**网络安全实战化防护能力提升项目需求说明**

目录

[**1. 项目概述** **4**](#_Toc18296_WPSOffice_Level1)

[1.1. 项目背景 4](#_Toc1151_WPSOffice_Level2)

[1.2. 项目目标和范围 4](#_Toc12820_WPSOffice_Level2)

[**2. 项目业务及管理需求** **5**](#_Toc1151_WPSOffice_Level1)

[2.1. 总体要求 5](#_Toc4534_WPSOffice_Level2)

[2.2. 项目详细需求 5](#_Toc1378_WPSOffice_Level2)

[2.3. 项目里程碑及周期 6](#_Toc20374_WPSOffice_Level2)

[**3. 投标方资质、成功案例和履约能力** **7**](#_Toc12820_WPSOffice_Level1)

[**4. 项目成员资质要求** **8**](#_Toc4534_WPSOffice_Level1)

[**5. 项目工期要求** **9**](#_Toc1378_WPSOffice_Level1)

[**6. 项目验收标准** **10**](#_Toc20374_WPSOffice_Level1)

# 项目概述

## 项目背景

根据世界经济论坛（WEF）发布的《2020年全球风险报告》显示，数据诈骗和数据盗取、网络攻击位列10大可能性最高的风险中的第6、7位，信息基础设施崩溃、网络攻击位列10大影响力最大的风险中的第6、8位。国家层面对信息安全重视程度不断加强，内保局、银保监会等机构加大了安全监管力度。公司已建设从信息安全设施、制度、人员等方面构建了较为完整信息安全体系，但具有专业的攻防经验的人员稍有不足，难以支撑后期多频次的攻防演练，仍然需要引入专业的培训提升集团信息安全人员队伍的实战能力。

## 项目目标和范围

组织集团以及各子公司信息安全条线约50人全面参与培训，预期通过学习顶级攻击队、防守队提供的实战案例，使其掌握实战中安全事件监测预警、分析研判、应急响应、溯源取证和协同联动等技术方法，提升其安全防护实战能力，形成一支懂业务、善攻防、能实战的信息安全队伍。从而提升集团整体安全防御能力。

# 项目业务及管理需求

## 总体要求

有计划的按照项目详细需求进行培训授课，及时提供授课信息供受训学员课前准备，组织讲师为学员答疑。通过培训切实提高学员的网络安全实战防护能力。

## 项目详细需求

网络安全实战化防护专业能力培训内容共分5个方面，监测预警、分析研判、应急响应、溯源取证、协调联动。

|  |  |  |
| --- | --- | --- |
| 课程方向 | 课程内容 | 课程时间 |
| 监测预警 | 提炼实战中监测预警方向的工作思路与方法，从攻击和防护两个维度讲解典型技战法，包含敏感信息泄露状况的监测手段与方法，多类边界突破、内网渗透、零日漏洞攻击的监测手段与方法，社会工程学攻击的发现和预警，资产测绘与管理、态势感知和威胁情报平台等监测手段的构建和运营方法等。 | 14课时 |
| 分析研判 | 提炼实战中分析研判方向的工作思路与方法，从攻击和防护两个维度讲解典型技战法，包含信息收集、密码字典构造等支撑分析方法，涉及边界突破、内网渗透、社会工程学攻击、工控网络攻击等方面的安全事件分析方法，以及基于流量行为画像、威胁情报、安全大数据等手段的分析思路和方法等。 | 14课时 |
| 应急响应 | 提炼实战中应急响应方向的工作思路与方法，从攻击和防护两个维度讲解典型技战法，包含攻击意图的识别与处置，应对零日漏洞攻击的应急处置，应对APT攻击的应急处置，应对专用设备、安全设备攻击的应急处置和联动响应方法等。 | 14课时 |
| 溯源取证 | 提炼实战中溯源取证方向的工作思路与方法，从攻击和防护两个维度讲解典型技战法，包含通过技术策略提升溯源和取证能力的思路与方法、全链条攻击路径追踪还原技术与分析方法、针对邮件等专项攻击的溯源思路和方法、基于定制化诱捕的主动防御方法等。 | 14课时 |
| 协同联动 | 提炼实战中协同联动方向的工作思路与方法，从技术和管理两个维度讲解典型技战法，包含多场景攻击案例详解、供应链安全管理思路、多层次主机防护策略、钓鱼社工攻击体系化防御方法、多维度精细化网络分区隔离技术战法、系统化口令攻击策略、网络安全建设整体防控的思路和方法等。 | 14课时 |

## 项目里程碑及周期

培训课程按月进行，每个月一个方向，每个方向14节课，单节课时长2小时左右，每月14节课集中在4-5天。

# 投标方资质、成功案例和履约能力

|  |  |
| --- | --- |
| 需求项 | 需求描述 |
| 1、成功案例 | 投标方近3年的金融行业、保险行业的培训案例 |
| 3、合作关系 | 投标供应商与我集团已经建立了合作关系 |
| 4、资质证明 | 1、在中华人民共和国境内注册，具有独立法人资格，且有效存续，通过历年工商年检，生产、经营资质通过相关职能部门历年年检；  2、具有相当的技术力量和信誉，良好的商业声誉和健全的财务会计制度；  3、具有履行合同所必须的专业技术能力，与专业机构合作的应有授权证明；  4、有依法纳税的良好记录；  5、近三年在经营活动中没有重大违法记录和声誉风险；  6、遵守有关的国家法律、法令和条例。 |
| 5、其他需求 | 1、第三方机构及其项目工作人员必须签署有关保密协议；  2、项目交付物知识产权由甲方所有。 |

# 项目成员资质要求

讲师团队应由在攻防实战演练工作中，表现特别突出、能够发挥一锤定音作用的攻击与防护指挥官组成。讲师团成员通过提炼网络攻防技战法，与国家级网络安全专家一起，制作课件、完成授课任务。

# 项目工期要求

培训课程每个月1个方向，项目启动至多在6个月完成内完成5个方向的培训。

# 项目验收标准

按培训计划的按照课程内容组织培训授课，及时提供授课信息供受训学员课前准备，按找培训内容要求提炼实战中监测预警方向的工作思路与方法，从攻击和防护两个维度讲解典型技战法，组织讲师为学员答疑。提供可供回看的视频，提供相应的远程授课所需要的接入设备及上门部署。