cyber threat intelligence analyst salary

cyber threat intelligence analyst salary is a crucial consideration for professionals in the cybersecurity field seeking to understand their earning potential and career trajectory. With the increasing incidence of cyberattacks and the growing importance of cybersecurity, the demand for skilled analysts who can interpret threat data and support organizational defense strategies has surged. This article will explore various factors influencing the cyber threat intelligence analyst salary, including geographic location, experience level, educational background, and industry sector. Additionally, it will cover common job responsibilities, required skills, and certifications that can impact compensation. Understanding these elements can help individuals and employers make informed decisions about career development and compensation planning in the cybersecurity domain. The following sections provide a detailed overview of key aspects related to the salary and professional landscape of cyber threat intelligence analysts.

Factors Influencing Cyber Threat Intelligence Analyst Salary

The salary of a cyber threat intelligence analyst is affected by a variety of factors that shape the compensation structure across different organizations and regions. These factors include individual qualifications, market demand, and the complexity of the analyst's role within the cybersecurity framework. Understanding these elements provides a clearer picture of what determines pay scales in this profession.

Experience and Expertise

Experience remains one of the most significant determinants of cyber threat intelligence analyst salary. Entry-level analysts typically earn less than seasoned professionals who have developed specialized skills in threat detection, malware analysis, and incident response. Expertise in advanced threat intelligence platforms or familiarity with emerging cyber threats can substantially increase earning potential.

Education Level

Educational qualifications such as a bachelor’s or master’s degree in cybersecurity, computer science, or related fields can influence salary. Higher education often correlates with better understanding of complex cybersecurity concepts, which employers value highly. Additionally, advanced degrees may open opportunities for leadership roles commanding higher compensation.

Certifications and Training

Professional certifications like Certified Threat Intelligence Analyst (CTIA), GIAC Cyber Threat Intelligence (GCTI), and Certified Information Systems Security Professional (CISSP) validate an analyst’s skills and knowledge, often leading to higher salaries. Continuous training on the latest cybersecurity tools and threat landscapes also adds to an analyst’s value.

Average Salary Range by Experience Level

Cyber threat intelligence analyst salary varies widely based on years of professional experience. The progression from entry-level to senior positions typically results in significant salary increases, reflecting the growing complexity of responsibilities and impact on organizational security.

Entry-Level Analysts

Individuals starting their careers in cyber threat intelligence can expect a salary range approximately between $60,000 and $80,000 annually. These roles often include monitoring cyber threats, initial data analysis, and supporting senior analysts. Entry-level salaries depend largely on geographic location and company size.

Mid-Level Analysts

With 3 to 5 years of experience, mid-level analysts generally earn between $80,000 and $110,000. They handle more complex threat assessments, collaborate on incident response, and may participate in strategic planning. Their growing expertise allows them to contribute more directly to the organization’s cybersecurity posture.

Senior Analysts and Specialists

Senior cyber threat intelligence analysts with over 5 years of experience typically command salaries exceeding $110,000, with some reaching $140,000 or more. These professionals lead threat intelligence teams, develop advanced threat models, and advise executive management on cybersecurity risks and mitigation strategies.

Impact of Education and Certifications on Salary

Education and certifications play a pivotal role in shaping the cyber threat intelligence analyst salary, as they demonstrate verified knowledge and commitment to the field. Employers often prioritize candidates who have pursued continuing education and earned industry-recognized credentials.

Relevant Degree Programs

Degrees in cybersecurity, information technology, computer science, or related disciplines provide foundational knowledge essential for cyber threat intelligence roles. Some organizations specifically require or prefer candidates with advanced degrees, which can positively affect salary offers.

Key Certifications

Certifications significantly enhance professional credibility and salary prospects. Common certifications that influence salary include:

- Certified Threat Intelligence Analyst (CTIA)
- GIAC Cyber Threat Intelligence (GCTI)
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- CompTIA Security+

These certifications validate skills in threat analysis, ethical hacking, security management, and incident response, making analysts more competitive in the job market.

Industry and Geographic Variations in Compensation

The cyber threat intelligence analyst salary also depends heavily on the industry sector and geographic location. Certain industries face higher cybersecurity risks, increasing demand for skilled analysts and resulting in higher pay. Similarly, salaries vary across regions due to cost of living and local market conditions.

Industry Differences

Industries such as finance, healthcare, defense, and technology typically offer higher salaries for cyber threat intelligence analysts due to the sensitive nature of their data and regulatory requirements. Analysts working in government agencies or defense contractors may also receive competitive pay, along with additional benefits.

Geographic Location

Location plays a critical role in compensation. Analysts working in major metropolitan areas or tech hubs like San Francisco, New York, or Washington D.C. often earn more than those in smaller cities or regions with lower living costs. Regional salary differences can range from 10% to 30% or more.

Skills and Responsibilities Affecting Salary

The complexity and scope of a cyber threat intelligence analyst’s skills and responsibilities directly impact their salary. Employers reward professionals who can effectively identify, analyze, and mitigate cyber threats while supporting broader cybersecurity strategies.

Technical Skills

Proficiency in threat intelligence platforms, malware analysis tools, and network security monitoring enhances salary potential. Skills in scripting languages like Python, knowledge of security information and event management (SIEM) systems, and familiarity with cyber threat frameworks are highly valued.

Analytical and Communication Skills

Strong analytical abilities to interpret complex data and the capacity to communicate findings clearly to technical and non-technical stakeholders contribute to higher compensation. Analysts who can produce actionable intelligence reports and guide decision-making processes are in demand.

Typical Responsibilities

Common responsibilities influencing salary include:

- Monitoring cyber threat landscapes and emerging vulnerabilities
- Conducting data collection and analysis on cyber incidents
- Collaborating with security teams to develop mitigation strategies
- Reporting intelligence findings to management and stakeholders
- Participating in incident response and forensic investigations

Career Growth and Salary Trends

The field of cyber threat intelligence is evolving rapidly, with growing demand for skilled analysts

driving positive salary trends. Career advancement opportunities often lead to roles in management, cybersecurity consulting, or specialized technical positions, all accompanied by increased compensation.

Emerging Trends

Adoption of artificial intelligence and machine learning in threat detection is reshaping analyst roles, requiring continuous skill development. Organizations increasingly seek analysts capable of leveraging advanced technologies, which is reflected in higher salary offers.

Long-Term Salary Outlook

As cyber threats become more sophisticated and frequent, the need for expert threat intelligence analysts is expected to grow, supporting steady increases in salary ranges. Professionals investing in education, certifications, and diverse skill sets position themselves well for sustained career success.

Frequently Asked Questions

What is the average salary of a cyber threat intelligence analyst in 2024?

As of 2024, the average salary of a cyber threat intelligence analyst in the United States ranges between $85,000 and $120,000 per year, depending on experience and location.

Which factors influence the salary of a cyber threat intelligence analyst?

Factors influencing the salary include years of experience, educational background, certifications, geographic location, industry sector, and the size of the employing organization.

How does certification impact the salary of a cyber threat intelligence analyst?

Certifications such as Certified Threat Intelligence Analyst (CTIA) or GIAC Cyber Threat Intelligence (GCTI) can significantly enhance a cyber threat intelligence analyst’s salary by validating expertise and increasing job opportunities.

What is the salary difference between entry-level and senior cyber threat intelligence analysts?

Entry-level cyber threat intelligence analysts typically earn between $65,000 and $85,000 annually, while senior analysts can earn upwards of $130,000 to $160,000 depending on their expertise and responsibilities.

How does the industry sector affect the salary of a cyber threat intelligence analyst?

Cyber threat intelligence analysts working in high-demand sectors like finance, government, and technology generally receive higher salaries compared to those in non-profit or smaller organizations due to the critical nature of cybersecurity in these industries.

Additional Resources

1. *Cyber Threat Intelligence Analyst Salary Guide 2024*
This comprehensive guide provides detailed insights into the current salary trends for cyber threat intelligence analysts across various industries. It covers factors influencing pay scales such as experience, certifications, and geographic location. Readers will find practical advice on negotiating salaries and understanding market demands.

2. *Breaking Down Cyber Threat Intelligence Careers and Compensation*
This book explores the career path of cyber threat intelligence analysts with a focus on compensation structures. It highlights the differences in pay based on job roles, company size, and regional demand. Additionally, it offers tips on career advancement to maximize earning potential.

3. *Understanding the Economics of Cybersecurity Jobs: Focus on Threat Intelligence*
Delving into the economics behind cybersecurity roles, this book focuses on the financial aspects of working as a threat intelligence analyst. It analyzes salary data and industry reports to provide a clear picture of what professionals can expect to earn. The book also discusses the impact of emerging threats on job market value.

4. *Negotiating Your Cyber Threat Intelligence Analyst Salary*
A practical handbook for professionals aiming to improve their compensation in cyber threat intelligence roles. It offers strategies for salary negotiation, including how to leverage certifications and experience effectively. The book also includes sample negotiation dialogues and preparation checklists.

5. *Global Salary Trends for Cyber Threat Intelligence Analysts*
This title presents a global overview of salary trends for cyber threat intelligence analysts. It compares compensation packages across continents, highlighting key differences and similarities. Readers gain insight into international job markets and factors driving salary variations worldwide.

6. *Cyber Threat Intelligence Analyst: Career Growth and Salary Insights*
Focusing on career development, this book links skill progression with salary increments for cyber threat intelligence analysts. It outlines typical career ladders within the field and what salary growth can be expected at each stage. The book also discusses essential skills that influence earning potential.

7. *The Impact of Certifications on Cyber Threat Intelligence Analyst Salaries*
This detailed analysis examines how various cybersecurity certifications affect salaries in threat intelligence roles. It reviews popular certifications such as CISSP, CEH, and GIAC and their return on investment. The book is a valuable resource for analysts planning their professional development.

8. *Salary Benchmarking for Cyber Threat Intelligence Analysts*

A resource designed to help organizations and professionals benchmark salaries against industry standards. It provides data-driven insights and practical tools to assess fair compensation in the cyber threat intelligence field. The book also addresses trends influencing salary adjustments.

9. *From Entry-Level to Expert: Salary Progression in Cyber Threat Intelligence*
This book traces the salary journey of cyber threat intelligence analysts from entry-level positions to expert roles. It offers detailed case studies and statistical data to illustrate typical earnings at each career stage. Readers can use this information to plan their career trajectory and salary expectations.

Cyber Threat Intelligence Analyst Salary

cyber threat intelligence analyst salary: Career Guide in Criminal Justice Douglas Klutz, 2019 Career Guide in Criminal Justice is the guide to getting hired and working in the criminal justice system. Featuring a straightforward and accessible writing style, it covers the three main components of the criminal justice system - law enforcement, courts, and corrections - discussing career opportunities in local, state, and federal government along with those in the private sector. The book also looks at careers in private investigations, the bond industry, forensic psychology, cybersecurity, and other related fields. Douglas Klutz helps students develop practical skills including succeeding as a student in higher education, acting ethically and professionally, writing cover letters and résumés, securing internships, preparing for interviews, and effective networking and career-building strategies. In addition, he addresses many of the common myths related to working in the criminal justice system, offering students invaluable real-world guidance.

cyber threat intelligence analyst salary: Break into Cybersecurity Career No Engineering Degree No Experience No Problem Rashmi Shah, Break into Cybersecurity Career No Engineering Degree No Experience No Problem is a comprehensive roadmap designed to launch individuals into a fulfilling, high-growth career within the in-demand cybersecurity industry, regardless of their prior technical background or experience. In an era where cybersecurity is fundamental to every organization, from startups to government agencies, the global demand for cybersecurity professionals is immense, spanning across the U.S., Europe, India, the Middle East, and Southeast Asia. This book directly challenges the common misconception that an engineering degree or prior IT experience is a prerequisite for entering the field. It aims to replace confusion with clarity, fear with confidence, and inaction with a structured action plan. Who This Book Is For: This guide is meticulously crafted for a diverse audience, including: Fresh graduates from any field, including non-technical disciplines such as BA, BCom, or BSc. Working professionals seeking a career transition, from support roles, teachers, and analysts to those in hospitality or HR. Students overwhelmed by the initial steps into cybersecurity. Self-learners and enthusiasts who have explored resources like YouTube but require a structured learning path. Anyone feeling excluded from the industry due to the absence of an engineering degree or work experience. What You'll Learn Inside: The Cybersecurity Opportunity: The book begins by elucidating why the present moment is opportune for entering the cybersecurity industry. It details how the global demand for cyber professionals has created a significant skill gap, which readers can fill even without formal technological education. It provides real job statistics, salary insights, and prevailing trends from

global markets, including the U.S., UK, India, UAE, and Southeast Asia, to illustrate the career's scope and potential. Top Beginner-Friendly Job Roles: It demystifies entry-level cybersecurity roles that do not necessitate deep technical skills. The book breaks down positions such as: SOC (Security Operations Center) Analyst GRC (Governance, Risk, Compliance) Analyst Threat Intelligence Analyst Vulnerability Management Analyst Security Support and Compliance roles For each role, it offers a clear understanding of responsibilities, expected skills, and global salary ranges. 50-Day Roadmap to Success: A core component of the book is its detailed 50-day plan, which outlines precisely what to learn, in what sequence, and the time commitment required for both part-time and full-time study. This structured path covers foundational skills like networking, operating systems, threat detection, incident response, and basic scripting, all utilizing free or low-cost learning resources. It guides users through platforms such as TryHackMe and HackTheBox for hands-on practice, recommends specific YouTube channels and MOOC platforms, and integrates learning from the Google Cybersecurity Certificate, IBM Cybersecurity Analyst (via Coursera), free learning labs, and blue team simulators. Build Skills Without a Degree or IT Job: The book provides practical instructions on developing real-world skills from home, including: Creating a personal home lab with just a laptop. Setting up Linux and SIEM tools like Splunk to run basic attacks and defenses. Simulating incident response scenarios. Practicing with Capture The Flag (CTF) challenges. Tracking learning progress to effectively showcase skills to prospective employers. How to Apply for Jobs Smartly: It offers targeted guidance on job application strategies based on geographical regions: India: Naukri, CutShort, LinkedIn, Instahyre U.S. & Canada: LinkedIn, Dice, CyberSecJobs UK & Europe: Technojobs, CV-Library Middle East & SEA: GulfTalent, Bayt, JobStreet Remote: Upwork, RemoteOK, Toptal, PeoplePerHour Readers learn how to filter roles, optimize their profiles with keywords, and effectively connect with recruiters. Resume, LinkedIn & Personal Branding: The book addresses the challenge of lacking job experience by teaching readers how to: Construct a project-based cybersecurity resume. Develop a professional LinkedIn profile that attracts recruiters. Effectively highlight labs, certificates, and their learning journey. Leverage platforms like GitHub or personal blogs to share work and enhance visibility. Interview Prep: Questions and Mindset: It prepares readers for interviews by providing over 20 real technical and behavioral questions, such as What is a port?, How would you respond to a phishing incident?, and Explain the CIA triad. It also covers essential soft skills, mindset, and communication tips, particularly beneficial for non-native English speakers and first-time applicants. What Comes After You Get the Job: The guide extends beyond job acquisition, assisting readers in: Choosing a specialization (e.g., Red Team, Blue Team, GRC, Cloud Security, Threat Intel). Planning a certification roadmap (e.g., Security+, CEH, CISSP, OSCP, CISA). Fostering continuous growth through blogs, open-source contributions, and mentorship. Developing a long-term career strategy to ensure sustained professional development. This book stands apart as a real-world, results-focused action guide, embodying the practical, accessible approach often championed by leading tech resources like QuickTechie.com. It is specifically crafted for individuals who feel hindered by a lack of traditional qualifications, such as an engineering degree or prior IT experience. It is not a generic, jargon-filled, or outdated cybersecurity text. Instead, it offers a clear, empowering plan to transition from uncertainty to a successful career in cybersecurity, requiring only effort and ambition, without gatekeeping or unnecessary theoretical complexities. The world of cybersecurity actively seeks curious, driven, and eager-to-learn individuals, and this book serves as the definitive plan to achieve that goal.

cyber threat intelligence analyst salary: The Complete Guide to Starting a Cybersecurity Career Johann Lahoud, 2025-08-15 Start your cybersecurity career , even without a degree , and step into one of the fastest-growing, highest-paying industries in the world. With over 4 million unfilled cybersecurity jobs worldwide, there’s never been a better time to start. Whether you aim to be a SOC analyst, penetration tester, GRC specialist, cloud security engineer, or ethical hacker, this guide gives you a clear, step-by-step roadmap to go from complete beginner to job-ready with confidence. Written by cybersecurity professional Johann Lahoud , with experience in compliance, engineering, red teaming, and mentoring , this comprehensive resource delivers proven strategies

and insider tips to help you: Inside, you'll learn: How the cybersecurity industry works and where you might fit The most in-demand cybersecurity jobs and their real responsibilities The essential skills every beginner must master: networking, Linux, Windows, and security fundamentals How to set up a home cybersecurity lab to practice safely Which certifications actually matter for entry-level roles How to write a cyber-ready CV and optimise your LinkedIn profile How to prepare for technical and behavioural interviews Ways to get hands-on experience before your first job , from CTFs to freelancing How to create a long-term growth plan to keep advancing in your career Why this guide is different: No filler. No generic fluff. Every chapter gives you actionable steps you can apply immediately , without expensive tools, unnecessary degrees, or years of waiting. Perfect for: Career changers looking to enter cybersecurity Students exploring cybersecurity paths IT professionals ready to move into security roles Anyone curious about cyber defence and career growth Your cybersecurity career starts now , take the first step and build your future with confidence.

cyber threat intelligence analyst salary: Android Malware Analysis & Defensive Exploitation 2025 (Hinglish Edition) A. Clarke, 2025-10-07 "Android Malware Analysis & Defensive Exploitation 2025 (Hinglish Edition)" by A. Clarke ek practical aur responsible guide hai jo Android apps aur mobile threats ko analyse, detect, aur mitigate karna sikhata hai — sab Hinglish (Hindi + English mix) mein.

cyber threat intelligence analyst salary: Budget Request Colorado. Department of Public Safety, 2014

cyber threat intelligence analyst salary: Cybersecurity Career Master Plan Dr. Gerald Auger, Jaclyn "Jax" Scott, Jonathan Helmus, Kim Nguyen, Heath "The Cyber Mentor" Adams, 2021-09-13 Start your Cybersecurity career with expert advice on how to get certified, find your first job, and progress Purchase of the print or Kindle book includes a free eBook in PDF format Key Features Learn how to follow your desired career path that results in a well-paid, rewarding job in cybersecurity Explore expert tips relating to career growth and certification options Access informative content from a panel of experienced cybersecurity experts Book Description Cybersecurity is an emerging career trend and will continue to become increasingly important. Despite the lucrative pay and significant career growth opportunities, many people are unsure of how to get started. This book is designed by leading industry experts to help you enter the world of cybersecurity with confidence, covering everything from gaining the right certification to tips and tools for finding your first job. The book starts by helping you gain a foundational understanding of cybersecurity, covering cyber law, cyber policy, and frameworks. Next, you'll focus on how to choose the career field best suited to you from options such as security operations, penetration testing, and risk analysis. The book also guides you through the different certification options as well as the pros and cons of a formal college education versus formal certificate courses. Later, you'll discover the importance of defining and understanding your brand. Finally, you'll get up to speed with different career paths and learning opportunities. By the end of this cyber book, you will have gained the knowledge you need to clearly define your career path and develop goals relating to career progression. What you will learn Gain an understanding of cybersecurity essentials, including the different frameworks and laws, and specialties Find out how to land your first job in the cybersecurity industry Understand the difference between college education and certificate courses Build goals and timelines to encourage a work/life balance while delivering value in your job Understand the different types of cybersecurity jobs available and what it means to be entry-level Build affordable, practical labs to develop your technical skills Discover how to set goals and maintain momentum after landing your first cybersecurity job Who this book is for This book is for college graduates, military veterans transitioning from active service, individuals looking to make a mid-career switch, and aspiring IT professionals. Anyone who considers cybersecurity as a potential career field but feels intimidated, overwhelmed, or unsure of where to get started will also find this book useful. No experience or cybersecurity knowledge is needed to get started.

cyber threat intelligence analyst salary: CEH v13 Exam Prep 2025 A. Khan, CEH v13 Exam Prep 2025: All-in-One Guide to Pass the Certified Ethical Hacker Certification by A. Khan is your

complete companion for mastering the CEH v13 syllabus and passing the exam with confidence.

cyber threat intelligence analyst salary: Intelligence and State Surveillance in Modern Societies Frederic Lemieux, 2024-09-13 Offering a compelling understanding of contemporary state surveillance dynamics, this second edition is a timely update that lands at the critical intersection of cutting-edge technology and international security.

cyber threat intelligence analyst salary: *Mastering Cyber Intelligence* Jean Nestor M. Dahj, 2022-04-29 Develop the analytical skills to effectively safeguard your organization by enhancing defense mechanisms, and become a proficient threat intelligence analyst to help strategic teams in making informed decisions Key FeaturesBuild the analytics skills and practices you need for analyzing, detecting, and preventing cyber threatsLearn how to perform intrusion analysis using the cyber threat intelligence (CTI) processIntegrate threat intelligence into your current security infrastructure for enhanced protectionBook Description The sophistication of cyber threats, such as ransomware, advanced phishing campaigns, zero-day vulnerability attacks, and advanced persistent threats (APTs), is pushing organizations and individuals to change strategies for reliable system protection. Cyber Threat Intelligence converts threat information into evidence-based intelligence that uncovers adversaries' intents, motives, and capabilities for effective defense against all kinds of threats. This book thoroughly covers the concepts and practices required to develop and drive threat intelligence programs, detailing the tasks involved in each step of the CTI lifecycle. You'll be able to plan a threat intelligence program by understanding and collecting the requirements, setting up the team, and exploring the intelligence frameworks. You'll also learn how and from where to collect intelligence data for your program, considering your organization level. With the help of practical examples, this book will help you get to grips with threat data processing and analysis. And finally, you'll be well-versed with writing tactical, technical, and strategic intelligence reports and sharing them with the community. By the end of this book, you'll have acquired the knowledge and skills required to drive threat intelligence operations from planning to dissemination phases, protect your organization, and help in critical defense decisions. What you will learnUnderstand the CTI lifecycle which makes the foundation of the studyForm a CTI team and position it in the security stackExplore CTI frameworks, platforms, and their use in the programIntegrate CTI in small, medium, and large enterprisesDiscover intelligence data sources and feedsPerform threat modelling and adversary and threat analysisFind out what Indicators of Compromise (IoCs) are and apply the pyramid of pain in threat detectionGet to grips with writing intelligence reports and sharing intelligenceWho this book is for This book is for security professionals, researchers, and individuals who want to gain profound knowledge of cyber threat intelligence and discover techniques to prevent varying types of cyber threats. Basic knowledge of cybersecurity and network fundamentals is required to get the most out of this book.

cyber threat intelligence analyst salary: United States Code Congress, 2010 The United States Code, 2006 Edition, contains the General and Permanent Laws of the United States Enacted Through the 109th Congress (Ending January 3, 2007, the Last Law of Which was Signed on January 15, 2007).

cyber threat intelligence analyst salary: Secret Intelligence Christopher Andrew, Richard J. Aldrich, Wesley K. Wark, 2019-07-26 The second edition of Secret Intelligence: A Reader brings together key essays from the field of intelligence studies, blending classic works on concepts and approaches with more recent essays dealing with current issues and ongoing debates about the future of intelligence. Secret intelligence has never enjoyed a higher profile. The events of 9/11, the conflicts in Iraq and Afghanistan, the missing WMD controversy, public debates over prisoner interrogation, together with the revelations of figures such as Edward Snowden, recent cyber attacks and the rise of 'hybrid warfare' have all contributed to make this a ‘hot’ subject over the past two decades. Aiming to be more comprehensive than existing books, and to achieve truly international coverage of the field, this book provides key readings and supporting material for students and course convenors. It is divided into four main sections, each of which includes full summaries of each article, further reading suggestions and student questions: • The intelligence

cycle • Intelligence, counter-terrorism and security • Ethics, accountability and secrecy • Intelligence and the new warfare This new edition contains essays by leading scholars in the field and will be essential reading for students of intelligence studies, strategic studies, international security and political science in general, and of interest to anyone wishing to understand the current relationship between intelligence and policy-making.

cyber threat intelligence analyst salary: The Oxford Handbook of National Security Intelligence Loch K. Johnson, 2010-03-12 The Oxford Handbook of National Security Intelligence is a state-of-the-art work on intelligence and national security. Edited by Loch Johnson, one of the world's leading authorities on the subject, the handbook examines the topic in full, beginning with an examination of the major theories of intelligence. It then shifts its focus to how intelligence agencies operate, how they collect information from around the world, the problems that come with transforming raw information into credible analysis, and the difficulties in disseminating intelligence to policymakers. It also considers the balance between secrecy and public accountability, and the ethical dilemmas that covert and counterintelligence operations routinely present to intelligence agencies. Throughout, contributors factor in broader historical and political contexts that are integral to understanding how intelligence agencies function in our information-dominated age.

cyber threat intelligence analyst salary: United States Code United States, 2006

cyber threat intelligence analyst salary: *Ethical Hacking 2025* A. Khan, 2025-10-07 “Ethical Hacking 2025: A Step-by-Step Guide (Hinglish Edition)” by A. Khan ek practical aur career-oriented kitab hai jo beginners se leke intermediate learners tak ko ethical hacking, penetration testing, aur cyber security ke core skills Hinglish (Hindi + English mix) mein sikhaati hai.

cyber threat intelligence analyst salary: Issues in Global Business SAGE Publishing, 2021-03-11 In 2020, COVID-19 starkly demonstrated the global interconnectedness of business, as it disrupted supply chains and manufacturing operations, broadly shuttered retail stores, and led to restrictions on movement and travel around the world. Other events in 2019 also showcased the undeniable globalization of business, be it from the (un)expected ramifications of Brexit to the impacts of data breaches across various industries. Riots in Hong Kong over an extradition bill also sparked huge debate and controversy, and the U.S.-China trade war also caused concern. All of these events may have largely and immediately impacted one region, yet effects reverberate across larger swathes of the globe—ultimately affecting vast areas, industries, and sectors across the international landscape. Issues in Global Business explores all of these and more, across a wide range of topics, including the on-demand economy, global manufacturing, Bitcoin, data security, and many more. Coupled with a comprehensive overview of the business landscape around the world by Dr. Mamoun Benmamoun, an assistant professor at the Boeing Institute of International Business at Saint Louis University, this book provides students with the essential information they need to assess business practices through an international lens.

cyber threat intelligence analyst salary: *Career Ideas for Teens in Government and Public Service* Diane Lindsey Reeves, Don Rauf, 2009 Want to serve your community? Whether you're interested in politics or policy, law or science, finance or law enforcement, a career in government or public service may be right for you. From local to federal government employment, this book covers it all. The careers profiled include: Air marshal; Air traffic controller; Budget analyst; City manager; Cryptographer; Ecologist; Firefighter; Meteorologist; Park ranger; Police officer; Politician; and Urban planner.

cyber threat intelligence analyst salary: Cyber Security: Masters Guide 2025 | Learn Cyber Defense, Threat Analysis & Network Security from Scratch Aamer Khan, Cyber Security: Masters Guide 2025 is a comprehensive and practical resource for mastering the art of digital defense. Covering everything from fundamental cybersecurity concepts to advanced threat detection, ethical hacking, penetration testing, and network security, this guide is ideal for students, IT professionals, and anyone looking to build a strong foundation in cyber defense. With real-world case studies, hands-on strategies, and up-to-date techniques, this book prepares you to combat modern cyber threats, secure networks, and understand the evolving landscape of digital security.

cyber threat intelligence analyst salary: Cracking the Emerging Tech Code Prayukth K V, 2020-11-13 Learn how to work towards making the most out of a career in emerging tech Ê KEY FEATURESÊ Understand the core concepts related to careers in emerging tech. Learn innovative, exclusive, and exciting ways to design a successful career in ET. Reduce your learning curve by examining the career trajectories of eminent ET professionals. Ways to evolve and adapt to changing ET paradigms. Practical perspective from the field. DESCRIPTIONÊÊ Cracking the emerging tech code will help you attain your Emerging Technology (ET) career goals faster without spending years in committing avoidable mistakes, recovering from them, and learning things the hard way. You can apply practical tips in areas such as improving your ability to craft market-friendly use cases and evolving a solution approach in new and diverse tech or business environments, to propel forward your career in strategic and proactive ways. It outlines ways in which you can explore and capitalize on hidden opportunities while working on important career aspects. The anecdotes and solutions provided will aid you in getting an inside out view to reduce your learning curve. This book will help you in gaining both magnitude and direction in your ET career journey and prevent you from getting overwhelmed or pinned down by the forces of ET. Authored by an ET professional, this book will take you through a series of steps to deepen your understanding of the forces that shape oneÕs ET career and successfully dealing with them. It also helps bust myths, addresses fallacies, and common misconceptions that could harm oneÕs career prospects. There are also practical and easy-to-adopt tips, methods, tracking mechanisms, and information that will improve career standing and professional growth. This book makes it easy for you to enhance your employability and job market relevance so that you can sprint towards a rewarding career. ÊÊ WHAT YOU WILL LEARNÊ Through this book, you will connect with ways and means to build a strong and rewarding emerging tech career. You will be able to work on identifying the right technology and employer, enhancing employability and differentiation in the job market, addressing challenges and connecting with enablers, accurate growth strategies and execution principles. Ê Ê WHO IS THIS BOOK FORÊ This book is for current and aspiring emerging tech professionals, students, and anyone who wishes to understand ways to have a fulfilling career in emerging technologies such as AI, blockchain, cybersecurity, IoT, space tech, and more. TABLE OF CONTENTS 1. Introduction 2. The best ET for me and some myth bursting 3. Getting prepared and charting a roadmap 4. Identifying the requirements and getting help 5. Dealing with headwinds and drawing a career change action plan 6. Building an ET friendly r□sum□ and finding the right employer 7. Getting hired through social media 8. Job search 9. Impressing the emerging tech jury 10. The secret sauce 11. Becoming a thought leader 12. Measuring success and making course corrections 13. Drawing the two-year plan 14. Building your leadership capabilities 15. To start-up or not? 16. Communications skills: getting it right 17. Building a personal brand 18. Post-script

cyber threat intelligence analyst salary: The Budget of the United States Government United States. Bureau of the Budget, 1968

cyber threat intelligence analyst salary: The CISO’s Transformation Raj Badhwar, 2021-10-19 The first section of this book addresses the evolution of CISO (chief information security officer) leadership, with the most mature CISOs combining strong business and technical leadership skills. CISOs can now add significant value when they possess an advanced understanding of cutting-edge security technologies to address the risks from the nearly universal operational dependence of enterprises on the cloud, the Internet, hybrid networks, and third-party technologies demonstrated in this book. In our new cyber threat-saturated world, CISOs have begun to show their market value. Wall Street is more likely to reward companies with good cybersecurity track records with higher stock valuations. To ensure that security is always a foremost concern in business decisions, CISOs should have a seat on corporate boards, and CISOs should be involved from beginning to end in the process of adopting enterprise technologies. The second and third sections of this book focus on building strong security teams, and exercising prudence in cybersecurity. CISOs can foster cultures of respect through careful consideration of the biases inherent in the socio-linguistic frameworks shaping our workplace language and through the cultivation of cyber

exceptionalism. CISOs should leave no stone unturned in seeking out people with unique abilities, skills, and experience, and encourage career planning and development, in order to build and retain a strong talent pool. The lessons of the breach of physical security at the US Capitol, the hack back trend, and CISO legal liability stemming from network and data breaches all reveal the importance of good judgment and the necessity of taking proactive stances on preventative measures. This book will target security and IT engineers, administrators and developers, CIOs, CTOs, CISOs, and CFOs. Risk personnel, CROs, IT, security auditors and security researchers will also find this book useful.

Related to cyber threat intelligence analyst salary

Cybersecurity Awareness Month Toolkit | CISA About Cybersecurity Awareness Month. Cybersecurity Awareness Month (October) is an international initiative that highlights essential actions to reduce cybersecurity

Cybersecurity Awareness Month - CISA Cyber threats don’t take time off. As the federal lead for Cybersecurity Awareness Month and the nation’s cyber defense agency, the Cybersecurity and Infrastructure Security Agency, or CISA,

DHS and CISA Announce Cybersecurity Awareness Month 2025 DHS and the Cybersecurity and Infrastructure Security Agency (CISA) announced the official beginning of Cybersecurity Awareness Month 2025. This year’s theme is Building a

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Widespread Supply Chain Compromise Impacting npm Ecosystem CISA is releasing this Alert to provide guidance in response to a widespread software supply chain compromise involving the world’s largest JavaScript registry,

Home Page | CISA JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Cybersecurity | Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and

Cyber Threats and Advisories | Cybersecurity and Infrastructure By preventing attacks or mitigating the spread of an attack as quickly as possible, cyber threat actors lose their power. CISA diligently tracks and shares information about the

Cybersecurity Incident & Vulnerability Response Playbooks - CISA Scope These playbooks are for FCEB entities to focus on criteria for response and thresholds for coordination and reporting. They include communications between FCEB entities and CISA;

Cybersecurity Awareness Month Toolkit | CISA About Cybersecurity Awareness Month. Cybersecurity Awareness Month (October) is an international initiative that highlights essential actions to reduce cybersecurity

Cybersecurity Awareness Month - CISA Cyber threats don’t take time off. As the federal lead for Cybersecurity Awareness Month and the nation’s cyber defense agency, the Cybersecurity and Infrastructure Security Agency, or CISA,

DHS and CISA Announce Cybersecurity Awareness Month 2025 DHS and the Cybersecurity and Infrastructure Security Agency (CISA) announced the official beginning of Cybersecurity Awareness Month 2025. This year’s theme is Building a

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Widespread Supply Chain Compromise Impacting npm Ecosystem CISA is releasing this

Alert to provide guidance in response to a widespread software supply chain compromise involving the world’s largest JavaScript registry, npmjs.com.

Home Page | CISA JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Cybersecurity | Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and

Cyber Threats and Advisories | Cybersecurity and Infrastructure By preventing attacks or mitigating the spread of an attack as quickly as possible, cyber threat actors lose their power. CISA diligently tracks and shares information about the

Cybersecurity Incident & Vulnerability Response Playbooks - CISA Scope These playbooks are for FCEB entities to focus on criteria for response and thresholds for coordination and reporting. They include communications between FCEB entities and CISA;

Cybersecurity Awareness Month Toolkit | CISA About Cybersecurity Awareness Month. Cybersecurity Awareness Month (October) is an international initiative that highlights essential actions to reduce cybersecurity

Cybersecurity Awareness Month - CISA Cyber threats don’t take time off. As the federal lead for Cybersecurity Awareness Month and the nation’s cyber defense agency, the Cybersecurity and Infrastructure Security Agency, or CISA,

DHS and CISA Announce Cybersecurity Awareness Month 2025 DHS and the Cybersecurity and Infrastructure Security Agency (CISA) announced the official beginning of Cybersecurity Awareness Month 2025. This year’s theme is Building a

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Widespread Supply Chain Compromise Impacting npm Ecosystem CISA is releasing this Alert to provide guidance in response to a widespread software supply chain compromise involving the world’s largest JavaScript registry,

Home Page | CISA JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Cybersecurity | Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and

Cyber Threats and Advisories | Cybersecurity and Infrastructure By preventing attacks or mitigating the spread of an attack as quickly as possible, cyber threat actors lose their power. CISA diligently tracks and shares information about the

Cybersecurity Incident & Vulnerability Response Playbooks - CISA Scope These playbooks are for FCEB entities to focus on criteria for response and thresholds for coordination and reporting. They include communications between FCEB entities and CISA;

Cybersecurity Awareness Month Toolkit | CISA About Cybersecurity Awareness Month. Cybersecurity Awareness Month (October) is an international initiative that highlights essential actions to reduce cybersecurity

Cybersecurity Awareness Month - CISA Cyber threats don’t take time off. As the federal lead for Cybersecurity Awareness Month and the nation’s cyber defense agency, the Cybersecurity and Infrastructure Security Agency, or CISA,

DHS and CISA Announce Cybersecurity Awareness Month 2025 DHS and the Cybersecurity and Infrastructure Security Agency (CISA) announced the official beginning of Cybersecurity Awareness Month 2025. This year's theme is Building a

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Widespread Supply Chain Compromise Impacting npm Ecosystem CISA is releasing this Alert to provide guidance in response to a widespread software supply chain compromise involving the world's largest JavaScript registry,

Home Page | CISA JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Cybersecurity | Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and

Cyber Threats and Advisories | Cybersecurity and Infrastructure By preventing attacks or mitigating the spread of an attack as quickly as possible, cyber threat actors lose their power. CISA diligently tracks and shares information about the

Cybersecurity Incident & Vulnerability Response Playbooks - CISA Scope These playbooks are for FCEB entities to focus on criteria for response and thresholds for coordination and reporting. They include communications between FCEB entities and CISA;

Back to Home: http://www.devensbusiness.com