Draft Computer Security Incident Handling Guide

OSBORN MOYER

FAA Computer Security DIANE Publishing
Using a well-conceived incident response plan in the aftermath of an online security breach enables your team to identify attackers and learn how they operate. But, only when you approach incident response with a cyber threat intelligence mindset will you truly understand the value of that information. With this practical guide, you’ll learn the fundamentals of intelligence analysis, as well as the best ways to incorporate these techniques into your incident response process. Each method reinforces the other: threat intelligence supports and augments incident response, while incident response generates useful threat intelligence. This book helps incident managers, malware analysts, reverse engineers, digital forensics specialists, and intelligence analysts understand, implement, and benefit from this relationship. In three parts, this in-depth book includes: The fundamentals: get an introduction to cyber threat intelligence, the intelligence process, the incident-response process, and how they all work together Practical application: walk through the intelligence-driven incident response (IDIR) process using the F3EAD process—Find, Fix Finish, Exploit, Analyze, and Disseminate The way forward: explore big-picture aspects of IDIR that go beyond individual incident-response investigations, including intelligence team building
Cyber Incident Response Springer Nature
The book discusses the categories of infrastucture that require protection. The issues associated with each, and the responsibilities of the public and private sector in securing this infrastructure.
FAA computer security recommendations to address continuing weaknesses : report to the Secretary of Transportation. Newnes
This book provides an overview of economic espionage as practiced by a range of nations from around the world focusing on the mass scale in which information is being taken for China's growth and development. It supplies an understanding of how the economy of a nation can prosper or suffer, depending on whether that nation is protecting its intellectual property, or whether it is stealing such property for its own use. The text concludes by outlining specific measures that corporations and their employees can practice to protect information and assets, both at home and abroad.
The Site Reliability Workbook DIANE Publishing
The escalation of security breaches involving personally identifiable information (PII) has contributed to the loss of millions of records over the past few years. Breaches involving PII are hazardous to both individuals and org. Individual harms may include identity theft, embarrassment, or blackmail. Organ. harms may include a loss of public trust, legal liability, or remediation costs. To protect the confidentiality of PII, org. should use a risk-based approach. This report provides guidelines for a risk-based approach to protecting the confidentiality of PII. The recommend. here are intended primarily for U.S. Fed. gov¿t. agencies and those who conduct business on behalf of the agencies, but other org. may find portions of the publication useful.
FISMA Certification and Accreditation Handbook DIANE Publishing
The urgency for a global standard of excellence for those who protect the networked world has never been greater. (ISC)2 created the information security industry’s first and only CBK®, a global compendium of information security topics. Continually updated to incorporate rapidly changing technologies and threats, the CBK continues to serve as the basis for (ISC)2’s education and certification programs. Unique and exceptionally thorough, the Official (ISC)2® Guide to the CISSP®CBK®provides a better understanding of the CISSP CBK — a collection of topics relevant to information security professionals around the world. Although the book still contains the ten domains of the CISSP, some of the domain titles have been revised to reflect evolving terminology and changing emphasis in the security professional’s day-to-day environment. The ten domains include information security and risk management, access control, cryptography, physical (environmental) security, security architecture and design, business continuity (BCP) and disaster recovery planning (DRP), telecommunications and network security, application security, operations security, legal, regulations, and compliance and investigations. Endorsed by the (ISC)2, this valuable resource follows the newly revised CISSP CBK, providing reliable, current, and thorough information. Moreover, the Official (ISC)2® Guide to the CISSP® CBK® helps information security professionals gain awareness of the requirements of their profession and acquire knowledge validated by the CISSP certification. The book is packaged with a CD that is an invaluable tool for those seeking certification. It includes sample exams that simulate the actual exam, providing the same number and types of questions with the same allotment of time allowed. It even grades the exam, provides correct answers, and identifies areas where more study is needed.
Computer Security Incident Response Planning at Nuclear Facilities John Wiley & Sons
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
Cyber Breach Response That Actually Works CRC Press
A log is a record of the events occurring within an org¿s. systems & networks. Many logs within an org. contain records related to computer security (CS). These CS logs are generated by many sources, incl. CS software, such as antivirus software, firewalls, & intrusion detection & prevention systems; operating systems on servers, workstations, & networking equip.; & applications. The no., vol., & variety of CS logs have increased greatly, which has created the need for CS log mgmt. -- the process for generating, transmitting, storing, analyzing, & disposing of CS data. This report assists org¿s. in understanding the need for sound CS log mgmt. It provides practical, real-world guidance on developing, implementing, & maintaining effective log mgmt. practices. Illus.
Cyber Security DIANE Publishing
Practitioners in Cybersecurity community understand that they are an unending war with opponents who have varying interests, but are mostly motivated by financial gains. New vulnerabilities are continuously discovered, new technologies are continuously being developed, and attackers are innovative in exploiting flaws to gain access to information assets for financial gains. It is profitable for attackers to succeed only few times. Security Operations Center (SOC) plays a key role in this perpetual arm wrestling to ensure you win most of the times. And if you fail once in a while, you can get back very quickly without much damage. People, who are part of SOC planning, architecture, design, implementation, operations, and incidents response will find this book useful.Many public and private sector organizations have built Security Operations Centers in-house whereas others have outsourced SOC operations to managed security services providers. Some also choose a hybrid approach by keeping parts of SOC operations in-house and outsourcing the rest of it. However, many of these efforts don't bring the intended results or

realize desired business outcomes.This book is an effort to learn from experiences of many SOC practitioners and researchers to find practices that have been proven to be useful while avoiding common pitfalls in building SOC. I have also explored different ideas to find a "balanced" approach towards building a SOC and making informed choices between functions that can/should be kept in-house and the ones that can be outsourced. Even if you are an experienced SOC professional, you will still find few interesting ideas as I have done significant research and interviewed many SOC professionals to include tips to help avoid pitfalls.

Information Security: Sustained management Commitment and Oversight Are Vital to Resolving Long-Standing Weaknesses at the Department of Veterans Affairs Jones & Bartlett Publishers

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.

Information Security in the Federal Government DIANE Publishing

Servers are frequently targeted by attackers because of the value of their data and services. For example, a server might contain personally identifiable info. that could be used to perform identity theft. This document is intended to assist organizations in installing, configuring, and maintaining secure servers. More specifically, it describes, in detail, the following practices to apply: (1) Securing, installing, and configuring the underlying operating system; (2) Securing, installing, and configuring server software; (3) Maintaining the secure configuration through application of appropriate patches and upgrades, security testing, monitoring of logs, and backups of data and operating system files. Illus.

Fundamentals of Information Systems Security Apress

This open access book explores the legal aspects of cybersecurity in Poland. The authors are not limited to the framework created by the NCSA (National Cybersecurity System Act - this act was the first attempt to create a legal regulation of cybersecurity and, in addition, has implemented the provisions of the NIS Directive) but may discuss a number of other issues. The book presents international and EU regulations in the field of cybersecurity and issues pertinent to combating cybercrime and cyberterrorism. Moreover, regulations concerning cybercrime in a few select European countries are presented in addition to the problem of collision of state actions in ensuring cybersecurity and human rights. The advantages of the book include a comprehensive and synthetic approach to the issues related to the cybersecurity system of the Republic of Poland, a research perspective that takes as the basic level of analysis issues related to the security of the state and citizens, and the analysis of additional issues related to cybersecurity, such as cybercrime, cyberterrorism, and the problem of collision between states ensuring security cybernetics and human rights. The book targets a wide range of readers, especially scientists and researchers, members of legislative bodies, practitioners (especially judges, prosecutors, lawyers, law enforcement officials), experts in the field of IT security, and officials of public authorities. Most authors are scholars and researchers at the War Studies University in Warsaw. Some of them work at the Academic Centre for Cybersecurity Policy - a thinktank created by the Ministry of National Defence of the Republic of Poland. .

21st European Conference on Cyber Warfare and Security American Bar Association

The Department of Defense (DOD) depends on interconnected information systems and communications networks for critical combat and business operations. Many of these systems and networks are interconnected through the public telecommunications infrastructure, including the Internet, and they may be targeted by an increasing variety of cyber attacks. If successful, these attacks could result in the loss or corruption of critical data, damage to information systems, or disruption of military operations. To address such threats, DOD has established organizations, known as computer incident response capabilities, at various locations worldwide. These organizations engage in a range of activities associated with preventing, detecting, and responding to computer incidents.

Guide to Protecting the Confidentiality of Personally Identifiable Information CRC Press

Strengthen your ability to implement, assess, evaluate, and enhance the effectiveness of information security controls based on ISO/IEC 27001/27002:2022 standards Purchase of the print or Kindle book includes a free PDF eBook Key Features Familiarize yourself with the clauses and control references of ISO/IEC 27001:2022 Define and implement an information security management system aligned with ISO/IEC 27001/27002:2022 Conduct management system audits to evaluate their effectiveness and adherence to ISO/IEC 27001/27002:2022 Book DescriptionISO 27001 and ISO 27002 are globally recognized standards for information security management systems (ISMSs), providing a robust framework for information protection that can be adapted to all organization types and sizes. Organizations with significant exposure to information-security–related risks are increasingly choosing to implement an ISMS that complies with ISO 27001. This book will help you understand the process of getting your organization's information security management system certified by an accredited certification body. The book begins by introducing you to the standards, and then takes you through different principles and terminologies. Once you completely understand these standards, you'll explore their execution, wherein you find out how to implement these standards in different sizes of organizations. The chapters also include case studies to enable you to understand how you can implement the standards in your organization. Finally, you'll get to grips with the auditing process, planning, techniques, and reporting and learn to audit for ISO 27001. By the end of this book, you'll have gained a clear understanding of ISO 27001/27002 and be ready to successfully implement and audit for these standards.What you will learn Develop a strong understanding of the core principles underlying information security Gain insights into the interpretation of control requirements in the ISO 27001/27002:2022 standard Understand the various components of ISMS with practical examples and case studies Explore risk management strategies and techniques Develop an audit plan that outlines the scope, objectives, and schedule of the audit Explore real-world case studies that illustrate successful implementation approaches Who this book is forThis book is for information security professionals, including information security managers, consultants, auditors, officers, risk specialists, business owners, and individuals responsible for implementing, auditing, and administering information security management systems. Basic knowledge of organization-level information security management, such as risk assessment, security controls, and auditing, will help you grasp the topics in this book easily.

Responding to Targeted Cyberattacks DIANE Publishing

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.

Guide to Computer Security Log Management Elsevier

The Official (ISC)2® Guide to the CISSP®-ISSEP® CBK® provides an inclusive analysis of all of the topics covered on the newly created CISSP-ISSEP Common Body of Knowledge. The first fully comprehensive guide to the CISSP-ISSEP CBK, this book promotes understanding of the four ISSEP domains: Information Systems Security Engineering (ISSE); Certification and Accreditation; Technical Management; and an Introduction to United States Government Information Assurance Regulations. This volume explains ISSE by comparing it to a traditional Systems Engineering model, enabling you to see the correlation of how security fits into the design and development process for information systems. It also details key points of more than 50 U.S. government policies and procedures that need to be understood in order to understand the CBK and protect U.S. government information. About the Author Susan Hansche, CISSP-ISSEP is the training director for information assurance at Nortel PEC Solutions in Fairfax, Virginia. She has more than 15 years of experience in the field and since 1998 has served as the contractor program manager of the information assurance training program for the U.S. Department of State.

Cybersecurity in Poland CRC Press

Some fed. agencies, in addition to being subject to the Fed. Information Security Mgmt. Act of 2002, are also subject to similar requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (EPHI). The EPHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. This publication discusses security considerations and resources that may provide value when implementing the requirements of the HIPAA Security Rule. Illustrations.

U.S. Preparedness for Catastrophic Attacks Oxford University Press

PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Revised and updated with the latest information from this fast-paced field, Fundamentals of Information System Security, Second Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today. Part 2 is adapted from the Official (ISC)2 SSCP Certified Body of Knowledge and presents a high-level overview of each of the seven domains within the System Security Certified Practitioner certification. The book closes with a resource for readers who desire additional material on information security standards, education, professional certifications, and compliance laws. With its practical, conversational writing style and step-by-step examples, this text is a must-have resource for those entering the world of information systems security. New to the Second Edition: - New material on cloud computing, risk analysis, IP mobility, OMNIBus, and Agile Software Development. - Includes the most recent updates in Information Systems Security laws, certificates, standards, amendments, and the proposed Federal Information Security Amendments Act of 2013 and HITECH Act. - Provides new cases and examples pulled from real-world scenarios. - Updated data, tables, and sidebars provide the most current information in the field.

The Oxford Handbook of Cyber Security Academic Conferences and publishing limited

The urgency for a global standard of excellence for those who protect the networked world has never been greater. (ISC)2 created the information security industry's first and only CBK, a global compendium of information security topics. Continually updated to incorporate rapidly changing technologies and threats, the CBK conti

Official (ISC)2 Guide to the CISSP CBK ISACA

This updated report provides an overview of firewall technology, and helps organizations plan for and implement effective firewalls. It explains the technical features of firewalls, the types of firewalls that are available for implementation by organizations, and their security capabilities. Organizations are advised on the placement of firewalls within the network architecture, and on the selection, implementation, testing, and management of firewalls. Other issues covered in detail are the development of firewall policies, and recommendations on the types of network traffic that should be prohibited. The appendices contain helpful supporting material, including a glossary and lists of acronyms and abreviations; and listings of in-print and online resources. Illus.

Information Security "O'Reilly Media, Inc."

Fed. agencies are facing a set of cybersecurity threats that are the result of increasingly sophisticated methods of attack & the blending of once distinct types of attack into more complex & damaging forms. Examples of these threats include: spam (unsolicited commercial e-mail), phishing (fraudulent messages to obtain personal or sensitive data), & spyware (software that monitors user activity without user knowledge or consent). This report determines: the potential risks to fed. systems from these emerging cybersecurity threats; the fed. agencies' perceptions of risk & their actions to mitigate them, fed. & private-sector actions to address the threats on a nat. level; & governmentwide challenges to protecting fed. systems from these threats. Illus.

Related with Draft Computer Security Incident Handling Guide:
• 9 Inch Round Cake Cutting Guide : click here