工程管理
Journal of Project Management
第 4 卷◆第 11 期◆版本 1.0◆2023 年
文章类型：论文| 刊号（ISSN）：2737-4580(P) / 2737-4599(O)

态势感知平台在网络安全中的作用

黎岗
江铃汽车集团有限公司
DOI:10.12238/jpm.v4i10.6316

[摘　要] 态势感知平台在网络安全中扮演着重要的角色。本文以某汽车集团有限公司为例，探讨了态势感知平台在网络安全中的重要作用。通过对网络攻击态势的实时监测和分析，态势感知平台可以帮助企业及时识别、预警和应对各类网络威胁，提高网络安全防护能力。文章从平台的工程概况、功能特点和应用实例等方面进行综述，旨在为其他企业在网络安全领域提供参考。
[关键词] 态势感知平台；网络安全；实时监测；预警；应对

The role of situational awareness platform in network security

Li Gang
Jiangling Automobile Group Co., LTD., Jiangxi Nanchang 330000

[Abstract] Situational awareness platform plays an important role in network security. This paper discusses the important role of situational awareness platform in network security. Through the real-time monitoring and analysis of the network attack situation, the situational awareness platform can help enterprises to timely identify, early warn and respond to all kinds of network threats, and improve the ability of network security protection. This paper summarizes the engineering overview, functional characteristics and application examples of the platform, aiming to provide reference for other enterprises in the field of network security.
[Key words] situational awareness platform; network security; real-time monitoring; early warning; response

前言

随着信息技术的飞速发展，网络攻击和威胁也日益增多和复杂化。某汽车集团有限公司面临着来自网络上的各种潜在风险和威胁。因此，通过建立一个高效可靠的网络安全防护系统成为了该公司的迫切需求。本文将重点探讨态势感知平台在网络安全中的作用，并结合某汽车集团有限公司的实践经验，展示该平台在实际应用中的效果和价值。

一、实时监测网络威胁

态势感知平台在网络安全中扮演着重要角色，其中实时监测网络威胁是其关键功能之一。以下将详细阐述实时监测网络威胁的具体内容。

（一）实时流量监测

态势感知平台通过监测网络流量，包括入口和出口数据流，实时获取网络中的通信情况。通过对流量数据的分析、挖掘和比对，平台可以检测到异常的网络活动和潜在的网络威胁。在某汽车集团有限公司的网络中，当态势感知平台发现某个内部计算机与境外主机建立大量的连接并传输大量数据时，平台会立即将该行为视为异常，可能存在恶意攻击或数据泄露的风险，并提醒相关人员采取适当的应对措施[1]。

（二）威胁情报收集和分析

态势感知平台还可以实时收集、整理和分析来自不同渠道的威胁情报。这些威胁情报包括已知的攻击方式、漏洞信息、恶意软件样本等。通过与实时流量数据的匹配和比对，平台可以发现威胁情报所描述的攻击行为并进行预警。在某汽车集团有限公司的网络中，当态势感知平台收到来自安全厂商的最新威胁情报，指出存在一种新型的勒索软件正在通过邮件传播时，平台会开始实时监测企业网络中是否有类似的恶意文件传输，及时发现潜在的威胁，并通知相关人员立即切断与该邮件相关的连接或采取其他相应措施。

（三）异常行为检测和分析

态势感知平台还可以利用机器学习和行为分析等技术，对网络中的异常行为进行检测和分析。通过学习正常的网络行为模式，当检测到与该模式不符的行为时，平台会发出警报，提示潜在的网络威胁。在某汽车集团有限公司的网络中，当态势感知平台观察到某个服务器在非工作时间频繁上传待加密的文件，并且这些文件与该服务器正常工作无关时，平台会认定

该行为为异常行为，可能存在数据泄露或内部威胁的风险，并发出相应的警报。

二、预警和预测网络攻击

态势感知平台可以利用历史数据和机器学习算法，进行网络攻击的预警和预测。通过对网络威胁的趋势分析和行为模式识别，平台能够提前发现潜在的网络攻击，并及时采取防护措施。下面将详细阐述预警和预测网络攻击的具体内容，并结合某汽车集团有限公司的实例进行说明。

（一）预警网络攻击

预警网络攻击是指通过态势感知平台对网络流量、威胁情报和异常行为等进行实时监测和分析，发现可能的网络攻击行为，并及时发送警报通知相关人员。预警可以帮助企业及时发现潜在的攻击活动，采取相应的应对措施，从而降低被攻击的风险。在某汽车集团有限公司的网络中，当态势感知平台检测到一组 IP 地址频繁尝试对内部服务器进行暴力破解时，系统会判断这是一个可能的恶意攻击，立即发出预警通知给安全团队。安全团队会根据预警信息及时调查并采取必要的措施，例如封锁相关 IP 地址或增强涉及的服务器的安全措施，从而防止该攻击产生不利后果。

（二）预测网络攻击

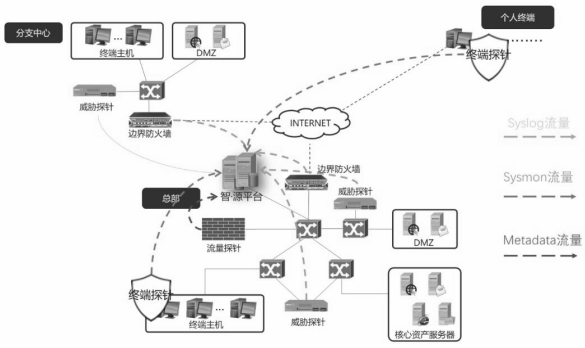
预测网络攻击是指通过态势感知平台利用机器学习、行为分析和威胁情报等技术，对已知的攻击类型和模式进行学习和分析，从而预测出新型攻击的可能性。通过预测网络攻击，企业可以提前采取相应的防护措施，有效降低风险。在某汽车集团有限公司的网络中，态势感知平台分析发现最近出现了一种新型的勒索软件攻击，它利用社交工程手段对员工进行钓鱼诈骗并传播恶意软件。基于该分析，平台会生成预测报告，并提供针对这种攻击的建议和注意事项。某汽车集团有限公司的安全团队收到预测报告后，可以加强员工教育和意识提醒，设置反钓鱼措施以及加强对社交工程攻击的监测与防护[2]。

三、应对网络攻击

态势感知平台在网络安全中的作用是帮助企业及时发现和应对各种网络攻击，确保网络系统和数据的安全。下面将详细阐述在某汽车集团有限公司中，态势感知平台如何应对网络攻击。

（一）实时监测与分析

态势感知平台通过实时监测和分析网络流量、日志信息以及其他安全事件数据，及时掌握网络环境中的异常行为和潜在威胁。这些数据可以包括用户登录行为、系统漏洞扫描、异常访问尝试等。通过对这些数据的分析，平台可以识别出可疑活动和潜在的攻击迹象。在某汽车集团有限公司的网络中，态势感知平台实时监测到一台服务器接收到大量来自外部 IP 地址的非法访问请求。平台会立即对此进行警报，并生成相应的事件报告。安全团队通过查看报告，可以了解到该服务器正在遭受 DDoS 攻击，攻击者试图通过资源耗尽使其停止服务。基于这一信息，安全团队能够迅速采取措施，如封锁攻击源 IP 地址、增强服务器防护等，以保护服务器的稳定运行。（如图一）



图一：山石网科态势感知智能安全运营系统

（二）威胁情报分析

态势感知平台还能够通过与外部威胁情报源的对接，获取最新的威胁情报数据。平台会将这些数据与内部网络数据进行关联分析，以识别出可能的攻击模式和攻击者的行为特征。这有助于企业提前预警和应对新型的网络攻击。在某汽车集团有限公司的网络中，态势感知平台从外部威胁情报源获取到一条信息，称最近出现了一种新型的勒索软件攻击，该攻击利用电子邮件的附件进行传播。平台会将这一情报与内部邮件系统的数据进行分析，检测是否有用户收到类似附件并进行下载。如果有发现相应的活动，平台会立即发出警报并通知安全团队。安全团队随后会及时采取应对措施，如对用户进行警示、加强入侵检测系统设置等，从而有效遏制该新型勒索软件的传播。

四、全面管理和优化网络安全

态势感知平台还可以对企业网络中的安全设备和防护措施进行全面管理和优化。通过对网络安全设备的集中监控和管理，平台能够及时发现设备故障或异常情况，并提供相应的处理建议。下面将详细阐述“全面管理和优化网络安全”的具体内容：

（一）风险分析与应急响应

态势感知平台通过对历史数据和实时数据的深入分析，能够识别出网络安全的潜在风险，并进行风险评估。平台根据风险评估结果，为某汽车集团提供合理的安全措施建议，协助企业制定网络安全策略和应急响应计划。当平台分析发现某个服务器存在漏洞且可能被攻击时，平台会向安全团队发出警报，并给出具体的修复建议和应急响应方案，帮助企业快速做出反应，最小化损失[3]。

（二）数据可视化与报告生成

态势感知平台可以将海量的网络安全数据进行可视化展示，并生成详尽的报告。通过图表、仪表盘和日志分析等方式，平台可以直观地展示网络安全的状态和趋势，帮助企业了解整体安全态势。平台可以生成每日、每周或每月的网络安全报告，

包括攻击事件统计、防御效果评估、安全事件响应时间等数据，为某汽车集团的决策者提供参考依据。

（三）漏洞管理和修复

态势感知平台能够扫描和识别网络系统中的漏洞，并提供修复建议。平台通过自动化工具对系统进行主动扫描，发现潜在的漏洞后，向安全团队生成报告，指导其进行修复措施。在某汽车集团有限公司的网络中，态势感知平台发现一台服务器上的操作系统存在一个已知的漏洞。平台会向安全团队发送报告，指导其升级或修补该系统，以修复漏洞并增强系统的安全性。

五、结语

态势感知平台在某汽车集团有限公司的网络安全防护中发挥了重要的作用。通过实时监测、预警和应对网络威胁，该平台有效提高了企业的网络安全防护能力。未来，企业应进一步完善和优化态势感知平台，结合人工智能和大数据技术，提升网络安全的智能化水平，并不断适应新兴的网络攻击手段和威胁。

[参考文献]

[1]费新秋.态势感知平台在网络安全中的应用[J].数码设计, 2023,42(16):112-113.

[2]章明,钱升宏,鞠海斌.基于大数据的网络安全态势感知平台的建设与应用[J].广播电视网络,2023,30(09):89-91.

[3]巩耀晓,杨继家,冯建军.态势感知平台在广播电视台网络安全中的应用[J].现代电视技术,2022,6(04):127-129.