CCDC Inject

INJECT NAME	Looking for Suspicious Kerberos Activity
INJECT ID	SOCS15T

INJECT DESCRIPTION:

There is a concern that hackers may be gaining access with forged Kerberos credentials, known as a Golden Ticket. Using Splunk the guidance below, search the centralized log repository for evidence of this activity.

Splunk Guidance:

To find the use of a golden ticket with Splunk:

- Search for Kerberos events (4768, 4769).
- Look for unusual patterns like long TGT validity periods or requests from non-standard accounts.
- Check for high-frequency ticket requests from suspicious users or IPs.
- Monitor for privileged accounts (e.g., Domain Admins) being accessed in unusual ways.

These queries and searches will help identify if a golden ticket has been created and used within your environment.

INJECT DELIVERABLE

Respond with a business memo that shows the commands you used in Splunk to accomplish this search. Show screen shots of the commands and response. Also, report how many log entries are in the centralized log to search. Report if any evidence of Golden Ticket use were found. If so, what actions are being taken to remediate this? Respond to the remediation issue regardless if any evidence was found.