SIU Southern Illinois University
CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 20: Security Monitoring of ICS

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

Information Management

Log Storage and Retention

Recall: Host Security and Access Controls

Host firewalls, Host IDS, Anti-virus, Application Whitelisting

All host access control and network security solutions should be implemented on all networked devices

- Not all devices capable of running such software
  - Additional delay
- Some ICS vendors began to offer security features for embedded devices (i.e., Siemens S7-400 PLC)

Device	Suitable Security Measures
HMI or similar device running a modern operating system. Application is not time sensitive	• Host firewall • HIDS • Anti-Virus or Application Whitelist • Disable all unused ports and services
HMI or similar device running a modern operating system. Application is time sensitive	• Host firewall • Disable all unused ports and services
PLC, RTU, or similar device running an embedded commercial OS	• Host firewall or HIDS if available • External security controls
PLC, RTU, IED, or similar device running an embedded operating environment	• External security controls

Recall: Behavioral Anomaly Detection

Anomalies can be detected by comparing monitored behavior against known "normal" values

- Cannot be detected without an established baseline of activity to compare against

Manually:

- Based on real-time monitoring or log review

Automated:

- Using a Network Behavior Anomaly Detection (NBAD) product, Log Analysis, or Security Information and Event Management (SIEM) tool

Recall: Behavioral Whitelisting

User Whitelists

- Locking critical functions to administrative personnel

Asset Whitelists

- Authorized devices can be used to whitelist known good network devices

Application Behavior Whitelists

- Can be whitelisted per host

Recall: Threat Detection

For the detection of an incident (vs. a discrete event), it is, therefore, necessary to look at multiple events together and search for larger patterns

- Even simple attacks consist of multiple steps

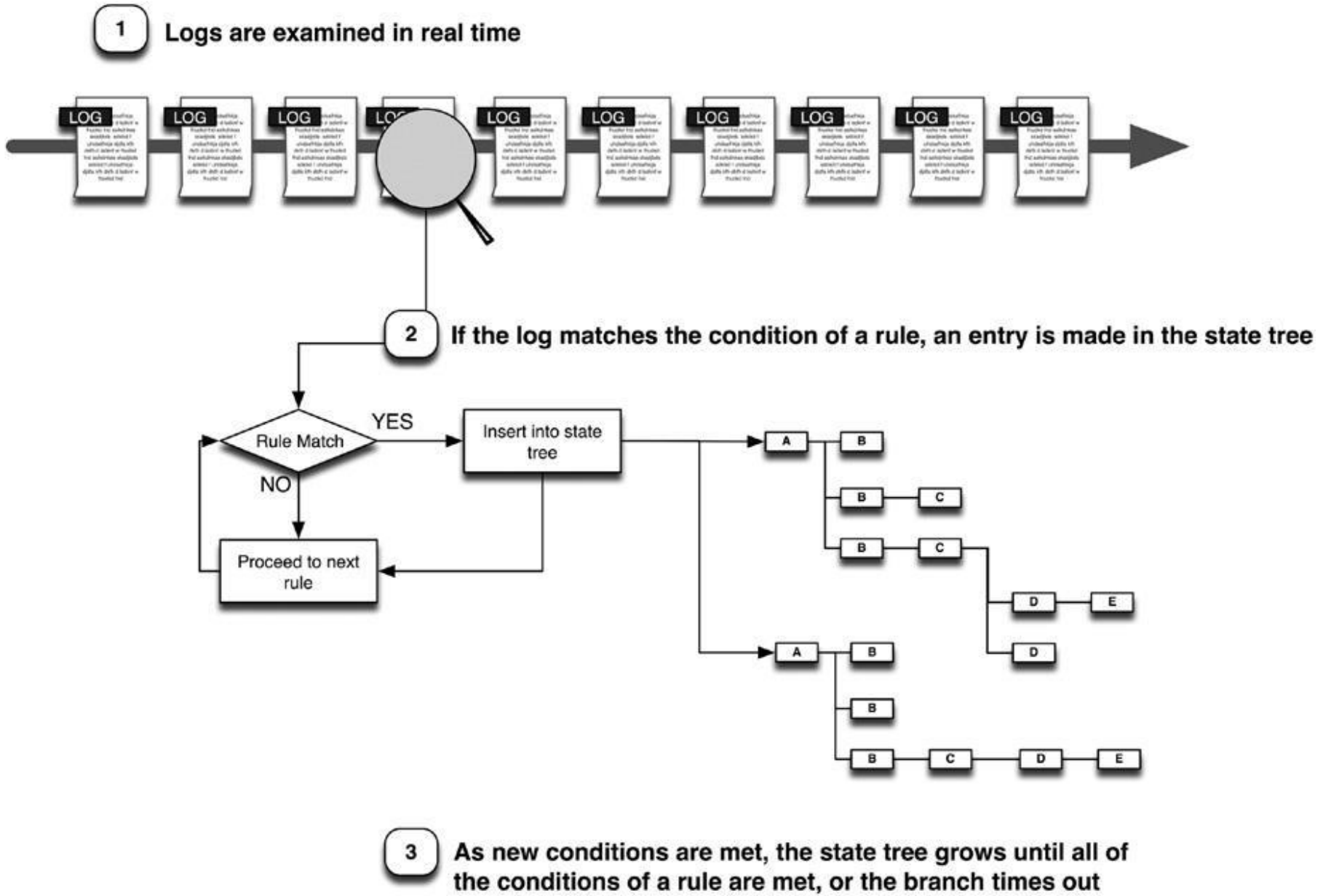
Event Correlation

- Simplifies the threat detection process by making sense of the massive amounts of discrete event data, analyzing it as a whole to find the important patterns and incidents that require immediate attention
- Events are collected from many types of information sources, such as firewalls, switches, authentication servers, etc.

Recall:

Event

Correlation



Recall: Data Enrichment

Process of appending or otherwise enhancing collected data with relevant context obtained from additional sources

- If a username is found within an application log, that username can be referenced against a central Identity system to obtain the user's actual name, departmental roles, privileges, etc.
- Additional information "enriches" the original log with this context

Primary way

- By performing lookup at the time of collection and appending the contextual information into the log

Recall: Normalization

Classification system, which categorizes events according to a defined taxonomy

Way the message is depicted varies sufficiently that without a compensating measure such as event normalization, a correlation rule looking for "logons" would need to explicitly define each known logon format

Log Source	Log Contents	Description
Juniper Firewall	<18> Dec 17 15:45:57 10.14.93.7 ns5xp: NetScreen device_id 5 ns5xp system-warning-00515: Admin User jdoe has logged on via Telnet from 10.14.98.55:39073 (2002-12-17 15:50:53)	Successful Logon
Cisco Router	<57> Dec 25 00:04:32:%SEC_LOGIN-5-LOGIN_SUCCESS:Login Success [user:jdoe] [Source:10.4.2.11] [localport:23] at 20:55:40 UTC Fri Feb 28 2006	Successful Logon
Redhat Linux	<122> Mar 4 09:23:15 localhost sshd[27577]: Accepted password for jdoe from ::ffff:192.168.138.35 port 2895 ssh2	Successful Logon

MONITORING INDUSTRIAL CONTROL SYSTEMS

Recall: Determining What to Monitor

"Everything"

- But so much information that can exhaust the analyst as well as storage

Security Events

Assets

Configurations

Applications

Networks

Users

Behavior

Recall: Monitoring Security Zones

Log collection and analysis

- Directing the log output to a log aggregation point, such as a network storage facility and/or a dedicated Log Management system

Direct monitoring or network inspection

- Use of a probe or other device to examine network traffic or hosts directly
- Useful when the system being monitored does not produce logs natively
  - Also useful as a verification of activity reported by logs

Recall: Information Collection and Management Tools (Log Management Systems, SIEMs)

Syslog Aggregation and Log Search

Log Management Systems

Security Information and Event Management Systems

- Designed to support real-time monitoring and analytical functions, it will parse the contents of a log file at the time of collection, storing the parsed information in some sort of structured data store, typically a database or a specialized flat-file storage system

Data Historians

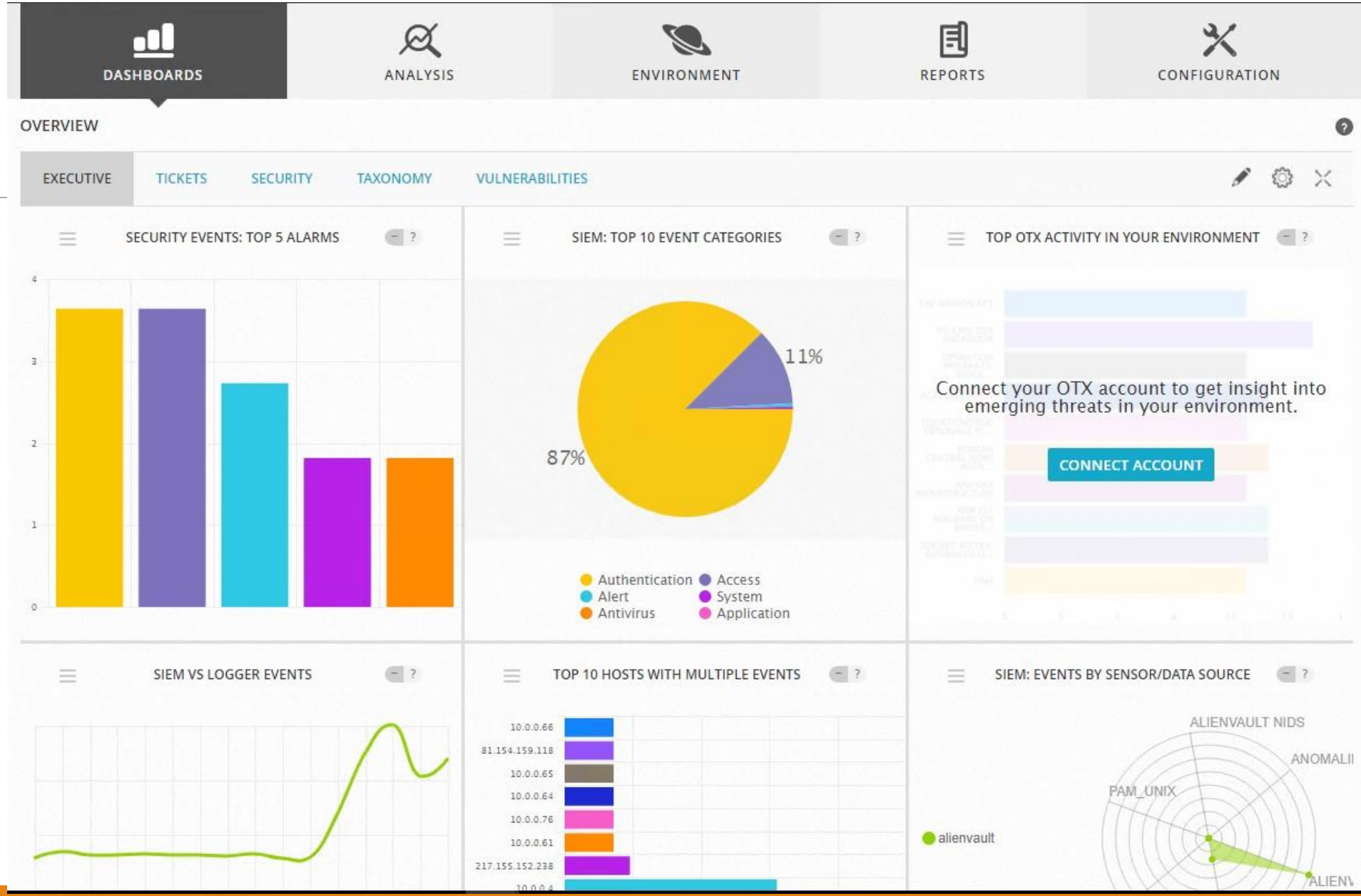
Information Management

Proper analysis in order to provide situational awareness to detect incident

SIEM (security information and event management) or Log Manager will perform many underlying detection functions automatically—including normalization, data enrichment, and correlation:

- The raw log and event details obtained by monitoring relevant systems and services, normalized to a common taxonomy
- The larger "incidents" or more sophisticated threats derived from those raw events
- The associated necessary context to what has been both observed (raw events) and derived (correlated events)

SIEM


DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
OVERVIEW
EXECUTIVE
TICKETS
SECURITY
TAXONOMY
VULNERABILITIES
SECURITY EVENTS: TOP 5 ALARMS
SIEM: TOP 10 EVENT CATEGORIES
11%
87%
Authentication
Access
Alert
System
Antivirus
Application
TOP OTX ACTIVITY IN YOUR ENVIRONMENT
Connect your OTX account to get insight into emerging threats in your environment.
CONNECT ACCOUNT
SIEM VS LOGGER EVENTS
TOP 10 HOSTS WITH MULTIPLE EVENTS
10.0.0.66
81.154.159.118
10.0.0.65
10.0.0.64
10.0.0.76
10.0.0.61
217.155.152.238
SIEM: EVENTS BY SENSOR/DATA SOURCE
ALIENVAULT NIDS
ANOMALI
PAM_UNIX
alienvault

Queries

Request for information from the centralized data store

- Structured Query Language (SQL)
- Plain-text request (SQL queries internally, hidden from the user)
  - Few examples that can be queried: open ports, running applications, services, etc.

Can be focused by providing additional conditions or filters, providing results more relevant to a specific situation

- For example: All ports and services used by a specific asset or assets

Queries

Results can be returned in a number of ways:

- In delimited text files,
- Via a graphical user interface or dashboard,
- Via pre-formatted executive reports,
- Via an alert that is delivered by text or e-mail, etc.

Defining function of an SIEM is to correlate events to find larger incidents

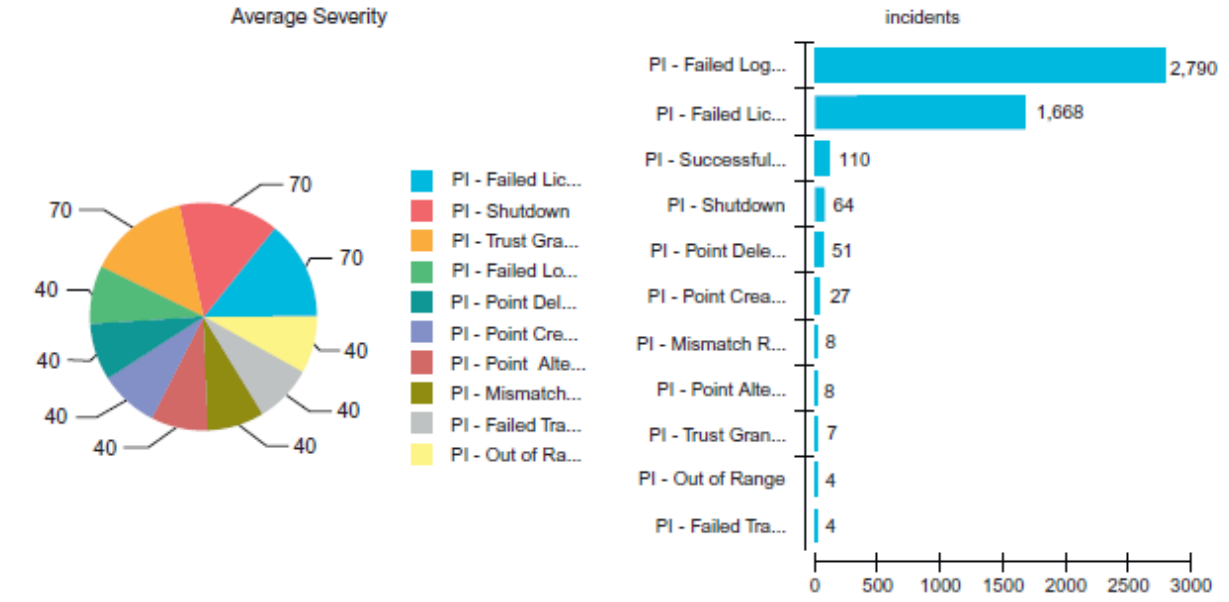
- The ability to both define correlation rules, as well as present the results via a dashboard
  - HTTP command and control

Reports

Organize and format all relevant data from the enriched logs and events (any data set) into a single document

Industrial Incidents
Report Generated: Mar 4, 2011 1:57 PM
Time Zone: Greenwich Mean Time: Dublin Edinburgh, Lisbon, London GMT+00:00
Report Period 2011/01/01 00:00:00 to 2011/04/01 00:00:00
Device Count:49

Incident Overview



Alerts

Active responses to observed conditions within SIEM

- Visual notification in a console or dashboard
- Direct communications (e-mail, page, text message, etc.) to a security administrator
- Execution of a custom script

Incident Investigation and Response

SIEM are useful for incident response;

- The structure and normalization of the data allows an incident response team to drill into a specific event to find additional details (often down to the source log file contents and/or captured network packets), and to pivot on specific data fields to find other related activities

Activities;

- Allowing direct control over switch or router interfaces via SNMP, to disable network interfaces
- Executing scripts to interact with devices within the network infrastructure, to re-route traffic, isolate users, etc.
  - Also with perimeter security devices (e.g., firewalls) to block subsequent traffic (i.e., malicious)
- Execute scripts to alter or disable a user account in response to observed malicious behavior

Log Storage and Retention

Security monitoring, log collection, and enrichment => a large quantity of data in the form of log files, which must be stored for audit and compliance purposes

- In the cases where direct monitoring is used in lieu of log collection, the monitoring device will still produce logs, which must still be retained

A few challenges;

- How to ensure the integrity of the stored files (a common requirement for compliance)
- How and where to store these files
- How they can be kept readily available for analysis

Nonrepudiation

Log file has not been tampered with

- The original raw log file can be presented as evidence, without question of authenticity, within a court of law

Can be achieved in several ways;

- Digitally signing log files upon collection as a checksum,
- Utilizing protected storage media,
- Use of third-party File Integrity Monitoring (FIM) systems

Digital Signature

Typically provided in the form of a **hash algorithm** that is calculated against the log file at the time of collection

The result provides a checksum against which the files can be verified to ensure they have not been tampered with:

- If the file is altered in any way, the hash will calculate a different value and the log file will fail the integrity check
- If the checksum matches, the log is known to be in its original form

Protected Storage and FIM

An example; By using Write Once Read Many (WORM) drives, raw log records can be accessed but not altered, as the write capability of the drive prevents additional saves

- Many managed storage area network (SAN) systems also provide varying levels of authentication, encryption, and other safeguards

FIM; observes the log storage facility for any sign of changes or alterations, providing an added level of integrity validation

Data Retention/Storage

How much data are we talking about?

- 170 GB over an 8-hour period for a medium-sized enterprise

What to and how long to store?

- Identifying the quantity of inbound logs
- Determining the average log file size
- Determining the period of retention required for logs
- Determining the supported file compression ratios of the Log Management or SIEM platform being used