网络安全威胁分析报告

生成时间：2025年07月09日 20:31:12
分析时间段：全量数据分析
报告状态：已完成

风险评估摘要

风险等级：高风险
风险评分：100.0/100
需要立即采取安全措施

威胁统计概览

指标	数值	描述
总威胁事件	19,843	检测到的威胁事件总数
威胁类别数	17	涉及的威胁类别种类
威胁源IP数	1194	产生威胁的源IP数量
风险评分	100.0/100	综合风险评估分数
severity_4等级威胁	15,830	severity_4等级威胁事件数量
severity_1等级威胁	2,848	severity_1等级威胁事件数量
severity_2等级威胁	661	severity_2等级威胁事件数量
severity_3等级威胁	451	severity_3等级威胁事件数量
severity_5等级威胁	53	severity_5等级威胁事件数量

1. 威胁类别分析

本次分析共发现以下威胁类别：

threat-intelligence-alarm: 15,110 起 (76.1%)
weird-behavior: 2,545 起 (12.8%)
tor-network-traffic: 647 起 (3.3%)
scan: 384 起 (1.9%)
encrypted-proxy: 303 起 (1.5%)
trojan-activity: 261 起 (1.3%)

covert-channel: 176 起 (0.9%)
malicious-encrypted-traffic: 143 起 (0.7%)
successful-recon-limited: 131 起 (0.7%)
policy-violation: 79 起 (0.4%)

2. 威胁等级分布

威胁等级统计分析:

severity_4等级威胁: 15,830 起 (79.8%)
severity_1等级威胁: 2,848 起 (14.4%)
severity_2等级威胁: 661 起 (3.3%)
severity_3等级威胁: 451 起 (2.3%)
severity_5等级威胁: 53 起 (0.3%)

3. 常见威胁类型 TOP 10

malicious-domain-dns-query: 15,001 起
remote-control-tool-identify: 2,414 起
tor-flow-identify: 647 起
4. scan: 384 起
5. vpn-flow-identify: 303 起
6. trojan-remote-control: 216 起
7. dns-tunneling: 176 起
8. encrypted-traffic-analysis-traffic: 143 起
9. successful-recon-limited: 131 起
10. penetration-tool-identify: 131 起

4. 威胁源分析

威胁源IP统计
- 涉及源IP总数: 1,194
- 平均每IP威胁数: 16.6

TOP 5 威胁源IP:
1. 172.29.31.8: 11,248 起
2. 172.16.22.227: 3,083 起
3. 210.30.97.179: 622 起
4. 172.29.22.212: 246 起
5. 172.16.66.164: 205 起

5. 客户端威胁分析

客户端威胁统计

以下是检测到威胁活动最频繁的客户端IP:

1. IP: 172.29.31.8 (共 11248 次威胁)
- [severity_4] malicious-domain-dns-query: 11204 次
- [severity_3] trojan-mining: 14 次
- [severity_4] trojan-mining: 28 次

2. IP: 172.16.22.227 (共 3083 次威胁)
- [severity_4] malicious-domain-dns-query: 3082 次
- [severity_1] scan: 1 次

3. IP: 172.29.22.212 (共 246 次威胁)
- [severity_4] tor-flow-identify: 244 次
- [severity_1] remote-control-tool-identify: 1 次
- [severity_3] tor-flow-identify: 1 次

4. IP: 172.16.66.164 (共 205 次威胁)
- [severity_4] trojan-remote-control: 205 次

5. IP: 192.168.79.87 (共 65 次威胁)
- [severity_5] penetration-tool-identify: 53 次
- [severity_1] remote-control-tool-identify: 11 次
- [severity_1] scan: 1 次

6. 服务端威胁分析

服务端威胁统计

以下是检测到威胁活动最频繁的服务端IP:

1. IP: 210.30.97.179 (共 622 次威胁)
- [severity_4] malicious-domain-dns-query: 621 次
- [severity_3] trojan-mining: 1 次

2. IP: 210.30.100.9 (共 192 次威胁)
- [severity_2] vpn-flow-identify: 14 次
- [severity_4] malicious-domain-dns-query: 84 次
- [severity_4] web-access-to-malicious-server: 42 次

3. IP: 210.30.97.173 (共 37 次威胁)
- [severity_1] remote-control-tool-identify: 7 次
- [severity_4] tor-flow-identify: 29 次
- [severity_3] tor-flow-identify: 1 次

4. IP: 210.30.97.78 (共 29 次威胁)
- [severity_2] vpn-flow-identify: 15 次
- [severity_1] vpn-flow-identify: 14 次

5. IP: 210.30.96.240 (共 21 次威胁)
- [severity_1] remote-control-tool-identify: 20 次
- [severity_2] remote-control-tool-identify: 1 次

7. 威胁时间分布

24小时威胁事件分布

威胁峰值时间: 13:00-14:00 (1957 起)

- 深夜(00:00-06:00): 6,689 起 (33.7%)
- 早晨(06:00-12:00): 8,750 起 (44.1%)
- 下午(12:00-18:00): 4,404 起 (22.2%)
- 晚间(18:00-24:00): 0 起 (0.0%)

8. 协议与端口分析

网络协议分布

1. dns: 16,684 次 (84.1%)
2. other: 1,324 次 (6.7%)
3. ssl: 1,233 次 (6.2%)
4. http: 567 次 (2.9%)
5. pop3: 28 次 (0.1%)
6. imap: 4 次 (0.0%)
7. dcerpc: 2 次 (0.0%)
8. ssh: 1 次 (0.0%)

常见目标端口

1. 端口 53 (DNS): 16,684 次

2. 端口 443 (HTTPS): 1,487 次
3. 端口 62149 (未知服务): 245 次
4. 端口 45 (未知服务): 216 次
5. 端口 80 (HTTP): 188 次
6. 端口 8081 (未知服务): 122 次
7. 端口 19000 (未知服务): 96 次
8. 端口 8443 (未知服务): 69 次
9. 端口 5995 (未知服务): 58 次
10. 端口 10012 (未知服务): 53 次

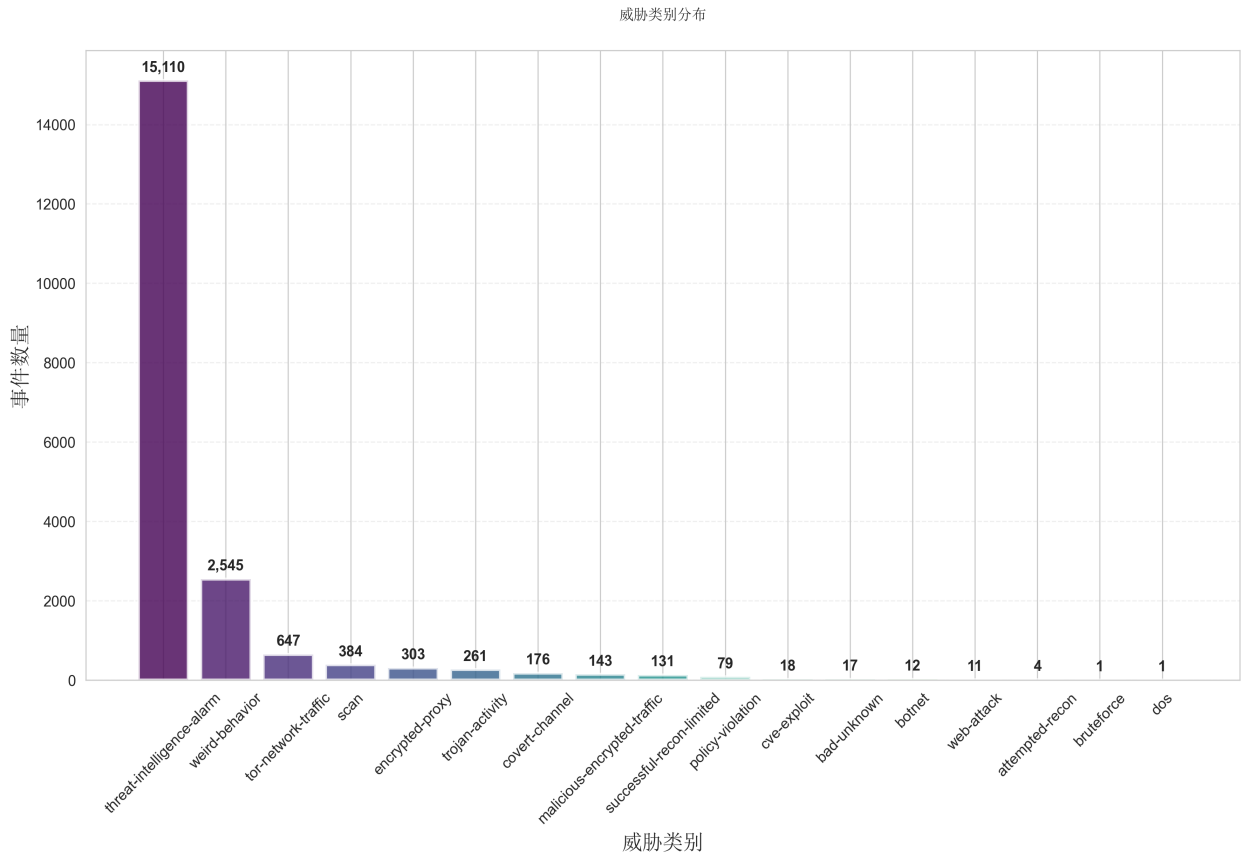
9. 安全建议

紧急建议：系统风险评分较高，建议立即进行全面安全检查
启动应急响应流程，隔离高风险IP地址
加强 13, 10, 12 时段的安全监控
威胁源IP数量较多，建议实施IP地址黑名单策略
定期更新威胁情报和安全规则
对高频威胁IP进行深度分析和追踪
建立长期威胁监控和趋势分析机制

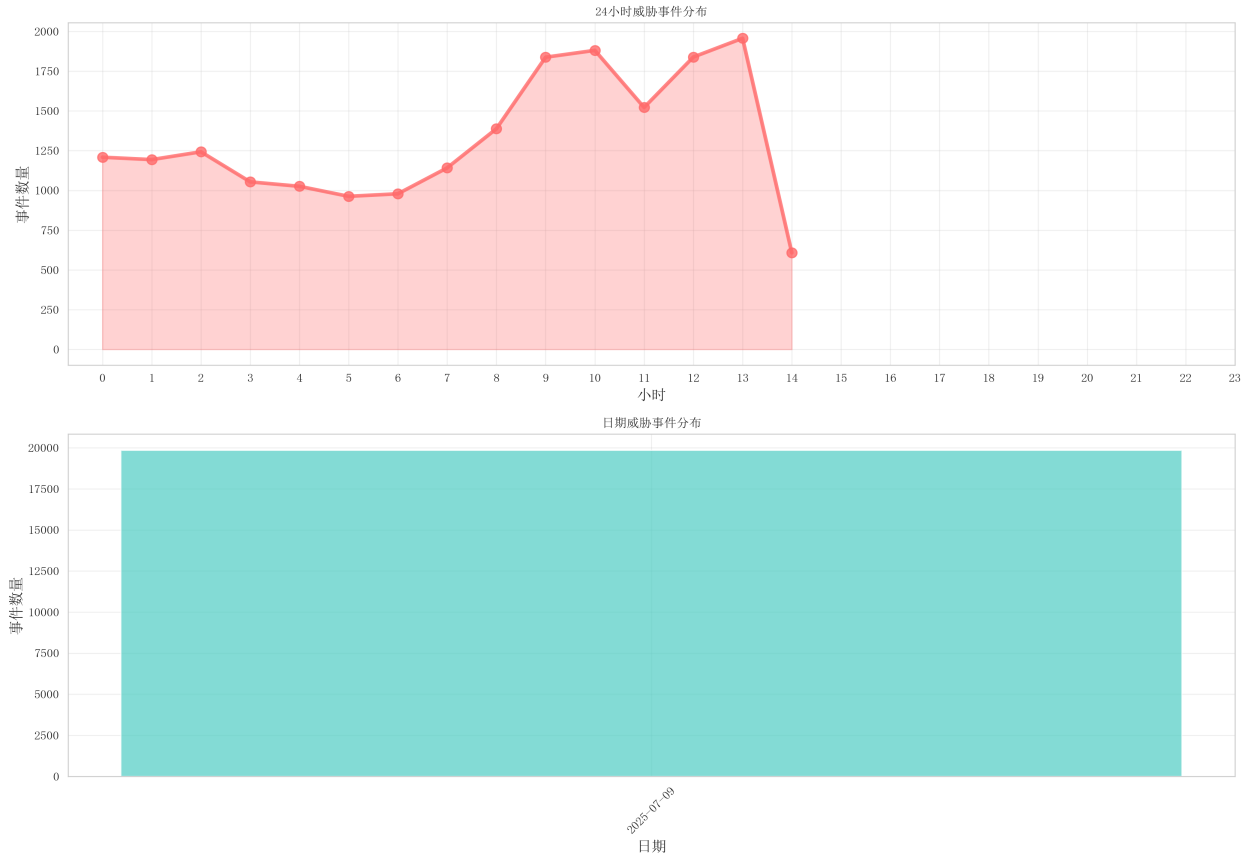
10. 数据可视化

以下图表展示了威胁数据的详细分析结果：

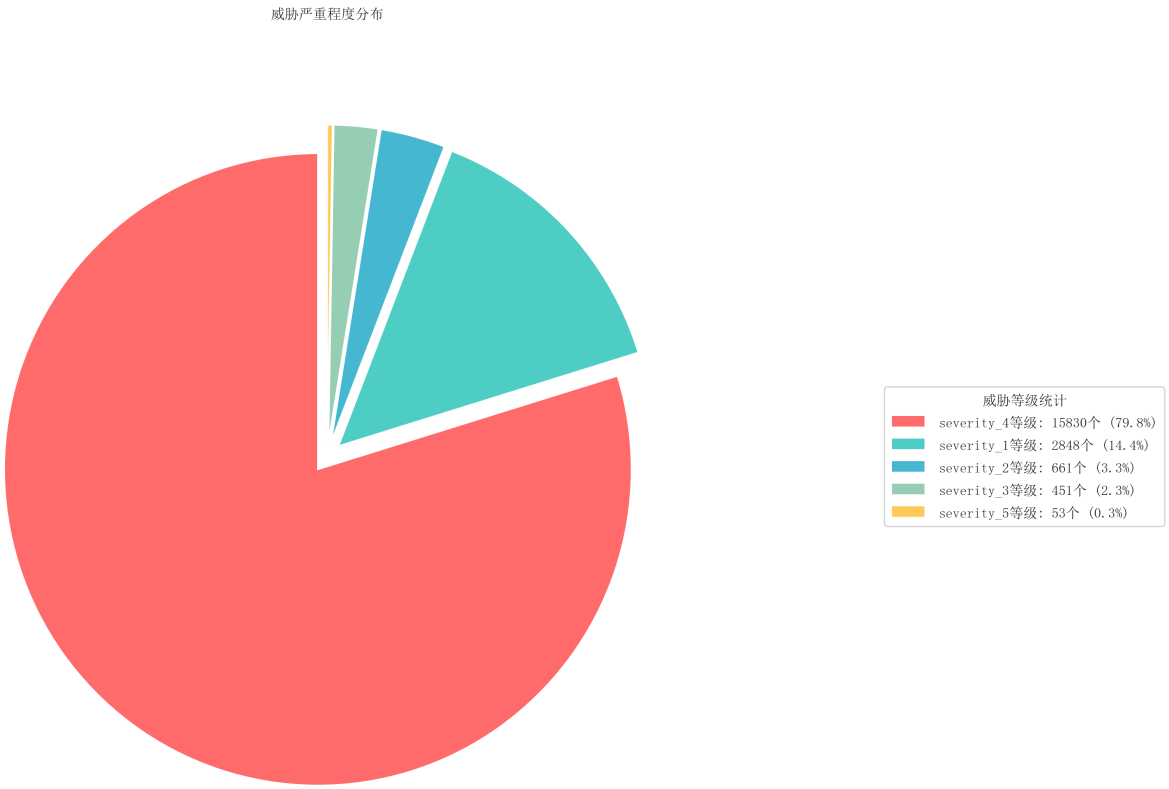
图表 1：威胁类别分布统计



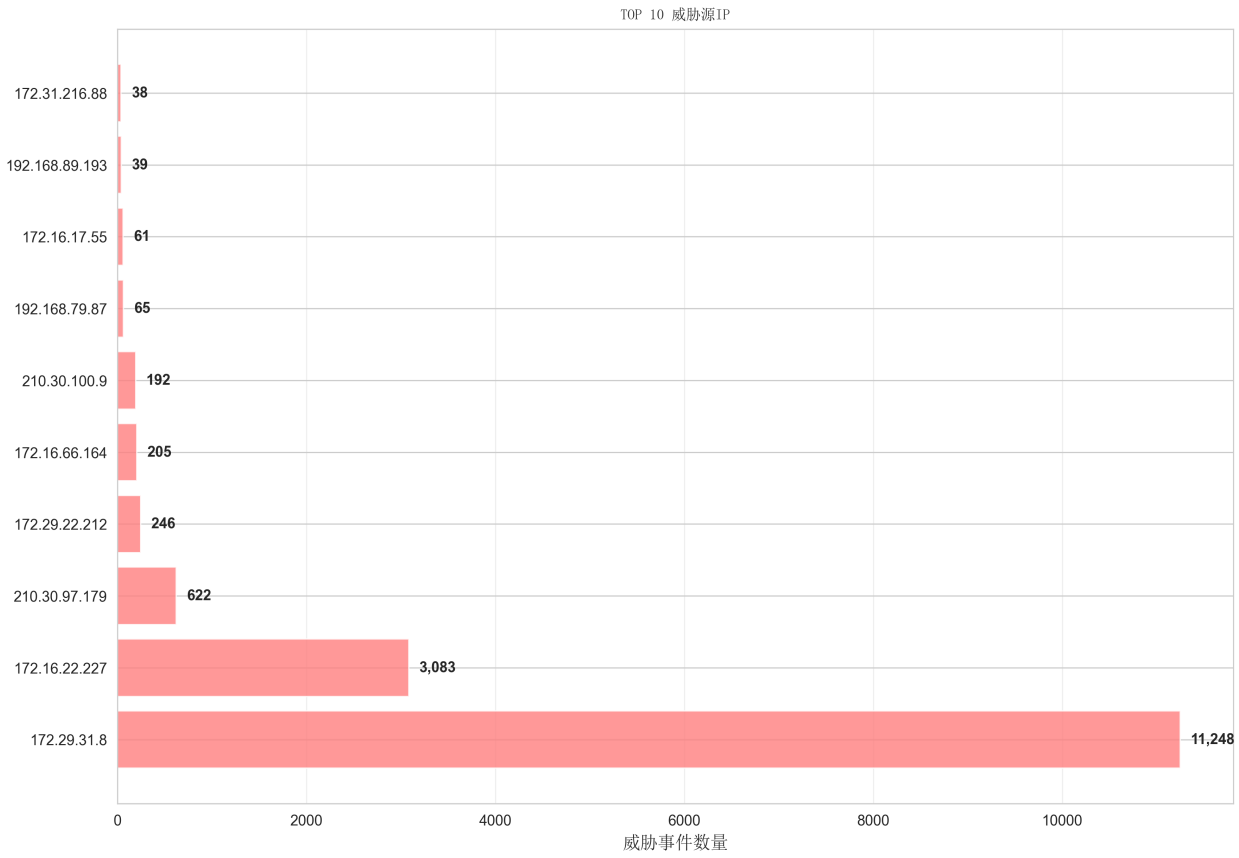
图表 2：威胁时间分布分析



图表 3：威胁严重程度分布



图表 4：TOP 10 威胁源IP分析



11. 报告总结

数据概览:

- 本次分析共处理威胁事件 19,843 起
- 涉及威胁类别 17 种
- 威胁源IP地址 1194 个
- 系统风险评分 100.0/100

关键发现:

- 最活跃的威胁类别: threat-intelligence-alarm
- 最频繁的威胁源IP: 172.29.31.8
- 威胁活动峰值时间: 13:00

后续行动:

- 持续监控高风险IP和威胁类别
- 定期更新安全策略和防护规则
- 加强团队安全意识培训
- 建立完善的威胁响应机制

--- 报告结束 ---
报告生成时间: 2025年07月09日 20:31:12