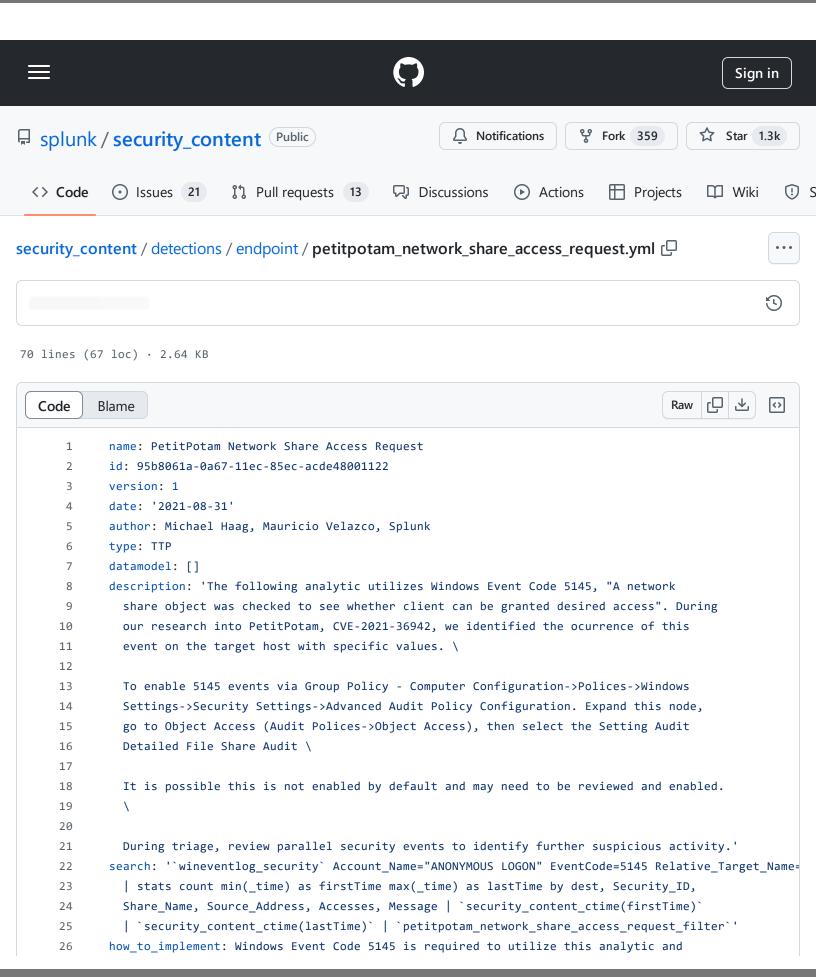
security\_content/detections/endpoint/petitpotam\_network\_share\_access\_request.yml at 0dd6de32de2118b2818550df9e65255f4109a56d · splunk/security\_content · GitHub - 31/10/2024 15:51 https://github.com/splunk/security\_content/blob/0dd6de32de2118b2818550df9e65255f4109a56d/detections/endpoint/petitpotal



https://github.com/splunk/security\_content/blob/0dd6de32de2118b2818550df9e65255f4109a56d/detections/endpoint/petitpotal

```
27
         it may not be enabled in most environments.
28
       known_false_positives: False positives have been limited when the Anonymous Logon
29
         is used for Account Name.
       references:
30
       - https://attack.mitre.org/techniques/T1187/
32
       - https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=5145
       - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5145
33
34
       tags:
         analytic_story:
35
36
         - PetitPotam NTLM Relay on Active Directory Certificate Services
37
         dataset:
         - https://media.githubusercontent.com/media/splunk/attack_data/master/datasets/attack_techniques/
38
39
         kill_chain_phases:
         - Exploitation
40
41
         - Lateral Movement
         mitre_attack_id:
42
43
         - T1187
44
         product:
         - Splunk Enterprise
45
         - Splunk Enterprise Security
46
47
         - Splunk Cloud
         required fields:
48
         - _time
49
50
         - dest
51
         - Security_ID
         - Share_Name
52
         - Source_Address
53
54
         - Accesses
55
         - Message
         security_domain: endpoint
56
57
         impact: 80
58
         confidence: 70
         risk score: 56
59
60
         context:
         - Source: Endpoint
61
62
         - Stage:Credential Access
         message: A remote host is enumerating a $dest$ to identify permissions. This is
63
           a precursor event to CVE-2021-36942, PetitPotam.
64
65
         observable:
         - name: dest
66
67
           type: Hostname
           role:
68
69
           - Victim
70
         automated_detection_testing: passed
```

security\_content/detections/endpoint/petitpotam\_network\_share\_access\_request.yml at 0dd6de32de2118b2818550df9e65255f4109a56d · splunk/security\_content · GitHub - 31/10/2024 15:51 https://github.com/splunk/security\_content/blob/0dd6de32de2118b2818550df9e65255f4109a56d/detections/endpoint/petitpotal