网络安全威胁分析报告

生成时间：2025年07月13日 16:52:49
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	40,536	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	1053	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	35,737	severity_4等级威胁事件数量
severity_1等级威胁	2,930	severity_1等级威胁事件数量
severity_2等级威胁	1,026	severity_2等级威胁事件数量
severity_3等级威胁	777	severity_3等级威胁事件数量
severity_5等级威胁	66	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: 32,928 起 (81.2%)
tor-network-traffic: 2,975 起 (7.3%)
weird-behavior: 2,639 起 (6.5%)
scan: 532 起 (1.3%)
covert-channel: 405 起 (1.0%)
malicious-encrypted-traffic: 358 起 (0.9%)

encrypted-proxy: 351 起 (0.9%)
successful-recon-limited: 160 起 (0.4%)
policy-violation: 74 起 (0.2%)
trojan-activity: 66 起 (0.2%)

2. 威胁等级分布

威胁等级统计分析:

severity_4等级威胁: 35,737 起 (88.2%)
severity_1等级威胁: 2,930 起 (7.2%)
severity_2等级威胁: 1,026 起 (2.5%)
severity_3等级威胁: 777 起 (1.9%)
severity_5等级威胁: 66 起 (0.2%)

3. 常见威胁类型 TOP 10

malicious-domain-dns-query: 32,772 起
tor-flow-identify: 2,975 起
remote-control-tool-identify: 2,550 起
4. scan: 532 起
5. dns-tunneling: 404 起
6. encrypted-traffic-analysis-traffic: 358 起
7. vpn-flow-identify: 351 起
8. successful-recon-limited: 160 起
9. outbound2malicious-server: 102 起
10. penetration-tool-identify: 89 起

4. 威胁源分析

威胁源IP统计
- 涉及源IP总数: 1,053
- 平均每IP威胁数: 38.5

TOP 5 威胁源IP:
1. 172.29.29.197: 32,585 起
2. 192.168.89.21: 2,206 起
3. 210.30.100.9: 251 起
4. 172.29.22.212: 234 起
5. 172.16.20.145: 147 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: 172.29.29.197 (共 32585 次威胁)
- [severity_4] malicious-domain-dns-query: 32536 次
- [severity_4] trojan-mining: 32 次
- [severity_3] trojan-mining: 16 次

2. IP: 192.168.89.21 (共 2206 次威胁)
- [severity_4] tor-flow-identify: 2187 次
- [severity_4] outbound2malicious-server: 16 次
- [severity_3] tor-flow-identify: 2 次

3. IP: 172.29.22.212 (共 234 次威胁)
- [severity_3] tor-flow-identify: 2 次
- [severity_4] tor-flow-identify: 232 次

4. IP: 172.16.20.145 (共 147 次威胁)
- [severity_3] tor-flow-identify: 1 次
- [severity_3] encrypted-traffic-analysis-traffic: 128 次
- [severity_4] outbound2malicious-server: 6 次

5. IP: 172.16.120.135 (共 106 次威胁)
- [severity_4] tor-flow-identify: 100 次
- [severity_3] tor-flow-identify: 1 次
- [severity_4] outbound2malicious-server: 3 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: 210.30.100.9 (共 251 次威胁)
- [severity_2] vpn-flow-identify: 27 次
- [severity_1] scan: 42 次
- [severity_4] tor-flow-identify: 4 次

2. IP: 210.30.97.179 (共 129 次威胁)

- [severity_4] malicious-domain-dns-query: 128 次
- [severity_3] trojan-mining: 1 次

3. IP: 210.30.97.173 (共 81 次威胁)
- [severity_3] tor-flow-identify: 2 次
- [severity_4] tor-flow-identify: 78 次
- [severity_2] remote-control-tool-identify: 1 次

4. IP: 210.30.97.78 (共 33 次威胁)
- [severity_1] vpn-flow-identify: 4 次
- [severity_2] vpn-flow-identify: 29 次

5. IP: 210.30.96.240 (共 24 次威胁)
- [severity_1] remote-control-tool-identify: 21 次
- [severity_2] remote-control-tool-identify: 3 次

7. 威胁时间分布

24小时威胁事件分布

威胁峰值时间: 14:00-15:00 (2844 起)

- 深夜(00:00-06:00): 14,145 起 (34.9%)
- 早晨(06:00-12:00): 13,945 起 (34.4%)
- 下午(12:00-18:00): 12,446 起 (30.7%)
- 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: 34,880 次 (86.0%)
2. other: 3,690 次 (9.1%)
3. ssl: 1,211 次 (3.0%)
4. http: 698 次 (1.7%)
5. pop3: 33 次 (0.1%)
6. dcerpc: 17 次 (0.0%)
7. imap: 4 次 (0.0%)
8. ssh: 3 次 (0.0%)

常见目标端口

1. 端口 53 (DNS): 34,880 次
2. 端口 6969 (未知服务): 2,179 次
3. 端口 443 (HTTPS): 1,484 次
4. 端口 19000 (未知服务): 298 次
5. 端口 80 (HTTP): 235 次
6. 端口 62149 (未知服务): 234 次
7. 端口 10012 (未知服务): 94 次
8. 端口 5938 (未知服务): 90 次
9. 端口 8081 (未知服务): 87 次
10. 端口 8443 (未知服务): 80 次

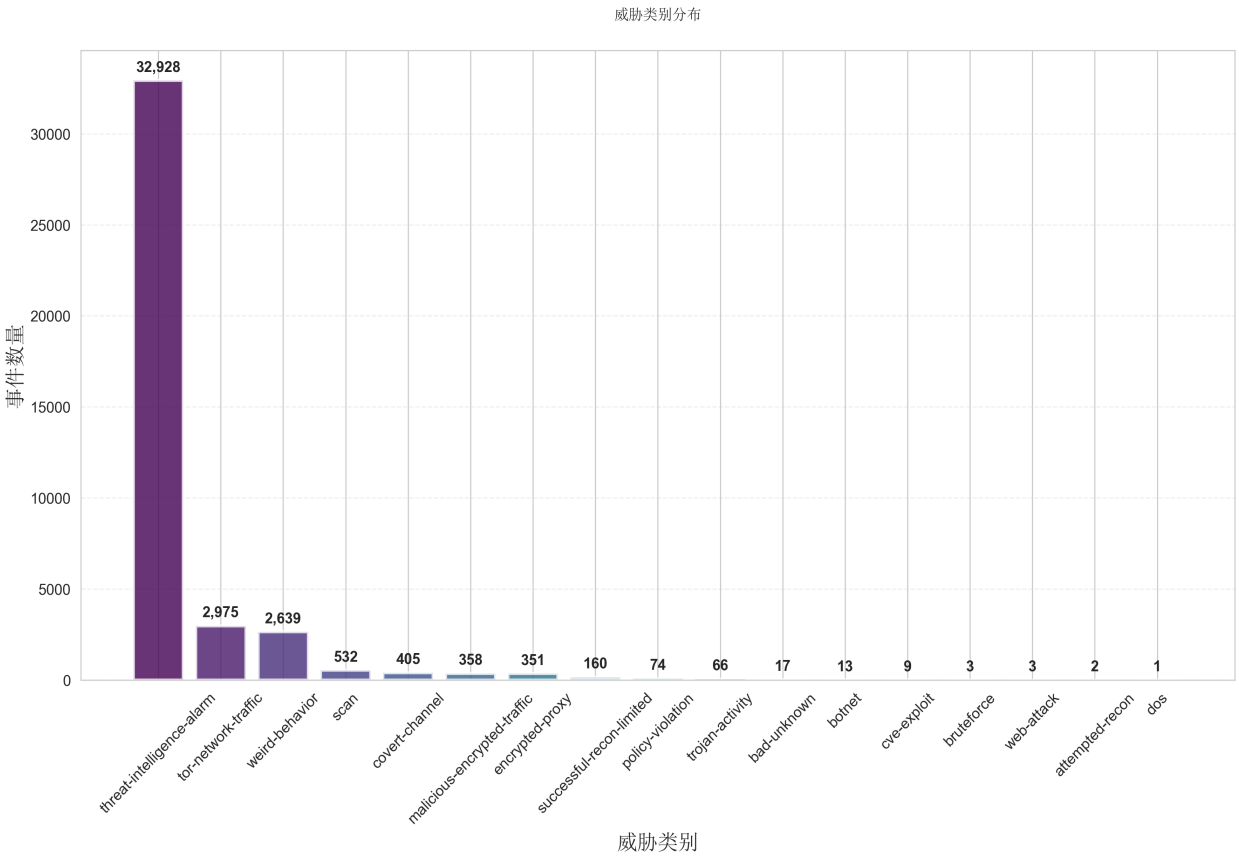
9. 安全建议

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 14, 0, 13 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

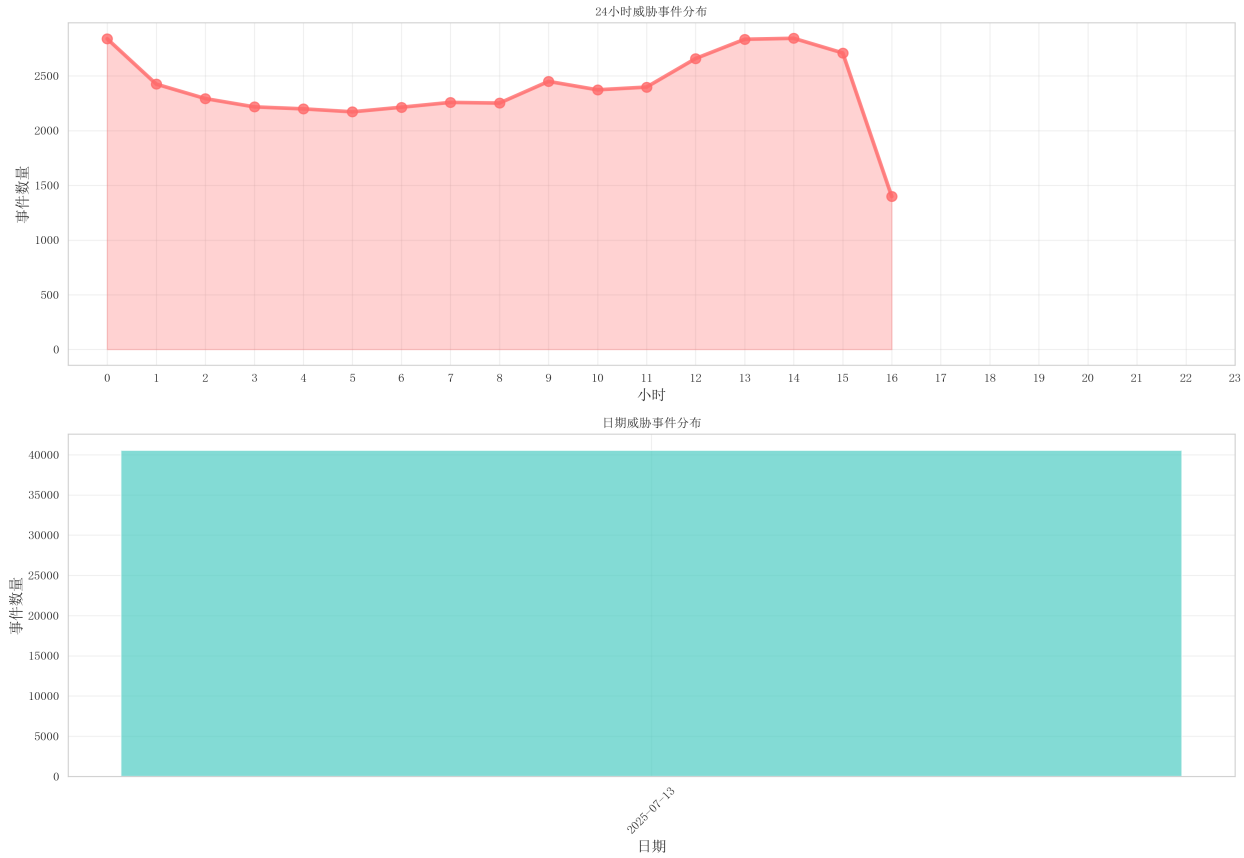
10. 数据可视化

以下图表展示了威胁数据的详细分析结果：

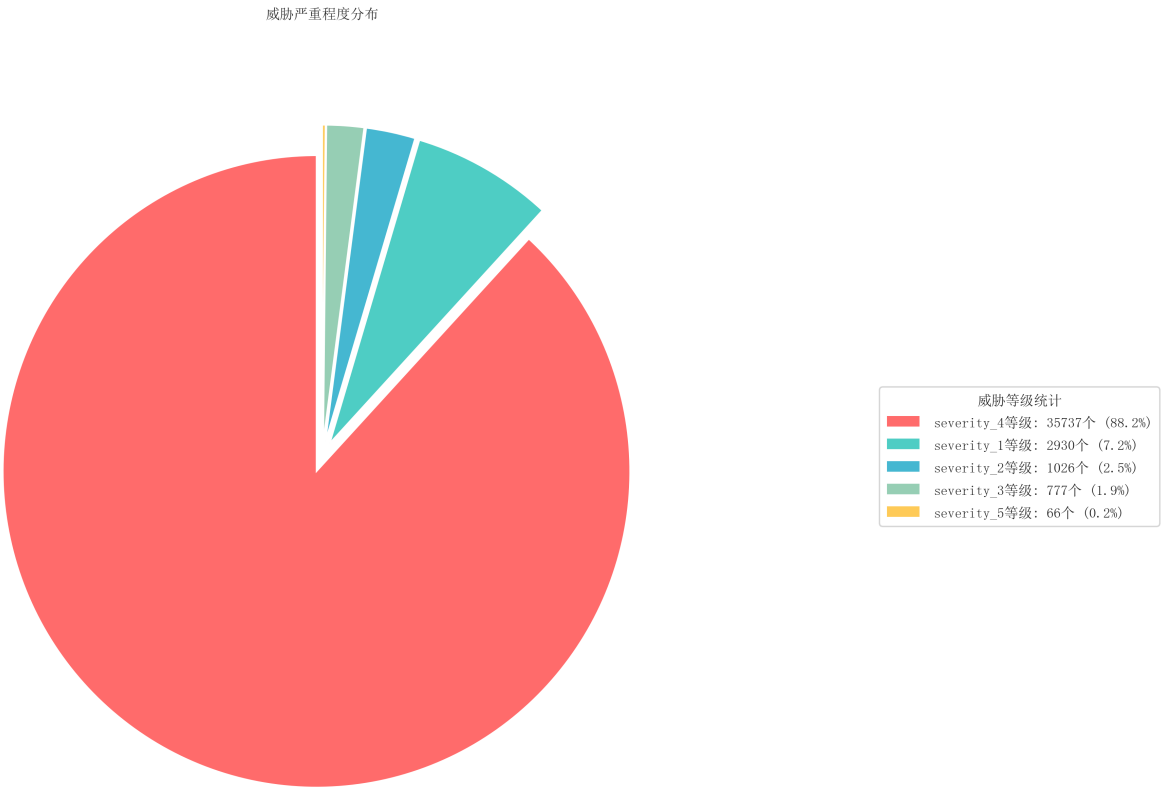
图表 1：威胁类别分布统计



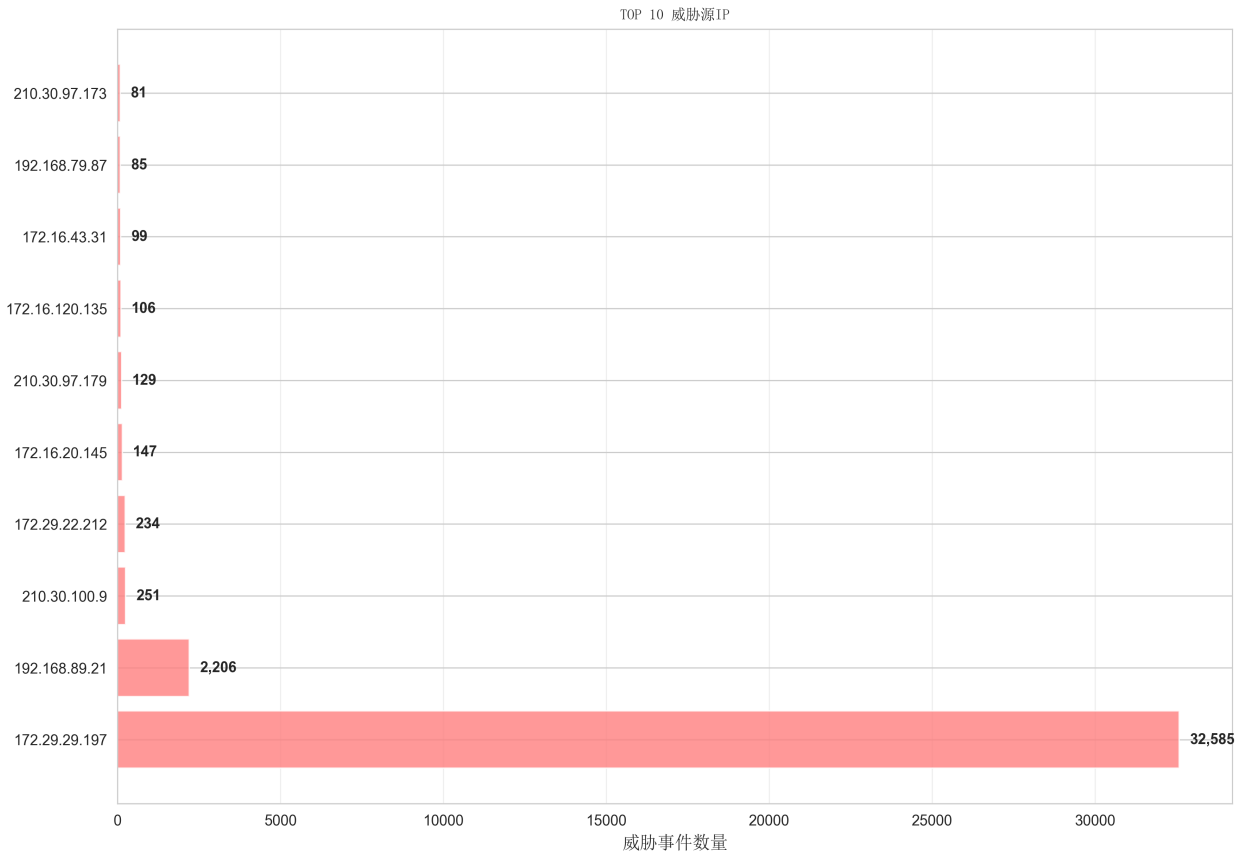
图表 2：威胁时间分布分析



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 40,536 起
- 涉及威胁类别 17 种
- 威胁源IP地址 1053 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: 172.29.29.197
- 威胁活动峰值时间: 14:00

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13日 16:52:49