

Blue Team Handbook Incident Response Edition A Condensed Field For The Cyber Security Incident Responder

As recognized, adventure as well as experience not quite lesson, amusement, as skillfully as arrangement can be gotten by just checking out a ebook **Blue Team Handbook Incident Response Edition A Condensed Field For The Cyber Security Incident Responder** with it is not directly done, you could recognize even more as regards this life, almost the world.

We come up with the money for you this proper as well as simple quirk to acquire those all. We have the funds for Blue Team Handbook Incident Response Edition A Condensed Field For The Cyber Security Incident Responder and numerous book collections from fictions to scientific research in any way. among them is this Blue Team Handbook Incident Response Edition A Condensed Field For The Cyber Security Incident Responder that can be your partner.

Blue Team Handbook Incident Response Edition A Condensed Field For The Cyber Security Incident Responder

2022-05-14

ZION OSCAR

The Practice of Network Security Elsevier

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 *Purple Team Field Manual* Createspace Independent Publishing Platform

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

Security Operations Center NWCG Training Branch
Blue Team defensive advice from the biggest names in cybersecurity The Tribe of Hackers team is back. This new guide is packed with insights on blue team issues from the biggest names in cybersecurity. Inside, dozens of the world's leading Blue Team security specialists show you how to harden systems against real and simulated breaches and attacks. You'll discover the latest strategies for blocking even the most advanced red-team attacks and preventing costly losses. The experts share their hard-earned wisdom, revealing what works and what doesn't in the real world of cybersecurity. Tribe of Hackers Blue Team goes beyond the bestselling, original Tribe of Hackers book and delves into detail on defensive and preventative techniques. Learn how to grapple with the issues that hands-on security experts and security managers are sure to build into their blue team exercises. Discover what it takes to get started building blue team skills Learn how you can defend against physical and technical penetration testing Understand the techniques that advanced red teamers use against high-value targets Identify the most important tools to master as a blue teamer Explore ways to harden systems against red team attacks Stand out from the competition as you work to advance your cybersecurity career Authored by leaders in cybersecurity attack and breach simulations, the Tribe of Hackers series is perfect for those new to blue team security, experienced practitioners, and cybersecurity team leaders. Tribe of Hackers Blue Team has the real-world advice and practical guidance you need to advance your information security career and ready yourself for the blue team

defense.

Incident Handling and Response John Wiley & Sons

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

GCIH GIAC Certified Incident Handler All-in-One Exam Guide SAGE

The Red Team and the Blue Team are now obsolete. The only manual you need is this: "TCTFM" The Complete Team Field Manual is the most comprehensive cybersecurity manual around that includes all the different techniques and approaches of the blue and red teams. This book contains: the basic syntax for commonly used Linux and Windows command line tools unique use cases for powerful tools such as Python and Windows PowerShell five core functions of Identify, Protect, Detect, Respond, and Recover tactical steps and commands to use when preparing working through recovering commands after Cyber Security Incident more importantly, it should teach you some new secret techniques Scroll up and buy this manual. It will be the only book you will use![]

The Complete Team Field Manual O'Reilly & Associates Incorporated

Implement information security effectively as per your organization's needs. About This Book Learn to build your own information security framework, the best fit for your organization Build on the concepts of threat modeling, incidence response, and security analysis Practical use cases and best practices for information security Who This Book Is For This book is for security analysts and professionals who deal with security mechanisms in an organization. If you are looking for an end to end guide on information security and risk analysis with no prior knowledge of this domain, then this book is for you. What You Will Learn Develop your own information security framework Build your incident response mechanism Discover cloud security considerations Get to know the system development life cycle Get your security operation center up and running Know the various security testing types Balance security as per your business needs Implement information security best practices In Detail Having an information security mechanism is one of the most crucial factors for any organization. Important assets of organization demand a proper risk management and threat model for security, and so information security concepts are gaining a lot of traction. This book starts with the concept of information security and shows you why it's important. It then moves on to modules such as threat modeling, risk management, and mitigation. It also covers the concepts of incident response systems, information rights management, and more. Moving on, it guides you to build your own information security framework as the best fit for your organization. Toward the end, you'll discover some best practices that can be implemented to make your security framework strong. By the end of this book, you will be well-versed with all the factors involved in information security, which will help you build a security framework that is a perfect fit your organization's requirements. Style and approach This book takes a practical approach, walking you through information security fundamentals, along with information security best practices.

Incident Response & Computer Forensics, Third Edition Newnes

Blue Team Field Manual (BTFM) is a Cyber Security Incident Response Guide that aligns with the NIST Cybersecurity Framework consisting of the five core functions of Identify,

Protect, Detect, Respond, and Recover by providing the tactical steps to follow and commands to use when preparing for, working through and recovering from a Cyber Security Incident.

Applied Incident Response Independently Published

This book is a comprehensive guide for organizations on how to prepare for cyber-attacks, control cyber threats and network security breaches in a way that decreases damage, recovery time, and costs, and adapt existing strategies to cloud-based environments.

Don's Story "O'Reilly Media, Inc."

From the creator of the popular website Ask a Manager and New York's work-advice columnist comes a witty, practical guide to 200 difficult professional conversations—featuring all-new advice! There's a reason Alison Green has been called "the Dear Abby of the work world." Ten years as a workplace-advice columnist have taught her that people avoid awkward conversations in the office because they simply don't know what to say. Thankfully, Green does—and in this incredibly helpful book, she tackles the tough discussions you may need to have during your career. You'll learn what to say when • coworkers push their work on you—then take credit for it • you accidentally trash-talk someone in an email then hit "reply all" • you're being micromanaged—or not being managed at all • you catch a colleague in a lie • your boss seems unhappy with your work • your cubemate's loud speakerphone is making you homicidal • you got drunk at the holiday party Praise for Ask a Manager "A must-read for anyone who works . . . [Alison Green's] advice boils down to the idea that you should be professional (even when others are not) and that communicating in a straightforward manner with candor and kindness will get you far, no matter where you work."—Booklist (starred review) "The author's friendly, warm, no-nonsense writing is a pleasure to read, and her advice can be widely applied to relationships in all areas of readers' lives. Ideal for anyone new to the job market or new to management, or anyone hoping to improve their work experience."—Library Journal (starred review) "I am a huge fan of Alison Green's Ask a Manager column. This book is even better. It teaches us how to deal with many of the most vexing big and little problems in our workplaces—and to do so with grace, confidence, and a sense of humor."—Robert Sutton, Stanford professor and author of The No Asshole Rule and The Asshole Survival Guide "Ask a Manager is the ultimate playbook for navigating the traditional workforce in a diplomatic but firm way."—Erin Lowry, author of Broke Millennial: Stop Scraping By and Get Your Financial Life Together

The Practice of Network Security Monitoring Pragma LLC

Enhance your organization's secure posture by improving your attack and defense strategies Key Features Gain a clear understanding of the attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics. Learn to unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies. A practical guide that will give you hands-on experience to mitigate risks and prevent attackers from infiltrating your system. Book Description The book will start talking about the security posture before moving to Red Team tactics, where you will learn the basic syntax for the Windows and Linux tools that are commonly used to perform the necessary operations. You will also gain hands-on experience of using new Red Team techniques with powerful tools such as python and PowerShell, which will enable you to discover vulnerabilities in your system and how to exploit them. Moving on, you will learn how a system is usually compromised by adversaries, and how they hack user's identity, and the various tools used by the Red Team to find vulnerabilities in a system. In the next section, you will learn about the defense strategies followed by the Blue Team to enhance the overall security of a system. You will also learn about an in-depth strategy to ensure that there are security controls in each network layer, and how you can carry out the recovery process of a compromised system. Finally, you will learn how to create a vulnerability management strategy and the different techniques for manual log analysis. By the end of this book, you will be well-versed with Red Team and Blue Team techniques and will have learned the techniques used nowadays to attack and defend systems. What you will learn Learn the importance of having a solid foundation for your security posture Understand the attack strategy using cyber security kill chain Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence Learn how to perform

an incident investigation Get an in-depth understanding of the recovery process Understand continuous security monitoring and how to implement a vulnerability management strategy Learn how to perform log analysis to identify suspicious activities Who this book is for This book aims at IT professional who want to venture the IT security domain. IT pentester, Security consultants, and ethical hackers will also find this course useful. Prior knowledge of penetration testing would be beneficial.

computer security and incident response Packt Publishing Ltd

"Incident Response is a complete guide for organizations of all sizes and types who are addressing their computer security issues."--Jacket.

Incident Response in the Age of Cloud John Wiley & Sons

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

Killer in the Pool Independently Published

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.

Ask a Manager "O'Reilly Media, Inc."

Successfully responding to modern cybersecurity threats requires a well-planned, organized, and tested incident management program based on a formal incident management framework. It must be comprised of technical and non-technical requirements and planning for all aspects of people, process, and technology. This includes evolving considerations specific to the customer environment, threat landscape, regulatory requirements, and security controls. Only through a highly adaptive, iterative, informed, and continuously evolving full-lifecycle incident management program can responders and the companies they support be successful in combatting cyber threats. This book is the first in a series of volumes that explains in detail the full-lifecycle cybersecurity incident management program. It has been developed over two decades of security and response experience and honed across thousands of customer environments, incidents, and program development projects. It accommodates all regulatory and security requirements and is effective against all known and newly evolving cyber threats.

Volume 1 - Preparation, Threat Response, & Post-Incident

Activity No Starch Press

The Wildland Fire Incident Management Field Guide is a revision of what used to be called the Fireline Handbook, PMS 410-1. This guide has been renamed because, over time, the original purpose of the Fireline Handbook had been replaced by the Incident Response Pocket Guide, PMS 461. As a result, this new guide is aimed at a different audience, and it was felt a new name was in order.

Infrastructure security with Red Team and Blue Team tactics McGraw Hill Professional

On February 24, 2010, Tilikum, the largest killer whale at SeaWorld, suddenly dragged Dawn Brancheau, his trainer, into the pool and killed her. Journalist Tim Zimmermann set out to find out why. His riveting account of Tilikum's life, and the history of killer whale entertainment at marine parks, dives into the world of the ocean's top predator. It chronicles Tilikum's capture and separation from his family, and the physical and psychological stress he experienced in marine park pools over some 30 years. It explores Tilikum's involvement in two previous deaths. And it details the inherent risks of using captive killer whales for human entertainment. Ultimately, Zimmermann explains how the life of Tilikum came to mean the death of Dawn Brancheau.

Deployment Strategies for Production Environments Apress

Implement a vendor-neutral and multi-cloud cybersecurity and risk mitigation framework with advice from seasoned threat hunting pros In *Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks*, celebrated cybersecurity professionals and authors Chris Peiris, Binil Pillai, and Abbas Kudrati leverage their decades of experience building large scale cyber fusion centers to deliver the ideal threat hunting resource for both business and technical audiences. You'll find insightful analyses of cloud platform security tools and, using the industry leading MITRE ATT&CK framework, discussions of the most common threat vectors. You'll discover how to build a side-by-side cybersecurity fusion center on both Microsoft Azure and Amazon Web Services and deliver a multi-cloud strategy for enterprise customers. And you will find out how to create a vendor-neutral environment with rapid disaster recovery capability for maximum risk mitigation. With this book you'll learn: Key business and technical drivers of cybersecurity threat hunting frameworks in today's technological environment Metrics available to assess threat hunting effectiveness regardless of an organization's size How threat hunting works with vendor-specific single cloud security offerings and on multi-cloud implementations A detailed analysis of key threat vectors such as email phishing, ransomware and nation state attacks Comprehensive AWS and Azure "how to" solutions through the lens of MITRE Threat Hunting Framework Tactics, Techniques and Procedures (TTPs) Azure and AWS risk mitigation strategies to combat key TTPs such as privilege escalation, credential theft, lateral movement, defend against command & control systems, and prevent data exfiltration Tools available on both the Azure and AWS cloud platforms which provide automated responses to attacks, and orchestrate preventative measures and recovery strategies Many critical components for successful adoption of multi-cloud threat hunting framework such as Threat Hunting Maturity Model, Zero Trust Computing, Human Elements of Threat Hunting, Integration of Threat Hunting with Security Operation Centers (SOCs) and Cyber Fusion Centers The Future of Threat Hunting with the advances in Artificial Intelligence, Machine Learning, Quantum Computing and the proliferation of IoT devices. Perfect for technical executives (i.e., CTO, CISO), technical managers, architects, system admins and consultants with hands-on responsibility for cloud platforms, *Threat Hunting in the Cloud* is also an indispensable guide for business executives (i.e., CFO, COO CEO, board members) and managers who need to understand their organization's cybersecurity risk framework and mitigation strategy.

What CISOs Need to Know about Risk-Based Cybersecurity Newnes

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

Intelligence-Driven Incident Response Createspace Independent Publishing Platform

Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases is having an amazing impact on Security Operations worldwide. BTHb:SOCTH is the go to guiding book for new staff at a top 10 MSSP, integrated into University curriculum, and cited in top ten courses from a major information security training company. This listing is for V1.02.BTHb:SOCTH provides the security practitioner with numerous field notes on building a security operations team, managing SIEM, and mining data sources to get the maximum amount of information out of them with a threat hunting approach. The author shares his fifteen years of experience with SIEMs and security operations is a no frills, just information format. Don Murdoch has implemented five major platforms, integrated over one hundred data sources into various platforms, and ran an MSSP practice for two years.This book covers the topics below using a "zero fluff" approach as if you hired him as a security consultant and were sitting across the table with him (or her).The book begins with a discussion for professionals to help them build a successful business case and a project plan, decide on SOC tier models, anticipate and answer tough questions you need to consider when proposing a SOC, and considerations in building a logging infrastructure. The book goes through numerous data sources that feed a SOC and SIEM and provides specific real world guidance on how to use those data sources to best possible effect. Most of the examples presented were implemented in one organization or another. These uses cases explain on what to monitor, how to use a SIEM and how to use the data coming into the platform, both questions that Don found is often answered poorly by many vendors. Several business concepts are also introduced, because they are often overlooked by IT: value chain, PESTL, and SWOT. Major sections include:An inventory of Security Operations Center (SOC) Services.Metrics, with a focus on objective measurements for the SOC, for analysts, and for SIEM's.SOC staff onboarding, training topics, and desirable skills. Along these lines, there is a chapter on a day in the life of a SOC analyst.Maturity analysis for the SOC and the log management program. Applying a Threat Hunt mindset to the SOC. A full use case template that was used within two major Fortune 500 companies, and is in active use by one major SIEM vendor, along with a complete example of how to build a SOC and SIEM focused use case. You can see the corresponding discussion of this chapter on YouTube. Just search for the 2017 Security Onion conference for the presentation.Critical topics in deploying SIEM based on experience deploying five different technical platforms for nineteen different organizations in education, nonprofit, and commercial enterprises from 160 to 30,000 personnel.Understanding why SIEM deployments fail with actionable compensators. Real life experiences getting data into SIEM platforms and the considerations for the many different ways to provide data. Issues relating to time, time management, and time zones.

Understanding Incident Detection and Response Packt Publishing Ltd

This self-study guide delivers complete coverage of every topic on the GIAC Certified Incident Handler exam Prepare for the challenging GIAC Certified Incident Handler exam using the detailed information contained in this effective exam preparation guide. Written by a recognized cybersecurity expert and seasoned author, GCIH GIAC Certified Incident Handler All-in-One Exam Guide clearly explains all of the advanced security incident handling skills covered on the test. Detailed examples and chapter summaries throughout demonstrate real-world threats and aid in retention. You will get online access to 300 practice questions that match those on the live test in style, format, and tone. Designed to help you prepare for the exam, this resource also serves as an ideal on-the-job reference. Covers all exam topics, including: Intrusion analysis and incident handling Information gathering Scanning, enumeration, and vulnerability identification Vulnerability exploitation Infrastructure and endpoint attacks Network, DoS, and Web application attacks Maintaining access Evading detection and covering tracks Worms, bots, and botnets Online content includes: 300 practice exam questions Test engine that provides full-length practice exams and customizable quizzes