从被动防御到主动安全：
把握现代企业的网络安全命脉，构筑数据防护的坚实城墙

主讲：黄辰 教授

【课程背景】

在全球电子互连、计算机病毒和电子黑客充斥、电子窃听和电子欺诈肆虐的时代，安全问题必须开始重视。互联网应用的深入发展，一直在深刻地影响着我们每个人的生活，改变着我们的社会。网络使我们的生活变得既丰富多彩又便利快捷，使我们的社会管理效率得到了空前提高。当然，在每个人享受网络为我们带来好处的同时，我们最关心的问题仍然是安全。可以肯定地说，在未来的就业领域、专业学习、技术开发和学术研究等方面网络安全仍将是大众最为关注的热门主题。

本课程将循序渐进地分析网络安全促使金融资产的底层逻辑。一方面，网络技术爆炸性的增长给数据泄露带来了很大的风险，促使企业必须保障数据和信息的真实性，并且仍需保护基于网络的系统免受攻击等。另一方面，网络安全已经成熟，并正在开发实用而有效的应用来增强网络安全，因此将企业战略提高到网络安全层面，有利于为企业数字化转型提供有力保障，有利于为企业在信用度上带来更多地潜在客户。未来，高端可防护且可持续升级的安全系统是企业发展壮大的必要准备之一。

【课程收益】

- 全面阐述了建设网络安全平台的方法论和关键因素，对不同行业的网络安全案例进行深入分析，给予企业有价值的指导
- 全面解读了什么是网络安全、信息安全以及数据安全如何保护商业创新
- 既有理论高度又有丰富的落地案例，能够帮助企业管理者快速建立网络安全认知和实施指导
- 帮助企业充分实现数据安全价值，实现数据服务的可靠性
- 可以有效地支持企业业务发展，提高企业的效能，降低企业运营风险
- 强调数据安全服务和智能安全服务，指导企业数据安全平台的建设，实现数据可用、易用、好用、可追溯、可复用和可管理
- 促进数据安全平台在不同行业中落地生根，让数据安全智能化发挥更大的价值

【课程特色】

- 从一线实战中提炼出有生命力的洞见，并将先进的理念付诸实践
- 明确的目标、创新的方式和清晰的执行路径
- 既有前瞻视野，又有丰富工具，更有翔实案例，为企业管理者提供具有借鉴意义的路线图和方法论
- 提供独到的视角，解读企业应该如何面对生命周期中重要的变革管理问题，实现核心业务的全方位进化
- 既有理论高度又有实践经验，坚持利他为先、利众为本的理念
- 案例丰富、逻辑清晰、洞察深刻、深入浅出、发人深思

【课程对象】

- 企业高层管理者：董事长、总裁、总经理、分管副总等
- 战略高层、战略规划、顶层设计负责人（CEO、CTO、CIO、CMO 等）
- 各个条线的业务负责人和技术专家
- 产品开发与创新人员、服务方案制定者
- 市场营销策划、客户经理、产品经理等
- 创新业务的负责人，创新创业导师及实践者

【课程时间】6-9 小时（6 小时/天）

【课程大纲】

第一部分、现代企业的网络安全以及数据安全意识建设

一、现代企业的网络安全意识建设

1、网络安全意识介绍

- 什么是信息安全意识？
- 影响信息安全有哪些基本原因

2、企业面临的主要安全威胁

- 网络安全问题
- 企业面临的主要安全威胁

3、网络安全防护措施

- 管理缺陷
- 技术缺陷

4、网络安全问题应对措施

- 基础
- 互联网边界控制
- 防篡改
- 数据安全保障
- 内部节点控制
- 安全服务

二、现代企业的数据安全意识建设

1、数据安全现状及面临的挑战

- 数据安全是重中之重
- 核心资产保护--数据冰山
- 数字化转型下，安全挑战日益严峻

2、数据安全已成为网络安全的重灾区

- 攻击者的构成

- 黑客攻击的动机
- “抢银行”不如“抢数据”
- 常见攻击方式
- 常规的攻击步骤
- 勒索软件是如何攻陷业务系统的？
- 一个常规安全事件的解决流程案例

3、数据安全的风险来源与分析

- 内部 IT 系统复杂化
- 泄露途径众多，防不胜防
- 安全管理之痛——安全设备孤岛无法有效保障业务数据整体安全
- 安全管理之痛——安全事件分析难
- 安全管理之痛——安全威胁处置难
- 数据安全管理之痛——信息安全资金投入难

4、安全相关的法规政策与要求

- 国际主要国家安全法案
- 我国出台法规政策推动网络安全
- 网络安全法明确等级保护制度
- 网络安全法的规定动作
- 信息安全三同步
- 等保之痛-难以应对新技术风险

三、数据安全高强度防护优化方案

1、安全防护能力提升的主要方式

- 加强自身基础运营--风险评估要素关系
- 基于表现形式的资产分类

2、找到核心数据，分类分级进行防护与治理

- 数据分类是数据保护的首要环节，是数据风险的重要依据
- 数据分级依据数据价值或等级，对敏感数据进行精准防护
- 数据脱敏

3、数据安全防护最佳实践

4、数据安全建设目标

第二部分、网络安全运营体系建设：安全运营为企业发展赋能

一、企业网络安全的发展

1、企业发展信息化背景

- 新一代信息技术的加速应用
- 新背景下安全风险加剧
- 网络安全息息相关
- 网络安全相关政策

2、网络安全运营体系理解

- 安全运营的定义
- 安全运营的三个阶段
- 安全运营的作用
- 安全运营体系的设计思路
- 安全运营管理方法论
- 信息安全体系规划实施步骤

3、落实安全运营体系

- 安全运营建设的关键因素
- Gartner 自适应安全模型
- 体系设计
  - （1）组织架构
  - （2）安全运维流程
  - （3）指标验证与度量
  - （4）安全规则
  - （5）安全运营架构
  - （6）态势感知
- 运营平台
  - （1）运行监控
  - （2）异常监测预警
  - （3）关联防御
  - （4）响应处置
  - （5）PDCA

4、安全运营的价值和收益

- 安全运营的价值
- 网络安全价值观

二、网络安全等级保护

1、网络安全发展

- 网络安全产业界定
- 网络安全风险统计
- 网络安全发展变化
- 网络安全攻击变化
- 网络安全建设全景图

2、等级保护建设

- 等级保护发展历程
- 等级保护适用行业
- 等级保护建设意义
- 等级保护实施流程
- 等级保护技术标准
- 等级保护等级划分
- 等级保护总体架构

三、综合分析案例

1、解决方案——等级保护 2.0 通用解决方案

2、某省政务云等保 2.0 建设

3、某医保局整体安全建设

4、某应急管理局网络安全项目

5、某教育局二级等保建设项目

第三部分、智能化网络安全平台以及综合解决方案

一、网络安全软件平台

1、安全分析与响应平台

2、安全事件智能分析平台

3、统一运维管理平台

4、数据安全管理平台

5、网络安全攻防竞技平台

6、安全运营服务平台

二、网络安全硬件平台

1、网络全流量智能管控系统

2、业务性能可视化管理平台

3、安全日志审计系统

4、下一代防火墙/行为管理

5、NTA 网络流量安全分析系统

6、APT 高级威胁监测系统

三、安全服务及解决方案

1、等级保护 2.0 通用解决方案

2、信创安全体系解决方案

3、电子政务外网安全建设

4、工业控制安全解决方案

5、云计算安全解决方案

6、移动互联网解决方案

7、数据安全解决方案

8、安全运维服务

- 风险评估
- 渗透测试
- 重保值守
- 攻防演练

四、综合分析案例：

1、大数据安全管理平台典型案例：政务云等保 2.0 建设

2、安全事件智能分析典型案例：国网电力网络安全预警分析平台

3、安全事件智能分析典型案例：智慧园区安全建设

4、安全事件智能分析典型案例：应急管理局网络安全

5、一体化运维管理平台典型案例：某公司运维统一监控平台

6、智能运维管理平台典型案例：某大型电商运维建设