日常情报，指令下发

1、Dark Reading: https://www.darkreading.com/

使用：订阅“Vulnerabilities”板块，快速获取CVE漏洞通报，每周五阅读“week in review”,掌握主流安全动态

2、Bleeping Computer: https://www.bleepingcomputer.com/

使用：以事件为核心，专注于勒索软件、恶意软件分析、修复方案等

3、iTnews(安全频道)： https://www.itnews.com.au/technology/security

使用：澳洲科技媒体，面向企业、政府的IT安全报道，结合Dark Reading使用，形成欧美+亚太视角的情报矩阵

4、Krebs on Security: https://krebsonsecurity.com/

使用：前《华盛顿邮报》调查记者Brian Krebs主持的博客，以深度报道闻名，推荐银行木马、数据泄露调查、政策与合规背景分析等专题

5、Threatpost:  https://threatpost.com/

使用：注重“易读性”的安全新闻站点，适合快速浏览，在开会或路上时用手机快速浏览，快速了解一天重要事件

6、The Register - Security:  https://www.theregister.com/security/

使用：英式毒舌媒体，含有不错的安全专栏

7、The DFIR Report:  https://thedfirreport.com/

使用：超高质量！专注于数字取证与应急响应（DFIR）的事件复盘，它详细记录的攻击链对红蓝对抗训练或有帮助

8、InfoSec Handles Diary Blog(SANS ISC):   https://isc.sans.edu/diary

使用：SANS ISC全球知名的安全培训机构，他们的Handler每天轮班写“日记”，丰富的日志分析技巧，开放的样本分析

9、TruKno: https://www.trukno.com/dashboard/news

使用：提供威胁情报仪表板式聚合，视觉化表现非常友好

10、Morning Security News: https://morningstarsecurity.com/news

使用：每日新闻摘要，风格类似邮件简报

11、ThreatABLE: https://www.threatable.io/

使用：新晋威胁情报聚站，设为浏览器首页，或使用RSS工具如Feedly集成订阅

12、Vx-underground:  https://vx-underground.org/?view=grid

使用：全球最大恶意软件样本资料库之一，收录攻击者工具、病毒构造器、战术战法文档，由于内容高度技术化，有部分样本涉及法律灰区，请在合法环境中使用

建议：

1、使用Feedly添加以上网站RSS

2、用Notion + Zapier 生成日报

3、高级用户可使用MISP自建情报共享系统

