KIET GROUP OF INSTITUTIONS
www.kiet.edu
Delhi-NCR, Ghaziabad
Connecting Life with Learning
Toll Free No.: 1800-1200-106
CELEBRATING 25 YEARS OF EXCELLENCE
CYBER PEACE CENTRE

October Edition, 2023

CYBER कवच

CYBER PEACE CENTRE

Trending Roles in the Domain of Cyber Security :

1. Cloud Security Architect: Organizations are increasingly migrating to the cloud, creating a growingneed for experts who can design and implement secure cloud environments. Cloud security architects focus on ensuring the confidentiality, integrity, and availability of data and applications hosted in cloud environments.

2. DevSecOps Engineer: DevSecOps integrates security practices into the DevOps process. DevSecOps engineers work to embed security into the software development lifecycle, automating security checks and aiding developers in building secure code from the outset.

3. Threat Hunter: Threat hunters proactively search for signs of malicious activity within an organization's network or systems. They employ advanced tools and techniques to identify and respond to threats that may have gone undetected by traditional security measures.

4. Data Privacy Officer (DPO): With the increasing importance of data protection regulations like GDPR and CCPA, DPOs are responsible for ensuring that an organization's data handling practices comply with relevant privacy laws. They also help implement data protection policies and respond to data breaches.

5. Security Operations Center (SOC) Analyst: SOC analysts monitor an organization's IT environment for security incidents, investigate alerts, and respond to threats. This role is crucial for identifying and mitigating cyber threats in real-time.

6. Incident Response Manager: Incident response managers coordinate the organization's response to security incidents and breaches. They play a pivotal role in managing the incident, containing the damage, and coordinating with relevant stakeholders.

8. AI and Machine Learning Security Expert: As AI and machine learning become more integral to cybersecurity, experts in this field focus on securing AI and ML algorithms, models, and data. They also use AI-driven tools for threat detection and analysis.

9. Red Teamer/Penetration Tester: Red teamers simulate cyberattacks on an organization's systems to identify vulnerabilities and weaknesses. They help organizations proactively strengthen their defenses by conducting controlled tests.

10. Compliance Auditor: Compliance auditors ensure that an organization complies with industryspecific regulations and standards, such as HIPAA, PCI DSS, or NIST. They assess and report on an organization's adherence to these requirements.

11. Blockchain Security Specialist: As blockchain technology gains wider adoption, specialists in blockchain security work to secure distributed ledger systems and associated applications, particularly in areas like cryptocurrencies and supply chain.

12. AI Ethics and Bias Analyst: With the use of AI in cybersecurity, professionals are needed to address ethical considerations and biases in AI algorithms and decision-making processes to ensure fairness and transparency.

Dr. Abhinav Juneja and **Dr. Arun K. Triphati**
Head Of Department [CSIT] Head Of Department [MCA]

Dark Web and Anonymity

The dark web is a part of the internet that is intentionally hidden and not indexed by traditional search engines like Google or Bing. It is a subset of the deep web, which includes all parts of the internet not indexed by search engines, such as private databases, password-protected websites, and more. What sets the dark web apart is that it is intentionally concealed and often associated with illegal activities and anonymity.

Anonymity: Users on the dark web often use special tools like Tor (The Onion Router) to access websites anonymously. This makes it difficult to trace their online activities and identity.
Hidden Websites: Websites on the dark web have ".onion" domain extensions and are not accessible through regular web browsers. They can only be accessed using Tor or similar anonymizing services.

Illicit Activities: While not all activity on the dark web is illegal, it is known for hosting a range of illegal activities, including the sale of drugs, firearms, stolen data, hacking services, and more.

Privacy and Security: Some users access the dark web for legitimate reasons, such as protecting their online privacy in countries with strict censorship or surveillance. Whistleblowers, journalists, and activists may also use it to communicate securely.

Risks: Exploring the dark web can be risky. There is a potential for encountering illegal content, scams, and cybercriminals. Law enforcement agencies actively monitor and investigate illegal activities on the dark web. It's important to note that not everything on the dark web is illegal or malicious, and it can have legitimate uses for privacy and security. However, individuals should exercise caution and be aware of the potential legal and security risks associated with accessing and interacting on the dark web.

KARTIKEYA SRIVASTAVA
PRESIDENT

CYBER PEACE CENTRE
CYBERकवच

Mitigating DDoS with Blockchain

DDoS attacks involve overwhelming a target server or network with an excessive volume of traffic, rendering it inaccessible to legitimate users. Attackers harness botnets, compromised devices, or amplification techniques to flood the target with traffic, leading to service disruptions and potential data breaches. Recent DDoS Insights Report confirms that cyberattacks and threats have surged 200% over the past year, with multiple industries irreversibly impacted.
DoS attacks involve overwhelming a target with a deluge of traffic, rendering it inaccessible to legitimate users. Conventional defenses rely on centralized servers, which can be overwhelmed themselves. Blockchain, on the other hand, operates on a decentralized network, making it significantly more resilient.

Blockchain's decentralized nature distributes traffic across a multitude of nodes, thwarting concentrated attacks. Its immutable record-keeping ensures the integrity of traffic data and prevents manipulation. Tokenization and smart contracts enable access control, allowing only authorized users to access resources.

During a DDoS attack, the bandwidth capacity of centralized servers is targeted by the attackers. As you may know, blockchain is decentralized. No database or other component of an IT infrastructure in a blockchain-based network will be at one particular location or under the control of a single administrator.

This decentralized nature enables blockchain-based cybersecurity tools to allocate data and bandwidth for mitigating the impact of a DDoS attack. Such decentralized tools create bandwidth for DDoS-generated traffic to use. This keeps important databases safe. Eventually, the DDoS attack will be weakened and controllable with firewall systems or anti-malware tools.

Real-world applications are already demonstrating the effectiveness of blockchain in DDoS mitigation. Decentralized Content Delivery Networks (CDNs) and token-based access mechanisms are bolstering resilience against attacks.

ADTIYA PANDEY
CORE MEMBER

CYBER PEACE CENTRE
CYBERकवच

Ransomware attacks

A Wake-Up Call for the Healthcare Industry
In July 2023, HCA Healthcare, one of the largest hospital operators in the United States, suffered a data breach that exposed the personal information of 11 million patients. The stolen data included names, addresses, phone numbers, emails, dates of birth, service dates, locations, and the dates of upcoming appointments.

HCA Healthcare has stated that the stolen data did not include Social Security numbers, payment information, or clinical information such as diagnoses. However, the breach is still a major concern for patients, as the stolen data could be used for identity theft, phishing attacks, and other types of fraud.

Colonial Pipeline Attack: A Ransomware Nightmare In March 2023, The Colonial Pipeline attack was carried out by a group known as DarkSide. The group used a ransomware attack to encrypt the Colonial Pipeline's systems and demand a ransom payment in exchange for the decryption key.
Colonial Pipeline initially resisted paying the ransom, but eventually decided to do so in order to restore service as quickly as possible. The company paid a ransom of 75 bitcoins, which was worth approximately $4.4 million at the time.

BMW Hack: A Teachable Moment for the Auto Industry In March 2023, BMW was the victim of a cyber attack, which resulted in the theft of sensitive customer data. The attack was carried out by a group of hackers known as RansomEXX, who demanded a ransom payment in exchange for the return of the data. BMW refused to pay the ransom, and the hackers released the data online.
The leaked data included customer names, addresses, phone numbers, and vehicle information. It also included some financial information, such as credit card numbers and bank account numbers. BMW has stated that it is working with law enforcement to investigate the attack and to protect its customers from fraud.

In the wake of the attack, BMW has taken a number of steps to improve its cybersecurity by implementing new security measures to protect its customer data, working with law enforcement to investigate the attack and to identify and apprehend the perpetrators, providing support to its customers who have been affected by the attack.

MAYANK KULSHRESHTA
CORE MEMBER

Secure Coding

Secure coding, the principle of designing code that adheres to code security best practices, safeguards and protects published code from known, unknown and unexpected vulnerabilities such as security exploits, the loss of cloud secrets, embedded credentials, shared keys,confidential business data and personally identifiable information (PII).

Some of the most commonly-seen technical attacks today, judging from the available literature, are buffer overflow attacks, exploitation of race conditions, and (in web applications) hidden field manipulation or parameter tampering. Later in this about how to develop defenses against these attacks is offered.

Hidden fields are often used in CGI scripts to save information about the client's session. This allows the normally stateless Web server to operate with a king of pseudo-state. The popular CGI.pm Perl package, for example, uses hidden fields to great effect. But it's possible for a malicious user to save a valid form, manipulate the hidden fields, then POST the modified form back to the server. This trick can devastate an application's security.

The buffer overflow vulnerability is difficult to characterize and define. There are many variations, but they essentially have some forms A program tries to copy some data from one object into another, does not check that the destination object is large enough to contain the source object, and uses a routine such as sprintf to do the copying.

Race conditions are also known as "time-of-check-to-time-of-use (TOCTTOU)" flaws. A subclass of TOCTTOU flaws, which we call TOCTTOU binding flaws, arise when object identifiers are fallaciously assumed to remain bound to an object. The archetypal TOCTTOU binding flaw in a privileged program on the UNIX operating system arises when a setuid to root program is to save data in a file owned by the user executing the program.

ADTIYA AGGRAWAL
CORE MEMBER

Networking in Cybersecurity

Data transfer on a network is a complex process that involves the transmission of digital information between devices or systems. This transfer is critical for modern communication, from sending emails and browsing websites to streaming videos and accessing cloud services. To understand how data is transferred on a network, it's essential to delve into the technical aspects of this process.

At its core, data transfer on a network relies on the principles of digital data representation and transmission. Data is typically organized into packets, which are discrete units of information. These packets contain both the data itself and control information, such as source and destination addresses, error-checking codes, and sequence numbers.

The physical layer of the network is responsible for converting the digital signals into physical signals, whether they are electrical voltages in wired networks or light pulses in optical fiber networks. These physical signals are transmitted through the network medium, whether it's copper cables, fiber-optic lines, or wireless radio waves.

Data transfer can occur over various types of networks, including local area networks (LANs), wide area networks (WANs), and the internet. Each type of network may have different technologies and protocols in place to facilitate data transfer, but the fundamental principles of packetization, addressing, and routing remain consistent.

In a network, various protocols govern data transfer. The Internet Protocol (IP) is one of the fundamental protocols that facilitates data transfer across the internet. IP ensures that data is properly addressed and routed to its destination. Other protocols, such as Transmission Control Protocol (TCP), provide reliability and ensure that data arrives in the correct order.

RIYA SINGHAL
CORE MEMBER

CYBER PEACE CENTRE

CYBERकवच

Ways to Prevent from CyberCrimes:

Do's

- Use Strong, Unique Passwords:
- Enable Multi-Factor Authentication (MFA)
- Keep Software Updated
- Educate Yourself and Others
- Use Secure Wi-Fi Connections:
- Employ Antivirus and Antimalware Software
- Regularly Backup Data
- Secure Your Social Media Profiles
- Practice Safe Online Shopping and Banking

Dont's

- Don't Use Weak Passwords
- Don't Share Passwords
- Don't Ignore Software Updates
- Don't Click on Suspicious Links:
- Don't Ignore Phishing Emails
- Don't Overshare Personal Information
- Don't Neglect Privacy Settings
- Don't Install Unauthorized Software
- Don't Use Public Computers for Sensitive Tasks
- Don't Ignore Red Flags

Help-Line : +91-9520869485

CYBER PEACE CENTRE

CYBERकवच

DSCI : Data Security Council of India, Delhi

15th edition of its Best Practices Meet (BPM 2023) in Delhi on August 22-23, 2023 hosted by DSCI.
DSCI Best Practices Meet (BPM) focuses on the contemporary evolution of security by organising its content and deliberations under a dominant theme.

The Hackers Meetup, Delhi

The event aims to bring together primarily security researchers, hackers, business leaders, entrepreneurs but also includes practitioners from academia, industry, government organizations as well as students to elaborate and discuss the IT Security challenges that we are facing today and also about the next generation computer security issues.

National Digital Summit 2023, Delhi

Confederation of India Industry (CII) is organising the **National Digital Summit 2023** with theme "**India-Digital Frontier to the World**" on **October 5, 2023**, from **9:30 AM to 2:00 PM** at **Jacaranda Hall, India Habitat Centre (IHC), New Delhi.**

WEB3 Builder Hackathon, DTU

The concept of the hackathon is to foster innovation and creativity in the web3 space. In Web3 hackathon our team created a secured network based on blockchain. Which provide Secured ecosystem for data transfer