# 360 安全分析与响应平台

# 产品白皮书

# 目 录

# 版权声明



本文信息如有变动，恕不另行通知。
本文包含的信息代表目前三六零安全科技股份有限公司对本文所述内容的观点。由于用户需求、市场和产品状况的不断变化，本文中的信息不代表三六零安全科技股份有限公司未来的观点，且不能保证本文的内容在未来时间的有效性。
三六零安全科技股份有限公司会根据需要不定期发布本文档的更新与修订本。

# 商标声明

让世界更安全更美好为三六零安全科技股份有限公司的商标。

本文中所提到的有关产品或公司的名称均可能为相关公司或机构的（注册）商标。

# 注意

除非特别说明，本文档中出现的安全分析与响应平台的名称在本文档中均代表三六零安全科技股份有限公司

# 一. 引言

## 1.1 文档主题

本文档主要介绍了 360 安全分析与响应平台的建设背景、平台概述、产品特点等几个方面内容，并对平台功能也进行了详细的介绍，以帮助读者对 360 安全分析与响应平台达到快速和全面的了解。

## 1.2 适用范围

本文档适用于需要对城市级安全运营中心、城市级态势感知建设或对 360 安全分析与响应平台感兴趣的客户。如需要了解平台的更多信息，请通过 https://b.360.cn 中的联系方式联系我们。

本文档密级：公开。

# 二. 安全现状与挑战

## 2.1 安全现状

伴随信息革命的飞速发展，互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间，正在全面改变人们的生产生活方式，极大促进了经济社会繁荣进步，同时也带来了新的安全风险和挑战。近年来，网络安全事件多有发生，因互联网应用遭受攻击而导致的经济损失巨大并有逐年增加的趋势。

在互联互通的全球数字经济背景下，我国加快 5G 基站、大数据中心、人工智能、工业互联网等新基建的建设进度，随之将会带动网络安全的常态化建设。新基建与传统基础设施的安全问题会进一步的融合。网络空间日益复杂，网络空间威胁事件逐渐倾向于有组织有规模的形式，国家、重要的省/市成为更多攻击者觊觎的目标。

为应对日益严峻的网络安全形势，响应国家网络空间战略、网络安全法等要求，针对国家关键信息基础设施的信息安全保障与监管需求，建设网络安全态势感知平台，确保对网络空间关键信息基础设施进行全方位全天候的掌控和预测，在满足安全合规的基础上进一步提升安全能力建设。

## 2.2 安全挑战

1. 辖区内各单位中普遍部署了各种类型的安全设备，碎片化严重，缺乏宏观层面的态势把控和整体评估。

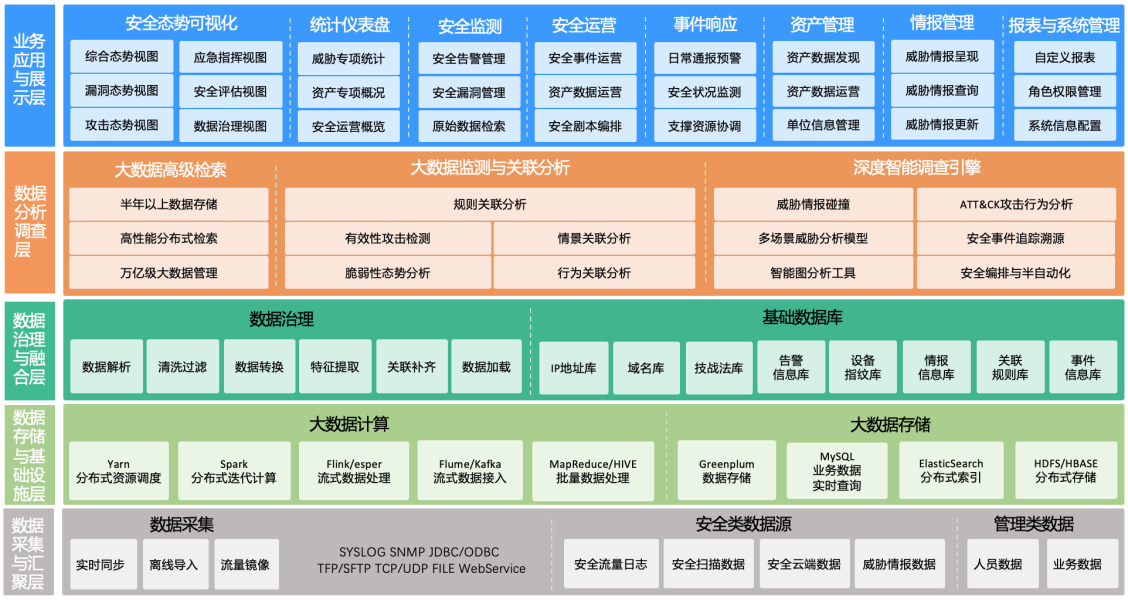
2. 网络安全监管与等保备案信息没有充分结合，缺少对关键信息基础设施的精准防护。
3. 辖区内重要资产梳理不清，很多未发现的重要“影子”资产存在严重安全问题。
4. 安全设备产生海量告警日志，缺少对有效告警的优先级识别，以及对告警有效性的准确性把关。
5. 安全运营过程中手工流程过多，安全运营自动化不足，运营效率低下，安全运营中心体系建设不完全，缺乏专业安全运营团队支撑。
6. 针对 APT 等高级威胁缺少防御手段，缺乏优秀威胁情报支撑，尤其是需要对监管行业关心的重点事件、重点规则进行单独监测。
7. 安全事件的追踪溯源能力较弱，缺乏对黑客、黑客组织的回溯。

# 三. 平台介绍

## 3.1 方案概述

360 安全分析与响应平台(360 Security Analysis and Response Platform，360-SARP)，面向网络安全监管单位提供关键信息基础设施威胁态势感知和安全运营中心能力。平台以关键信息基础设施资产为核心，以大数据架构为基础，连接 360 安全大脑知识云、情报云、分析云赋能，采集本地多源异构数据，结合城市级资产测绘、多维威胁知识图谱分析、安全编排与自动化响应、可视化呈现等技术，配合本地安全服务团队，帮助客户实现安全态势的可见性、安全分析调查能力、安全威胁的实时预警、通报预警、资产及漏洞的管理及敏捷化的应急响应能力，协助客户快速发现、分析、处置安全事件，实现安全闭环管理，有效辅助监管单位构建网络安全中心化监管治理工作。

如下图，平台整体架构从下到上由数据采集与汇聚层、数据存储基础设施层、数据治理与融合层、数据分析调查层、业务应用与展示层构成，同时具备相配套的标准体系以及安全保障体系。




## 3.2 方案内容

### 3.2.1 态势感知

态势感知子系统对网络空间关键信息基础设施安全态势进行多层次、多角度、细粒度感知，包括但不限于对重点行业、重点单位、重点网站，重要信息系统、网络基础设施等保护对象的态势进行感知。

主要分为两部分，态势分析和态势呈现。

态势分析：针对辖区内单位、网站数据采集分析，通过安全监测子系统对 DDoS 攻击监测、高级威胁攻击检测监测、僵木蠕毒监测、重大漏洞监测等能力，通过恶意代码检测、异常流量分析、情报联动、威胁关联分析、攻防模拟对抗等技术进行深度分析后，结合监管单位资产视角，对辖区内的单位安全状态进行宏观和微观层面的安全态势监测与分析。

态势呈现：通过对威胁在行业、单位、类别、级别、来源、攻击

分析、同比、环比等的数据统计，全方位地呈现整体安全态势。可帮助用户分别对宏观和专项的安全状况进行快速直观地了解，包括综合态势、漏洞态势、攻击态势、应急指挥等。


*注：图中为模拟数据。*

### 3.2.2 仪表盘

仪表盘子系统是安全分析与响应平台针对数据分析时输出的统计分析结果数据的整体展示，可通过默认集成的统计模板，来定制展现优先关注的安全及业务等数据。数据来自各业务数据模块，并可支持配置威胁、资产等相关专项仪表盘。作为平台数据分析转化图分析的可视化分析工具，仪表盘子系统可对平台所有数据进行响应地聚合统计和专项分析，不仅能够为安全运营人员提供高效可视的分析支撑，还能在总结汇报场景下发挥数据统计可视化的能力。

### 3.2.1 安全监测

安全监测子系统是安全分析与响应平台中多源异构安全数据的集中，一部分为接入的原始安全数据，另一部分为将多源异构数据接入解析、预处理、合并和关联分析后产生的安全告警数据。平台的运营人员可在该系统中查看威胁相关的数据，提供威胁数据专项仪表盘，以及全量原始数据检索、分析调查、告警数据管理、漏洞数据管理的能力。

### 3.2.2 安全运营

安全运营子系统作为平台的运营抓手，为平台运营人员提供良好地运营引导和支撑。该子系统聚焦告警数据运营能力，分为告警任务生成、告警分析验证、告警处置响应。

告警任务生成，即对平台收集汇聚的各类安全数据，例如网站告警、安全漏洞等，通过相对公平的机制以任务的形式自动化地聚合告警信息，从而减少运营人员验证告警的数量，同时自动计算告警的可信度和处置优先级，帮助管理员聚焦关键告警。

告警分析验证，即安全分析专家针对告警数据的真实有效性进行分析和验证。剔除误报告警，并将模糊、低质量告警转化高质量、有价值的告警的过程。

告警处置响应，为有效安全事件提供开展相应的处置和响应动作。包括日常的通报处置和预警，以及进一步地深度调查分析等。

### 3.2.3 深度调查

调查分析子系统是安全分析与响应平台针对网络安全事件的深度调查分析模块，安全事件的有效性在不能通过简单分析手段来判定之时，可以选择使用深度调查分析功能进行深度关联和调查分析。

深度调查分析过程中，高级安全分析专家可以调用安全编排与自动化的剧本或者动作，对安全事件的关联维度和方向进行深度分析，还可借助半自动化 ATT&CK 模型标签引擎和图关联分析等工具，通过对安全事件的深度透视和关联性分析，获得对安全事件本身和攻击者的攻击路径、技战法等信息更全面的可见性，精准地将安全事件的相关信息及关联关系呈现出来。

基于安全编排与自动化系统技术（SOAR），能有效优化安全告警的 MTTD（平均检测时间）和 MTTR（平均响应时间），为监管侧用户和安全分析人员的进一步决策提供及时有效地数据支撑。

### 3.2.4 资产管理

资产管理子系统是安全分析与响应平台针对网络资产进行监测的子系统，对汇聚上来的城市网络空间资产探测数据、手动填报等多源异构的资产数据进行统一的生命周期运营和管理，数据来源主要包括资产探测设备的主动扫描采集、被动流量识别和人工录入。记录各种类型资产的详细信息，并对资产信息的变化和异动进行监测和管理。目前主要包括资产概览、资产发现和资产管理三部分。可重点实现资产发现、资产运营、资产归档、资产管理、单位管理等业务能力。通

过主动扫描探测和被动流量识别相结合的方式，结合信息补全和人工运营等方式完成资产数据的“准而全”，最终实现关键资产的识别发现与生命周期的管理。

### 3.2.5 报告管理

报告管理子系统是安全分析与响应平台订制、查看和下载报告的入口。该子系统的数据源，来自各业务数据模块，并可支持对平台全量数据源统计分析、生成报告的能力，贴合用户业务需求，支持高定制化配置能力。

### 3.2.6 应急指挥

应急指挥子系统是安全分析与响应平台针对网络安全突发事件进行及时分析研判和决策部署的功能系统。实现网络安全的态势感知、监测预警、指挥调度、通知通告、应急处置及资源协同等能力，对网络安全威胁、风险、隐患、突发事件、攻击等进行通报预警，对重点保护对象进行全要素数据采集，重点保护，并进行全要素显示和展示，实现重大事件或特殊时期的指挥调度能力。

### 3.2.7 情报管理

情报管理子系统是安全分析与响应平台接收 360 安全大脑情报云的赋能，是 360 高级威胁情报能力赋能的主要体现。平台主动从云端情报平台获取最新威胁情报，用于本地威胁检测和告警优先级排序。此外，安全分析、调查过程中会主动连接获取威胁的上下文情报信息，助力安全分析人员进行分析和研判。

### 3.2.8 数据规则

数据规则子系统是安全分析与响应平台采集数据和分析规则设定的入口。安全数据接入（包括各设备、系统的日志及告警，以及流量日志）是安全分析的基础，而安全数据模型普遍具有碎片化的特点。360 分析与响应平台采用了安全日志数据建模技术，预置可扩展的无模式元数据模型，平台运行过程中可以便捷接入各类数据，接入过程都通过直观便捷的可视化编辑器进行。

# 四. 方案创新与价值

## 4.1 技术优势

### ■ 城市级网络空间资产测绘

基于自主研发设计的全网空间测绘系统，能够对全球全量 IPv4、IPv6 地址进行持续性测绘工作。通过结合人工智能与机器学习的方式，具备全网资产设备精准发现、精准识别能力，同时系统利用强大、灵活的底层核心扫描引擎，将丰富的安全漏洞数据库、安全漏洞知识库与海量资产识别数据相结合，从而达到对城市级网络空间漏洞风险感知的目标，对潜在暴露在网络的影子关键信息基础设施进行全方位发现，实现对网络空间真正的看见，成为了网络空间中的预警雷达。

### ■ 开放式数据理解技术

对多源数据的汇聚，是安全分析与响应平台“看得见、看得清”的基础。平台基于高易用性的数据源接入配置、解析配置功能和标准化的数据字典，且支持用户按需自定义配置解析规则及映射字段，让数据接入和解析更加开放且高效。

### ■ 高级威胁情报赋能

360 安全大脑情报云高级威胁情报能力行业领先，目前已发现对我的 40 多个 APT 组织和多起重大攻击事件。平台联动云端高级威胁

情报数据，为防御能力建设从“被动防御”到“主动防御”的快速提供有效支撑。

### ■ 攻击链分析推理

攻击链分析模型通过对平台收集的安全日志和流量日志进行 MITRE ATT&CK 框架化处理，在平台深度调查子系统中，会自动反向推理还原攻击情景，最大化观察网络攻击者的技战术。

### ■ 威胁图谱分析技术

基于 360 安全大脑的知识云图分析技术，在实时关联的同时，便于对威胁数据和历史分析行为和进行回放和总结，是针对安全时间进行深度安全分析的黑科技。目前 360 威胁图谱综合恶意代码样本、C2 信息、whois、证书等信息，已经形成百亿顶点、千亿边的图数据库。

### ■ 安全编排自动化技术

现代的安全运营中心引入安全编排与自动化响应技术（SOAR）来更一步解决碎片化的安全设备接入、管理联动、安全运营人员水平参差不齐、告警分析响应效率低下、安全运营手动流程过多等挑战。

平台实现的安全编排与自动化响应的重要核心技术之一，剧本库（Playbook）、动作库技术，贯穿事件监测、分析、调查、响应流

程。通过该功能，将不同的系统协同联动起来的目标，就像一个交响乐队的指挥。

平台的安全编排与自动化具备流程化自动执行功能，能够依据场景或案例，制定执行计划和执行脚本，并具备自动、半自动和手动执行的能力系统。通过内置 playbook，将大量的数据按照预定的模板使用自动化方式去处理，有效优化安全告警的 MTTD（平均检测时间）和 MTTR（平均响应时间），避免人在处理大量数据的过程中带来的误差或失误。

与此之外，提供高级自定义能力。通过编程的方式，不仅可以输出特定行为和专项场景的行为脚本，还可以针对节点之间等进行策略的自定义定制，为安全编排工具提供更灵活智能方式。

### ■ 高级专家协同防御

360 安全专家团队全程参与安全事件处置过程，从事前、事中、事后，做好分析、研判、处置，结合 360 安全大脑专家云服务(MDR)赋能，帮助各单位做好协同防御。

## 4.2 产品价值

### ■ 安全大数据分析能力

基于平台安全大数据处理技术，结合 360 安全大脑的先验的知识云、情报云、分析云引擎赋能、对海量安全数据进行安全分析，可以发现很多传统手段无法发现的安全问题。

## ■ 智能敏捷安全运营能力

面对海量告警日志的日常安全运营，平台结合 360 安全大脑情报云、机器学习降噪、高性能流式关联、安全编排与自动化响应技术（SOAR）等技术手段，构建本地化的智能和敏捷安全运营中心。

## ■ 高级威胁情报监测能力

360 安全大脑情报云高级威胁情报能力行业领先，目前已发现对我的 40 多个 APT 组织和多起重大攻击事件。平台联动具有自运营机制的 360 本地和云端的高质量威胁情报数据，自动关联碰撞出威胁与预警信息，是安全能力从“被动防御”到“主动防御”转换的有效手段。

## ■ 融合安全运营服务

安全运营服务(MDR)采用一体化集成方式为企业提供端到端的服务。基于 MDR 服务模式，降低平台建设人员、技术、运营经验不足的风险，可大幅度降低安全运营带来的负担。MDR 支持 360 安全大脑专家云远程服务，也支持本地安全专家提供驻场服务。