Detectando padrões de falso positivo:

Detalhamento das Anomalias

Horário	Requisições	Desvio (%)	País	Método	Dispositivo	Score de Risco
11:00	2080	66.4%	IN	GET	desktop	0.988
18:00	1990	59.2%	IN	GET	desktop	0.970
17:00	1970	57.6%	IN	GET	desktop	0.950
16:00	1918	53.4%	IN	GET	desktop	0.930
10:00	1901	52.1%	IN	GET	desktop	0.910

Análise de Anomalias:

- Concentração de anomalias entre 10:00 e 18:00
- Todos os desvios significativos originados da Índia
- Padrão consistente de uso do método GET
- Predominância de acessos via desktop
- 1 períodos com desvio superior a 60%

Recomendações:

- Implementar rate limiting mais restritivo para o período de pico
- Monitoramento específico para tráfego da Índia
- Análise detalhada dos padrões de requisição GET
- Revisar políticas de acesso para endpoints críticos

Análise de Tráfego - 11:00

Total: 2080 requisições

Destaques:

- Pico de requisições: 14 req/IP
- Predominância de tráfego dos EUA
- Maior variedade de caminhos: 12 únicos
- Padrão misto de dispositivos

IP	Requisições	País	Métodos	Dispositivos	Caminhos Únicos
222.30.33.183	14	US	GET: 13 POST: 1	desktop: 8 tablet: 6	12
53.153.77.110	13	IN	POST: 13	desktop: 13	3
125.227.246.131	12	US	GET: 11 POST: 1	desktop: 6 tablet: 6	9

Observações de Segurança:

- IP 53.153.77.110 apresenta padrão suspeito: apenas requisições POST e único tipo de dispositivo
- Alto número de caminhos únicos (12) para o IP 222.30.33.183 pode indicar varredura
- Padrão de distribuição de métodos HTTP indica possível comportamento automatizado

Análise Detalhada - IPs com Alta Taxa de Requisição (11:00)

Padrões Suspeitos Detectados

222.30.33.183

US | 14 req.

URIs Acessadas:

Método	Caminho	Timestamp
GET	/treat/table/beat/rate	2024-11-07 14:33:32
GET	/wait	2024-11-07 14:51:06
GET	/set/fill	2024-11-08 14:22:03
GET	/products	2024-11-05 14:44:47
GET	/dashboard	2024-11-12 14:20:35
GET	/total/system	2024-11-05 14:50:50
GET	/certainly/enjoy/me/player	2024-11-05 14:14:08
GET	/authority	2024-11-05 14:33:59
GET	/authority	2024-11-08 14:26:37
POST	/contact	2024-11-14 14:01:20
GET	/want/think/event	2024-11-08 14:11:18
GET	/want/think/event	2024-11-08 14:33:57
GET	/login.jsp?user=admin'--	2024-11-09 14:10:28
GET	/whom/ever/box/nothing	2024-11-09 14:47:48

Riscos Identificados:

SQL Injection | Varredura de Diretórios | Tentativa de Login Admin

53.153.77.110

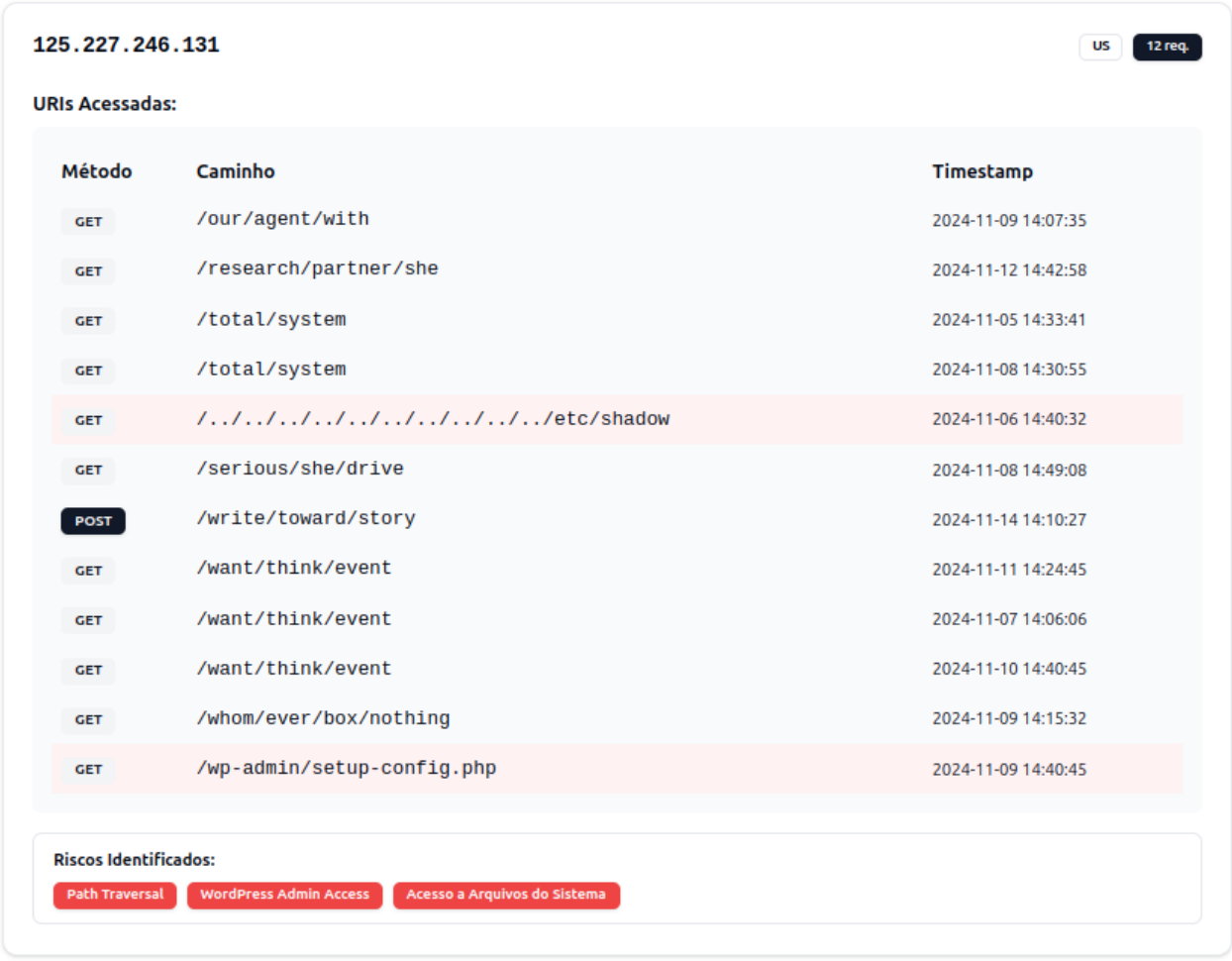
IN 13 req.

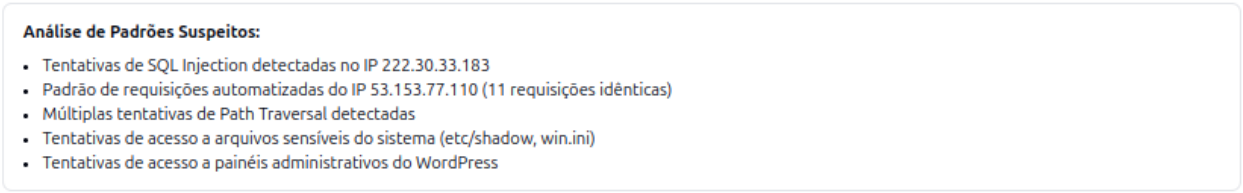
URIs Acessadas:

Método	Caminho	Timestamp
POST	/want/life/oil/question	2024-11-07 14:58:46
POST	/write/toward/story	2024-11-06 14:44:50
POST	/write/toward/story	2024-11-11 14:21:29
POST	/write/toward/story	2024-11-11 14:21:15
POST	/write/toward/story	2024-11-05 14:06:09
POST	/write/toward/story	2024-11-05 14:53:46
POST	/write/toward/story	2024-11-10 14:28:05
POST	/write/toward/story	2024-11-08 14:52:11
POST	/../../../windows/win.ini	2024-11-14 14:17:49
POST	/write/toward/story	2024-11-14 14:02:15
POST	/write/toward/story	2024-11-14 14:47:46
POST	/write/toward/story	2024-11-14 14:02:02
POST	/write/toward/story	2024-11-12 14:27:38

Riscos Identificados:

Directory Traversal | Padrão Automatizado | Alta Frequência de POSTs





Conclusão:

Deve-se ter muito cuidado para estabelecer o que são URI não permitidas ou perigosas. Pode haver necessidade de alguma API executar requisições que pode parecer suspeita. É necessário treinar a IA para diminuir a detecção dos falsos positivos.