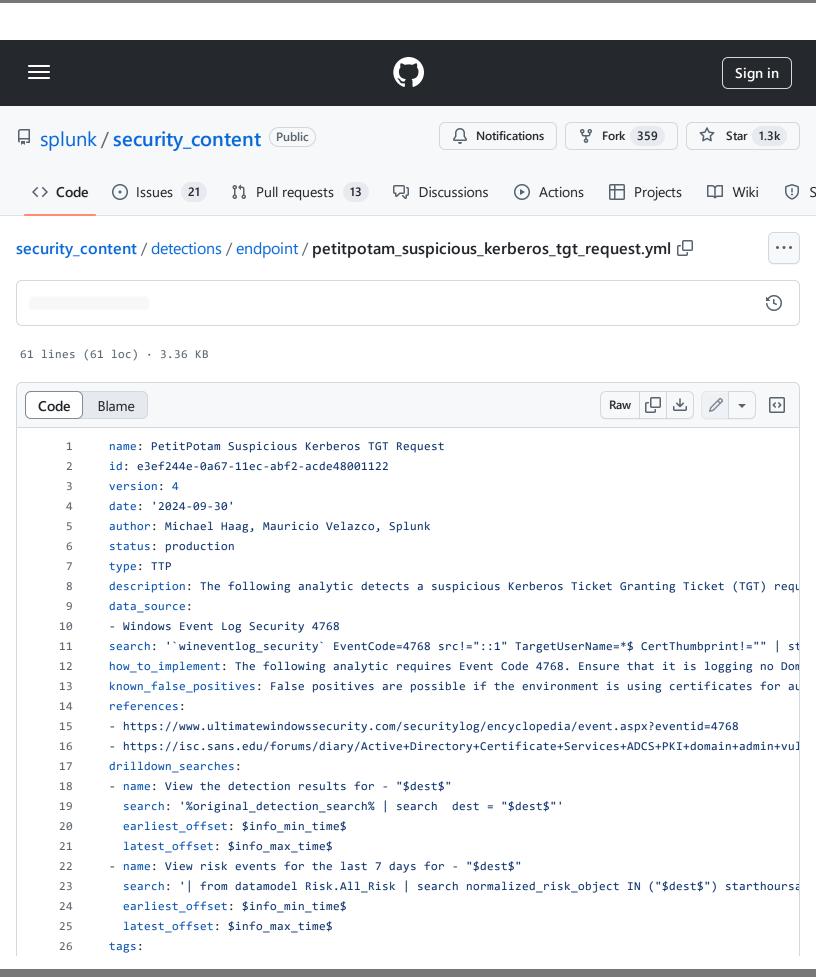
security_content/detections/endpoint/petitpotam_suspicious_kerberos_tgt_request.yml at develop splunk/security_content · GitHub - 31/10/2024 15:51

https://github.com/splunk/security content/blob/develop/detections/endpoint/petitpotam suspicious kerberos tgt request.yml



security_content/detections/endpoint/petitpotam_suspicious_kerberos_tgt_request.yml at develop · splunk/security_content · GitHub - 31/10/2024 15:51

https://github.com/splunk/security content/blob/develop/detections/endpoint/petitpotam suspicious kerberos tgt request.yml

```
27
         analytic_story:
28
         - PetitPotam NTLM Relay on Active Directory Certificate Services
         - Active Directory Kerberos Attacks
29
         asset_type: Endpoint
30
31
         confidence: 70
32
         cve:
         - CVE-2021-36942
33
34
         impact: 80
         message: A Kerberos TGT was requested in a non-standard manner against $dest$, potentially relate
35
         mitre_attack_id:
36
         - T1003
37
         observable:
38
39
         - name: dest
40
           type: Hostname
41
           role:
           - Victim
42
43
         product:
         - Splunk Enterprise
44
         - Splunk Enterprise Security
45
         - Splunk Cloud
46
         required_fields:
47
         - _time
48
         - dest
49
50
         - Account_Name
51
         - Client_Address
         - action
52
53
         - Message
54
         risk_score: 56
         security_domain: endpoint
55
       tests:
56
       - name: True Positive Test
57
         attack_data:
58
         - data: https://media.githubusercontent.com/media/splunk/attack_data/master/datasets/attack_techr
59
           source: XmlWinEventLog:Security
60
           sourcetype: XmlWinEventLog
61
```