

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

Q

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

a02ce85

Q

Q

Go to file

> .azure-pipelines

> .github

> .script

> .vscode

> ASIM

> BYOML

> Dashboards

> DataConnectors

> Detections

> Exploration Queries

> Functions

> Hunting Queries

> Logos

> MasterPlaybooks

> Notebooks

> Parsers

> Playbooks

> QueryLanguageSamples

> Sample Data

> Solutions

> 42Crunch API Protection

> AI Analyst Darktrace

> AIShield AI Security Monitoring

> ALC-WebCTRL

> ARGOSCloudSecurity

> AWSAthena

> AWS\_IAM

> AbnormalSecurity

> AbuseIPDB

> Agari

> AgileSec Analytics Connector

> Akamai Security Events

> Alibaba Cloud

> Alsid For AD

> Amazon Web Services

> Apache Log4j Vulnerability Dete...

Azure-Sentinel / Solutions / Legacy IOC based Threat Protection / Analytic Rules

...

/ GalliumIOCs.yaml

v-atulyadav Update version

f926e11 · last year

History

Code

Blame

145 lines (144 loc) · 7.02 KB ·

Raw

1id: 26a3b261-b997-4374-94ea-6c37f67f4f39

2name: Known GALLIUM domains and hashes

3description: |

4'GALLIUM command and control domains and hash values for tools and malware used by GA

5Matches domain name IOCs related to the GALLIUM activity group with CommonSecurityLo

6References: https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-glo

7severity: High

8status: Available

9tags:

10- Schema: ASIMDns

11SchemaVersion: 0.1.1

12requiredDataConnectors:

13- connectorId: DNS

14dataTypes:

15- DnsEvents

16- connectorId: AzureMonitor(VMInsights)

17dataTypes:

18- VMConnection

19- connectorId: CiscoASA

20dataTypes:

21- CommonSecurityLog

22- connectorId: PaloAltoNetworks

23dataTypes:

24- CommonSecurityLog

25- connectorId: SecurityEvents

26dataTypes:

27- SecurityEvent

28- connectorId: AzureFirewall

29dataTypes:

30- AzureDiagnostics

31- AZFWApplicationRule

32- AZFWDnsQuery

33- connectorId: Zscaler

34dataTypes:

35- CommonSecurityLog

36- connectorId: InfobloxNIOS

37dataTypes:

38- Syslog

39- connectorId: GCPDNSDataConnector

40dataTypes:

41- GCP\_DNS\_CL

42- connectorId: NXLogDnsLogs

43dataTypes:

44- NXLog\_DNS\_Server\_CL

45- connectorId: CiscoUmbrellaDataConnector

46dataTypes:

47- Cisco\_Umbrella\_dns\_CL

48- connectorId: Corelight

49dataTypes:

50- Corelight\_CL

51

52queryFrequency: 1d

53queryPeriod: 1d

54triggerOperator: gt

55triggerThreshold: 0

56actions:

Page 1 of 3

- > ApacheHTTPServer
- > AristaAwakeSecurity
- > Armis
- > Armorblox
- > Aruba ClearPass
- > AtlassianConfluenceAudit

```
56     let Rules =
57         - CommandAndControl
58         - CredentialAccess
59     query: |
60         let DomainNames = dynamic(["asyspy256.ddns.net","hotkillmail9sddcc.ddns.net","rosaf11
61         let SHA1Hash = dynamic (["53a44c2396d15c3a03723fa5e5db54cafd527635", "9c5e496921e3bc8
62         let SHA256Hash = dynamic (["9ae7c4a4e1cfe9b505c3a47e66551eb1357affee65bfefb0109d02f4e
63         let SigNames = dynamic(["TrojanDropper:Win32/BlackMould.A!dha", "Trojan:Win32/BlackMo
64         (union isfuzzy=true
65         (CommonSecurityLog
66         | parse Message with * '(' DNSName ')' *
67         | where isnotempty(FileHash)
68         | where FileHash in (SHA256Hash) or DNSName in~ (DomainNames)
69         | extend Account = SourceUserID, Computer = DeviceName, IPAddress = SourceIP
70         ),
71         ( _Im_Dns(domain_has_any=DomainNames)
72         | extend DNSName = DnsQuery
73         | extend IPAddress = SrcIpAddr
74         ),
75         (VMConnection
76         | parse RemoteDnsCanonicalNames with * '[' DNSName '"' *
77         | where isnotempty(DNSName)
78         | where DNSName in~ (DomainNames)
79         | extend IPAddress = RemoteIp
80         ),
81         (Event
82         //This query uses sysmon data depending on table name used this may need updataing
83         | where Source == "Microsoft-Windows-Sysmon"
84         | extend EvData = parse_xml(EventData)
85         | extend EventDetail = EvData.DataItem.EventData.Data
86         | extend Hashes = EventDetail.[16].["#text"]
87         | parse Hashes with * 'SHA1=' SHA1 ',' *
88         | where isnotempty(Hashes)
89         | where Hashes in (SHA1Hash)
90         | extend Account = UserName
91         ),
92         (SecurityAlert
93         | where ProductName == "Microsoft Defender Advanced Threat Protection"
94         | extend ThreatName = tostring(parse_json(ExtendedProperties).ThreatName)
95         | where isnotempty(ThreatName)
96         | where ThreatName has_any (SigNames)
97         | extend Computer = tostring(parse_json(Entities)[0].HostName)
98         ),
99         (AzureDiagnostics
100        | where ResourceType == "AZUREFIREWALLS"
101        | where Category == "AzureFirewallApplicationRule"
102        | parse msg_s with Protocol 'request from ' SourceHost ':' SourcePort 'to ' Destinati
103        | where isnotempty(DestinationHost)
104        | where DestinationHost has_any (DomainNames)
105        | extend DNSName = DestinationHost
106        | extend IPAddress = SourceHost
107        ),
108        (AzureDiagnostics
109        | where ResourceType == "AZUREFIREWALLS"
110        | where Category == "AzureFirewallDnsProxy"
111        | project TimeGenerated,Resource, msg_s, Type
112        | parse msg_s with "DNS Request: " ClientIP ":" ClientPort " - " QueryID " " Request_
113        | where Request_Name has_any (DomainNames)
114        | extend DNSName = Request_Name
115        | extend IPAddress = ClientIP
116        ),
117        (AZFWApplicationRule
118        | where isnotempty(Fqdn)
119        | where Fqdn has_any (DomainNames)
120        | extend DNSName = Fqdn
121        | extend IPAddress = SourceIp
122        ),
123        (AZFWDnsQuery
124        | where isnotempty(QueryName)
125        | where QueryName has_any (DomainNames)
126        | extend DNSName = QueryName
127        | extend IPAddress = SourceIp
128        )
129    )
130    | extend timestamp = TimeGenerated, AccountCustomEntity = Account, HostCustomEntity =
```

```
131     entityMappings:
132       - entityType: Account
133         fieldMappings:
134           - identifier: FullName
135             columnName: AccountCustomEntity
136       - entityType: Host
137         fieldMappings:
138           - identifier: FullName
139             columnName: HostCustomEntity
140       - entityType: IP
141         fieldMappings:
142           - identifier: Address
143             columnName: IPCustomEntity
144   version: 1.6.1
145   kind: Scheduled
```