

# 绿盟安全管理平台 白皮书

■ 文档编号 请输入文档编号

■ 密级 完全公开

■ 版本编号 V1.0

■ 日期 2021-1-12



---

#### ■ 版权声明

---

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**绿盟科技**所有，受到有关产权及版权法保护。任何个人、机构未经**绿盟科技**的书面授权许可，不得以任何方式复制或引用本文的任何片断。

---

---

#### ■ 版本变更记录

---

时间	版本	说明	修改人

---

---

#### ■ 适用性声明

---

本模板用于撰写绿盟科技内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

---

# 目录

一. 安全管理的新需求和挑战 .....	1
1.1 安全现状 .....	1
1.2 面临挑战 .....	2
1.3 应对措施 .....	3
二. 绿盟安全管理平台 .....	4
2.1 产品概述 .....	4
2.2 产品架构 .....	4
2.3 客户价值 .....	4
2.4 产品亮点 .....	5
2.4.1 强大的数据整合能力 .....	5
2.4.2 完善的安全分析能力 .....	6
2.4.3 高效的响应处置能力 .....	6
2.4.4 全面的态势感知能力 .....	7
2.4.5 有效的安全运营能力 .....	7
2.4.6 便捷的产品部署能力 .....	7
2.5 典型应用场景 .....	7
2.5.1 等保合规 .....	7
2.5.2 日志审计 .....	8
2.5.3 攻击检测 .....	9
2.5.4 响应处置 .....	10
2.5.5 资产发现 .....	11
2.5.6 漏洞管理 .....	11
2.5.7 情报预警 .....	12
2.5.8 态势感知 .....	13
2.5.9 安全运营 .....	14
2.5.10 安全报表 .....	15
2.6 产品优势 .....	16
2.6.1 合规, 满足合规政策要求 .....	16
2.6.2 智能, 减轻工作量提高效率 .....	17
2.6.3 运营, 有效实现安全价值 .....	17
三. 典型部署 .....	18
3.1 单机部署 .....	18
3.2 级联部署 .....	19
四. 总结 .....	19

# 一. 安全管理的新需求和挑战

## 1.1 安全现状

随着企业信息化的不断发展，企业信息化资产数量日趋增多、系统的关联性和复杂度不断增强，然而当前信息安全形势日益严峻，信息安全防护工作面临前所未有的困难和挑战。为了更好地监控和保障信息系统运行，及时识别和防范安全风险，同时满足国家和行业监管要求，保证信息安全管理工作的依法合规，亟需建立一个全数据、集中管理的安全管理平台，做到事前预警、事中监控、事后分析，全面提升信息安全管理与防护水平。

同时，IT 技术及攻防技术的不断演进，企业对信息安全技术人员的依赖日益加深，对技术人员的安全能力也有了更高的要求。这不仅加剧了技术人员的需求缺口，也增加了管理人员使用成本。企业在转变生产方式和业务拓展的大背景下，IT 运维和人员数量和人员成本的与日俱增，又使得企业预算捉襟见肘。

与此同时，中国把网络安全提升到国家战略层面，相关法规政策接二连三密集出台。

2016 年 4 月 19 日，国家主席习近平在网络安全和信息化工作座谈会上发表“4.19 讲话”，强调网络安全建设的重要性，并提出：“要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力，要加快网络立法进程，完善依法监管措施，化解网络风险。”

2016 年 12 月 27 日，国务院印发《“十三五”国家信息化规划》，要求健全网络安全保障体系，提出“全天候全方位感知网络安全态势”。

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式施行，顺应了网络安全发展法制化大趋势，对我国网络安全产业发展有着重要的意义。其中第二十一条，国家实行网络安全等级保护制度。要求网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。第五十二条，负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、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。

2019 年 5 月 13 日，国家市场监督管理总局召开新闻发布会，等级保护 2.0 标准正式发布，并于 2019 年 12 月 1 日正式实施。等级保护 2.0 安全框架中提出建设“一个中心，三重防护”的安全体系，即一个中心就是安全管理中心，三重防护是安全通讯网络、安全区域边界、安全计算环境。其中突出了网络安全综合防御体系以及态势感知等内容。

## 1.2 面临挑战

随着移动互联网、物联网、云计算和大数据技术的快速发展和不断应用，组织和企业的网络和信息系统每天都在产生大量的数据，而且产生的速度越来越快，大数据时代的安全信息具有海量、高速、多样、低价值密度等特点，如何对安全大数据进行管理和分析，帮助用户及时发现安全问题、及时响应处理变成了信息安全管理领域的重要课题之一。

传统安全管理平台的采集、分析和处理能力已无法满足海量数据环境下的信息安全管理需求，主要面临着以下几种挑战：

### 1) 看不见的安全威胁

- 新型未知威胁难检测：黑客攻击手段越来越复杂隐蔽，比如勒索病毒、鱼叉邮件攻击、水坑攻击，0day 漏洞攻击等，缺乏多样化检测手段，缺乏多技术互补协同。
- 内部隐藏威胁难发现：黑客长期持续潜伏，通过肉鸡发起攻击，也有内鬼作案，缺乏内外无死角的全场景探针覆盖。

### 2) 摸不清的安全风险

- 看不到风险在哪里：不清楚有多少资产在哪里，不清楚资产有哪些漏洞，不清楚资产遭受哪些攻击，安全风险摸不清，缺乏资产发现、漏洞识别、威胁检测、态势感知为核心的综合分析能力。
- 难以看清安全全貌：安全设备各自为战，海量日志误报多，难以识别有效告警，而且安全数据分散，盲人摸象，难以描绘全局安全态势，缺乏基于大数据平台的企业安全大脑。

### 3) 赶不及的响应处置

- 响应处置效率低：安全设备相互割裂，设备之间难以协同响应，安全人员到处救火，处置效率低，缺乏安全设备联动，以及安全编排与自动化响应能力。
- 安全运营不到位：运维人员精力与能力有限，攻防对抗，安全风险不可控，风险趋势不可知，措施不到位，问题未闭环，缺乏有组织支持、有流程保障、有平台和设备支撑的安全运营体系。

## 1.3 应对措施

客户需要一套全新的安全管理平台来应对新型攻击和海量数据带来的所有挑战，该平台能够通过数据采集和分析，协助企业 IT 运维人员和安全分析人员快速发现威胁。以威胁情报为驱动，针对企业 IT 资产情况进行全方位的监控和告警，协助用户进行网络安全威胁的统一管理。

综合来说，安全管理平台具备三大核心要素：

### 1) 安全可视

首先安全可视需要练就“火眼金睛”，通过多源异构数据采集，获得全面、有效的数据：

- 场景覆盖：实现内外网无死角监控，网络、终端全场景覆盖；
- 技术互补：支持多探针组合部署，日志、流量等多种采集技术互补，资产、漏洞、威胁等多种识别技术互补，火眼金睛洞察一切；

### 2) 态势可感

其次态势可感需要打造基于大数据平台的“智慧大脑”，对安全数据进行精准分析并可视化呈现：

- 精准分析：通过多源关联分析、异常行为分析、机器学习等技术实现威胁精准分析，通过威胁情报实现情报预警与安全分析增强；
- 安全感知：通过可视化技术，实现资产可视、漏洞可视、威胁可视以及态势感知，安全大脑辅助客户决策；

### 3) 风险可控

最后风险可控需要“强健体魄”，实现快速响应，避免风险扩散：

- 技术可控：通过安全设备联动，以及安全编排与自动化响应能力，自动化协同联动，控制风险，达到出则能战、战则必胜；
- 管理到位：通过安全运营体系，实现有组织、有流程、天、地、人、机协同的安全管理机制，让安全运营；

## 二. 绿盟安全管理平台

### 2.1 产品概述

针对医疗、教育、政府、企业等中小客户，绿盟科技基于安全大数据平台应用基础，推出满足合规要求的轻量级安全态势感知平台，绿盟安全管理平台 ESP 集安全态势感知与预警、威胁检测与响应、漏洞发现与管理、日志收集与审计等全面的安全管理能力于一体，支持软硬一体化的形态，部署快捷，维护简单。

### 2.2 产品架构

如图所示，从技术的角度出发的平台系统架构：

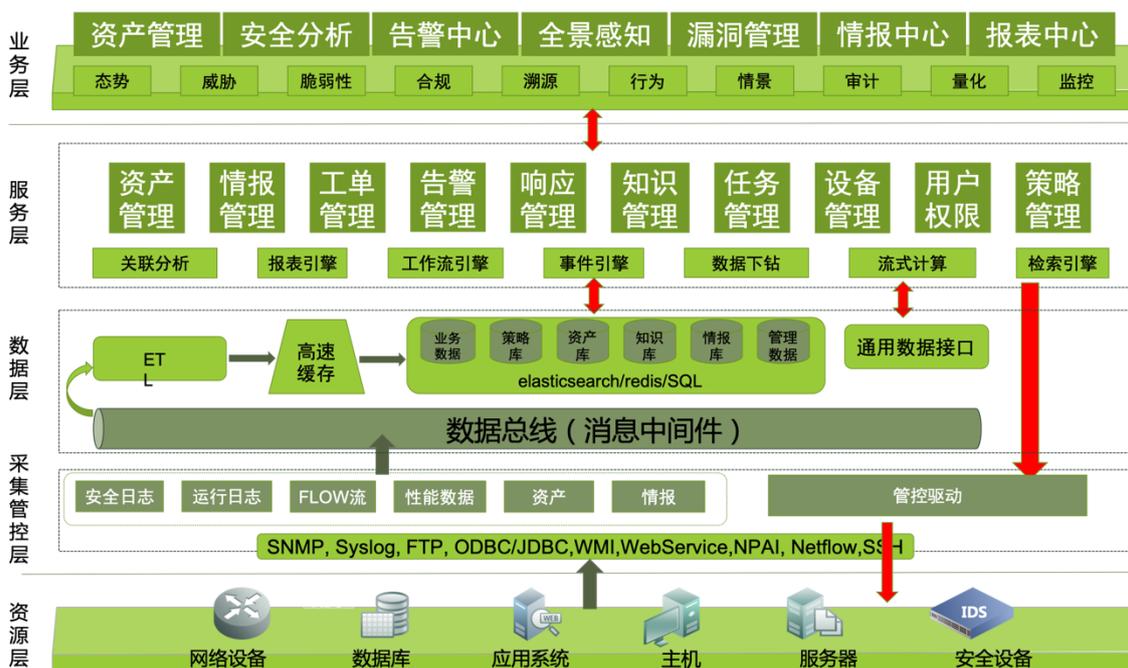


图 2.1 绿盟安全管理平台系统架构图

### 2.3 客户价值

绿盟安全管理平台帮助客户实现三大价值：

### 1、高层：辅助决策

全局安全态势可视化，帮助高层管理者掌握企业全网安全状况，随时了解最新的安全趋势和风险状态，辅助决策安全建设方向和投资。

### 2、中层：管理落地

威胁、漏洞、资产集中闭环管理，帮助中层管理者落地安全管理和技术体系，威胁事件预警和追溯，漏洞监控并闭环处置，动态发现资产变化，做到心中有数。

### 3、基层：运营支撑

帮助运维人员精准攻击发现，及时事件预警，日志审计回溯，协同应急处置，减轻运维工作量，提高工作效率。

## 2.4 产品亮点

### 2.4.1 强大的数据整合能力

针对各种层出不穷的安全数据源类型，绿盟科技提出了交互式日志语义解析引擎的实现思路，保证了多厂家、多层次数据免插件、自动柔性接入，大幅降低后期各类数据接入的技术及人力成本。不仅可实时采集不同厂商的安全设备、网络设备、服务器操作系统以及各种应用系统产生的多源异构的日志信息，还使用大数据技术，在并发内存的内处理机制方面能够带来数倍于采用磁盘访问方式的解决方案，借助离线计算引擎在小时级别内，即可完成对海量日志的处理。

除了安全设备日志、服务器日志、网络设备日志等各类数据接入之外，安全管理平台也接入基于绿盟威胁情报中心 NTI 的威胁情报数据。安全管理平台将本地告警数据、网络资产数据、漏洞数据与绿盟威胁情报数据按照多个维度进行关联分析，实时感知资产的威胁和脆弱性，通过平台安全规则的筛选和过滤最终形成漏斗效应，保证告警的更加精准和有效，并洞察新的威胁动向。借助 NTI 的威胁情报支撑，用户可及时洞悉资产面临的安全威胁进行准确预警，了解最新的威胁动态，实施积极主动的威胁防御和快速响应策略，结合安全数据的深度分析全面掌握安全威胁态势，并准确地进行威胁追踪和攻击溯源。

## 2.4.2 完善的安全分析能力

绿盟安全管理平台是以资产为核心、风险为导向的态势感知解决方案，能够通过多源异构的日志数据采集和大数据分析，利用多源数据关联分析引擎、攻击链分析引擎、安全态势理解及推理引擎、威胁情报分析引擎、机器学习引擎、用户行为分析引擎等多种智能安全分析引擎，协助企业 IT 运维人员和安全分析人员快速发现资产面临的威胁和脆弱性。并且以情报为驱动，针对企业 IT 资产情况进行全方位的监控和告警，协助用户进行安全闭环管理。

基于全流量威胁管理场景，安全管理平台针对原始流量进行采集和监控，对流量信息进行深度还原、存储、查询和分析，利用其强大的大数据分析能力及各类机器学习算法，快速检测各类重点事件，如 APT 攻击事件、Botnet 事件、恶意样本传播、WebShell、隐蔽隧道等高危安全事件，结合攻击链模型向用户展示失陷主机，帮助客户从海量告警事件中，快速定位需要关注和处理的资产，并且溯源取证。

基于网站安全监测场景，安全管理平台能够针对网站安全事件、web 入侵攻击、网站漏洞进行持续监控，并结合威胁情报及网站资产信息进行关联分析，能够有效针对网站进行风险监控、事件闭环。

基于资产和漏洞管理场景，安全管理平台将资产发现与管理、漏洞识别、修复、整改、加固、验证和预警整个过程进行全程监控，通过平台将资产、漏洞、IT 运维人员、责任人和管理流程紧密绑定，并有效监控和管理，使每一个漏洞的管理都会落实到人，实现最终的闭环管理的目的。

## 2.4.3 高效的响应处置能力

绿盟安全管理平台提供一键封堵闭环管理解决方案，通过网络安全预警研判和处置，实现快速、闭环的行业安全事件预警处置能力。平台通过内外部的态势数据、评估数据、情报数据的综合分析，形成安全事件告警，并可以与防火墙、入侵防御系统、Web 应用防火墙、综合威胁探针、抗拒绝服务系统等安全设备进行自动化联动，及时封堵 IP 或阻断会话，并可通过邮件、工单等方式快速通知到相关单位和责任人，达到及时发现攻击行为、快速控制安全风险的目的，在小时级的时间内实现行业重大安全事件的闭环处置管理。

作为高级版的响应处置能力，安全编排与自动化响应 (SOAR) 通过可视化编排将人、安全技术、流程进行深度融合，通过 Playbook 剧本串并联构建安全事件处置的工作流，自动化触发不同安全设备执行响应动作。基于对安全事件上下文有更全面、端到端的理解，有助于将复杂的事件响应过程和任务转换为一致的、可重复的、可度量的和有效的工作流，变被动

应急响应为自动化持续响应。这样既可以缩短响应处置时间，又可以将高级工程师从日常运维中释放出来，节约企业人员成本。

#### 2.4.4 全面的态势感知能力

绿盟安全管理平台可以针对整体范围或某一特定时间与环境进行安全态势理解与分析，最终形成历史的整体态势以及对未来短期的预测。通过对入侵、异常流量、僵尸蠕、主机安全、网站安全等态势进行多维度分析，能够很好的洞察企业内部整体安全状态，并通过量化的评判指标直观的理解当前态势情况。

#### 2.4.5 有效的安全运营能力

绿盟安全管理平台融合了安全运营服务，可将客户本地的安全管理平台跟绿盟科技云端安全运营支撑平台对接，由绿盟云端专家给客户 7x24 小时的运营服务，并跟客户本地侧的驻场运营人员配合，实现热点事件的预警与防护、高危访问源的检测与封杀、可疑安全事件的发现与确认等系列闭环的安全运营服务，帮助企业降低整体的安全运营投入成本和风险、减轻客户的安全运营负担，保障企业网络安全。

#### 2.4.6 便捷的产品部署能力

绿盟安全管理平台提供软硬一体形态的安全管理平台管理能力，可通过修改 IP 等简单配置快速接入客户现网环境，通过内置日志接入规则、内置事件规则快速接入日志数据，从而实现安全管理平台所需能力。

### 2.5 典型应用场景

#### 2.5.1 等保合规

##### 1、需求：

- 已经购买一些安全产品，现在业务系统要通过等级保护 2.0 标准测评，怎么办？

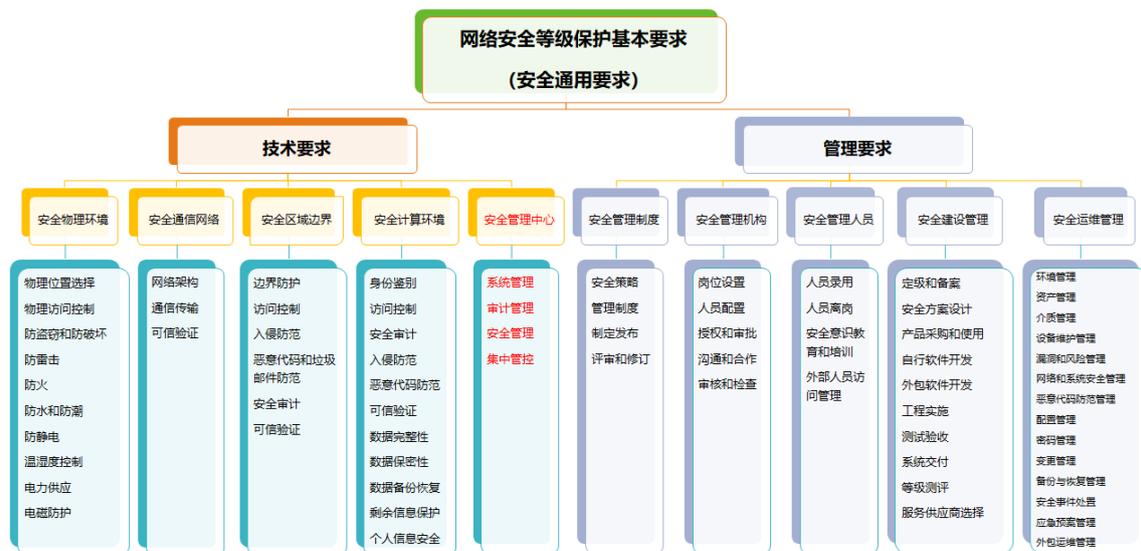
2、问题：

- 如何按照等保 2.0 标准搭建“一个中心、三重防护”的安全体系？

3、方案：

在等级保护 2.0 标准中，明确要求：安全管理中心要求具备集中管控能力，要求“应对网络中发生的各类安全事件进行识别、报警和分析”。

作为安全管理中心，绿盟安全管理平台统一接入部署的安全设备，实现数据采集、分析、响应、呈现，配套其他安全产品，建立“一个中心，三重防护”安全体系，轻松过等保。



## 2.5.2 日志审计

1、需求：

- 买了不少的不同厂家安全设备，日志分散在不同设备里，查询很麻烦，合规有要求，怎么办？

2、问题：

- 如何进行统一的日志集中收集、存储、分析和查询，满足 6 个月日志存储合规要求？

3、方案：

在等级保护 2.0 标准中，明确要求：安全管理中心要求具备集中管控能力，要求“应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求”。

作为安全管理中心，绿盟安全管理平台支持多源异构日志集中采集、存储、分析、检索，实现统一集中的日志审计，满足 6 个月日志存储要求，方便 IT 人员集中查询，满足合规要求



## 2.5.3 攻击检测

### 1、需求：

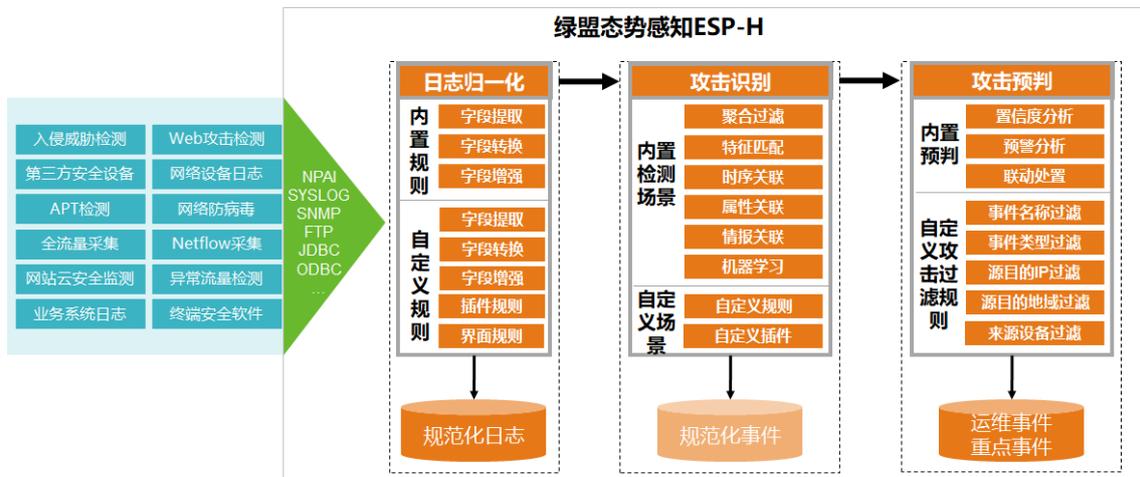
- 购买了一些安全设备，但服务器还是中了勒索病毒，数据还是被窃取，怎么能及时发现攻击？
- 不同安全设备产生的事件告警众多，有很多误报，排查事件和处置花费很多时间，处理不过来，怎么办？

### 2、问题：

- 如何及时发现网络中的攻击事件，方便排查并处置？
- 如何检测到单个安全设备难以发现的攻击事件？

### 3、方案：

绿盟态势感知解决方案包括三部分，一是部署专业探针设备，练就火眼金睛，二是部署安全管理平台，打造基于大数据平台的安全大脑，三是部署联动设备，强健体魄，及时响应处置，实现 1+1>2 的安全闭环管理。而作为方案的核心，绿盟安全管理平台具备攻击链分析、关联分析、机器学习等高级分析技术，实现平台比单个设备告警更准确、告警更少，比单个独立设备发现更多的隐蔽攻击，精准的事件告警减轻 IT 人员工作量。



## 2.5.4 响应处置

### 1、需求:

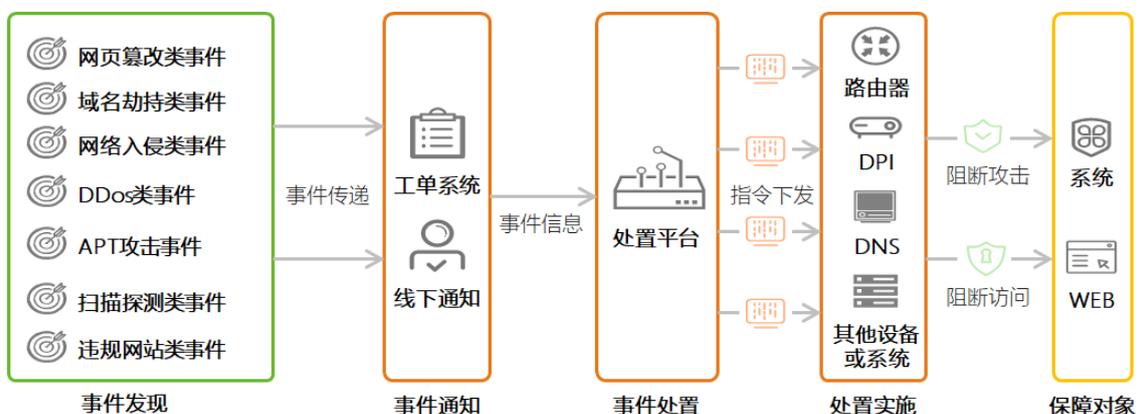
- 事件告警频发，如何第一时间知晓重大事件来紧急处理？
- 登录到防火墙或服务器上去处置，速度慢，风险控制效果差，怎么办？

### 2、问题:

- 如何通过平台把告警事件责任到人、及时处置事件避免风险扩散？

### 3、方案:

绿盟安全管理平台具备灵活的响应处置方式，首先第一时间通知到人，通过邮件及时提醒，让 IT 人员随时了解重大事件告警；并且通过工单把任务派发到责任人，处置任务责任到人保证闭环。其次自动化一键封堵，通过联动防火墙、入侵防御系统、Web 应用防火墙、综合威胁探针、抗拒绝攻击系统等设备，及时避免风险扩散。另外可扩展安全编排与自动化响应能力 SOAR，编排可视化，采集/分析/响应自动化，安全运营经验固化，提高运营效率。



## 2.5.5 资产发现

### 1、需求：

- 资产数不过来，不清楚有多少资产在哪里，也不清楚资产有哪些变化，不清楚哪些非授权资产私自上线，怎么办？

### 2、问题：

- 如何通过平台主动和被动发现网络中的资产？
- 如何及时发现资产的变化？

### 3、方案：

绿盟安全管理平台下发扫描任务给漏洞扫描器，通过漏扫主动发现网络里的资产，还可以从收集到的日志中被动发现资产，并且可以对变动资产进行资产稽查，轻松了解资产清单，了解资产变更最新情况，盘点资产不用愁。



## 2.5.6 漏洞管理

### 1、需求：

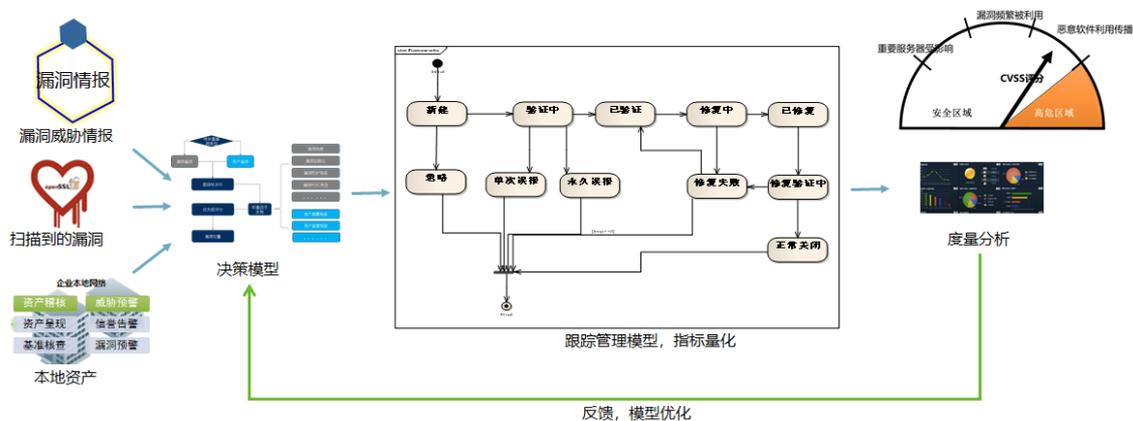
- 漏洞持续变化，如何及时发现系统漏洞、Web漏洞、配置漏洞？发现漏洞后怎么办？
- 资产很多，漏洞很多，如何知道多少漏洞被修补上？漏洞修补责任分配到个人，怎么跟踪？

## 2、问题：

- 如何通过平台主动识别资产上的脆弱性？
- 如何跟踪漏洞的验证确认和闭环处置，避免带病上阵？

## 3、方案：

绿盟安全管理平台可以从平台上下发系统漏洞、Web 漏洞、配置漏洞扫描任务，和威胁情报配合，及时发现最新的安全漏洞。安全漏洞具备详细的危害描述与解决方案，方便处置。通过漏洞闭环管理，从发现、修复、验证到预警，全流程监控，轻松操作。



## 2.5.7 情报预警

### 1、需求：

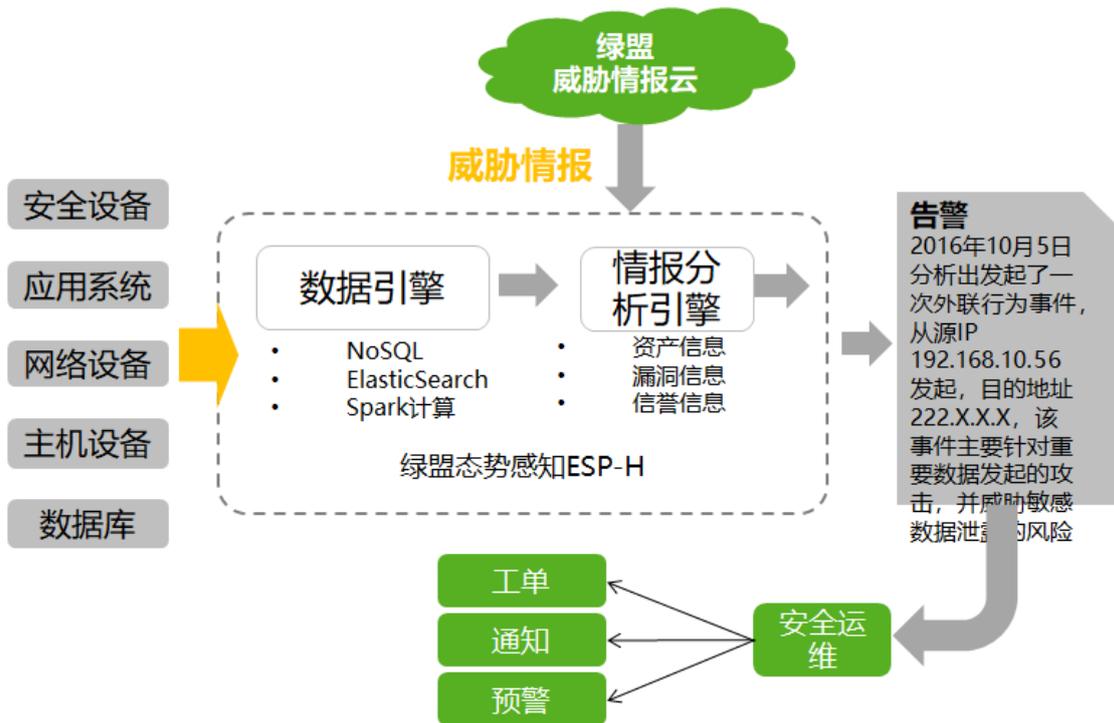
- 安全事件频发，经常到处救火，遇到重大漏洞和攻击总是晚人一步，怎么办？

### 2、问题：

- 如何提前预知 Oday 漏洞或重大攻击，实现主动预防？

### 3、方案：

绿盟安全管理平台支持威胁情报预警，全球第一时间接到预警，安全员提前处理，“主动预防”胜过“事后救火”，提前预防 Oday 漏洞和重大攻击的发生，减少安全损失。



## 2.5.8 态势感知

### 1、需求:

- 每次要钱做安全建设, 说不清楚安全投资效果, 领导不满意, 怎么办?

### 2、问题:

- 如何展示整体安全态势、洞察安全治理状态、体现安全投资价值?

### 3、方案:

绿盟安全管理平台支持安全可视化, 攻击、漏洞、资产分类态势呈现, 多种大屏展示, 清晰展现整体安全状态, 方便领导参观。另外支持安全治理, 风险管理数字量化, 安全风险持续跟踪, 安全投资效果说得清楚, 工作成果一目了然。



## 2.5.9 安全运营

### 1、需求：

- 每天发现很多漏洞和事件，忙不过来，不知道进度怎么样，不知道是否处理完，怎么办？

### 2、问题：

- 如何让安全运营责任到人、安全事件有始有终？

### 3、方案：

绿盟安全管理平台支持安全运营闭环，工单把责任到个人，事件可响应处置，运维有数据统计和报表，有始有终，全程跟踪，运营不用愁。



## 2.5.10 安全报表

### 1、需求：

- 工作阶段总结，向领导汇报，数据分散在各处，人工做报告费时费力，怎么办？

### 2、问题：

- 如何轻松完成安全报表，展示工作成绩？

### 3、方案：

绿盟安全管理平台将安全数据集中统计分析形成报表，具备威胁报表、漏洞报表等多种类型报表模板，支持日、周、月等不同周期，支持 html、pdf、word 等不同报表格式，支持自动化定期邮件发送报表，让 IT 人员轻松搞定报表，工作成绩有数据有报告。

运维报表

- 一、综述
  - 1.1 分析结果概览
    - 1.1.1 被攻击IP列表
    - 1.1.2 攻击者IP列表
    - 1.1.3 攻击源信息统计
- 二、高风险资产分析
  - 2.1 10.67.1.64(10.67.1.64)
    - 2.1.1 资产详情
    - 2.1.2 事件分析
      - 2.1.2.1 事件发现
    - 2.1.3 资产漏洞
    - 2.1.4 处置建议
  - 2.2 SMB共享文档(192.168.1.10)
    - 2.2.1 资产详情
    - 2.2.2 事件分析
      - 2.2.2.1 事件发现

## 一、综述

绿盟智能安全运营平台服务深入分析您在2020-06-29至2020-07-06期间的网络流量，发现3615616起威胁事件，616个资产，17138个威胁源

### 1.1 分析结果概览

#### 1.1.1 被攻击IP列表

序号	被攻击IP	威胁状态	安全事件
1	10.67.1.126	疑似失陷	
2	10.67.1.154	疑似失陷	
3	10.67.1.167	疑似失陷	
4	10.67.1.50	疑似失陷	
5	10.67.1.164	疑似失陷	
6	10.67.1.168	疑似失陷	
7	10.67.1.131	疑似失陷	

## 2.6 产品优势

绿盟安全管理平台具备三大优势：

### 2.6.1 合规，满足合规政策要求

绿盟安全管理平台在设计之初就充分考虑国家制定的等级保护标准中对于安全管理中心的安全设计技术要求。作为一个中心的安全管理中心，安全管理平台能够对定级系统中涉及安全计算环境、安全区域边界、安全通信网络的三重防护体系的安全信息进行集中化的安全信息与事件采集、分析、响应、处置，监测与分析系统的运行状态、用户行为，为定级系统信息安全管理体系的实施、检查和改进过程提供支持。

另外，绿盟安全管理平台支持等保合规检查。在通用合规检查方面按照等保二级、三级、四级展示检查项，用户可以对照检查项自行检测，检测时将实际网络环境与对比检查项进行比对，并自行给出检测结果（合规/不合规）。而面对业务系统合规检查，按照业务系统整体情况、等保二级、三级、四级展示检查项，用户可以对照检查项自行检测，检测时将实际网络环境与对比检查项进行比对，并自行给出检测结果（合规/不合规/不适用/未检测）。方便客户在等保合规日常运营中使用，随时检查合规符合度。

## 2.6.2 智能，减轻工作量提高效率

为了减轻客户工作量，提高效率，绿盟安全管理平台采用多种先进技术来提高平台的智能水平，让客户轻松使用。

### 1、事前，“智能”情报预警

绿盟安全管理平台支持威胁情报预警，全球第一时间接到预警，安全员提前处理，“主动预防”胜过“事后救火”，提前预防 0day 漏洞和重大攻击的发生，减少安全损失。

### 2、事中，“智能”安全分析

绿盟安全管理平台通过多源异构的日志数据采集和大数据分析，利用多源数据关联分析引擎、攻击链分析引擎、安全态势理解及推理引擎、威胁情报分析引擎、机器学习引擎、用户行为分析引擎等多种智能安全分析引擎，提升威胁检测准确性、覆盖度，实现平台比单个设备告警更准确、告警更少，比单个独立设备发现更多的隐蔽攻击，精准的事件告警减轻 IT 人员工作量。

### 3、事后，“智能”响应处置

绿盟安全管理平台具备灵活的响应处置方式，自动化一键封堵，通过联动防火墙、入侵防御系统、Web 应用防火墙、综合威胁探针、抗拒绝攻击系统等设备，及时避免风险扩散。还可扩展安全编排与自动化响应能力 SOAR，编排可视化，采集/分析/响应自动化，安全运营经验固化，提高运营效率。

## 2.6.3 运营，有效实现安全价值

绿盟安全管理平台支持安全运营闭环，工单把责任到个人，事件可响应处置，运维有数据统计和报表，有始有终，全程跟踪，运营不用愁。

同时绿盟安全管理平台融合了安全运营服务，可将客户本地的安全管理平台跟绿盟科技云端安全运营支撑平台对接，由绿盟云端专家给客户 7x24 小时的运营服务，并跟客户本地侧的驻场运营人员配合，实现热点事件的预警与防护、高危访问源的检测与封杀、可疑安全事件的发现与确认等系列闭环的安全运营服务，帮助企业降低整体的安全运营投入成本和风险、减轻客户的安全运营负担，保障企业网络安全，做到有组织，有流程，平台+设备+人，实现天、地、人、机协同的安全运营体系

作为有 20 年安全行业经验的安全行业领导企业，绿盟安全态势感知解决方案作为唯一的安全解决方案入选工信部《大数据优秀产品、服务和应用解决方案案例集》，并有多个相关项目入选工信部试点示范项目。绿盟科技的安全运营团队服务于运营商、金融、政府、能源、

交通、企业等各行各业，广泛应用于企事业单位“日常运维”、“红蓝对抗”、“上级安全检查”、“重大活动安全保障”等运营场景，拥有安全运营的最佳实践。

## 三. 典型部署

### 3.1 单机部署

单机部署是最简洁的系统部署模式，也是最典型的部署模式，适用于大部分企业客户的网络环境。在单机部署场景中，用户仅需在安全管理区旁路部署一台绿盟安全管理平台，并部署相应的安全探针设备，配置数据上传平台。用户就可以通过浏览器登录平台的交互界面，根据相应的权限进行各种管理操作。

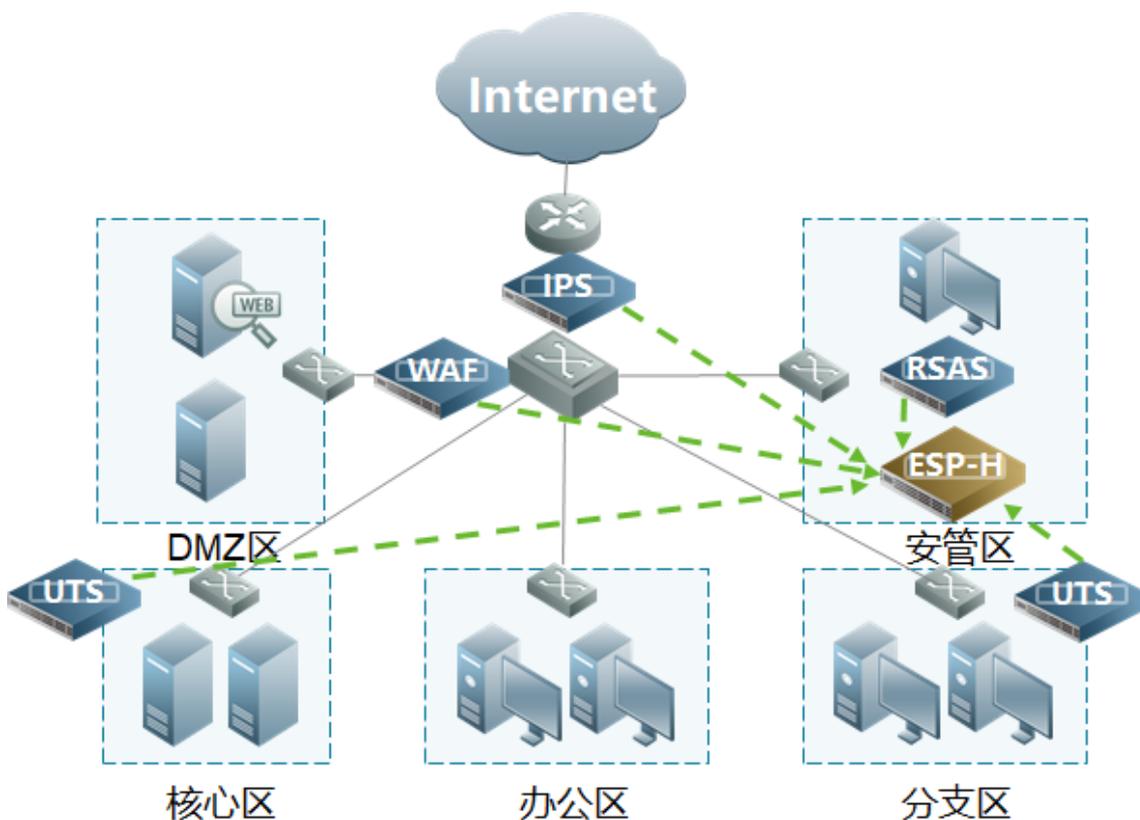


图 3.1 单机部署模式

## 3.2 级联部署

级联部署是指部署多个安全管理平台，并构建起一个一级平台连接若干个二级平台的部署模式。此时，在网络中就部署了多个安全管理平台，各个二级平台的管理员通过浏览器登录各自的二级平台所辖网络进行安全管理，一级平台的管理员则通过浏览器登录一级平台进行全网的统一管理、集中展现，并可以监督各个二级平台的管理工作。

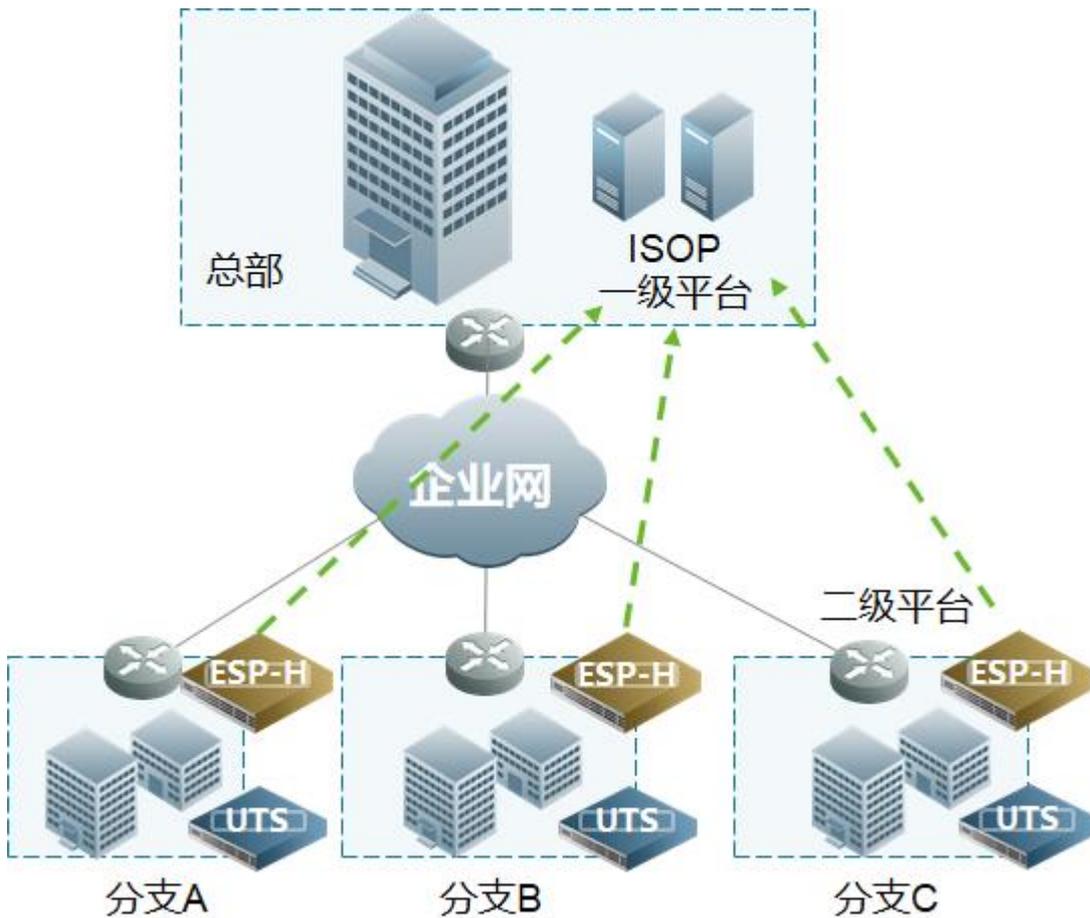


图 3.2 级联部署模式

## 四. 总结

随着安全技术的发展，安全管理平台或态势感知平台呈现多元化发展态势，什么样的态势感知方案是最佳选择？我们从三个方面来解读：

### 1、更多的专业探针，决定平台的价值

平台的数据来自探针，不同探针具有不同安全能力，适应不同的应用场景。可以说不同类型的探针越多，适用更多的场景，平台的价值越大。因此探针的专业能力越强，平台的价值越大，形成 1+1>2。

### 2、安全研究能力，决定方案的价值

懂安全，就要懂攻防。安全攻防研究能力越强，平台和探针的安全能力越强，整体方案才越有价值。比如：能否检测到最新的攻击，体现在平台和探针的规则和模型升级上，体现在机器学习的算法上。更强的安全研究能力，让规则和模型升级更快、更准确。比如：威胁情报来自对全球安全威胁的深入研究与跟踪，第一时间将最新漏洞或重大攻击通报给平台，提前处置，事前预警。

### 3、从平台、产品到运营，决定客户的价值

以平台和探针为工具，以运营服务为纽带，形成客户安全运营的核心。所以懂运营，有安全服务团队，才能帮助客户解决安全问题，才能让客户投资产生真正价值。

随着“互联网+”的全面推进，信息技术在国家社会经济建设中的应用也越来越广泛，新型的网络安全威胁也更加突出，传统以“防护”为主的安全体系将面临极大挑战。未来网络安全防御体系将更加看重网络安全的监测和响应能力，充分利用网络全流量、大数据分析及预测技术，大幅提高安全事件监测预警和快速响应能力，应对大量未知安全威胁。

作为满足合规要求的轻量级安全态势感知平台，绿盟安全管理平台聚焦威胁、脆弱性、资产的风险三要素，以安全分析为核心，结合云端威胁情报，通过各种攻防场景及可视化手段，协助企业构建一个从防御、检测、响应、到预测于一体的自适应系统，从安全运营角度落实平台与流程，帮助客户运营好安全。