The Computer Incident Response Planning Handbook Executable Plans For Protecting Information At Risk

Computer Incident Response and Product Security
Responding to Targeted Cyberattacks
Computer Security Incident Handling Guide (draft) :.
Ten Strategies of a World-Class Cybersecurity Operations Center
Computer Forensics
Trinity
Security Incidents & Response Against Cyber Attacks
Information Security Policies, Procedures, and Standards
Principles of Incident Response and Disaster Recovery
Investigating Computer Crime
The Art of Scalability

Computer Security Incident Response Planning at Nuclear Facilities
How to Contain, Eradicate, and Recover from Incidents
Incident Response in the Age of Cloud
Computer Incident Response and Product Security
Physical Security for IT
Computer Incident Response and Forensics Team Management
A Holistic Approach for an Efficient Security Incident Management.
A Practitioner's Reference
Digital Forensics and Incident Response
Cybersecurity Blue Team Toolkit
A Strategic Guide to Handling System and Network Security Breaches
The Digital Forensics Guide for the Network Engineer
The CIO’s Guide to Information Security Incident Management
Intelligence-Driven Incident Response
Incident Response
COMPUTER SECURITY INCIDENT RESPONSE PLANNING AT NUCLEAR FACILITIES (SPANISH EDITION).
Organizational Approach to Managing Residual Risk
Incident Handling and Response
Incident Response Essentials
Cybersecurity Resilience Planning Handbook
Computer Incident Response and Product

Security
Threat Analysis and Response Solutions
Crafting the InfoSec Playbook
Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition
Conducting a Successful Incident Response
Principles of Incident Response and Disaster Recovery
Outwitting the Adversary
Applied Incident Response
Scalable Web Architecture, Processes, and Organizations for the Modern Enterprise

ANGEL MARIELA

Computer Incident Response and Product Security

Packt Publishing Ltd

You will be breached—the only question is whether you'll be ready A cyber breach could cost your organization millions of dollars—in 2019, the average cost of a cyber breach for companies was $3.9M, a figure that is increasing 20-30% annually. But effective planning can lessen the impact and duration of an inevitable cyberattack. Cyber Breach Response That Actually Works provides a business-focused methodology that will allow you to address the aftermath of a cyber breach and reduce its

impact to your enterprise. This book goes beyond step-by-step instructions for technical staff, focusing on big-picture planning and strategy that makes the most business impact. Inside, you'll learn what drives cyber incident response and how to build effective incident response capabilities. Expert author Andrew Gorecki delivers a vendor-agnostic approach based on his experience with Fortune 500 organizations. Understand the evolving threat landscape and learn how to address tactical and strategic challenges to build a comprehensive and cohesive cyber breach response program Discover how incident response fits within your overall information security program, including a look at risk management Build a capable incident response team and create an actionable incident response plan to prepare for cyberattacks and minimize their impact to your organization Effectively investigate small and large-scale incidents and recover faster by leveraging proven industry practices Navigate legal issues impacting incident response, including laws and regulations, criminal cases

and civil litigation, and types of evidence and their admissibility in court In addition to its valuable breadth of discussion on incident response from a business strategy perspective, Cyber Breach Response That Actually Works offers information on key technology considerations to aid you in building an effective capability and accelerating investigations to ensure your organization can continue business operations during significant cyber events. Responding to Targeted Cyberattacks John Wiley & Sons As security professionals, our job is to reduce the level of risk to our organization from cyber security threats. However Incident prevention is never 100% achievable. So, the best option is to have a proper and efficient security Incident Management established in the organizationT his book provides a holistic approach for an efficient IT security Incident Management. Key topics includes,1) Attack vectors and counter measures 2) Detailed Security Incident handling framework explained in six phases._Prepa ration_Identifi cation_Contain ment_Eradicat ion_Recovery_ Lessons Learned/Follo w-up3)

Building an Incident response plan and key elements for an efficient incident response.4) Building Play books.5) How to classify and prioritize incidents.6) Proactive Incident management. 7) How to conduct a table-top exercise.8) How to write an RCA report /Incident Report.9) Briefly explained the future of Incident management. Also includes sample templates on playbook, table-top exercise, Incident Report, Guidebook.

Computer Security Incident Handling Guide (draft) :. Pearson Education

PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Revised and updated with the latest data in the field, the Second Edition of Managing Risk in Information Systems provides a comprehensive overview of the SSCP(r) Risk, Response, and Recovery Domain in addition to providing a thorough overview of risk management and its implications on IT infrastructures and compliance. Written by industry experts, and using a wealth of examples and exercises, this book incorporates hands-on activities to walk the reader through the

fundamentals of risk management, strategies and approaches for mitigating risk, and the anatomy of how to create a plan that reduces risk. Instructor's Material for Managing Risk in Information Systems include: PowerPoint Lecture Slides Instructor's Guide Course Syllabus Quiz & Exam Questions Case Scenarios/Handouts

Ten Strategies of a World-Class Cybersecurity Operations Center CRC Press "This book describes how to apply application threat modeling as an advanced preventive form of security"--

Computer Forensics ISACA Computer Incident Response and Forensics Team Management provides security professionals with a complete handbook of computer incident response from the perspective of forensics team management. This unique approach teaches readers the concepts and principles they need to conduct a successful incident response investigation, ensuring that proven policies and procedures are established and followed by all team members. Leighton R. Johnson III describes the processes within an incident response event and shows the

crucial importance of skillful forensics team management, including when and where the transition to forensics investigation should occur during an incident response event. The book also provides discussions of key incident response components. Provides readers with a complete handbook on computer incident response from the perspective of forensics team management Identify the key steps to completing a successful computer incident response investigation Defines the qualities necessary to become a successful forensics investigation team member, as well as the interpersonal relationship skills necessary for successful incident response and forensics investigation teams *Trinity* John Wiley & Sons A practical guide to deploying digital forensic techniques in response to cyber security incidents About This Book Learn incident response fundamentals and create an effective incident response framework Master forensics investigation utilizing digital investigative techniques Contains real-life scenarios that effectively use threat intelligence and modeling techniques Who This Book

Is For This book is targeted at Information Security professionals, forensics practitioners, and students with knowledge and experience in the use of software applications and basic command-line experience. It will also help professionals who are new to the incident response/digital forensics role within their organization. What You Will Learn Create and deploy incident response capabilities within your organization Build a solid foundation for acquiring and handling suitable evidence for later analysis Analyze collected evidence and determine the root cause of a security incident Learn to integrate digital forensic techniques and procedures into the overall incident response process Integrate threat intelligence in digital evidence analysis Prepare written documentation for use internally or with external parties such as regulators or law enforcement agencies In Detail Digital Forensics and Incident Response will guide you through the entire spectrum of tasks associated with incident response, starting with preparatory activities associated with creating an incident response plan

and creating a digital forensics capability within your own organization. You will then begin a detailed examination of digital forensic techniques including acquiring evidence, examining volatile memory, hard drive assessment, and network-based evidence. You will also explore the role that threat intelligence plays in the incident response process. Finally, a detailed section on preparing reports will help you prepare a written report for use either internally or in a courtroom. By the end of the book, you will have mastered forensic techniques and incident response and you will have a solid foundation on which to increase your ability to investigate such incidents in your organization. Style and approach The book covers practical scenarios and examples in an enterprise setting to give you an understanding of how digital forensics integrates with the overall response to cyber security incidents. You will also learn the proper use of tools and techniques to investigate common cyber security incidents such as malware infestation, memory analysis, disk analysis, and network analysis.

Security Incidents & Response Against Cyber Attacks Sams Uncertainty and risk, meet planning and action. Reinforce your organization's security posture using the expert information contained in this tactical guide. The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk shows you how to build and manage successful response plans for the cyber incidents that have become inevitable for organizations of any size. Find out why these plans work. Learn the step-by-step process for developing and managing plans built to address the wide range of issues organizations face in times of crisis. Contains the essentials for developing both data breach and malware outbreak response plans—and best practices for maintaining those plans Features ready-to-implement CIRPs—derived from living incident response plans that have survived the rigors of repeated execution and numerous audits Clearly explains how to minimize the risk of post-event litigation, brand impact, fines and penalties—and how to protect shareholder value Supports corporate

compliance with industry standards and requirements, including PCI, HIPAA, SOX, and CA SB-24

Information Security Policies, Procedures, and Standards

Newnes

The Comprehensive, Proven Approach to IT Scalability–Updated with New Strategies, Technologies, and Case Studies In The Art of Scalability, Second Edition, leading scalability consultants Martin L. Abbott and Michael T. Fisher cover everything you need to know to smoothly scale products and services for any requirement. This extensively revised edition reflects new technologies, strategies, and lessons, as well as new case studies from the authors' pioneering consulting practice, AKF Partners. Writing for technical and nontechnical decision-makers, Abbott and Fisher cover everything that impacts scalability, including architecture, process, people, organization, and technology. Their insights and recommendations reflect more than thirty years of experience at companies ranging from eBay to Visa, and Salesforce.com to Apple. You'll find updated strategies for structuring organizations to maximize agility and

scalability, as well as new insights into the cloud (IaaS/PaaS) transition, NoSQL, DevOps, business metrics, and more. Using this guide's tools and advice, you can systematically clear away obstacles to scalability–and achieve unprecedented IT and business performance. Coverage includes • Why scalability problems start with organizations and people, not technology, and what to do about it • Actionable lessons from real successes and failures • Staffing, structuring, and leading the agile, scalable organization • Scaling processes for hyper-growth environments • Architecting scalability: proprietary models for clarifying needs and making choices–including 15 key success principles • Emerging technologies and challenges: data cost, datacenter planning, cloud evolution, and customer-aligned monitoring • Measuring availability, capacity, load, and performance

Principles of Incident Response and Disaster Recovery

Cisco Press

"The purpose of this publication is to assist Member States in developing comprehensive contingency plans for computer security

incidents with the potential to impact nuclear security and/or nuclear safety. It provides an outline and recommendations for establishing a computer security incident response capability as part of a computer security programme, and considers the roles and responsibilities of the system owner, operator, competent authority, and national technical authority in responding to a computer security incident with possible nuclear security repercussions. "--Publisher's description.

Investigating Computer Crime

"O'Reilly Media, Inc." Every computer crime leaves tracks–you just have to know where to find them. This book shows you how to collect and analyze the digital evidence left behind in a digital crime scene. Computers have always been susceptible to unwanted intrusions, but as the sophistication of computer technology increases so does the need to anticipate, and safeguard against, a corresponding rise in computer-related criminal activity. Computer forensics, the newest branch of computer security, focuses on the aftermath of a computer security incident. The goal of computer

forensics is to conduct a structured investigation to determine exactly what happened, who was responsible, and to perform the investigation in such a way that the results are useful in a criminal proceeding. Written by two experts in digital investigation, Computer Forensics provides extensive information on how to handle the computer as evidence. Kruse and Heiser walk the reader through the complete forensics process–from the initial collection of evidence through the final report. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present your evidence and conclusions in court. Unique forensic issues associated with both the Unix and the Windows NT/2000 operating systems are thoroughly covered. This book provides a detailed methodology for collecting, preserving, and effectively using evidence by addressing the three A's of computer forensics: Acquire the evidence without altering or damaging the original data. Authenticate that your recorded evidence is the same as the original seized data. Analyze the data without modifying the

recovered data. Computer Forensics is written for everyone who is responsible for investigating digital criminal incidents or who may be interested in the techniques that such investigators use. It is equally helpful to those investigating hacked web servers, and those who are investigating the source of illegal pornography. *The Art of Scalability* LexisNexis Information Security Policies, Procedures, and Standards: A Practitioner's Reference gives you a blueprint on how to develop effective information security policies and procedures. It uses standards such as NIST 800-53, ISO 27001, and COBIT, and regulations such as HIPAA and PCI DSS as the foundation for the content. Highlighting key terminology, policy development concepts and methods, and suggested document structures, it includes examples, checklists, sample policies and procedures, guidelines, and a synopsis of the applicable standards. The author explains how and why procedures are developed and implemented rather than simply provide information and examples. This is an important distinction because no

two organizations are exactly alike; therefore, no two sets of policies and procedures are going to be exactly alike. This approach provides the foundation and understanding you need to write effective policies, procedures, and standards clearly and concisely. Developing policies and procedures may seem to be an overwhelming task. However, by relying on the material presented in this book, adopting the policy development techniques, and examining the examples, the task will not seem so daunting. You can use the discussion material to help sell the concepts, which may be the most difficult aspect of the process. Once you have completed a policy or two, you will have the courage to take on even more tasks. Additionally, the skills you acquire will assist you in other areas of your professional and private life, such as expressing an idea clearly and concisely or creating a project plan.

Computer Security Incident Response Planning at Nuclear Facilities CRC Press

"This book provides a valuable resource by addressing the most pressing issues facing cyber-security from both a national and global

perspective"--Provided by publisher.

How to Contain, Eradicate, and Recover from Incidents

Apress

Learn how to identify vulnerabilities within computer networks and implement countermeasures that mitigate risks and damage with Whitman/Mattord's PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 3rd Edition. This edition offers the knowledge you need to help organizations prepare for and avert system interruptions and natural disasters. Comprehensive coverage addresses information security and IT in contingency planning today. Updated content focuses on incident response and disaster recovery. You examine the complexities of organizational readiness from an IT and business perspective with emphasis on management practices and policy requirements. You review industry's best practices for minimizing downtime in emergencies and curbing losses during and after system service interruptions. This edition includes the latest NIST knowledge, expanded coverage of security information and event management (SIEM) and unified threat management,

and more explanations of cloud-based systems and Web-accessible tools to prepare you for success. **Incident Response in the Age of Cloud** Packt Publishing Ltd The physical security of IT, network, and telecommunications assets is equally as important as cyber security. We justifiably fear the hacker, the virus writer and the cyber terrorist. But the disgruntled employee, the thief, the vandal, the corporate foe, and yes, the terrorist can easily cripple an organization by doing physical damage to IT assets. In many cases such damage can be far more difficult to recover from than a hack attack or malicious code incident. It does little good to have great computer security if wiring closets are easily accessible or individuals can readily walk into an office and sit down at a computer and gain access to systems and applications. Even though the skill level required to hack systems and write viruses is becoming widespread, the skill required to wield an ax, hammer, or fire hose and do thousands of dollars in damage is even more common. Although many books cover computer security from one perspective or another, they do not

thoroughly address physical security. This book shows organizations how to design and implement physical security plans. It provides practical, easy-to-understand and readily usable advice to help organizations to improve physical security for IT, network, and telecommunications assets. * Expert advice on identifying physical security needs * Guidance on how to design and implement security plans to prevent the physical destruction of, or tampering with computers, network equipment, and telecommunications systems * Explanation of the processes for establishing a physical IT security function * Step-by-step instructions on how to accomplish physical security objectives * Illustrations of the major elements of a physical IT security plan * Specific guidance on how to develop and document physical security methods and procedures

Computer Incident Response and Product Security

Cisco Systems Incident response is a multidisciplinary science that resolves computer crime and complex legal issues, chronological methodologies and technical computer techniques. The

commercial industry has embraced and adopted technology that detects hacker incidents. Companies are swamped with real attacks, yet very few have any methodology or knowledge to resolve these attacks. Incident Response: Investigating Computer Crime will be the only book on the market that provides the information on incident response that network professionals need to conquer attacks. *Physical Security for IT* The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk Learn how to build a Security Incident Response team with guidance from a leading SIRT from Cisco Gain insight into the best practices of one of the foremost incident response teams Master your plan for building a SIRT (Security Incidence Response Team) with detailed guidelines and expert advice for incident handling and response Review legal issues from a variety of national perspectives, and consider practical aspects of coordination with other organizations "Network Security Incident Response" provides practical guidelines for building an SIRT team as

well offering advice on responding to actual incidents. For many companies, incident response is new territory. Some companies do not have an incidence response team at all. Some would like to have one but need guidance to start and others would like to improve existing practices. Today, there are only a handful of organizations that do have mature and experienced teams. For that reason this book is structured to provide help in both creating and running an effective Security Incident Response Team. Organizations who are evaluating whether to invest in a SIRT or who are just getting started building one will find the information in this book to be invaluable in helping them understand the nature of the threats, justifying resources, and building effective IR (Incidence Response) teams. Established IR teams will also benefit from the best practices highlighted in building IR teams as well as information on the current state of incident response handling, incident coordination, and legal issues. Written by a leading SIRT (Security Incident Response Team) from Cisco, the

expertise and guidance provided in this book will serve as the blueprint for successful incidence response planning for most any organization.

Computer Incident Response and Forensics Team Management

John Wiley & Sons

This book provides use case scenarios of machine learning, artificial intelligence, and real-time domains to supplement cyber security operations and proactively predict attacks and preempt cyber incidents. The authors discuss cybersecurity incident planning, starting from a draft response plan, to assigning responsibilities, to use of external experts, to equipping organization teams to address incidents, to preparing communication strategy and cyber insurance. They also discuss classifications and methods to detect cybersecurity incidents, how to organize the incident response team, how to conduct situational awareness, how to contain and eradicate incidents, and how to cleanup and recover. The book shares real-world experiences and knowledge from authors from academia and industry.

A Holistic Approach for an Efficient Security Incident

Management. Elsevier An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is a must for all organizations. This book offers concrete and detailed guidance on how to conduct the full spectrum of incident response and digital forensic activities.

A Practitioner's Reference Pearson Education "This reference book considers all emerging aspects of cybersecurity in the business sector including frameworks, models, best practices, and emerging areas of interest, discussing items such as audits and risk assessments that businesses can conduct to ensure the security of their systems, training and awareness initiatives for staff that promotes a security culture and software and systems that can be used to secure and manage cybersecurity threats"--

Digital Forensics and Incident Response Packt Publishing Ltd This book will help IT and business operations managers who have been tasked with addressing security issues. It provides a solid understanding of security incident response and detailed guidance in

the setting up and running of specialist incident management teams. Having an incident response plan is required for compliance with government regulations, industry standards such as PCI DSS, and certifications such as ISO 27001. This book will help organizations meet those compliance requirements.

Related with The Computer Incident Response Planning Handbook Executable Plans For Protecting Information At Risk:
• What Language Is Spoken In Egypt Today : click here