Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

Azure / Azure-Sentinel Public

Notifications Fork 3k Star 4.6k

Code Issues 28 Pull requests 84 Actions Projects Wiki Security Insights

Files

f99542b

Go to file

- .azure-pipelines
- .github
- .script
- .vscode
- ASIM
- BYOML
- Dashboards
- DataConnectors
- Detections
  - ASimAuthentication
  - ASimDNS
    - imDNS_Miners.yaml
    - imDNS_TorProxies.yaml
    - imDns_DomainEntity_DnsEven...
    - imDns_ExcessiveNXDOMAIND...
    - imDns_HighNXDomainCount_...
    - imDns_IPEntity_DnsEvents.yaml
  - ASimFileEvent
  - ASimNetworkSession
  - ASimProcess
  - ASimWebSession
  - AWSCloudTrail
  - AWSGuardDuty
  - AuditLogs
  - AzureActivity
  - AzureAppServices
  - AzureDevOpsAuditing
  - AzureDiagnostics
  - AzureFirewall
  - CiscoUmbrella
  - CommonSecurityLog
  - DeviceEvents
  - DeviceFileEvents
  - DeviceNetworkEvents
  - DeviceProcessEvents
  - DnsEvents

Azure-Sentinel / Detections / ASimDNS / imDNS_TorProxies.yaml

oshezaf remove-tabs-from-detections 8ad8ab9 · 2 years ago History

Code Blame 62 lines (62 loc) · 2.11 KB · Raw

```
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
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/DnsEven
    version: 1.0.0
  - Schema: ASIMDns
    SchemaVersion: 0.1.1
query: |
  let torProxies=dynamic(["tor2web.org", "tor2web.com", "torlink.co", "onion.to", "onio
  "onion.it", "onion.city", "onion.direct", "onion.top", "onion.casa", "onion.plus", "o
  "tor2web.blutmagie.de", "onion.sh", "onion.lu", "onion.pet", "t2w.pw", "tor2web.ae.or
  "s1.tor-gateways.de", "s2.tor-gateways.de", "s3.tor-gateways.de", "s4.tor-gateways.de
  _Im_Dns(domain_has_any=torProxies)
  | extend timestamp = TimeGenerated, IPCustomEntity = SrcIpAddr, HostCustomEntity = Dv
entityMappings:
  - entityType: Host
    fieldMappings:
      - identifier: FullName
        columnName: HostCustomEntity
  - entityType: IP
```

- Duo Security
- GitHub
- Heartbeat
- LAQueryLogs
- MultipleDataSources
- OfficeActivity

```
  - entityType: IP
    fieldMappings:
      - identifier: Address
        columnName: IPCustomEntity
version: 1.3.1
kind: Scheduled
```