Incident Response

Every computer 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.

Build your organization's cyber defense system by effectively implementing digital forensics and incident management techniques Key Features Create a solid incident response framework and manage cyber incidents effectively Perform malware analysis for effective incident response Explore real-life scenarios that effectively use threat intelligence and modeling techniques Book Description An understanding of how digital forensics integrates with the overall response to cybersecurity incidents is key to securing your organization's infrastructure from attacks. This updated second edition will help you perform cutting-edge digital forensic activities and incident response. After focusing on the fundamentals of incident response that are critical to any information security team, you'll move on to exploring the incident response framework. From understanding its importance to creating a swift and effective response to security incidents, the book will guide you with the help of useful examples. You'll later get up to speed with digital forensic techniques, from acquiring evidence and examining volatile memory through to hard drive examination and network-based evidence. As you progress, you'll discover the role that threat intelligence plays in the incident response process. You'll also learn how to prepare an incident response report that documents the findings of your analysis. Finally, in addition to various incident response activities, the book will address malware analysis, and demonstrate how you can proactively use your digital forensic skills in threat hunting. By the end of this book, you'll have learned how to efficiently investigate and report unwanted security breaches and incidents in your organization. What you will learn Create and deploy an incident response capability within your own organization Perform proper evidence acquisition and handling Analyze the evidence collected and determine the root cause of a security incident Become well-versed with memory and log analysis Integrate digital forensic techniques and procedures into the overall incident response process Understand the different techniques for threat hunting Write effective incident reports that document the key findings of your analysis Who this book is for This book is for cybersecurity and information security professionals who want to implement digital forensics and incident response in their organization. You will also find the book helpful if you are new to the concept of digital forensics and are looking to get started with the fundamentals. A basic understanding of operating systems and some knowledge of networking fundamentals are required to get started with this book.

Explore the world of modern human-operated ransomware attacks, along with covering steps to properly investigate them and collecting and analyzing cyber threat intelligence using cutting-edge methods and tools Key Features Understand modern human-operated cyber attacks, focusing on threat actor tactics, techniques, and procedures Collect and analyze ransomware-related cyber threat intelligence from various sources Use forensic methods and tools to reconstruct ransomware attacks and prevent them in the early stages Book Description Ransomware attacks have become the strongest and most persistent threat for many companies around the globe. Building an effective incident response plan to prevent a ransomware attack is crucial and may help you avoid heavy losses. Incident Response Techniques for Ransomware Attacks is designed to help you do just that. This book starts by discussing the history of ransomware, showing you how the threat landscape has changed over the years, while also covering the process of incident response in detail. You'll then learn how to collect and produce ransomware-related cyber threat intelligence and look at threat actor tactics, techniques, and procedures. Next, the book focuses on various forensic artifacts in order to reconstruct each stage of a human-operated ransomware attack life cycle. In the concluding chapters, you'll get to grips with various kill chains and discover a new one: the Unified Ransomware Kill Chain. By the end of this ransomware book, you'll be equipped with the skills you need to build an incident response strategy for all ransomware attacks. What you will learn Understand the modern ransomware threat landscape Explore the incident response process in the context of ransomware Discover how to collect and produce ransomware-related cyber threat intelligence Use forensic methods to collect relevant artifacts during incident response Interpret collected data to understand threat actor tactics, techniques, and procedures Understand how to reconstruct the ransomware attack kill chain Who this book is for This book is for security researchers, security analysts, or anyone in the incident response landscape who is responsible for building an incident response model for ransomware attacks. A basic understanding of cyber threats will be helpful to get the most out of this book. 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 organizationThis 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._Preparation_Identification_Containment_Eradication_Recovery_Lessons Learned/Follow-up3) Building an Incident response plan and key elements for an efficient IT security Incident Management.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.

Security Monitoring and Incident Response Master Plan
How to Contain, Eradicate, and Recover from Incidents
Incident Handling and Response
Cybersecurity Incident Response
Incident Response Program Guide
The Coastguard, Emergency Towing Vessels and the Maritime Incident Response Group

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. 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

Learn to identify security incidents and build a series of best practices to stop cyber attacks before they create serious consequences Key FeaturesDiscover Incident Response (IR), from its evolution to implementationUnderstand cybersecurity essentials and IR best practices through real-world phishing incident scenariosExplore the current challenges in IR through the perspectives of leading expertsBook Description Cybercriminals are always in search of new methods to infiltrate systems. Quickly responding to an incident will help organizations minimize losses, decrease vulnerabilities, and rebuild services and processes. In the wake of the COVID-19 pandemic, with most organizations gravitating towards remote working and cloud computing, this book uses frameworks such as MITRE ATT&CK® and the SANS IR model to assess security risks. The book begins by introducing you to the cybersecurity landscape and explaining why IR matters. You will understand the evolution of IR, current challenges, key metrics, and the composition of an IR team, along with an array of methods and tools used in an effective IR process. You will then learn how to apply these strategies, with discussions on incident alerting, handling, investigation, recovery, and reporting. Further, you will cover governing IR on multiple platforms and sharing cyber threat intelligence and the procedures involved in IR in the cloud. Finally, the book concludes with an "Ask the Experts" chapter wherein industry experts have provided their perspective on diverse topics in the IR sphere. By the end of this book, you should become proficient at building and applying IR strategies pre-emptively and confidently. What you will learnUnderstand IR and its significanceOrganize an IR teamExplore best practices for managing attack situations with your IR teamForm, organize, and operate a product security team to deal with product vulnerabilities and assess their severityOrganize all the entities involved in product security responseRespond to security vulnerabilities using tools developed by Keepnet Labs and BinalyzeAdapt all the above learnings for the cloudWho this book is for This book is aimed at first-time incident responders, cybersecurity enthusiasts who want to get into IR, and anyone who is responsible for maintaining business security. It will also interest CIOs, CISOs, and members of IR, SOC, and CSIRT teams. However, IR is not just about information technology or security teams, and anyone with a legal, HR, media, or other active business role would benefit from this book. The book assumes you have some admin experience. No prior DFIR experience is required. Some infosec knowledge will be a plus but isn't mandatory.

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

Creating Standardized Incident Management Workflows
Security Incidents & Response Against Cyber Attacks
Investigating Computer Crime
Intelligence-Driven Incident Response
Practical insights into developing an incident response capability through intelligence-based threat hunting
Understanding Incident Detection and Response

"Incident Response is a complete guide for organizations of all sizes and types who are addressing their computer security issues."--Jacket.
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
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.
Computer Incident Response and Product Security The practical guide to building and running incident response and product security teams Damir Rajnovic Organizations increasingly recognize the urgent importance of effective, cohesive, and efficient security incident response. The speed and effectiveness with which a company can respond to incidents has a direct impact on how devastating an incident is on the company's operations and finances. However, few have an experienced, mature incident response (IR) team. Many companies have no IR teams at all; others need help with improving current practices. In this book, leading Cisco incident response expert Damir Rajnoviĉ presents start-to-finish guidance for creating and operating effective IR teams and responding to incidents to lessen their impact significantly. Drawing on his extensive experience identifying and resolving Cisco product security vulnerabilities, the author also covers the entire process of correcting product security vulnerabilities and notifying customers. Throughout, he shows how to build the links across participants and processes that are crucial to an effective and timely response. This book is an indispensable resource for every professional and leader who must maintain the integrity of network operations and products—from network and security administrators to software engineers, and from product architects to senior security executives. -Determine why and how to organize an incident response (IR) team -Learn the key strategies for making the case to senior management -Locate the IR team in your organizational hierarchy for maximum effectiveness -Review best practices for managing attack situations with your IR team -Build relationships with other IR teams, organizations, and law enforcement to improve incident response effectiveness -Learn how to form, organize, and operate a product security team to deal with product vulnerabilities and assess their severity -Recognize the differences between product security vulnerabilities and exploits -Understand how to coordinate all the entities involved in product security handling -Learn the steps for handling a product security vulnerability based on proven Cisco processes and practices -Learn strategies for notifying customers about product vulnerabilities and how to ensure customers are implementing fixes This security book is part of the Cisco Press Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end, self-defending networks.

Incident Response & Computer Forensics, 2nd Ed.
Computer Incident Response and Product Security
Crafting the InfoSec Playbook
Incident Response in the Age of Cloud
Incident response techniques and procedures to respond to modern cyber threats
A Guidebook for First Responders during the Initial Phase of a Dangerous Goods/Hazardous Materials Transportation Incident

Create, maintain, and manage a continual cybersecurity incident response program using the practical steps presented in this book. Don't allow your cybersecurity incident responses (IR) to fall short of the mark due to lack of planning, preparation, leadership, and management support Surviving an incident, or a breach, requires the best response possible. This book provides practical guidance for the containment, eradication, and recovery from cybersecurity events and incidents. The book takes the approach that incident response should be a continual program. Leaders must understand the organizational environment, the strengths and weaknesses of the program and team, and how to strategically respond. Successful behaviors and actions required for each phase of incident response are explored in the book. Straight from NIST 800-61, these actions include: Planning and practicing Detection Containment Eradication Post-incident actions What You'll Learn Know the sub-categories of the NIST Cybersecurity Framework Understand the components of incident response Go beyond the incident response plan Turn the plan into a program that needs vision, leadership, and culture to make it successful Be effective in your role on the incident response team Who This Book Is For Cybersecurity leaders, executives, consultants, and entry-level professionals responsible for executing the incident response plan when something goes wrong
Any good attacker will tell you that expensive security monitoring and prevention tools aren't enough to keep you secure. This practical book demonstrates a data-centric approach to distilling complex security monitoring, incident response, and threat analysis ideas into their most basic elements. You'll learn how to develop your own threat intelligence and incident detection strategy, rather than depend on security tools alone. Written by members of Cisco's Computer Security Incident Response Team, this book shows IT and information security professionals how to create an InfoSec playbook by developing strategy, technique, and architecture. Learn incident response fundamentals—and the importance of getting back to basics Understand threats you face and what you should be protecting Collect, mine, organize, and analyze as many relevant data sources as possible Build your own playbook of repeatable methods for security monitoring and response Learn how to put your plan into action and keep it running smoothly Select the right monitoring and detection tools for your environment Develop queries to help you sort through data and create valuable reports Know what actions to take during the incident response phase
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
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

Hazardous Materials Incident Response Operations
Techniques and best practices to effectively respond to cybersecurity incidents

Incident Response with Threat Intelligence

Hearing Before the Subcommittee on Prevention of Nuclear and Biological Attack of the Committee on Homeland Security, House of Representatives, One Hundred Ninth Congress, First Session, October 27, 2005

Blue Team Handbook

Incident Response Techniques for Ransomware Attacks

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 explanation of cloud-based systems and Web-accessible tools to prepare you for success. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Written by FBI insiders, this updated best-seller offers a look at the legal, procedural, and technical steps of incident response and computer forensics. Including new chapters on forensic analysis and remediation, and real-world case studies, this revealing book shows how to counteract and conquer today's hack attacks.

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 contain and eradicate incidents, and how to cleanup and recover. The book shares real-world experiences and knowledge from authors from academia and industry.

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.

Incident Response Essentials

sixth report of session 2010-12, Vol. 1: Report, together with formal minutes, oral and written evidence

A Strategic Guide to Handling System and Network Security Breaches

Oracle Incident Response and Forensics

OS X Incident Response

Conducting a Successful Incident Response

Are you satisfied with the way your company responds to IT incidents? How prepared is your response team to handle critical, time-sensitive events such as service disruptions and security breaches? IT professionals looking for effective response models have successfully adopted the Incident Management System (IMS) used by firefighters throughout the US. This practical book shows you how to apply the same response methodology to your own IT operation. You'll learn how IMS best practices for leading people and managing time apply directly to IT incidents where the stakes are high and outcomes are uncertain.

Under current proposals the Maritime & Coastguard Agency plans to close ten of the existing 14 Maritime Rescue Coordination Centres and to leave three that remain open on a 24-hour basis and five that will operate in "daylight" hours only. The Transport Committee found little support for the measures and has no confidence that, under these proposals, the Coastguard will in future be able to respond to emergencies at sea as well as they do now, let alone in a more effective way. The Committee is not convinced by the Government's claim that technology can, at present, replace local knowledge. Serious concerns were raised that the safety of people at sea, on cliffs and beaches will be jeopardised if the proposals proceed in their current form. Ministers must issue revised proposals for further consultation. The Committee also strongly condemns the Government's cost-cutting decision to withdraw funding for the four Emergency Towing Vessels (ETVs) stationed around the UK coast - large tugs that intercept disabled ships to prevent environmental pollution disasters. The Transport Committee also criticises proposals to completely remove government funding for the Maritime Incident Response group (MIRG), a national fire-fighting-at-sea capability. Ministers should instead adopt a slimmed-down MIRG which is more cost-effective than the present arrangement. Lastly, the Committee records its disappointment that Mike Penning MP, Minister for Shipping, instructed regular coastguards not to give oral evidence to the committee on the basis that they were junior civil servants.

This guide teaches security analysts to minimize information loss and system disruption using effective system monitoring and detection measures. The information here spans all phases of incident response, from pre-incident conditions and considerations to post-incident analysis. This book will deliver immediate solutions to a growing audience eager to secure its networks.

If you're involved in cybersecurity as a software developer, forensic investigator, or network administrator, this practical guide shows you how to apply the scientific method when assessing techniques for protecting your information systems. You'll learn how to conduct scientific experiments on everyday tools and procedures, whether you're evaluating corporate security systems, testing your own security product, or looking for bugs in a mobile game. Once author Josiah Dykstra gets you up to speed on the scientific method, he helps you focus on standalone, domain-specific topics, such as cryptography, malware analysis, and system security engineering. The latter chapters include practical case studies that demonstrate how to use available tools to conduct domain-specific scientific experiments. Learn the steps necessary to conduct scientific experiments in cybersecurity Explore fuzzing to test how your software handles various inputs Measure the performance of the Snort intrusion detection system Locate malicious "needles in a haystack" in your network and IT environment Evaluate cryptography design and application in IoT products Conduct an experiment to identify relationships between similar malware binaries Understand system-level security requirements for enterprise networks and web services

The Incident Response System

Scripting and Analysis

Computer Incident Response and Forensics Team Management

Digital Forensics and Incident Response

The Practice of Network Security Monitoring

Computer Forensics

Does the identification number 60 indicate a toxic substance or a flammable solid, in the molten state at an elevated temperature? Does the identification number 1035 indicate ethane or butane? What is the difference between natural gas transmission pipelines and natural gas distribution pipelines? If you came upon an overturned truck on the highway that was leaking, would you be able to identify if it was hazardous and know what steps to take? Questions like these and more are answered in the Emergency Response Guidebook. Learn how to identify symbols for and vehicles carrying toxic, flammable, explosive, radioactive, or otherwise harmful substances and how to respond once an incident involving those substances has been identified. Always be prepared in situations that are unfamiliar and dangerous and know how to rectify them. Keeping this guide around at all times will ensure that, if you were to come upon a transportation situation involving hazardous substances or dangerous goods, you will be able to help keep others and yourself out of danger. With color-coded pages for quick and easy reference, this is the official manual used by first responders in the United States and Canada for transportation incidents involving dangerous goods or hazardous materials.

OS X Incident Response: Scripting and Analysis is written for analysts who are looking to expand their understanding of a lesser-known operating system. By mastering the forensic artifacts of OS X, analysts will set themselves apart by acquiring an up-and-coming skillset. Digital forensics is a critical art and science. While forensics is commonly thought of as a function of a legal investigation, the same tactics and techniques used for those investigations are also important in a response to an incident. Digital evidence is not only critical in the course of investigating many crimes but businesses are recognizing the importance of having skilled forensic investigators on staff in the case of policy violations. Perhaps more importantly, though, businesses are seeing enormous impact from malware outbreaks as well as data breaches. The skills of a forensic investigator are critical to determine the source of the attack as well as the impact. While there is a lot of focus on Windows because it is the predominant desktop operating system, there are currently very few resources available for forensic investigators on how to investigate attacks, gather evidence and respond to incidents involving OS X. The number of Macs on enterprise networks is rapidly increasing, especially with the growing prevalence of BYOD, including iPads and iPhones. Author Jaron Bradley covers a wide variety of topics, including both the collection and analysis of the forensic pieces found on the OS. Instead of using expensive commercial tools that clone the hard drive, you will learn how to write your own Python and bash-based response scripts. These scripts and methodologies can be used to collect and analyze volatile data immediately. For online source codes, please visit: https://github.com/jbradley89/osx_incident_response_scripting_and_analysis Focuses exclusively on OS X attacks, incident response, and forensics Provides the technical details of OS X so you can find artifacts that might be missed using automated tools Describes how to write your own Python and bash-based response scripts, which can be used to collect and analyze volatile data immediately Covers OS X incident response in complete technical detail, including file system, system startup and scheduling, password dumping, memory, volatile data, logs, browser history, and exfiltration

Learn everything you need to know to respond to advanced cybersecurity incidents through threat hunting using threat intelligence Key Features Understand best practices for detecting, containing, and recovering from modern cyber threats Get practical experience embracing incident response using intelligence-based threat hunting techniques Implement and orchestrate different incident response, monitoring, intelligence, and investigation platforms Book Description With constantly evolving cyber threats, developing a cybersecurity incident response capability to identify and contain threats is indispensable for any organization regardless of its size. This book covers theoretical concepts and a variety of real-life scenarios that will help you to apply these concepts within your organization. Starting with the basics of incident response, the book introduces you to professional practices and advanced concepts for integrating threat hunting and threat intelligence procedures in the identification, contention, and eradication stages of the incident response cycle. As you progress through the chapters, you'll cover the different aspects of developing an incident response program. You'll learn the implementation and use of platforms such as TheHive and ELK and tools for evidence collection such as Velociraptor and KAPE before getting to grips with the integration of frameworks such as Cyber Kill Chain and MITRE ATT&CK for analysis and investigation. You'll also explore methodologies and tools for cyber threat hunting with Sigma and YARA rules. By the end of this book, you'll have learned everything you need to respond to cybersecurity incidents using threat intelligence. What you will learn Explore the fundamentals of incident response and incident management Find out how to develop incident response capabilities Understand the development of incident response plans and playbooks Align incident response procedures with business continuity Identify incident response requirements and orchestrate people, processes, and technologies Discover methodologies and tools to integrate cyber threat intelligence and threat hunting into incident response Who this book is for If you are an information security professional or anyone who wants to learn the principles of incident management, first response, threat hunting, and threat intelligence using a variety of platforms and tools, this book is for you. Although not necessary, basic knowledge of Linux, Windows internals, and network protocols will be helpful.

Take the right steps when a breach of your Oracle Database environment becomes known or suspected. You will learn techniques for discerning how an attacker got in, what data they saw, and what else they might have done. This book helps you understand forensics in relation to Oracle Database, and the tools and techniques that should be used to investigate a database breach. You will learn the measures to put in place now to make it harder for an attack to be successful, and to aid in the detection and investigation of future attacks. You will know how to bring together tools and methods to create a holistic approach and investigation when an event occurs, helping you to be confident of your ability to react correctly and responsibly to threats against your organization's data. What You'll Learn Detect when breaches have or may have occurred React with confidence using an organized plan Determine whether a suspected breach is real Determine the scope of data that has been compromised Preserve evidence for possible criminal prosecutions Put in place measures to aid future investigations Who This Book is For Database administrators, system administrators, and other technology professionals who may be called upon to investigate breaches of security involving Oracle Database

Emergency Response Guidebook

Incident Response & Computer Forensics, Third Edition

Nuclear Incident Response Teams

A Holistic Approach for an Efficient Security Incident Management.

Incident Management for Operations

Information security challenges to improving DOD's incident response capabilities

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.

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

Updated, Expanded, and released to print on 10/5/14! Complete details below! Two new sections, five protocol header illustrations, improved formatting, and other corrections. The Blue Team Handbook is a zero fluff reference guide for cyber security incident responders and InfoSec pros alike. The BTHb includes essential information in a condensed handbook format about the incident response process, how attackers work, common tools, a methodology for network analysis developed over 12 years, Windows and Linux analysis processes, tcpdump usage examples, Snort IDS usage, and numerous other topics. The book is peppered with practical real life techniques from the authors extensive career working in academia and a corporate setting. Whether you are writing up your cases notes, analyzing potentially suspicious traffic, or called in to look over a misbehaving server - this book should help you handle the case and teach you some new techniques along the way. Version 2.0 updates: - *** A new section on Database incident response was added. - *** A new section on Chain of Custody was added. - *** Matt Baxter's superbly formatted protocol headers were added! - Table headers bolded. - Table format slightly revised throughout book to improve left column readability. - Several sentences updated and expanded for readability and completeness. - A few spelling errors were corrected. - Several sites added to the Web References section. - Illustrations reformatted for better fit on the page. - An index was added. - Attribution for some content made more clear (footnotes, expanded source citing) - Content expanded a total of 20 pages

This book comes with access to a customizable word template that can be used in implementing an IT Security Incident Response Program in any organization. Most companies have requirements to document their incident response processes, but they lack the knowledge and experience to undertake such documentation efforts. That means businesses are faced to either outsource the work to expensive consultants or they ignore the requirement and hope they do not get in trouble for being non-compliant with a compliance requirement. In either situation, it is not a good place to be. The good news is that your CyberSecurityResource developed a viable incident response program, which is the "gold standard" for incident response programs. This document is capable of scaling for any sized company.The reality is that incidents do not care if your responders are or are not prepared and generally with incident response operations if you fail to plan you plan to fail. What matters most is appropriate leadership that is capable of directing response operations in an efficient and effective manner. This is where the Incident Response Program (IRP) is an invaluable resource for cybersecurity and business leaders to have a viable plan to respond to cybersecurity related incidents.The IRP is an editable Microsoft Word document, that contains the program-level documentation and process flows to establish a mature Incident Response Program. This product addresses the "how?" questions for how your company manages cybersecurity incident response. The IRP helps address the fundamental expectations when it comes to incident response requirements: Defines the hierarchical approach to handling incidents.Categorizes eleven different types of incidents and four different classifications of incident severity.Defines the phases of incident response operations, including deliverables expected for each phase.Defines the Incident Response Team (IRT) to enable a unified approach to incident response operations.Defines the scientific method approach to incident response operations.Provides guidance on forensics evidence acquisition

Digital Forensics and Incident Response - Second Edition

Essential Cybersecurity Science

Outwitting the Adversary
Understand modern ransomware attacks and build an incident response strategy to work through them
The Site Reliability Workbook
Nuclear incident response teams : hearing