8_Documentation_Standards

What to Learn

Documentation ensures SOC activities are properly recorded for compliance, learning, and evidence in investigations.

Analysts must follow consistent standards in documenting incidents, alerts, and escalations.

Clear documentation is vital for forensic analysis and organizational transparency.

How to Learn

Review templates and guidelines used in industry-standard SOC documentation.

Practice creating incident tickets and after-action reports.

Seek feedback on clarity and completeness from peers or mentors.

Example / Use-Case

When documenting a phishing incident, the analyst records the suspicious email details, investigation findings, actions taken, and preventive recommendations. This record can later be used for awareness training.