# CYBER SECURITY PROCESSES

# Cyber Security Processes

*When architecting a solution, the people responsible for managing the solution should be considered*

# Cyber Security Processes

- Incident Response
- Audit & Reporting
- Risk Management

# Incident Response Frameworks

- NIST 800-61
- CERT
- ISACA

# Incident Response

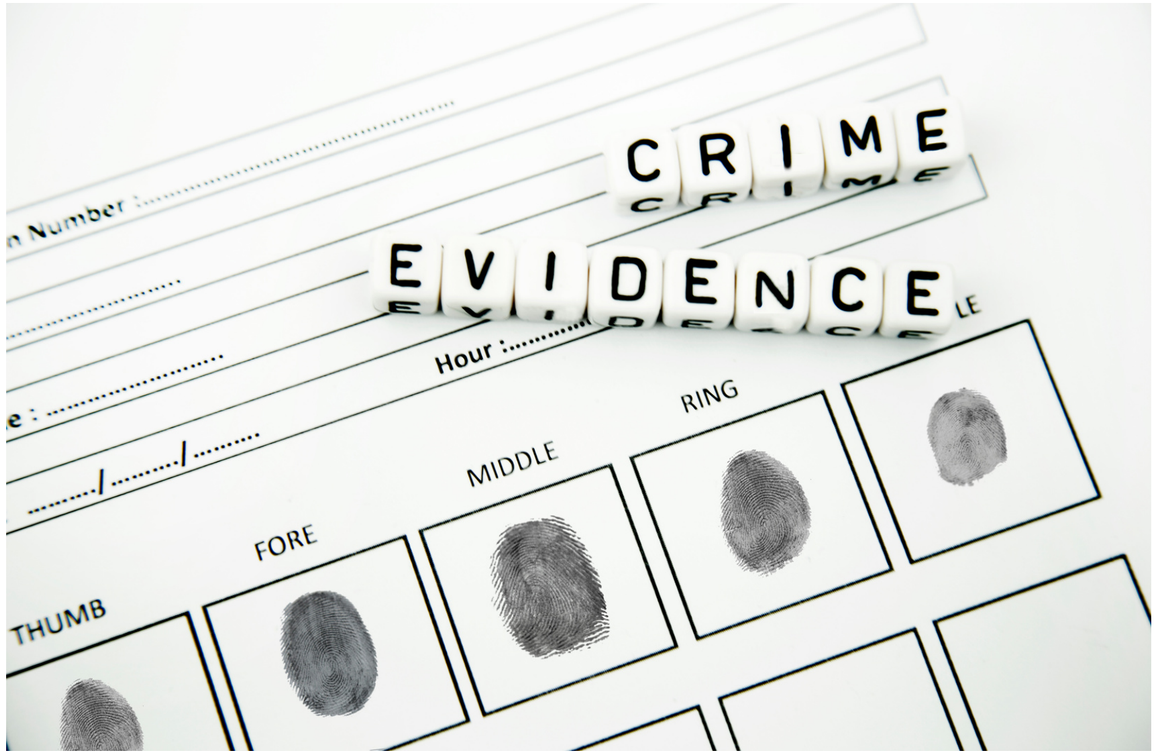
Systems must be designed to support the organization's ability to respond to security incidents as quickly as possible.

# Incident Response Architecture Considerations

Is there sufficient logging to help the incident responder rebuild the steps up to the incident?

# Incident Response Architecture Considerations

Can enough evidence be provided for investigations such as logs and snapshots?



# Incident Response Architecture Considerations

Can the logs be easily parsed?

# Incident Response Architecture Considerations

Where are the logs stored?
Locally or in a central repository?

# Incident Response Architecture Considerations

Longevity of the logs


# Auditing & Reporting Architecture Considerations

Is there a corporate board these reports need to be sent to?

# Auditing & Reporting Architecture Considerations

Is the industry the organization is in highly regulated?

# Auditing & Reporting Architecture Considerations

What are the audit requirements for the organization?