List of CSV files used in dashboards

Dashboard	**CSV File**
Secure Channel Insights	ssh_inference_lookup.csv
RDP Inferences Overview	corelight_inferences_description.csv
SSH Inferences Overview	ssh_inference_lookup.csv
Alert Aggregation	corelight_aggregations_enrichment.csv
Alert Aggregation Details	corelight_aggregations_enrichment.csv
Security Posture	corelight_aggregations_enrichment.csv

Limitations in CrowdStrike NG-SIEM dashboards

1. Percentage calculation is not possible when displaying data in ascending order.
2. Sparkline cannot be displayed in table or grid view.
3. DNS lookup to determine the hostname associated with an IP address is not supported in CrowdStrike NG-SIEM.
4. Division operations are not feasible when dividing the total count (sum) by another sum, count, or column.
5. Setting a default value for any parameter is not possible without explicitly providing the value * (ALL).
6. Each inference type can have a maximum value of 20,000 in the panel, as it is stored in an array and split into different columns in NG-SIEM (alternative to mv-expand in Splunk).
7. When displaying data through grouping multiple columns, the event count is limited to 1,000,000. (Document Link)
8. A trendline cannot be implemented in a single-value panel with event count, as the count may mismatch due to NG-SIEM functions and widget behavior. (Document Link)
    a. After confirmation from James in a meeting, event count is displayed in a single widget, while the trendline is shown in a separate widget.
9. The map widget does not support legends.
10. Input lookup (adding real-time data into a CSV file) similar to Splunk is not possible, so ingested data is used instead.
11. A dynamic legend based on calculated values is not supported.
    Dashboard: Sensor Overview Dashboard
12. Dynamic field selection for calculations (e.g., calculating the average of all fields starting with "CPU") is not possible using regex or other methods similar to Splunk.
13. The **join** operation has a limitation of processing only 200,000 records. (Document Link)
14. Cell drill-down is not supported, so it has been implemented based on a more suitable column or multiple columns as required.
15. Listing aggregated SID hashes is not possible as in Splunk, so only a list of aggregated SIDs is provided.
    a. For the same reason, hash-based filtering in the entity filter is not considered.
16. The **Oldest CVE Date** has been removed from the Alert Aggregations dashboard due to inconsistencies in the CSV file's date format.

17. Payload - It's quite complex and tedious to decode the encoded payload field using the CrowdStrike query and it will degrade the performance of the dashboard.
18. Separate panels have been provided for Suricata and other sources (except Suricata) to ensure accurate event counts.