```yaml
id: 3fe3c520-04f1-44b8-8398-782ed21435f8
name: DNS events related to ToR proxies  (ASIM DNS Schema)
description: |
  'Identifies IP addresses performing DNS lookups associated with common ToR proxies.
  This analytic rule uses [ASIM](https://aka.ms/AboutASIM) and supports any built-in or custom sour
severity: Low
requiredDataConnectors:
  - connectorId: DNS
    dataTypes:
      - DnsEvents
  - connectorId: AzureFirewall
    dataTypes:
      - AzureDiagnostics
  - connectorId: Zscaler
    dataTypes:
      - CommonSecurityLog
  - connectorId: InfobloxNIOS
    dataTypes:
      - Syslog
  - connectorId: GCPDNSDataConnector
    dataTypes:
      - GCP_DNS_CL
  - connectorId: NXLogDnsLogs
    dataTypes:
      - NXLog_DNS_Server_CL
  - connectorId: CiscoUmbrellaDataConnector
```

```
        dataTypes:
          - Cisco_Umbrella_dns_CL
      - connectorId: Corelight
        dataTypes:
          - Corelight_CL
    queryFrequency: 1d
    queryPeriod: 1d
    triggerOperator: gt
    triggerThreshold: 0
    tactics:
      - Exfiltration
    relevantTechniques:
      - T1048
    tags:
      - ParentAlert: https://github.com/Azure/Azure-Sentinel/blob/master/Detections/DnsEvents/DNS_TorPr
        version: 1.0.0
      - Schema: ASIMDns
        SchemaVersion: 0.1.1
    query: |
      let torProxies=dynamic(["tor2web.org", "tor2web.com", "torlink.co", "onion.to", "onion.ink", "oni
      "onion.it", "onion.city", "onion.direct", "onion.top", "onion.casa", "onion.plus", "onion.rip", "
      "tor2web.blutmagie.de", "onion.sh", "onion.lu", "onion.pet", "t2w.pw", "tor2web.ae.org", "tor2web
      "s1.tor-gateways.de", "s2.tor-gateways.de", "s3.tor-gateways.de", "s4.tor-gateways.de", "s5.tor-g
      _Im_Dns(domain_has_any=torProxies)
      | extend timestamp = TimeGenerated, IPCustomEntity = SrcIpAddr, HostCustomEntity = Dvc
    entityMappings:
      - entityType: Host
        fieldMappings:
          - identifier: FullName
            columnName: HostCustomEntity
      - entityType: IP
        fieldMappings:
          - identifier: Address
            columnName: IPCustomEntity
    version: 1.3.1
    kind: Scheduled
```