Spikes in volume of DNS queries

You might need to review the volume of DNS queries on your network when doing the following:

- [Monitoring a network for DNS exfiltration](#)

## Prerequisites

In order to execute this procedure in your environment, you may need to first on-board the data, services, or apps shown in the following table.

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Network resolution data</td>
<td>Required</td>
</tr>
<tr>
<td>App</td>
<td>Splunk Stream</td>
<td>Recommended</td>
</tr>
</tbody>
</table>

## Example

*The purpose of this example is to show how this procedure works in a general environment. In your environment, you can optimize the search by specifying an index, a time range, or a different data source.*

You want to monitor your network for spikes in DNS queries, which can be an early sign of data exfiltration.

1. Run the following search:

```plaintext
eventtype="stream_dns" message_type="Query"
| timechart span=1h limit=10 usenull=f useother=f count AS Requests by src
```

## 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.

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
**Splunk Search**

```
eventtype="stream_dns"
message_type="Query"
| timechart span=1h limit=10 usenull=f useother=f count AS Requests by src
```

**Explanation**

- Search Stream DNS events.
- Search for queries.
- Display a maximum of 10 results in a table that shows the number of queries for each source in one hour increments. Exclude events that do not contain the split-by field, in this case, `src`. Do not merge all series excluded by the limit into a single new series.

**Result**

Examine the results for clients that have a large number of events compared to other clients in the organization. This is a potential indicator of data transfers using DNS. Investigate any unusual findings, or use the results to build a baseline or set thresholds for alerts.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.