Hi There,

We appreciate your interest in learning Cyber Security from our institute STRUGGLERNOOB. You are on the right track.

You Are Now Way AHEAD OF OTHERS....6`bdca

Cyber Security has become a Paramount important sector, As the dependency on computers is increasing, as it's being used increasingly in every major sector like DEFENCE, AVIATION, SPACE, MEDICINE, INFRASTRUCTURE to name a few, the surface for cyber-attacks has increased significantly. Hence Cyber Security is Blooming as a CAREER.

Following are some key benefits of Pursuing Cyber Security:

Pursuing a career in cybersecurity offers numerous benefits, both professionally and personally. Here are some key advantages:

1. High Demand and Job Security:

- With the increasing number of cyber threats and the growing importance of protecting sensitive information, there is a high demand for cybersecurity professionals. This demand is expected to continue rising, providing excellent job security.

2. Competitive Salaries:

- **Cybersecurity roles often come with competitive salaries and benefits. Due to the high demand for skilled professionals and the critical nature of the work, employers are willing to offer attractive compensation packages, around 1-2 lakhs per Month.**

3. Diverse Career Opportunities:

- The field of cybersecurity offers a wide range of career paths, including roles such as security analyst, ethical hacker, security consultant, incident responder, and more. This diversity allows individuals to find a niche that suits their interests and skills.

4. Continuous Learning and Growth:

- Cybersecurity is a dynamic and evolving field. Professionals need to stay up to date with the latest threats, technologies, and best practices, which provides ongoing learning opportunities and keeps the work interesting and challenging.

5. Impactful Work:

- Cybersecurity professionals play a crucial role in protecting organizations, governments, and individuals from cyber threats. This work can have a significant positive impact, contributing to the safety and security of society.

6. Global Opportunities:

- Cybersecurity skills are in demand worldwide, offering opportunities to work in different countries and cultures. This global demand also allows for remote work opportunities, providing flexibility in terms of work location.

7. Interdisciplinary Nature:

- Cybersecurity intersects with various fields such as law, business, and technology, offering a multidisciplinary work environment. This can be intellectually stimulating and allows for collaboration with professionals from diverse backgrounds.

8. Job Satisfaction:

- Many cybersecurity professionals find their work rewarding due to the combination of problem-solving, continuous learning, and the opportunity to make a tangible difference in protecting assets and information.

9. Career Advancement:

- There are clear paths for career advancement in cybersecurity. With experience and additional certifications, professionals can move into senior and leadership positions, further enhancing their career prospects.

10. Contributing to National Security:

- For those working in government or defense sectors, a career in cybersecurity can provide a sense of pride and purpose by contributing to national security and protecting critical infrastructure.

Overall, a career in cybersecurity OFFERS STABILITY, GROWTH POTENTIAL, INTELLECTUAL ENGAGEMENT, and the opportunity to make a MEANINGFUL IMPACT.

Courses provided by STRUGGLERNOOB Cyber Security Institute.

1. Ethical Hacking
2. Cyber Security Analyst
3. SOC Analyst and EDR Tool

There are some Courses not mentioned here, feel free to reach out at +91 8871907507 to gather information.

What's included in above Courses:

1. Ethical Hacking:
    - a. Reconnaissance (Gather Intelligence on target)
        - i. Passive
            1. OSINT
            2. Domain and IP Address Information
            3. Metadata Analysis
            4. Public Network Information
            5. Search Engines and Online Tools
            6. Social Engineering
            7. Network Scanning (Passive)
            8. Third party data breaches
        - ii. Active
            1. Port Scanning
            2. Network Scanning
            3. Ping Sweeping
            4. Banner Grabbing

5. OS Fingerprinting
6. Traceroute
7. Wireless Scanning
8. Phishing

b. Weaponization (Creating Malware)
   - i. Create malware using Various frameworks
   - ii. Wrapper or Delivery Mechanism Preparation
   - iii. Packaging

c. Delivery (transportation of the Malware)
   - i. TeensyDANNY
   - ii. Phishing
   - iii. Malicious Attachments
   - iv. Malicious Links
   - v. Social Engineering
   - vi. Removable Media
   - vii. Network Injection
   - viii. Third-Party Services
   - ix. Instant Messaging and Social Networks
   - x. Remote Services

d. Exploitation (Exploit Vulnerability/Security misconfiguration)
   - i. Code Injection
   - ii. Cross-Site Scripting (XSS)
   - iii. Cross-Site Request Forgery (CSRF)
   - iv. Remote Code Execution (RCE)
   - v. Man-in-the-Middle (MitM)
   - vi. Phishing and Social Engineering
   - vii. Cryptographic Exploits
   - viii. Frameworks and Toolkits

e. Installation (Install desired software's)
   - i. Malware Installation
   - ii. Persistence Mechanisms
   - iii. Fileless Malware
   - iv. Exploitation of Legitimate Software
   - v. User Account Creation
   - vi. Backdoors
   - vii. Hooking and Injection
   - viii. Security Software Evasion
   - ix. Browser Extensions
   - x. Mobile Device Malwares

f. C2C (Setup Command and Control)
   - i. Network Protocols
   - ii. Custom Protocols
   - iii. Steganography
   - iv. Domain Generation Algorithms (DGAs)
   - v. Fast Flux and Double Flux
   - vi. Social Media and Web Services
   - vii. Peer-to-Peer (P2P) Networks
   - viii. Email and Messaging Services
   - ix. Fallback Channels
   - x. Command Obfuscation

g. Actions on objectives (Data Theft)

i. Data exfiltration: stealing sensitive data such as intellectual property, financial information, personal data.
ii. Data destruction: deleting or corrupting data to disrupt operations.
iii. Espionage: gathering intelligence and conducting surveillance.
iv. Sabotage: damaging systems or infrastructure.
v. Financial gain: conducting fraud, theft, or ransomware activities.
vi. Credential harvesting: obtaining usernames and passwords for further exploitation.

2. Cyber Security Analyst

a. Monitoring and Analyzing Security Alerts
   i. Task: Continuously monitor security systems (e.g., SIEM, IDS/IPS) for suspicious activities and alerts.
   ii. Action: Investigate and analyze security alerts to determine their nature and potential impact.

b. Incident Response
   i. Task: Respond to security incidents promptly to mitigate damage.
   ii. Action: Conduct initial triage, containment, eradication, and recovery processes. Document and report incidents.

c. Threat Intelligence and Analysis
   i. Task: Stay informed about current threat landscape and emerging threats.
   ii. Action: Analyze threat intelligence reports and apply findings to improve security posture. Disseminate relevant threat information within the organization.

d. Vulnerability Management
   i. Task: Identify, assess, and prioritize vulnerabilities in the organization's systems.
   ii. Action: Conduct regular vulnerability assessments and scans. Collaborate with IT teams to ensure timely patching and remediation.

e. Security Assessments and Audits
   i. Task: Perform security assessments and audits to evaluate the effectiveness of security controls.
   ii. Action: Conduct penetration testing, risk assessments, and compliance audits. Report findings and recommend improvements.

f. Security Policy Development and Enforcement
   i. Task: Develop and enforce security policies, procedures, and standards.
   ii. Action: Create and update security policies. Ensure compliance with regulatory requirements and internal standards.

g. User Training and Awareness
   i. Task: Educate employees on cybersecurity best practices and awareness.
   ii. Action: Develop and deliver training programs, conduct phishing simulations, and promote security awareness campaigns.

h. User Training and Awareness
   i. Task: Educate employees on cybersecurity best practices and awareness.
   ii. Action: Develop and deliver training programs, conduct phishing simulations, and promote security awareness campaigns.

i. Security Tool Management
   i. Task: Manage and maintain security tools and technologies.
   ii. Action: Configure, update, and monitor firewalls, antivirus software, intrusion detection systems, and other security tools.

j. Forensic Analysis
   i. Task: Conduct forensic investigations to determine the root cause of security incidents.
   ii. Action: Collect and analyze digital evidence. Preserve the integrity of evidence for potential legal proceedings.

k. Security Metrics and Reporting
   i. Task: Track and report on security metrics to management.

    ii. Action: Develop dashboards and reports to illustrate the effectiveness of security measures and identify areas for improvement.

l. Collaboration and Coordination

    i. Task: Work closely with other IT and business teams to ensure security is integrated across the organization.
    ii. Action: Participate in cross-functional teams, provide security expertise in projects, and coordinate with external partners and law enforcement when necessary.

m. Proactive Threat Hunting

    i. Task: Actively seek out potential threats that have evaded existing security measures.
    ii. Action: Use advanced techniques and tools to detect hidden threats within the network.

By performing these tasks, cybersecurity analysts play a crucial role in safeguarding an organization's digital assets and ensuring the overall security of its IT infrastructure.

STRUGGLER NOOB

StrugglerNOOB Cyber Security Institute
Mangla,besides Green garden Colony, Bilaspur
495001
+91 8839750722