**国家电网公司**

**基于深度学习的全流量高级可持续威胁智能分析技术研究及平台开发项目**

**工作方案**

**目录**

[1. 项目概要 1](#_Toc16188459)

[1.1. 项目基本信息 1](#_Toc16188460)

[1.2. 项目说明 1](#_Toc16188461)

[1.3. 项目期间 2](#_Toc16188462)

[1.4. 项目预计成果 2](#_Toc16188463)

[2. 项目工作方案 3](#_Toc16188464)

[2.1. 项目计划内容 3](#_Toc16188465)

[2.2. 设备硬件部署 3](#_Toc16188466)

[2.3. 实现功能分析 4](#_Toc16188467)

[2.4. 系统平台特色 7](#_Toc16188468)

[3. 项目工作量与进度安排 8](#_Toc16188469)

[3.1. 项目工作量 8](#_Toc16188470)

[3.2. 项目进度安排 9](#_Toc16188471)

工作方案变更记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本号 | 变更次 | 变更原因/变更内容 | 修订部门/修订人 | 实施日期 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 项目概要

## 项目基本信息

项目名称：基于深度学习的全流量高级可持续威胁智能分析技术研究及平台开发项目

项目经理：

项目单位：

项目开始时间：

项目结束时间：

## 项目说明

长期以来，病毒问题是困扰工业控制系统的一个棘手问题，全球工控安全事件频发逐年增加，2016年290起，2017年305起，2018年320起，平均是2010年伊朗震网事件爆发的8倍多，工控信息安全形势愈发严峻。从2008年到2017年发生的事件情况来看，主要是APT攻击、蠕虫病毒、特洛伊木马、恶意软件、勒索病毒等导致的安全事件。如果不针对工控网采取措施，极有可能成为下一个攻击目标，与传统IT不同，不但会导致系统DOWN机，还可能导致人身伤害。如：

1、2008年北京奥运会和2010年上海世博会等重要活动期间，我国电力系统受到了来自境外各种高密度、高强度的恶意网络渗透和攻击；

2、2011年5月1日，华能某电厂恶性电气误操作事件，导致1人死亡，1人重伤；

3、2014年10月17日，云南电网某供电局变电站误操作事故，导致1人触电死亡；

4、2015年，上海某电厂工程师感染病毒，导致监控数据采集异常，经调查确认是技术人员使用U盘拷贝数据造成。

5、2017年，山东43座风电、光伏电站由于电力监控系统安全防护和机组网络管理方面存在重大隐患，被强制断网；

6、2018年1月8日，黑龙江省电力调控中心一侧网络安全管理平台发出重要告警，告警来源为安达某40KMW光伏电站，涉及三套电力生产业务系统，国家能源局东北监管局高度重视，立即责成国网黑龙剑省电力调控中心就相关情况进行处理。

目前公司还缺乏针对全省集中开展网络安全分析、溯源和取证方面的能力，为提升省公司网络攻击、日志审计和关联分析能力和网络安全协同防护水平，通过利用数据分析和深度学习技术，通过研发一种基于深度学习的全流量网络安全智能分析平台，对公司系统网络流量数据采集、预处理、清洗、特征选择、深度神经网络训练和预测等一系列步骤来识别电力网络中的异常流量，对网络恶意流量的在线智能检测及未知威胁的发现具有重要理论意义和实际应用价值。

## 项目期间

预计项目开始时间：

预计项目结束时间：

实际项目开始时间：

## 项目预计成果

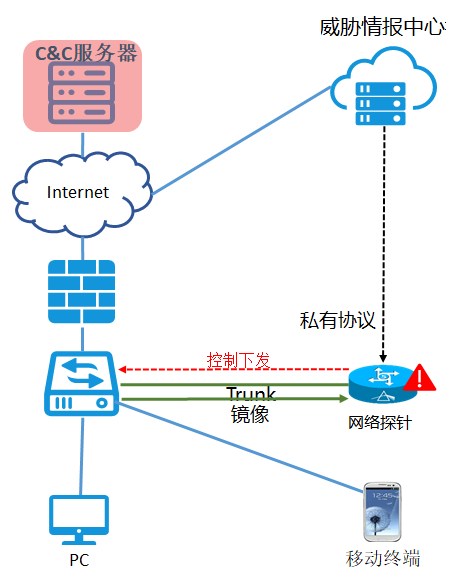
* 提交面向深度学习的全量威胁数据处理子系统1套；
* 提交基于复杂线索关联分析技术的快速恶意流量侦测子系统1套；
* 提交基于深度神经网络技术的未知威胁检测与验证子系统1套；
* 提交网络威胁全流量回溯子系统1套；
* 提交基于大数据可视化技术的网络威胁和态势监控子系统1套；
* 建立以上模块的全流量网络安全智能分析平台；

# 项目工作方案

## 项目计划内容

通过镜像方式对流量进行捕获，研究从流量中提取资产主机指纹技术，主动探测网络中存活主机设备，提升资产识别的精准度，实现自动、智能、快速定位的资产管理, 并可视化动态绘制资产网络拓扑。通过调研国内外TensorFLow、Keras、CNTK等深度学习技术的发展方向以及恶意流量高级安全分析技术领域的应用情况；开展全流量、离线安全日志的威胁建模研究，分析电力行业恶意流量及离线日志中威胁的特征参数，研究特征向量降维和归一化预处理技术，针对恶意攻击不同场景设计多种类型的深度学习模型和算法来进行训练和威胁建模，并在线验证模型对恶意攻击和未知威胁检测的准确性和实用性；最终实现原型系统研发，基于深度学习算法、架构及威胁建模研究，研发基于机器学习的全流量网络安全智能分析原型系统，结合信息资产和威胁的深度分析，实现动态感知全网威胁的能力。

## 设备硬件部署



## 实现功能分析

根据招标要求，基于深度学习的全流量网络安全智能分析平台，主要实现以下8个方面的内容：

* 信息资产主动式识别技术研究；
* 基础深度学习算法的恶意流量高级安全分析技术研究；
* 全流量、离线安全日志的威胁建模研究；
* 基于大数据的网络安全风险智能分析技术和可视化技术研究；
* 信息系统生态环境（实现信息资产、网络拓扑的主动发现）感知平台研发；
* 信息系统脆弱性感知平台研发；
* 信息系统威胁感知平台研发；
* 信息系统风险分析及安全态势综合展示平台研发。

**1.信息资产识别：**

通过主动和被动信息采集技术，智能采集设备的IP/MAC信息、路由信息、身份信息、主机名、操作系统、位置信息、流量信息等。基于设备画像技术，智能识别网络拓扑、设备的类型、设备厂家、设备状态（新设备/在线设备/离线设备）、设备安全状态（安全、较安全、不安全）、设备之间的连接关系等，包括对PC设备、网络设备、移动设备、IoT设备（含视频终端等）、ICS设备等主流设备类型和厂家的识别。

**2.全流量、离线安全日志的威胁分析：**

* 采用旁路进行方式，对流量进行捕获分析，根据数据包检测匹配安全事件库，形成基于全流量的威胁分析平台。
* 通过与第三方安全日志做对接，进行基于离线安全日志的威胁分析。

**3.恶意流量高级安全分析**：

* 通过平台集中展示当前网络的实时流量总数，互联网上行/下行流量及实时会话数以及实时连接关系，流量主机、应用层协议、服务器端口流量、发送者流量等信息。
* 通过流量地图展示互联网流量实时的连接位置。
* 分析局域网间互访以及局域网访问外网时产生的不明流量、违规流量、恶意流量、可信流量等。

**4.基于大数据的网络安全风险智能分析**：

* 基于设备类型、IP、MAC、设备名、操作系统、系统服务、流量特征、行为特征的设备仿冒检测。发现设备仿冒时，系统会发出告警或者自动阻断。
* 自动学习网络中设备之间的连接关系以及访问互联网的行为，自动构建用户正常的访问行为模式，智能发现异常的连接。发现异常连接时，系统会发出告警或者自动阻断。
* 自动学习网络中设备之间的流量行为特征以及访问互联网的流量特征，在某一时间段内流量发生异常时，系统会发出告警或者自动阻断。
* 及时发现异常协议的访问（如80端口，跑的是非http协议流量），可立即报警并阻断。
* 自动学习设备的在线时长，一旦发现设备在线时间异常，可立即报警或阻断。
* 对于服务器、哑终端设备、IoT设备等接入位置相对固定的设备，一旦发现设备接入位置发生变化，会立即报警或阻断。
* 采用机器学习和威胁情报相结合的方式，对域名进行可疑度分析，发现恶意域名立即告警或者阻断。

**5.信息系统生态环境网络拓扑感知：**

* 智能识别，采用设备画像技术，智能识别网络拓扑、设备的类型、设备厂家、设备状态（新设备/在线设备/离线设备）、设备安全状态（安全、较安全、不安全）、设备之间的连接关系等，支持对PC设备、网络设备、移动设备、IoT设备（含视频终端等）、ICS设备等主流设备类型和厂家的识别。

**6.信息系统脆弱性感知**:

* 对Web/SSH/TELNET/FTP等应用的弱口令进行实时检查，用户可通过导入自主的账号和密码字典的方式进行系统弱口令的检查。
* 漏洞检测，发现终端、服务器等的漏洞情况。
* 补丁安装情况检查，发现终端、服务器等的补丁修复情况。

**7.信息系统威胁感知**:

* + C&C攻击检测：检测设备与C&C（命令与控制服务器）的连接行为，发现时可立即告警或者阻断；
  + DoS攻击检测：SMTP/MYSQL/RDP/DNS/HTTP等协议的DOS攻击检测，发现时可立即告警或者阻断；
  + 暴力破解检测：RDP/SSH/FTP等协议的暴力破解攻击检测，发现时可立即告警或者阻断；
  + 勒索病毒检测：检测WantCry等勒索病毒的检测；
  + 僵尸网络、蠕虫、木马攻击检测：发现僵尸网络、病毒、蠕虫等攻击行为可立即告警或者阻断；
  + 网络扫描检测：Nmap、Nessus、Nikto等常见扫描工具的端口、数据库、Web页面扫描，操作系统探测等扫描行为检测，发现时可立即告警或者阻断；
  + Shellcode攻击检测：如利用SHELL编写一段代码，发送到服务器利用代码的特定漏洞获取权限，发现时可立即告警或者阻断;
  + 恶意软件攻击检测：检测间谍软件、仿冒的防病毒软件等恶意软件，发现时可立即告警或者阻断；
  + 权限破解攻击检测：检测普通或者超级管理员的权限破解攻击，发现时可立即告警或者阻断；
  + 视频语音协议攻击检测：检测视频和语音协议的攻击，发现时可立即告警或者阻断。

**8.信息系统风险处置及安全态势综合展示**:

( 1 )对存在风险的设备，系统可以采用以下几种方式进行智能处置：

* 通过SMS/Email/Web等方式通知管理员和使用者，及时做出响应；
* 根据系统预设置的策略，对设备阻断，重认证或跳转到安全区域进行修复；
* 通过Syslog/SNMP Trap等方式通知事件中心，如SOC/SIEM等。

（2）可视化管理

* + - * 展现全网风险状态：包括设备的异常行为、攻击行为、合规性、脆弱性的严重程度和分布情况。
      * 展现入侵视图及过程：展示全网设备分布图、攻击链分析视图、准入状态视图、不合规设备趋势图、异常行为设备趋势图、攻击行为设备趋势图、流量视图、域名分析视图等；
      * 可导出取证报告，包含设备的安全指数，设备的基本信息、不合规信息、攻击行为信息、异常行为信息、网络连接行为信息、IP地址及其它相关辅助信息等。

## 系统平台特色

**风险精准识别**

* 动态“陷马坑”：能够准确捕获网络攻击行为。（智能幻影：可以按比例自动幻影出与在线设备一致的设备类型和数量，也可以手动创建幻影设备，发现恶意访问幻影设备立即告警或者阻断；）
* 通过高质量的大数据与AI算法实现精准识别，高质量表现为数据自行从源头直接采集、加工，避免数据失真；另外高质量还表现为数据维度多，包括设备的类型、安全状态、使用者、接入位置、接入时间、网络行为、访问对象、使用习惯等信息

**发现未知类型攻击**

* 动态“陷马坑”：通过诱捕方式发现攻击，不需要知道攻击类型即可捕获
* 通过大数据和机器学习算法发现未知类型攻击，包括画像式发现、关联分析、可疑域名分析等

**安全可视化**

* 资产可视化：自动发现网络资产，识别高价值资产（如数据库、源代码服务器、域控服务器、ERP服务器等），可视化展现资产的状态、类型、位置、使用者等信息
* 行为可视化：自动识别设备与用户行为，可视化展现访问关系和使用习惯
* 攻击可视化：智能识别网络攻击，可视化展现攻击入侵路径、横向移动过程、攻击方式等

**部署简单、扩展性强**

* 采用旁路部署的方式，无需修改现有的网络拓扑，配置简单
* 无需终端电脑安装任何的客户端软件和插件，无需修改任何配置
* 支持分布式部署和集中部署，管理中心可支持线性扩展（集群）

# 项目工作量与进度安排

## 项目工作量

| **研究阶段** | **研究内容** | **内容描述** | **投入人数** | **投入时间** | **工作量** |
| --- | --- | --- | --- | --- | --- |
| 前期准备与技术调研阶段 | 前期准备 | 制定项目工作方案 |  |  |  |
| 工作计划、组建项目团队 |  |  |  |
| 需求调研 | 从软硬件基础环境、应用、业务、数据现状和技术现状五个维度对进行调研分析。 |  |  |  |
| 调研分析 | 开展深入的分析和研讨，对应用性能监测管理的现状进行总结提炼。 |  |  |  |
| 调研汇总 | 对需求调研分析的整体情况进行汇总，为后续研究做好基础铺垫工作。 |  |  |  |
| 关键技术研究阶段 | 解决方案设计 | 项目的解决方案 |  |  |  |
| 研究关键技术 | 识别核心方法及关键技术点，开发技术研究和技术研发 |  |  |  |
| 结合典型应用场景进行设计 | 开展典型应用场景设计工作，为技术验证提供依据。 |  |  |  |
| 技术验证阶段 | 对关键技术点开展技术验证 | 针对技术研发成果，开展技术验证 |  |  |  |
| 典型业务场景验证 | 开展针对项目的验证。 |  |  |  |
| 项目总结与验收阶段 | 方案完善 | 分析存在问题，结合潜在用户需求，完成整体方案制定。 |  |  |  |
| 报告编制 | 编制项目成果报告。 |  |  |  |
| 系统评审 | 编制项目验收评审材料。 |  |  |  |
| 项目验收 | 组织参与项目验收评审。 |  |  |  |
| 总计（人天） | | | | |  |

## 项目进度安排

| 序号 | 时间段 | 内 容 |
| --- | --- | --- |
|  | 2019.7-2019.8 | **研究内容：**  1、确定项目的主要的内容，明确项目的目标，确定项目主要的工作内容、工作思路、工作方法；  2、讨论并制定项目的进度计划，讨论确立项目计划，并评审项目的项目计划，办理项目的立项手续，协调资源，组建项目的团队，明确的项目的组织架构及职责  **输出成果：**  1、完成项目工作方案的编制  2、完成项目计划书及进度表的编制 |
|  | 2019.8-2019.12 | **研究内容**：   1. 信息资产主动式识别技术研究； 2. 基础深度学习算法的恶意流量高级安全分析技术研究； 3. 基于大数据的网络安全风险智能分析技术和可视化技术研究； 4. 信息系统生态环境（实现信息资产、网络拓扑的主动发现）感知平台研发； 5. 信息系统脆弱性感知平台研发； 6. 信息系统威胁感知平台研发； 7. 信息系统风险分析及安全态势综合展示平台研发。   输出成果：   1. 基于深度学习的全流量高级可持续威胁智能分析平台研究报告。 2. 基于深度神经网络技术核心期刊2篇发表申请 |
|  | 2020.1-2020.4 | **研究内容：**  全流量高级可持续威胁智能分析平台平台设计和原型软件研发：  **输出成果：**   1. 完成系统的需求分析报告的编制，完成系统功能和界面设计。 2. 态势感知发明专利申请 3. 态势方向论文2篇 |
|  | 2020.5-2020.7 | **研究内容：**  1、进行系统功能的验证工作，通过验证工作，对前期研究成果进行验证，以验证结果为基础完成报告的编制。  3、进行项目的验收材料编制工作并完成项目的验收工作  **输出成果：**  1、完成基于深度学习的全流量高级可持续威胁智能分析平台研究报告的编制；  2、发表全流量网络安全智能分析领域论文3篇，专利1项，软著5项 |