Principles Of Incident Response And Disaster Recovery

Principles of Incident Response and Disaster Recovery
The Experience Economy
Computer Security Incident Handling Guide (draft) :.
Principles and Practice
PMS-210
How to Contain, Eradicate, and Recover from Incidents
Site Reliability Engineering
How Google Runs Production Systems
Building an Effective Incident Management Plan
Practical Windows Forensics
Traffic Incident Management Handbook
Conducting a Successful Incident Response
Digital Forensics and Incident Response
Developing Cybersecurity Programs and Policies
97 Things Every Information Security Professional Should Know
Incident Management for Operations
Principles of Information Security
The Practice of Network Security Monitoring
Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition
Understanding Incident Detection and Response
The Site Reliability Workbook
Cybersecurity Incident Response
Outwitting the Adversary
Principles and Practices
The CIO’s Guide to Information Security Incident Management
Principles of Information Security
Hazardous Materials Incidents
Principles of Information Security, Loose-Leaf Version
Principles, Methods and Applications
Surviving the Initial Response
Ten Strategies of a World-Class Cybersecurity Operations Center
Principles for Cyber Security Operations
Disaster Recovery
Principles of Information Security
Computer Incident Response and Forensics Team Management
GCIH GIAC Certified Incident Handler All-in-One Exam Guide
Incident Response & Computer Forensics, Third Edition
How action-based intelligence can be an effective response to incidents

AVERY MICHAEL

Principles of Incident Response and Disaster Recovery Cengage Learning
Discover the latest trends, developments and technology in information security today with Whitman/Mattord's market-leading PRINCIPLES OF INFORMATION SECURITY, 7th Edition. Designed specifically to meet the needs of those studying information systems, this edition's balanced focus addresses all aspects of information security, rather than simply offering a technical control perspective. This overview explores important terms and examines what is needed to manage an effective information security program. A new module details incident response and detection strategies. In addition, current, relevant updates highlight the latest practices in security operations as well as legislative issues, information management toolsets and digital forensics. Coverage of the most recent policies and guidelines that correspond to federal and international standards further prepare you for success both in information systems and as a business decision-maker. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
The Experience Economy No Starch Press
Your one stop solution to implement a Cyber Defense Intelligence program in to your organisation. Key Features Intelligence processes and procedures for response mechanisms Master F3EAD to drive processes based on intelligence Threat modeling and intelligent frameworks Case studies and how to go about building intelligent teams Book Description Cyber intelligence is the missing link between your cyber defense operation teams, threat intelligence, and IT operations to provide your organization with a full spectrum of defensive capabilities. This book kicks off with the need for cyber intelligence and why it is required in terms of a defensive framework. Moving forward, the book provides a practical explanation of the F3EAD protocol with the help of examples. Furthermore, we learn how to go about threat models and intelligence products/frameworks and apply them to real-life scenarios. Based on the discussion with the prospective author I would also love to explore the induction of a tool to enhance the marketing feature and functionality of the book. By the end of this book, you will be able to boot up an intelligence program in your organization based on the operation and tactical/strategic spheres of Cyber defense intelligence. What you will learn Learn about the Observe-Orient-Decide-Act (OODA) loop and it's applicability to security Understand tactical view of Active defense concepts and their application in today's threat landscape Get acquainted with an operational view of the F3EAD process to drive decision making within an organization Create a Framework and Capability Maturity Model that integrates inputs and outputs from key functions in an information security organization Understand the idea of communicating with the Potential for Exploitability based on cyber intelligence Who this book is for This book targets incident managers, malware analysts, reverse engineers, digital forensics specialists, and intelligence analysts; experience in, or knowledge of, security operations, incident responses or investigations is desirable so you can make the most of the subjects presented.
Computer Security Incident Handling Guide (draft) :. "O'Reilly Media, Inc."
Discover the latest trends, developments and technology in information security with Whitman/Mattord's market-leading PRINCIPLES OF INFORMATION SECURITY, 7th Edition. Designed specifically to meet the needs of information systems students like you, this edition's balanced focus addresses all aspects of information security, rather than simply offering a technical control perspective. This overview explores important terms and examines what is needed to manage an effective information security program. A new module details incident response and detection strategies. In addition, current, relevant updates highlight the latest practices in security operations as well as legislative issues, information management toolsets, digital forensics and the most recent policies and guidelines that correspond to federal and international standards. MindTap digital resources offer interactive content to further strength your success as a business decision-maker.
Principles and Practice Newnes
Cyber Security – Essential principles to secure your organisation takes you through the fundamentals of cyber security, the principles that underpin it, vulnerabilities and threats, and how to defend against attacks.
PMS-210 "O'Reilly Media, Inc."
In 2016, Google’s Site Reliability Engineering book ignited an industry discussion on what it means to run production services today—and why reliability considerations are fundamental to service design. Now, Google engineers who worked on that bestseller introduce The Site Reliability Workbook, a hands-on companion that uses concrete examples to show you how to put SRE principles and practices to work in your environment. This new workbook not only combines practical examples from Google’s experiences, but also provides case studies from Google’s Cloud Platform customers who underwent this journey. Evernote, The Home Depot, The New York Times, and other companies outline hard-won experiences of what worked for them and what didn’t. Dive into this workbook and learn how to flesh out your own SRE practice, no matter what size your company is. You’ll learn: How to run reliable services in environments you don’t completely control—like cloud Practical applications of how to create, monitor, and run your services via Service Level Objectives How to convert existing ops teams to SRE—including how to dig out of operational overload Methods for starting SRE from either greenfield or brownfield
How to Contain, Eradicate, and Recover from Incidents Apress
Network security is not simply about building impenetrable walls—determined attackers will eventually overcome traditional defenses. The most effective computer security strategies integrate network security monitoring (NSM): the collection and analysis of data to help you detect and respond to intrusions. In The Practice of Network Security Monitoring, Mandiant CSO Richard Bejtlich shows you how to use NSM to add a robust layer of protection around your networks—no prior experience required. To help you avoid costly and inflexible solutions, he teaches you how to deploy, build, and run an NSM operation using open source software and vendor-neutral tools. You'll learn how to: –Determine where to deploy NSM platforms, and size them for the monitored

networks –Deploy stand-alone or distributed NSM installations –Use command line and graphical packet analysis tools, and NSM consoles –Interpret network evidence from server-side and client-side intrusions –Integrate threat intelligence into NSM software to identify sophisticated adversaries There's no foolproof way to keep attackers out of your network. But when they get in, you'll be prepared. The Practice of Network Security Monitoring will show you how to build a security net to detect, contain, and control them. Attacks are inevitable, but losing sensitive data shouldn't be.

Site Reliability Engineering McGraw Hill Professional

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.

How Google Runs Production Systems Packt Publishing Ltd

The definitive guide to incident response--updated for the first time in a decade! Thoroughly revised to cover the latest and most effective tools and techniques, Incident Response & Computer Forensics, Third Edition arms you with the information you need to get your organization out of trouble when data breaches occur. This practical resource covers the entire lifecycle of incident response, including preparation, data collection, data analysis, and remediation. Real-world case studies reveal the methods behind--and remediation strategies for--today's most insidious attacks. Architect an infrastructure that allows for methodical investigation and remediation Develop leads, identify indicators of compromise, and determine incident scope Collect and preserve live data Perform forensic duplication Analyze data from networks, enterprise services, and applications Investigate Windows and Mac OS X systems Perform malware triage Write detailed incident response reports Create and implement comprehensive remediation plans

Building an Effective Incident Management Plan Pearson IT Certification

First responders who arrive on scene of a hazardous materials incident may be assigned to an engine, ladder truck, rescue, or ambulance with very little sophisticated HAZMAT equipment. Despite these limitations, their actions during the initial response will often set the stage for the success or failure of the entire event. Many incidents start out as minor "routine" events that suddenly escalate when something goes terribly wrong. Perhaps first responders did not anticipate the involvement of hazardous materials in a response to a rear-end collision involving two passenger vehicles, an EMS call at a residence for difficulty breathing, or a trash fire. That is until it was too late! First responders, despite their best intentions, can quickly become part of any hazardous materials problem. The results can be first responders who are killed or seriously injured, or those who suffer devastating illnesses years after exposure to a hazardous material. Even if you have hours of training on hazardous materials response, this book will provide every reader with... • Practical advice based on the real-life experiences of first responders • A one-stop source on topics such as atmospheric monitors and class B foam • Steps to managing "routine" incidents to prevent them from becoming disasters • Limitations of federal hazardous materials regulations you need to know • Real-world examples of first responders who won (or lost) the battle with hazardous materials First responders who arrive on scene of a hazardous materials incident may be assigned to an engine, ladder truck, rescue, or ambulance with very little sophisticated HAZMAT equipment. Despite these limitations, their actions during the initial response will often set the stage for the success or failure of the entire event. Many incidents start out as minor "routine" events that suddenly escalate when something goes terribly wrong. Perhaps first responders did not anticipate the involvement of hazardous materials in a response to a rear-end collision involving two passenger vehicles, an EMS call at a residence for difficulty breathing, or a trash fire. That is until it was too late! First responders, despite their best intentions, can quickly become part of any hazardous materials problem. The results can be first responders who are killed or seriously injured, or those who suffer devastating illnesses years after exposure to a hazardous material. Even if you have hours of training on hazardous materials response, this book will provide every reader with... • Practical advice based on the real-life experiences of first responders • A one-stop source on topics such as atmospheric monitors and class B foam • Steps to managing "routine" incidents to prevent them from becoming disasters • Limitations of federal hazardous materials regulations you need to know • Real-world examples of first responders who won (or lost) the battle with hazardous materials

Practical Windows Forensics IT Governance Ltd

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

Traffic Incident Management Handbook "O'Reilly Media, Inc."

Leverage the power of digital forensics for Windows systems About This Book Build your own lab environment to analyze forensic data and practice techniques. This book offers meticulous coverage with an example-driven approach and helps you build the key skills of performing forensics on Windows-based systems

using digital artifacts. It uses specific open source and Linux-based tools so you can become proficient at analyzing forensic data and upgrade your existing knowledge. Who This Book Is For This book targets forensic analysts and professionals who would like to develop skills in digital forensic analysis for the Windows platform. You will acquire proficiency, knowledge, and core skills to undertake forensic analysis of digital data. Prior experience of information security and forensic analysis would be helpful. You will gain knowledge and an understanding of performing forensic analysis with tools especially built for the Windows platform. What You Will Learn Perform live analysis on victim or suspect Windows systems locally or remotely Understand the different natures and acquisition techniques of volatile and non-volatile data. Create a timeline of all the system actions to restore the history of an incident. Recover and analyze data from FAT and NTFS file systems. Make use of various tools to perform registry analysis. Track a system user's browser and e-mail activities to prove or refute some hypotheses. Get to know how to dump and analyze computer memory. In Detail Over the last few years, the wave of the cybercrime has risen rapidly. We have witnessed many major attacks on the governmental, military, financial, and media sectors. Tracking all these attacks and crimes requires a deep understanding of operating system operations, how to extract evident data from digital evidence, and the best usage of the digital forensic tools and techniques. Regardless of your level of experience in the field of information security in general, this book will fully introduce you to digital forensics. It will provide you with the knowledge needed to assemble different types of evidence effectively, and walk you through the various stages of the analysis process. We start by discussing the principles of the digital forensics process and move on to show you the approaches that are used to conduct analysis. We will then study various tools to perform live analysis, and go through different techniques to analyze volatile and non-volatile data. Style and approach This is a step-by-step guide that delivers knowledge about different Windows artifacts. Each topic is explained sequentially, including artifact analysis using different tools and techniques. These techniques make use of the evidence extracted from infected machines, and are accompanied by real-life examples.

Conducting a Successful Incident Response NWCG Training Branch

"This book provides academia and organizations insights into practical and applied solutions, frameworks, technologies, and implementations for situational awareness in computer networks"--Provided by publisher.

Digital Forensics and Incident Response "O'Reilly Media, Inc."

Incorporating both the managerial and technical aspects of this discipline, the authors address knowledge areas of Certified Information Systems Security Professional certification throughout and include many examples of issues faced by today's businesses.

Developing Cybersecurity Programs and Policies IGI Global

Specifically oriented to the needs of information systems students, PRINCIPLES OF INFORMATION SECURITY, 5e delivers the latest technology and developments from the field. Taking a managerial approach, this bestseller teaches all the aspects of information security-not just the technical control perspective. It provides a broad review of the entire field of information security, background on many related elements, and enough detail to facilitate understanding of the topic. It covers the terminology of the field, the history of the discipline, and an overview of how to manage an information security program. Current and relevant, the fifth edition includes the latest practices, fresh examples, updated material on technical security controls, emerging legislative issues, new coverage of digital forensics, and hands-on application of ethical issues in IS security. It is the ultimate resource for future business decision-makers. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

97 Things Every Information Security Professional Should Know Harvard Business Press

Whether you're searching for new or additional opportunities, information security can be vast and overwhelming. In this practical guide, author Christina Morillo introduces technical knowledge from a diverse range of experts in the infosec field. Through 97 concise and useful tips, you'll learn how to expand your skills and solve common issues by working through everyday security problems. You'll also receive valuable guidance from professionals on how to navigate your career within this industry. How do you get buy-in from the C-suite for your security program? How do you establish an incident and disaster response plan? This practical book takes you through actionable advice on a wide variety of infosec topics, including thought-provoking questions that drive the direction of the field. Continuously Learn to Protect Tomorrow's Technology--Alyssa Columbus Fight in Cyber Like the Military Fights in the Physical--Andrew Harris Keep People at the Center of Your Work--Camille Stewart Infosec Professionals Need to Know Operational Resilience--Ann Johnson Taking Control of Your Own Journey--Antoine Middleton Security, Privacy, and Messy Data Webs: Taking Back Control in Third-Party Environments--Ben Brook Every Information Security Problem Boils Down to One Thing--Ben Smith Focus on the WHAT and the Why First, Not the Tool--Christina Morillo

Incident Management for Operations Cengage Learning

PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 2nd Edition presents methods to identify vulnerabilities within computer networks and the countermeasures that mitigate risks and damage. From market-leading content on contingency planning, to effective techniques that minimize downtime in an emergency, to curbing losses after a breach, this text is the resource needed in case of a network intrusion. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Principles of Information Security Principles of Incident Response and Disaster Recovery

Rev. ed. of: The experience economy: work is theatre & every business a stage. 1999.

The Practice of Network Security Monitoring McGraw Hill Professional

Discover the latest trends, developments and technology in information security with Whitman/Mattord's market-leading PRINCIPLES OF INFORMATION SECURITY, 7th Edition. Designed specifically to meet the needs of information systems students like you, this edition's balanced focus addresses all aspects of information security, rather than simply offering a technical control perspective. This overview explores important terms and examines what is needed to manage an effective information security program. A new module details incident response and detection strategies. In addition, current, relevant updates highlight the latest practices in security operations as well as legislative issues, information management toolsets, digital

forensics and the most recent policies and guidelines that correspond to federal and international standards. MindTap digital resources offer interactive content to further strength your success as a business decision-maker.

Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition John Wiley & Sons
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.

Understanding Incident Detection and Response Cengage Learning
Incident response is critical for the active defense of any network, and incident responders need up-to-date, immediately applicable techniques with which to engage the adversary. Applied Incident Response details effective ways to respond to advanced attacks against local and remote network resources, providing proven response techniques and a framework through which to apply them. As a starting point for new incident handlers, or as a technical reference for hardened IR veterans, this book details the latest techniques for responding to threats against your network, including: Preparing your environment for effective incident response Leveraging MITRE ATT&CK and threat intelligence for active network defense Local and remote triage of systems using PowerShell, WMIC, and open-source tools Acquiring RAM and disk images locally and remotely Analyzing RAM with Volatility and Rekall Deep-dive forensic analysis of system drives using open-source or commercial tools Leveraging Security Onion and Elastic Stack for network security monitoring Techniques for log analysis and aggregating high-value logs Static and dynamic analysis of malware with YARA rules, FLARE VM, and Cuckoo Sandbox Detecting and responding to lateral movement techniques, including pass-the-hash, pass-the-ticket, Kerberoasting, malicious use of PowerShell, and many more Effective threat hunting techniques Adversary emulation with Atomic Red Team Improving preventive and detective controls