Administering Splunk Enterprise Security

Duration: 40 Hours

Module 1 - Introduction to Enterprise Security

- Explain the function of a SIEM
- Give an overview of Splunk's Enterprise Security (ES)
- Describe detections and findings
- Configure ES roles and permissions
- Give an overview of ES navigation

Module 2 - Customizing the Analyst Queue and findings

- Give an overview of the Analyst Queue
- Create and use Analyst Queue Views
- Customize the Analyst Queue
- Modify Urgency
- Create new Status values
- Add fields to Finding attributes
- Create ad hoc Findings
- Suppress Findings

Module 3 - Working with Investigations

- Give an overview of an investigation
- Use and create Response Plans
- Add Splunk events to an investigation
- Use Playbooks and Actions

Module 4 - Asset & Identity Management

- Review the Asset and Identity Management interface
- Describe Asset and Identity KV Store collections
- Configure and add asset and identity lookups to the interface
- Configure settings and fields for asset and identity lookups
- Explain the asset and identity merge process
- Describe the process for retrieving LDAP data for an asset or identity lookup

Module 5 - Data Normalization

- Understand how ES uses accelerated data models
- Verify data is correctly configured for use in ES
- Validate normalization configurations
- Install additional add-ons
- Ingest custom data in ES
- Create an add-on for a custom sourcetype
- Describe add-on troubleshooting

Module 6 -Detection Engineering

- Give an overview of how to create Event-based detections

- Review the Detection Editor
- Give an overview of how to create Finding-based detections •

Module 7 -Risk-Based Alerting

- Give an overview of Risk-Based Alerting (RBA)
- Explain risk scores and how they can be changed by detections or manually
- Review the Risk analysis dashboard
- Understand Finding-based detections
- Describe annotations
- View risk information in Analyst Queue findings

Module 8 -Managing Threat Intelligence

- Understand and configure threat intelligence
- Use the Threat Intelligence interface to configure threat lists
- Configure new threat lists

Module 9 -Post-Deployment Configuration

- Give an overview of general ES install requirements
- Explain the different add-ons and where they are installed
- Provide ES pre-installation requirements
- Describe the Splunk_TA_ForIndexers app and where it is installed
- Set general configuration options
- Configure local and cloud domain information
- Work with the Incident Review KV Store
- Customize navigation
- Configure Key Indicator searches