windows防御策略采集分类

硬化 (Harden)

- 账户密码策略
- 访问控制策略
- Windows 服务安全
- 域内组策略
- 用户账户控制
- Windows Update与补丁
- 数据安全
  - Office安全
  - bitlocker
- 证书与信任根管理

检测 (Detect)

- 系统日志审计
- 恶意软件检测
  - windows defender
- 系统审计

隔离 (Isolate)

- 网络防火墙
- 访问控制策略ACL
- 数据安全
  - bitlocker

欺骗 (Deceive)

- 网络防火墙
  - 重定向

驱逐 (Evict)

- Windows Defender
- 账户密码策略

修复(Restore)

- 域内组策略
- Windows Update与补丁
- 账户密码策略

Presented with xmind