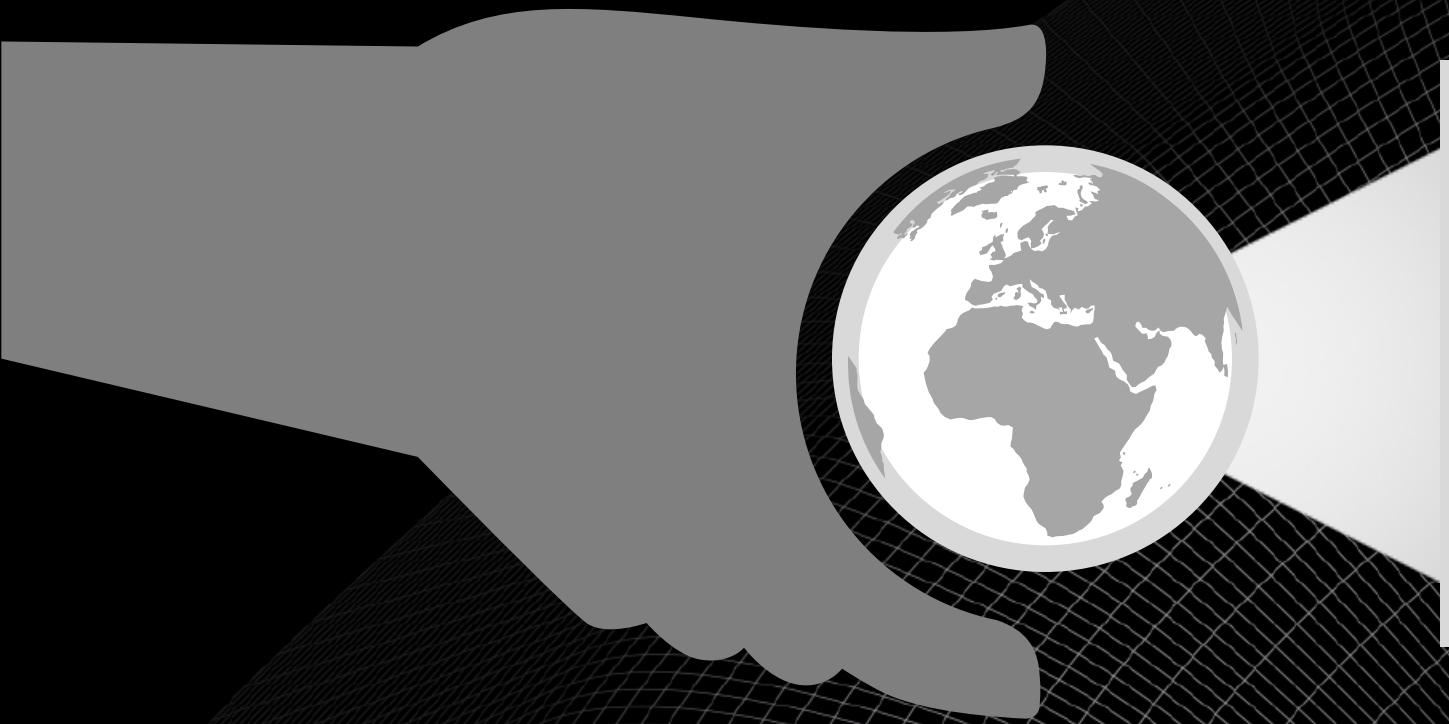
周运营回顾会

敏捷宣言

个体与交互 胜过 过程和工具

响应变化 胜过 遵循计划

精益求精 胜过 简单执行



项目与架构安全大运营职责

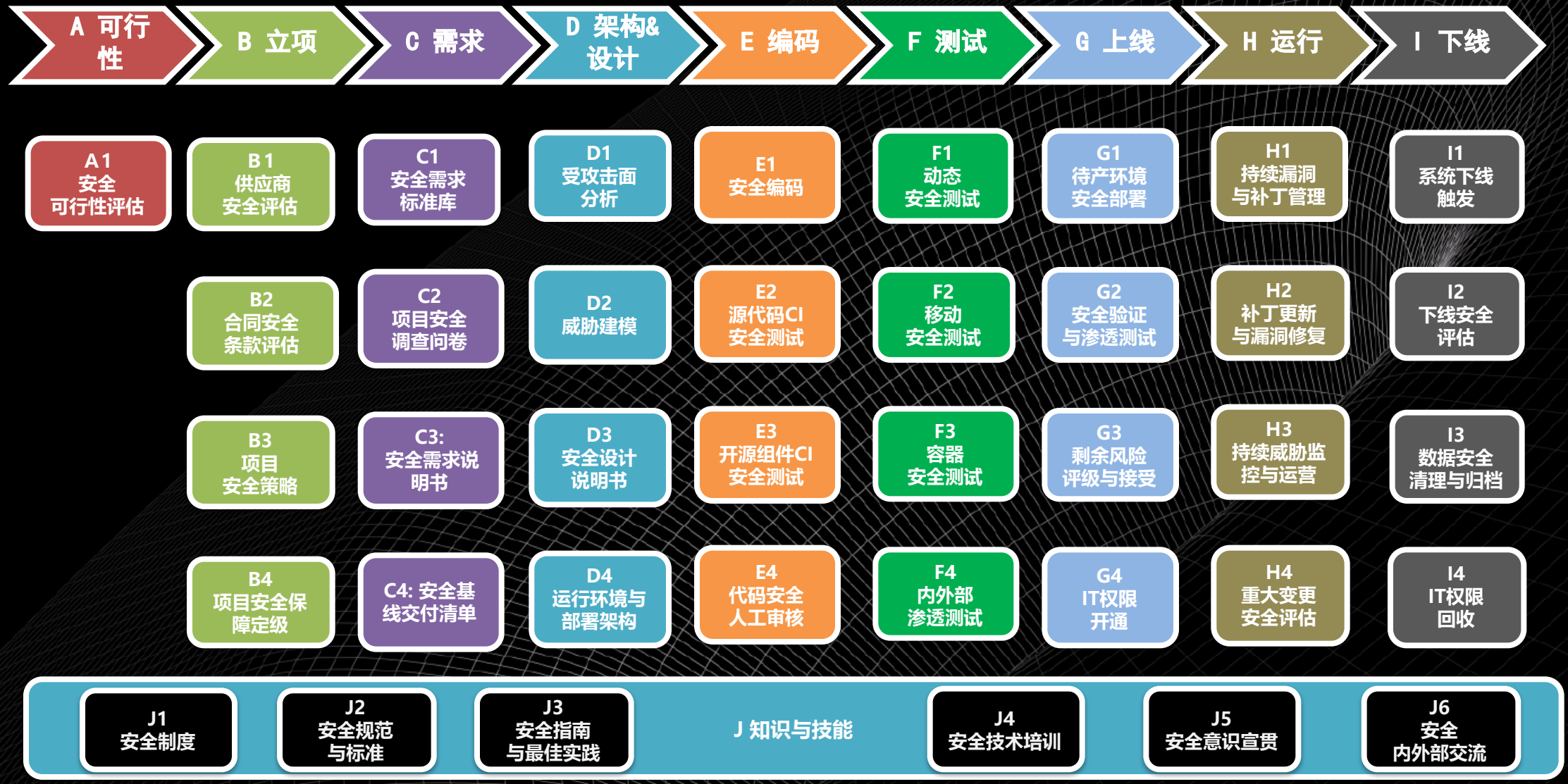
负责项目的安全评估，进行安全架构设计、安全需求分析、项目安全建设SDL全过程跟踪等，向研发团队交付端到端安全解决方案。

安全评估小组

组员来自职能团队，专家领域包括：安全架构、应用安全、隐私安全、数据安全、业务安全、移动安全、云安全、安全测试等。

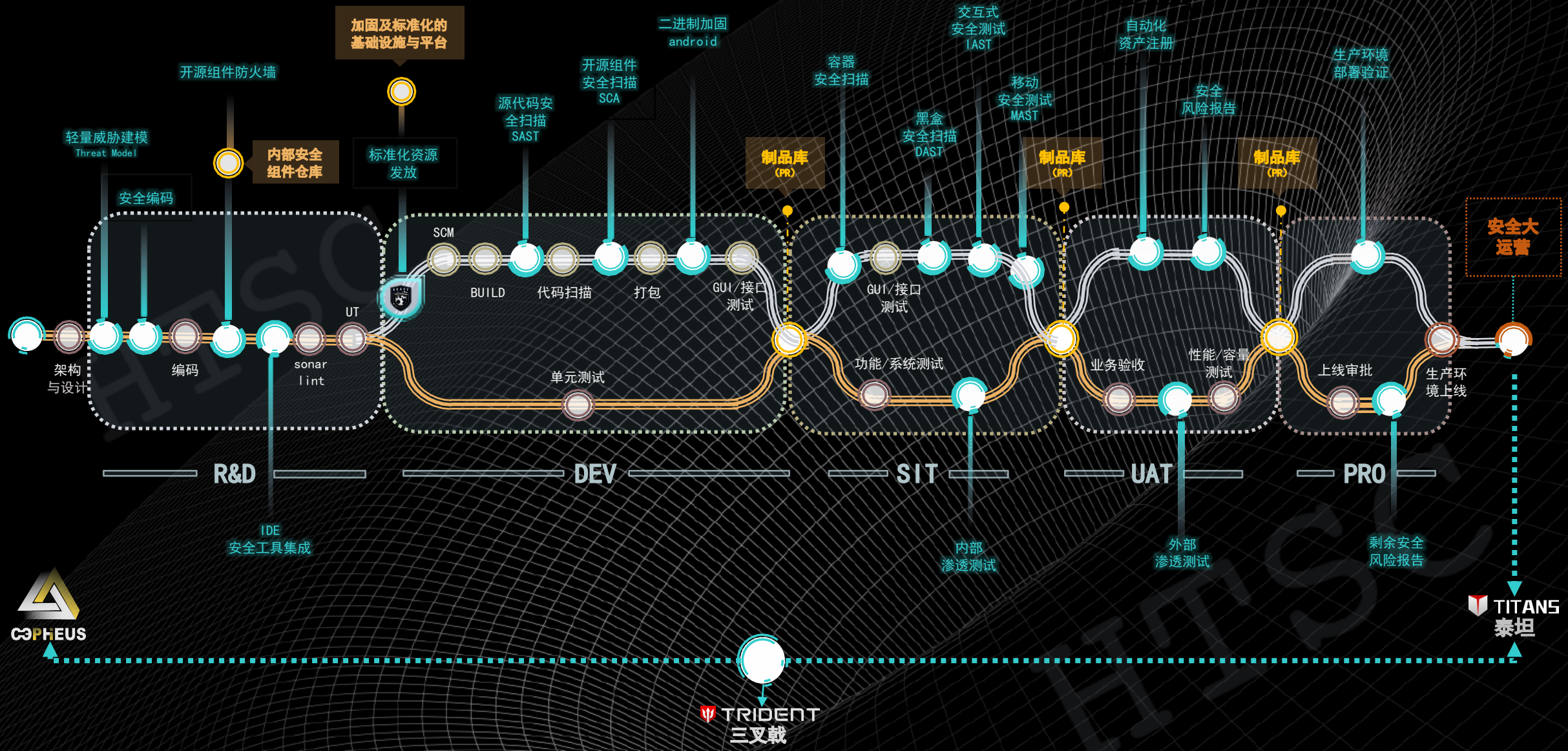
项目与架构安全 - SDL（BSI）框架

网络安全创新大会
Cyber Security Innovation Summit



项目与架构安全 - DevSecOps

CIS 网络安全创新大会
Cyber Security Innovation Summit



业务黑灰产对抗 – 全链路治理运营体系

问题

事前	事中	事后
• 安全意识低 • 信息泄露 • 信息流转/买卖	• 盗卡/盗账户 • 垃圾注册 • 营销作弊	• 黑产持续攻击 • 风控效能退化

治理

事前	事中	事后
情报建设	实时风控	溯源反制
安全教育	离线分析	风控生命周期管理
业务蓝军	安全评审	

业务黑灰产对抗 – 基础支撑

平台产品

风控引擎-宙斯盾　情报服务-潘多拉　监控管理-泰坦

算法模型

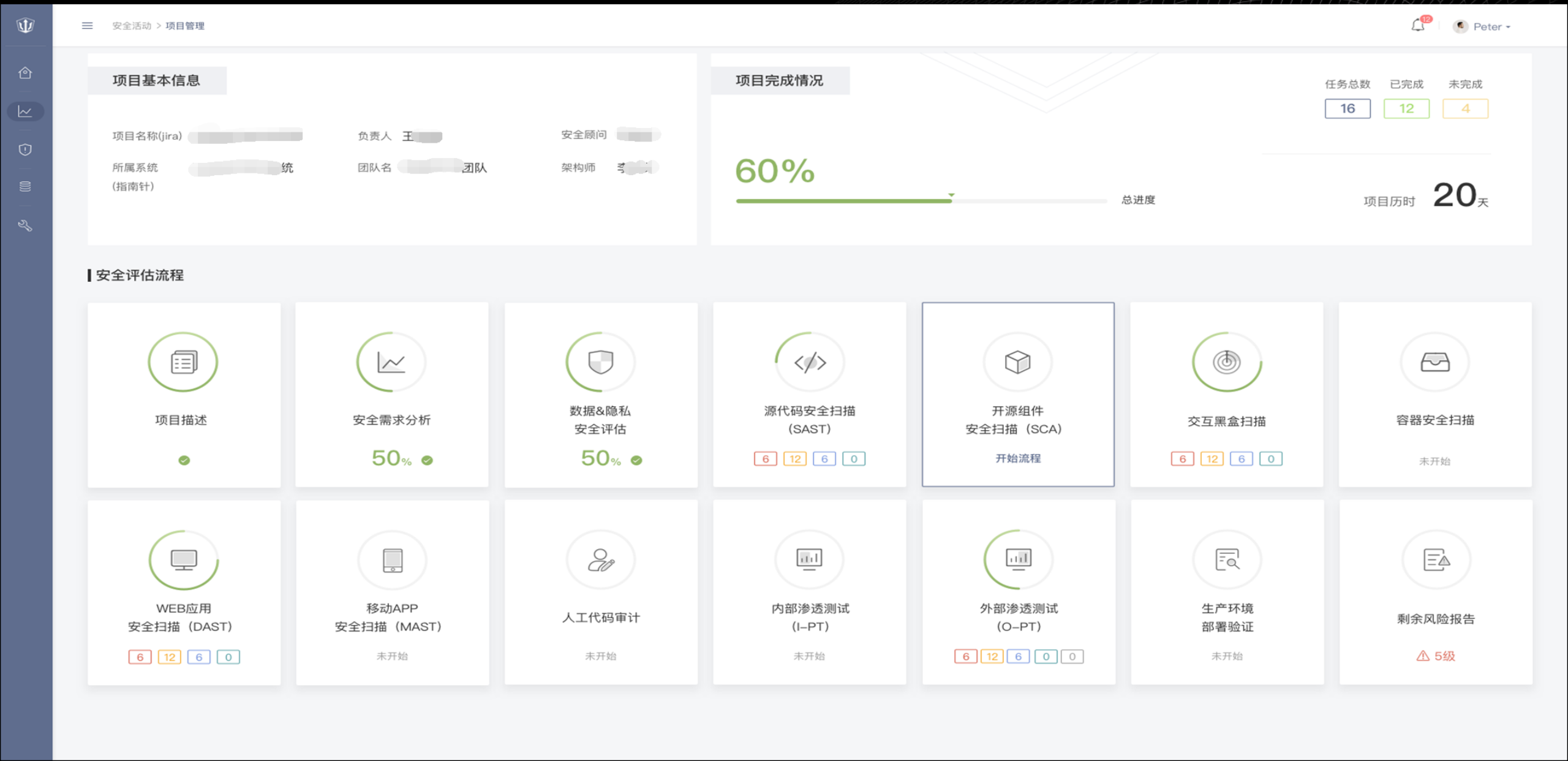
账户质量　异动偏离　团伙关联　异常聚集

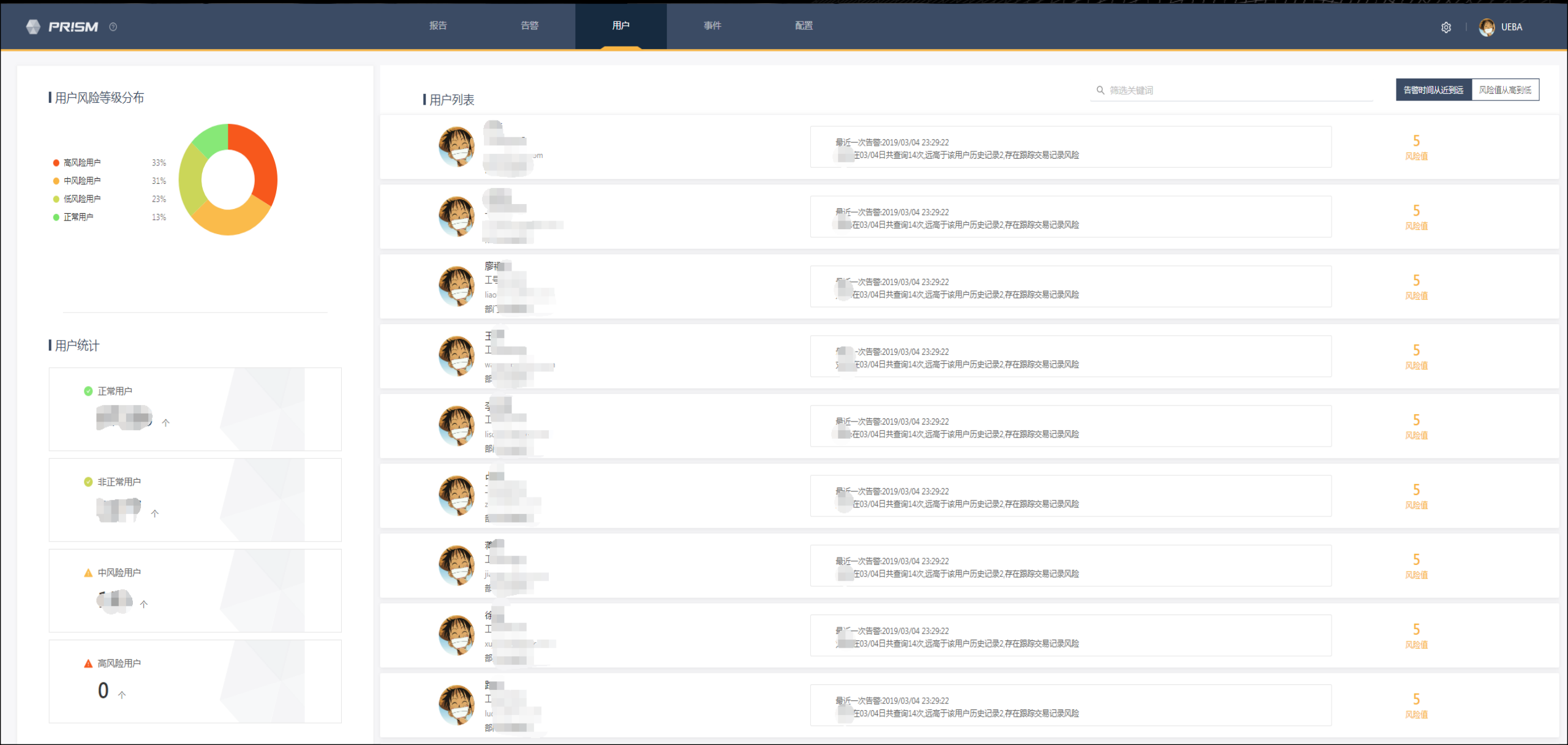
深度学习　异常检测　无/半监督学习　统计指标

基础数据

行为　身份　关系　环境　标签　第三方数据


资产源
SecurityCenter SC
IT资源管理平台
KOLIDE
TITANS
扫描器
AppScan
IBM Security
acunetix
nessus
Professional
metasploit
express
salmap
展示层
仪表盘
安全测试
漏洞管理
资产管理
SDL
接口层
API
服务层
任务管理
节点管理
策略管理
调度引擎
解析器
漏洞知识库
聚合引擎
规则管理
风险引擎
漏洞采集
资产图谱
资产风险画像
分析引擎
资产ETL
资产采集
安全需求
流程管理
量化管理
报表管理
系统联动
数据层
mongoDB
MySQL
漏洞源
BLACKDUCK
sonar
qube
tenable.io
Container Security
PANDORA
情报中心
Atlassian
JIRA
DEVOPS


安全活动 > 项目管理
Peter
项目基本信息
项目名称(jira)
负责人 王
安全顾问
所属系统(指南针)
统
团队名
团队
架构师
项目完成情况
任务总数 16
已完成 12
未完成 4
60%
总进度
项目历时 20天
安全评估流程
项目描述
安全需求分析
50%
数据&隐私安全评估
50%
源代码安全扫描(SAST)
6 12 6 0
开源组件安全扫描（SCA）
开始流程
交互黑盒扫描
6 12 6 0
容器安全扫描
未开始
WEB应用安全扫描（DAST)
6 12 6 0
移动APP安全扫描（MAST)
未开始
人工代码审计
未开始
内部渗透测试(I-PT)
未开始
外部渗透测试(O-PT)
6 12 6 0 0
生产环境部署验证
未开始
剩余风险报告
5级


PRISM
报告
告警
用户
事件
配置
UEBA
用户风险等级分布
高风险用户 33%
中风险用户 31%
低风险用户 23%
正常用户 13%
用户统计
正常用户
非正常用户
中风险用户
高风险用户
0
用户列表
筛选关键词
告警时间从近到远
风险值从高到低
最近一次告警:2019/03/04 23:29:22
在03/04日共查询14次,远高于该用户历史记录2,存在跟踪交易记录风险
5
风险值

SO?

网络空间入侵对抗 – DAILY REPORT

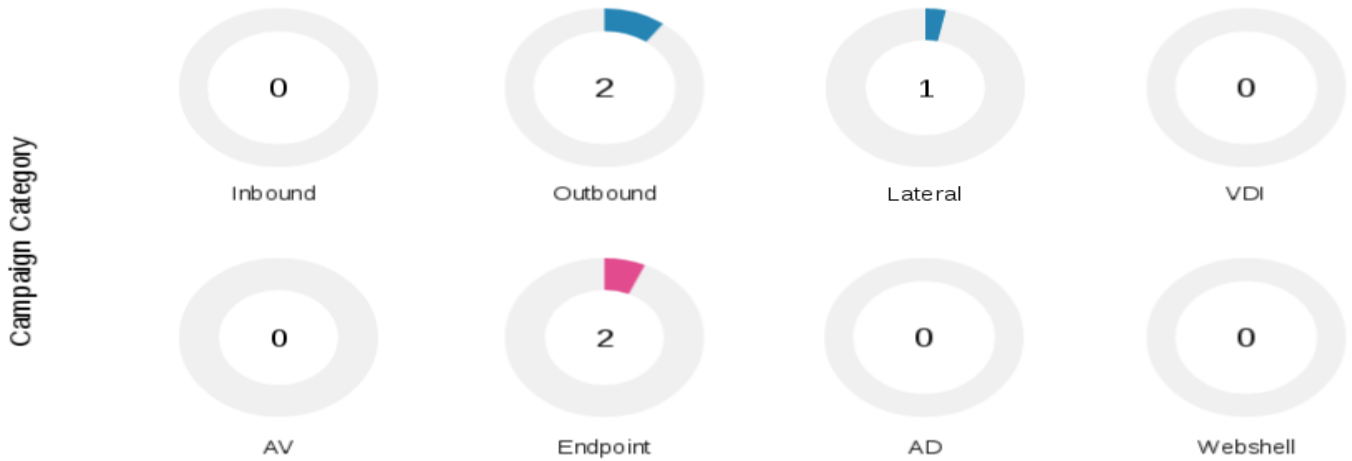
CIS 网络安全创新大会 Cyber Security Innovation Summit

901110556 Events	209440 Alerts	5946 Threats	5 Campaign

Last 7 Days Threat Trend

Alert Category

alert_category	num
bro_http	126
dns_tunnel_detect	993
sepm_av	413
sepm_hips	108869
suricata	12752
sysmon	42
threat_dns	14221
threat_domain	60
threat_ip	71944
waf	20

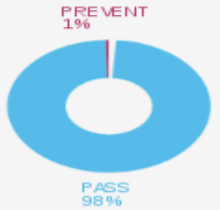


风控处置

17385
总事件

2048
风险识别事件

95
风控处置事件



事件处置率

用户处置率

总事件场景分布

opType	event_cnt
LOGIN	17385

风险处置事件场景分布

opType	event_cnt
LOGIN	95

各场景风险处置方式

登录	邀请好友	理财节
入黑	入黑，且阻断	入黑，且阻断

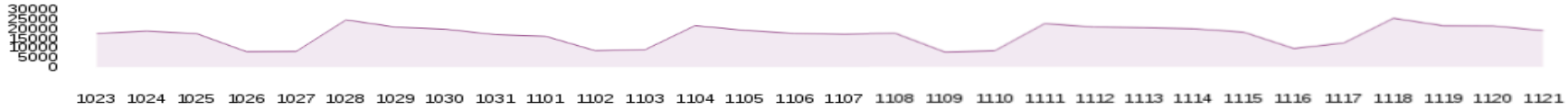
处置最多的设备-型号分布

重点设备型号处置事件量

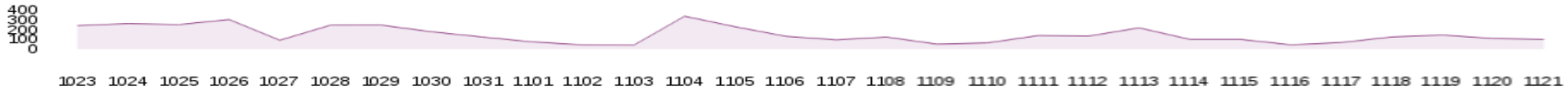
处置最多的账户

user	prevent_cnt
135****6415	27
134****9155	19
189****8626	17
188****1508	15
188****3482	13
173****4326	12
150****3525	10
136****4456	9
138****4059	9
181****4521	9

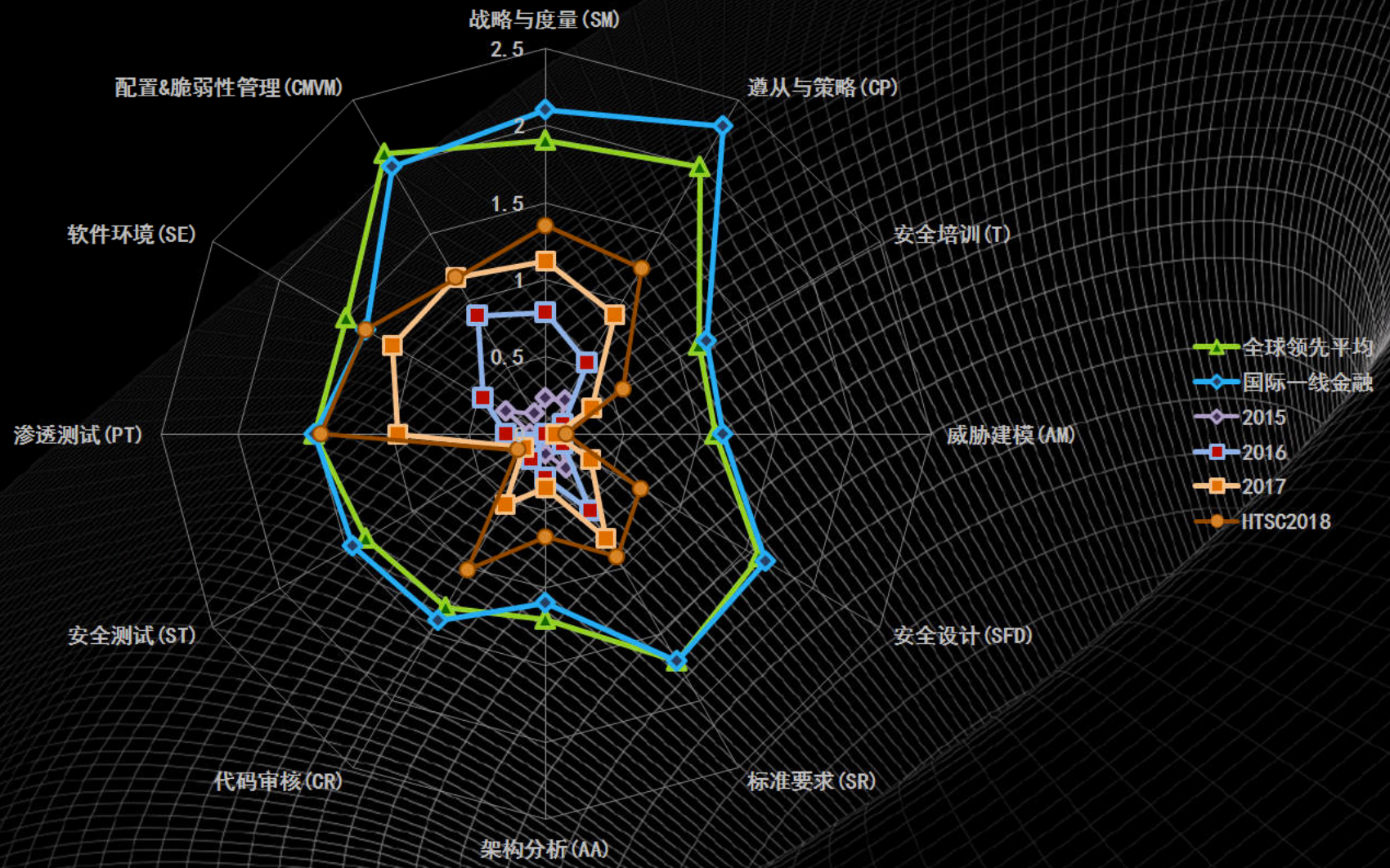
过去30天总事件量趋势



过去30天处置事件量趋势



软件安全成熟度度量


战略与度量(SM)
2.5
2
1.5
1
0.5
遵从与策略(CP)
安全培训(T)
威胁建模(AM)
安全设计(SFD)
标准要求(SR)
架构分析(AA)
代码审核(CR)
安全测试(ST)
渗透测试(PT)
软件环境(SE)
配置&脆弱性管理(CMVM)
全球领先平均
国际一线金融
2015
2016
2017
HTSC2018

CIS 网络安全创新大会
Cyber Security Innovation Summit

THANKS

姓名 神秘小姐姐

公司 华泰证券

联系方式 hr.security@htsc.com 【信息安全招聘邮箱】