TRIVID TECHNOLOGY SERVICES

Security Information and Event Management (SIEM)

Module 1 - Getting Started

- Provide an overview of Splunk for Enterprise Security (ES)
- Identify the differences between traditional security threats and new adaptive threats
- Describe correlation searches, data models and notable events

Module 2 - Security Monitoring and Incident Investigation

- Use the Security Posture dashboard to monitor enterprise security status
- Use the Incident Review dashboard to investigate notable events
- Take ownership of an incident and move it through the investigation workflow
- Use adaptive response actions during incident investigation

+91 8007377665
+1(404)491-8800
abhay@trividtech.com
www.ttstechloot.com
Block AE-23 , Salt Lake City , Sector - I, Tank No:- 4. Land Mark : Lake Town Foot Bridge, Kolkata : 700064
737 Saint George's Ave Woodbridge, NJ, 07065

Module 3 – Investigations

- Use ES investigation timelines to manage, visualize and coordinate incident investigations
- Use timelines and journals to document breach analysis and mitigation efforts

Module 5 – Risk and Network Analysis

- Understand and use Risk Analysis
- Use the Risk Analysis dashboard
- Manage risk scores for objects or users

Module 6 – Web Intelligence

- Use HTTP Category Analysis, HTTP User Agent Analysis, New Domain Analysis, and Traffic Size Analysis to spot new threats
- Filter and highlight events

Module 7 – User Intelligence

- Evaluate the level of insider threat with the user activity and access anomaly dashboards
- Understand asset and identity concepts

Module 8 – Threat Intelligence

- Use the Threat Activity dashboard to analyze traffic to or from known malicious sites
- Inspect the status of your threat intelligence content with the threat artifact dashboard

Module 10 – Glass Tables

- Build glass tables to display security status information
- Add glass table drilldown options
- Create new key indicators for metrics on glass tables

Note: The above mentioned SIEM course should only be undertaken only after the successful completion of Splunk development and admin modules.

+91 8007377665
+1(404)491-8800
abhay@trividtech.com
www.ttstechloot.com
Block AE-23 , Salt Lake City , Sector - I, Tank No:- 4. Land Mark : Lake Town Foot Bridge, Kolkata : 700064
737 Saint George's Ave Woodbridge, NJ, 07065