Analysing DNS Log Files Using Splunk

pujitha sambeta
@pujithasambeta

Introduction

DNS (Domain Name System) logs are crucial for understanding network activity and identifying potential security threats. Splunk SIEM (Security Information and Event Management) provides powerful capabilities for analyzing DNS logs and detecting anomalies or malicious activities.

pujitha sambeta
@pujithasambeta

Prerequisites

Before analyzing DNS logs in Splunk, ensure the following:

- Splunk instance is installed and configured.
- DNS log data sources are configured to forward logs to Splunk.

pujitha sambeta
@pujithasambeta

Steps to Upload Sample DNS Log Files to Splunk SIEM

pujitha sambeta
@pujithasambeta

Prepare Sample DNS Log Files

- 1Obtain sample DNS log file in a suitable format (e.g., text files).

- Ensure the log files contain relevant DNS events, including source IP, destination IP, domain name, query type, response code, etc.

- Save the sample log files in a directory accessible by the Splunk instance.

pujitha sambeta
@pujithasambeta

Upload Log Files to Splunk

- Log in to the Splunk web interface.
- Navigate to Settings > Add Data.
- Select Upload as the data input method.

pujitha sambeta
@pujithasambeta

Choose File

- Click on Select File and choose the sample DNS log file you prepared earlier.

pujitha sambeta
@pujithasambeta

Set Source Type

- In the Set Source Type section, specify the source type for the uploaded log file.

- Choose the appropriate source type for DNS logs (e.g., dns or a custom source type if applicable).

pujitha sambeta
@pujithasambeta

Review Settings

- Review other settings such as index, host, and sourcetype.

- Ensure the settings are configured correctly to match the sample DNS log file.

pujitha sambeta
@pujithasambeta

Click Upload

- Once all settings are configured, click on the Review button.

- Review the settings one final time to ensure accuracy.

- Click Submit to upload the sample DNS log file to Splunk.

pujitha sambeta
@pujithasambeta

Verify Upload

- After uploading, navigate to the search bar in the Splunk interface.

- Run a search query to verify that the uploaded DNS events are visible.

pujitha sambeta
@pujithasambeta

Verify Upload

- After uploading, navigate to the search bar in the Splunk interface.

- Run a search query to verify that the uploaded DNS events are visible.

```
index=<your_dns_index> sourcetype=<your_dns_sourcetype>
```

pujitha sambeta
@pujithasambeta

Steps to Analyze DNS Log Files in Splunk SIEM

pujitha sambeta
@pujithasambeta

Search for DNS Events

- Open Splunk interface and navigate to the search bar.

- Enter the following search query to retrieve DNS events

```
index=* sourcetype=dns_sample
```

pujitha sambeta
@pujithasambeta

Extract Relevant Fields

- Identify key fields in DNS logs such as source IP, destination IP, domain name, query type, response code, etc.

- As mentioned below, | regex _raw="(?i)\b(dns|domain|query|response|port 53)\b": This regex searches for common DNS-related keywords in the raw event data.

- Example extraction command:

```
index=* sourcetype=dns_sample | regex _raw="(?i)\b(dns|domain|query|response|port 53)\b"
```

pujitha sambeta
@pujithasambeta

Identify Anomalies

- Look for unusual patterns or anomalies in DNS activity.
- Example query to identify spikes

```
index=_* OR index=* sourcetype=dns_sample  | stats count by fqdn
```

pujitha sambeta
@pujithasambeta

Find the top DNS sources

- Use the top command to count the occurrences of each query type:

```
index=* sourcetype=dns_sample | top fqdn, src_ip
```

pujitha sambeta
@pujithasambeta

Investigate Suspicious Domains

- Search for domains associated with known malicious activity or suspicious behavior.

- Utilize threat intelligence feeds or reputation databases to identify malicious domains such virustotal.com

- Example search for known malicious domains:

```
index=* sourcetype=dns_sample fqdn="maliciousdomain.com"
```

pujitha sambeta
@pujithasambeta

Conclusion

- Analyzing DNS log files using Splunk SIEM enables security professionals to detect and respond to potential security incidents effectively.

- By understanding DNS activity and identifying anomalies, organizations can enhance their overall security posture and protect against various cyber threats.

pujitha sambeta
@pujithasambeta

THANK YOU

Like.Share.Follow

pujitha sambeta
@pujithasambeta