Cyber Security The Mitigation Strategies

Cybersecurity Threats, Malware Trends, and Strategies
Becoming a Global Chief Security Executive Officer
Infosec Strategies and Best Practices
Solving Cyber Risk
Modern Theories and Practices for Cyber Ethics and Security Compliance
Cyber Security Risk Management Essentials
Mastering Cybersecurity Risk Management
Cybersecurity and Secure Information Systems
Cybersecurity for Business
The Digital Battle
Cybersecurity Threats, Malware Trends, and Strategies
Cyber-Security Threats, Actors, and Dynamic Mitigation
Industrial Cybersecurity
The Insider Threat
Cybersecurity – Attack and Defense Strategies
Modern Cybersecurity Strategies for Enterprises
Cyber Security and Adversarial Machine Learning
Threat Hunting in the Cloud
Cyber Strategy
Risk Management Program Guide
Cybersecurity Management in Education Technologies
Recommended Practice
Cybersecurity Threats, Malware Trends, and Strategies
Cybersecurity - Attack and Defense Strategies
How to Measure Anything in Cybersecurity Risk
U.S. Cyber Strategies
Insider Threat
Optimal Spending on Cybersecurity Measures
Strategic Cyber Security
Advances in Cybersecurity Management
Cybersecurity Risk Management
Confronting Cyber Risk
Asset Attack Vectors
Strategic Cyber Security
DNS Security Management
Optimal Spending on Cybersecurity Measures
Russian Cyber Attack - Grizzly Steppe Report & The Rules of Cyber Warfare
Cyber Security for Critical Infrastructure
Internet of Things Technology in Healthcare: Fundamentals, Principles and Cyber Security Issues
Cyber Security

PONCE KATELYN

Cybersecurity Threats, Malware Trends, and Strategies Kenneth Geers Becoming a Global Chief Security Executive Officer provides tangible, proven, and practical approaches to optimizing the security leader’s ability to lead both today’s, and tomorrow’s, multidisciplined security, risk, and privacy function. The need for well-trained and effective executives who focus on business security, risk, and privacy has exponentially increased as the critical underpinnings of today’s businesses rely more and more on their ability to ensure the effective operation and availability of business processes and technology. Cyberattacks, e-crime, intellectual property theft, and operating globally requires sustainable security programs and operations led by executives who cannot only adapt to today’s requirements, but also focus on the future. The book provides foundational and practical methods for creating teams, organizations, services, and operations for today’s—and tomorrow’s—physical and information converged security program, also teaching the principles for alignment to the business, risk management and mitigation strategies, and how to create momentum in business operations protection. Demonstrates how to develop a security program’s business mission Provides practical approaches to organizational design for immediate business impact utilizing the converged security model Offers insights into what a business, and its board, want, need, and expect from their security executives“/li> Covers the 5 Steps to Operational Effectiveness: Cybersecurity – Corporate Security – Operational Risk – Controls Assurance – Client Focus Provides templates and checklists for strategy design, program development, measurements and efficacy assurance Becoming a Global Chief Security Executive Officer Kogan Page Publishers This book explores the intersection of cybersecurity and education technologies, providing practical solutions, detection techniques, and mitigation strategies to ensure a secure and protected learning environment in the face of evolving cyber threats. With a wide range of contributors covering topics from immersive learning to phishing detection, this book is a valuable resource for professionals, researchers,

educators, students, and policymakers interested in the future of cybersecurity in education. Provides practical solutions, detection techniques, and mitigation strategies to ensure a secure and protected learning environment in the face of evolving cyber threats. Covers a wide range of topics including immersive learning, cybersecurity education, and malware detection, making it a valuable resource for professionals, researchers, educators, students, and policymakers. Offers both theoretical foundations and practical guidance for fostering a secure and protected environment for educational advancements in the digital age. Addresses the need for cybersecurity in education in the context of worldwide changes in education sources and advancements in technology. Highlights the significance of integrating cybersecurity into educational practices and protecting sensitive information to ensure students' performance prediction systems are not misused.

Infosec Strategies and Best Practices John Wiley & Sons

This book explores the strategic decisions made by organizations when implementing cybersecurity controls and leveraging economic models and theories from the economics of information security and risk-management frameworks. Based on unique and distinct research completed within the field of risk-management and information security, this book provides insight into organizational risk-management processes utilized in determining cybersecurity investments. It describes how theoretical models and frameworks rely on either specific scenarios or controlled conditions and how decisions on cybersecurity spending within organizations—specifically, the funding available in comparison to the recommended security measures necessary for compliance—vary depending on stakeholders. As the trade-off between the costs of implementing a security measure and the benefit derived from the implementation of security controls is not easily measured, a business leader’s decision to fund security measures may be biased. The author presents an innovative approach to assess cybersecurity initiatives with a risk-management perspective and leverages a data-centric focus on the evolution of cyber-attacks. This book is ideal for business school students and technology professionals with an interest in risk management.

Solving Cyber Risk CRC Press

This book concentrates on a wide range of advances related to IT cybersecurity management. The topics covered in this book include, among others, management techniques in security, IT risk management, the impact of technologies and techniques on security management, regulatory techniques and issues, surveillance technologies, security policies, security for protocol management, location management, GOS management, resource management, channel management, and mobility management. The authors also discuss digital contents copyright protection, system security management, network security management, security management in network equipment, storage area networks (SAN) management, information security management, government security policy, web penetration testing, security operations, and vulnerabilities management. The authors introduce the concepts, techniques, methods, approaches and trends needed by cybersecurity management specialists and educators for keeping current their cybersecurity management knowledge. Further, they provide a glimpse of future directions where cybersecurity management techniques, policies, applications, and theories are headed. The book is a rich collection of carefully selected and reviewed manuscripts written by diverse cybersecurity management experts in the listed fields and edited by prominent cybersecurity management researchers and specialists.

Modern Theories and Practices for Cyber Ethics and Security Compliance John Wiley & Sons

Playing A Game…. And Don’t Know the Cyber Security Rules. Networking in the form of internet, extranet, intranet, and virtual private network (vpn) has opened many doors for businesses. No longer is commerce inhibited by time zones or geographic locations to conduct financial transactions. Cyberspace affords businesses enormous revenue opportunities with reduced associated costs. All that is necessary for customers to make online purchases is internet availability and connectivity, an internet of things (IoT) digital media (i.e. laptop, desktop, tablet, smartphone, etc), and a method of payment (i.e. bank account, credit card debit card, etc). The problem resonates from the protection of your personal identifiable information (PII) during authentication and validation processes. The Digital Battle: Cyber Security is an attempt to assist consumers by protecting their PII, trade secrets, and critical infrastructure from compromise. To prevent exploitation, consumers need vigilance paired with knowledge. Using strategies of cyber security outlined in the three domains within this book, readers can gain the tools they need to succeed. Be Ready, cover your Defenses, and take the Offensive with Cyber Warfare Tactics.

Cyber Security Risk Management Essentials Springer Nature

Today, cyberspace has emerged as a domain of its own, in many ways like land, sea and air. Even if a nation is small in land area, low in GDP per capita, low in resources, less important in geopolitics, low in strength of armed forces, it can become a military super power if it is capable of launching a cyber-attack on critical infrastructures of any other nation including superpowers and crumble that nation. In fact cyber space redefining our security assumptions and defense strategies. This book explains the current cyber threat landscape and discusses the strategies being used by governments and corporate sectors to protect Critical Infrastructure (CI) against these threats.

Mastering Cybersecurity Risk Management CRC Press

Cyber Strategy: Risk-Driven Security and Resiliency provides a process and roadmap for any company to develop its unified Cybersecurity and Cyber Resiliency strategies. It demonstrates a methodology for companies to combine their disassociated efforts into one corporate plan with buy-in from senior management that will efficiently utilize resources, target high risk threats, and evaluate risk assessment methodologies and the efficacy of resultant risk mitigations. The book discusses all the steps required from conception of the plan from preplanning (mission/vision, principles, strategic objectives, new initiatives derivation), project management directives, cyber threat and vulnerability analysis, cyber risk and controls assessment to reporting and measurement techniques for plan success and overall strategic plan performance. In addition, a methodology is presented to aid in new initiative selection for the following year by identifying all relevant inputs. Tools utilized include: Key Risk Indicators (KRI) and Key Performance Indicators (KPI) National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) Target State Maturity interval mapping per initiative Comparisons of current and target state business goals and critical success factors A quantitative NIST-based risk assessment of initiative technology components Responsible, Accountable, Consulted, Informed (RACI) diagrams for Cyber Steering Committee tasks and Governance Boards’ approval processes Swimlanes, timelines, data flow diagrams (inputs,

resources, outputs), progress report templates, and Gantt charts for project management The last chapter provides downloadable checklists, tables, data flow diagrams, figures, and assessment tools to help develop your company’s cybersecurity and cyber resiliency strategic plan.

Cybersecurity and Secure Information Systems Routledge

The Enterprise Risk Management Program (ERMP) Guide provides program-level risk management guidance that directly supports your organization's policies and standardizes the management of cybersecurity risk and also provides access to an editable Microsoft Word document template that can be utilized for baselining your organizations risk management practices. Unfortunately, most companies lack a coherent approach to managing risks across the enterprise: When you look at getting audit ready, your policies and standards only cover the "why?" and "what?" questions of an audit. This product addresses the "how" questions for how your company manages risk.The ERMP provides clear, concise documentation that provides a "paint by numbers" approach to how your organization manages risk.The ERMP addresses fundamental needs when it comes to what is expected in cybersecurity risk management, how risk is defined, who can accept risk, how risk is calculated by defining potential impact and likelihood, necessary steps to reduce risk.Just as Human Resources publishes an "employee handbook" to let employees know what is expected for employees from an HR perspective, the ERMP does this from a cybersecurity risk management perspective.Regardless if your cybersecurity program aligns with NIST, ISO, or another framework, the Enterprise Risk Management Program (ERMP) is designed to address the strategic, operational and tactical components of IT security risk management for any organization. Policies & standards are absolutely necessary to an organization, but they fail to describe HOW risk is actually managed. The ERMP provides this middle ground between high-level policies and the actual procedures of how risk is managed on a day-to-day basis by those individual contributors who execute risk-based controls.

Cybersecurity for Business Anand Vemula

Cyber attacks are a real threat to our country. This report presents the opposed views of USA and Russia on cyber security and gives insight into the activities of the Russian civilian and military intelligence Services (RIS) conducted during the 2016 U.S. presidential election campaign. The Grizzly Steppe Report provides details regarding the tools and hacking techniques used by the Russian hackers in order to interfere the 2016 U.S. elections. This activity by RIS is just part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information. In foreign countries, RIS actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. This report provides technical indicators related to many of these operations, recommended mitigations, suggested actions to take in response to the indicators provided, and information on how to report such incidents to the U.S. Government. The edition also provides crucial information on the legality of hostile cyber activity at state level. While the United States and its allies are in general agreement on the legal status of conflict in cyberspace, China, Russia, and a number of like-minded nations have an entirely different concept of the applicability of international law to cyberspace.

The Digital Battle Packt Publishing Ltd

In "Mastering Cybersecurity Risk Management," acclaimed author Benoit Leroy offers a comprehensive guide to navigating the complex and ever-evolving landscape of cybersecurity. This book stands as a beacon for individuals and organizations seeking not only to understand the intricacies of cybersecurity but also to master the strategies that lead to a resilient and secure future. Key Highlights: 1. A Holistic Approach to Cybersecurity: Benoit Leroy takes readers on a journey that goes beyond mere risk mitigation. The book advocates for a holistic approach to cybersecurity, encompassing not only technological aspects but also cultural and procedural dimensions. By understanding the interconnectedness of these elements, Leroy guides readers toward building a robust security foundation. 2. Proactive Risk Management Strategies: Leroy delves deep into the realm of risk management, providing actionable strategies to identify, assess, and mitigate cybersecurity risks proactively. From foundational risk management models to the integration of risk management into business processes, readers gain insights into creating a resilient security framework. 3. Real-world Case Studies: The book is enriched with real-world case studies, offering practical insights derived from notable cybersecurity incidents. Leroy meticulously analyzes these cases, extracting valuable lessons that readers can apply to fortify their own cybersecurity defenses. 4. Collaboration and Leadership: Recognizing the collaborative nature of cybersecurity, Leroy emphasizes the role of leadership and effective governance. The book provides guidance on establishing security-conscious cultures, fostering collaboration with third-party partners, and aligning cybersecurity efforts with broader business goals. 5. Continuous Improvement and Adaptation: Leroy champions the concept of continuous improvement, urging readers to adapt to evolving threats. From establishing a learning culture within organizations to incorporating feedback into strategies, the book serves as a roadmap for staying ahead in the dynamic cybersecurity landscape. 6. Future-proofing Strategies: In a forward-looking exploration, Leroy anticipates future threats and trends. The book covers innovations in cybersecurity technologies, the integration of AI and predictive analytics, and strategies for preparing for emerging challenges. Readers gain insights into future-proofing their cybersecurity initiatives. "Mastering Cybersecurity Risk Management" by Benoit Leroy is your definitive guide to conquering the challenges of the digital era. With a focus on practical strategies and real-world applications, this book transcends conventional cybersecurity guides. Leroy, a recognized authority in the field, demystifies complex concepts, making them accessible to both novices and seasoned professionals. Leroy's approach is not just theoretical; it's a roadmap crafted from years of hands-on experience. From risk management frameworks to the nuances of regulatory compliance, each chapter equips you with actionable strategies. In "Mastering Cybersecurity Risk Management," Benoit Leroy doesn't just share knowledge; he invites you to embark on a transformative journey. Whether you're an aspiring cybersecurity professional, a business leader, or an enthusiast, this book arms you with the tools to not only survive but thrive in the ever-changing digital landscape. Make it your companion in the pursuit of cybersecurity excellence.

Cybersecurity Threats, Malware Trends, and Strategies BPB Publications
An advanced Domain Name System (DNS) security resource that explores the operation of DNS, its vulnerabilities, basic security approaches, and mitigation strategies DNS Security Management offers an overall role-based security approach and discusses the various threats to the Domain Name Systems (DNS). This vital resource is filled with proven strategies for detecting and mitigating these all too frequent threats. The authors—noted experts on the topic—offer an introduction to the role of DNS and explore the operation of DNS. They cover a myriad of DNS vulnerabilities and include preventative strategies that can be implemented. Comprehensive in scope, the text shows how to secure DNS resolution with the Domain Name System Security Extensions (DNSSEC). In addition, the text includes discussions on security applications facility by DNS, such as anti-spam, SPF, DANE and related CERT/SSHFP records. This important resource: Presents security approaches for the various types of DNS deployments by role (e.g., recursive vs. authoritative) Discusses DNS resolvers including host access protections, DHCP configurations and DNS recursive server IPs Examines DNS data collection, data analytics, and detection strategies With cyber attacks ever on the rise worldwide, DNS Security Management offers network engineers a much-needed resource that provides a clear understanding of the threats to networks in order to mitigate the risks and assess the strategies to defend against threats.
Cyber-Security Threats, Actors, and Dynamic Mitigation Independently Published
Updated edition of the bestselling guide for planning attack and defense strategies based on the current threat landscape Key FeaturesUpdated for ransomware prevention, security posture management in multi-cloud, Microsoft Defender for Cloud, MITRE ATT&CK Framework, and moreExplore the latest tools for ethical hacking, pentesting, and Red/Blue teamingIncludes recent real-world examples to illustrate the best practices to improve security postureBook Description Cybersecurity – Attack and Defense Strategies, Third Edition will bring you up to speed with the key aspects of threat assessment and security hygiene, the current threat landscape and its challenges, and how to maintain a strong security posture. In this carefully revised new edition, you will learn about the Zero Trust approach and the initial Incident Response process. You will gradually become familiar with Red Team tactics, where you will learn basic syntax for commonly used tools to perform the necessary operations. You will also learn how to apply newer Red Team techniques with powerful tools. Simultaneously, Blue Team tactics are introduced to help you defend your system from complex cyber-attacks. This book provides a clear, in-depth understanding of attack/defense methods as well as patterns to recognize irregular behavior within your organization. Finally, you will learn how to analyze your network and address malware, while becoming familiar with mitigation and threat detection techniques. By the end of this cybersecurity book, you will have discovered the latest tools to enhance the security of your system, learned about the security controls you need, and understood how to carry out each step of the incident response process. What you will learnLearn to mitigate, recover from, and prevent future cybersecurity eventsUnderstand security hygiene and value of prioritizing protection of your workloadsExplore physical and virtual network segmentation, cloud network visibility, and Zero Trust considerationsAdopt new methods to gather cyber intelligence, identify risk, and demonstrate impact with Red/Blue Team strategiesExplore legendary tools such as Nmap and Metasploit to supercharge your Red TeamDiscover identity security and how to perform policy enforcementIntegrate threat detection systems into your SIEM solutionsDiscover the MITRE ATT&CK Framework and open-source tools to gather intelligenceWho this book is for If you are an IT security professional who wants to venture deeper into cybersecurity domains, this book is for you. Cloud security administrators, IT pentesters, security consultants, and ethical hackers will also find this book useful. Basic understanding of operating systems, computer networking, and web applications will be helpful.
Industrial Cybersecurity CRC Press
A comprehensive guide for cybersecurity professionals to acquire unique insights on the evolution of the threat landscape and how you can address modern cybersecurity challenges in your organisation Key FeaturesProtect your organization from cybersecurity threats with field-tested strategiesDiscover the most common ways enterprises initially get compromisedMeasure the effectiveness of your organization's current cybersecurity program against cyber attacksBook Description After scrutinizing numerous cybersecurity strategies, Microsoft's former Global Chief Security Advisor in this book helps you understand the efficacy of popular cybersecurity strategies and more. Cybersecurity Threats, Malware Trends, and Strategies offers an unprecedented long-term view of the global threat landscape by examining the twenty-year trend in vulnerability disclosures and exploitation, nearly a decade of regional differences in malware infections, the socio-economic factors that underpin them, and how global malware has evolved. This will give you further perspectives into malware protection for your organization. It also examines internet-based threats that CISOs should be aware of. The book will provide you with an evaluation of the various cybersecurity strategies that have ultimately failed over the past twenty years, along with one or two that have actually worked. It will help executives and security and compliance professionals understand how cloud computing is a game changer for them. By the end of this book, you will know how to measure the effectiveness of your organization's cybersecurity strategy and the efficacy of the vendors you employ to help you protect your organization and yourself. What you will learnDiscover cybersecurity strategies and the ingredients critical to their successImprove vulnerability management by reducing risks and costs for your organizationLearn how malware and other threats have evolved over the past decadeMitigate internet-based threats, phishing attacks, and malware distribution sitesWeigh the pros and cons of popular cybersecurity strategies of the past two decadesImplement and then measure the outcome of a cybersecurity strategyLearn how the cloud provides better security capabilities than on-premises IT environmentsWho this book is for This book is designed to benefit engineers, leaders, or any professional with either a responsibility for cyber security within their organization, or an interest in working in this ever-growing field.
The Insider Threat John Wiley & Sons
Industrial control systems are an integral part of critical infrastructure, helping facilitate operations in vital sectors such as electricity, oil and gas, water, transportation, and chemical. A growing issue with cybersecurity and its impact on industrial control systems have highlighted some fundamental risks to critical infrastructures. To address cybersecurity issues for industrial control systems, a clear understanding of the security challenges and specific defensive

countermeasures is required. A holistic approach, one that uses specific countermeasures to create an aggregated security posture, can help defend against cybersecurity threats and vulnerabilities that affect an industrial control system. This approach, often referred to as "defense-in-depth," can be applied to industrial control systems and can provide for a flexible and useable framework for improving cybersecurity defenses. Concerns in regard to cybersecurity and control systems are related to both the legacy nature of some of the systems as well as the growing trend to connect industrial control systems to other networks. These concerns have lead to a number of identified vulnerabilities and have introduced new categories of threats that have not been seen before in the industrial control systems domain. Many of the legacy systems may not have appropriate security capabilities that can defend against modern day threats, and the requirements for availability can preclude using contemporary cybersecurity solutions. An industrial control system's connectivity to a corporate, vendor, or peer network can exacerbate this problem. This book provides insight into some of the more prominent cyber risk issues and presents them in the context of industrial control systems. It provides commentary on how mitigations strategies can be developed for specific problems and provides direction on how to create a defense-in-depth security program for control system environments. The goal is to provide guidance regarding cyber mitigation strategies and how to apply them specifically to an industrial control systems environment.

Cybersecurity – Attack and Defense Strategies John Wiley & Sons

Build an effective vulnerability management strategy to protect your organization’s assets, applications, and data. Today’s network environments are dynamic, requiring multiple defenses to mitigate vulnerabilities and stop data breaches. In the modern enterprise, everything connected to the network is a target. Attack surfaces are rapidly expanding to include not only traditional servers and desktops, but also routers, printers, cameras, and other IOT devices. It doesn’t matter whether an organization uses LAN, WAN, wireless, or even a modern PAN—savvy criminals have more potential entry points than ever before. To stay ahead of these threats, IT and security leaders must be aware of exposures and understand their potential impact. Asset Attack Vectors will help you build a vulnerability management program designed to work in the modern threat environment. Drawing on years of combined experience, the authors detail the latest techniques for threat analysis, risk measurement, and regulatory reporting. They also outline practical service level agreements (SLAs) for vulnerability management and patch management. Vulnerability management needs to be more than a compliance check box; it should be the foundation of your organization’s cybersecurity strategy. Read Asset Attack Vectors to get ahead of threats and protect your organization with an effective asset protection strategy. What You’ll Learn Create comprehensive assessment and risk identification policies and procedures Implement a complete vulnerability management workflow in nine easy steps Understand the implications of active, dormant, and carrier vulnerability states Develop, deploy, and maintain custom and commercial vulnerability management programs Discover the best strategies for vulnerability remediation, mitigation, and removal Automate credentialed scans that leverage least-privilege access principles Read real-world case studies that share successful strategies and reveal potential pitfalls Who This Book Is For New and intermediate security management professionals, auditors, and information technology staff looking to build an effective vulnerability management program and defend against asset based cyberattacks

Modern Cybersecurity Strategies for Enterprises CRC Press

Advance your career as an information security professional by turning theory into robust solutions to secure your organization Key FeaturesConvert the theory of your security certifications into actionable changes to secure your organizationDiscover how to structure policies and procedures in order to operationalize your organization's information security strategyLearn how to achieve security goals in your organization and reduce software riskBook Description Information security and risk management best practices enable professionals to plan, implement, measure, and test their organization's systems and ensure that they're adequately protected against threats. The book starts by helping you to understand the core principles of information security, why risk management is important, and how you can drive information security governance. You'll then explore methods for implementing security controls to achieve the organization's information security goals. As you make progress, you'll get to grips with design principles that can be utilized along with methods to assess and mitigate architectural vulnerabilities. The book will also help you to discover best practices for designing secure network architectures and controlling and managing third-party identity services. Finally, you will learn about designing and managing security testing processes, along with ways in which you can improve software security. By the end of this infosec book, you'll have learned how to make your organization less vulnerable to threats and reduce the likelihood and impact of exploitation. As a result, you will be able to make an impactful change in your organization toward a higher level of information security. What you will learnUnderstand and operationalize risk management concepts and important security operations activitiesDiscover how to identify, classify, and maintain information and assetsAssess and mitigate vulnerabilities in information systemsDetermine how security control testing will be undertakenIncorporate security into the SDLC (software development life cycle)Improve the security of developed software and mitigate the risks of using unsafe softwareWho this book is for If you are looking to begin your career in an information security role, then this book is for you. Anyone who is studying to achieve industry-standard certification such as the CISSP or CISM, but looking for a way to convert concepts (and the seemingly endless number of acronyms) from theory into practice and start making a difference in your day-to-day work will find this book useful.

Cyber Security and Adversarial Machine Learning Independently Published

Optimal Spending on Cybersecurity Measures: DevOps aims to discuss the integration of risk management methodologies within the DevOps process. This book introduces the cyber risk investment model, and the cybersecurity risk management framework within the DevOps process. This can be used by various stakeholders who are involved in the implementation of cybersecurity measures to safeguard sensitive data. This framework facilitates an organization’s risk management decision-making process to demonstrate the mechanisms in place to fund cybersecurity measures within DevOps practices, and demonstrates the application of the process using a case study: Cascade. This book also discusses the elements used within DevOps, DevSecOps, and will define a strategic

approach to minimize cybersecurity risks within DevOps known as DevRiskOps. Features: Aims to strengthen the reader’s understanding of industry governance, risk and compliance practices. Incorporates an innovative approach to assess cyber security initiatives with DevOps. Explores the strategic decisions made by organizations when implementing cybersecurity measures and leverages an integrated approach to include risk management elements into DevOps.
Threat Hunting in the Cloud Notion Press
Cybersecurity Risk Management In Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework, veteran technology analyst Cynthia Brumfield, with contributions from cybersecurity expert Brian Haugli, delivers a straightforward and up-to-date exploration of the fundamentals of cybersecurity risk planning and management. The book offers readers easy-to-understand overviews of cybersecurity risk management principles, user, and network infrastructure planning, as well as the tools and techniques for detecting cyberattacks. The book also provides a roadmap to the development of a continuity of operations plan in the event of a cyberattack. With incisive insights into the Framework for Improving Cybersecurity of Critical Infrastructure produced by the United States National Institute of Standards and Technology (NIST), Cybersecurity Risk Management presents the gold standard in practical guidance for the implementation of risk management best practices. Filled with clear and easy-to-follow advice, this book also offers readers: A concise introduction to the principles of cybersecurity risk management and the steps necessary to manage digital risk to systems, assets, data, and capabilities A valuable exploration of modern tools that can improve an organization’s network infrastructure protection A practical discussion of the challenges involved in detecting and responding to a cyberattack and the importance of continuous security monitoring A helpful examination of the recovery from cybersecurity incidents Perfect for undergraduate and graduate students studying cybersecurity, Cybersecurity Risk Management is also an ideal resource for IT professionals working in private sector and government organizations worldwide who are considering implementing, or who may be required to implement, the NIST Framework at their organization.
Cyber Strategy Springer
Written in an easy to understand style, this book provides a comprehensive overview of the physical-cyber security of Industrial Control Systems benefitting the computer science and automation engineers, students and industrial cyber security agencies in obtaining essential understanding of the ICS cyber security from concepts to realization. The Book Ø Covers ICS networks, including zone based architecture and its deployment for product delivery and other Industrial services. Ø Discusses SCADA networking with required cryptography and secure industrial communications. Ø Furnishes information about industrial cyber security standards presently used. Ø Explores defence-in-depth strategy of ICS from conceptualisation to materialisation. Ø Provides many real-world documented examples of attacks against industrial control systems and mitigation techniques. Ø Is a suitable material for Computer Science and Automation engineering students to learn the fundamentals of industrial cyber security.
Risk Management Program Guide Oxford University Press
Key Features Gain a clear understanding of the attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics Learn to unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies A practical guide that will give you hands-on experience to mitigate risks and prevent attackers from infiltrating your system Book DescriptionThe book will start talking about the security posture before moving to Red Team tactics, where you will learn the basic syntax for the Windows and Linux tools that are commonly used to perform the necessary operations. You will also gain hands-on experience of using new Red Team techniques with powerful tools such as python and PowerShell, which will enable you to discover vulnerabilities in your system and how to exploit them. Moving on, you will learn how a system is usually compromised by adversaries, and how they hack user's identity, and the various tools used by the Red Team to find vulnerabilities in a system. In the next section, you will learn about the defense strategies followed by the Blue Team to enhance the overall security of a system. You will also learn about an in-depth strategy to ensure that there are security controls in each network layer, and how you can carry out the recovery process of a compromised system. Finally, you will learn how to create a vulnerability management strategy and the different techniques for manual log analysis.What you will learn Learn the importance of having a solid foundation for your security posture Understand the attack strategy using cyber security kill chain Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence Learn how to perform an incident investigation Get an in-depth understanding of the recovery process Understand continuous security monitoring and how to implement a vulnerability management strategy Learn how to perform log analysis to identify suspicious activities Who this book is for This book aims at IT professional who want to venture the IT security domain. IT pentester, Security consultants, and ethical hackers will also find this course useful. Prior knowledge of penetration testing would be beneficial.