2024 WEST LAKE DIGITAL SECURITY CONFERENCE 西湖论剑·数字安全大会 12th

智绘安全X 乘数而上 INTELLIGENCE ENHANCE SECURITY ADVANCING WITH DIGITALIZATION

安全运营实践分享

朱志伟

三棵树涂料股份有限公司

目 录
CONTENTS

01 三棵树集团介绍

三棵树集团介绍

- **2002年**诞生于妈祖故里福建莆田，2016年登陆上海证券交易所在A股主板上市（股票代码：603737），成为中国主板上市的民用涂料第一股。现已成为**中国涂料第一品牌**、北京2022年冬奥会和冬残奥会官方涂料独家供应商，全球建筑装饰涂料行业第8位。

- 在上海、北京、广州设立**3个中心**，并在福建、四川、河南、天津、安徽、河北、广东、湖北等设有及在建**13个生产基地**；已成为**全资及控股33家公司**的企业集团，现有员工**近10000名**，在全球拥有**近30000家合作伙伴**。独具特色的“道法自然”生态文化和被誉为“醉美企业”的生态园区，每年吸引数万人前来参观学习和交流。

- 自成立以来，三棵树始终关注人类美好生活和家居健康，践行“ 让家更健康、让城市更美丽、让生活更美好” 的使命，致力于在工程领域打造绿色建材一站式集成系统。因此在发展的过程中积极拥抱数字化，利用科技帮助业务进步。

三棵树集团发展历程

三棵树文化哲学源于中国老子《道德经》思想——道法自然
三棵树文化的核心就是处理好企业与生态环境、企业与社会、企业与个人、企业自我发展的关系

品牌起步阶段（2002—2006）

- 三棵树品牌诞生
- 第一条涂料生产线完成
- 第一支产品“金叶墙面漆”诞生
- 第一个倡导“健康漆”概念的涂料品牌
- 第一支广告《小鸟篇》投入央视并获第八届福建优秀广告影视类唯一金奖
- 成为“神六搭载涂料品牌“
- 荣获“中国名牌” “国家免检产品”

高速发展阶段（2007—2011）

- 发行企业文化书籍《道法自然•三棵树生态文化》
- 成为“神七搭载涂料品牌”
- 夺得央视年度黄金广告资源“中国建材行业第一标”
- 获评“国家认定企业技术中心” “中国驰名商标” “消费者最喜爱的绿色商标”
- 洪杰董事长荣获“2007年福建经济年度杰出人物”称号
- 15层智能化办公大楼落成并全面启用

跨越发展阶段（2012—2016）

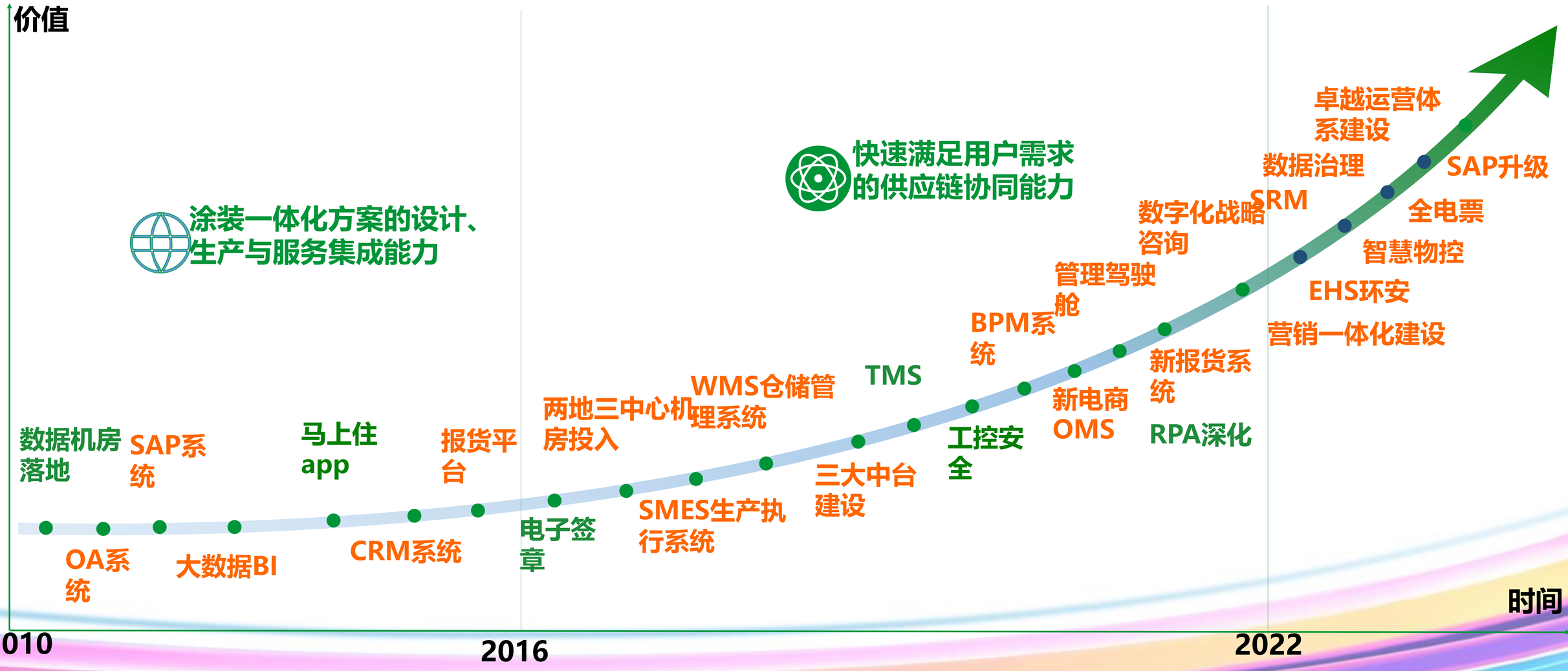
- 时任国务院总理温家宝莅临三棵树考察
- 洪杰董事长当选第十二届全国人大代表
- 首创“健康+”五项新标准，系列“健康+”产品上市
- 获评“国家级绿色工厂” “国家认可实验室” “福建省政府质量奖”
- 聘任诺贝尔化学奖得主杰马里·莱恩教授为首席技术顾问
- 文化升级，发行《道法自然•三棵树生态文化》
- 在上海A股主板上市，成为“中国民用涂料第一股”

高质量发展阶段（2017—至今）

- 成立上海、北京、广州中心和全球研发中心，布局全球战略
- 2019年两会期间，习近平总书记亲切接见洪杰董事长
- 洪杰董事长被党中央、国务院授予“全国脱贫攻坚先进个人”
- 并购大禹防水、廊坊富达新型建材公司、江苏麦格美节能科技公司
- 成为北京2022年冬奥会和冬残奥会官方涂料独家供应商
- 2021年位居全球建筑装饰涂料第8位
- 2021年全球涂料上市公司市值排名第8位

三棵树集团数字化介绍

为满足消费者需求持续打造新型能力，满足用户需求的供应链协同能力；
三棵树一直在数字化转型的路上前进



三棵树集团网络安全蓝图介绍

信息安全风险应对

制定信息安全方针政策并明确组织架构及善职责分工

加强信息安全意识和事前预防性管控，提升安全管理水平

建立完善的管理制度和流程，加强IT和安全运维事中管控

完善系统故障及灾难的事后响应和恢复能力

加强安全监控、提升安全防护，有效减小信息安全漏洞和缺陷

规范信息数据分级分类，保护公司关键信息数据安全

信息安全体系建设蓝图框架

信息安全治理

安全战略	治理与组织	政策与标准	度量与报告
信息安全建设规划	安全组织架构与职责	管理制度文档	信息安全管理指标
信息安全方针政策	安全管理人员能力	规范标准文档	定期评估与报告

信息安全运营

信息安全意识	运维管理		资产管理	事件响应
培训计划与形式	变更管理	容量管理	IT资产管理规范	安全事件定义和分类
安全意识考核	故障管理	配置管理	IT资产盘点及自动发现	安全事件跟踪与处置
身份和访问控制	**第三方管理**		**个人信息保护**	**业务连续性管理**
特权帐号管理	第三方管理规范		个人信息识别	业务影响分析
基于角色的授权	第三方评估与审计		隐私保护政策	恢复预案与演练

信息安全技术

威胁情报	软件安全	主机安全		漏洞管理
情报收集	源代码版本和访问控制	配置基线	终端标准化	渗透测试和漏扫
日志分析	开发流程安全	移动MDM	公有云安全	漏洞和补丁管理
安全监控	**网络安全**	**安全架构**		**数据保护**
IT性能监控	网络准入控制	安全需求设计		数据分级分类
SIEM统一安全监控	机房及网络架构安全	安全架构评审		DLP数据防泄漏

IT信息化管理

- IT系统优化
- 管理流程优化
- IT信息化战略规划

业务数据管理

- 数据治理体系规划
- 主数据管理优化
- 数据质量与标准化

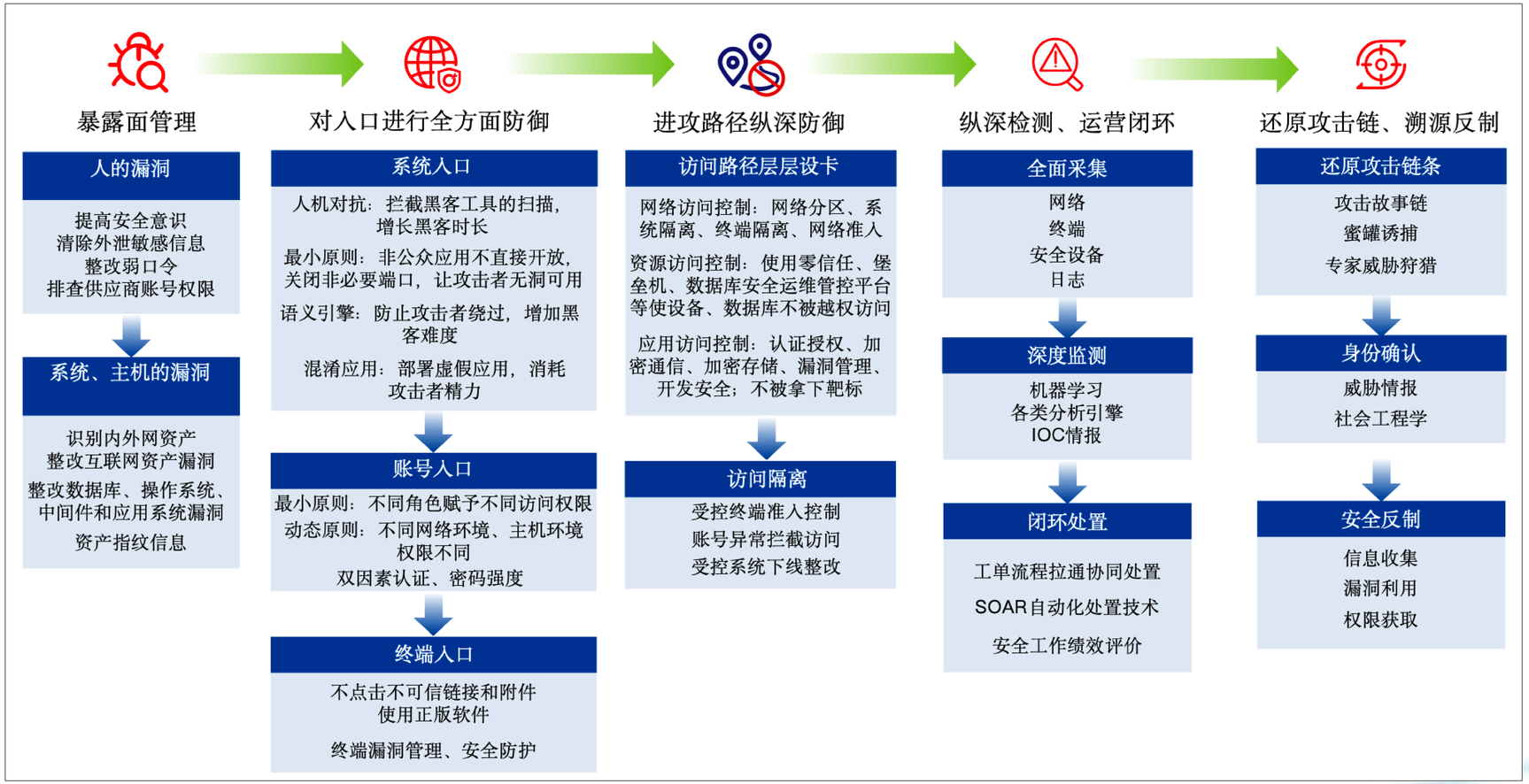
事前预防 | 事中抵御 | 事后应对

02

安全运营工作分享

当前集团安全运营建设思路

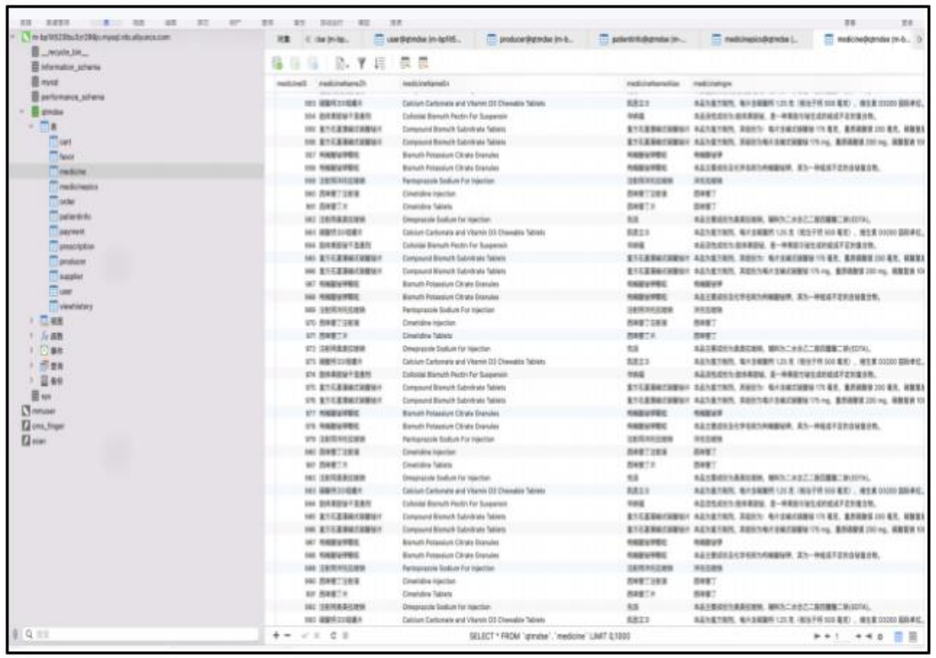
当前三棵树的安全运营建设思路以蓝队视角为主，红队视角为辅
在各环节增加设备和服务能力建设，从各环节避免安全事件的产生

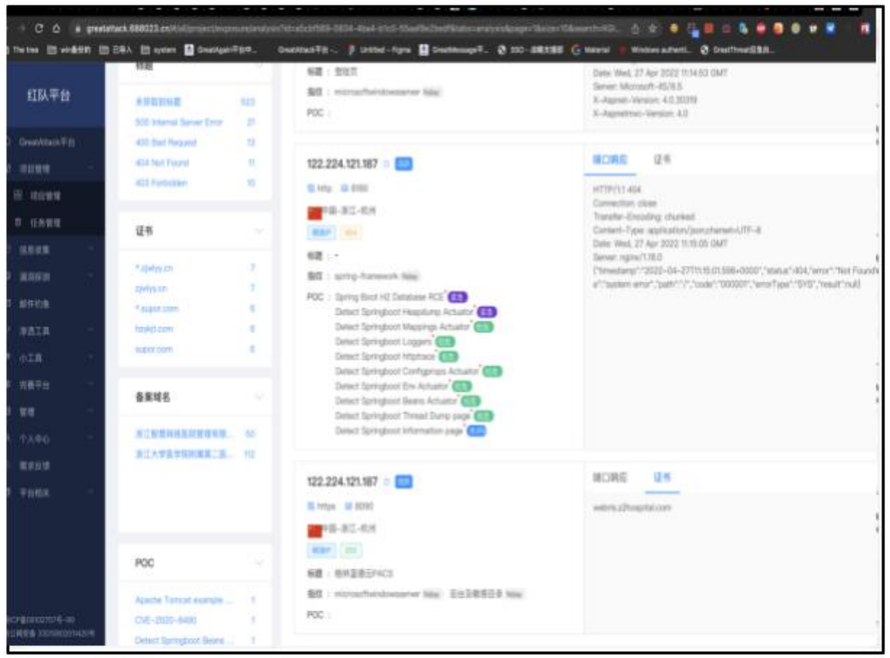


暴露面工作实例

集团多次从攻击者视角出发,有效识别集团内网、外网、云上资产的暴露情况

判断可能存在的影子资产，以及配置错误、漏洞、数据泄漏等多种风险类型，及时进行收敛，缩小攻击入口





漏洞管理工作实例

多次针对近三年被高频使用的漏洞进行检测
实现漏洞管理工作效率和质量的平衡

- fastjson反序列化、struts2远程代码执行、Weblogic反序列化系列
- Microsoft Exchange：CVE-2020-0688、CVE-2021-26855、CVE-2021-26857、CVE-2021-26858 、CVE-2021-27065
- Microsoft Office：CVE-2017-11882、CVE-2019-0604
- Microsoft Windows：CVE-2020-0787、CVE-2020-1472
- Citrix ADC gateway：CVE-2019-19781
- Atlassian Confluence：CVE-2019-3396、CVE-2019-11580、CVE-2021-26084
- Pulse Secure: CVE-2019-11510、CVE-2021-22893、CVE-2021-22894、CVE-2021-22899、CVE- 2021-22900
- Accellion FTA：CVE-2021-27101、CVE-2021-27102、CVE-2021-27103、CVE-2021-27104
- Telerik Ui For Asp.net Ajax ： CVE- 2019-18935
- Vmware Vcenter Server：CVE-2021-21985
- Debian Drupal Core Multiple：CVE-2018-7600
- Fortinet Fortios : CVE-2018-13379、CVE-2020-12812、CVE-2019-5591
- MobileIron Monitor And Reporting Database：CVE-2020-15505
- OA系统：泛微、蓝凌、致远、金蝶

威胁诱捕工作实例

搭建动态、沉浸式欺骗诱捕网络，诱导攻击进入诱捕环境，迷惑、干扰攻击者收集情报。

蜜饵

感知型、反制型蜜饵：伪造攻击者感兴趣的资源、数据，投放在公网、主机或邮箱上。

引诱型蜜饵：在主机或蜜罐上生成伪装数据，例如浏览器缓存等，引诱攻击者攻击蜜罐。

流量转发Agent

安装轻量级Agent代理，混合进真实业务系统中，将指定设备的指定端口**流量牵引**至蜜罐中

流量黑洞

流量黑洞节点能够占用指定地址段内任何空闲IP，**扩大诱捕**范围。

蜜罐

（**60多**种通用型+**5**种5G网元+**6**种物联网蜜罐）

WEB服务：OA、Zabbix、Nginx、Jboss、Tomcat…

数据库：MySQL、MongoDB、Redis、Oracle…

系统服务：SSH、Samba、VPN、RDP、扫描检测…

操作系统：Windows、Centos…

中间件：Weblogic、Tomcat…

综合型服务：WordPress、Mongo、Web克隆…

5G网元：UDR、SMF、AMF、UPF、NRF

物联网蜜罐：Trendnet路由器、Dlink摄像头…

漏洞事件蜜罐：SonarQube、Log4j2

工控蜜罐

克隆影子业务系统


影子系统


真实系统

预置漏洞

Gitlab任意文件读取漏洞
PostgreSQL高权限命令执行漏洞
Struts2 S2-057远程命令执行漏洞
……

自定义伪装

支持用户自定义配置登录页标题、web界面背景、logo、登录头像、二维码等信息，提升蜜罐仿真度。

定制化伪造用户真实数据上传至蜜罐中，监控攻击者拖拽、下载等行为。

威胁检测工作实例

引入现场+远程专家保障团队

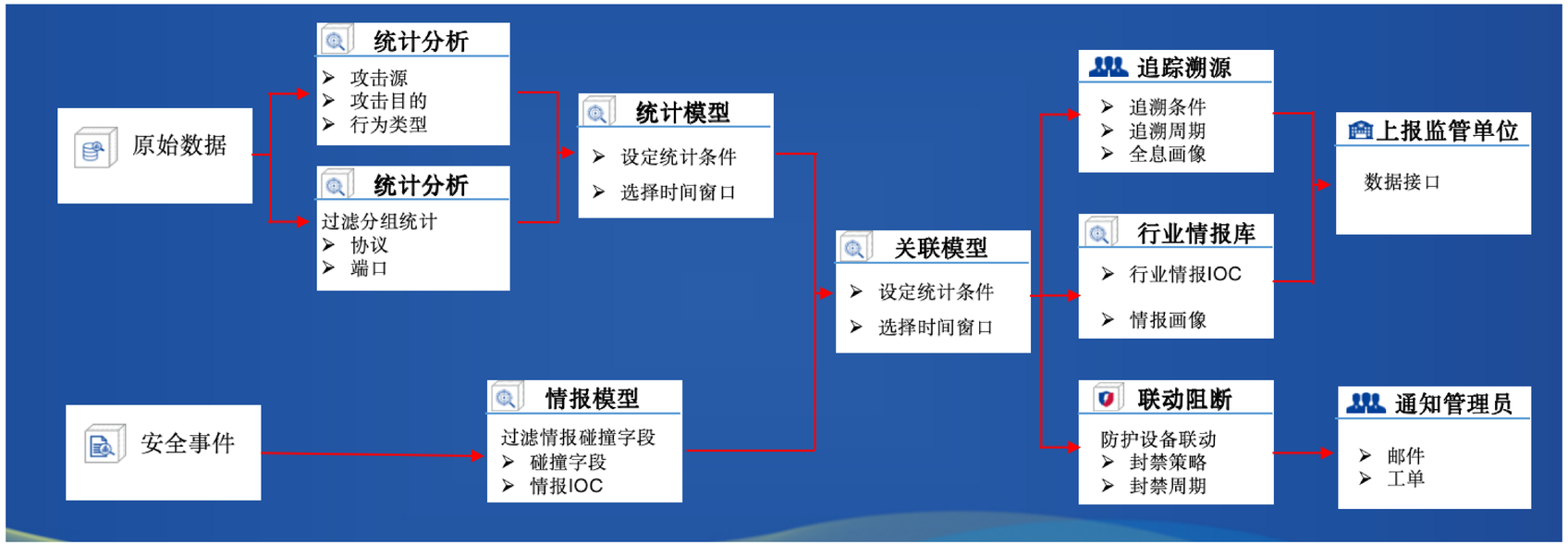
建立常态化安全监测机制，过程中双方相互赋能

自动化响应处置工作实例

从数据采集、问题定位、决策、响应行动

集团正在构建安全事件的自动化响应处置能力

期望通过自动执行重复性任务，使分析人员将精力聚焦关键任务



03 安全运营未来畅想

安全运营畅想（一）

真正实现情报共享，通过情报推动更多网络安全工作的效率和效果提升

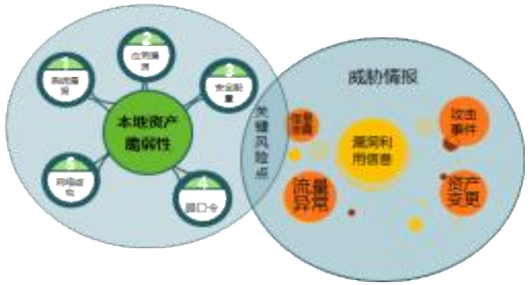
情报驱动应急响应

云端威胁情报中心实时跟踪热点漏洞事件，本地平台获取后直接定位到客户网络受影响资产范围，进行漏洞预警，帮助安全运维人员尽快完成确认、分析、修复工作，并确认修复效果。

漏洞名称	收录时间	更新日期	标签	详情
Adobe Reader Mobile for Android信息泄露 CVE-2020-24441	2020-11-10 00:00:00 GMT	2020-11-13 05:09:24 GMT 中风险	高热度 Obtain information	当地时间11月10日，Adobe官方发布了11月安全更新，修复了Adobe Connect、Adobe Reader Mobile中的多个漏洞。 Adobe发布的Adobe Connect安全更新，共修复了2个安全漏洞。 Adobe 官方指定以下更新优先级为3级。（优先级定义见下文解决方案中 Adobe优先级评估系统）。
Adobe Connect跨站点脚本 CVE-2020-24443	2020-11-10 00:00:00 GMT	2020-11-13 04:35:17 GMT 中风险	低热度 Cross site scripting	当地时间11月10日，Adobe官方发布了11月安全更新，修复了Adobe Connect、Adobe Reader Mobile中的多个漏洞。 Adobe发布的Adobe Connect安全更新，共修复了2个安全漏洞。 Adobe 官方指定以下更新优先级为3级。（优先级定义见下文解决方案中 Adobe优先级评估系统）。
Adobe Connect跨站点脚本 CVE-2020-24442	2020-11-10 00:00:00 GMT	2020-11-13 04:34:01 GMT 中风险	高热度 Cross site scripting	当地时间11月10日，Adobe官方发布了11月安全更新，修复了Adobe Connect、Adobe Reader Mobile中的多个漏洞。 Adobe发布的Adobe Connect安全更新，共修复了2个安全漏洞。 Adobe 官方指定以下更新优先级为3级。（优先级定义见下文解决方案中 Adobe优先级评估系统）。

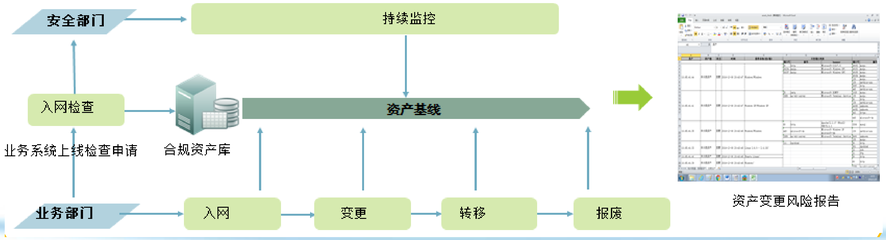
利用情报聚焦关键风险

利用外部威胁情报，快速定位影响本地资产安全的关键风险点，结合业务系统资产重要等级，给出更为有效的风险评估分析。



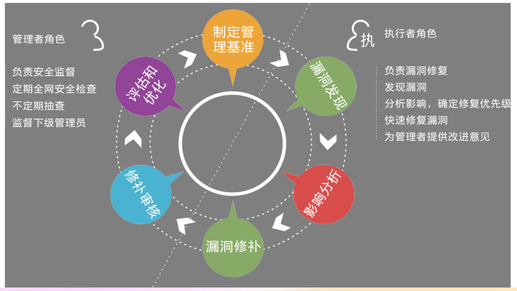
情报驱动资产持续监控

对采集到的情报、脆弱性数据进行预处理，排除重复、无用数据、尽量消除误报信息，是最终评估分析结果更为精确。



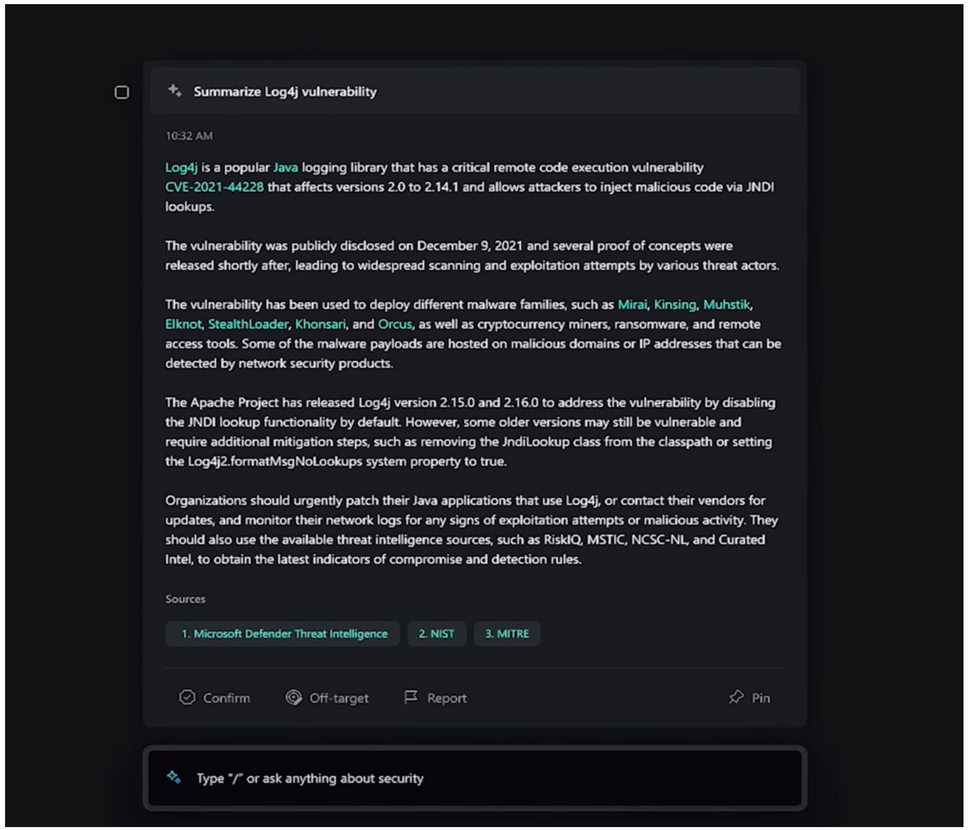
情报驱动漏洞闭环管理

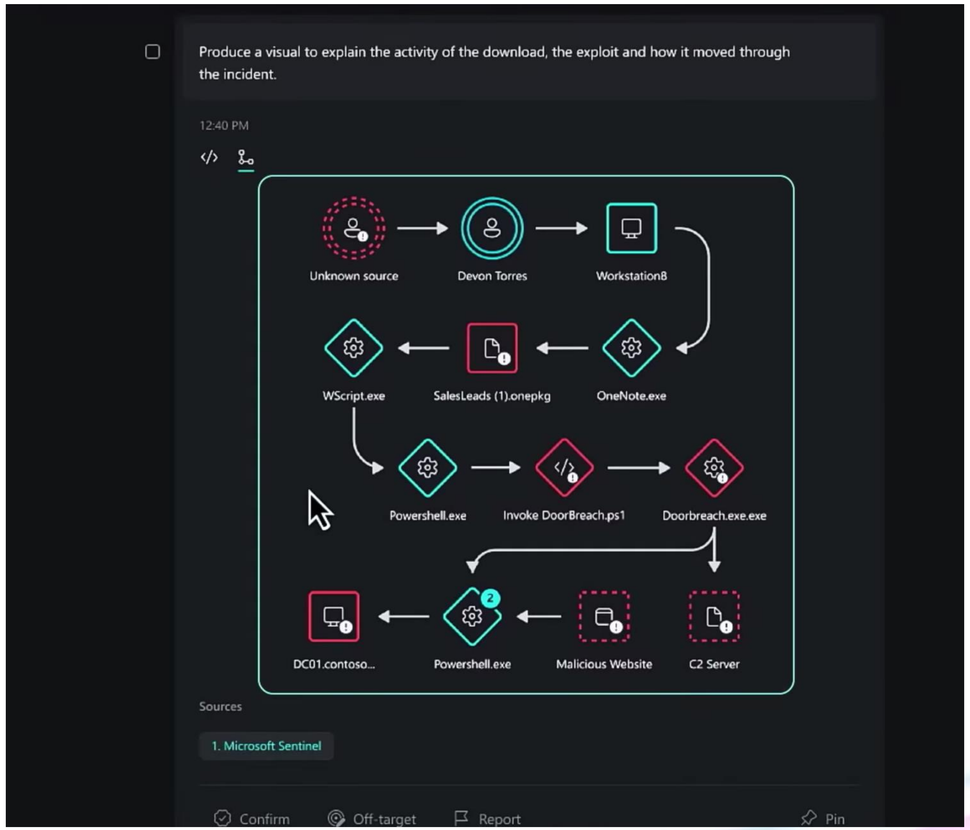
内置漏洞闭环过程处理引擎，成为漏洞闭环管理的技术支撑，对漏洞处置跟踪分析和量化，并支持多用户协作修复，和经验共享。



安全运营畅想（二）

安全AI大模型可落地，真正实现可以汇总所有安全、调查事件，“分钟级”评估和响应网络安全事件，直观地展示最重要的安全信息，并对其做出安全防护对策。





谢 谢