Analyzing DNS Log Files Using Splunk SIEM

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.

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.

Steps to Upload Sample DNS Log Files to Splunk SIEM

1. Prepare Sample DNS Log Files

- Obtain 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.

2. Upload Log Files to Splunk

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

3. Choose File

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

4. 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).

5. Review Settings

- Review other settings such as index, host, and sourcetype.
- Ensure the settings are configured correctly to match the sample DNS log file.

6. 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.

7. 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.
- #CODE: index=<your_dns_index> sourcetype=<your_dns_sourcetype>

Steps to Analyze DNS Log Files in Splunk SIEM

1. Search for DNS Events

- Open Splunk interface and navigate to the search bar.
- Enter the following search query to retrieve DNS events
- #CODE: index=* sourcetype=dns_sample

2. 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:
- #CODE: index=* sourcetype=dns_sample | regex _raw="(?i)\b(dns|domain|query|response|port 53)\b"

3. Identify Anomalies

- Look for unusual patterns or anomalies in DNS activity.
- Example query to identify spikes
- #CODE: index=_* OR index=* sourcetype=dns_sample | stats count by fqdn

4. Find the top DNS sources

- Use the top command to count the occurrences of each query type:
- #CODE: index=* sourcetype=dns_sample | top fqdn, src_ip

5. 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:
- #CODE: index=* sourcetype=dns_sample fqdn="maliciousdomain.com"

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.

Feel free to customize these steps according to your specific use case and requirements.