网络安全态势感知技术

陆　军　编著

WANGLUO ANQUAN TAISHI GANZHI JISHU

中国铁道出版社有限公司
CHINA RAILWAY PUBLISHING HOUSE CO., LTD.

网络安全态势感知技术

陆　军　编著

中国铁道出版社有限公司
CHINA RAILWAY PUBLISHING HOUSE CO., LTD.

内 容 简 介

本书首先介绍网络安全态势感知的基础知识以及网络安全态势感知的主要技术，其次针对网络安全态势感知的过程进行详细的数据分析及模拟，主要包括网络安全态势感知的框架及数据融合、网络安全态势感知的识别、网络安全态势感知的评估建模、网络安全态势感知的态势预测。

本书适合作为高等院校网络安全相关专业的教材，也可供网络安全工程师及研究人员阅读。

图书在版编目（CIP）数据

网络安全态势感知技术/陆军编著. —北京：中国铁道出版社有限公司，2019.4

ISBN 978-7-113-25645-6

Ⅰ.①网… Ⅱ.①陆… Ⅲ.①计算机网络-网络安全 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2019）第 049708 号

书　　名：网络安全态势感知技术

作　　者：陆　军　编著

策　　划：潘晨曦　孙晨光　　**读者热线：**（010）63550836

责任编辑：秦绪好　包　宁

封面设计：刘　颖

责任校对：张玉华

责任印制：郭向伟

出版发行：中国铁道出版社有限公司（100054，北京市西城区右安门西街 8 号）

网　　址：http://www.tdpress.com/51eds/

印　　刷：北京虎彩文化传播有限公司

版　　次：2019 年 4 月第 1 版　2019 年 4 月第 1 次印刷

开　　本：787 mm×1 092 mm　1/16　**印张：**9　**字数：**188 千

书　　号：ISBN 978-7-113-25645-6

定　　价：32.00 元

Preface

前 言

近年来，随着互联网在全球的迅速发展和各种互联网应用的快速普及，网络已成为人们日常工作生活中不可或缺的信息承载工具，网络改变了人们的生活、工作方式，使信息的获取、传递、处理和利用更加高效、迅捷，这不仅促进了社会生产，也丰富了人们的生活。与此同时计算机网络也成为一个国家最为关键的政治、经济和军事资源，成为国家实力的象征。然而，随着网络规模的不断壮大，网络结构的日益复杂，网络病毒、DDoS 攻击等构成的威胁和损失越来越大，传统的网络安全管理模式仅仅依靠防火墙、防病毒、IDS 等单一的网络安全防护技术来实现被动的网络安全管理，已满足不了目前网络安全的要求，因此迫切需要新的技术来对网络安全状况进行实时监控和预警。安全态势感知技术就是对当前和未来一段时间内的网络安全状态进行定量和定性的评价，实时监测和预警的一种新的安全技术。

网络安全态势感知可看成自然空间战场态势感知在虚拟环境中的一次延伸。开展这项研究旨在建立网络安全态势感知系统，为网络安全管理员了解网络安全态势，迅速做出反应提供决策支持和指挥控制。目前网络正朝着大规模、高度分布式的方向发展，同时入侵攻击行为也正朝规模化、分布化、复杂化等方向发展和演化。网络威胁态势感知可对获取到的大量多源异构威胁信息进行融合处理，将融合结果进行图形化展示，为管理员应对网络威胁提供决策参考。由于网络威胁态势感知技术的数据源覆盖了各类网络安全设备，感知结果比较客观、准确，同时具有较好的实时性，使得网络管理员能够迅速判断当前网络威胁态势，及时制定应对措施，减小和预防网络威胁带来的破坏。因此，开展网络威胁态势感知研究具有重要意义和实用价值。

本书主要内容包括网络安全态势的基础知识、网络安全态势感知中的关键技术、基于 Agent 理论的网络安全态势感知框架构建、基于径向基神经网络的多源数据融合、网络安全态势的识别研究、网络安全态势评估及其建模、网络安全态势的预测研究。

限于作者水平有限，书中不当甚至疏漏之处在所难免，诚恳期待有关专家批评指正。

编 者

2018 年 12 月

Contents

目 录

第1章 网络安全态势的基础知识

“态势感知（Situation Awareness，SA）”严格来说并不是一个新名词。早在 20 世纪 80 年代，美国空军就提出了态势感知的概念，覆盖感知（感觉）、理解和预测三个层次。90 年代，态势感知的概念开始逐渐被接受，并随着网络的兴起而升级为“网络态势感知（Cyberspace Situation Awareness，CSA）”，是指在大规模网络环境中对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及最近发展趋势的顺延性预测，而最终的目的是要进行决策与行动。

随着网络安全重要性的凸显，态势感知开始在网络安全领域崭露头角。2009 年，美国白宫在公布的网络空间安全战略文件中明确提出要构建态势感知能力，并梳理出具备态势感知能力和职责的国家级网络安全中心或机构，包含了国家网络安全中心（NCSC）、情报部门、司法与反间谍部门、US-CERT、网络作战部门的网络安全中心（Cyber Security Center）等，覆盖了国家安全、情报、司法、公私合作等各个领域。

2016 年 4 月 19 日，习近平主席在与网络安全业界人士座谈会上明确指出：“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。”全天候全方位感知网络安全态势。知己知彼，才能百战不殆。没有意识到风险是最大的风险。网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是“谁进来了不知道，是敌是友不知道，干了什么不知道”，长期“潜伏”在里面，一旦有事就发作了。

现阶段面对传统安全防御体系失效的风险，态势感知能够全面感知网络安全威胁态势、洞悉网络及应用运行健康状态、通过全流量分析技术实现完整的网络攻击溯源取证，帮助安全人员采取针对性响应处置措施。

所以态势感知系统应该具备网络空间安全持续监控能力，能够及时发现各种攻击威胁与异常；具备威胁调查分析及可视化能力，可以对威胁相关的影响范围、攻击路径、目的、手段进行快速判别，从而支撑有效的安全决策和响应；能够建立安全预警机制，来完善风险控制、应急响应和整体安全防护的水平。

随着《网络安全法》和《国家网络安全战略》的相继出台，态势感知被提升到了战略高度，众多大行业、大型企业都开始倡导、建设和积极应用态势感知系统，以应对网络空间安全严峻挑战。

如今，“态势感知”已经成为网络空间安全领域聚焦的热点，也成为网络安全技术、产品、方案不断创新、发展、演进的汇集体现，更代表了当前网络安全攻防对抗的最新趋势。

网络安全态势感知主要应用方向为监管机构：从国家层面、省市大地域层面，对国计民生相关的关键信息基础设施的安全态势进行整体的监测与关注。大型行业：从体系内部建立态势感知，应用于内部系统的安全运营，发现重要威胁，解决问题，把安全能力落地；通过态势感知对多分支或二级单位进行外部监管，以提升整体的安全状态的掌握，同时与监管机构进行事件应急处置及威胁情报的合作。大型机构或企业：从日常安全工作角度出发，对内部有价值的核心资产、业务系统安全状态进行感知，发现各类威胁与内部的异常违规，保证业务系统能够比较平稳、顺畅地运行。

网络安全态势感知是未来网络安全管理系统的发展方向，网络安全管理的需求决定了网络安全态势感知的研究内容。为准确地感知网络安全态势，需要高效的事件检测方法和态势评价指标体系。态势感知作为网络安全管理中新的研究领域，为网络安全管理系统的设计指明了努力的方向。结合当前网络安全态势领域的研究成果，定义并介绍了网络安全态势感知过程中的各处理阶段：① 网络安全态势识别；② 网络安全态势理解；③ 网络安全态势预测。

1.1 态势感知的概念

态势感知（Situation Awareness，SA）是一个来自于军事领域的概念，源于 A&A 领域中的人因（Human Factor，HF）研究，被认为是对态势进行评估以获得决策执行的过程，常用于人机交互（Human-Computer Interactions，HCI）系统。在数据融合领域中，这个术语被态势评估（Situation Assessment）所替代。态势感知是为了在环境对象和环境自身之间建立相互映射关系，其由分布式传感器、位置信息、用户规则或系统监视和维护的工具所提供。

态势是趋势和状态的合称，是对当前或者未来环境状况的一种反映，脱离了环境来谈论态势都是行不通的，网络态势指的是整个网络环境在运行过程中所呈现出来的状况和趋势。态势感知最初在 20 世纪 80 年代中期由 Endsley 提出，他认为态势感知是在某种条件下对某种环境的各个因素进行分析，从而预测出该环境的未来走向。Bass 在其第一次对在网络环境基础上的态势感知进行概念界定的时候，通过对多元化的网络数据来源进行分析，把结构各不相同的数据进行统一化处理，形成架构类型相同的数据，然后把这些数据进行处理，绘出网络态势模型，在模型上标注时间维度和空间维度，对网络空间环境的各个影响因子进行评测，根据各个因子的状况和走势，从而评估和预测网络空间当前和未来的态势，同时他利用 IDS 的多个网络传感器的安全事件构成多源数据，将传感器信息转化为高层次的网络行为。

目前，人们对网络安全态势感知的研究存在 3 种观点：① 认为 NSSA 是网络安全事件应用大数据处理和可视化技术的汇总结果，如传统的安全服务提供商（McAfee、Symantec）

及新出现的重点关心 APT 攻击的企业（Fire Eye、Mandiant）等，通过公开一些技术报告记录 APT 的攻击实例；② 认为 NSSA 是基于网络安全事件融合计算的网络安全状态量化表达；③ 认为 NSSA 作为一种网络安全管理工具，是网络安全监测的一种实现形式，并提出了诸多模型。

Endsley 提出了适用于自动化及人机接口系统的态势感知过程，并将态势感知的信息处理过程分为三个阶段：

（1）识别（Perception）：检测和获取环境中的重要线索或元素，这是态势感知中基础的一步。

（2）理解（Comprehension）：整合识别到的数据和信息，分析其相关性。

（3）预测（Projection）：基于对环境信息的感知和理解，预测未来的发展趋势，这是态势感知中最高层次的要求。

Dominguez 把态势感知的基本定义扩展为如下 4 个阶段：

（1）提取环境信息。

（2）整合当前环境的信息和相关的环境内部元素的信息，生成当前态势视图。

（3）利用当前的视图去指导更进一步的感知获取。

（4）对未来的事件进行预测。

1.2 网络安全态势感知

网络安全态势是什么？这是一个在研究过程中需要首先明确的概念。网络安全态势是由各种网络设备运行状况、网络行为以及用户行为等因素所构成的整个网络当前状态和未来变化趋势。网络安全态势感知（又称网络安全态势评估）则是在大规模网络环境中，对能够引起网络安全态势变化的安全要素进行获取、理解、显示以及预测未来的发展趋势的过程。“态势”作为一种状态、一种趋势，是一个整体和全局的概念，任何单一情况或状态均不能称为态势。

1999 年，TimBass 首次提出了网络安全态势感知概念，并将其与空中交通监管领域的态势感知过程进行类比，目的是把 ATC 中态势感知的相关成熟理论和技术借鉴到网络安全态势感知中来。TimBass 建立的基于多源数据融合和数据挖掘技术的网络态势感知框架主要是在入侵检测的基础上，通过识别攻击者的身份、攻击速度、威胁程度和攻击目标，进行网络态势的感知。网络态势感知是在大规模网络环境中，对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。

网络安全态势感知 NSSA 是对网络系统安全状态的认知过程，包括对从系统中测量到的原始数据逐步进行融合处理和实现对系统的背景状态及活动语义的提取，识别出存在的各类网络活动以及其中异常活动的意图，从而获得据此表征的网络安全态势和该态势对网络系统正常行为影响的了解。定义中需要解释的是：网络系统是对各种形态网络的抽象，包括计算机互联网、物联网以及其他采用不同通信方式和终端类型的网络，这

意味着不同类型的网络在网络安全态势感知的概念和方法上是具有共性的，测量是对各种网络检测功能的抽象，包括网络管理数据和网络安全监测数据，测量数据的生成不是 NSSA 的任务，而这些数据的获取则是 NSSA 的任务。这意味着网络安全态势感知的研究目标与研究内容与网络管理和网络入侵检测等这些传统的研究领域之间有着区分和不同的侧重点。背景状态是系统当前所处的运行状态，这是动态变化的，与系统之前的部署和定义可能是不一致的。“安全”只有在动态的系统中才有意义，因此，攻击活动及安全缺陷对系统的影响效果，应当基于系统当前的状态进行判定，活动语义是系统中的主体作用于客体的动作所构成的序列，要进行安全态势察觉，管理人员应当了解系统中存在的所有活动，不能仅止于辨识攻击活动，即要辨清敌我。响应决策本身不是 NSSA 的任务，因为态势感知只是 OODA 的支撑技术。这意味着安全响应技术和安全策略管理技术等传统上属于网络安全管理领域的内容，不属于网络安全态势感知的研究范畴。

根据上述定义，NSSA 的任务包括网络安全态势觉察、网络安全态势理解、网络安全态势投射这 3 个层面。其中，态势觉察完成原始测量数据的融合与语义提取任务以及活动辨识任务，态势理解完成这些辨识出的活动的意图理解任务，态势投射完成这些活动意图所产生的威胁判断任务。层与层之间存在依赖关系，即如果网络安全态势觉察和网络安全态势理解没有合理的结果，得到网络安全态势投射很可能也是不正确的或不完整的，但另一方面，每层的结果均可独立呈现并直接使用，以满足不同的网络安全管理需要。这意味着网络安全态势感知的结果及其表达方式具有多样性，蕴含的语义粒度也可以随需求的视角而不同，但是无论如何，网络安全态势感知的结果应当是可响应的（Reactionable），否则，缺乏实际意义。另外，网络安全态势感知是一个测量数据驱动的认知过程，测量数据的数量与质量影响感知的结果。

基于上述理解，我们给出网络安全态势感知的一般功能模型，图 1.1 所示模型包含网络安全态势觉察、网络安全态势理解、网络安全态势投射及可视化等模块，下面简要概括各模块的功能。

网络安全态势觉察的主要目的是辨识出系统中的活动，即对网络中相关的检测设备与管理系统产生的 Raw Data 进行降噪、规范化处理，得到有效信息，然后对这些信息进行关联性分析，识别出系统中有“谁”（系统中的主体、客体）存在，进一步分辨出异常的活动；网络安全态势理解的主要任务是在网络安全态势觉察的基础上发现攻击活动，理解并关联攻击活动的语义，然后在此基础上理解其意图；网络安全态势投射的主要任务是在前两步的基础上分析并评估攻击活动对当前系统中各个对象的威胁情况，这种投射包括发现这些攻击活动在对象上已经产生和可能产生（即预测）的效果，通过将态势感知的结果投射到确定的系统对象上，可以获得该对象在当前态势下的状态。尽管要感知的是系统中的活动，而感知的最终结果则应表达为这些活动对系统对象的影响，不能仅止于活动的识别，因为系统因之而产生的反应是施加于对象的，而不是直接施加于活动本身。这是一个再认识的过程，即融合从系统中观察到的各个对象的状态以构成态势，再看这个态势对系统各个对象的意义。

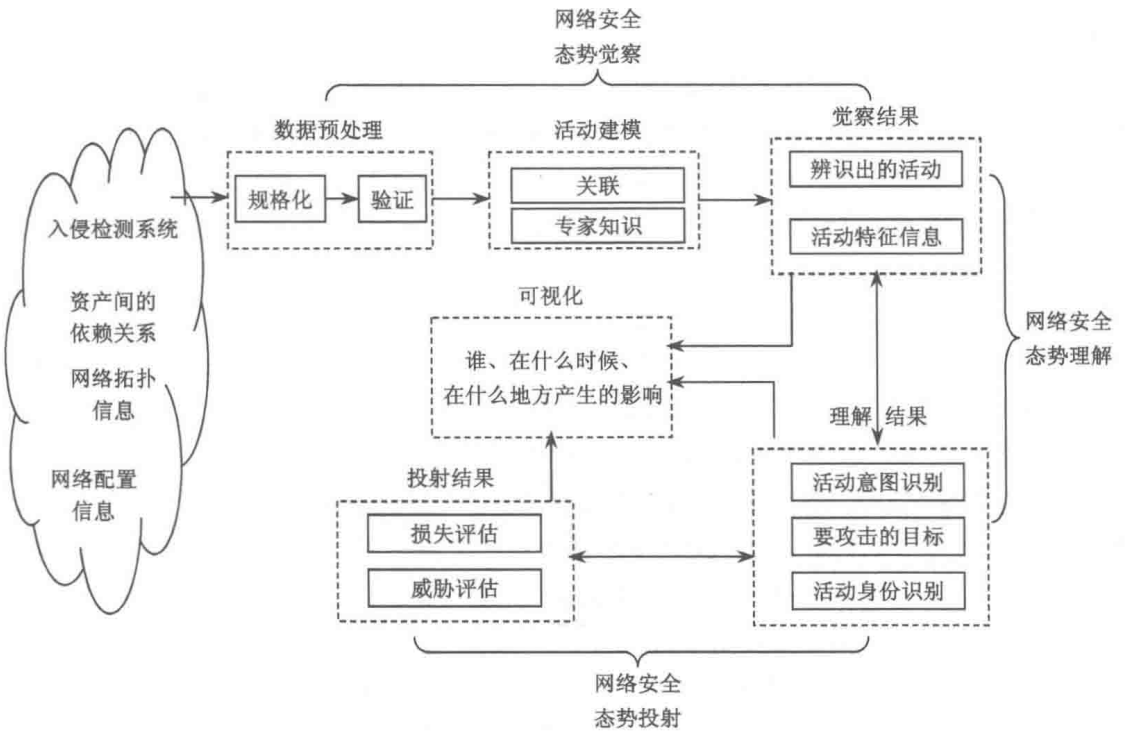

图 1.1　网络安全感知模型

网络态势感知是网络管理发展的重要拐点，在如今极为动荡和复杂化的网络环境中需要更为强大的态势感知功能，能够快速而高效地获取有用信息，实现系统化和多元化的网络特征指标体系，让它能够具体呈现网络整体区域的安全状态，进而帮助实际网络得到高效管理与控制，有效提升对于网络安全的理解能力，并提供决策支持。网络安全态势感知过程主要是通过提取出网络安全态势分析指标体系，建立基于复杂网络行为模型与模拟的网络安全态势分析与预测体系，进而得出量化的或定性的网络安全态势评估结果并通过对历史态势的分析、建模，对未来的网络安全态势演化进行预测，以便网络安全管理人员对网络内的安全要素、安全设备、信息系统进行合理的调整、升级，应对网络安全态势的变化。因此，开展网络安全态势分析研究具有十分重要的意义。

1.2.1　国内外研究现状

将态势感知应用于网络管理就衍生出网络态势感知技术。1999 年，TimBass 首次通过把从多种数据源得到的数据信息进行融合，形成准确和有效的信息和知识库，帮助和指导网络管理员对自身网络安全状况做出合理的决策。TimBass 模型明确了基于多源数据融合的态势感知是下一代分布式入侵检测系统的研究方向。

早期进行网络安全态势感知研究的还有 Stephen G. Batsell、Jason Shifflet、William Yurcik、A. DeMontigny-Leboeuf 等，但只是做了将态势感知在不同领域的移植工作，并没有提出针对网络本身的态势感知技术。2004 年，Seng 指出“网络态势感知是网络环境中所有信息按照逻辑约束关系进行组合的结果”。2007 年，Lacey 等提出了一个网络空间态

势感知框架，对网络态势感知进行系统研究。

随着网络呈现出多样化、复杂化和规模化的发展趋势，网络安全问题越来越受到人们的广泛关注，如何有效应对各类网络入侵和威胁、及时准确地感知当前网络安全态势，成为网络与信息安全领域关注的重点问题。传统的以防火墙、入侵检测、防病毒等单点防御设备为基础的解决方案，只能对网络入侵信息进行单独处理，彼此间缺乏协同操作，在应对大规模协同攻击时，防御能力更显力不从心。为解决这一问题，网络安全态势感知（Network Security Situation Awareness）技术应运而生，该技术从整体上综合考虑各种安全要素，动态反映网络安全状态，准确预测潜在恶意行为，协助网络管理员进行科学决策。近年来，广大研究人员围绕网络安全态势感知技术展开了大量研究。2012 年，King 等指出深度包检测技术能够在分类属性网络中提供全面深刻的态势感知结果。2013 年，Varun 等基于事件学习理论构建网络攻击检测模型，用于分析网络攻击态势。2014 年，Bode 等构建了一个贝叶斯网络模型用于网络态势的风险管理。2015 年，Friedberg 等提出一个新型安全机制——基于事件自动关联的事件检测 AECID，用于网络异常行为的态势感知。

目前，国内网络安全态势感知的研究处于快速发展阶段，大多是从全面获取网络安全数据入手，研究数据之间的关联性和进行数据融合的方法，制定指标体系，进而得到网络安全态势评估结果。陈秀真提出基于层次化网络安全态势威胁态势评估方法，通过对报警日志进行统计分析，综合考虑服务和主机的重要性以及网络结构，提出层次化的量化评估模型和对应的网络安全态势计算方法。但其没有考虑攻击威胁的关联和发展过程，只是笼统地给出不同时间点的综合威胁量化值，不能说明各种攻击在安全态势变化过程中的作用和关联关系。

韦勇提出了基于信息融合的网络安全态势评估框架，该框架借鉴了层次化的思想，利用证据理论对节点上的安全要素进行融合，然后，依据节点、子网、全网的思路，对态势进行层层融合，从而得到整个网络的态势值。该框架能够对多源安全事件进行有效处理，合理地利用了多源信息之间的互补性，提高了态势感知的准确性。

刘效武提出基于多源异质融合的网络安全态势生成与评估 NSSA 方法，将支持向量机作为融合引擎，融合异质多传感器的数据信息，结合特征约简算法，提高融合实时性，并在此基础上，设计态势生成算法，计算网络安全态势。最后，运用安全态势评价指标对量化态势感知进行了评价。

湖南工业大学的叶健健构建了基于贝叶斯方法的感知模型，该模型在对历史监测数据进行分析的基础上，得到先验概率，然后根据时序模型对实时监测数据进行处理，在结合历史统计数据及实时数据基础上进行安全预测，利用层次化的网络结构，该模型可以准确、快速地对网络实时事件进行响应。华北电力大学的李淳创造性地开发了一个以时间维度为主要感知模式的评估手段，李淳依据预测时长的不同，针对短期及长期评估采用了不同的方法，短期评估主要依据安全监测设备的告警信息为数据基础，通过告警确定主机的状态进而得到网络短期内的安全态势趋势；而长期评估主要依据短期评估的结果，综合考虑各项指标数据，以熵值法确定指标的权重。这种评估方法对短期及长期

的评估进行了区别对待，弥补了由于时间段不一造成的态势评估的偏差。南京航空航天大学的黄同庆针对预测实时性的问题，提出了一种实时预测方法，设计了基于隐马尔科夫模型的实时 NSSA 预测模型，利用网络中的所有主机及关键安全设备预测网络的安全态势变化。辽宁工程技术大学的陈虹提出一种基于多源数据融合定量评估体系，该体系综合考虑主机及链路信息，利用 D-S 证据理论进行数据融合，得到各类安全事件的集合，从而得出网络环境是否安全的结论。

以上研究多数是从全面获取网络安全相关信息入手，在此基础上研究各种信息之间的关联性，以及如何将这些信息通过数据融合方法进行融合，从中提取出更深层次的信息，进而根据制定的指标体系得到对网络当前安全状态的评估。上述方法基本覆盖了态势感知的模型、评估方法和预测方法等各个层面，比较全面地解决了态势感知的各个阶段。但是，这些研究在态势要素的考虑上还不够全面，在态势评估方法和预测方法等方面的研究主要是把其他领域的研究成果运用到态势感知领域，并未为其进行有效的优化工作，从而导致现有评估方法和预测方法与实际结果的拟合性出现较大偏差，感知结果的精确性不高。这些都为网络安全态势感知模型的算法优化留下了研究的空间。

1.2.2 网络安全的主要威胁及态势分析

1. 网络安全的主要威胁

由于网络和信息系统的开放性，信息在生成、存储、处理、传输的整个生命周期内都容易受到窃取、篡改、破坏等安全威胁。近年来，随着计算机和网络技术的飞速发展，信息系统的应用领域日益广泛。与此同时，网络攻击技术和手段也不断提高，计算机网络所面临的威胁日趋严峻。网络安全的三要素包括：机密性、完整性、可用性。安全威胁是指对网络安全三要素造成破坏的事件或要素。目前，计算机网络所面临的安全威胁主要表现行为有：

1）假冒

假冒是指伪造合法者的凭证，假冒合法者的身份，访问或破坏未授权信息的行为。假冒一般通过盗窃密钥、重放数据包等形式进行，对信息系统的威胁较大。

该类攻击主要影响安全三要素中的机密性和完整性。

2）拒绝服务

拒绝服务是指对系统进行攻击，造成信息系统的正常对外服务中断，服务的中断可能是暂时性的，也可能是永久性的。该类攻击主要影响安全三要素中的可用性。

3）窃听

窃听是指通过搭线等方式对信号进行监听。攻击者利用计算机信息在产生、处理、传输、存储等环节所可能存在的安全漏洞，对信息进行监听截获。该类攻击主要影响安全三要素中的机密性。

4）后门

后门是进入系统的一种方法。后门一般由开发者预设，主要用于对目标系统的远程

监视与控制，对目标系统进行潜在的恶意破坏。少数情况下，后门是由于开发者在系统设计过程中的疏忽而形成。

随着 Internet 急剧扩大和上网用户迅速增加，风险变得更加严重和复杂。原来由单个计算机安全事故引起的损害可能传播到其他系统，引起大范围的瘫痪和损失；另外加上缺乏安全控制机制和对 Internet 安全政策的熟悉不足，这些风险正日益严重。针对这个企业局域网中存在的安全隐患，在进行安全方案设计时，下述安全风险我们必须要认真考虑，并且要针对面临的风险，采取相应的安全措施。从网络态势安全感知系统的角度来看，针对办公局域网安全需求主要包含了资产识别、脆弱性识别、威胁检测、安全态势评估以及安全态势的预测。

网络安全的首要评估要素是资产，其他的评估都主要是以资产评估为基础的，也即是在网络的安全态势感知当中，首先需要关注的安全问题就是资产面临的安全问题，脆弱性评估主要是指对资产本身的脆弱性，潜在的影响评估主要是针对资产的负面影响的评估。对现有的安全措施的评估也主要是指对资产当前安全措施情况进行的评估，因此一般来说，资产评估对于安全态势感知的综合性评估至关重要。在资产识别过程中，主要识别的是网络中的主机信息。资产识别主要包括两个方面：资产赋值和资产的自动识别，资产识别主要是为下一阶段的评估打基础，也是为下一阶段的评估提供一定的信息基础，从而使得后续的评估具有一定的数据。以下主要对资产自动识别和资产赋值两个资产识别的过程进行分析：

（1）资产识别的内容主要包括主机软件资产的识别和硬件资产的识别。

软件资产主要包括主机操作系统相关的信息，包括操作系统的版本、安全措施、端口等内容。硬件资产主要包括主机的 CPU、主机的内存、主机的硬盘、主机的网卡等信息。包括型号、频率、带宽、分辨率、系统文件等内容。

（2）资产赋值是指根据《信息安全风险评估规范》的相关要求，对网络安全的资产进行详细的分析和研究，从而赋值。

造成网络信息安全问题的主要原因是系统的防御能力较弱，系统本身存在较大的缺陷和漏洞，从而使得一些病毒等容易入侵。许多企业为了加强网络的安全性会设置一些防御措施，在网络的防御当中，第一道防御措施是加强网络的坚固性，降低网络的脆弱性，网络安全的脆弱性主要用来衡量网络的抵御系数，从而使得第一道安全防线能够识别网络的脆弱，然后利用采取相关的措施进行抵御。由此可知，识别网络安全的脆弱性对于发展系统漏洞至关重要。因此也是网络安全识别的重要内容。

网络安全的脆弱性识别是指对网络节点进行扫描，包括系统的版本信息、硬件信息、漏洞补丁、系统服务、系统所使用和安装的安全软件等内容都需要进行详细的扫描和分析，通过利用网络安全管理规范的软件开发包实现系统的网络编程；通过 WMI 可以对系统的补丁安装情况等进行扫描，通过对比补丁安装库可以了解系统的补丁安装情况，然后查找出哪些补丁没有安装；可以利用端口扫描技术对系统的安装端口进行分析和研究，从而及时检测端口的安全状态。通过脆弱性识别可以在系统受到攻击时进行准确的测评，

不仅能够有效地分析外部对系统的攻击，而且还可以对系统内部进行分析和预测，通过评估结果可以分析出系统的安全状态，展示系统容易受到攻击的地方，从而加强这些方面的安全管理，使得整个系统一直处于较为安全的状态，提高系统的安全性。

2. 系统的威胁检测

系统的威胁检测主要包括三个方面，资源控制、入侵检测和文件监视。下面主要对这三个方面的检测内容进行分析和研究：

1）资源控制

资源控制主要是对网络中的硬件、软件等资源进行管理与控制。网络资源包括系统的软件和硬件资源，包括系统中心处理器的使用情况、系统内存的使用情况、系统硬盘的使用情况、系统的运行状况等内容。例如，如果系统中心处理器的使用频率过高，病毒容易入侵系统，从而导致中央处理器额外的功耗，通过实施监控可以分析出病毒，并及时对系统进行杀毒，从而保证整个系统的资源处于正常状态，保证整个网络的安全。同时在资源监控的过程中，会存储很多系统资源评定数据，例如，各类资源运行的正常阈值等，这些阈值用来评定系统资源是否处于正常状态，也为网络安全的态势评估提供了一定的数据。

2）入侵检测

入侵检测主要是指通过分析和研究，对系统的网络数据进行监控，一旦发现数据存在问题就将这些数据记录下来，从而为下一个简单的威胁识别提供一定的分析数据，网络数据包的检测主要是将系统的网络数据进行监控和调节，发现系统中存在的异常数据，这些异常数据可以是基于数据特征而得到的数据以及通过统计分析得出的数据，这些数据都有可能对网络的安全造成危险。

基于特征的数据主要是指按照之前系统中存储的各类数据的特征以及规则，然后将系统的数据与存储的数据进行检测，如果发现两者之间存在较大差异，则认定这些数据是异常数据。这种方法的主要优点是较为简单，能够及时排除一些基础的异常数据，但是毕竟系统中存数的数据类型有限，而现在网络中流动的数据类型较多，因此对于一些系统没有存储的数据类型，该方法不能很好地检测出来。由此可知，这种检测效率较低。而基于统计的检测则主要使用通过对系统的流量进行分析得到的，通过一定的流量监测模型分析系统当中一定时期内的流量行为，一旦发现系统的流量异常则就判定系统中存在入侵威胁，这种方式的优点是可以很好地判定系统是否受到新威胁，但是不能够准确地了解威胁的原因。

3）文件监视

文件监视主要是指对主机文件的访问、修改、删除等信息进行监视与控制。当前很多企业为了加强企业内部的信息共享，建立各种局域网，这些局域网能够提高信息的共享率，但是也容易导致一些网络安全问题出现。因此及时查找文件中存在的问题也能够很好地对威胁进行检测。一旦发现系统中的文件被篡改，就需要及时报告，从而采取措施对这些威胁进行抵御，以防出现安全危险。