Changes in DNS record type queries

You might need to review the types of DNS resource records being queried when doing the following:

- Monitoring a network for DNS exfiltration

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- DNS data

Example

You want to monitor your network for changes in resource type behavior, which can be an early sign of data exfiltration.

To optimize the search shown below, you should specify an index and a time range. In addition, this sample search uses Stream DNS data. You can replace this source with any other DNS data used in your organization.

1. Run the following search:

```
| eventtype="stream_dns" message_type="Query"
| timechart span=1h count BY record_type
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventtype=&quot;stream_dns&quot;</td>
<td>Search only Stream DNS events.</td>
</tr>
<tr>
<td>message_type=&quot;Query&quot;</td>
<td>Search for queries.</td>
</tr>
</tbody>
</table>
### Splunk Search

```plaintext
| timechart span=1h count BY record_type
```

### Explanation

Display a table that shows the types of DNS records accessed during one hour increments over the time span you set the search for.

### Result

Examine the results for changes in types of records being queried. Both A records and TXT records should be observed carefully as these are commonly used in command and control or exfiltration activity. If you have already identified a suspicious IP address, you can add it to the search to see if it is correlated with the changes in record types queried. You can also use the results to build a baseline or set thresholds for alerts.