聚铭工控网络流量审计系统

产品白皮书

聚铭网络科技有限公司

2024 年 04 月

目录

声明 1
联系信息 2
前言 3
1. 客户需求 4
2. 解决方案 5
2.1. 产品价值 5
2.2. 产品架构 6
2.3. 主要功能 6
2.3.1. 全流量采集深度包解析 6
2.3.2. 全流量数据包留存 7
2.3.3. 工控网络行为审计 7
2.3.4. 网络质量检测 7
2.3.5. 网络攻击检测 7
2.3.6. 异常流量挖掘 8
2.3.7. 威胁情报检测 9
2.3.8. 文件安全检测 9
2.3.9. 失陷分析 9
2.3.10. 网络威胁态势感知 9
2.4. 部署方案 10

2.4.1. 经典部署方案.....10

声明

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司和北京聚铭信安科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

北京总部：北京市海淀区丹棱街 18 号创富大厦 9 层

南京总部：南京市雨花台区软件大道 180 号南京大数据产业基地 7 栋 4 层

电　　话：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

聚铭网络技术服务以及营销网络覆盖全国，并在各地设有办事处和分支机构，为客户提供无微不至的解决方案和高效的服务支持。聚铭专家团队 7x24 小时全天候在线，确保在安全事件发生时提供分钟级应急响应。

前言

近年来，工业控制系统被广泛应用于电力、交通、能源、水利、冶金、航空航天等国家重要基础设施。随着工业互联网与自动控制技术的融合，5G 通信技术的普及，IT 和 OT 深度融合呼之欲出。这给工业控制领域带来了新机遇，同时也带来了新的网络安全威胁。恶意软件及恶意工具层出不穷，定向勒索攻击、工业网络间谍事件也逐年增长，工控安全事件给人们带来巨大的损失。

目前国内工控安全建设相对落后，工控环境的风险主要来源于三个方面：外部攻击、病毒传播、人为过失。

外部攻击

保密性是传统信息安全领域最重要的部分，在工业控制系统领域则有较大的不同。工业控制系统强调的是工业自动化程度及对相关设备的智能控制、监测与管理能力。因此工业控制系统对完整性和可用性要求更高，导致工业控制系统，安全性不足，安全漏洞不断涌现。另外，随着黑客大会、白帽社区、开源社区的出现，大量工控系统软硬件设备的漏洞及利用方式都可以在网络上以各种渠道获得，工控网络的攻击难度正在降低，外部攻击风险逐年攀升。

病毒传播

近年，国内恶意软件感染有所上升。定向勒索软件、工业间谍软件、工业蠕虫等恶意软件层出不穷。主要原因在于，OT 系统在安全设计上的不足，当接入互联网后，相比 IT 系统，更容易受到攻击，造成的损害更大，更难于防护。这也促使了工业系统成了勒索软件攻击所青睐的目标。

人为过失

企业内部人员的误操作、违规操作、非法设备接入、故意的破坏性操作等，成为工业控制系统面临安全风险。

1.客户需求

针对上述问题和挑战，工业企业的信息安全管理人员不仅对各类安全合规操作的审计有着较高要求，还对工业网络环境安全问题的发现、潜在问题的萃取、未发生问题的预防等都有较高期望，特别是对于一些隐蔽性强的未知威胁的追根溯源（包括各类高级持续威胁等）也有现实需求，包括：

1. 工控网络遭受外部的攻击，如漏洞利用、扫描、DDOS、密码猜测、缓冲区溢等；
2. 工控网络遭受有害程序感染，如僵尸、木马、蠕虫、钓鱼软件等；
3. 工控网络内部人员的不合规操作，如非法接入、违规操作等；
4. 工控网络中的异常流量，如异常指令、通讯中断、隐蔽信道、加密流量、异常协议、异常端口等；
5. 工控网络中 IT 管理系统和工业控制系统相连，容易造成威胁扩散，缺乏全面的审计监测。

以上仅列举了部分内容，但在现实中安全问题远远不止上述部分，例如还有针对各种 0day 漏洞的攻击等等，所以客户对网络流量分析审计的要求应包含了对于未知威胁的检测和防御，而不仅仅是对于已知威胁的发现。

2.解决方案

聚铭工控网络流量审计系统（ICTA）是南京聚铭网络科技有限公司研发的具有自主知识产权的工业控制系统网络审计产品，它是一款以全流量还原为基础，结合工控网络行为审计、网络质量检测、网络攻击检测、威胁情报分析、基于学习的异常流量挖掘、文件安全检测、失陷分析等技术，对工控网络中 IT 及 OT 流量全面、实时威胁感知及行为分析，是对工控安全防御系统的完善和补充，为客户在高级威胁入侵时，及时察觉，及时止损。

同时，也是满足国家等保、网络安全法及行业安全规范的最佳解决方案。

2.1.产品价值

1. 全流量回溯，系统全流量采集、分析、存储、检索，不仅能够支持事中发现，还能够在用户已经遭受攻击的情况下，对历史流量进行回溯分析。
2. 异常工控行为审计，可以针对工控会话、工控关键操作、工控协议指令进行审计，发现工控设备的异常操作。
3. 全面覆盖 IT 及 OT 网络威胁行为检测，能够识别网站攻击、数据库攻击、明文传输、恶意木马、勒索软件、隐蔽通道、DGA、拒绝服务攻击、弱口令等网络威胁。
4. 异常网络行为检测，基于智能动态基线、模式信息熵等算法，通过一段时间对学习对象的流量特征分析、建模，能够识别设备的异常流量、端口，例如发现未授权设备接入、网络中断、非法开放端口等。
5. 发现恶意文件及数据泄漏，能够识别加密文件、包含敏感词的文件、恶意文件。
6. 通过失陷分析，帮助用户把安全问题聚焦于设备，减少运维工作量。
7. 流量数据可视化，将流量中的常用应用还原，并呈现应用的关键数据。
8. 可满足如等级保护 2.0、《中华人民共和国网络安全法》、中华人民共和国

工业和信息化部第 11 号令、《中华人民共和国密码法》等法律、法规对于网络数据审计的要求。

2.2. 产品架构

聚铭工控网络流量审计系统创新的融合了 IT、OT 领域的网络流量安全分析，其功能架构如下：

◆ 基础分析层

系统采用零拷贝技术，实现高速流量接入。实时进行会话重建、协议识别、异常协议检测等功能。

◆ 安全分析层及高级分析层

结合失陷分析、网络威胁态势分析、威胁情报分析、异常流量行为挖掘、文件检测、网络质量检测、隐蔽通道检测、工控关键操作审计、网络风暴检测等技术，对全网流量实时进行威胁感知、可疑流量分析。

2.3. 主要功能

2.3.1. 全流量采集深度包解析

采用零拷贝、全程无锁化技术处理网络流量数据包，而且充分利用 CPU 向量化指令对各类模式进行识别或匹配，故即使在超大流量情况下，也能保证系统

整体处理无延时；独有的智能协议识别技术，可高速、准确地识别上千种应用，检测各种协议伪装行为；支持 HTTP、TLS、SMTP、POP3、IMAP、FTP、SMB、RDP、SSH、Telnet 等应用协议，支持 IEC104、MODBUS、OPCDA、OPCUA、EtherNet/IP CIP、SINEC-H1、ENIP、MMS/S7Comm、SUPCON 等工控协议的解析的精准解码、元数据提取及存储、搜索、统计功能，并对可疑网络流量进行了全包留存。

2.3.2. 全流量数据包留存

系统具备基于高速包留存技术（HPRT）及高速包检索技术（HPST）的全流量留存及回溯分析，支持针对网络协议的数据包全量留存或自定义部分留存。当发现安全事件时，可以用于上下文分析，还原“作案现场”，系统支持秒级数据包检索，并可在线分析或离线下载。

用户可根据数据包留存吞吐曲线查看实时落地的数据包流量大小，对于大流量或留存要求高的场景，提供专业磁盘阵列，支持一键挂载，稳定、安全。

2.3.3. 工控网络行为审计

基于工控协议深度解析结果，生成工控网络会话，包括 IEC104、MODBUS、OPCDA、OPCUA、EtherNet/IP CIP、SINEC-H1、ENIP、MMS/S7Comm、SUPCON 等工控协议会话，支持 MODBUS、OPCUA、CIP 等工控协议指令审计，如线圈、寄存器操作等，并支持对 MODBUS 关键操作审计，例如联机、上载、下载等

2.3.4. 网络质量检测

支持网络带宽占用异常检测、小包攻击、泛洪攻击、ARP 风暴、ICMP Flood、TCP 建连时延过长、TCP 重传过多、TCP 零窗口过多等常见的网络通讯质量问题检测，同时网络性能监控还能支持用户针对历史网络质量情况进行溯源分析。

2.3.5. 网络攻击检测

内置多种网络攻击检测策略，支持对一般网络攻击、明文传输、过期系统或

软件、木马检测、隐蔽通道、电子加密货币活动、勒索软件、数据库攻击等进行检测。

1. 常见协议攻击：DNS、FTP、ICMP、RPC、SNMP、Telnet、TFTP、VOIP、工控等协议及相关服务的恶意通讯、漏洞利用、扫描、DDOS、密码猜测、混合攻击检、提权、隐蔽通讯等攻击检测；
2. 工控应用 SCADA 攻击检测：远程代码执行、缓冲区溢出、漏洞利用；
3. 数据库攻击检测：用户扫描、提权、创建用户、缓冲区溢出等漏洞利用；
4. 邮件攻击检测：DDOS 邮件、垃圾邮件、钓鱼邮件、间谍木马附件邮件、缓冲区溢出等漏洞利用、黑邮箱检测；
5. 控件攻击检测：缓冲溢出、远程代码执行、任意文件下载、恶意控件等；（控件常包含在 IE、播放器、office、Adobe、邮件客户端等应用中）
6. WEB 服务器攻击：Webshell 执行、信息泄漏、缓冲区溢出、提权、后门木马、sql 注入、xss 攻击；
7. WEB 客户端攻击：浏览器 Edge、IE、Adobe 等客户端的钓鱼、信息泄漏、缓冲区溢出、恶意 Cookie、恶意代码执行；
8. WEB 应用攻击：Weblogic、wordpress、Jenkins、KLOG、Joomla、PHPAccounts 等上千种应用的注入、后门、代码执行、提权、路径遍历、xss 等。

2.3.6. 异常流量挖掘

基于 AI 算法识别隐蔽通道、DGA 域名、异常流量、工控未授设备等无法通过规则发现的安全隐患。

其中异常流量中集成了自主研发的智能动态基线、模式信息熵等生成算法，通过一段时间对学习对象的流量特征分析、建模，智能生成该对象多维度的网络特征，实施多维度的纵深检测机制，针对工控行业恶意流量、不合规网络通讯、异常指令操作、异常通讯中断等，具有较高的准确性。

2.3.7. 威胁情报检测

支持僵尸网络、C&C 节点、木马回连、垃圾邮件、钓鱼节点、扫描节点、恶意软件等威胁 IP、URL、文件 HASH 的实时检测。

支持情报详情追踪溯源，支持恶意 IP、恶意域名、恶意 URL、恶意文件溯源查询，呈现威胁情报详细信息，包含情报历程、恶意标签、相关事件、相关样本等，多维数据助力威胁分析。

2.3.8. 文件安全检测

实现从 HTTP、邮件、SMB、FTP、QQ 等协议中还原文件，并对文件进行黑名单检测、敏感词检测，不仅能够发现恶意软件，还能够检测客户的核心数据外泄。

除此之外还支持未知威胁文件的识别。基于启发式静态文件扫描技术的恶意文件识别；基于虚拟仿真环境动态文件扫描技术的文件威胁行为检测。

2.3.9. 失陷分析

在利用安全情报技术、大数据技术、AI 技术进行安全分析的基础上，结合 Kill-Chain 技术实时发现资产安全失陷情况，并支持分析溯源，详细展示各个失陷阶段的具体安全事件与原因；让运维人员摆脱海量安全事件、告警的困扰，聚焦问题所在，极大提升运维效率。

使用黄金眼功能对失陷主机进行举证分析，支持对失陷主机的外部威胁、外连威胁、内部主动威胁、内部被动威胁以及失陷主机开放端口服务进行全面分析，使客户更容易理解主机失陷的根本原因，以及如何进行威胁处置及安全加固防护。

2.3.10. 网络威胁态势感知

综合外部威胁、外连威胁、内部互连威胁三个方向全面监控网络威胁态势感知情况，关注扫描探测、外部攻击、口令猜测、风险访问、C&C 回连、隐蔽通道、恶意程序活动等网络威胁行为，并支持大屏投放监控。

2.4. 部署方案

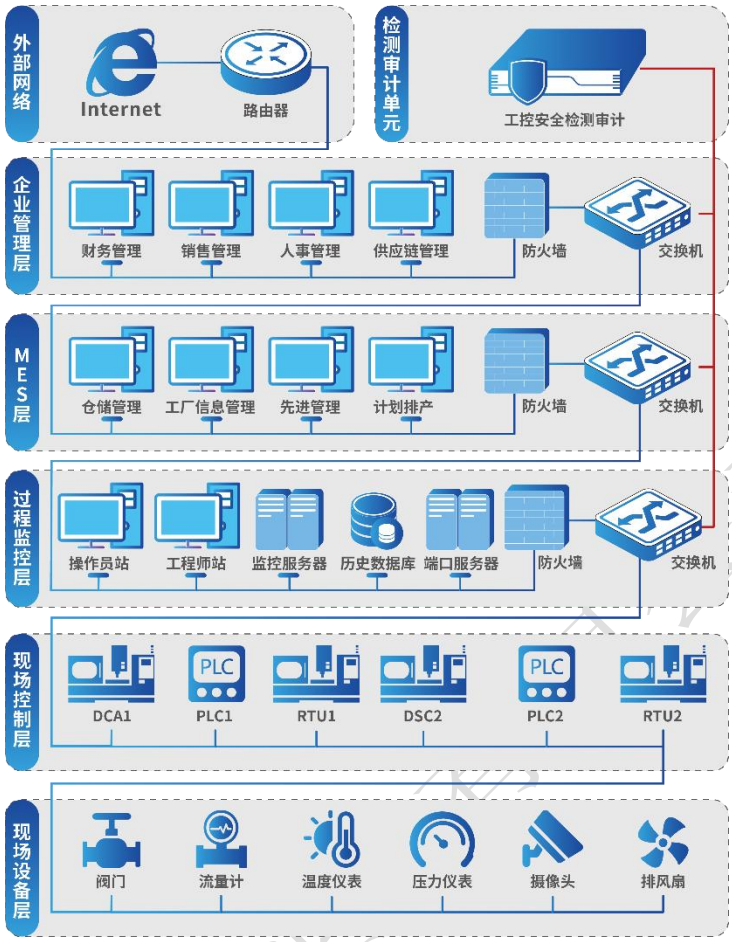
聚铭工控网络流量审计系统采用旁路 SPAN 部署方式和 TAP 部署方式，两种部署方式均不会改变用户现有网络架构和网络配置，且不会对用户现有的生产业务或应用产生任何影响。

2.4.1. 经典部署方案

经典部署方案可以帮助用户及时有效的发现网络中的异常情况，提升运维人员对安全问题处置效率，为客户在高级威胁入侵时，及时察觉，及时止损。

此方案能够解决如下安全问题

1. 全流量采集、分析、会话存储及检索，为安全回溯提供强大的支撑。
2. 发现网络威胁，包含常规网络攻击及未知威胁检测。
3. 发现网络中异常流量、端口。
4. 发现恶意文件及数据泄漏。


外部网络
Internet
路由器
检测审计单元
工控安全检测审计
企业管理层
财务管理
销售管理
人事管理
供应链管理
防火墙
交换机
MES层
仓储管理
工厂信息管理
先进管理
计划排产
防火墙
交换机
过程监控层
操作员站
工程师站
监控服务器
历史数据库
端口服务器
防火墙
交换机
现场控制层
DCA1
PLC1
RTU1
DSC2
PLC2
RTU2
现场设备层
阀门
流量计
温度仪表
压力仪表
摄像头
排风扇