Section xx – Install & Admin Splunk Enterprise Security

1. Module 5 – Installation
   1. Prepare a Splunk environment for installation
   2. Download and install ES on a search head
   3. Test a new install
   4. Post-install configuration tasks
2. Initial ES Configuration
   1. Set general configuration options
   2. Add external integrations
   3. Configure local domain information
   4. Customize navigation
   5. Configure Key Indicator searches
3. Validating ES Data
   1. Verify data is correctly configured for use in ES
   2. Validate normalization configurations
   3. Install additional add-ons
4. Custom Add-ons
   1. Design a new add-on for custom data
   2. Use the Add-on Builder to build a new add-on
5. Tuning Correlation Searches
   1. Configure correlation search scheduling and sensitivity
   2. Tune ES correlation searches
6. ES functions
   1. Review how ES functions
   2. Understand how ES uses data models
   3. Configure ES roles and permissions
7. Security Monitoring Configs
   1. Customize the Security Posture and Incident Review dashboards
   2. Create ad hoc notable events
   3. Create notable event suppressions
8. Risk-Based Alerting Configs
   1. Explain Risk-Based Alerting
   2. Explain risk scores
   3. Review the Risk Analysis dashboard
   4. Use annotations
9. Incident Investigation Configs
   1. Review the Investigations dashboard
   2. Customize the Investigation Workbench
   3. Manage investigations
10. Creating Correlation Searches
    1. Create a custom correlation search
    2. Manage adaptive responses
    3. Export/Import content
11. Asset & Identity Management
    1. Review the Asset and Identity Management interface
    2. Describe Asset and Identity KV Store collections
    3. Configure and add asset and identity lookups to the interface
    4. Configure settings and fields for asset and identity lookups
    5. Explain the asset and identity merge process
    6. Describe the process for retrieving LDAP data for an asset or identity lookup
12. Manage Threat Intelligence
    1. Configure threat intelligence
    2. Use the Threat Intelligence Management interface to configure a new threat list

Section xx – Using Splunk Enterprise Security

1. Introduction to Splunk Enterprise Security
   1. Features and capabilities of Splunk Enterprise Security (ES)
   2. How ES helps security practitioners prevent, detect, and respond to threats
   3. Correlation searches, data models and notable events
   4. User roles in ES
   5. Log into Enterprise Security
2. Security Monitoring and Incident Investigation
   1. Security Posture dashboard to monitor ES status
   2. Incident Review dashboard to investigate notable events
   3. Take ownership of an incident and move it through the investigation workflow
   4. Create notable events
   5. Suppress notable events
3. Risk-Based Alerting
   1. Give an overview of Risk-Based Alerting
   2. View Risk Notables and risk information on the Incident Review dashboard
   3. Explain risk scores and how to change an object's risk score
   4. Review the Risk Analysis dashboard
   5. Describe annotations
   6. Describe the process for retrieving LDAP data for an asset or identity lookup
4. Assets & Identities
   1. Overview of the ES Assets and Identities framework
   2. Where asset or identity data is missing from ES dashboards or notable events
   3. View the Asset & Identity Management Interface
   4. Contents of an asset or identity lookup table
5. Investigations
   1. Use investigations to manage incident response activity
   2. Use the investigation workbench to manage, visualize and coordinate incident investigations
   3. Items to investigations (notes, action history, collaborators, events, assets, identities, files and URLs)
   4. Investigation timelines, lists and summaries to document and review breach analysis and mitigation efforts
6. Security Domain Dashboards
   1. Describe the ES security domains
   2. Use the Security Domain dashboards to troubleshoot various security threats
   3. Launch the Security Domain dashboards from Incidents Review and from a notable event Action menu
7. User Intelligence
   1. Understand and use user activity analysis
   2. Use investigators to analyze events related to an asset or identity
   3. Use access anomalies to detect suspicious access patterns
8. Web Intelligence
   1. Use the web intelligence dashboards to analyze your network environment
   2. Filter and highlight events
9. Threat Intelligence
   1. Overview of the Threat Intelligence framework and how threat intel is configured in ES
   2. Threat Activity dashboard to see which threat sources are interacting with your environment
   3. Threat Artifacts dashboard to examine the status of threat intelligence information in your environment
10. Protocol Intelligence
    1. Explain how network data is input into Splunk events
    2. Describe stream events
    3. Overview of the Protocol Intelligence dashboards and how they can be used to analyze network data