

蓝盾信息安全技术股份有限公司投资者关系活动记录表

| | |
|----------------------------------|---|
| <p>投资者关系 活动类别</p> | <p><input checked="" type="checkbox"/>特定对象调研 <input type="checkbox"/>分析师会议 <input type="checkbox"/>媒体采访 <input type="checkbox"/>业绩说明会 <input type="checkbox"/>新闻发布会 <input type="checkbox"/>路演活动 <input type="checkbox"/>现场参观 <input type="checkbox"/>其他</p> |
| <p>参与单位名称及 人员姓名</p> | <p>中金方寸基金 李一伦 前海开源基金 郑建鑫 盈峰资本 赵开勋 永安国富资管 姚乐平 中信建投 石泽蕤 中信证券 余经纬 申万宏源 宁柯瑜 万联证券 曾超巩 国泰君安 肖沛</p> |
| <p>时间</p> | <p>2018年11月09日15:30-17:30</p> |
| <p>地点</p> | <p>蓝盾信息安全产业基地5楼会议室</p> |
| <p>上市公司接待人 员姓名</p> | <p>总裁 柯宗贵 首席技术官 杨育斌 董事会秘书 李德桂 投资者关系主管 黄美华</p> |
| <p>投资者关系活动 主要内容介绍</p> | <p>投资者关心的问题及回答如下： 1、公司态势感知产品针对的主要客户有哪些？与行业同类产品相比突出优势是什么？ 答：公司态势感知平台采用行业化营销方式推广，目前客户已覆盖政府、运营商、广电、公安、电力、教育、医疗、保密等多个行业。这款产品此前已在中国移动南方基地</p> |

获得成功部署，这是中国地区运营商第一次大范围态势感知试点实践应用。我们推出的态势感知方案属于深度态势感知，利用业内独有的软件基因技术（这是一个军转民的技术），同时结合机器学习、关联分析、UEBA 行为建模、失陷主机等技术，能把握安全威胁种群共性基因，实现从微观结构对安全威胁更为精准的深层认知，可提供僵木蠕毒来源通信检测及结构溯源、恶意代码种群分析与扫描检测、APT 种群家族关系分析、脆弱性靶向分析、挖掘未知漏洞等深度数据分析功能。同时，还可以用来进行未知威胁和未公开漏洞的挖掘，从海量数据中发现有用的、可理解的数据模式，自动构建检测模型，并与机器学习、模式识别、归纳推理、数据可视化和高性能计算等相关领域有机结合，达到快速挖掘与分析的最佳效果。

2、业务应用安全的技术壁垒高吗？主要客户有哪些？

答：业务应用安全的技术壁垒挺高的，因为业务系统的信息泄露 70% 是合法人员非法操作而导致的，它存在泄密渠道管控难、操作行为限制难、操作性质识别难等问题。但蓝盾成功解决了这一问题，“蓝盾业务应用安审平台”从核心应用系统/资源库的应用日志入手，通过对用户操作行为（增、删、改、查询、登录）和接口服务情况（批量对比、查询等）进行完整记录，并对日志数据进行分析，实现对业务操作行为的实时监管、违规操作预警、违法事件的倒查追溯，是破解当前信息安全事件“跟踪不下去、查不到源头、取不到证据”的难题，为用户提供了防范敏感信息泄露、保护数据安全的有效途径。因此面向业务的应用安全管控是当今信息安全的核心和制高点，未来将成为信息安全建设的刚需。目前该平台已在公检法司、教育、医疗、城市管理等领域得到广泛应用。

3、公司云安全部署情况是怎样的？突出优势是什么？

答：公司 2017 年以来陆续推出蓝盾云平台、云桌面和一系列虚拟安全器件，并与国内领先的云服务商云宏信息达成战略合作，参股云海麒麟、精灵云等，建设蓝盾大安全研发

与产业化基地，投入一站式安全云计算体系研发项目等，深化云计算安全业务。与国家信息中心、数字福建、山东电信等重要政务云及运营商云运营中心深入合作，为政府企业及互联网公司提供全面的云计算安全服务。同时，公司还陆续在各地落地政务云安全、智慧城市云安全、工业控制网络云安全、医疗云安全、教育云安全、金融云安全、互联网游戏云安全等行业云安全解决方案，全面拓展行业云计算安全业务。

公司的云安全已获得国内首批 CSA CS-CMMI5 认证，在云安全部署上，采用节约化部署方式，通过容器技术可将所有的虚拟组件部署到一个 docker 上运行，与传统的虚拟机部署方式相比可大大降低用户的成本。同时，公司还拥有虚拟防火墙、虚拟数据库审计、虚拟堡垒机等 8 款业内最齐全的云端防护的安全产品，完全符合等保 2.0 要求。此外，公司还建立了自己的云安全平台，统一实现计算虚拟化、存储虚拟化、网络虚拟化、网络功能虚拟化和安全虚拟化。同时还结合大数据、SDN、NFV 等前沿技术手段，可及早预测危险事件，有效预防安全隐患的爆发。

4、公司目前有哪些产品引入了 AI 技术？

答：公司目前已积极运用人工智能、机器学习等技术对传统安全产品进行了全面升级，形成涵盖 IaaS、PaaS、SaaS 三个层面整体解决方案服务能力。同时，公司多个云产品如云防线、云管理平台、云态势感知、云防火墙等产品都引入 AI 引擎，进行病毒样本学习，攻击特征学习，以提供智能的基础设施平台，更智能的进行攻击防护。不仅如此，公司还通过云端能力为无法安装安全系统的各种物联网设备提供“AI 安全大脑”。其中，最具代表性的产品包括：①蓝盾人工智能防火墙。它与传统防火墙最大的区别在于它不依赖特征对威胁进行匹配和判断，而是通过机器学习模型判定安全威胁。它能检测木马变种和未知威胁攻击、0 day 攻击等，误报率极低，且能做到主动防御。②蓝盾态势感知平台。公司推出的态势感知属于深度态势感知，它利用业内独有的软件基因技术，能把握安全威胁种群共性基因，实现从微观结构

| | |
|----------|---|
| | <p>对安全威胁更为精准的深层认知。同时，还可自动构建检测模型，与机器学习、模式识别、归纳推理、数据可视化和高性能计算等相关领域有机结合，达到快速挖掘与分析的最佳效果。③蓝盾 AI 安全云。这款产品打造的是一个智能、专业的威胁分析平台，以云的方式提供基于人工智能的可疑文件、高危应用检测分析服务，适用客户群体可扩展到需要威胁深度分析能力的企业或个人，为传统网络、IoT 网络的终端设备通过基于云的安全大脑。</p> |
| 附件清单（如有） | |
| 日期 | 2018 年 11 月 09 日 |