安全大模型技术与市场研究报告

前言

网络安全领域中，传统的安全防护方法存在效率低、攻防不对等和误报率高等问题。生成式人工智能大模型（AIGC）技术作为一种“新锤子”，在自然语言处理、自动化响应和威胁识别方面展示了巨大的潜力。大模型的出现让网络安全从业者看到了突破现有安全技术瓶颈的希望。

一、网络安全领域中的大模型应用概述

大模型带来的网络安全新可能性

1. **自然语言处理能力的提升**：大模型让机器对人类语言的理解更为准确，可以在情感分析、事件检测和威胁情报提取中提供支持。
2. **多任务处理性能的提升**：大模型具备处理多种网络安全任务的能力，从威胁检测到用户行为分析，再到情报分析，大模型展现了出色的灵活性。
3. **推理和逻辑能力**：大模型在复杂威胁模式分析中具备一定的推理能力，有助于识别潜在的攻击链和预测威胁走向。

大模型驱动的网络攻击

随着AI技术的发展，攻击者开始利用大模型增强攻击效果。具体表现如下：

1. **自动化攻击生成**：大模型能自动生成攻击代码，使得零日攻击和APT攻击更具隐蔽性。
2. **钓鱼邮件和社交工程攻击**：大模型在钓鱼邮件的生成和社交工程攻击中可以精确模拟真实场景，提高了攻击成功率。
3. **逃避检测**：通过大模型生成的恶意样本可以绕过传统安全检测系统。

大模型驱动的风险识别

大模型在数据分析、异常检测和动态学习方面的能力使其成为网络安全中重要的风险识别工具。其特点包括：

1. **数据分析与理解**：通过分析大量数据和提取威胁情报，大模型帮助安全团队快速识别风险。
2. **异常检测**：利用深度学习技术，大模型能识别出行为异常，适用于金融、电子商务和网络安全等领域的欺诈检测。
3. **动态学习与适应**：大模型能够适应新的威胁环境，自动调整和优化威胁检测策略。

二、网络安全领域的大模型应用场景

威胁检测

1. **恶意代码检测**：通过深度学习和大模型技术，能够识别出未知恶意软件。大模型可以快速适应恶意软件变种，有效应对零日攻击。
2. **攻击流量检测**：大模型可以实时分析网络流量数据，识别异常通信并检测DDoS攻击、恶意扫描等行为。

3. **用户与实体行为分析（UEBA）**：大模型基于用户的历史行为模式，检测偏离正常行为的活动，从而预防内部威胁。

数据安全

1. **数据分类和分级**：大模型通过自然语言处理技术理解数据上下文，对数据进行准确分类与分级，确保敏感数据得到有效保护。
2. **数据脱敏**：大模型可以根据数据敏感性智能选择脱敏策略，动态调整数据脱敏的方式，有效降低数据泄露风险。
3. **风险评估与策略制定**：大模型能够自动评估数据风险，根据数据类型和使用场景生成安全策略，确保数据的全生命周期安全。

网络安全运营

1. **告警降噪**：大模型通过分析历史告警数据，过滤掉误报或低优先级事件，仅将高风险事件交给安全人员处理，提高响应效率。
2. **攻击研判与自动响应**：大模型具备对复杂攻击进行分析与自动响应的能力，能够触发自动化剧本并实时调整安全策略。
3. **报告自动生成**：大模型的文本生成能力使其能够高效生成安全事件报告，为管理决策提供实时支持。

鉴伪与认知安全

生成式AI技术的应用也带来了认知安全问题，主要表现在虚假信息、社交操控和心理操纵方面。大模型可用于识别和阻止假新闻、深度伪造内容，保护用户免受虚假信息的影响。

三、市场分析与产业发展

国外代表性供应商

国外的安全大模型供应商（如Anomali、Check Point、Cisco等）通过大模型技术在威胁情报、XDR（扩展检测和响应）和加密流量分析等领域取得显著进展。这些公司依托大模型优化了威胁检测和安全运营效率，为全球网络安全市场提供支持。

国内代表性厂商

国内的安全厂商（如360、安恒、奇安信等）纷纷在安全大模型应用上投入资源，形成了完善的安全大模型产品生态。在威胁检测、数据安全和网络安全运营等领域取得显著成效，为本地客户提供定制化解决方案。

四、企业安全大模型能力评估与选择

评估纬度

在选择安全大模型时，需综合考虑以下能力：

1. **安全能力**：企业在威胁检测、风险评估等方面的表现。
2. **深度学习与大模型能力**：企业的深度学习技术积累与模型精度。
3. **算力与基础设施**：支持大模型运行所需的算力资源。

4. **产品化与场景适用性**：大模型在用户场景中的适配程度。

国内主要网络安全公司能力评估

国内安全公司在大模型产品性能、场景覆盖、用户适用性上各具优势，如360和安恒在数据安全和威胁检测方面表现较好，适合不同企业的安全需求。

五、解决方案与应用案例

360安全大模型

360的安全大模型系统广泛应用于安全运营和威胁情报分析，具备高效的数据处理能力和灵活的部署模式，支持多种场景的实时威胁检测和事件响应。

安恒恒脑安全大模型

安恒恒脑安全大模型通过场景化应用和技术优化，在数据分类、告警管理和自动化响应方面提供了显著的性能提升，为客户提供多样化的安全运营支持。

金睛云华安全运营智能体

金睛云华的安全智能体在数据脱敏和用户行为分析方面表现突出，支持自定义配置和高效的自动化威胁管理，提升企业的数据安全管理效率。

深信服安全GPT

深信服的安全大模型系统在恶意软件检测、入侵检测和自动化响应中应用广泛，能够有效协助企业提升安全响应能力。

天融信天问安全大模型方案

天融信的安全大模型在认知安全和动态威胁响应方面有明显优势，广泛适用于多种行业的安全需求，增强了客户的综合防御能力。