

registry where event.type in ("creation", "change") and (registry.path: "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Mic_____t registry.data.strings: "1") or (registry.path: "HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\DnsO registry.data.strings: "secure")

NOTE: Going to expand this query for the other browsers

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-dnsover-https-doh-microsoft-edge.html
- https://chromeenterprise.google/policies/?policy=DnsOverHttpsMode



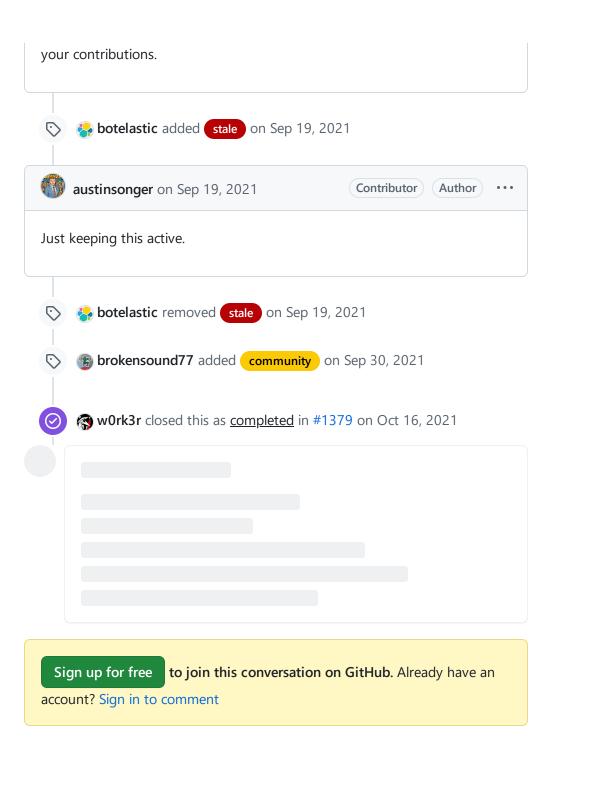
austinsonger mentioned this on Jul 23, 2021

[New Rule] DNS-over-HTTPS Enabled by Registry #1379



🎓 **botelastic** on Sep 19, 2021

This issue has been automatically marked as stale because it has not had recent activity. It will be closed if no further activity occurs. Thank you for



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