THE ROLES WITHIN A CYBER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

Lead investigator:
Like a forensic detective, this person analyses evidence from the attack to determine the cause.

Team leader:
Oversees and manages all incident response activities.

Legal:
Support with any potential regulatory and legal issues arising from the event.

Communications:
Responsible for communications about the incident internally and with third parties.

Finance:
Assist by releasing funds and resources as needed to respond to an incident.

Analysts:
Support the investigator in understanding the incident, remediation and minimising further damage.

evalian