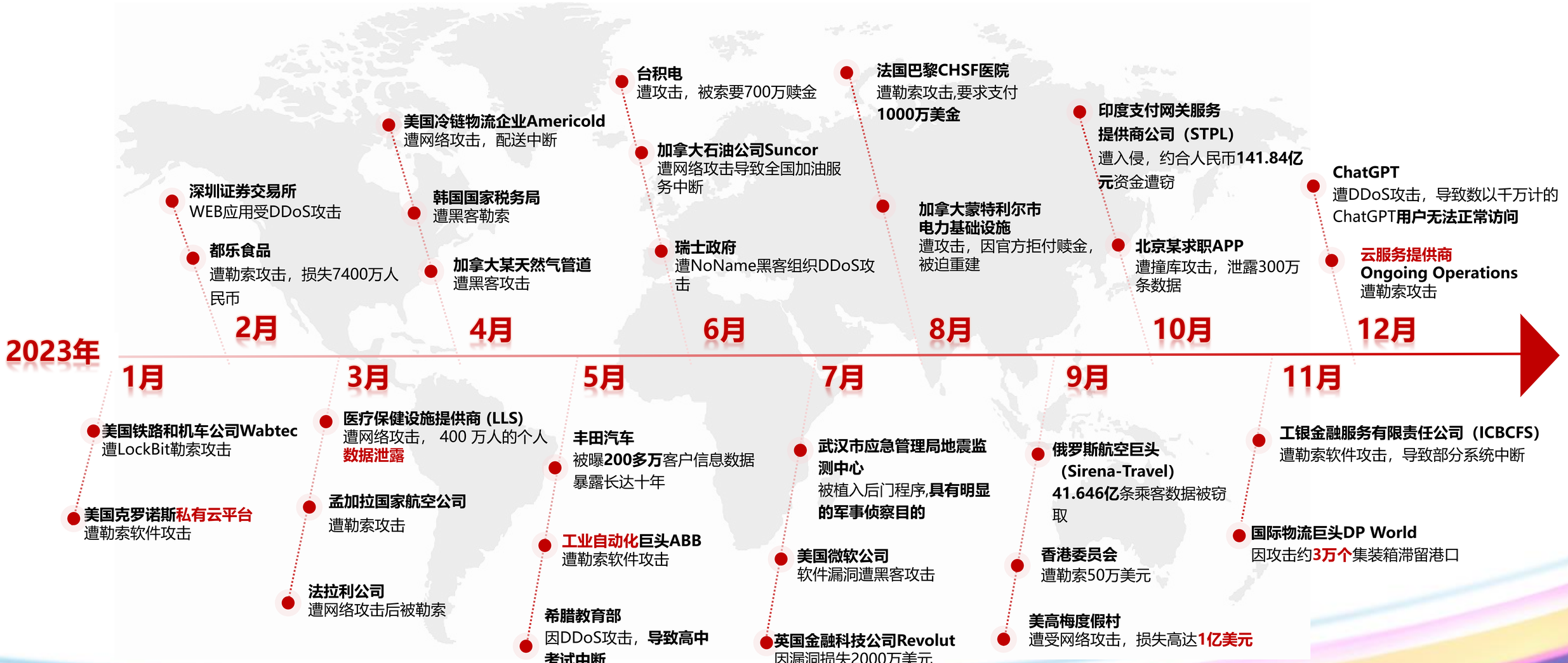
有关安全运营的几点思考

周凯

联通数科安全事业部

国内外网络安全形势日益严峻

国内外网络安全形势日益严峻，网络攻击和安全事件频发，攻击手段多样，攻击范围逐步扩大。



新技术产生新风险，技术变革催生安全新需求

云计算、大数据、物联网、工业互联网、AI等新场景新技术落地，网络和数据资产价值不断放大，网络安全运营与服务的量级和复杂度迈上新台阶，亟需网络与数据驱动、多端联动的立体防御模式。

云计算

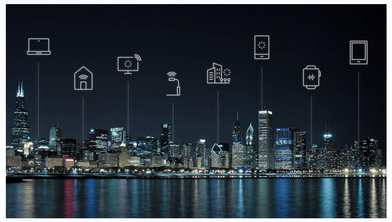
- 云计算下数据资产更加集中，遭受攻击更加频繁；
- 传统边界安全原则逐渐失效，以云化交付方式解决**云安全**问题趋于普及；

大数据

- 数据应用场景与参与角色均发生了变化，“可用不可见”是大**数据安全**新需求；
- 数据字段关联分析、零信任等架构能够有效保护数据资产；

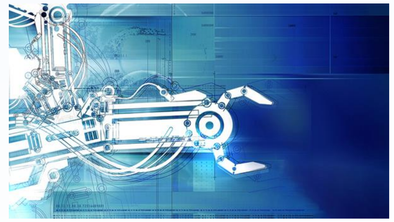
物联网

- 随着万物互联，针对平台、设备终端、移动终端等攻击日益趋多；
- 传统边界防御无法有效保障物联网安全，关联性分析技术成为应对**物联网安全**的有效方案；



工业互联网

- 网络下沉带来更多的暴露面；
- 5G+**工业互联网**催生新业务场景，**安全**性要求更高，网络安全需具备需要具备态势感知能力；



AI

- 在ChatGPT的触动下，**人工智能正在对网络安全进行重塑；**
- 提高模型的鲁棒性、增强系统的安全性以及加强用户隐私保护，将使**人工智能系统**更加**可靠可信；**

来源：内容根据腾讯安全、赛迪咨询、中金公司报告内容整理

我们所面临的安全挑战

政府与企业数字化转型速度加快，我们的工作、生活已经全面进入到数字化时代。在数字化蓬勃发展的同时，网络与数据安全等方面却面临着诸多安全挑战。

安全体系建设速度滞后

政府及企业数字化转型速度明显加快，但在基础工作、能力建设、资源投入、常态运营、攻防对抗、联防联控等方面明显滞后于数字化转型的速度。

- **国内 2023 年信息化支出 36,000 亿，网络安全产业规模 1000 亿（Gartner）；**
- **全球网络安全专业人员缺口 400 万（ISC²）；**
- **对网络安全的重视程度亟待提升，网络安全意识亟待提升；**

我们所面临的安全挑战

政府与企业数字化转型速度加快，我们的工作、生活已经全面进入到数字化时代。在数字化蓬勃发展的同时，网络与数据安全等方面却面临着诸多安全挑战。

安全体系建设速度滞后

防守理念演变速度落后

从攻击方视角看，无论攻击路径、攻击手法、攻击模式都不停地在进行演进和升级。从防守方视角看，虽然技术有迭代，但整体防守理念却相对落后。

- 2020 年 **SolarWinds** 事件刷新了我们对攻击路径、攻击手法的认知；
- 安全攻击服务化 **RaaS/DaaS** 降低攻击成本，提升攻击效率；
- 从 **业务管理、网络管理、系统管理** 等不同视角看安全；
- 针对关基系统及核心系统，从黑名单机制向 **白名单** 机制转变；

我们所面临的安全挑战

政府与企业数字化转型速度加快，我们的工作、生活已经全面进入到数字化时代。在数字化蓬勃发展的同时，网络与数据安全等方面却面临着诸多安全挑战。

安全体系建设速度滞后

防守理念演变速度落后

安全运营精细程度不够

安全运营工作缺乏对应用系统和业务系统的充分了解，包括：网络拓扑、人员账号、系统软件、安全配置、运行环境等。

- **突出重点，安全前置，追求合理的 ROI/MTTD；**
- **通过 量化指标 考核安全运营效果，如：资产纳管率、漏洞闭环率等；**
- **多 业务场景 给安全运营提出了更高要求；**

我们所面临的安全挑战

政府与企业数字化转型速度加快，我们的工作、生活已经全面进入到数字化时代。在数字化蓬勃发展的同时，网络与数据安全等方面却面临着诸多安全挑战。

安全体系建设速度滞后

防守理念演变速度落后

安全运营精细程度不够

整体联防联控功能不足

各级各类平台缺乏联动机制，缺乏资源调配，难以保证应急实效和效果，多源数据形成孤岛，难以汇聚和挖掘，安全应急支撑能力亟待打通和协同。

- 构建 **城市级** 的安全运营中心；
- 构建 **集团企业级** 的安全运营中心；

谢 谢