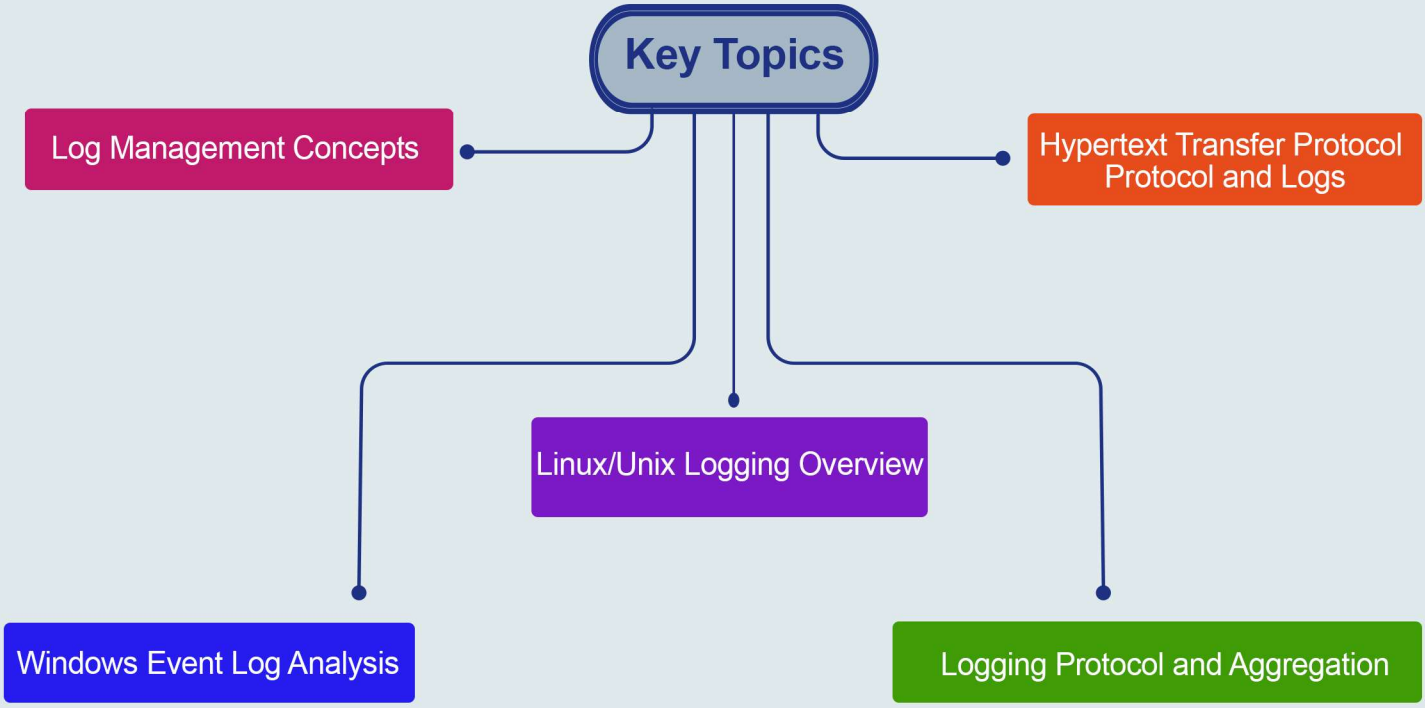
About the Course

Many organizations have logging capabilities but lack the people and processes to analyze it. In addition, logging systems collect vast amounts of data from a variety of data sources which require an understanding of the sources for proper analysis. This course is designed to provide individuals, methods, and processes for enhancing existing logging solutions. It will also provide the understanding of the when, what, and why behind the logs.

Learning Objectives

Key Topics



Pre Requisites

- Information Security Concepts and Principles Course

What You Will Receive

Course Presentation File

Complementary Files

Log Management eBook

Who Should Attend

Attend this course if you are responsible for log management. This course is also for:

- Cyber Intelligence Specialists

Syllabus

Log Management Overview

- Logging Overview
- Setting Up and Configuring Logging
- Logging Analysis Basics
- Key Logging Activity
- The Importance of Time Synchronization
- How to Setup NTP on each Platform
- Goals for a Centralized Collection System
- Components of a Log Collection System
- Designing an Architecture

Monitoring and Attack Detection

- Log Aggregation and SIEM
- Log Files
- Log Parsing

Log Parsing and Analysis

- Log Basics
- Log Formats
- Log Recovery
- Security Software Logs
- Operating System Logs
- Application Logs
- Challenges in Log Management
- Architecture of Log Management Infrastructure
- Log Management Functions
- Storage
- Analysis
- Disposal
- Analysis and Parsing Tools

Syllabus

Logging Protocol and Aggregation

- Syslog
- Microsoft Eventing
- Log Data Collection, Aggregation, and Analysis

Centralized Logging with Syslog-NG

- Hints and Hacks for Tunneling Log Data
- Log Analysis Tools and Strategies

Windows Event Log Analysis

- EVTX and EVT Log Files
- Track Account Usage including RDP, Password Attacks, and Rogue Local Account
- Audit and Analyze File and Folder Access
- Prove System Time Manipulation
- Track Bring Your Own Device (BYOD) and External Devices
- Geo-locate a Device via Event Logs
- Log aggregation, management and Analysis

Linux/Unix Logging Overview

- Syslog Configuration
- System Accounting
- Process Accounting
- Kernel-Level Auditing

Syllabus

Event Log Analysis for Incident Responders and Hunters

- Profiling Account Usage
- Tracking and Hunting Lateral Movement
- Identifying Suspicious Services
- Detecting Rogue Application Installation
- Finding Malware Execution and Process Tracking
- Capturing Command Lines and Scripts
- Anti-Forensics and Event Log Clearing

Hypertext Transfer Protocol (HTTP): Protocol and Logs

- Forensic value
- Request/response dissection
- Useful HTTP fields
- Artifact extraction
- Log formats
- Analysis methods

Domain Name Service (DNS): Protocol and Logs

- Architecture and core functionality
- Tunneling
- Fast flux and domain name generation algorithms (DGAs)
- Logging methods
- Amplification attacks

Firewall, Intrusion Detection System, and Network Security Monitoring Logs

- What Gets Recorded
- What to Look for
- Spotting Patterns in the Stream

Syllabus

- o Identifying when a Firewall Gives You Incorrect Info
- o The Process for Parsing any Firewall Log
- o Families of firewall solutions
- o Additional features
- o Syntax and log formats
- o Rules and signatures
- o Families of IDS and NSM solutions

Hands-on Training

- Lab 1: Windows Log Analysis
- Lab 2: Firewall Log Analysis
- Lab 3: Unix/Linux Log Analysis
- Lab 4: HTTP Log Analysis
- Lab 5: DNS Log Analysis