ChatGPT for Splunk

Helping you ask ChatGPT the right questions for help with Splunk

Build a Splunk search to....

- Create Splunk search for failed windows event logs.
- Create Splunk search to identify the time difference in minutes between two events.
- Create a Splunk search to find all successful authentication events from the Authentication data model.
- Create a Splunk search to show a timeline to show overall network traffic by day for the last 2 week.
- How do I create a scheduled alert in Splunk to notify me when certain conditions are met?
- What is the best way to visualize my data in a line chart using Splunk?
- What are some best practices for improving the performance of my Splunk searches?
- Create a Splunk search to find a Phishing email that has an invoice related attachment.
- Using the URL Parser app, write a Splunk search to calculate the Shannon entropy of urls
- How can I detect MITRE technique T1570 in Splunk?

Help with data

- What security logs should you collect from Linux devices?
- What are the most important Windows Event Codes?
- Explain to me what important fields are in Palo Alto network logs.
- What are the top 10 data sources for security teams
- What security logs should I collect from aws?
- How can I extract custom fields from my log data in Splunk?
- What security logs should I collect from GCP for wazuh?
- What security logs should I collect from Azure?
- What security measures should I take to protect sensitive data in Splunk?

How does Splunk work?

- In Splunk explain what the stats command does and provide 5 examples.
- Explain it like I'm 5 how Splunk works.
- What are the default user roles in Splunk Enterprise Security and what all can they do?
- What are the most common ways to bring data into Splunk?

- How do I create a dashboard in Splunk that has a panel that has a drop down box with a list of user names? Once a user is selected it will show you all of their authentication events.
- What are the top 10 most useful Splunk search commands and provide examples of how they work?

- Explain the Splunk architecture and what each component does.
- What is the difference between a Report and Alert in Splunk?
- What is a Data Model in Splunk, and what does it mean if one is accelerated?
- In Splunk how should I use eventtypes?

Roles

As a SOC Manager...

- write a Splunk search to show me the number of notable events closed in the last 7 days and how they were closed.
- write a Splunk search to show me the number of alerts worked by each analysts over the last 30 days.
- help me write a Splunk search to calculate the mean time to respond to alerts.

As a SOC Analyst...

- write a Splunk search to show me my last 50 searches.
- explain how the following Splunk search works: <insert search>
- help me write a Splunk search to find any time power shell is used with base64 encoded commands

As an Incident Responder...

- build a Splunk search to show me all events associated with <insert IP Address>
- help me write a Splunk search that will calculate the time between two events.
- create a Splunk search that looks for data exfiltration events

Misc

- Map these signatures to the MITRE ATT&CK framework, format in a table with the Tactic, Technique, and ID number.
- Write regex to extract an IP address from this example: date:07/03/23, user:sample_user,ip:127.0.0.1

RBA

- Which field in this Splunk search would be the best candidate for risk_object:
- Which field in this Splunk search would be the best candidate for threat_object:
- Explain how Splunk's Risk Based Alerting works and each component.
- In a threat hunt I found an interesting event, now I need to add that to the risk index in Splunk, how do I do this, please provide steps and any Splunk commands?

Admin Stuff

- As a Splunk admin, what steps should I take to implement role based access to indexes?
- As a Splunk admin, how do you audit roles assigned to users?
- As as Splunk admin, how do you convert a lookup file to a kvstore?