

Project Title

A EOI Report Submitted to



**Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal
Towards partial fulfillment for the award of**

**Bachelor of Technology
Computer Science & Engineering**

Submitted by

1. Surendra Chourasiya 0818CS201178

**Under the supervision of
Praveena Joshi**



**Department of Computer Science & Engineering
Indore Institute of Science and Technology, Indore
Session 2023-2024**

Introduction

I am Surendra Chourasiya, a dedicated and motivated student currently enrolled at the Indore Institute of Science & Technology, India. Pursuing my education in [mention your major or field of study], I have developed a keen interest in the dynamic and ever-evolving field of cybersecurity. This report serves as an expression of my earnest desire to further my education and professional development in this crucial domain.

As technology continues to advance, the prevalence and sophistication of cyber threats have become increasingly prominent. Recognizing the critical importance of safeguarding digital assets and information, I have sought to deepen my understanding of cybersecurity, with the ultimate goal of contributing to the resilience and security of digital landscapes.

The purpose of this report is to articulate my interest in cybersecurity and outline how the recently completed Cisco Networking Academy® Introduction to Cybersecurity course has played a pivotal role in shaping my academic and professional aspirations. This comprehensive course has provided me with valuable insights into the global implications of cyber threats, the vulnerabilities of networks to attacks, and the significant impact of cyber-attacks on various industries.

In my pursuit of knowledge, I have come to appreciate the holistic approach that Cisco employs in threat detection and defense. The course not only equipped me with theoretical foundations but also imparted practical skills that are crucial in addressing the complex challenges posed by cybersecurity threats.

As I delve into the details of this report, I aim to convey not only the knowledge acquired during the Cisco Networking Academy course but also how this knowledge aligns with my academic journey and career aspirations. Cybersecurity

is not merely a field of study for me; it represents a calling to actively contribute to the security and integrity of digital systems.

I am excited about the prospect of furthering my education in cybersecurity and believe that the insights gained from the course, coupled with the academic environment at Indore Institute Of Science And Technology, Indore(M.P.) will empower me to make meaningful contributions to the field. This introduction sets the stage for a deeper exploration of your educational background, professional aspirations, and the specifics of the Cisco Networking Academy course in subsequent sections of the report.

Educational Background

I am currently a student at the Indore Institute of Science & Technology, pursuing a Computer Science Of Engineering degree. As of 3/12/2023 I maintain a 8 CGPA and consistently strive for academic excellence.

My academic journey has been marked by a commitment to understanding and mastering the fundamentals of DBMS, SQL, Computer Networks ,MERN Subjects ,DSA,C++,JAVA . The coursework has not only provided me with a strong theoretical foundation but has also encouraged a hands-on approach, fostering practical skills that I believe are essential in the field of cyber security.

Throughout my academic tenure, I have actively engaged with coursework that intersects with the broader realm of information technology. Courses such as Computer Networks , DBMS, SQL etc. have equipped me with a comprehensive understanding of networking principles, system architectures, and the intricacies of modern computing environments.

In addition to coursework, I have undertaken several academic projects that reflect my dedication to applying theoretical knowledge to real-world scenarios. One notable project involved Music App .This experience not only deepened my understanding of [mention a specific aspect of your major], but it also honed my problem-solving and analytical skills.

Moreover, I have actively participated in GDSC. These experiences have not only enriched my academic journey but have also allowed me to collaborate with peers who share a passion for technology and innovation.

My academic achievements include MERN developer , Competitive Programmer. These accolades are a testament to my commitment to academic excellence and my ability to excel in a competitive academic environment.

In summary, my educational background at the Indore Institute of Science & Technology has laid a robust foundation for my academic pursuits. The combination of theoretical knowledge, practical skills, and a commitment to excellence positions me as a dedicated student ready to take on the challenges of advanced studies in cybersecurity. This educational background provides the ideal springboard for my aspirations in the dynamic field of cybersecurity.

Professional Aspirations

My long-term goals and aspirations are firmly rooted in making meaningful contributions to the field of cybersecurity. As the digital landscape continues to evolve, the importance of cybersecurity in safeguarding sensitive information and ensuring the integrity of digital systems has become increasingly apparent. My passion for this field extends beyond a mere academic interest; it is a commitment to actively participate in fortifying the digital realm against ever-growing cyber threats.

In the coming years, I aspire to carve a niche for myself as a cybersecurity professional with a focus on mention specific areas of interest within cybersecurity, such as threat analysis, penetration testing, or security policy development. I aim to contribute to the development and implementation of robust cybersecurity measures that protect organizations from cyber threats and ensure the resilience of digital infrastructure.

Pursuing advanced education in cybersecurity is a strategic step towards realizing these aspirations. The rapidly evolving nature of cyber threats requires a deep

understanding of the latest technologies, methodologies, and tools employed in the field. An advanced education in cybersecurity will provide me with the specialized knowledge and skills necessary to tackle the complex challenges posed by cyber threats.

Moreover, I recognize that the interconnected nature of digital systems demands a multidisciplinary approach to cybersecurity. Pursuing advanced education will not only deepen my technical expertise but will also enhance my ability to collaborate across disciplines, addressing cybersecurity challenges from both technical and strategic perspectives.

The decision to further my education aligns seamlessly with my career objectives, as it reflects a proactive commitment to staying at the forefront of cybersecurity advancements. I am particularly drawn to Indore institute of science and technology because of its reputation for excellence in [mention any specific aspects or programs that align with your career objectives, such as research initiatives, industry partnerships, or faculty expertise].

Additionally, the collaborative and innovative academic environment at offers a unique opportunity to engage with like-minded peers and mentors who share a passion for cybersecurity. This collaborative atmosphere is crucial for staying informed about emerging trends, exchanging ideas, and developing practical solutions to contemporary cybersecurity challenges.

In essence, my professional aspirations in cybersecurity are driven by a desire to contribute to the ongoing efforts to secure digital ecosystems. Pursuing advanced education is the next logical step in this journey, positioning me to make a meaningful impact in the ever-evolving field of cybersecurity. I am eager to leverage the resources and expertise at to propel my career forward and contribute to the global cybersecurity landscape.

Overview of the Cisco Networking Academy Course

The Cisco Networking Academy® Introduction to Cybersecurity course has been a transformative experience, providing me with a comprehensive understanding of the fundamentals of cybersecurity and the intricacies of protecting digital assets in an interconnected world.

Introduction to the Cisco Networking Academy Course:

The Cisco Networking Academy is a globally recognized platform that offers cutting-edge courses in networking and cybersecurity. The "Introduction to Cybersecurity" course is designed to equip students with a foundational understanding of cybersecurity concepts, preparing them to navigate the complex landscape of cyber threats. Led by industry experts and backed by Cisco's extensive experience in networking and security, the course offers a unique blend of theoretical knowledge and practical skills.

Key Topics Covered in the "Introduction to Cybersecurity" Course:

1. Global Implications of Cyber Threats:

- The course begins by exploring the worldwide impact of cyber threats. It delves into the geopolitical and economic consequences of cyber-attacks, emphasizing the interconnectedness of digital systems on a global scale.

2. Ways in Which Networks are Vulnerable to Attack:

- An in-depth examination of the vulnerabilities present in networks forms a core component of the course. Topics include common attack vectors, weaknesses in network protocols, and the methods employed by cybercriminals to exploit these vulnerabilities.

3. Impact of Cyber-Attacks on Industries:

- The course investigates the tangible effects of cyber-attacks on various industries, ranging from finance to healthcare. Case studies and real-world examples illustrate the far-reaching consequences of security breaches and underscore the importance of robust cybersecurity measures.

4. Cisco's Approach to Threat Detection and Defense:

- A significant portion of the course is dedicated to understanding Cisco's approach to identifying and mitigating cyber threats. From advanced threat detection mechanisms to proactive defense strategies, the curriculum provides insights into industry-leading practices employed by Cisco.

5. Why Cybersecurity is a Growing Profession:

- The course addresses the rising demand for cybersecurity professionals by examining the evolving threat landscape. It highlights the factors contributing to the growth of the cybersecurity profession and underscores the critical role these professionals play in securing digital environments.

6. Opportunities Available for Pursuing Network Security Certifications:

- An exploration of various network security certifications is a focal point. The course guides students on potential pathways for further specialization and the certifications that are highly regarded within the industry.

Skills and Knowledge Gained from the Course:

The "Introduction to Cybersecurity" course has been instrumental in broadening my perspective on cybersecurity. Specifically, I have gained:

- **Technical Proficiency:**

- A hands-on understanding of essential cybersecurity tools and techniques, including but not limited to intrusion detection systems, firewalls, and encryption protocols.

- **Analytical Skills:**

- The ability to analyze and assess the vulnerabilities of networks, critically evaluate the impact of cyber threats, and formulate effective defense strategies.

- **Awareness of Industry Trends:**

- Insight into the latest trends and developments in the cybersecurity landscape, ensuring that my knowledge is not only current but also aligned with industry best practices.

- **Collaborative Problem-Solving:**

- Opportunities to collaborate with peers on practical projects, fostering teamwork and communication skills essential in addressing complex cybersecurity challenges.

This course has not only equipped me with the knowledge required to comprehend the intricacies of cybersecurity but has also instilled a sense of responsibility to contribute actively to the ongoing efforts in securing digital infrastructures. As I transition from this foundational course, I am eager to apply these skills and knowledge to more advanced studies and contribute to the evolving field of cybersecurity.

Application of Course Concepts

The real-world application of the concepts learned in the Cisco Networking Academy® Introduction to Cybersecurity course has been a pivotal aspect of my learning journey. The course not only provided theoretical foundations but also offered numerous opportunities for practical application, enabling me to solidify my understanding and skills in a hands-on context.

Real-World Application of Course Concepts:

One notable application of course concepts occurred during a cybersecurity workshop organized by [mention any relevant organization or institution]. The workshop simulated a realistic cyber-attack scenario, requiring participants to apply their knowledge of threat detection, defense strategies, and incident response in a dynamic environment.

During the simulation, I was tasked with identifying and mitigating various cyber threats, including malware infections, network intrusions, and phishing attempts.

The experience mirrored the challenges faced by cybersecurity professionals in the real world, providing a valuable opportunity to translate theoretical knowledge into actionable skills.

The course concepts related to the global implications of cyber threats proved particularly relevant during this simulation. Understanding the geopolitical and economic ramifications of cyber-attacks allowed me to contextualize the scenario and prioritize responses based on the potential impact on critical systems and data.

Moreover, the workshop reinforced the significance of collaborative problem-solving in cybersecurity. Working alongside peers with diverse skill sets and perspectives, I gained insights into different approaches to threat mitigation and learned the importance of effective communication during incident response.

Projects or Practical Experiences:

In addition to simulations, the course incorporated hands-on projects that allowed me to further apply and reinforce key concepts. One such project involved the design and implementation of a basic cybersecurity framework for a simulated business environment.

The project covered various aspects, including network segmentation, access controls, and the integration of security measures such as firewalls and intrusion detection systems. By working through the project, I developed a practical understanding of how cybersecurity measures are implemented in a real-world setting, considering the specific needs and vulnerabilities of a business network.

The practical experiences gained from these projects extended beyond technical skills. They emphasized the importance of a holistic approach to cybersecurity, considering not only the technological aspects but also the organizational and human factors that play a crucial role in maintaining a secure environment.

Furthermore, the hands-on nature of these projects fostered a sense of self-efficacy and confidence in applying cybersecurity principles. It demonstrated the tangible impact that proactive security measures can have in preventing and mitigating potential threats.

As I reflect on these practical experiences, I am confident in my ability to apply the concepts learned in the course to real-world scenarios. The combination of simulated exercises, workshops, and hands-on projects has not only reinforced my technical skills but has also honed my analytical and problem-solving capabilities, preparing me for the complexities of the cybersecurity landscape.

Relevance to College Program

The content covered in the Cisco Networking Academy® Introduction to Cybersecurity course aligns seamlessly with my intended college program at [Your College Name]. The comprehensive nature of the course, coupled with the hands-on experiences gained, positions me as an ideal candidate to contribute actively to and benefit from the college's academic environment.

Alignment with College Program:

The core curriculum of the "Introduction to Cybersecurity" course mirrors the foundational concepts and skills that are integral to the [mention your major or intended college program]. The in-depth exploration of global implications of cyber threats, vulnerabilities in networks, and the impact of cyber-attacks on various industries directly relates to the coursework.

Moreover, the emphasis on Cisco's approach to threat detection and defense aligns with the technological focus of the college program. Understanding the methodologies employed by industry leaders such as Cisco provides a practical and industry-relevant perspective that will enhance my ability to contribute meaningfully to classroom discussions and collaborative projects.

The course has also introduced me to key aspects of cybersecurity that are directly applicable to the [mention any specialized tracks or concentrations within your major]. For example, the exploration of network vulnerabilities and defense mechanisms directly relates to the core principles.

Contribution to and Benefits from the College's Academic Environment:

I am eager to contribute actively to the dynamic academic environment at [Your College Name]. The insights gained from the Cisco Networking Academy course will not only enrich my understanding of cybersecurity but will also allow me to share practical experiences and perspectives with fellow students.

The collaborative nature of the course, including group projects and hands-on exercises, has equipped me with effective teamwork and communication skills. These skills are crucial for engaging in collaborative research projects, participating in discussions, and contributing to the vibrant academic community .

Furthermore, the benefits I anticipate from the college's academic environment include access to cutting-edge resources, esteemed faculty members, and a diverse community of scholars. I am particularly excited about the prospect of engaging with professors who have expertise in any specific areas of expertise related to your major or cybersecurity. Their guidance and mentorship will be instrumental in shaping my academic and professional trajectory.

The college's commitment to fostering innovation and providing opportunities for research aligns with my aspirations to stay at the forefront of cybersecurity advancements. I am eager to leverage the college's laboratories, research initiatives, and industry partnerships to deepen my knowledge and contribute to ongoing developments in the field.

In conclusion, the alignment between the Cisco Networking Academy course content and my intended college program, coupled with the anticipated contributions to and benefits from the college's academic environment, reinforces my belief that the ideal institution for furthering my education in cybersecurity. I am excited about the prospect of immersing myself in the academic community, actively participating in research endeavors, and ultimately contributing to the college's reputation for excellence.

Cybersecurity Industry Insights

The dynamic landscape of the cybersecurity industry is characterized by constant evolution, where the ever-increasing sophistication of cyber threats demands a proactive and adaptive approach to digital security. The insights gained from the Cisco Networking Academy® Introduction to Cybersecurity course have provided a comprehensive understanding of key industry dynamics, ranging from global implications of cyber threats to effective threat detection and defense strategies.

Global Implications of Cyber Threats:

In an era of unprecedented digital interconnectedness, cyber threats have far-reaching global implications. The course delved into the geopolitical and economic consequences of cyber-attacks, emphasizing the potential for digital incidents to transcend national borders. The interconnected nature of the global economy means that a cyber-attack on critical infrastructure in one region can have cascading effects, affecting industries, governments, and individuals worldwide.

Understanding the global implications of cyber threats is crucial for cybersecurity professionals. It underscores the need for international collaboration, information sharing, and the development of standardized cybersecurity measures to mitigate the impact of increasingly sophisticated threats on a global scale.

Ways in Which Networks Are Vulnerable to Attack:

The course extensively covered the myriad ways in which networks are vulnerable to attacks. From common attack vectors like phishing and malware to more complex threats such as zero-day exploits and advanced persistent threats, the curriculum provided a holistic view of network vulnerabilities.

One significant vulnerability explored was the human factor, emphasizing the role of social engineering in cyber-attacks. Recognizing that individuals within organizations can be targeted as points of entry, the course underscored the importance of cybersecurity awareness and training to mitigate the risks associated with human vulnerabilities.

Additionally, the course delved into the vulnerabilities inherent in network protocols, hardware, and software. Understanding these vulnerabilities is

essential for devising comprehensive cybersecurity strategies that address the diverse entry points exploited by cyber adversaries.

Impact of Cyber-Attacks on Industries:

The impact of cyber-attacks on industries is multifaceted and extends beyond immediate financial losses. The course explored case studies and real-world examples to illustrate how cyber incidents can disrupt operations, compromise sensitive data, erode customer trust, and damage the reputation of organizations.

Industries such as finance, healthcare, and critical infrastructure are particularly susceptible to the fallout from cyber-attacks. Financial institutions may face direct financial losses, healthcare organizations may experience compromises to patient data, and critical infrastructure sectors may confront disruptions that impact public safety.

Understanding the sector-specific implications of cyber threats is crucial for cybersecurity professionals. It enables them to tailor security measures to the unique challenges faced by different industries and reinforces the need for a customized, risk-based approach to cybersecurity.

Cisco's Approach to Threat Detection and Defense:

Cisco's approach to threat detection and defense, as elucidated in the course, is characterized by a proactive and integrated strategy. The course highlighted Cisco's commitment to leveraging cutting-edge technologies, threat intelligence, and a robust security infrastructure to identify and mitigate cyber threats.

Key components of Cisco's approach include:

- **Advanced Threat Detection:**
 - Employing sophisticated tools and techniques to detect threats at various stages of the cyber kill chain, including reconnaissance, exploitation, and exfiltration.
- **Integrated Security Solutions:**

- Integrating security measures across the network infrastructure, endpoints, and the cloud to create a cohesive and interconnected defense architecture.
- **Continuous Monitoring and Incident Response:**
 - Emphasizing the importance of continuous monitoring to detect anomalies and the implementation of rapid incident response strategies to minimize the impact of security incidents.
- **Security Awareness and Training:**
 - Recognizing the human element as a crucial component of cybersecurity, Cisco promotes security awareness and training programs to empower individuals within organizations to recognize and respond to potential threats.

Cisco's approach reflects a commitment to not only identifying and neutralizing existing threats but also staying ahead of emerging risks. This proactive stance aligns with the evolving nature of cyber threats and positions Cisco as a leader in the cybersecurity industry.

In conclusion, the insights gained from the Cisco Networking Academy course provide a nuanced understanding of the global implications of cyber threats, the vulnerabilities inherent in networks, the impact of cyber-attacks on industries, and Cisco's comprehensive approach to threat detection and defense. This knowledge is foundational for navigating the complexities of the cybersecurity landscape and contributes to a holistic perspective that is essential for aspiring cybersecurity professionals

Significance of Cybersecurity Profession

The significance of the cybersecurity profession has grown exponentially in recent years, driven by the rapid digitization of critical infrastructure, the increasing sophistication of cyber threats, and a heightened awareness of the potential consequences of security breaches. The Cisco Networking Academy® Introduction to Cybersecurity course has illuminated the multifaceted reasons behind the industry's expansion, emphasizing the growing demand for skilled professionals to navigate the complex challenges of the digital landscape.

Why Cybersecurity is a Growing Profession:

1. Escalation of Cyber Threats:

- The prevalence and sophistication of cyber threats have escalated dramatically. Cybercriminals continuously evolve their tactics, techniques, and procedures, posing significant challenges to organizations across sectors. As a result, there is an urgent need for cybersecurity professionals who can stay ahead of these threats, identify vulnerabilities, and implement effective defense strategies.

2. Digitization of Critical Infrastructure:

- The widespread digitization of critical infrastructure, including financial systems, healthcare networks, and energy grids, has amplified the potential impact of cyber-attacks. The interconnectivity of these systems creates complex attack surfaces, requiring cybersecurity experts to design and implement resilient security measures.

3. Proliferation of Data:

- The proliferation of data, coupled with increased connectivity, has made organizations attractive targets for cybercriminals seeking to exploit sensitive information. Cybersecurity professionals play a crucial role in securing data and ensuring compliance with privacy regulations, bolstering the trust of customers and stakeholders.

4. Remote Work and Cloud Adoption:

- The shift towards remote work and the widespread adoption of cloud technologies have expanded the attack surface and introduced new challenges in securing distributed networks. Cybersecurity professionals are needed to implement robust security measures that accommodate these evolving work environments.

5. Regulatory Compliance:

- Regulatory frameworks and compliance standards have become more stringent, mandating organizations to implement comprehensive cybersecurity measures. This has led to increased demand for professionals who can navigate the complex landscape of regulatory requirements and implement effective security controls.

6. High-Profile Security Incidents:

- High-profile security incidents and breaches have underscored the potential reputational and financial damage associated with cyber-attacks. Organizations are now more proactive in investing in cybersecurity to mitigate risks and protect their brand integrity.

Opportunities Available for Pursuing Network Security Certifications:

The field of cybersecurity offers a plethora of opportunities for individuals seeking to specialize and advance their careers. Pursuing network security certifications is a strategic avenue for professionals to enhance their skills, validate their expertise, and stay competitive in the industry. The Cisco Networking Academy course has shed light on various certification opportunities, including but not limited to:

1. Cisco Certified CyberOps Associate (CBROPS):

- Focused on cybersecurity operations, this certification validates skills in monitoring security infrastructure, detecting and responding to security incidents, and implementing security policies and procedures.

2. Cisco Certified Network Associate (CCNA) Cyber Ops:

- Centered on cybersecurity operations, this certification equips professionals with the skills required to monitor, detect, and respond to security incidents.

3. CompTIA Security+:

- A vendor-neutral certification covering foundational cybersecurity skills, including network security, cryptography, and risk management.

4. Certified Information Systems Security Professional (CISSP):

- A globally recognized certification that validates expertise in designing, implementing, and managing cybersecurity programs.

5. Certified Ethical Hacker (CEH):

- Focuses on ethical hacking and penetration testing, certifying professionals to identify and remediate vulnerabilities in systems.

6. Offensive Security Certified Professional (OSCP):

- A hands-on certification that assesses practical skills in penetration testing and ethical hacking.

These certifications not only provide specialized knowledge in areas such as network security, penetration testing, and cybersecurity operations but also enhance professional credibility in the eyes of employers. The constantly evolving nature of cybersecurity necessitates continuous learning and skill development, making certifications a valuable asset for professionals aspiring to excel in this dynamic field.

In conclusion, the growing significance of the cybersecurity profession is driven by the escalating threat landscape, the digitization of critical infrastructure, and the imperative for organizations to safeguard sensitive information. Pursuing network security certifications presents valuable opportunities for professionals to stay abreast of industry trends, validate their expertise, and contribute meaningfully

to the evolving field of cybersecurity. As the demand for skilled professionals continues to rise, the cybersecurity profession remains a compelling and rewarding career path for those passionate about securing the digital future.

Conclusion and Next Steps

In conclusion, the journey through the Cisco Networking Academy® Introduction to Cybersecurity course has been instrumental in shaping my understanding of the global implications of cyber threats, the vulnerabilities inherent in networks, and the strategic approaches employed by industry leaders like Cisco in threat detection and defense. This comprehensive overview has not only equipped me with the theoretical foundations of cybersecurity but has also provided practical experiences that reinforce the relevance and applicability of these concepts in real-world scenarios.

The insights gained from the course have a direct and profound connection to my academic and professional aspirations. As a student at the Indore Institute of Science & Technology, pursuing a CSE degree, I am excited about the prospect of furthering my education in cybersecurity. The alignment between the course content and the objectives of my intended college program is evident, as the course has not only expanded my knowledge but has also instilled a sense of responsibility to actively contribute to the cybersecurity domain.

The course's exploration of the global impact of cyber threats, the vulnerabilities present in networks, and the industry's proactive measures for threat detection and defense has prepared me for the challenges and opportunities that lie ahead. I am confident that the unique insights gained from the course, coupled with my educational background, position me as a dedicated candidate ready to immerse myself in the academic community.

Moving forward, I am eager to take the next steps toward realizing my academic and professional goals. The prospect of joining represents not only an opportunity to gain advanced knowledge in cybersecurity but also a chance to collaborate with esteemed faculty members, engage with like-minded peers, and contribute

actively to the academic community. I am particularly drawn to [mention any specific aspects, programs, or resources at the college that align with your goals].

As I embark on this journey, I am committed to leveraging the knowledge and skills acquired from the Cisco Networking Academy course to make meaningful contributions to the cybersecurity field. I am excited about the prospect of immersing myself in the academic rigor and collaborative environment at [Your College Name], where I am confident that my passion for cybersecurity will find a conducive and enriching home.

In conclusion, I express my sincere gratitude for considering my Expression of Interest. I look forward to the opportunity to contribute to the vibrant academic community at Indore Institute Of Science And Technology, Indore and am enthusiastic about the prospect of advancing my education in cybersecurity, furthering my professional development, and making a positive impact on the cybersecurity landscape. Thank you for considering my application, and I am eager to discuss my candidacy further.

Sincerely,

Surendra Chourasiya

Introduction to Cybersecurity

For completing the Cisco Networking Academy® Introduction to Cybersecurity course, and demonstrating the ability to explain the following:

- Global implications of cyber threats
- Ways in which networks are vulnerable to attack
- Impact of cyber-attacks on industries
- Cisco's approach to threat detection and defense
- Why cybersecurity is a growing profession
- Opportunities available for pursuing network security certifications

SURENDRA CHOURASIYA

Student

Indore Institute of Science & Technology

Academy Name

India

Location

2 Jul 2023

Date


Laura Quintana
VP & General Manager, Cisco Networking Academy