

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

Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases provides the security practitioner with numerous field notes on building a security operations team 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 after implementing five major platforms, integrating over one hundred data sources into various platforms, and running a MSSP practice. 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). Topics covered include:

- * The book begins with a discussion for professionals to help them build a successful business case and a project plan, and deciding on SOC tier models. There is also a list of tough questions you need to consider when proposing a SOC, as well as a discussion of layered operating models.
- * It then goes through numerous data sources that feed a SOC and SIEM and provides specific guidance on how to use those data sources. Most of the examples presented were implemented in one organization or another. These uses cases explain how to use a SIEM and how to use the data coming into the platform, a question that is poorly answered by many vendors.
- * An inventory of Security Operations Center (SOC) Services.
- * Several business concepts are also introduced, because they are often overlooked

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

by IT: value chain, PESTL, and SWOT. * Metrics. * 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 on YouTube - search for the 2017 Security Onion conference. * 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. * Critical factors in log management, network security monitoring, continuous monitoring, and security architecture related directly to SOC and SIEM.* A table of useful TCP and UDP port numbers.This is the second book in the Blue Team Handbook Series. Volume One, focused on incident response, has over 32,000 copies in print and has a 4.5/5.0 review rating!

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 organization This 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

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

phases. Preparation Identification Containment Eradication Recovery Lessons Learned/Follow-up

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

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

Digital Forensics with Open Source Tools is the definitive book on investigating and analyzing computer systems and media using open source tools. The book is a technical procedural guide, and explains the use of open source tools on Mac, Linux and Windows systems as a platform for performing computer forensics. Both well-known and novel forensic methods are

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

demonstrated using command-line and graphical open source computer forensic tools for examining a wide range of target systems and artifacts. Written by world-renowned forensic practitioners, this book uses the most current examination and analysis techniques in the field. It consists of 9 chapters that cover a range of topics such as the open source examination platform; disk and file system analysis; Windows systems and artifacts; Linux systems and artifacts; Mac OS X systems and artifacts; Internet artifacts; and automating analysis and extending capabilities. The book lends itself to use by students and those entering the field who do not have means to purchase new tools for different investigations. This book will appeal to forensic practitioners from areas including incident response teams and computer forensic investigators; forensic technicians from legal, audit, and consulting firms; and law enforcement agencies. Written by world-renowned forensic practitioners Details core concepts and techniques of forensic file system analysis Covers analysis of artifacts from the Windows, Mac, and Linux operating systems

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

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

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

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

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. 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

The idea of "The Green Book" is to give the Motorist and Tourist a Guide not only of the Hotels and Tourist Homes in all of the large cities, but other classifications that will be found useful wherever he may be. Also facts and information that the Negro Motorist can use and depend upon. There are thousands of places that the public doesn't know about and aren't listed. Perhaps you know of some? If so send in their names and addresses and the kind of business,

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

so that we might pass it along to the rest of your fellow Motorists. You will find it handy on your travels, whether at home or in some other state, and is up to date. Each year we are compiling new lists as some of these places move, or go out of business and new business places are started giving added employment to members of our race.

Look around your office. Turn on the TV. Incompetent leadership is everywhere, and there's no denying that most of these leaders are men. In this timely and provocative book, Tomas Chamorro-Premuzic asks two powerful questions: Why is it so easy for incompetent men to become leaders? And why is it so hard for competent people--especially competent women--to advance? Marshaling decades of rigorous research, Chamorro-Premuzic points out that although men make up a majority of leaders, they underperform when compared with female leaders. In fact, most organizations equate leadership potential with a handful of destructive personality traits, like overconfidence and narcissism. In other words, these traits may help someone get selected for a leadership role, but they backfire once the person has the job. When competent women--and men who don't fit the stereotype--are unfairly overlooked, we all suffer the consequences. The result is a deeply flawed system that rewards arrogance rather than humility, and loudness rather than wisdom. There is a better way. With clarity and verve, Chamorro-Premuzic shows us what it really takes to lead and how new systems and processes can help us put the right people in charge.

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

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

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

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

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. Tired of playing catchup with hackers? Does it ever seem they have all of the cool tools? Does it seem like defending a network is just not fun? This books introduces new cyber-security defensive tactics to annoy attackers, gain attribution and insight on who and where they are. It discusses how to attack attackers in a way which is legal and incredibly useful.

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

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

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. Blue Team Handbook Incident Response Edition: a Condensed Field Guide for the Cyber Security Incident Responder CreateSpace

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

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

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

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

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

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.

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.

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.

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

Security Operations Center Building, Operating, and Maintaining Your SOC The complete, practical guide to planning, building, and operating an effective Security Operations Center (SOC) Security Operations Center is the complete guide to building, operating, and managing Security Operations Centers in any environment. Drawing on experience with hundreds of customers ranging from Fortune 500 enterprises to large military organizations, three leading experts thoroughly review each SOC model, including virtual SOCs. You'll learn how to select the right strategic option for your organization, and then plan and execute the strategy you've chosen. Security Operations Center walks you through every phase required to establish and run an effective SOC, including all significant people, process, and technology capabilities. The authors assess SOC technologies, strategy, infrastructure, governance, planning, implementation, and more. They take a holistic approach considering various commercial and open-source tools found in modern SOCs. This best-practice guide is written for anybody interested in learning how to develop, manage, or improve a SOC. A background in network security, management, and operations will be helpful but is not required. It is also an indispensable resource for anyone preparing for the Cisco SCYBER exam. • Review high-level issues, such as vulnerability and risk management, threat intelligence, digital investigation, and data collection/analysis

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

- Understand the technical components of a modern SOC
- Assess the current state of your SOC and identify areas of improvement
- Plan SOC strategy, mission, functions, and services
- Design and build out SOC infrastructure, from facilities and networks to systems, storage, and physical security
- Collect and successfully analyze security data
- Establish an effective vulnerability management practice
- Organize incident response teams and measure their performance
- Define an optimal governance and staffing model
- Develop a practical SOC handbook that people can actually use
- Prepare SOC to go live, with comprehensive transition plans
- React quickly and collaboratively to security incidents
- Implement best practice security operations, including continuous enhancement and improvement

Cortex XSOAR is the Security Orchestration, Automation and Response (SOAR) solution from Palo Alto Networks. Cortex XSOAR provides a centralized security orchestration and Automation solution to accelerate incident response and increase analyst productivity. A SOAR platform integrates your organization's security and monitoring tools, helping you centralize, standardize your incident handling processes. This book is a beginner friendly, step by step, practical guide that helps you to understand and learn Palo Alto Cortex XSOAR from scratch. No previous knowledge about the product is required and have explained all the

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

important topics step by step, with screenshots. Covers, 1) Solution architecture 2) Incident lifecycle in Cortex XSOAR 3) Integrations and incident creation 4) Playbook development 5) Layout customization 6) Report creation 7) Backup options 8) Threat Intel management and EDL integration. 9) Introduction to MSSP. 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.

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

The Red Team Field Manual (RTFM) is a no fluff, but thorough reference guide for serious Red Team members who routinely find themselves on a mission without Google or the time to scan through a man page. The RTFM contains the basic syntax for commonly used Linux and Windows command line tools, but it also encapsulates unique use cases for powerful tools such as Python and Windows PowerShell. The RTFM will repeatedly save you time looking up the hard to remember Windows nuances such as Windows wmic and dsquery command line tools, key registry values, scheduled tasks syntax, startup locations and Windows scripting. More importantly, it should teach you some new red team techniques.

The ultimate guide for anyone wondering how President Joe Biden will respond to the COVID-19 pandemic—all his plans, goals, and executive orders in response to the coronavirus crisis. Shortly after being inaugurated as the 46th President of the United States, Joe Biden and his administration released this 200 page guide detailing his plans to respond to the coronavirus pandemic. The National Strategy for the COVID-19 Response and Pandemic Preparedness breaks down seven crucial goals of President Joe Biden's administration with regards to the coronavirus pandemic: 1. Restore trust with the American people. 2. Mount a safe, effective, and comprehensive vaccination campaign. 3. Mitigate spread

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

through expanding masking, testing, data, treatments, health care workforce, and clear public health standards. 4. Immediately expand emergency relief and exercise the Defense Production Act. 5. Safely reopen schools, businesses, and travel while protecting workers. 6. Protect those most at risk and advance equity, including across racial, ethnic and rural/urban lines. 7. Restore U.S. leadership globally and build better preparedness for future threats. Each of these goals are explained and detailed in the book, with evidence about the current circumstances and how we got here, as well as plans and concrete steps to achieve each goal. Also included is the full text of the many Executive Orders that will be issued by President Biden to achieve each of these goals. The National Strategy for the COVID-19 Response and Pandemic Preparedness is required reading for anyone interested in or concerned about the COVID-19 pandemic and its effects on American society.

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

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

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 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

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

cloud-based environments.

JUMPSTART YOUR NEW AND EXCITING CAREER AS A PENETRATION TESTER The Pentester BluePrint: Your Guide to Being a Pentester offers readers a chance to delve deeply into the world of the ethical, or "white-hat" hacker. Accomplished pentester and author Phillip L. Wylie and cybersecurity researcher Kim Crawley walk you through the basic and advanced topics necessary to understand how to make a career out of finding vulnerabilities in systems, networks, and applications. You'll learn about the role of a penetration tester, what a pentest involves, and the prerequisite knowledge you'll need to start the educational journey of becoming a pentester. Discover how to develop a plan by assessing your current skillset and finding a starting place to begin growing your knowledge and skills. Finally, find out how to become employed as a pentester by using social media, networking strategies, and community involvement. Perfect for IT workers and entry-level information security professionals, The Pentester BluePrint also belongs on the bookshelves of anyone seeking to transition to the exciting and in-demand field of penetration testing. Written in a highly approachable and accessible style, The Pentester BluePrint avoids unnecessarily technical lingo in favor of concrete advice and practical strategies to help you get your start in pentesting. This book will teach

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

you: The foundations of pentesting, including basic IT skills like operating systems, networking, and security systems The development of hacking skills and a hacker mindset Where to find educational options, including college and university classes, security training providers, volunteer work, and self-study Which certifications and degrees are most useful for gaining employment as a pentester How to get experience in the pentesting field, including labs, CTFs, and bug bounties

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.

A practical handbook to cybersecurity for both tech and non-tech professionals As reports of major data breaches fill the headlines, it has become impossible for any business, large or small, to ignore the importance of cybersecurity. Most books on the subject, however, are either too specialized for the non-technical professional or too general for positions in the IT trenches. Thanks to author Nadean Tanner's wide array of experience from teaching at a University to working for the Department of Defense, the Cybersecurity Blue Team Toolkit strikes the perfect balance of substantive and accessible, making it equally useful to those in IT or management positions across a variety of industries. This handy guide takes a simple and strategic look at best practices and tools available to both cybersecurity management and hands-on professionals, whether they be new to the field or looking to expand their expertise.

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

Tanner gives comprehensive coverage to such crucial topics as security assessment and configuration, strategies for protection and defense, offensive measures, and remediation while aligning the concept with the right tool using the CIS Controls version 7 as a guide. Readers will learn why and how to use fundamental open source and free tools such as ping, tracer, PuTTY, pathping, sysinternals, NMAP, OpenVAS, Nexpose Community, OSSEC, Hamachi, InSSIDer, Nexpose Community, Wireshark, Solarwinds Kiwi Syslog Server, Metasploit, Burp, Clonezilla and many more. Up-to-date and practical cybersecurity instruction, applicable to both management and technical positions • Straightforward explanations of the theory behind cybersecurity best practices • Designed to be an easily navigated tool for daily use • Includes training appendix on Linux, how to build a virtual lab and glossary of key terms The Cybersecurity Blue Team Toolkit is an excellent resource for anyone working in digital policy as well as IT security professionals, technical analysts, program managers, and Chief Information and Technology Officers. This is one handbook that won't gather dust on the shelf, but remain a valuable reference at any career level, from student to executive.

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"

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

• 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*

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

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

version.

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

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

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

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

The Operator Handbook takes three disciplines (Red Team, OSINT, Blue Team) and combines them into one complete reference guide. The book contains 123 individual cheat sheet references for many of the most frequently used tools and techniques by practitioners. Over 400 pages of content to assist the most seasoned cybersecurity veteran or someone just getting started in the career field. The goal of combining all disciplines into one book was to remove the artificial barriers that only certain knowledge exists within a "Team". The reality is today's complex digital landscape demands some level of knowledge in all areas. The "Operator" culture should mean a well-rounded team member no matter the "Team" you represent. All cybersecurity practitioners are Operators. The Blue Team should observe and understand Red Team tactics, Red Team should continually push collaboration with the Blue Team, and OSINT should continually work to peel back evidence of evil doers scattered across disparate data sources. In the spirit of having no separation, each reference is listed in alphabetical order. Not only does this remove those team separated notions, but it also aids in faster lookup. We've all had the same experience where we knew there was an "NMAP Cheat Sheet" but did it fall under Networking, Windows, or Tools? In the Operator Handbook it begins with "N" so flip to the N's section. Also almost every topic is covered in "How to exploit X" and

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

"How to defend X" perspectives. Tools and topics covered: Cloud (AWS, Azure, GCP), Windows, macOS, Linux, Android, iOS, DevOps (Docker, Kubernetes), OSINT, Ports, Forensics, Malware Resources, Defender tools, Attacker tools, OSINT tools, and various other supporting tools (Vim, iptables, nftables, etc...). This handbook was truly meant to be a single source for the most common tool and techniques an Operator can encounter while on the job. Search Copy Paste L33t.

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

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

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

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 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

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

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

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

The New York Times best-selling book exploring the counterproductive reactions white people have when their assumptions about race are challenged, and how these reactions maintain racial inequality. In this "vital, necessary, and beautiful book" (Michael Eric Dyson), antiracist educator Robin DiAngelo deftly illuminates the phenomenon of white fragility and "allows us to understand racism as a practice not restricted to 'bad people' (Claudia Rankine). Referring to the defensive moves that white people make when challenged racially, white fragility is characterized by emotions such as anger, fear, and guilt, and by behaviors including argumentation and silence. These behaviors, in turn, function to reinstate white racial

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

equilibrium and prevent any meaningful cross-racial dialogue. In this in-depth exploration, DiAngelo examines how white fragility develops, how it protects racial inequality, and what we can do to engage more constructively.

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 This comprehensive book instructs IT managers to adhere to federally mandated compliance requirements. FISMA Compliance Handbook Second Edition explains what the requirements are for FISMA compliance and why FISMA compliance is mandated by federal law. The

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

evolution of Certification and Accreditation is discussed. This book walks the reader through the entire FISMA compliance process and includes guidance on how to manage a FISMA compliance project from start to finish. The book has chapters for all FISMA compliance deliverables and includes information on how to conduct a FISMA compliant security assessment. Various topics discussed in this book include the NIST Risk Management Framework, how to characterize the sensitivity level of your system, contingency plan, system security plan development, security awareness training, privacy impact assessments, security assessments and more. Readers will learn how to obtain an Authority to Operate for an information system and what actions to take in regards to vulnerabilities and audit findings. FISMA Compliance Handbook Second Edition, also includes all-new coverage of federal cloud computing compliance from author Laura Taylor, the federal government's technical lead for FedRAMP, the government program used to assess and authorize cloud products and services. Includes new information on cloud computing compliance from Laura Taylor, the federal government's technical lead for FedRAMP Includes coverage for both corporate and government IT managers Learn how to prepare for, perform, and document FISMA compliance projects This book is used by various colleges and universities in information security and MBA curriculums

Despite the increase of high-profile hacks, record-breaking data leaks, and ransomware attacks, many organizations don't have the budget to establish or outsource an information security (InfoSec) program, forcing them to learn on the job. For companies obliged to improvise, this pragmatic guide provides a security-101 handbook with steps, tools, processes, and ideas to help you drive maximum-security improvement at little or no cost. Each chapter in

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

this book provides step-by-step instructions for dealing with a specific issue, including breaches and disasters, compliance, network infrastructure and password management, vulnerability scanning, and penetration testing, among others. Network engineers, system administrators, and security professionals will learn tools and techniques to help improve security in sensible, manageable chunks. Learn fundamentals of starting or redesigning an InfoSec program Create a base set of policies, standards, and procedures Plan and design incident response, disaster recovery, compliance, and physical security Bolster Microsoft and Unix systems, network infrastructure, and password management Use segmentation practices and designs to compartmentalize your network Explore automated process and tools for vulnerability management Securely develop code to reduce exploitable errors Understand basic penetration testing concepts through purple teaming Delve into IDS, IPS, SOC, logging, and monitoring

[Copyright: 0bfea9a8d5aeaa45aafe229bca202425](https://www.pdfdrive.com/blue-team-handbook-incident-response-edition-a-condensed-field-guide-for-the-cyber-security-incident-responder-ebook.html)