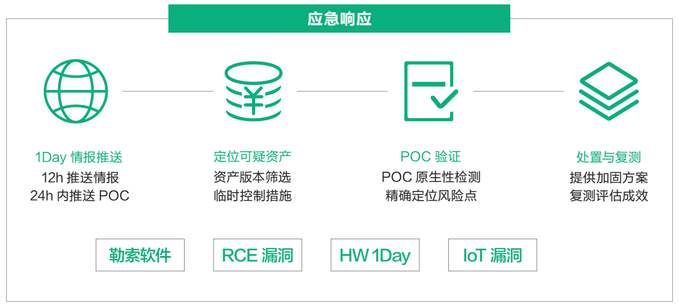
如图所示，天相 1Day 应急响应服务与传统 1Day 漏洞应急的区别在于：

- 服务团队持续关注 1Day 披露情报，第一时间进行情报验证与推送，无需用户人工搜寻 POC；
- 基于完善的内外网安全资产信息，可第一时间基于版本信息进行初筛，并针对高危风险执行策略加固等临时应对措施；
- POC 结合资产信息进行定向原理验证，无需全资产监测，极大提升风险定位速度；
- 管理信息打通处置流程，加固方案协助风险处置，复测能力度量处置成效。



◇ 联防联控：多平台间数据增值应用

1 提供全量 API，三方系统通过 API 调用系统内数据。

2 为态势感知、SOC 等平台、系统提供准确的资产威胁数据。

◇ 平台赋能：IT 资产测绘能力常态化

通过标准化资产威胁测绘及管理能力落地，帮助用户实现其所需的安全运营管理场景，包括但不限于企业资产威胁管理、集团资产威胁管理、行业内外网 web 漏洞监管。

6 部署方式

可提供软硬一体机版本。

可提供纯软件版本。

支持 1+N 星型结构部署，支持“1 总部 +N 分支机构”的资产威胁管理场景。

政企官网

政企公众号

联系我们
公司官网：360.net
客服热线：400-0309-360
售后邮箱：service-tech@360.cn

360政企安全

数 字 安 全 的 领 导 者

360 资产威胁与漏洞管理系统 天相

资产安全自主掌控

1 产品概述

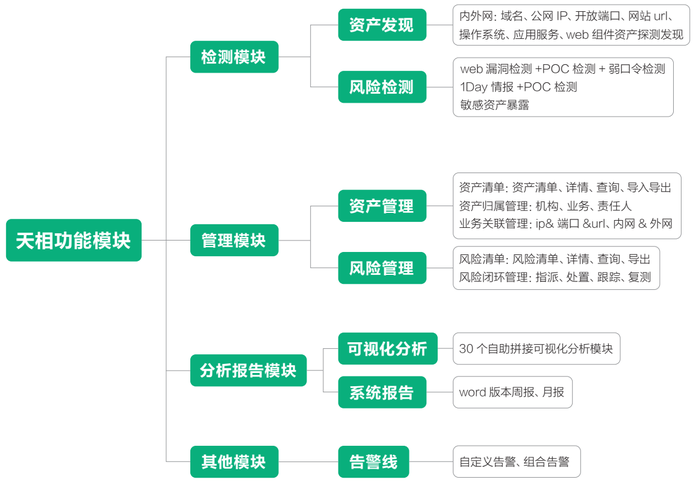
360 资产威胁与漏洞管理系统【简称：天相】，是基于安全运营、应急响应需求场景开发的常态化资产威胁管理系统。通过运用资产威胁情报以及先进的资产威胁探测引擎，全面识别、管理组织 IT 边界，确定资产属性、快速发现安全漏洞、精准定位安全风险。通过专业安全加固建议和风险复测，助力组织实现资产安全自主掌控。

天相通过对组织 IT 资产信息的长期管控，帮助组织完善安全资产管理制度，有效应对业务发展引起的资产

2 天相业务场景和安全价值提炼

	功能点	业务场景	安全价值
1	资产探测	• 域名资产发现 • 内外网 IP\url 资产发现 • OS、应用服务、业务组件识别 • 摄像头、打印机设备识别	• 摸清家底，自动化发现 IT 资产。 • 周期任务，常态化管理 IT 资产。
2	资产管理	• 归属部门 \ 业务 \ 责任人管理	• 资产定责，明确责任归属。
3	风险探测	• 敏感资产识别 • Web 漏洞、弱口令检测 • 1day 情报 +POC 检测	• 风险检测，检测覆盖更全、更准、更及时，减少误报、漏报。 • 应急响应，1day 自动关联受影响资产，安全应急有的放矢。
4	风险管理	• 漏洞生命周期管理 • 敏感资产管理	• 闭环漏洞管理，全流程跟踪。 • 敏感资产识别、关停、复测。
5	系统管理	• 系统升级 • 用户 \ 角色管理 • 日志管理	• 在线、离线升级。 • 多用户数据东西向隔离。 • 本地化加密存储资产风险数据，安全可靠。 • 日志长期保存。

3 产品功能



4 产品优势

建立安全资产管理体系

天相除具备发现企业开放在内外网上的 IP、URL 等多种数字资产外，还具备内外网资产关联、资产动态持续监测、多维 IT 资产检索定位、不同管理角色权限定义等结构化的安全管理方式。

海量指纹库积累

指纹库是准确识别安全资产版本类型的核心能力，天相指纹库融合开源指纹库、商业指纹库、行业指纹库在内的多源指纹信息。通过数据清洗、融合，已形成 5 大类、17 小类，涵盖操作系统、应用服务、中间件与数据库、工控与物联网设备、区块链协议与服务、虚拟化设备、安防办公设备以及部分金融行业特色业务系统指纹。不记版本号的指纹库条目数量在 24000 项以上，计入版本信息可达 50 万条以上。

漏洞全生命周期管理

天相通过周期性漏洞监测，持续跟踪漏洞修复和加固状态，通过提供漏洞对应责任人的指派流程，帮助用户掌握漏洞的生命周期变化情况，能够直观展示监测结果和流程结果的比对情况，有效识别新增和重现（未修复成功）的漏洞。

无介入式安全检测能力

天相采取黑盒检测（网络可达即可检测）+ 被动情报碰撞的方式，实现资产威胁监测能力。不对目标资产进行任何安装 agent、植入脚本等深度敏感操作，对目标系统影响较低，检测安全性较高。

快速响应 1day 应急

通过长期资产监控维护资产列表，当出现 1day 的时候，天相能够快速推送相关情报，并根据 1day 系统 / 设备 / 应用版本信息快速定位到可能受到影响的资产，帮助用户排查并修复 1day 漏洞。360 有快速获取最新 1day 的多种渠道，并能在 24 小时内形成检测插件更新到天相上，帮助用户检测最新 1day。

资产发现深度广度相结合

在深度上，天相可对目标端口进行深度探测，通过获取指纹信息和 banner 信息识别真实组件小版本。系统内置的指纹库可支持 38 大类指纹信息，能全面识别系统应用组件信息。自定义检测范围涵盖全 IP 段资产至单个 IP 端口，可灵活定义资产发现任务的检测范围。在广度上，支持内外网域名、IP、端口、url、应用组件、web 组件等资产发现能力。天相的内外网全局资产发现能力，对标重保时期的内外网资产暴露监测需求，可满足用户在护网行动等特殊时代的资产威胁暴露监测场景。

全面的数据能力支撑

天相具备众多数据能力，可有效支撑组织数字资产威胁监管能力，包括：全球域名库数据、全国备案库数据、全球 IP 地理信息库数据、漏洞 POC 库数据。

全量 API 数据赋能

支持基于 API 的数据输出，可对接 360 本地安全大脑，为其提供全面、准确、及时的 IT 资产信息。

5 客户价值

◇ 主动排查：内外网攻击面持续收敛

1 系统周期性执行资产威胁检测任务，并对检测结果及时确认与处置，降低了网络安全事件发生的概率。

2 通过持续对攻击暴露面的识别与处置，尽可能收窄攻击暴露面，从而达到业务攻击暴露面最小化的目的。

◇ 精准定位：1Day 高危漏洞应急响应

1Day 高危漏洞应急响应，是利用资产数据及威胁情报进行主动、精确防御的典型场景。（平台内置 POC1500+）