Blue Team Handbook

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

Hundreds of organizations around the world have already benefited from DisciplinedAgile Delivery (DAD). Disciplined Agile (DA) is the only comprehensive tool kit available for guidance on building high-performance agile teams and optimizing your way of working(WoW). As a hybrid of all the leading agile and lean approaches, it provides hundreds of strategies to help you make better decisions within your agile teams, balancing self-organization with the realities and constraints of your unique enterprise context.The highlights of this handbook include:&•As the official source of knowledge on DAD, it includes greatly improved and enhanced strategies with a revised set of goal diagrams based upon learnings from applying DAD in the field.&•It is an essential handbook to help coaches and teams make better decisions in their daily work, providing a wealth of ideas for experimenting with agile and lean techniques while providing specific guidance and trade-offs for those &“it depends&” questions.&•It makes a perfect study guide for Disciplined Agile certification.Why &“fail fast&” (as our industry likes to recommend) when you can learn quickly on your journey to high performance? With this handbook, you can make better decisions based upon proven, context-based strategies, leading to earlier success and better outcomes.

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

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.

Essential reading for business leaders and policymakers, an in-depth investigation of red teaming, the practice of inhabiting the perspective of potential competitors to gain a strategic advantage Red teaming. The concept is as old as the Devil's Advocate, the eleventh-century Vatican official charged with discrediting candidates for sainthood. Today, red teams are used widely in both the public and the private sector by those seeking to better understand the interests, intentions, and capabilities of institutional rivals. In the right circumstances, red teams can yield impressive results, giving businesses an edge over their competition, poking holes in vital intelligence estimates, and troubleshooting dangerous military missions long before boots are on the ground. But not all red teams are created equal; indeed, some cause more damage than they prevent. Drawing on a fascinating range of case studies, Red Team shows not only how to create and empower red teams, but also what to do with the information they produce. In this vivid, deeply-informed account, national security expert Micah Zenko provides the definitive book on this important strategy -- full of vital insights for decision makers of all kinds.

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

This book is a practical guide to discovering and exploiting security flaws in web applications. The authors explain each category of vulnerability using real-world examples, screen shots and code extracts. The book is extremely practical in focus, and describes in detail the steps involved in detecting and exploiting each kind of security weakness found within a variety of applications such as online banking, e-commerce and other web applications. The topics covered include bypassing login mechanisms, injecting code, exploiting logic flaws and compromising other users. Because every web application is different, attacking them entails bringing to bear various general principles, techniques and experience in an imaginative way. The most successful hackers go beyond this, and find ways to automate their bespoke attacks. This handbook describes a proven methodology that combines the virtues of human intelligence and computerized brute force, often with devastating results. The authors are professional penetration testers who have been involved in web application security for nearly a decade. They have presented training courses at the Black Hat security conferences throughout the world. Under the alias "PortSwigger", Dafydd developed the popular Burp Suite of web application hack tools.

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. 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, tracert, 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.

This book is the culmination of years of experience in the information technology and cybersecurity field. Components of this book have existed as rough notes, ideas, informal and formal processes developed and adopted by the authors as they led and executed red team engagements over many years. The concepts described in this book have been used to successfully plan, deliver, and perform professional red team engagements of all sizes and complexities. Some of these concepts were loosely documented and integrated into red team management processes, and much was kept as tribal knowledge. One of the first formal attempts to capture this information was the SANS SEC564 Red Team Operation and Threat Emulation course. This first effort was an attempt to document these ideas in a format usable by others. The authors have moved beyond SANS training and use this book to detail red team operations in a practical guide. The authors' goal is to provide practical guidance to aid in the management and execution of professional red teams. The term 'Red Team' is often confused in the cybersecurity space. The terms roots are based on military concepts that have slowly made their way into the commercial space. Numerous interpretations directly affect the scope and quality of today's security engagements. This confusion has created unnecessary difficulty as organizations attempt to measure threats from the results of quality security assessments. You quickly understand the complexity of red teaming by performing a quick google search for the definition, or better yet, search through the numerous interpretations and opinions posted by security professionals on Twitter. This book was written to provide a practical solution to address this confusion. The Red Team concept requires a unique approach different from other security tests. It relies heavily on well-defined TTPs critical to the successful simulation of realistic threat and

adversary techniques. Proper Red Team results are much more than just a list of flaws identified during other security tests. They provide a deeper understanding of how an organization would perform against an actual threat and determine where a security operation's strengths and weaknesses exist.Whether you support a defensive or offensive role in security, understanding how Red Teams can be used to improve defenses is extremely valuable. Organizations spend a great deal of time and money on the security of their systems. It is critical to have professionals who understand the threat and can effectively and efficiently operate their tools and techniques safely and professionally. This book will provide you with the real-world guidance needed to manage and operate a professional Red Team, conduct quality engagements, understand the role a Red Team plays in security operations. You will explore Red Team concepts in-depth, gain an understanding of the fundamentals of threat emulation, and understand tools needed you reinforce your organization's security posture.

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 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

Healthcare providers, consumers, researchers and policy makers are inundated with unmanageable amounts of information, including evidence from healthcare research. It has become impossible for all to have the time and resources to find, appraise and interpret this evidence and incorporate it into healthcare decisions.

Cochrane Reviews respond to this challenge by identifying, appraising and synthesizing research-based evidence and presenting it in a standardized format, published in The Cochrane Library (www.thecochranelibrary.com). The Cochrane Handbook for Systematic Reviews of Interventions contains methodological guidance for the preparation and maintenance of Cochrane intervention reviews. Written in a clear and accessible format, it is the essential manual for all those preparing, maintaining and reading Cochrane reviews. Many of the principles and methods described here are appropriate for systematic reviews applied to other types of research and to systematic reviews of interventions undertaken by others. It is hoped therefore that this book will be invaluable to all those who want to understand the role of systematic reviews, critically appraise published reviews or perform reviews themselves.

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.

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.

"Collaborations that integrate diverse perspectives are critical to addressing many of our complex scientific and societal problems. Yet those engaged in cross-disciplinary team science often face institutional barriers and collaborative challenges. Strategies for Team Science Success offers readers a

comprehensive set of actionable strategies for reducing barriers and overcoming challenges and includes practical guidance for how to implement effective team science practices. More than 100 experts--including scientists, administrators, and funders from a wide range of disciplines and professions-- explain evidence-based principles, highlight state-of the-art strategies, tools, and resources, and share first-person accounts of how they've applied them in their own successful team science initiatives. While many examples draw from cross-disciplinary team science initiatives in the health domain, the handbook is designed to be useful across all areas of science. Strategies for Team Science Success will inspire and enable readers to embrace cross-disciplinary team science, by articulating its value for accelerating scientific progress, and by providing practical strategies for success. Scientists, administrators, funders, and others engaged in team science will also leave equipped to develop new policies and practices needed to keep pace in our rapidly changing scientific landscape. Scholars across the Science of Team Science (SciTS), management, organizational, behavioral and social sciences, public health, philosophy, and information technology, among other areas of scholarship, will find inspiration for new research directions to continue advancing cross-disciplinary team science." -- Prové de l'editor.

The world’s challenges are becoming more and more complex and adapting to those challenges will increasingly come from teams of people innovating together. The Practitioner’s Handbook of Team Coaching provides a dedicated and systematic guide to some of the most fundamental issues concerning the practice of team coaching. It seeks to enhance practice through illustrating and exploring an array of contextual issues and complexities entrenched in it. The aim of the volume is to provide a comprehensive overview of the field and, furthermore, to enhance the understanding and practice of team coaching. To do so, the editorial team presents, synthesizes and integrates relevant theories, research and practices that comprise and undergird team coaching. This book is, therefore, an invaluable specialist tool for team coaches of all levels; from novice to seasoned practitioners. With team coaching assuming an even more prominent place in institutional and organizational contexts nowadays, the book is bound to become an indispensable resource for any coaching training course, as well as a continuing professional development tool. This book is essential reading for anyone with an interest in coaching, in both practice and educational settings. It will be of use not only for professional coaches, but also for leaders, managers, HR professionals, learners and educators, in the business, public, independent and voluntary sectors.

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

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 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

#1 NEW YORK TIMES AND WALL STREET JOURNAL BESTSELLER Pay brand-new employees $2,000 to quit Make customer service the responsibility of the entire company-not just a department Focus on company culture as the #1 priority Apply research from the science of happiness to running a business Help employees grow-both personally and professionally Seek to change the world Oh, and make money too . . . Sound crazy? It's all standard operating procedure at Zappos, the online retailer that's doing over $1 billion in gross merchandise sales annually. After debuting as the highest-ranking newcomer in Fortune magazine's annual "Best Companies to Work For" list in 2009, Zappos was acquired by Amazon in a deal valued at over $1.2 billion on the day of closing. In DELIVERING HAPPINESS, Zappos CEO Tony Hsieh shares the different lessons he has learned in business and life, from starting a worm farm to running a pizza business, through LinkExchange, Zappos, and more. Fast-paced and down-to-earth, DELIVERING HAPPINESS shows how a very different kind of corporate culture is a powerful model for achieving success-and how by concentrating on the happiness of those around you, you can dramatically

increase your own. To learn more about the book, go to www.deliveringhappinessbook.com.
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

This second edition of the Handbook of Employee Selection has been revised and updated throughout to reflect current thinking on the state of science and practice in employee selection. In this volume, a diverse group of recognized scholars inside and outside the United States balance theory, research, and practice, often taking a global perspective. Divided into eight parts, chapters cover issues associated with measurement, such as validity and reliability, as well as practical concerns around the development of appropriate selection procedures and implementation of selection programs. Several chapters discuss the measurement of various constructs commonly used as predictors, and other chapters confront criterion measures that are used in test validation. Additional sections include chapters that focus on ethical and legal concerns and testing for certain types of jobs (e.g., blue collar jobs). The second edition features a new section on technology and employee selection. The Handbook of Employee Selection, Second Edition provides an indispensable reference for scholars, researchers, graduate students, and professionals in industrial and organizational psychology, human resource management, and related fields.

Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1. 02)A Condensed Guide for the Security Operations Team and Threat Hunter

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

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 "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.

“An excellent guide on how teams can effectively work together, regardless of location.” —STEPHANE KASRIEL, former CEO of Upwork IN TODAY’S MODERN GLOBAL ECONOMY, companies and organizations in all sectors are embracing the game-changing benefits of the remote workplace. Managers benefit by saving money and resources and by having access to talent outside their zip codes, while employees enjoy greater job opportunities, productivity, independence, and work-life satisfaction. But in this new digital arena, companies need a plan for supporting efficiency and fostering streamlined, engaging teamwork. In Work Together Anywhere, Lisette Sutherland, an international champion of virtual-team strategies, offers a complete blueprint for optimizing team success by supporting every member of every team, including: • Employees advocating for work-from-home options • Managers seeking to maximize productivity and profitability • Teams collaborating over complex projects and long-term goals • Organizations reliant on sharing confidential documents and data • Company owners striving to save money and attract the best brainpower Packed with hands-on materials and actionable advice for cultivating agility, camaraderie, and collaboration, Work Together Anywhere is a thorough and inspiring must-have guide for getting ahead in today’s remote-working world.

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

A revised and updated edition of the best-selling guide for schools implementing PBIS Tier 1 PBIS (positive behavior interventions and supports) is the most important tool educators have to deal with disruptive student behaviors. This revised and updated handbook provides detailed guidelines for implementing and sustaining PBIS for schools and teams. New in this edition is a chapter addressing inequity and bias in behavior referrals and discipline; a tiered fidelity inventory (TFI) to evaluate adherence to PBIS practices; different methods of data collection; and new research on sustainability. Positive school climates are not achieved through expulsions, suspensions, or detentions, but instead through collective analysis and data-driven decision-making. Downloadable digital content offers a PDF presentation to aid staff buy-in and customizable forms to help manage data and assess progress with ease.

"... a curriculum geared toward helping students gain skills in consciously regulating their actions, which in turn leads to increased control and problem solving abilities. Using a cognitive behavior approach, the curriculum's learning activities are designed to help students recognize when they are in different states called "zones," with each of four zones represented by a different color. In the activities, students also learn how to use strategies or tools to stay in a zone or move from one to another. Students explore calming techniques, cognitive strategies, and sensory supports so they will have a toolbox of methods to use to move between zones. To deepen students' understanding of how to self-regulate, the lessons set out to teach students these skills: how to read others' facial expressions and recognize a broader range of emotions, perspective about how others see and react to their behavior, insight into events that trigger their less regulated states, and when and how to use tools and problem solving skills. The curriculum's learning activities are presented in 18 lessons. To reinforce the concepts being taught, each lesson includes probing questions to discuss and instructions for one or more learning activities. Many lessons offer extension activities and ways to adapt the activity for individual student needs. The curriculum also includes worksheets, other handouts, and visuals to display and share. These can be photocopied from this book or printed from the accompanying CD."--Publisher's website.

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.

The way autoimmune disease is viewed and treated is undergoing a major change as an estimated 50 million Americans (and growing) suffer from these conditions. For many patients, the key to true wellness is in holistic treatment, although they might not know how to begin their journey to total recovery. The Autoimmune Wellness Handbook, from Mickey Trescott and Angie Alt of Autoimmune-Paleo.com, is a comprehensive guide to living healthfully with autoimmune disease. While conventional medicine is limited to medication or even surgical fixes, Trescott and Alt introduce a complementary solution that focuses on seven key steps to recovery: inform, collaborate, nourish, rest, breathe, move, and connect. Each step demystifies the process to reclaim total mind and body health. With five autoimmune conditions between them, Trescott and Alt have achieved astounding results using the premises laid out in the book. The Autoimmune Wellness Handbook goes well beyond nutrition and provides the missing link so that you can get back to living a vibrant, healthy life.

Veterinary medicine is a dynamic field allowing team members growthin every aspect of the science and profession. In a single day, ateam member may be involved in administrative, emergency andcritical care, internal medicine, surgical and radiological teams.With increasing expectations of quality care and technology, teammembers’ knowledge and responsibilities are growing at anexponential rate. The Veterinary Medical Team Handbook is designed as atraining resource for veterinarians, technicians and staff.Coverage ranges from administrative tasks and client communicationto common diseases, disorders and procedures. The aim is toincrease the staff's ability to detect and manage health problemsand to enable the team to be more effective communicators with eachother and with clients. Two accompanying CD-ROMs contain trainingmodules and interactive case studies for further learning andpractice. A valuable training guide for veterinary practices andhospitals. Designed for easy reference with abundant bullet points,algorithms, lists and key point boxes. Covers common diseases, disorders and procedures, as well asadministrative tasks and client communication. Includes two CD-ROMs with training modules and interactive casestudies.

This handbook is the practical guide to becoming a great manager. It covers all the major topics including hiring, coaching, feedback, one-on-ones, and decision making. It also covers some of softer, but equally important, topics like conflict resolution and mental health. Great management changes lives. In fact, it's one of the most single overlooked pieces of leverage in the world. Great managers are remembered like great teachers, inspirations who help others soar. That's why it's such a shame management training is so often overlooked. Successful individual-contributors are rewarded with a 'promotion' into management and then, more often

than not, left to sink or swim. If you're a new manager, this book will shine a friendly light on the road ahead. And if you're an old dog, perhaps it'll teach you a trick or two. This handbook was written by Alex MacCaw and stress-tested at a company called Clearbit.

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 · 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

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.

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 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!

This book is a comprehensive resource book that provides everything you need to know to create high performing teams.

Published by OpenStax College, U.S. History covers the breadth of the chronological history of the United States and also provides the necessary depth to ensure the course is manageable for instructors and students alike. U.S. History is designed to meet the scope and sequence requirements of most courses. The authors introduce key forces and major developments that together form the American experience, with particular attention paid to considering issues of race, class and gender. The text provides a balanced approach to U.S. history, considering the people, events and ideas that have shaped the United States from both the top down (politics, economics, diplomacy) and bottom up (eyewitness accounts, lived experience).

This is a 'how to' book on project management, quality and problem solving using teams. Table of contents: * Doing business in a new business world * The basics of quality improvement (improvement concepts, tools of the scientific approaches and tools for making team decisions) * Setting the stage for a successful project (selecting members) * Getting underway (guidelines for productive meetings, record keeping, goal setting, preparing for and conducting the first meeting,

evaluation) * Building an improvement plan (five crucial improvement activities, project planning and improvement strategies) * Learning to work together (team dynamics, roller coaster rides, recipe for a successful team, common problem solving * Team building activities (14 activities and 10 team building exercises) * Appendix: the planning grid.

In a futuristic military adventure a recruit goes through the roughest boot camp in the universe and into battle with the Terran Mobile Infantry in what historians would come to call the First Interstellar War

Worship in an interactive way! This down-to-earth guide will help your worship team work together to lead others in praise by discussing key elements from music to drama and showing you how to worship interactively as an authentic leader. Edited by Allison Siewert.

Your Road Map to Teamwork Success in any Entrepreneurial Company Making the shift from a large organization to a smaller entrepreneurial company seems like a dream come true for many. But the transition from a rigid environment to a more fluid one that focuses on relationships and the value each employee brings means a change in mindset. While working with Strategic Coach(R) Program team members, Shannon Waller saw these challenges first hand. Using her experience in creating successful entrepreneurial companies, she created a collection of teamwork strategies. By adopting these 12 Entrepreneurial Attitudes, team members can become increasingly valuable to their organization and transform their "job" into a source of endlessly expanding personal growth and meaningful rewards. This guidebook will help you: - Recognize your Unique Ability(R) and learn how to integrate it in life and work. - Develop and maintain an Entrepreneurial Attitude. - Maximize personal contributions and professional rewards. - Lose your fear of sharing insights and ideas with the company. - Begin to live in the Results Economy, not the Time-and-Effort Economy. - Build and maintain the trust of Entrepreneur. - Experience functioning as the Entrepreneur's valued partner. - Exchange personal perfectionism for company-wide collaboration. - Become a highly effective communicator by learning how to share information the way others need to receive it and receive it the way others share it. - Achieve new levels of patience, compassion, and perseverance. Experience a new level of Team Success, starting today!