DOIS

2018 | 中国·北京站

DevOps 落地，从这里开始

DevOps 国际峰会

暨 DevOps 金融峰会

指导单位：云计算开源产业联盟 OpenSource Cloud Alliance for IndustRy OSCAR

主办单位：DevOps时代　高效运维社区 GreatOPS Community

2018年6月29日-30日

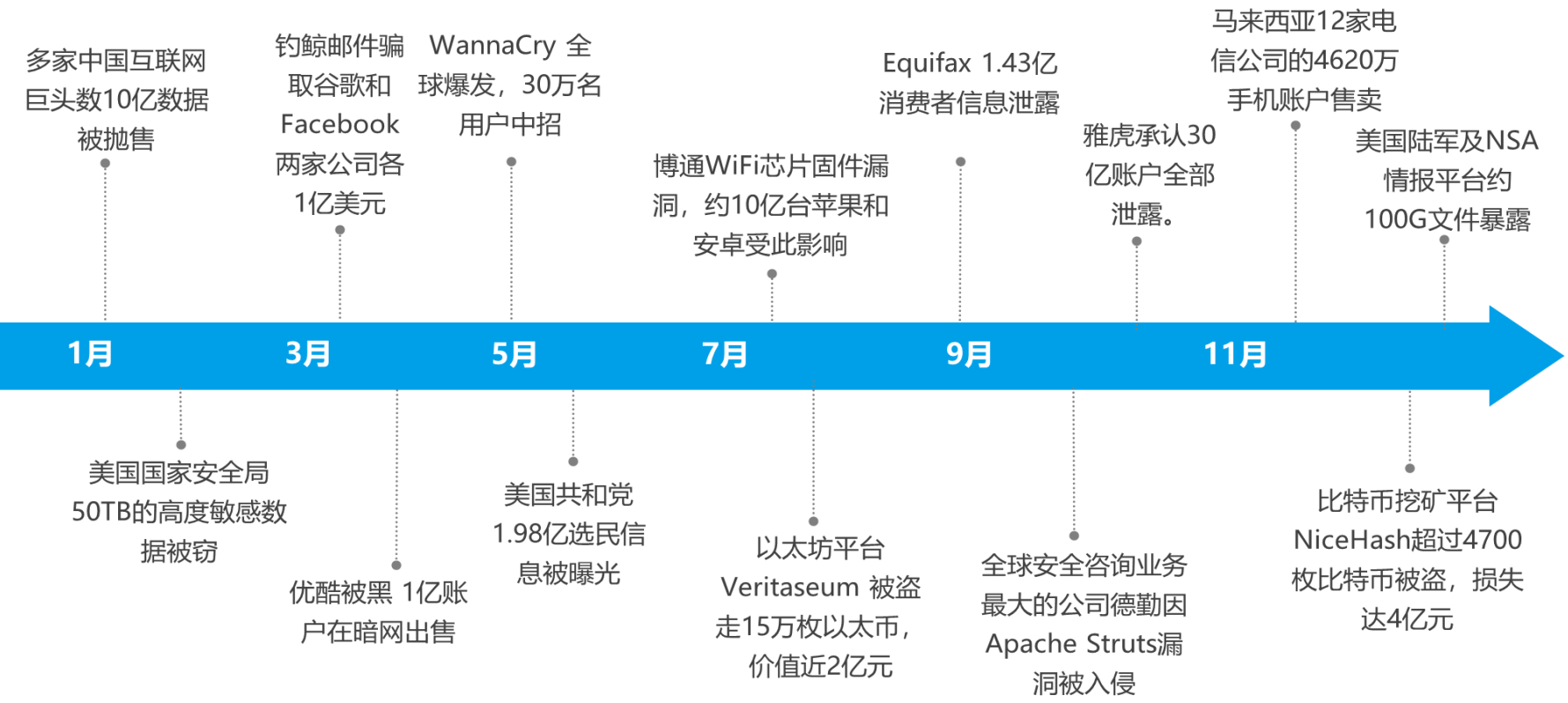
地址：北京悠唐皇冠假日酒店

DOIS

大数据安全分析及DecSecOps在企业落地的探索

北京燃气集团 王广清

2017 重大安全事件追踪



2017 重大安全事件追踪

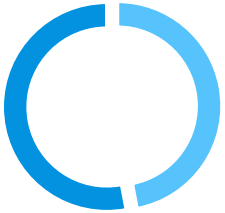
DOIS

51%

企业在过去12个月
发生过数据泄露.

99天

平均探测时间 MTTD
外部通知 107 天
内部发现 80 天



■ 内部发现47% ■ 外部通知53%

48%

企业在过去12个月
至少发生过两起

140

国家运用了网络战

$3.62M

平均每个数据泄露事件造成损失

Forrester Data
Global Business Technographics Security Survey, 2017

CYBERSECURITY ALMANAC | 2018, Momentum Cyber

网络安全法的出台（部分摘录）

DOIS

第五十一条：国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条：建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

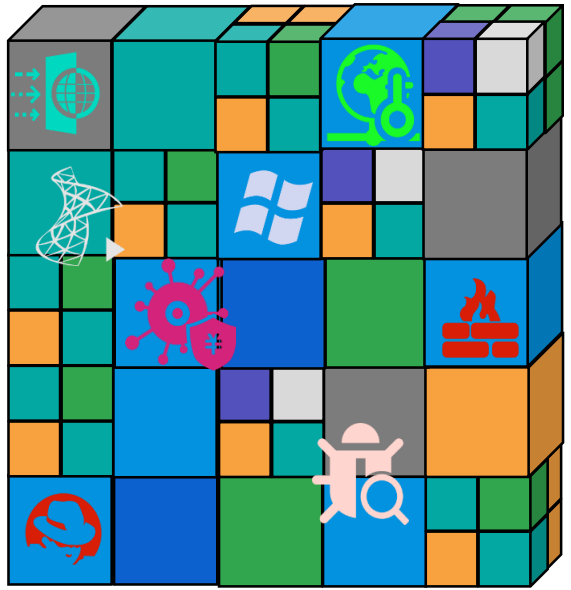
第五十五条　发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估。

IT设备众多，各自为政形成信息安全孤岛

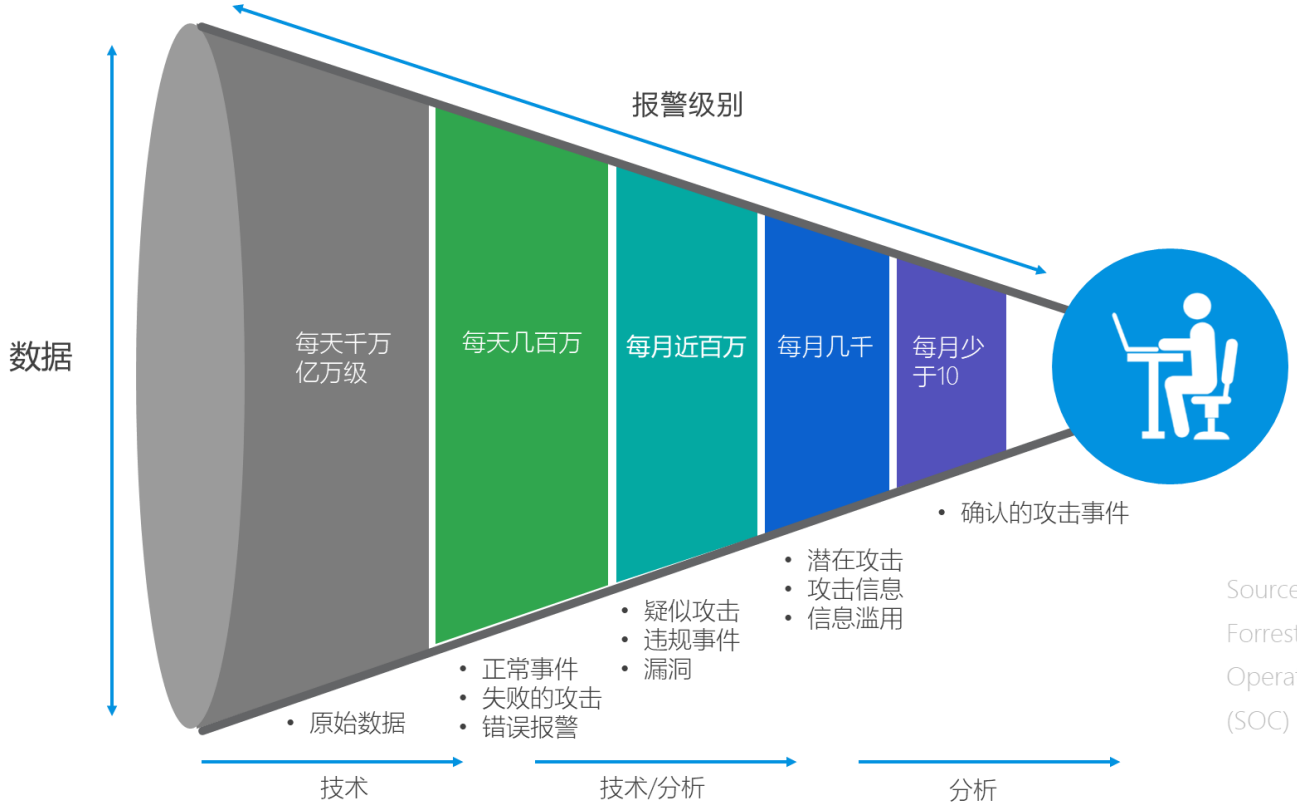
DOIS

单点防护

综合防护壁垒



安全分析人员的困境-事多人少



Source:
Forrester' Security
Operations Center
(SOC) Staffing

人员少，海量数据分析效率低

DOIS


应用系统


主机系统

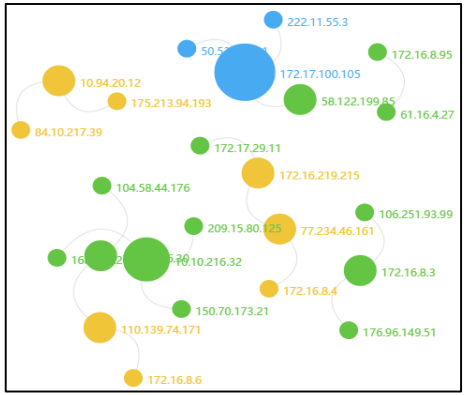

网络设备

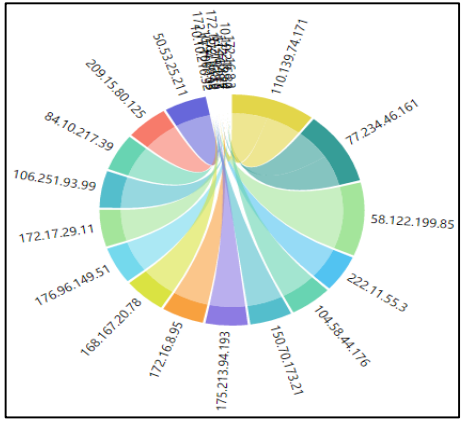

安全设备

日志

流量数据

<11>Feb 18 11:12:23 localhost waf: tag:waf_log_websec site_id:1428395845 protect_id:2442566278 dst_ip:172.17.100.105 dst_port:80 src_ip:50.53.25.211 src_port:28684 method:UNKNOWN domain:None uri:None alertlevel:MEDIUM event_type:HTTP_Protocol_Validation stat_time:2017-02-18 11:12:19 policy_id:1 rule_id:0 action:Block block:No block_info:None http: alertinfo:request method begin with non-capital letters or over load content-lenth proxy_info:None characters:None count_num:1 protocol_type:HTTP wci:None wsi:None

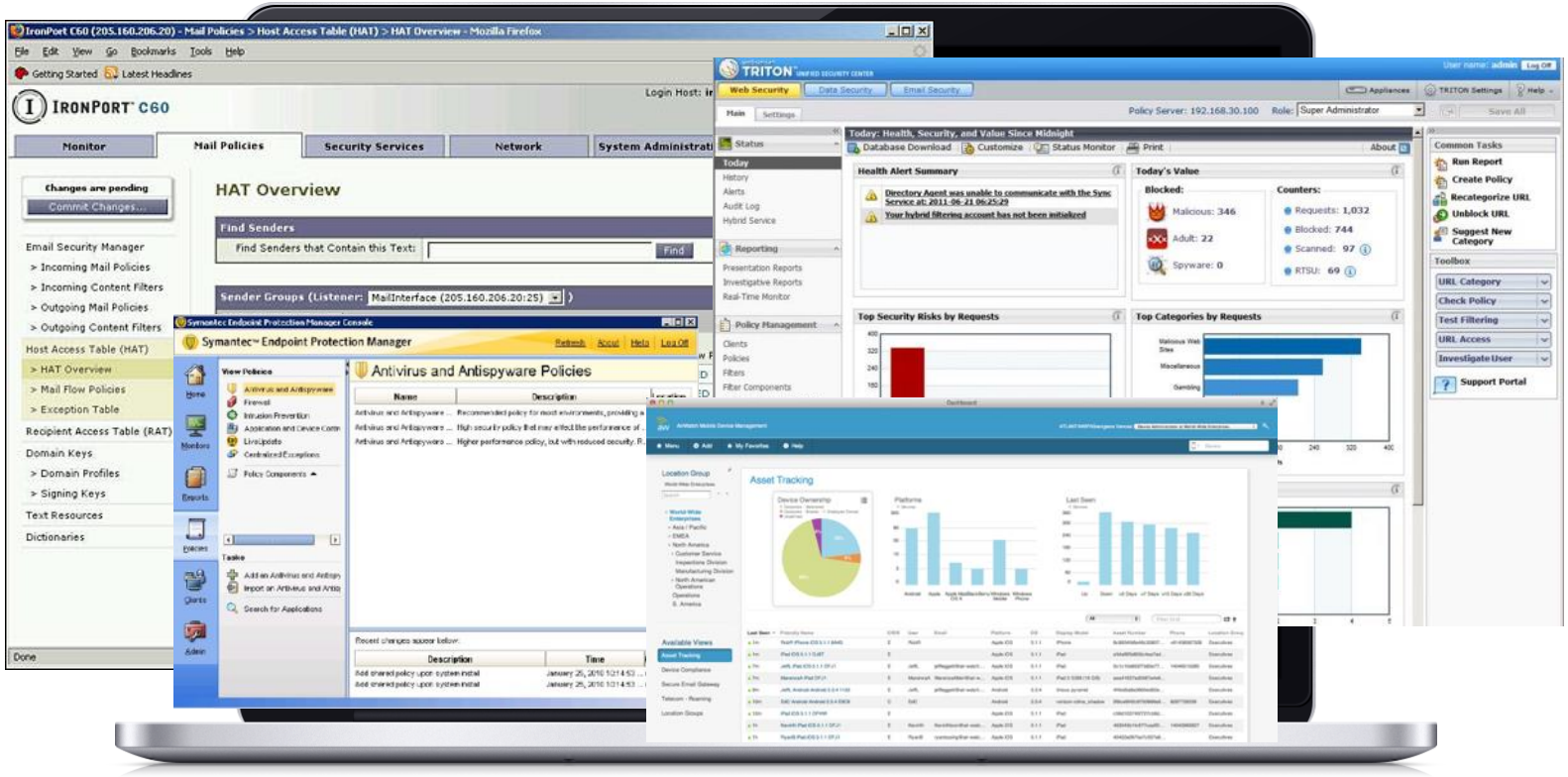




海量数据分析困难　　原始信息晦涩难懂

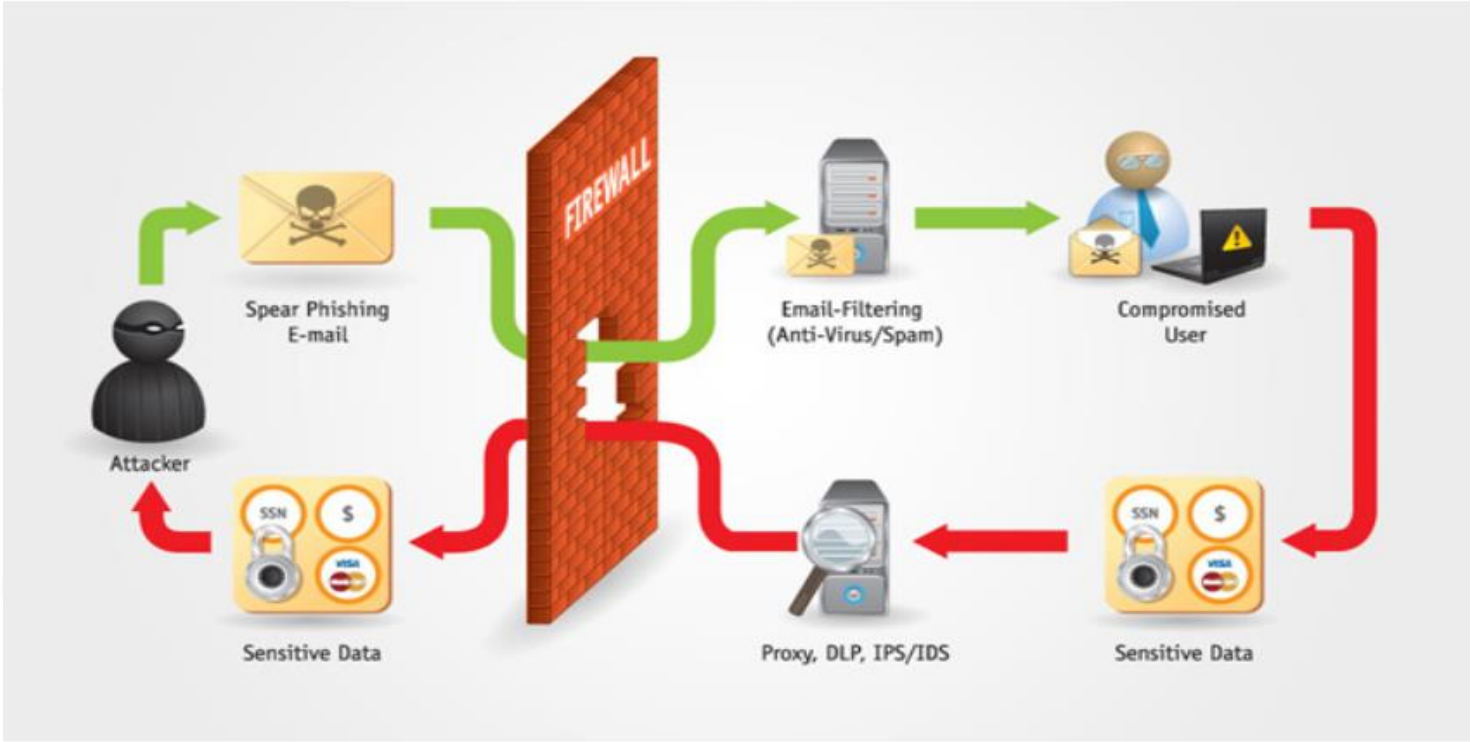
安全分析人员的困境-信息量太多太分散

DOIS



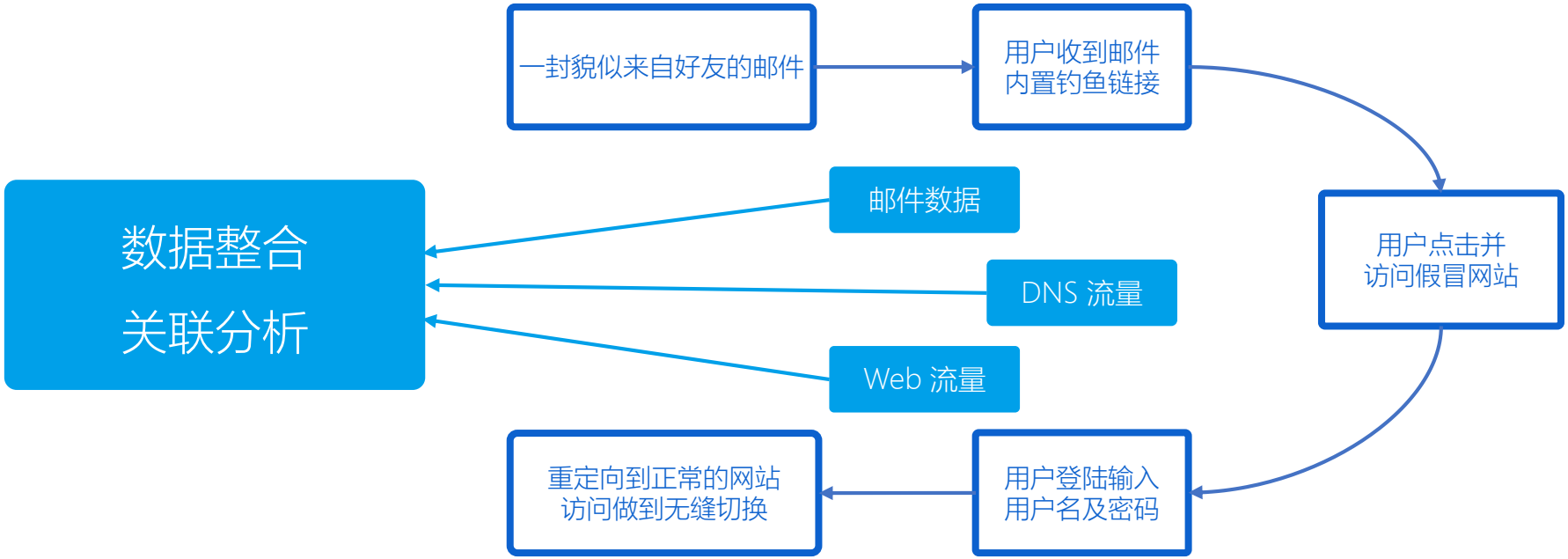
高级威胁-典型的钓鱼攻击

DOIS



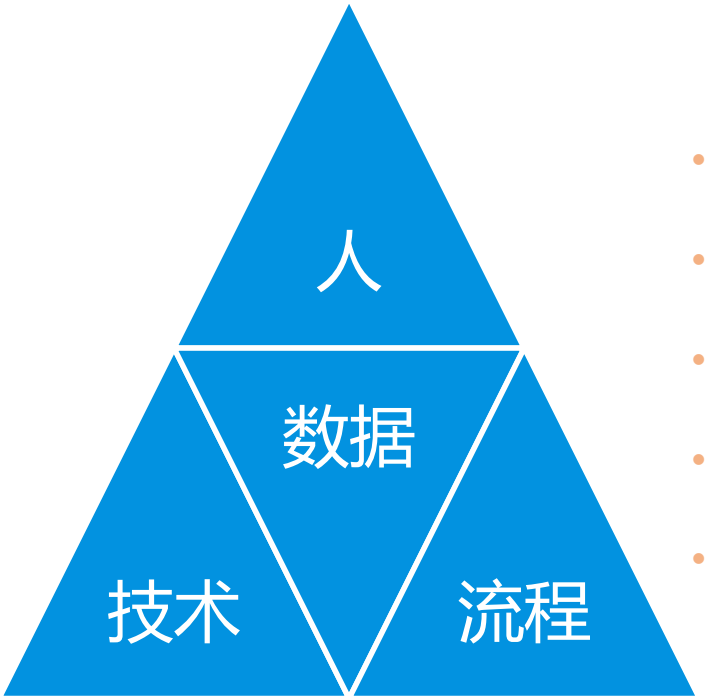
钓鱼深度攻击解析

DOIS



安全智能重在整合

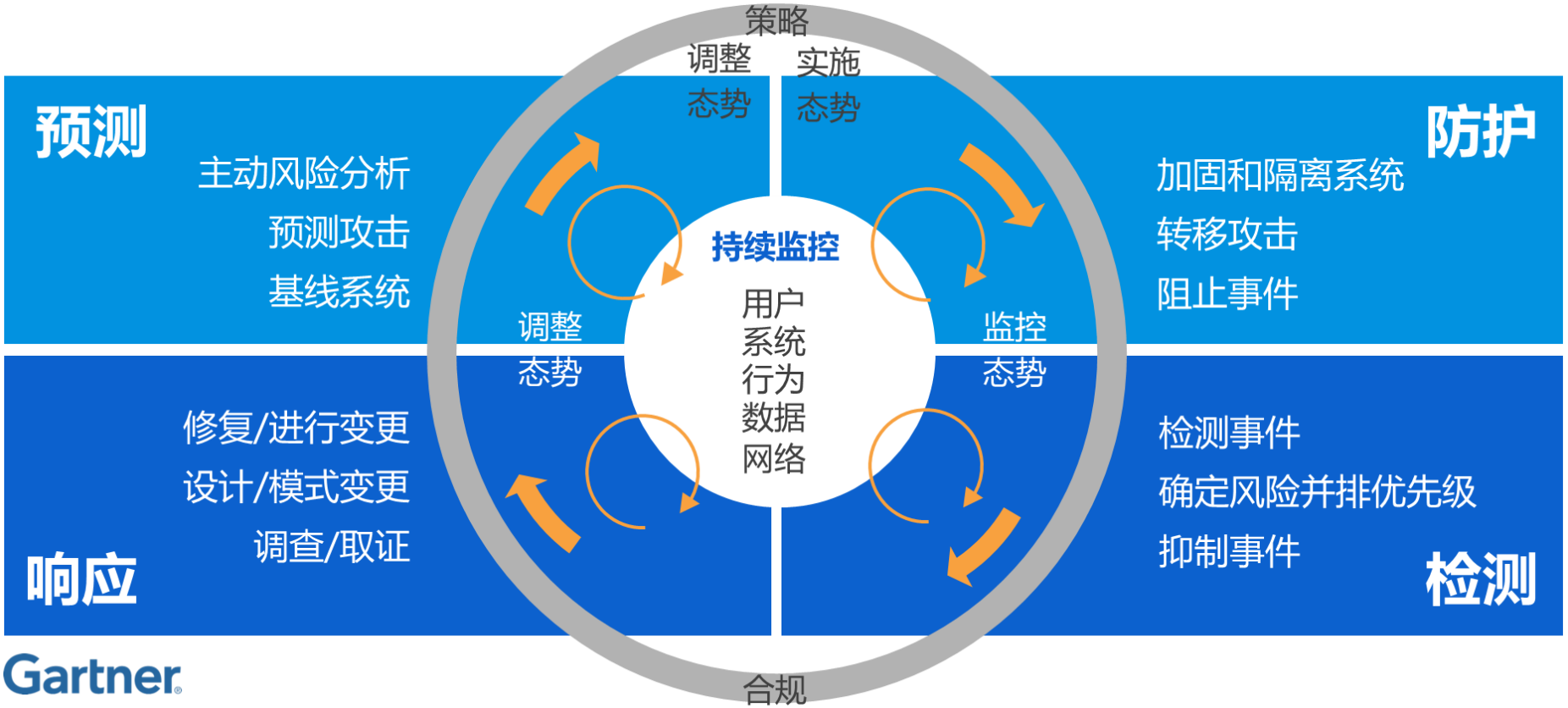
DOIS



- 监控预测
- 关联分析
- 告警排序
- 应急响应
- 溯源取证

安全自适应架构

DOIS

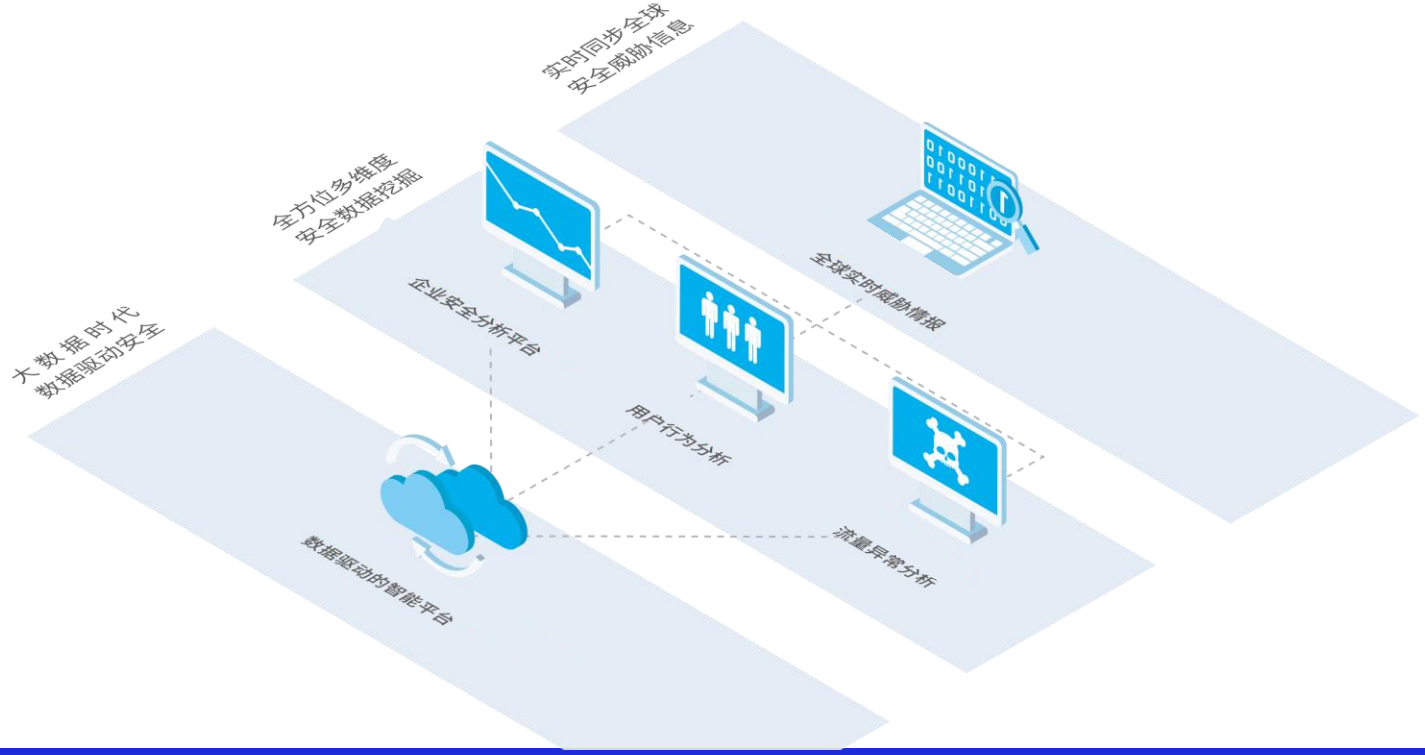


Gartner

新一代安全建设体系

DOIS

数据驱动的智能平台，基于人工智能、大数据分析等技术，提供安全事件自动感知、智能分析、应急响应、辅助决策。



安全运营中心发展历程

DOIS

2000年以前 SIM/SEM/SIEM

- SIM关注于内控，重视合规性需求
- SEM则关注于威胁行为监控，安全事故应急处理，偏重于安全本身

2000年 SOC1.0

- 以资产为核心
- 安全事件管理为关键流程
- 安全域划分的思想，建立一套实时的资产风险模型
- 协助管理员进行事件分析、风险分析、预警管理和应急响应处理的集中安全管理系统

2009年 SOC2.0

- 以业务为核心的、一体化的安全管理系统
- 体系设计方面围绕业务的功能设计
- 技术支撑方面面向业务链的信息收集;
- 实施过程中面向业务的实施和运维过程

2014年 大数据SOC

- 基于大数据存储计算
- 准实时大规模异常检测
- 机器学习
- 威胁情报共享
- 基于用户异常行为分析
- 全流量分析
- 安全态势感知

安全运营中心的职责

DOIS

职责	细化
调查与分析	① 负责日常信息安全运行状况监控 ② 负责信息安全事件的分析和调查取证
报告与沟通	① 负责信息安全检查和信息安全通报 ② 负责等级保护工作的定级、备案、检查、测评和督促整改（合规）
响应与改进	① 负责处理信息安全突发和重大事件 ② 负责信息安全运行体系建设与完善 ③ 培养信息安全专家和骨干力量

建设目标

DOIS

目标1—安全运营体系化

- 规划安全运营团队，设定相应的运营岗位，细化职责分工
- 规范化安全运营管理的操作规范、流程，并形成常态化的工作
- 制定安全运营管理规范，标准化安全运维操作

目标2—安全运营平台化

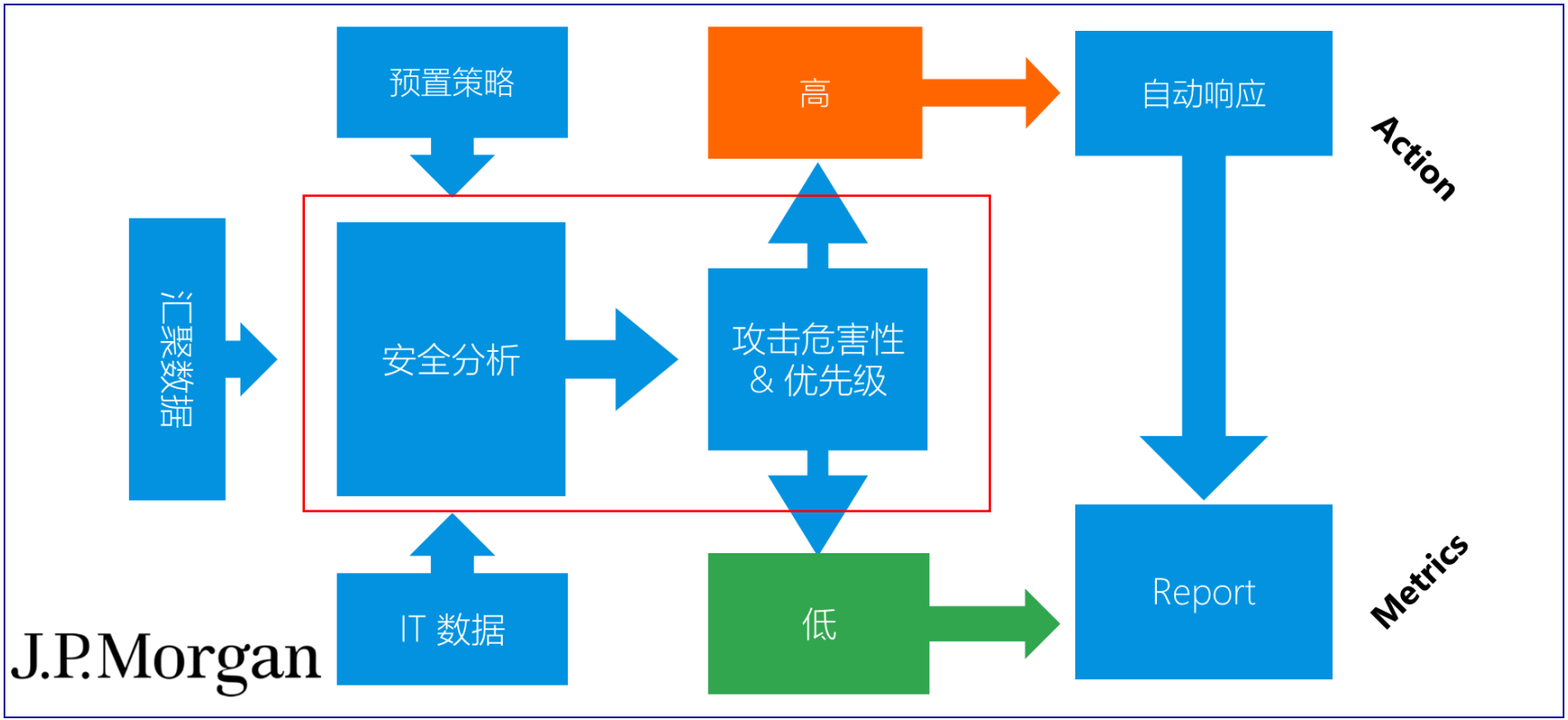
- 分析管理层和业务部门安全管理需求，设计安全告警规则
- 明确安全运营监控范围，收集分析各类安全运营数据
- 建设SOC技术平台，使技术、流程和人员三者有机结合，可实施落地

目标3—安全运营可视化

- 根据管理层和业务部门安全管理需求，设计各类安全运营报告
- 针对安全运营流程和安全事件处理流程，设计安全管理流程报告
- 生成各类报表，综合分析安全状态和安全趋势，定期向管理层汇报

企业应如何建立智能安全运营中心

DOIS



建设原则

DOIS

分阶段建设，快速见效；

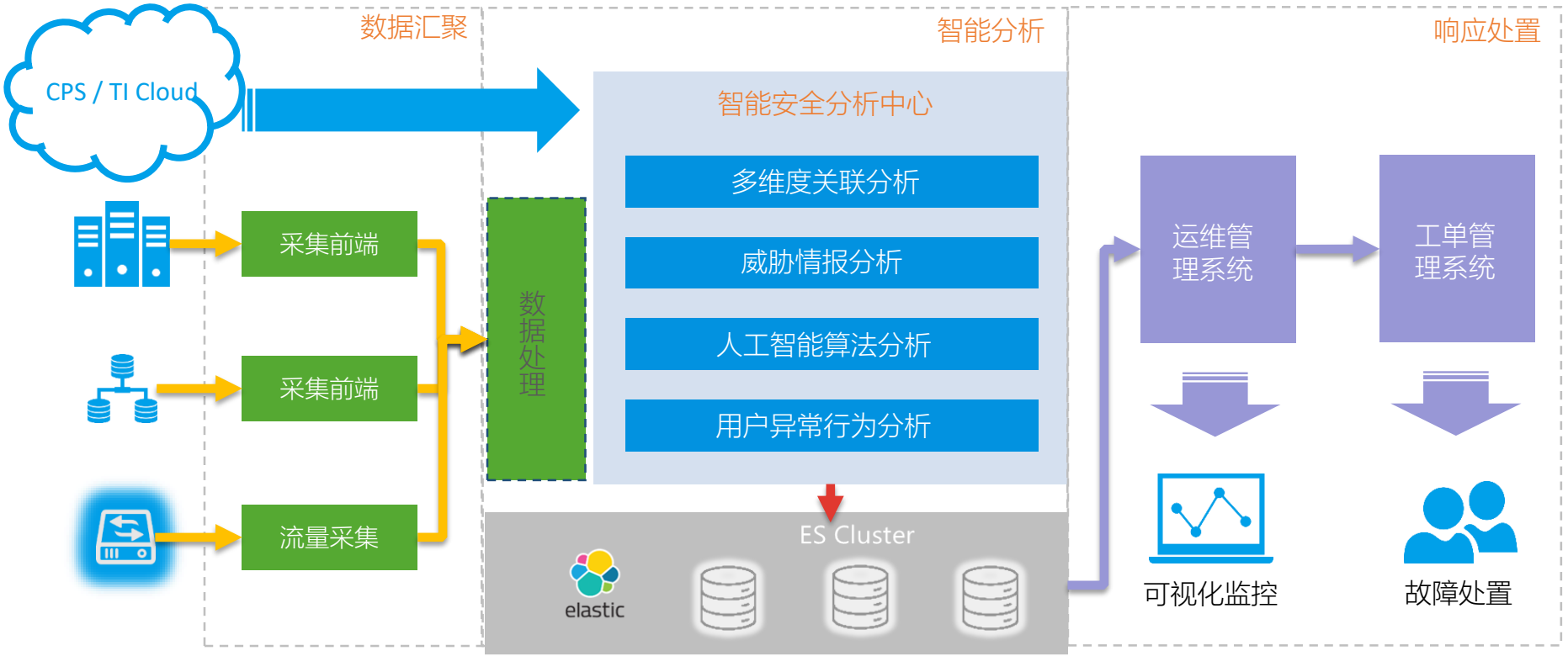
长远规划，逐步建成；

符合国家信息安全标准和技术规范要求；

可灵活扩展和快速功能迭代；

安全运营中心智能安全分析平台架构

DOIS



安全事件分级

DOIS

安全事件分类	系统损失	社会影响
特别重大事件（Ⅰ级）	会使特别重要信息系统遭受特别严重的系统损失	波及到一个或多个省市的大部分地区，极大威胁国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者严重损害公众利益。
重大事件（Ⅱ级）	会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失；	波及到一个或多个地市的大部分地区，威胁到国家安全，引起社会恐慌，对经济建设有重大的负面影响，或者损害到公众利益。
较大事件（Ⅲ级）	会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、一般信息信息系统遭受特别严重的系统损失；	波及到一个或多个地市的部分地区，可能影响到国家安全，扰乱社会秩序，对经济建设有一定的负面影响，或者影响到公众利益。
一般事件（Ⅳ级）	会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失；	波及到一个地市的部分地区，对国家安全、社会秩序、经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益会造成损害。
特别重大事件（V级）	会使特别重要信息系统遭受特别严重的系统损失	波及到一个或多个省市的大部分地区，极大威胁国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者严重损害公众利益。

安全事件分类

DOIS

参考标准： GB/Z20986（信息安全技术信息安全事件分类分级指南）；
安全事件分类：操作记录事件、状态信息事件、有害程序事件、网络攻击事件、信息破坏事件、违规行为事件六大类。

安全事件分类	描述说明
操作记录事件	记录各种操作事件，包括访问、配置变更、软件安装、申请、设备操作命令等；
状态信息事件	系统、应用、网络等日常运行、自身维护、管理资源产生的事件。如进程变化、服务启停、普通流量、CPU内存、硬件状态等。
有害程序事件	计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件等7个子类。
网络攻击事件	拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件等7个子类。
信息破坏事件	信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件等6个子类。
违规行为事件	包括人、应用、网络发生的违规操作、访问等异常行为事件。

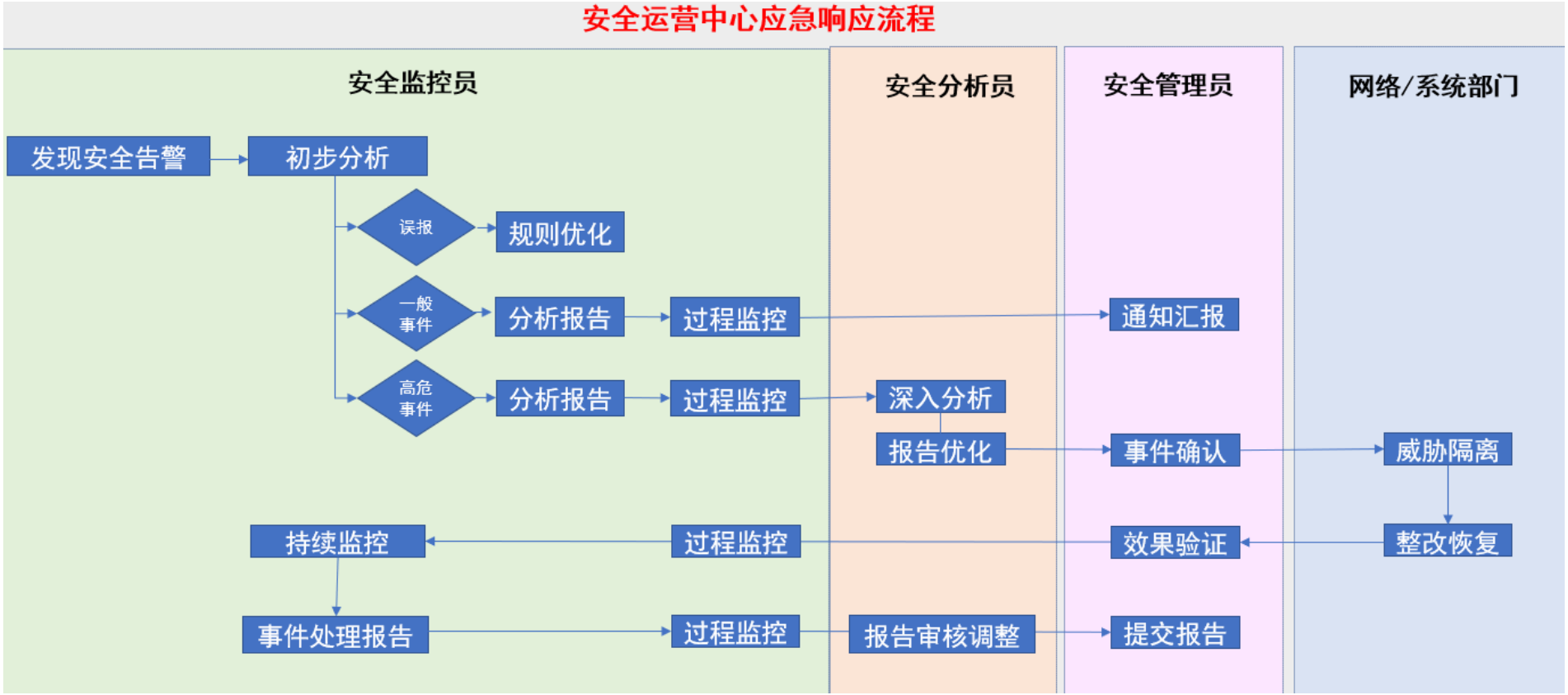
安全运营中心安全人员能力培养

DOIS

序号	培训时间	培训对象	岗位所需能力	培训内容
1	平台建设前期	安全管理人员	中心日常管理能力	CISP培训 ISO27001培训 信息安全风险管理课程 信息安全等级保护工作业务认证课程
2	平台上线前	安全监控人员	安全事件监控及应急响应能力	ISO27001培训
3	平台上线前	安全分析人员	安全事件分析能力	CISP/CISA培训 产品培训 黑客攻防培训 等级保护工作业务认证课程
4	平台上线前	安全响应人员	应急响应处理能力	CISP/CISA培训 产品培训 黑客攻防培训 信息安全风险管理课程 等级保护工作业务认证课程
5	平台上线前	平台运维人员	平台管理运维能力	安全运营中心平台管理运维培训

安全运营中心应急响应流程

DOIS



案例-针对集团邮件网站的webshell上传攻击事件

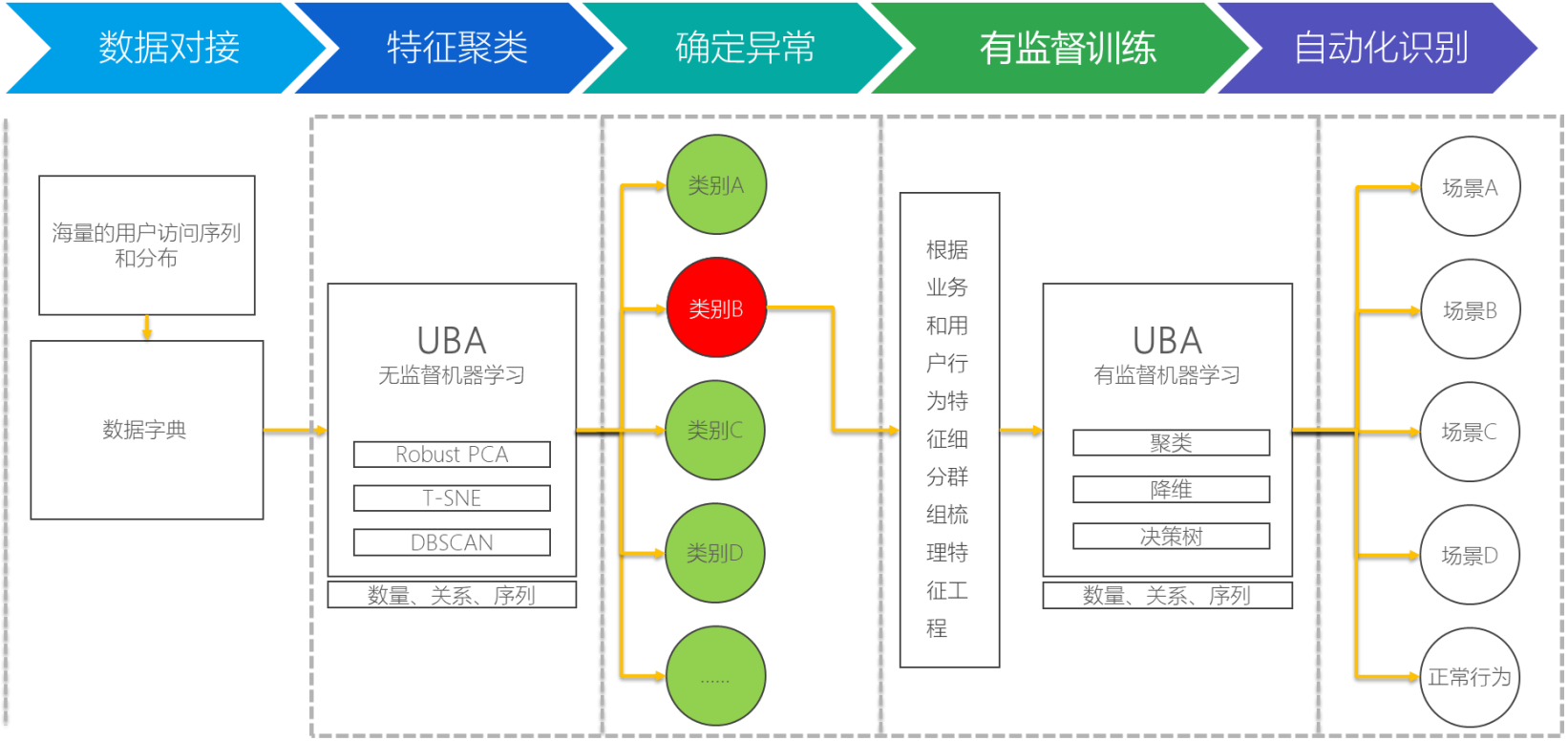
22:23:30大数据分析平台告警【webshell上传攻击】；排查发现目的IP为邮箱服务器地址，安全监控员初步判定为针对集团邮箱网站的恶意攻击事件，升级为【高危事件】启动应急响应流程：

1. 网络管理员2分钟内完成封禁攻击源IP；
2.服务器管理员5分钟内完成临时隔离邮箱服务器；
3.分析人员20分钟到达现场分析事件影响范围；

总结：从平台22:23:30发现攻击事件，到22:53:30完成处理，共耗时30分钟，成功防范了针对集团邮件业务的网络攻击,避免了集团邮件信息的泄露，有效保障了集团邮件业务的运行。

算法在智能安全分析平台中的应用

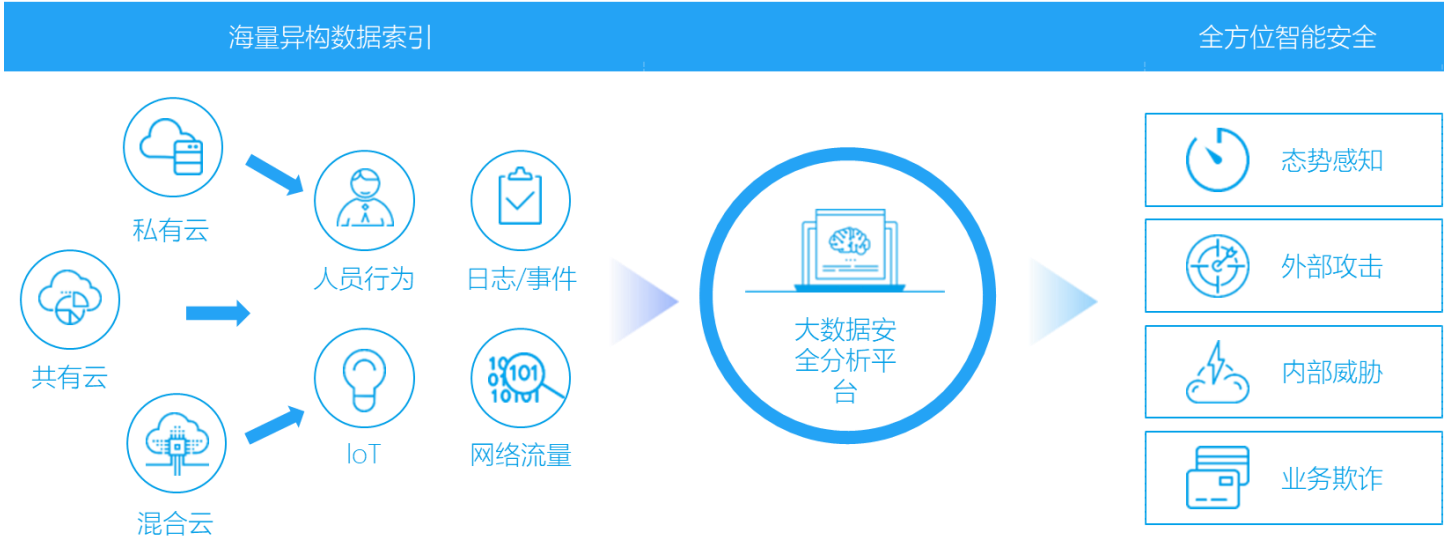
DOIS



解决了哪些问题

通过采集与分析企业内外部海量异构数据，利用大数据技术、实现安全策略由“被动防御”转向“主动智能”，满足合规监管诉求，实现全方位安全态势感知，抵御外部攻击、内部威胁和业务欺诈。

智能分析——让安全可见、可知、可控



取得的成果

DOIS

大数据安全智能分析平台中的规则检测引擎、用户行为分析引擎、威胁情报分析、流量分析引擎、机器学习引擎5大引擎来检测和发现网络中存在的5大类400多种外部攻击行为和内部违规行为，其准确高达85%以上。

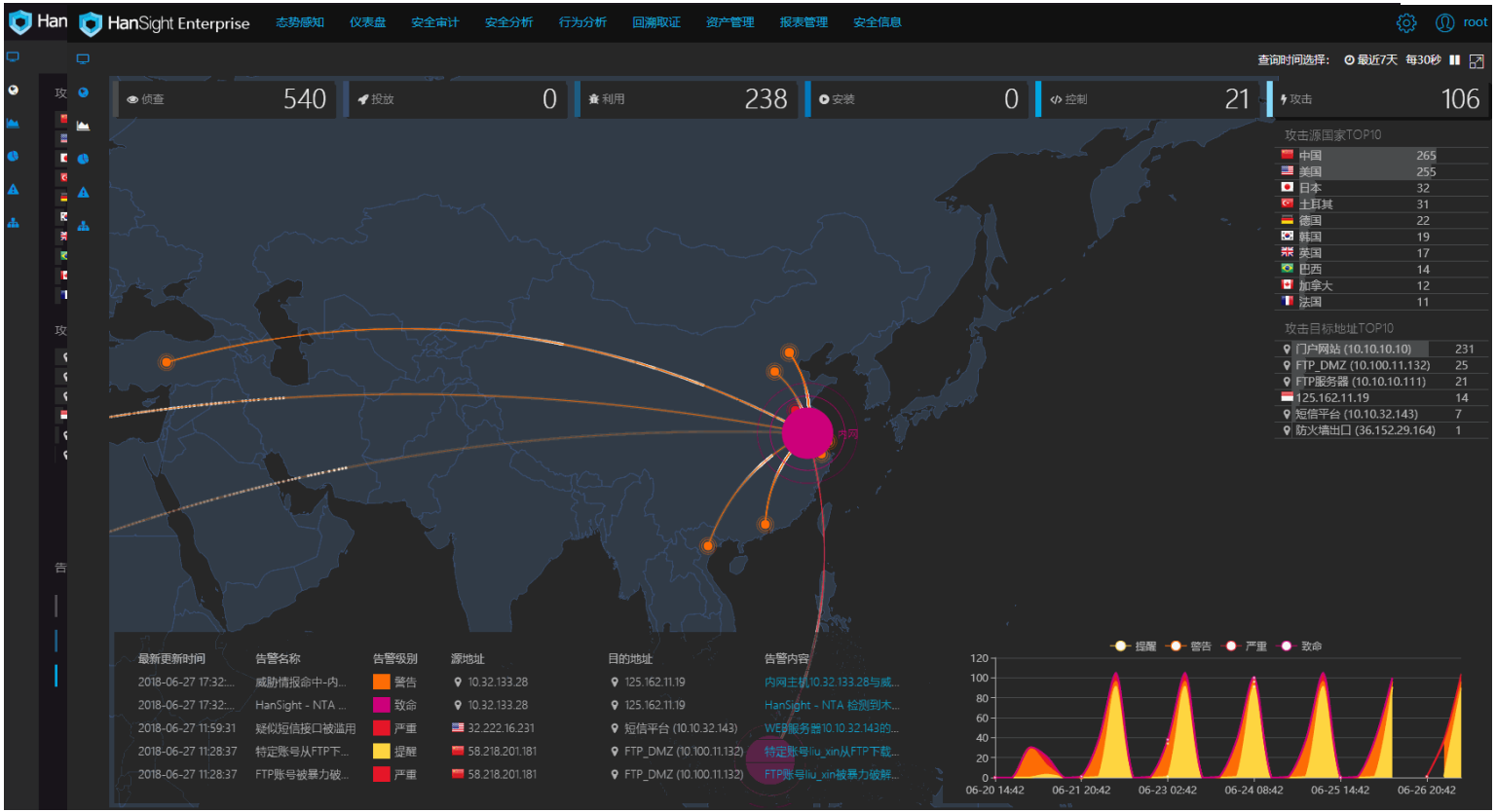
截至到2018年初，收集58T安全日志数据、720次安全事件的收集，集中处置高危事件9起，确保了集团系统的安全稳定运行。

安全风险态势感知

DOIS

- 3D态势
- 外部态势

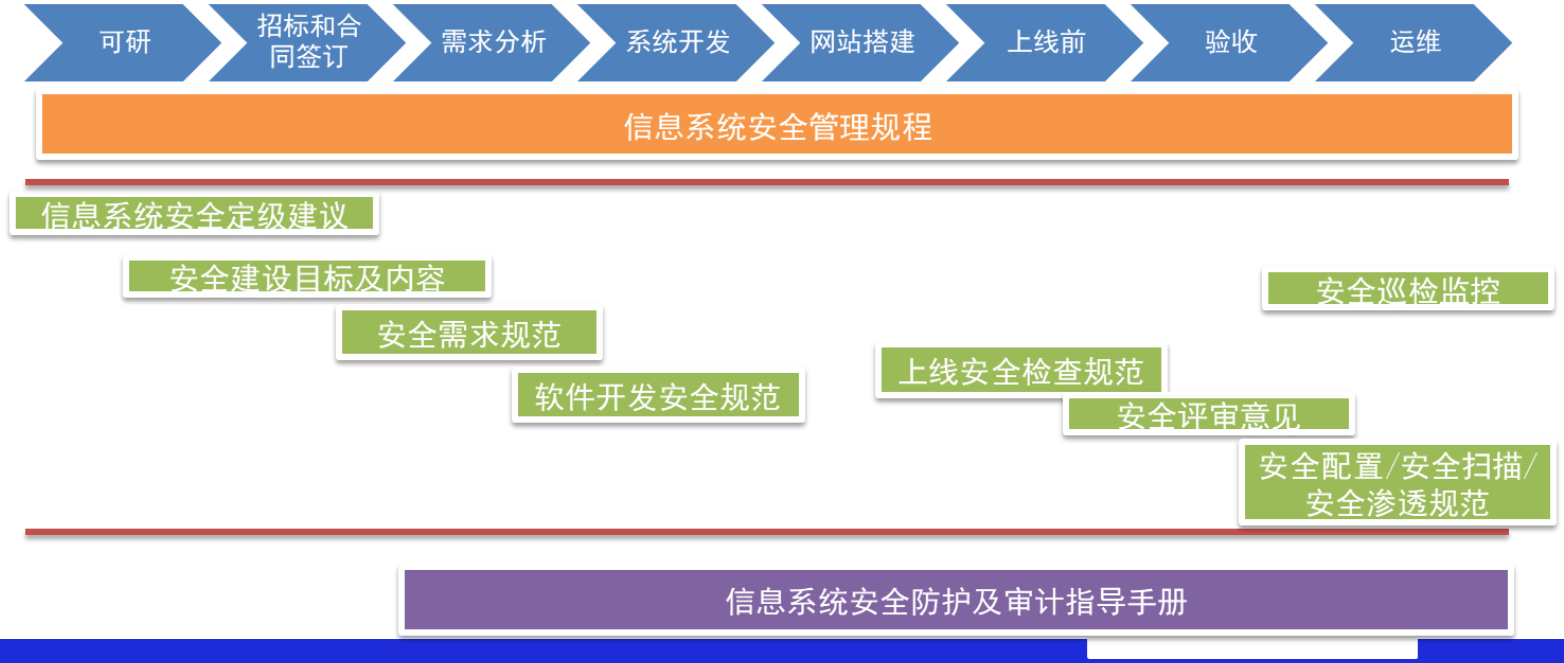
演示数据



对信息系统进行全生命周期安全管理

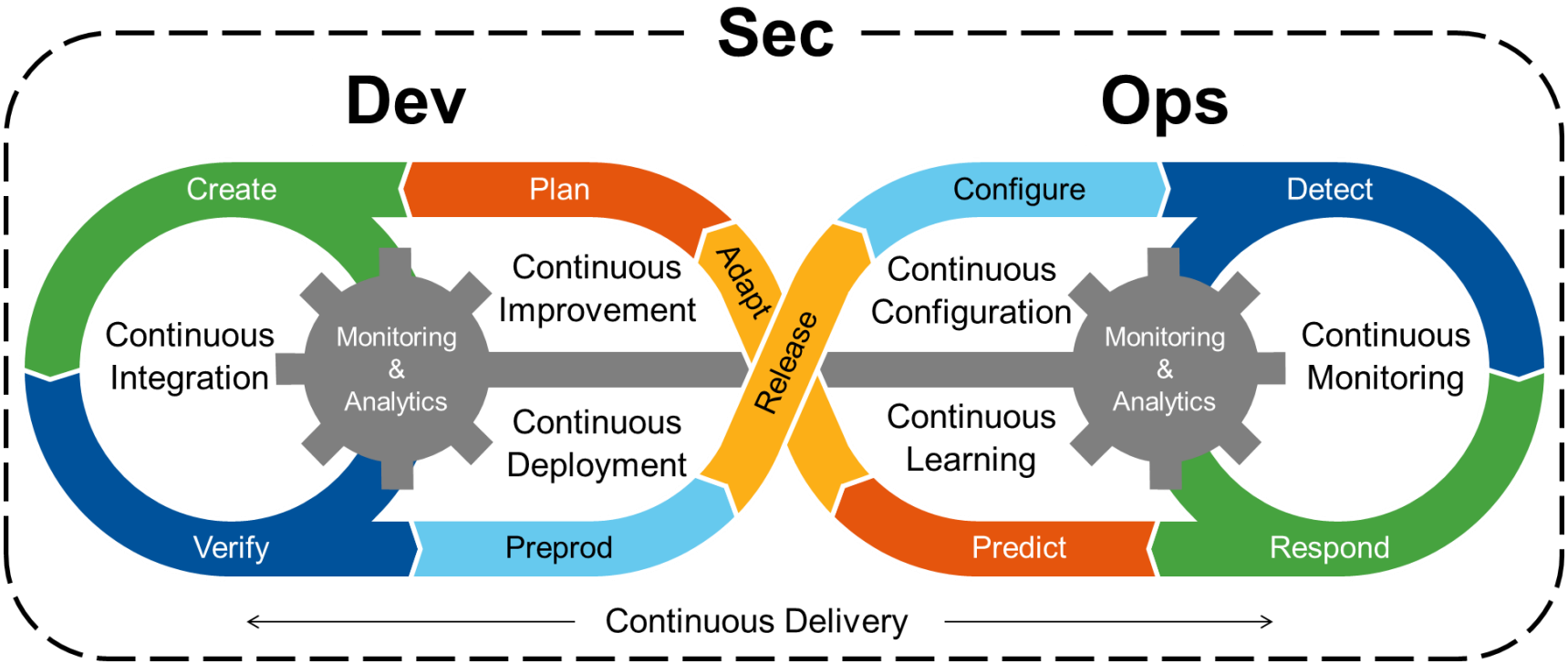
DOIS

信息安全工作以**风险评估**为依据，抓住信息安全工作重点，将信息安全工作落实到信息系统全生命周期中，与信息系统**同步规划、同步建设、同步运行**，实现信息安全的全面防御。



DevSecOps定义：将安全无缝集成到DevOps中

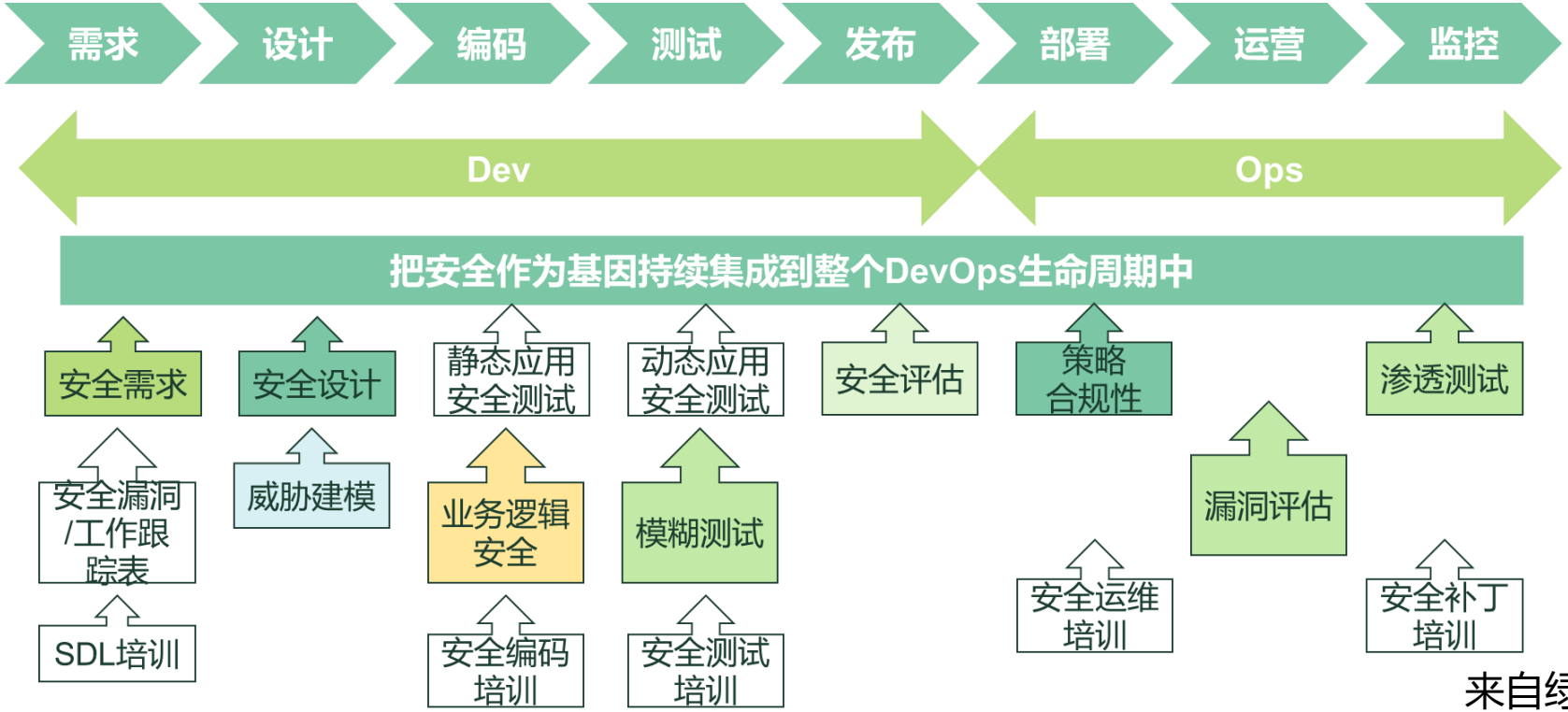
DOIS



来自Gartner

DevSecOps视角下的应用全生命周期安全管理

DOIS

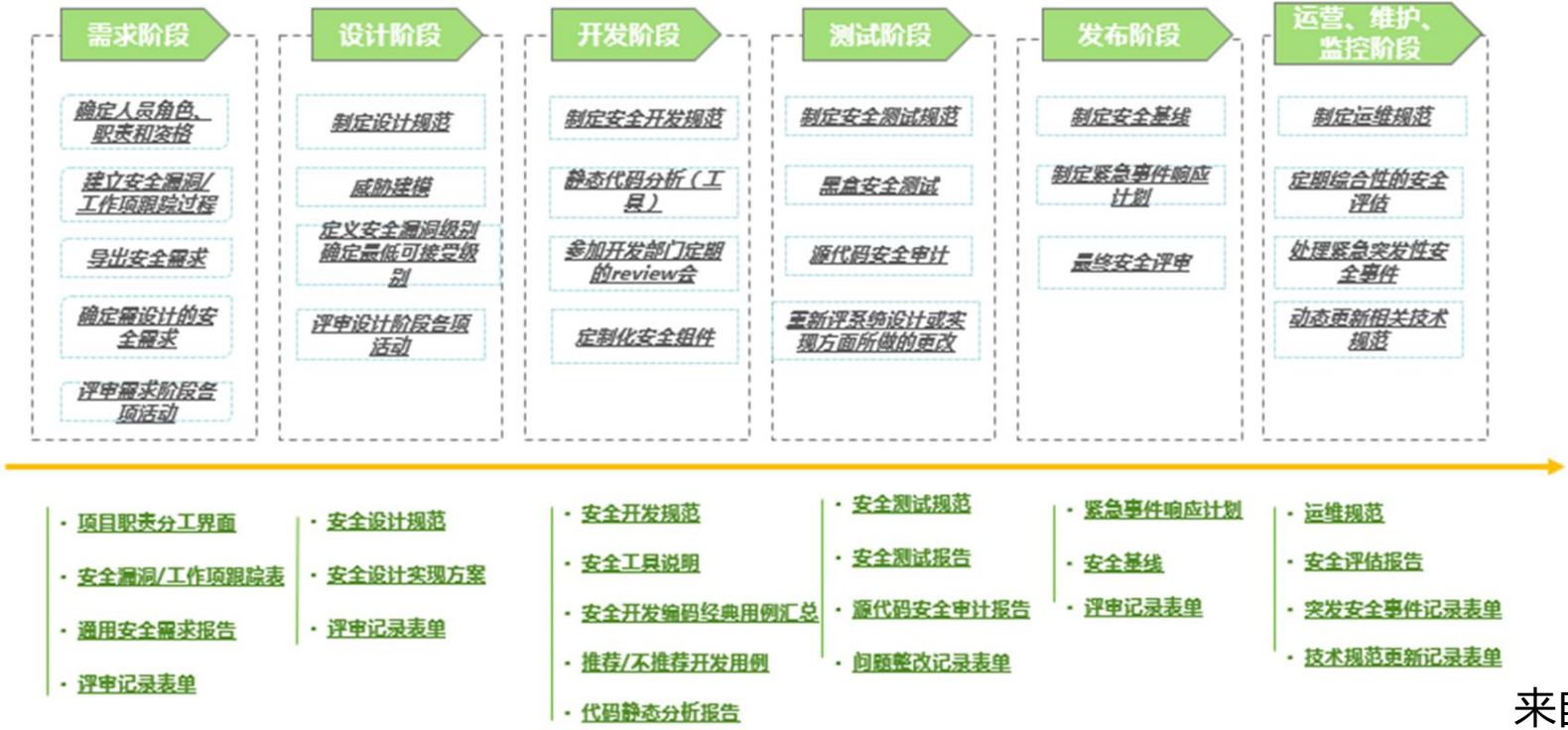


来自绿盟

DevSecOps实施方法论

DOIS

从DevSecOps现阶段的发展来说，要将DevSecOps理念抽象出来形成具体的办法实施，不能一蹴而就，更多的是选择生命周期中最需优化的点来逐步建设



来自绿盟

DOIS

Thanks

DevOps 时代社区 **荣誉出品**

DOIS

想第一时间看到高效运维社区的新动态吗?