NOVA南凌

2023-05-29至2023-06-04即时报表

目录

CONTENTS

NOVA 南凌 | 300921
股票代码

01
整体概述

安全概述

风险等级

无风险

系统整体风险值 3 分，风险等级 无风险，较上个周期 上升

安全事件数量

396

共检测到 396 起安全事件，其中紧急事件 38 起，严重事件 350 起，
较上个周期总量（上升395起），
紧急事件（上升38起），
严重事件（上升349起）。

合并告警数量

246775

共检测到 246775次合并告警，其中紧急告警 14 次，严重告警 6039 次，
较上个周期总量（上升246775次），
紧急告警（上升14次），
严重告警（上升6039次）。

运营总览

资产

主机	670	服务	0	网站	0	域名	0
变更	上升 668	变更	持平	变更	持平	变更	持平

脆弱性

2023-05-29-2023-06-04内
更新0个脆弱性，修复0个脆弱性

截止到2023-06-04
还存在 0 个未修复脆弱性

脆弱性级别

此部分暂无数据

安全事件处置

2023-05-29-2023-06-04内
共处置0 个安全事件，其中：
0 个未读
0 个攻击成功
0 个攻击失败
0 个误报 0 个未知

合并告警处置

2023-05-29-2023-06-04内
共处置0 个合并告警，其中：
0 个攻击成功
0 个攻击失败
0 个误报
0 个未知

运行概述

运行状态

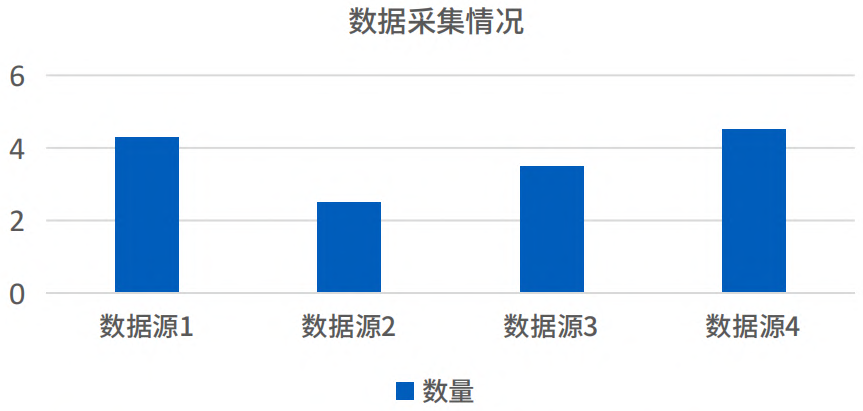
[无计算结果]-[无计算结果]内系统运作状态[无计算结果]

时间	系统异常告警

数据采集

当前启动的数据源共[无计算结果]个

共接收日志[无计算结果]条。



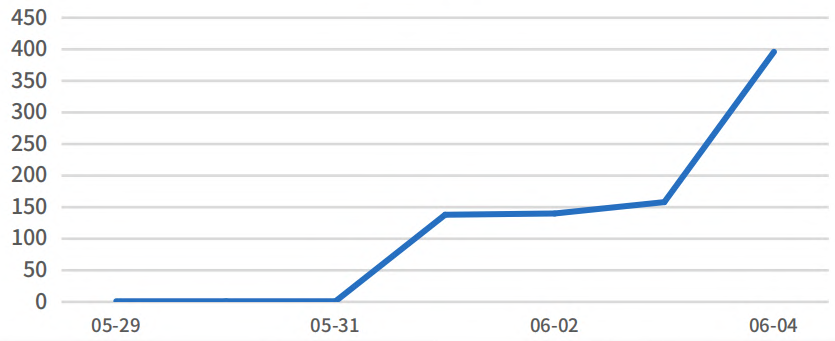
NOVA 南凌 | 300921
股票代码

02
安全态势

威胁态势

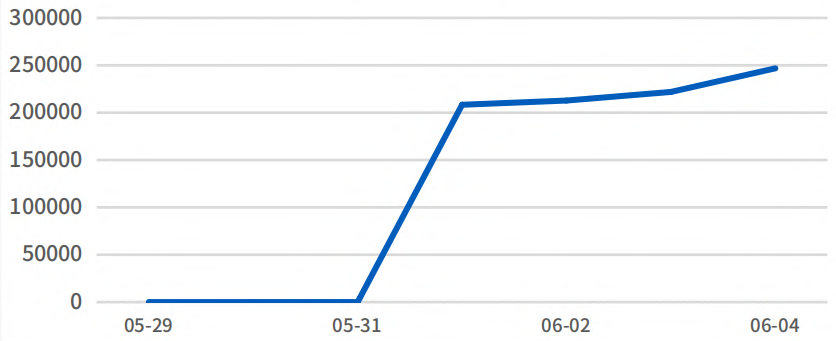
共检测到 396 起安全事件

安全事件趋势

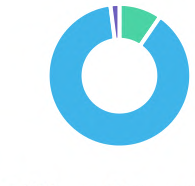


共检测到 246775 次合并告警

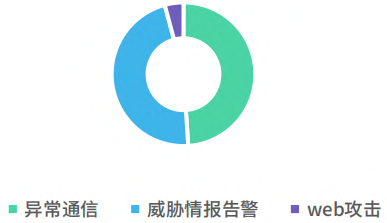
合并告警趋势



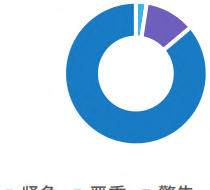
安全事件级别分布



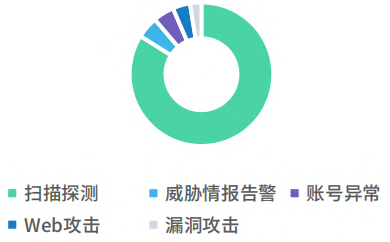
安全事件类型TOP5



合并告警级别分布



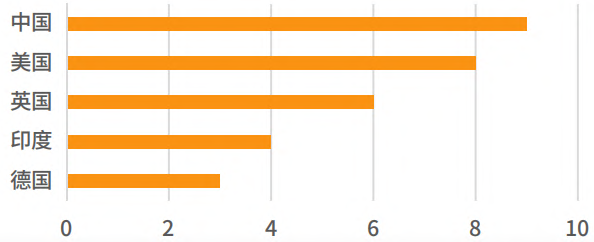
合并告警类型TOP5



攻击者态势

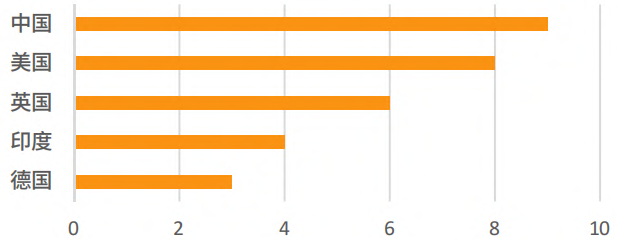
境外攻击者总量 5

攻击源国家TOP5



国内攻击者总量 136

攻击源省份TOP5



在 2023-05-29到 2023-06-04 内，共发现攻击源 184 个
其中 39 个攻击源为首次发现，
0 个攻击源已持续攻击至少 两天。

高频攻击源TOP10

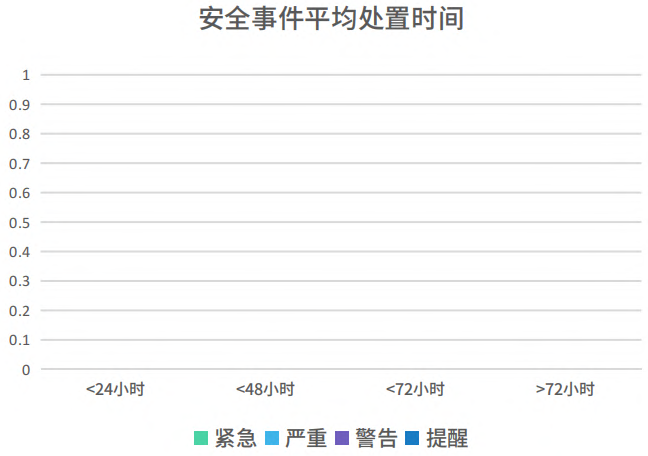
攻击源	地理位置	威胁级别	攻击总量
223.5.5.5	["中国"]	无风险	1282
8.8.8.8	["美国"]	无风险	1005
47.91.46.193			

处置态势

安全事件处置率

0.0%

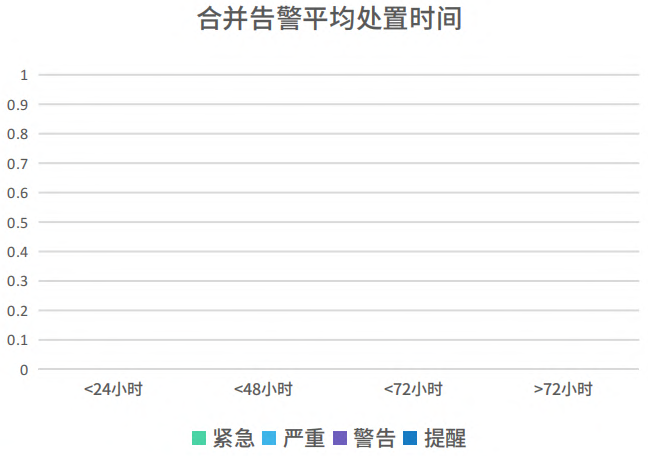
安全事件平均处置时间



合并告警处置率

0.0%

合并告警平均处置时间



运营态势

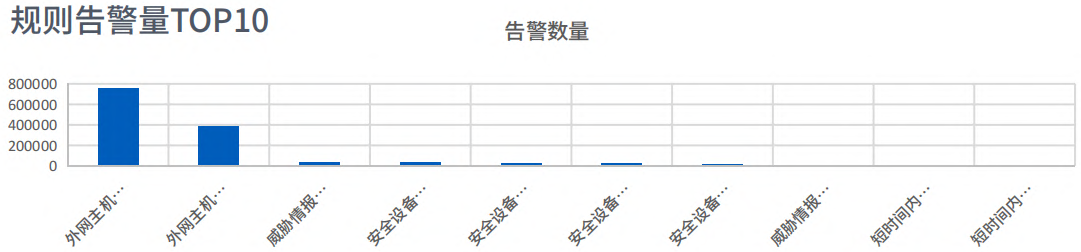
日志采集

目前共有 29 个数据源，
其中停用 20 个

规则运营

目前共有 839 条规则，
其中更新 0 条，
停用 62 条。

目前 28 条规则被触发，
811 条规则未被触发。



NOVA 南凌 | 300921
股票代码

03
重点事件分析

[场景模型]安全设备检测到勒索软件攻击

攻击者

10.25.33.99

10.25.3.33

攻击阶段：利用、安装、攻击

攻击分类：异常通信

研判结果：未知

攻击时间：2023-05-31 17:38:38

受害者

8.8.8.8

114.114.114.114

223.5.5.5

合并告警时间线

2023-05-31 18:25:35

首次捕获该事件

8.8.8.8 主机发生该事件

2023-05-31 20:37:43

8.8.8.8 主机发生该事件

[场景模型]安全设备检测到勒索软件攻击

攻击者

10.25.33.99

10.25.3.33

攻击阶段：利用、安装、攻击

攻击分类：异常通信

研判结果：未知

攻击时间：2023-05-31 18:09:35

受害者

8.8.8.8

114.114.114.114

223.5.5.5

合并告警时间线

2023-05-31 18:25:35

首次捕获该事件

8.8.8.8 主机发生该事件

2023-05-31 20:37:43

8.8.8.8 主机发生该事件

[场景模型]安全设备检测到勒索软件攻击

攻击者

10.25.33.99

10.25.3.33

攻击阶段：利用、安装、攻击

攻击分类：异常通信

研判结果：未知

攻击时间：2023-05-31 18:25:35

受害者

8.8.8.8

114.114.114.114

223.5.5.5

合并告警时间线

2023-05-31 18:25:35

首次捕获该事件

8.8.8.8 主机发生该事件

2023-05-31 20:37:43

8.8.8.8 主机发生该事件

[场景模型]安全设备检测到勒索软件攻击

攻击者

10.25.33.99

47.91.46.193

攻击阶段：利用、安装、攻击

攻击分类：异常通信

研判结果：未知

攻击时间：2023-06-04 09:19:12

受害者

8.8.8.8

116.214.132.2

116.214.132.1

合并告警时间线

2023-06-04 09:19:12

首次捕获该事件

8.8.8.8 主机发生该事件

2023-06-05 09:08:42

8.8.8.8 主机发生该事件

[场景模型]安全设备检测到勒索软件攻击

攻击者

10.25.33.99

47.91.46.193

攻击阶段：利用、安装、攻击

攻击分类：异常通信

研判结果：未知

攻击时间：2023-06-04 09:19:12

受害者

8.8.8.8

116.214.132.2

116.214.132.1

合并告警时间线

2023-06-04 09:19:12

首次捕获该事件

8.8.8.8 主机发生该事件

2023-06-05 09:08:42

8.8.8.8 主机发生该事件

[场景模型]安全设备检测到勒索软件攻击

攻击者

10.25.33.99

47.91.46.193

攻击阶段：利用、安装、攻击

攻击分类：异常通信

研判结果：未知

攻击时间：2023-06-04 08:57:21

受害者

8.8.8.8

116.214.132.2

116.214.132.1

合并告警时间线

2023-06-04 09:19:12

首次捕获该事件

8.8.8.8 主机发生该事件

2023-06-05 09:08:42

8.8.8.8 主机发生该事件

[场景模型]安全设备检测到勒索软件攻击

攻击者

10.25.33.99

47.91.46.193

攻击阶段：利用、安装、攻击

攻击分类：异常通信

研判结果：未知

攻击时间：2023-06-04 09:19:12

受害者

8.8.8.8

116.214.132.2

116.214.132.1

合并告警时间线

2023-06-04 09:19:12

首次捕获该事件

8.8.8.8 主机发生该事件

2023-06-05 09:08:42

8.8.8.8 主机发生该事件

NOVA 南凌 | 300921
股票代码

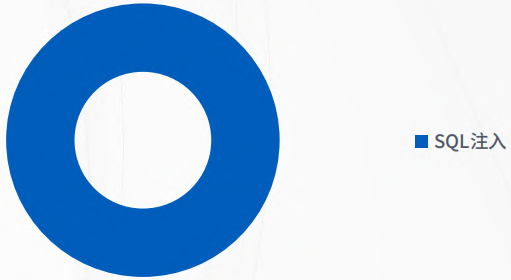
04
热点安全场景分析

通用Web攻击

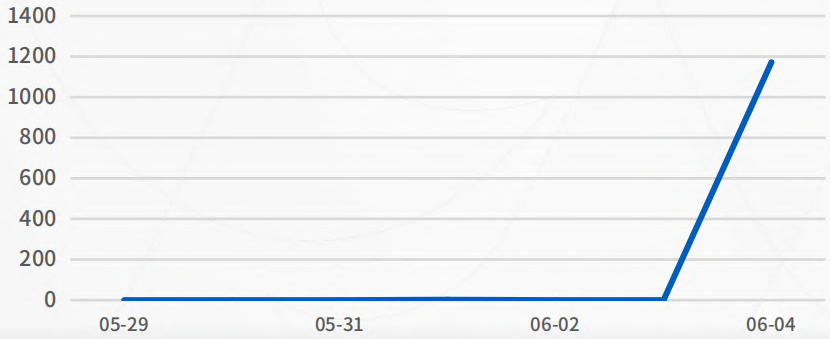
- 累计捕获通用Web攻击**1174**次，涉及**48**个主机，**1**个资产组
- **210.75.24.205、116.214.32.165、202.170.136.235** 等主机连续多次、多天发现被通用Web攻击行为攻击，疑似已经失陷
- Web攻击趋势整体呈**上升**趋势，及时排除风险

受害资产数	影响资产组	攻击源数
48 个	1个	7个

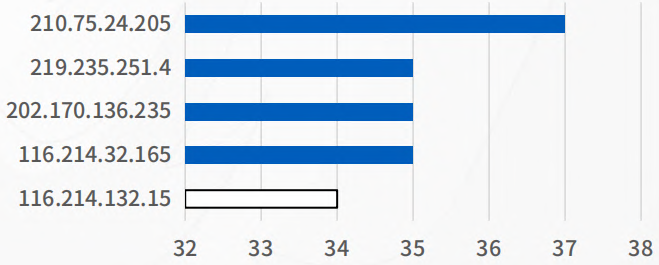
攻击类型分布



Web攻击趋势



受害Web服务TOP5



威胁情报

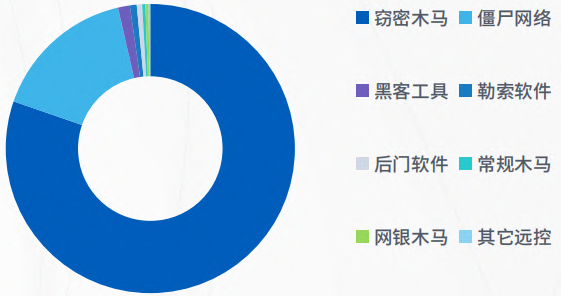
- 累计命中威胁情报11768次，涉及0个主机，0个资产组
- 威胁情报命中趋势整体呈上升趋势，及时排除风险

受害资产数
0 个

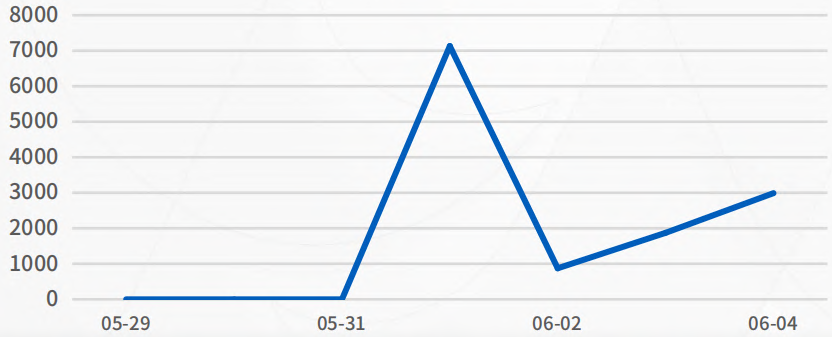
影响资产组
0个

命中情报总数
56个

命中情报类型分布



威胁情报命中趋势



命中IOC信息	情报标签
176.113.115.16	blacklisthit$xmon$report、squirtdanger
194.195.211.98	blacklisthit$xmon$report、threat$family$moobot
179.43.182.61	ddos mirai、threat$family$fbot
43.142.160.140	漏洞利用

NOVA 南凌 | 300921
股票代码

谢谢观看

南凌科技股份有限公司
服务热线：400-700-6699