

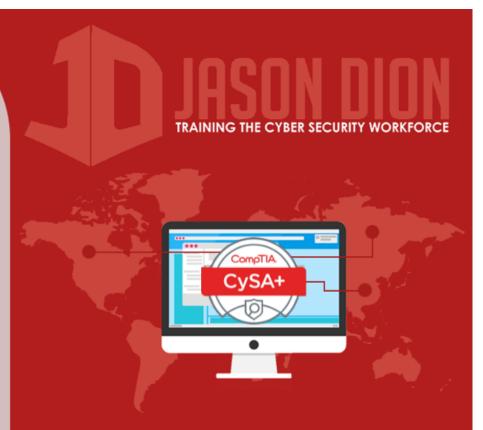


System and Host Log Files

THREAT MANAGEMENT

Host/Server Log Files

- System logs are collected by the system
- Useful for troubleshooting and reconstructed a cyber attack
- Log files provide information on system configuration, applications, and user accounts
- You have to have system access to get these logs, though



Windows System Log Types

- Application logs
 - Logged by programs/applications
- Security logs
 - Records login events, resource usage, files created/open/deleted, etc.
- Setup logs
 - Records application setup actions
- System logs
 - Events from Windows components
- ForwardedEvents logs
 - -Event subscriptions from remote computers





Linux System Logs

/var/log directory

 Other applications may store their own log files elsewhere

