XXXX安全运营周报

**（2021/04/25—2021/04/30）**

**目录**

[一、 本周SOC情况综述 3](#_Toc70517330)

[二、 弱口令与文件上传检查与整改情况 4](#_Toc70517334)

[三、 内外部安全预警事件响应与处置情况 4](#_Toc70517335)

[四、 提请关注或审议事项 4](#_Toc70517336)

1. 本周SOC情况综述
2. **安全运营总览**

截至4月30日,本周安全运营平台告警总数285866条，其中重要告警事件1978条，攻击总量比上周增加15%。去除重复报警和误报后，本周实际上报安全事件6起，已完成处置5起,待后续跟进1起。

1. **安全威胁态势**
   1. 互联网数据统计

本周互联网网站安全防护状态正常，检测并阻断各类Web攻击行为98888次。相关安全事件排查如下：

1）2021/4/28 12:11，来自北京的攻击源IP 36.112.185.22使用pop3协议登陆XX用户邮箱，在失败一百多次后成功登陆，疑似遭到暴力破解攻击。立即联系软开XX，回复其在北京出差，IP 36.112.185.22为其当前正在使用的4G网络地址，确认为非安全事件。

* 1. 内网数据统计

本周内网安全防护状态正常，检测到内网横向攻击行为688次，相关安全事件排查如下：

1）2021/4/25 12:11，办公测试网有终端查询恶意域名XXX.mioft.com的CDN解析地址, 疑似中了木马。通过DNS解析日志，找到发起请求的终端属于XX部XXX，已通知XX禁用该员域账号，通知本人暂不接入任何网络并立即全盘杀毒。

2）2021/4/26 13:38，XX上报源IP 10.198.255.1尝试暴力破解主机10.188.40.90的SSH服务账号密码。经排查，此源IP为堡垒机IP，属于正常操作，设备告警的规则是使用了不存在的账号，因此告警，经核实为员工误操作导致。

* 1. 专线数据统计

本周专线安全防护状态正常，检测到通过专线发起的攻击行为668次，相关安全事件排查如下：

1）4月26日XX银行测试专线（地址35.1.36.X）扫描我方58个测试IP的445端口,疑似病毒传播，已通知XX银行客户经理并在测试防火墙上临时封禁该IP，待银行反馈后再解封，此事件待跟进。

1. 弱口令与文件上传检查与整改情况
2. **弱口令问题**

1）2021/4/27 13:38，XX系统发现测试两台主机部署的XXX应用存在空口令情况，已通知XX部应用负责人XX整改。2021-4-28 10:00，经复查，已完成弱口令整改。

1. **文件上传问题**

本周无相关安全事件。

1. 内外部安全预警事件响应与处置情况

1）2021/11/20，安全团队获悉Drupal官方安全更新，修复了 Drupal 远程代码执行漏洞（CVE-2021-18888），。。。

2）

1. 提请关注或审议事项

XX银行测试专线IPX.X.X.X被我方防火墙封禁，具体原因待银行反馈。