Module 14– Objectives and Key Instruction Points

Objectives:
Event management and analysis is a critical activity in operational settings. Designing, deploying and maintaining security controls are significant activities as well, but no matter their effectiveness with respect to prevention, of which some controls provide no prevention value, situational awareness of the IT environment's operational and security condition is vital. The operational mantra of "prevent, detect and respond" assumes prevention will fail. Event management and analysis addresses detection within the mantra when detection is to be operationalized. Hundreds of deployed controls generating activity logs are nearly meaningless if there is no action taken to ensure the logging occurs, logs are collected and troublesome events are being analyzed. Today, the task of analysis falls on people. Software assists in facilitating the analysis, but discernment and judgment requires a competent person to perform.
The guiding question is "What concepts and skills do students need to be successful building an IT environment suitable for the CDC?"

Video Segment 1 –

1. Significance
    a. Situational Awareness
2. Time and context
3. Log Review and Collection
    a. OS, Applications (e.g. DNS, Apache)
4. Monitoring
    a. Operating statistics
    b. Operating services
    c. User activities
5. Analysis tools
    a. Log processing
    b. Event correlation
    c. Link analysis
    ~~d. Visualization~~ Like SIEM, visualizations take large investments of time and energy to implement and understand. For this audience, it doesn't appear to be practical to reference
6. Analysis strategy

Activities

Name	Objectives	Content ideas
Activity1	Event analysis exercise	Provide a scenario to provide context for the analysis of provided logs. Provide several guiding questions to help students perform log review and analysis
Activity 2	Link analysis exercise	If possible, identify a practical link analysis tool for students to install

		and use. The data set initially would need to be provided. Questions should be asked that leverage link analysis. If time or tools permitted, have students prepare a dataset from raw data sources. Ideally there would be a methodology adopted that would be practical in a CDC setting.

Activity design

Handouts
Title:
Objectives:
Length: X pages
Notes:

Title: Guidance to analysis of syslog files
Objectives: Describe the record structure of the syslog files. Discuss common techniques to process syslog formatted logs.
Length: X pages
Notes:
This handout should be written from the context of a distinct system's log as well as the syslog of a log host.

Title: Guidance to analysis of services log entries
Objectives: Describe the operational context of each service and how it influences the semantics of the corresponding log entry types. Describe the meaning of regularly observed log entry types.
Length: X pages
Notes:
Web logs may be need to be handled in a distinct handout.

Title: Interpretation of the output fields of the most common Windows tools
Objectives: Explain the meaning and significance of the fields in the various tools mentioned in the video presentation.
Length: X pages
Notes:
Some of the tools are Task Manager (all tabs), Computer Management

Title: Interpretation of the output fields of the most common Unix tools
Objectives: Explain the meaning and significance of the fields in the various tools mentioned in the video presentation.

Length: X pages
Notes:
top, ps, who, vm_stat/vmstate, iostat,

Title: Log analysis guidelines
Objectives: Primarily focused analysis of log entries as opposed to the details pre-analysis event management details.
Length: X pages
Notes:
Guidance for log analysis varies by analytical objective, available event sources and, in some part, the available tools. This handout can’t be a swiss army knife, so focusing on CDC specific objectives and context would provide the most value.