

No projects

Milestone

No milestone

Relationships

Development

Participants

Registry

elastic/detection-rules

[New Rule] DNS-over-HTTPS Enabled by

None yet

Platforms

Windows

Optional Info

Target indexes

Query

registry where event.type in ("creation", "change") and (registry.path: "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\BuiltInDnsClience...b registry.data.strings: "1") or (registry.path: "HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\DnsOverHttpsMode" and registry.data.strings: "secure")

NOTE: Going to expand this query for the other browsers

winlogbeat-*, "logs-endpoint.events.*, "logs-windows.*

New fields required in ECS/data sources for this rule?

Related issues or PRs

False Positives

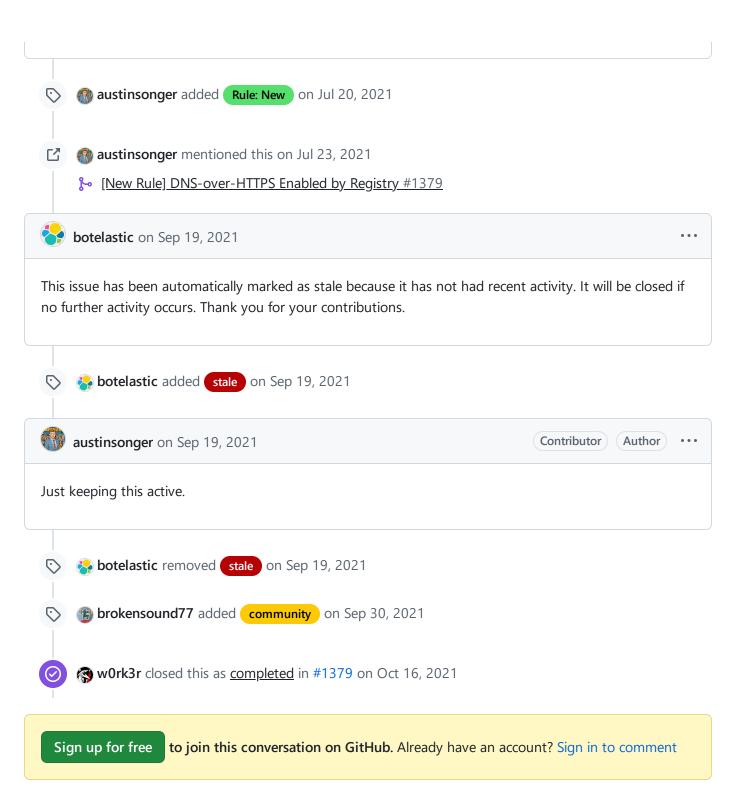
- •
- _

MITRE

Tactic	Technique ID	Technique Name	Sub-Technique Name

References

- https://www.tenforums.com/tutorials/151318-how-enable-disable-dns-over-https-doh-microsoft-edge.html
- $\bullet \quad \underline{https://chromeenterprise.google/policies/?policy=DnsOverHttpsMode}$



© 2024 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information