



中联绿盟信息技术(北京)有限公司

NSFocus Information Technology Co. Ltd.



绿盟科技应急处理经验介绍

March 2005

专业服务部总监 王红阳

why@nsfocus.com

Professional Security Solution Provider



Agenda



- 绿盟科技应急处理经验
- 如何更好的应急处理

愈演愈烈



- 2004年11月底到2005年1月初，北京某网站连续3个月遭受猛烈的拒绝服务攻击。
- 攻击流量最高达到**800Mbps**。
- UDP Flood (dst port 80) & Connection Flood
- 多个厂商的设备均不能有效的防御。

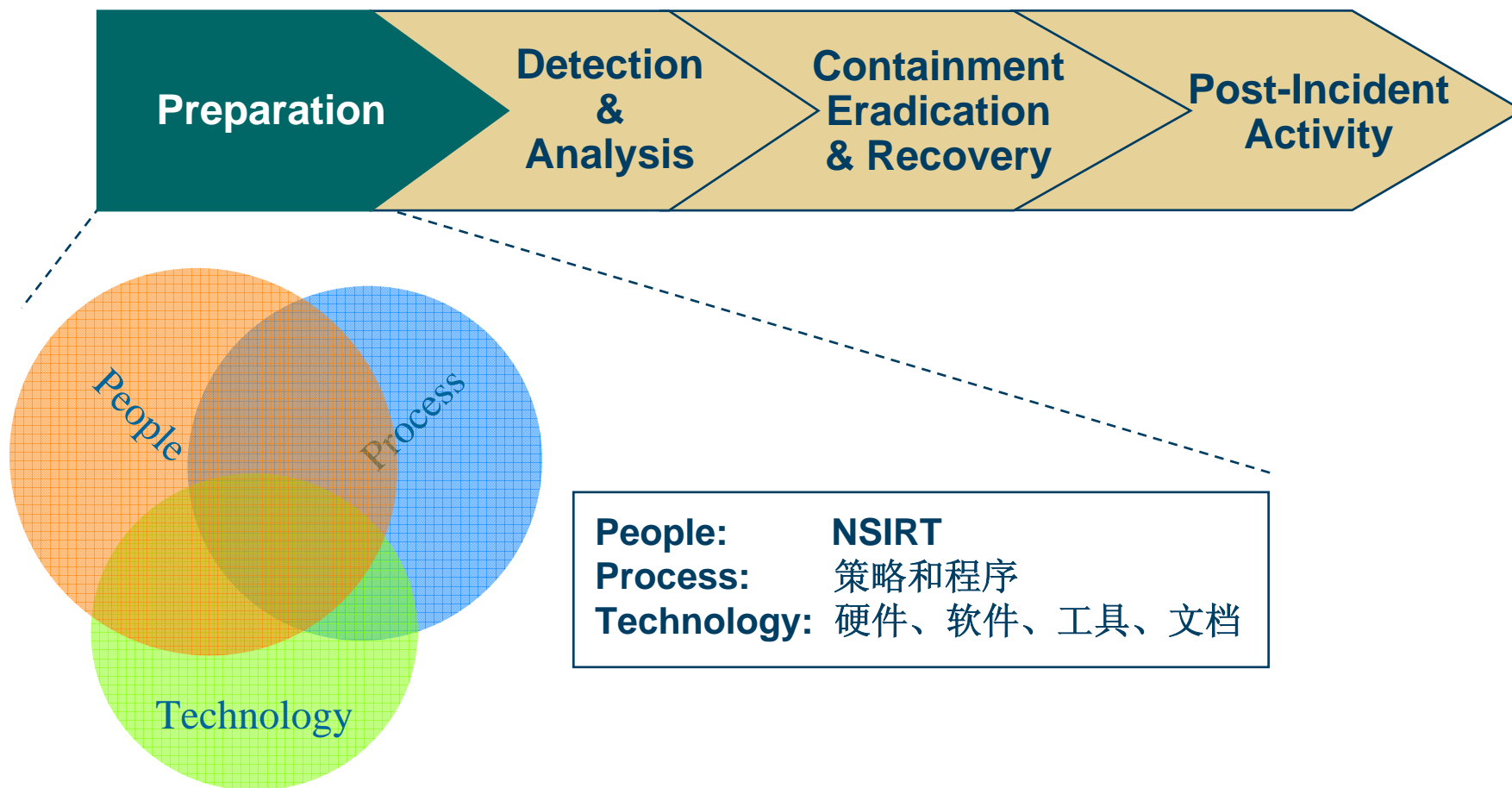
绿盟科技应急处理经验

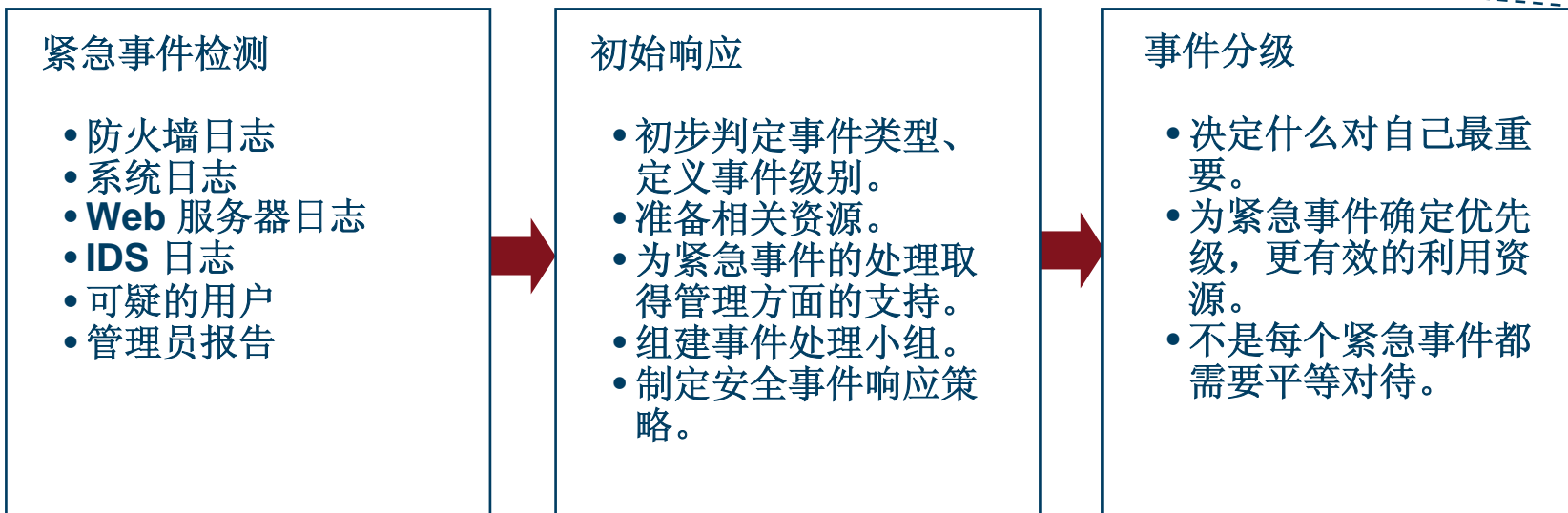
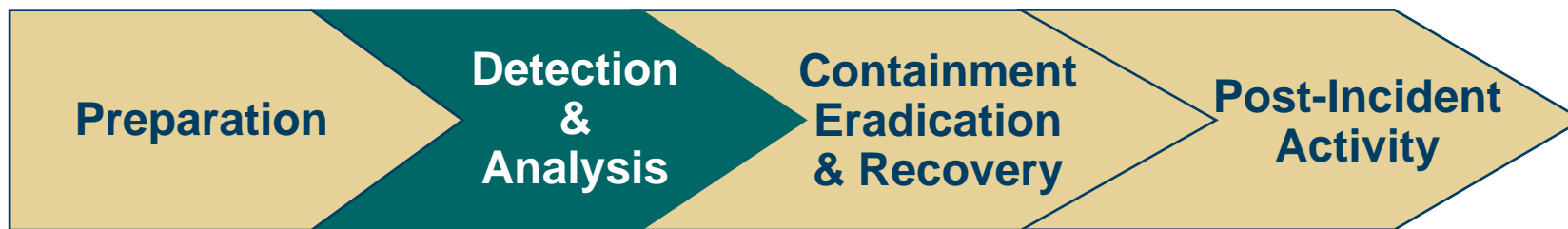
- 避免没有章法、可能造成灾难的响应。
- 更快速和标准化的响应。
- 确认或排除是否发生了紧急事件。
- 使紧急事件对业务或网络造成的影响最小化。
- 保护企业、组织的声誉和资产。
- 教育高层管理人员。
- 提供准确的报告和有价值的建议。

应急处理类别

- 入侵调查。
- 拒绝服务攻击响应。
- 大规模病毒爆发响应。
- 主机、网络异常响应。
-

如何有效的遏制DDoS的影响、恢复业务连续性、追踪来源
是一次拒绝服务攻击应急处理中的主要目标。





紧急事件检测

- 防火墙日志
- 系统日志
- **Web** 服务器日志
- **IDS** 日志
- 可疑的用户
- 管理员报告

初始响应

- 初步判定事件类型、定义事件级别。
- 准备相关资源。
- 为紧急事件的处理取得管理方面的支持。
- 组建事件处理小组。
- 制定安全事件响应策略。

事件分级

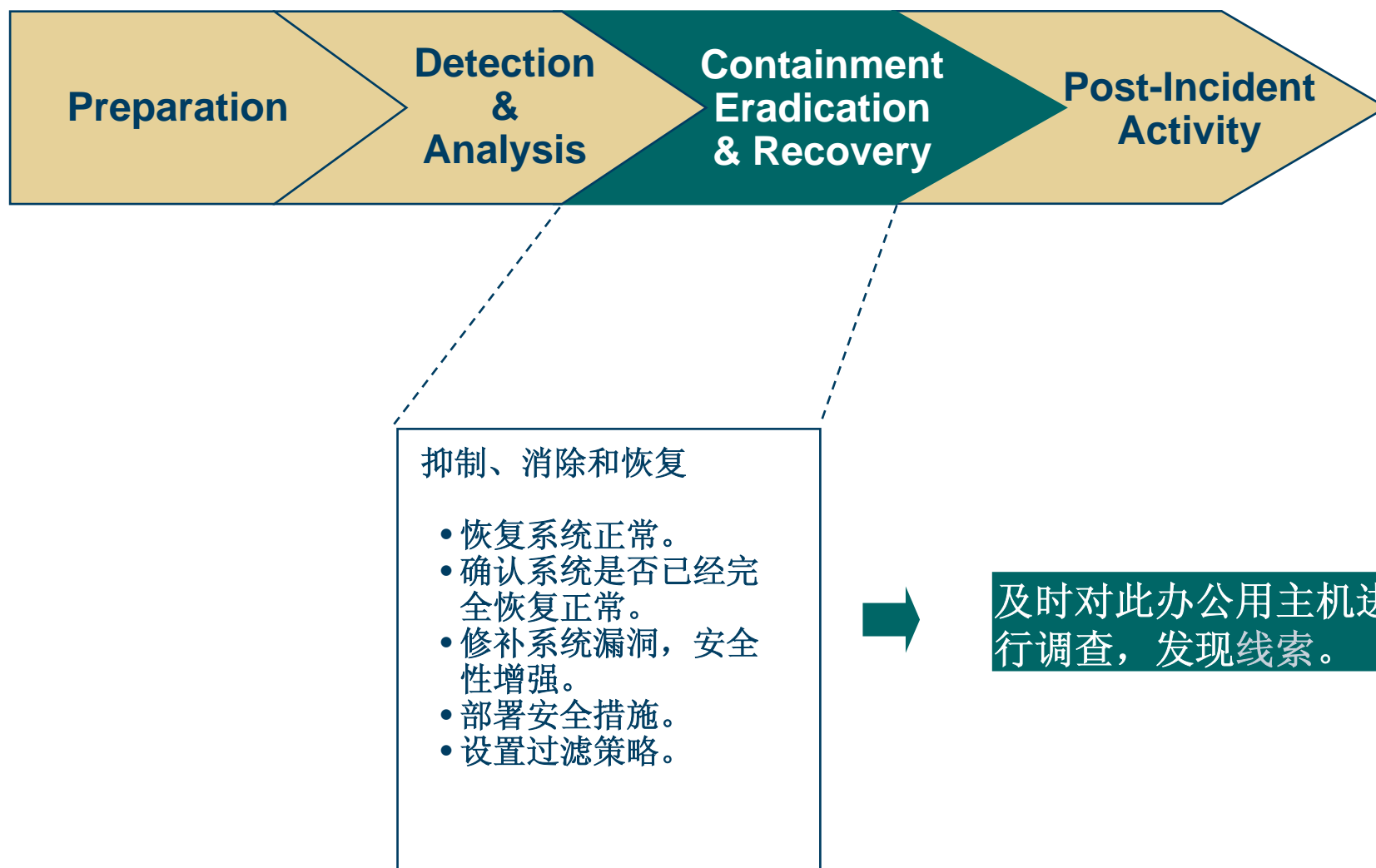
- 决定什么对自己最重要。
- 为紧急事件确定优先级，更有效的利用资源。
- 不是每个紧急事件都需要平等对待。

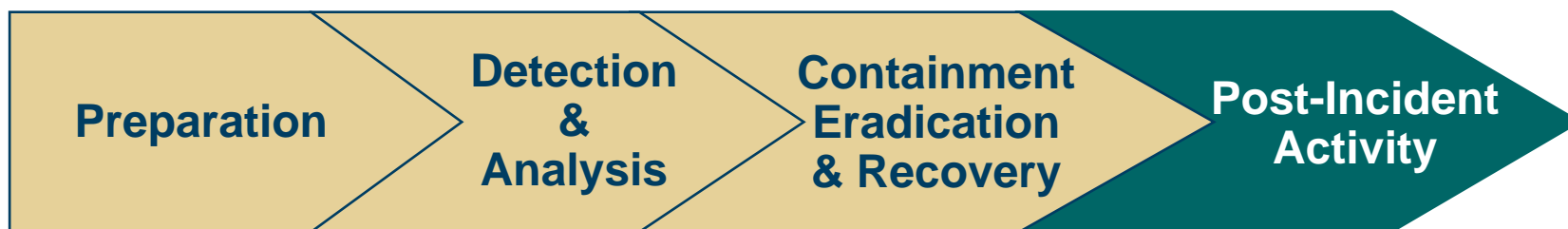
调查

- 事件起因分析。
- 事件取证追查。
- 系统后门检查、漏洞分析。
- 数据收集、数据分析。



从黑洞日志中发现，网站托管机房中一台办公主机有嫌疑。





追踪

- 提交事件处理报告
- 根据情况查找事件来源



教育

- 完善应急处理知识库、流程和规范
- 教育、培训，传播经验

经过追踪，

- 托管机房 -> X市IDC
- X市IDC -> Y省Y市
- 找出“僵尸网络(BotNet)”
- 找到元凶
- 发现更多隐藏的BotNet

如何更好的应急处理

主动(Proactive)

- 密切的国际合作。
- 必要的安全事件响应组织(CSIRT/CERT)。
- 通畅的信息沟通渠道。
- 及时的信息发布。

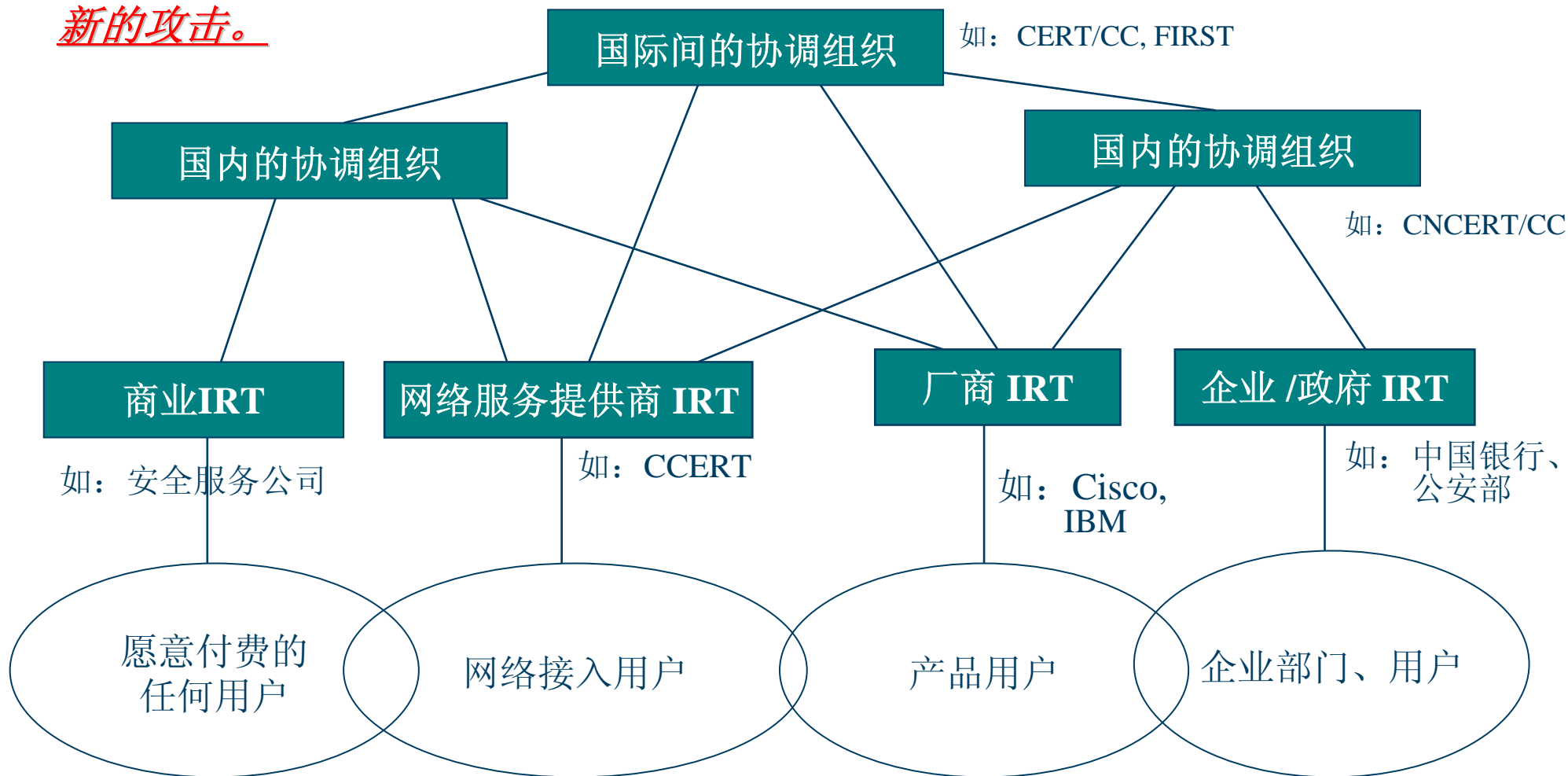
开放(Open)

- 信息、数据、方法的共享。
- 多方合作（政府、专业厂商、专业组织、ISPs、IDCs、应急组织等）。
- 安全事件处理的相互配合与支持。

有效(Effective)

- 大规模异常事件的发现能力。
- 重大网络安全事件的初步监测分析（种类、特征）能力。
- 安全事件的快速定位。
- 充分、综合发挥各种相关产品、工具的优势。
- 更快速和标准化的响应。
- 多方协作。

协作最重要，尤其面对新的攻击。





永远的行动

- 马拉松的准备，并非短跑。
- 并肩协作，相互支持。
- **No “One Size Fits All” Solution.**
- **Expect the unexpected.**



Thank You!



Professional Security Solution Provider