一、蓝队防守方案

> 蓝队防守，需要做到攻防前未雨绸缪，平日里下足功夫，从前期企业资产梳理、安全排查，到日常员工安全意识培训，以及规范化的安全管理与运营，软硬件安全防护体系的建设，到被攻击时完善的应急响应流程，都是蓝队的制胜法宝。

1. 资产梳理

- 对自身目标系统及关联资产梳理，形成资产清单。
- 资产清单应包括 IP 地址、操作系统、中间件、应用软件、域名、端口、服务、责任人、联系方式等，便于快速的进行资产定位、风险处置、应急等工作的开展。

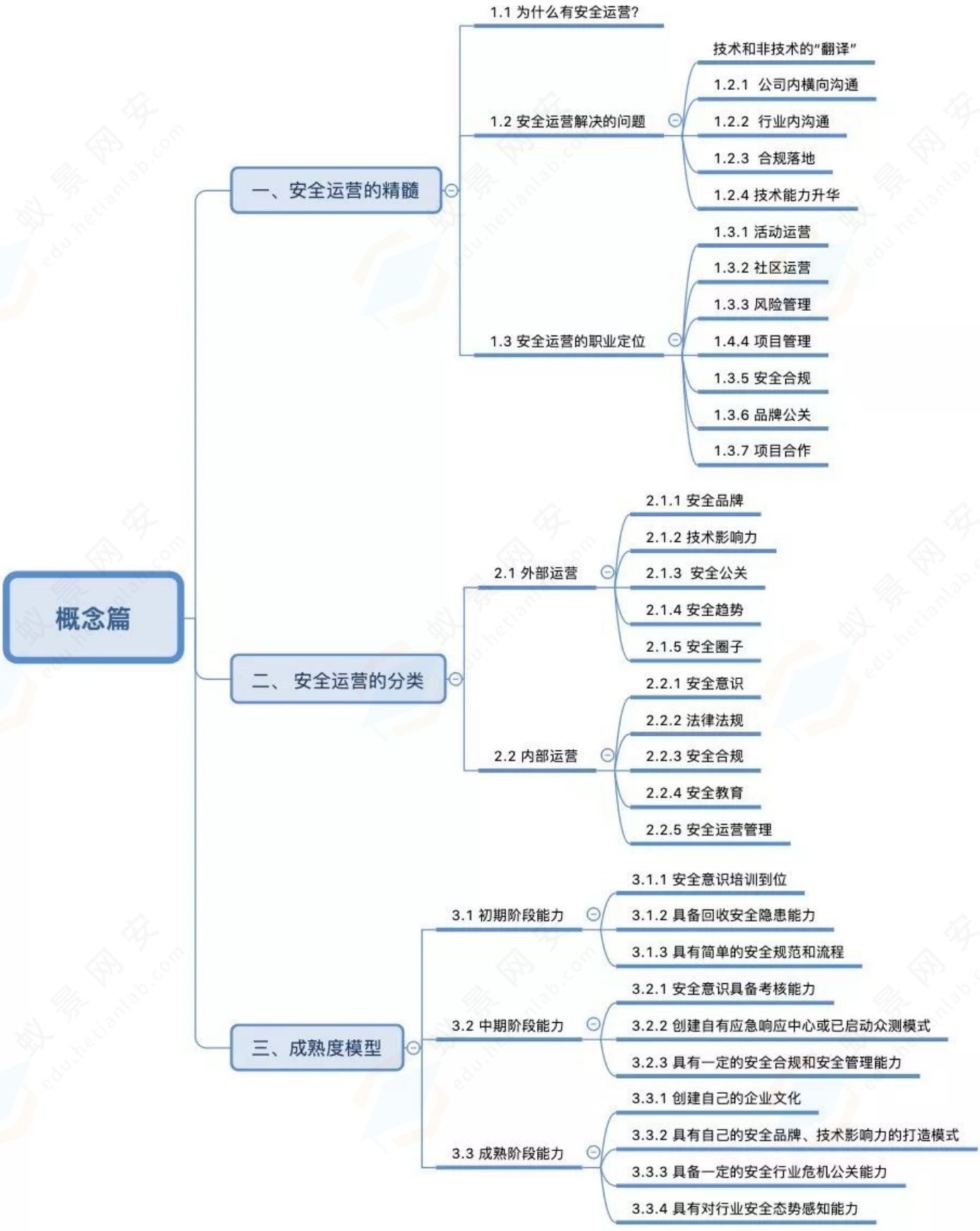
(1) 安全意识

- 攻防演练攻击方正面无法达到预期目标时，社工、钓鱼、进源就会被红队应用
- 以钓鱼邮件举例，攻击者常常会首先通过信息收集或爆破邮箱等手段获取相关目标邮箱账号，再通过获取的邮箱，向该单位有选择的发送钓鱼邮件，骗取账号密码或投放木马程序。由于钓鱼邮件来自内部邮箱及邮件内容经过精心伪造，所以会导致人很容易被诱骗点开邮件中的钓鱼链接或木马附

件，进而导致关键终端被控，甚至整个网络沦陷。

(2) 安全运营

- 网络安全运营是指为维护和保护计算机网络系统的安全而进行的一系列活动和过程。它涉及规划、实施、监控和响应各种安全措施，以确保网络的机密性、完整性和可用性。



(3) 应急响应

> 主要是课程中入侵排查部分

(4) 安全防护

> 企业安全建设中使用到的网络安全设备

参考绿盟、启明星辰、深信服
https://www.nsfocus.com.cn/
https://www.venustech.com.cn/

(5) “技战法”

> 技战法是指在战争或竞争中应用的特定的战术或策略。这个词源自中国古代军事经典《孙子兵法》，提出了许多关于如何取得优势和胜利的原则。"技战法"所指的是这些原则和策略。技战法可以包括各种方面，从战略计划到战术操作，以及与情报、资源管理、组织和领导力等相关的内容。它可以适用于不同领域，例如战争、竞争性体育比赛、商业竞争等等。

> 在战争中，技战法被用来指导军事行动，包括选择进攻或防守的策略、调动部队、制定作战计划以及在战场上选择和使用武器和装备等。在商业竞争中，技战法包括市场营销策略、产品差异化、成本管理、供应链优化等。
> - 参考长亭防守“技战法”
>   - https://mp.weixin.qq.com/s/NFeTazuPDUWTCEckca-vnA