Cybersecurity

- Hand on activities
- Detecting and responding to attacks
- Monitoring and protecting network
- Investigating incidents
- Writing code to automate task

Program overview
- Core security concepts
- Security domain
- Network security
- Computing basics
- Assets threats and vulnerabilities
- Incident detection and response
- Python
- Find and apply for jobs

Foundation of cyber security

In course
- Define the field of security
- Recognize core skill and knowledge needed to become security a
- Identify how security attacks impact business operat
- Identify 8 security domain
- Define security framework and control

Skill set
- Communicating effectively
- Collaboration with other
- Identify threat risk and vulnerability
- Problem solving.

Raj
DATE / /
PAGE

What you'll learn
- Define security
- Job responsibilities
- Core skills of security analyst
- Value of security

Later in course
- Eight security domain
- Security framework and control
- Common tools and programming language

Cybersecurity : The practice of ensuring confidentiality integrity and availability of information by protecting network, devices people and data from unauthorized access or criminal exploitation exploitation

Threat actor : Any person or groups that presents a security risk.

Benefits of Security
- Protect against external and internal threats
- Meet regulatory compet compliance
- Maintains and improve business productivity
- Reduce expense
- Maintain brand Trust

Raj
DATE / /
PAGE

Jobs to look for after course

- Security analyst and specialist
- Cybersecurity analyst and specialist
- security operation centre (SOC) analyst
- Information security analyst

Security analyst

- Security analyst are responsible for monitoring and protecting information and system.

Responsibility

- Protecting computer and network systems
- Install prevention softwares
- Conducting periodic security audit

Terminology

- Compliance : Process of adhering to internal standard and external regulation and enable organizations to avoid fines and security breaches.

- Security framework : Are guidelines for building plans to help mitigate risk and threat to data and privacy.

- Security controls : are safeguards designed to reduce specific security risks. They are used with security framework to establish a strong security posture.

Raj
DATE / /
PAGE

Security posture : is an organization's ability to manage its defence of critical assets and data and react to change. A strong security posture leads to lower risk for org.

Internal Threat: can be a current or former employee, an external vendor or a trusted partner who poses a security risk. At times internal threat is accidental

Network security is the practice of keeping an organization network infrastructure secure from unauthorized access.

Cloud Security : Is the process of ensuring that assets stored in the ~~cloud~~ cloud are properly configured or set up correctly and access to those assets is limited to authorized ~~a~~ user.

Programming : Set of instruction for computer to execute task. Consider :
- Automation of repetitive task
- Reviewing web traffic
- Alerting suspicious activity.