AISA 产品白皮书

版本信息

文档名称	文档版本	密级	创建日期
AISA 产品白皮书	V1.2	公开	2019/08/13

目录

1. 概述

随着互联网、云基础设施和大数据技术的发展，移动互联网的普及，企业事业单位的信息数字化进程快速上升，同时系统网络也面临更加严峻、更加多样化的安全问题。

在安全形势不断恶化的情况下，即使布上各式的防护设备，原有的安全检测手段也已经无法抵御日益更新的所有攻击手法。尤其是原有单纯依赖专家规则的全流量入侵感知系统，难以应对层出不穷的变种攻击手法。

企业迫切需要能够集中监测、分析全网的流量信息，识别已经发生或者正在发生的 APT 攻击，定位入侵行为、追溯攻击源、实时响应、阻断入侵、降低损失。

奇虎 360 基于对大型互联网企业内部的网络入侵检测的安全实践，丰富的安全事件处置运营经验，再结合对最新攻防手法与“入侵攻击链”的深刻理解和研究，以及配合强大的安全大数据处理技术，正式发布首款基于机器学习的入侵检测系统 AISA。

本产品采用了全新的攻击模型，综合运用攻击模型智能识别、专家规则判定和行为分析技术，为企业用户提供一份高检出、易运营、可追溯的网络入侵检测解决方案，是目前入侵防护市场内里程碑式的产品。

2. 当前面临的威胁及不足

2.1. 面临的威胁

针对日益更新的攻击手法和威胁，传统安全防护设备缺乏积极主动的防护能力。企业安全管理者可能遇到以下情况：

- 企业是否被入侵？
- 企业哪里存在安全漏洞？
- 安全漏洞造成了什么危害？
- 黑客到底是怎么进来的？
- 面对黑客入侵怎么应对？

当内部系统或业务系统发生异常时，却不能在第一时间定性问题、了解系统是否被入侵。当知道系统被入侵了，或有敏感信息泄露，造成巨大损失，却不知道哪里存在安全漏洞，不清楚系统何时被入侵。面对业务系统多而复杂的情况，内外网多处都可能受到威胁，真正发生安全事件时，难以溯源分析黑客攻击行为并还原攻击链。

另一方面，已部署全流量入侵感知系统的企业事业单位，在面对 0day 漏洞和各种 payload 的各种变形，仅依靠专家规则定期更新的安全设备无法及时应对和检测。更严重的是，大多数企业缺乏有经验的专业安全运营人员，而告警量大、误报率高的传统全流量入侵感知系统难以运营，这使企业安全防护难上难。

3. AISA 全流量入侵感知系统介绍

3.1. 简介

面对 Web 攻击，渗透入侵，服务器控制，横向渗透，奇虎 360 提供了全新前沿的完善的网络检测解决方案。AISA 全流量入侵感知系统(以下简称“AISA” ,Artificial Intelligence Security Analysis)，是拥有自主专利的基于机器学习技术的新一代安全产品，其主要目标旨在适应攻防的变种和更新发展，准确监控网络传输或者系统的入侵动作，并预测黑客的下一步攻击行为。弥补了目前常见全流量入侵感知系统的不足，动态的、主动的检查是否有可疑活动或者违反企业的政策。当侦测到时，发出警报或者采取主动反应措施。实现事前告警、事中预测、事后取证，为企业事业单位用户提供高检出、易运营、可追溯的网络入侵检测解决方案，是目前入侵防护市场内里程碑式的产品。

3.2. 主要功能

AISA 应用了机器学习和大数据技术来进行攻击行为识别 ,辅以专家规则来界定攻击成功，构造真实的事件告警。下面将细述本产品应用的全新产品理念。

3.2.1. Web 攻击检测

AISA 对 Web 漏洞利用、常规渗透入侵、内网横向渗透等各类黑客攻击和恶意流量进行实时检测及报警。

3.2.2. 系统受控检测

AISA 能够通过流量中的异常行为，检测出系统中受控的服务器，定位出当前企业受影响的业务模块。

3.2.3. 还原攻击链

AISA 面对善于用不同身份和地址进行攻击的黑客，将多条攻击告警分析汇总，做攻击事件还原，这对事后的审计、溯源、取证有极大的帮助，同时也将减轻安全运营的工作量。

3.2.4. 预测下一步入侵行为

AISA 基于对攻击链深入的理解，通过观察成功入侵动作在攻击链的位置信息，AISA 能预测该入侵事件的下一步动作，感知当前区域的成功攻击情况，真实刻画该区域的安全态势。提供决策参考，以便及时做出调整和防御动作，早一步扼杀黑客的攻击，避免造成严重的财产损失和进一步的敏感信息泄露。

3.2.5. 可视化展示攻击过程和相关数据

对流量数据监测分析，是通过数据间的关联关系，识别并还原整个攻击过程，通过攻击链理论能够识别当前攻击所处的环节，追踪定位攻击发起的时间、攻击利用的位置、攻击源相关的信息，通过攻击链能够完整的还原整个攻击过程，系统可视化展示事件的信息侦查、攻击入侵、命令控制、横向渗透、数据外泄、痕迹清理整个攻击过程，并统计主流的攻击方式、攻击源、被攻击资产，实时展示告警趋势图，用户可一目了然知道自己网络资产安全现状。

3.3. 产品特性

3.3.1. 实锤告警体系

AISA 拥有对攻击进行实锤告警的能力，并且 AISA 的检测思路与黑客攻击思路一致。黑客攻击时，判断被攻击的信息系统是否存在漏洞，绝大多数情况下都是对响应做判断。AISA 在检测方面，会对每一个访问响应做判断，因此能够实时发出攻击成功告警。

3.3.2. 高性能的海量数据处理能力

AISA 拥有高性能的处理能力，具备单机最高处理 30G 网络流量的能力，此外集群部署可以满足大型互联网企业 100+IDC（Internet Data Center，互联网数据中心）规模的实时入侵感知需求。

3.3.3. 无规则攻击检测

AISA 使用无规则攻击检测，即使用模型引擎检测流量中的攻击行为，增加了检出结果的

精确性和识别未知攻击的能力，避免了由于单纯使用专家规则正则式生硬匹配而导致的误报告警。相比传统的全流量入侵检测系统，大大降低了误报率，减轻日常运营工作量。

3.3.4. 机器学习标签数据收集

AISA 深知未来安全检测会是基于深度学习的，深度学习不仅能带来卓越的检测已知问题能力，还能带来非凡的检测未知问题能力。AISA 系统能为客户提供基于自身流量的精准攻击标签数据，为企业在未来深度学习的战场上提供坚实的数据基础。

3.3.5. 发现未知漏洞能力

为了绕过企业部署的安全设备的检测，黑客不断更新变形的攻击手法，AISA 可以识别出已知的各种 payload 变形和部分 0day 漏洞，例如可预见的 Struts2 系列漏洞，SQL 注入类漏洞，Java 反序列化漏洞，CMS 类型漏洞。这类“已知的未知”漏洞，是对公开的漏洞做出调整，多变且难以用规则正则式完全识别。由于 AISA 使用模型引擎检测攻击行为，可以对行为本身做识别，而不用规则正则式匹配。这使 AISA 拥有可以发现未知却可预见的 0day 漏洞的能力。

3.3.6. 攻击链模型刻画

攻击者入侵动作还原描绘能力。AISA 通过检测流量中存在的威胁行为，按照攻击链理论将入侵动作映射到攻击链模型上，分为信息侦查、攻击入侵、命令控制、横向渗透、数据外泄、痕迹清理六步。

4.5.5 攻击链模型

3.3.7. 后续攻击预测

通过观察入侵动作在攻击链模型的位置信息，AISA 能在攻击事件正在进行时，预测该

入侵事件的下一步动作。基于奇虎 360 多年的攻防数据分析和研究，能较准确地预知攻击者的攻击思路，从被动修复攻击者利用的系统漏洞，到提早攻击者一步，去主动防护企业信息财产，AISA 使得企业安全管理者从更高的层面去防护企业安全。

3.3.8. 攻击入侵事件输出

基于攻击成功告警的能力，AISA 的安全事件的数据具备出色的下钻能力，可做到威胁狩猎、攻击者画像、APT 感知、入侵事件还原、渗透测试监控，达到实时反馈安全问题的目标。从告警运营转换为事件运营，化繁为简，大大减轻日常运营工作量。

3.3.9. 检测能力覆盖广

AISA 不仅支持 HTTP 协议的成功攻击检测，还支持其他 TCP 层协议的成功攻击检测，如 RMI，T3，REDIS 等。此外还支持弱口令检测、敏感信息泄漏检测等。

3.3.10. 多源的模型训练数据

拥有奇虎 360 的安全资源作为模型训练数据，AISA 使用以下来源数据作为模型的训练数据，提高模型识别准确率：

- 脱敏的渗透测试数据
- 红蓝对抗复盘数据
- 安全研究数据
- 自动化 fuzz 生成数据
- 入侵事件复盘数据
- 网络攻防开源数据

3.4. 产品亮点

3.4.1. 安全威胁—点线面理论

点线面理论是指：

点：单条实锤告警为单点。

线：根据对实锤告警点的分析，把多个实锤告警点串联安全事件。

面：基于多个安全事件的分析，把多个安全事件刻画防区安全态势。

4.2.1 点线面理论

过往安全运营以单条 IDS 告警为单位，这样的做法有比较片面的明显缺点，无法悉知或很难还原一连串攻击事件的真实情况，在溯源和取证的过程会耗费较大的人力，且告警量大而重复告警同一攻击事件，平日运营工作变得艰难。

而 AISA 产品区别于过去单点运营思路，以汇集多个实锤告警为基础生产安全事件，进一步将事件按照攻击链理论将入侵动作映射到攻击链模型上，分为信息侦查、攻击入侵、命令控制、横向渗透、数据外泄、痕迹清理六步。通过观察成功入侵动作在攻击链的位置信息，AISA 能预测该入侵事件的下一步动作，感知当前区域的成功攻击情况，真实刻画该区域的安全态势。

3.4.2. 达成“已知的未知”层面

基于专家规则的全流量入侵感知系统，只能发现符合已知攻击手法的漏洞，但不能检测不符合专家规则的同类漏洞，我们称之为“已知的已知”层面。而基于机器学习，AISA 使用无规则的模型识别引擎，利用机器学习模型引擎的泛化能力，达到“已知的未知”层面，不仅能识别已知攻击手法的漏洞，也能进一步识别出各类 0day 漏洞和各种 payload 的变形，例如可预见的 Struts2 系列漏洞，Sql 注入类漏洞，反序列化漏洞，CMS 类型漏洞。

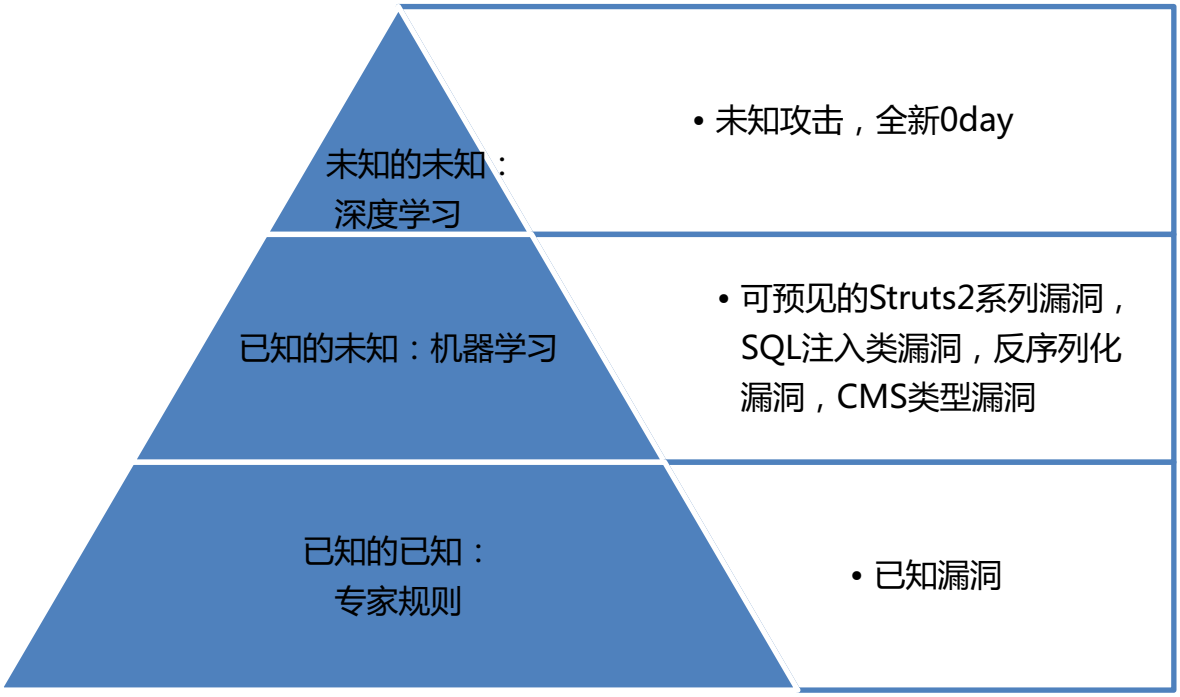


图 4.2.2. 不同识别方式的威胁检测能力分层

3.4.3. 攻击成功识别模式

目前的常用识别模式是使用已知专家经验形成的规则来识别攻击行为和判定攻击是否进行。依靠 360 本身的大量安全数据及强大的安全数据处理能力，AISA 采用进阶方式——机器学习模型识别攻击行为，使用专家规则做最后的攻击成功实锤判定。

4. 应用场景

4.1. 企业入侵感知解决方案

在当前环境下，现有的传统安全设备无法有效的、及时的发现入侵攻击，企业甚至不知道已经被黑客入侵了。告警信息泛滥、海量数据堆积，发生安全事件后，缺乏有效的技术手段，难以溯源，难以定位问题、解决问题。被攻击的资产有哪些、资产被攻击后会有哪些影响等一系列的问题缺乏有效的手段进行管控。

AISA 通过采用了全新的攻击模型，综合运用攻击模型智能识别、专家规则判定和行为分析技术，为企业用户提供一份高检出、易运营、可追溯的网络入侵检测解决方案。

4.2. 区域监控安全解决方案

对于大型企业和政企单位，尤其是需要监管多个下属单位的系统网络安全和入侵威胁情况的企业用户，AISA 可提供实时的入侵威胁检测的态势感知，方便管理用户迅速了解当前下属系统的安全情况，是否发生入侵威胁事件，哪些单位部门发生入侵事件，近期承受较多入侵威胁的单位部门，脆弱点，常见爆发的漏洞类型。面对不断的攻击行为，AISA 可以实时反馈安全问题，并拥有高精准性。

4.3. 攻防演习、红蓝对抗解决方案

随着网络信息安全的越来越引起重视，企业用户通过攻防演习来发现和检验内部安全的系统防护能力、安全工程师的应对能力。应对此类特殊的攻防场景，AISA 能够满足实时性，识别准确性，日志溯源分析能力的要求。可提供对演习中的实时入侵事件威胁检测，日志分析攻击行为一系列操作，还原攻击事件，记录 webshell 等便于事后分析复盘的源数据和数据分析功能。

可以通过单机部署或云部署的方式，来满足数据采集、行为分析、大屏实时展示攻防情况、日志数据存储中心、运营后台中心的功能需求。

5. 技术架构

5.1. 关键技术

5.1.1. 成功入侵识别模块

目前的常用识别模式是使用已知专家经验形成的规则来识别攻击行为和判定攻击是否进行。依靠 360 本身的大量安全数据及强大的安全数据处理能力，AISA 采用进阶方式——机器学习模型识别攻击行为，使用专家规则做最后的攻击成功实锤判定。

5.1.2. Webshell 页面识别模块

利用 360 大数据，积累入侵页面特征，利用机器学习进行 webshell 页面识别

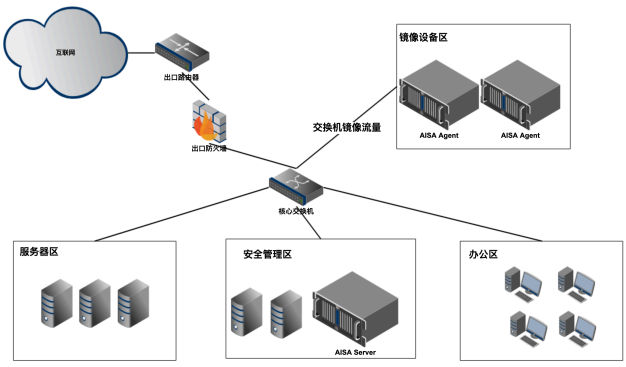
5.1.3. 弱口令模块

利用 360 大数据 ,积累登陆页面特征 ,利用机器学习进行登陆页面识别 ,再配合 top1000 弱口令数据集进行弱口令登陆识别。

5.2. 部署架构

单节点模式： AISA Agent * 1，AISA Server * 1

多节点模式： AISA Agent * N，AISA Server * 1



企业AISA系统部署方案

6. 总结

随着攻防不断升级，黑客的技巧也随之产生变化，破坏能力不断提高，网络受到难以用已知规则来识别的攻击，传统防火墙、传统全流量入侵感知系统和防病毒系统都无法有效地检测和阻止。

AISA 全流量入侵感知系统引入基于机器学习和大数据技术的新型入侵检测技术，实时监控网络资源，为政府、金融、能源、运营商、大型企业等客户提供未知威胁的发现、分析与溯源功能，提供一份高检出、易运营、可追溯的网络入侵检测解决方案。