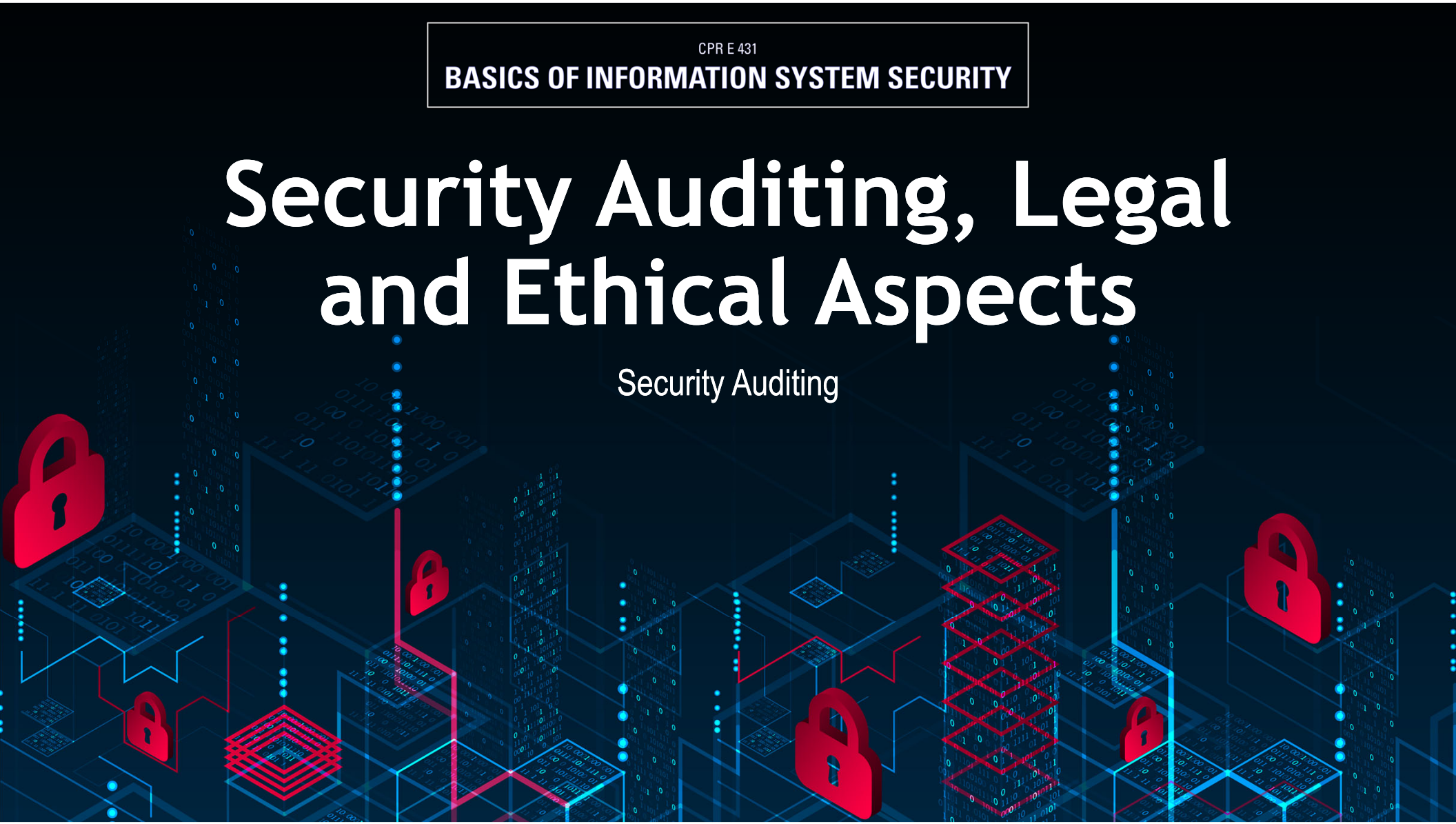
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Security Auditing, Legal and Ethical Aspects

Security Auditing



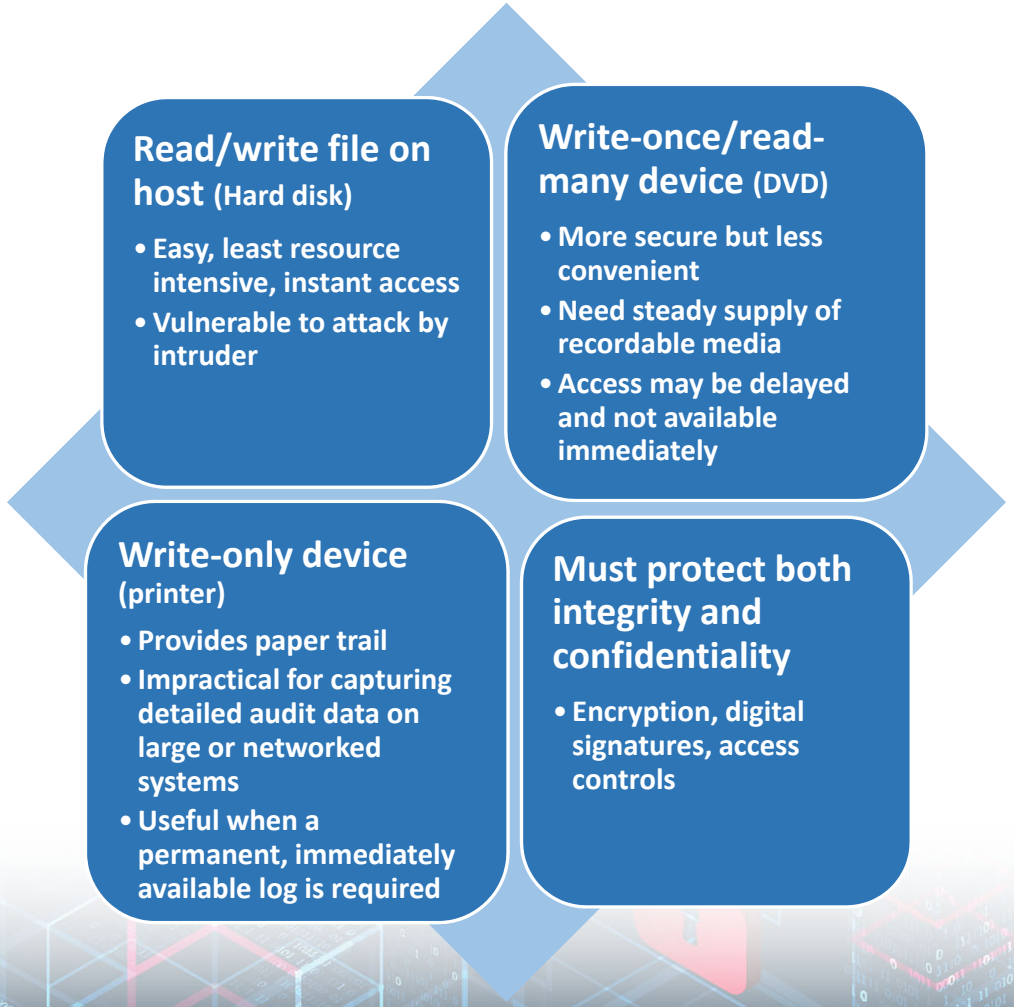
Video Summary

- Auditing Physical Access
- Protecting Audit Trail Data
- Windows Event Categories
- Unix System Log
- Audit Review and Analysis
- SIEM System

Physical Access Audit Trails

- Generated by equipment that controls physical access
  - Card-key systems, alarm systems
- Sent to central host for analysis and storage
- Data of interest:
  - Date/time/location/user of access attempt
  - Both valid and invalid access attempts
  - Attempts to add/modify/delete physical access privileges
  - May send violation messages to personnel

Protecting Audit Trail Data



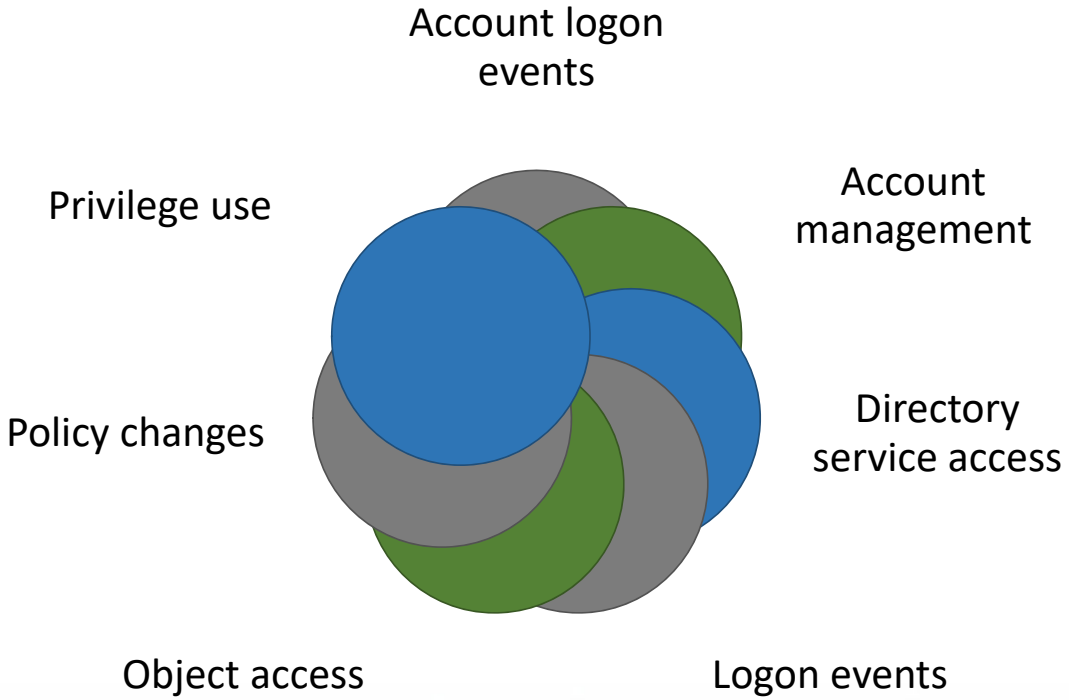
Windows Event Log

- Three types of event logs:
  - System: system related apps and drivers (installed system services)
  - Application: user-level apps
  - Security: This event log is for exclusive use of the Windows Local Security Authority

```
Event Type:      Success Audit
Event Source:    Security
Event Category:  (1)
Event ID:        517
Date:            3/6/2006
Time:            2:56:40 PM
User:            NT AUTHORITY\SYSTEM
Computer:        KENT
Description:     The audit log was cleared
Primary User Name:   SYSTEM          Primary Domain:   NT AUTHORITY
Primary Logon ID:    (0x0,0x3F7)     Client User Name: userk
Client Domain:       KENT            Client Logon ID:  (0x0,0x28BFD)
```

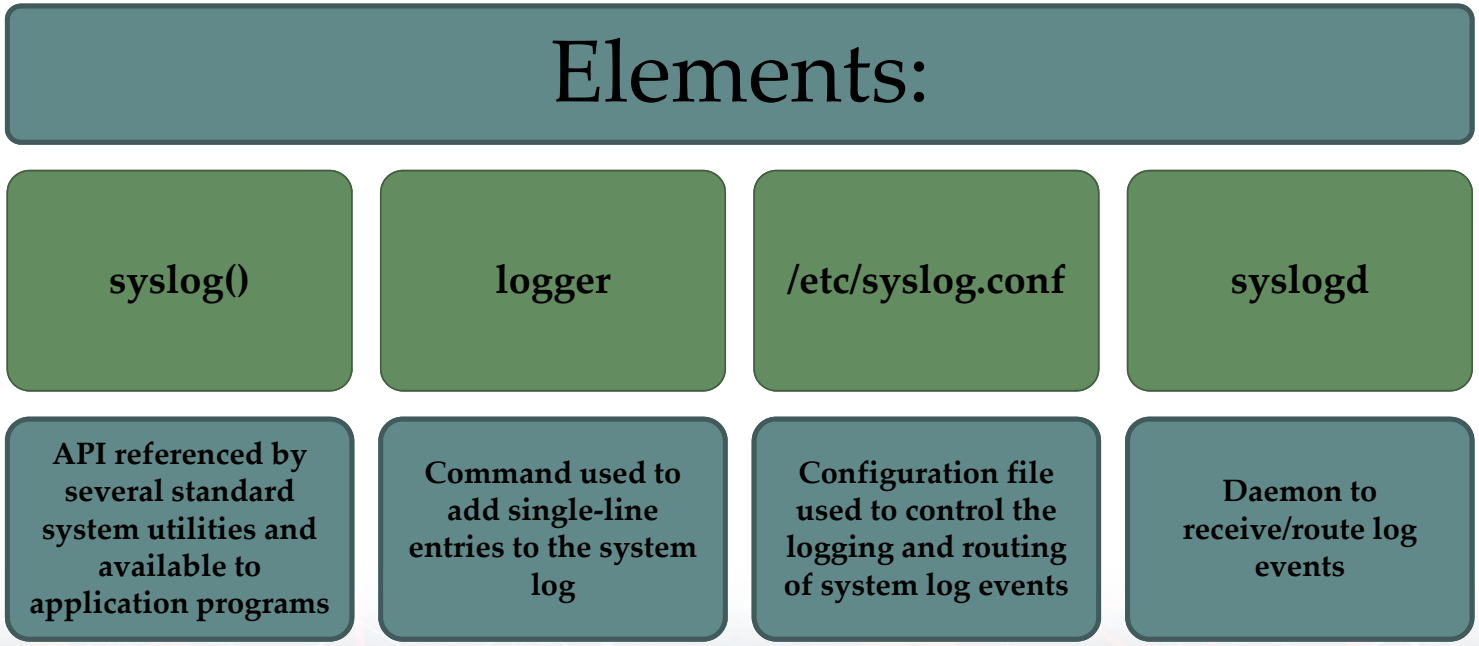
Example of data exported from a Windows system event log

Windows Event Categories

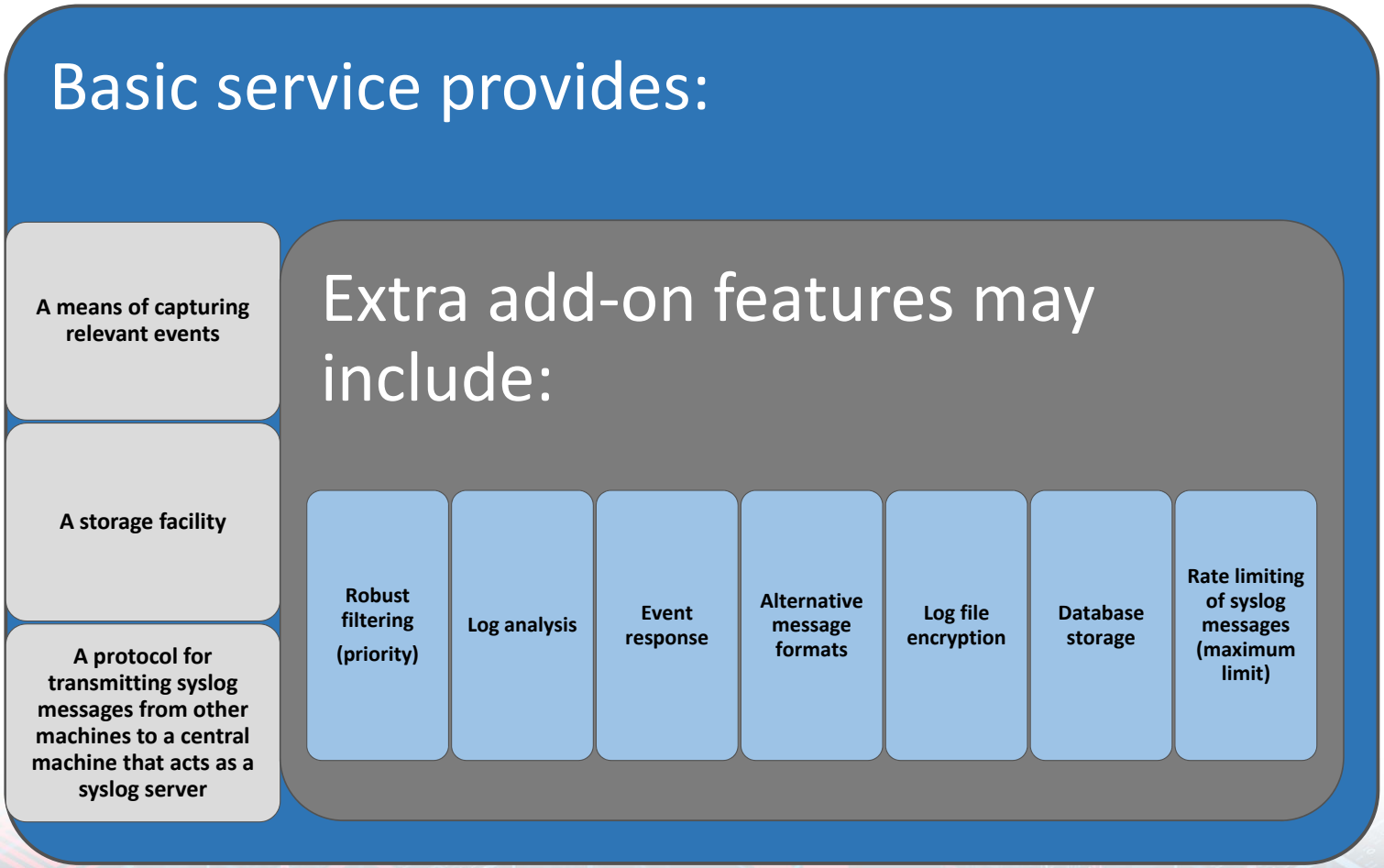


UNIX Syslog

- UNIX's general-purpose logging mechanism
  - Found on all UNIX / Linux variants



Syslog Service



Syslog Protocol

- A transport protocol allowing hosts to send IP event notification messages to syslog servers
  - Provides a very general message format
  - Allowing processes and applications to use suitable conventions for their logged events

```
Mar 1 06:25:43 server1 sshd[23170]: Accepted publickey for server2 from
172.30.128.115 port 21011 ssh2

Mar 1 07:16:42 server1 sshd[9326]: Accepted password for murugiah from
10.20.30.108 port 1070 ssh2

Mar 1 07:16:53 server1 sshd[22938]: reverse mapping checking getaddrinfo for
ip10.165.nist.gov failed - POSSIBLE BREAKIN ATTEMPT!

Mar 1 07:26:28 server1 sshd[22572]: Accepted publickey for server2 from
172.30.128.115 port 30606 ssh2

Mar 1 07:28:33 server1 su: BAD SU kkent to root on /dev/ttyp2

Mar 1 07:28:41 server1 su: kkent to root on /dev/ttyp2
```

Types of Audit Trail Analysis

Audit trails can be used in multiple ways

- This depends in part on when done

Possibilities include:

- Audit trail review after an event
  - Triggered by event to diagnose cause and remediate
  - Focuses on the audit trail entries that are relevant to the specific event
- Periodic review of audit trail data
  - Review bulk data to identify problems and behavior
- Real-time audit analysis
  - Part of an intrusion detection function

Audit Review

- Audit review capability provides administrator with information from selected audit records
  - Actions of one or more users
  - Actions on a specific object or resource
  - Actions on a specific system/security attribute
- May be filtered by time/source/frequency

Approaches to Data Analysis

Basic alerting

- Indicate interesting type of event has occurred

Baselining

- Define normal versus unusual events/patterns
- Compare with new data to detect changes
- Thresholding is the identification of data that exceed a particular baseline value

Windowing

- Detection of events within a given set of parameters

Correlation

- Seeks relationships among events

SIEM Systems

- Software is a centralized logging software package similar to, but much more complex than, syslog
- Provide a centralized, uniform audit trail storage facility and a suite of audit data analysis programs

➢ **There are two general configuration approaches:**

- *Agentless*
  - SIEM server receives data from the individual log generating hosts without needing to have any special software installed on those hosts
- *Agent-based*
  - An agent program is installed on the log generating host to perform event filtering and aggregation and log normalization for a particular type of log, and then transmit the normalized log data to a SIEM server, usually on near-real-time basis for analysis and storage

Video Summary

- Auditing Physical Access
- Protecting Audit Trail Data
- Windows Event Categories
- Unix System Log
- Audit Review and Analysis
- SIEM System