The Red Team Handbook The Armys Guide To Making Better Decisions

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**

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!

#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.

Although communities feel magical, they don't come together by magic. Get Together is a guide to cultivating a community-people who come together over what they care about. Whether starting a run crew, helping online streamers connect with fans, or sparking a movement of K-12 teachers, the secret to community-building is the same: don't fixate on what you can do for people (or what they can do for you). Instead, focus on what you can do with them. In Get Together, the People & Company team provides stories, prompts, and principles for each stage of cultivating a passionate group of people. Every organization holds the potential to build and sustain a thriving community. Get Together shows readers how companies and customers, artist and fans, or organizers and advocates, can join forces to accomplish more together than they could have alone.

AI is radically transforming business. Are you ready? Look around you. Artificial intelligence is no longer just a futuristic notion. It's here right now--in software that senses what we need, supply chains that "think" in real time, and robots that respond to changes in their environment. Twenty-first-century pioneer companies are already using AI to innovate and grow fast. The bottom line is this: Businesses that understand how to harness AI can surge ahead. Those that neglect it will fall behind. Which side are you on? In Human + Machine, Accenture leaders Paul R. Daugherty and H. James (Jim) Wilson show that the essence of the AI paradigm shift is the transformation of all business processes within an organization--whether related to breakthrough innovation, everyday customer service, or personal productivity habits. As humans and smart machines collaborate ever more closely, work processes become more fluid and adaptive, enabling companies to change them on the fly--or to completely reimagine them. AI is changing all the rules of how companies operate. Based on the authors' experience and research with 1,500 organizations, the book reveals how companies are using the new rules of AI to leap ahead on innovation and profitability, as well as what you can do to achieve similar results. It describes six entirely new types of hybrid human + machine roles that every company must develop, and it includes a "leader's guide" with the five crucial principles required to become an AI-fueled business. Human + Machine provides the missing and much-needed management playbook for success in our new age of AI. BOOK PROCEEDS FOR THE AI GENERATION The authors' goal in publishing Human + Machine is to help executives, workers, students and others navigate the changes that AI is making to business and the economy. They believe AI will bring innovations that truly improve the way the world works and lives. However, AI will cause disruption, and many people will need education, training and support to prepare for the newly created jobs. To support this need, the authors are donating the royalties received from the sale of this book to fund education and retraining programs focused on developing fusion skills for the age of artificial intelligence.

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

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 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.

The Antifascist Handbook
Incident Response Edition: a Condensed Field Guide for the Cyber Security Incident Responder
Human + Machine
Employee Food Safety Handbook
Antifa
Cybersecurity Blue Team Toolkit
The Practice of Network Security Monitoring
A Practical Guide
Red Team Development and Operations
The Cyber Intelligence Handbook
A practical guide to mastering Red Team operations
Defensive Security Handbook
The DevOps Handbook:
An Authoritative Guide for the C-Suite, IT Staff, and Intelligence Team

Best Practices for Security Operations Centers (SOC), written by an experienced practitioner.

Lead your organization into the 21st century with the help of this groundbreaking book that is already creating a stir in corporate boardrooms across America! In a book that does for managers what his mega-bestseller, The Team Handbook, did for teams, Peter Scholtes, who is widely acknowledged as one of the most influential Quality leaders of the decade, shows the real root of management problems. Learn how to stop blaming your workers and start changing the systems with the help of activities and exercises that enable you to immediately begin implementing breakthrough improvements in all your work processes!

Discusses the different types of computer viruses and how they work, recommends preventive measures to take and those to avoid and suggests ways to handle a virus once it occurs, and provides information on a variety of anti-virus programs

Our nation's greatest assets - our Soldiers - face a dynamic, competitive, and lethal operational environment (OE) that has evolved in recent years, one in which our adversaries will employ a mix of traditional, unconventional, and hybrid strategies. Our Army's physical readiness program must evolve to keep pace with the demands of modern war - our physical fitness test must evolve as well. Based on results of years of scientific study, the Secretary and Chief of Staff of the Army have directed replacement of the Army Physical Fitness Test (APFT). While the legacy APFT is an acceptable test for measuring general fitness, it does not adequately assess the domains of combat physical fitness. The six-event Army Combat Fitness Test (ACFT) was developed to better predict a Soldier's readiness for the demands of the modern battlefield. Like combat, the ACFT is both age and gender neutral. The desired end-states of ACFT implementation are an increase in physical readiness...

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.

Following the narrative of the popular video game series, a companion book, which resembles a collection of Abstergo case files, provides a glimpse into the inner-workings of the fictional corporation through data, schematics and artifacts.

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.

Network security is not simply about building impenetrable walls—determined attackers will eventually overcome traditional defenses. The most effective computer security strategies integrate network security monitoring (NSM): the collection and analysis of data to help you detect and respond to intrusions. In The Practice of Network Security Monitoring, Mandiant CSO Richard Bejtlich shows you how to use NSM to add a robust layer of protection around your networks—no prior experience required. To help you avoid costly and inflexible solutions, he teaches you how to deploy, build, and run an NSM operation using open source software and vendor-neutral tools. You'll learn how to: —Determine where to deploy NSM platforms, and size them for the monitored networks —Deploy stand-alone or distributed NSM installations —Use command line and graphical packet analysis tools, and NSM consoles —Interpret network evidence from server-side and client-side intrusions —Integrate threat intelligence into NSM software to identify sophisticated adversaries There's no foolproof way to keep attackers out of your network. But when they get in, you'll be prepared. The Practice of Network Security Monitoring will show you how to build a security net to detect, contain, and control them. Attacks are inevitable, but losing sensitive data shouldn't be.

The Leader's Handbook: Making Things Happen, Getting Things Done
An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage
Soc, Siem, and Threat Hunting Use Cases: A Condensed Field Guide for the Security Operations Team
Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1. 02)
A Path to Profits, Passion, and Purpose
How to Build a Community with Your People. E
Tribe of Hackers Blue Team
Red Team + OSINT + Blue Team Reference
How to Create World-Class Agility, Reliability, and Security in Technology Organizations
Rtfm
Tribal Knowledge from the Best in Defensive Cybersecurity
Operator Handbook
How to Succeed By Thinking Like the Enemy

Increase profitability, elevate work culture, and exceed productivity goals through DevOps practices. More than ever, the effective management of technology is critical for business competitiveness. For decades, technology leaders have struggled to balance agility, reliability, and security. The consequences of failure have never been greater?whether it's the healthcare.gov debacle, cardholder data breaches, or missing the boat with Big Data in the cloud. And yet, high performers using DevOps principles, such as Google, Amazon, Facebook, Etsy, and Netflix, are routinely and reliably deploying code into production hundreds, or even thousands, of times per day. Following in the footsteps of The Phoenix Project, The DevOps Handbook shows leaders how to replicate these incredible outcomes, by showing how to integrate Product Management, Development, QA, IT Operations, and Information Security to elevate your company and win in the marketplace.

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.

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.

Chief of Staff of the U.S. Army General Mark A. Milley repeatedly warns of increased complexity, ambiguity, and speed in future warfare. The decision-making process at all levels of command will be challenged by the environment, the situation, and the enemy, as well as by the perception and interpretation of our thoughts. The requirement to frame decisions around the scope and rate of information sharing on the modern battlefield and adapting those frames to the complexity of context and content, necessitates the ability to think critically and creatively. The curriculum at the University of Foreign Military and Cultural Studies (UFMCS) directly addresses these challenges by training and preparing students to operate as a Red Teamer. Red Teaming creates and illuminates pathways to better decisions by employing structured techniques to identify hidden dangers, reveal unseen possibilities, and facilitate creative alternatives. It is, in essence, a form of risk management for the human brain. The U.S. Army chartered UFMCS with the mission to teach Red Teaming to the U.S. Army and other authorized organizations. As the nature of warfare has evolved, so too has our curriculum and academic offerings. Version 9.0 of the Red Team Handbook represents the current state of our program. Although the contents of this volume and our courses are not official doctrine, the practices discussed directly support and are in both Joint and U.S. Army Doctrine. This handbook provides the reader with an introduction to the fundamental concepts, methods, and tools essential to the practice of U.S. Army Red Teaming.

Like American business executives, many government leaders realize that a continuation of the traditional management of objectives approach will achieve failure. Those willing to change are searching for a new approach to managing government. The authors of Teams in Government believe the best approach is Total Quality Management (TQM). Why TQM? Because it consists of gradual, unending improvement activities that involve every person in the organization in a totally integrated effort to improve performance and quality at every level and to increase customer satisfaction. The government has two types of customers-the person who receives the benefits of its services and the taxpayer who supplies the money to fuel an efficient and effective operation. If you are looking for the tools and techniques that will enable you to deliver government services that not only meet but exceed the expectations of your customers, to do it right the first time, you need Teams in Government. Any government organization that wants to switch from focusing solely upon meeting the needs of the bureaucracy (primarily on meeting objectives and quotas designed by the upper echelon), who are furthest from your customers, will find TQM to be extremely effective.

Develop your red team skills by learning essential foundational tactics, techniques, and procedures, and boost the overall security posture of your organization by leveraging the homefield advantage Key Features Build, manage, and measure an offensive red team program Leverage the homefield advantage to stay ahead of your adversaries Understand core adversarial tactics and techniques, and protect pentesters and pentesting assets Book Description It's now more important than ever for organizations to be ready to detect and respond to security events and breaches. Preventive measures alone are not enough for dealing with adversaries. A well-rounded prevention, detection, and response program is required. This book will guide you through the stages of building a red team program, including strategies and homefield advantage opportunities to boost security. The book starts by guiding you through establishing, managing, and measuring a red team program, including effective ways for sharing results and findings to raise awareness. Gradually, you'll learn about progressive operations such as cryptocurrency mining, focused privacy testing, targeting telemetry, and even blue team tooling. Later, you'll discover knowledge graphs and how to build them, then become well-versed with basic to advanced techniques related to hunting for credentials, and learn to automate Microsoft Office and browsers to your advantage. Finally, you'll get to grips with protecting assets using decoys, auditing, and alerting with examples for major operating systems. By the end of this book, you'll have learned how to build, manage, and measure a red team program effectively and be well-versed with the fundamental operational techniques required to enhance your existing skills. What you will learn Understand the risks associated with security breaches Implement strategies for building an effective penetration testing team Map out the homefield using knowledge graphs Hunt credentials using indexing and other practical techniques Gain blue team tooling insights to enhance your red team skills Communicate results and influence decision makers with appropriate data Who this book is for This is one of the few detailed cybersecurity books for penetration testers, cybersecurity analysts, security leaders and strategists, as well as red team members and chief information security officers (CISOs) looking to secure their organizations from adversaries. The program management part of this book will also be useful for beginners in the cybersecurity domain. To get the most out of this book, some penetration testing experience, and software engineering and debugging skills are necessary.

The Handbook of Fraud Deterrence encompasses the applicable professional standards and common applications for forensic accounting, fraud deterrence, and fraud investigation services. It is the first book that explains fraud deterrence through internal control improvement within the structure of forensic accounting procedures.

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.

Training Circular (TC) 3-21.76 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which TC 3-21.76 is the proponent publication (the authority) are italicized in the text and are marked with an asterisk (*) in the glossary. Terms and definitions for which TC 3-21.76 is the proponent publication are boldfaced in the text. For other definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition. The principal audience for TC 3-21.76 are U.S. Army Rangers and combat arms units. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army will also use this publication.

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.

Fairy Haven's newest arrival, Prilla, along with Rani and Vidia, embarks on a journey filled with danger, sacrifice, and adventure. The fate of Never Land rests on their shoulders.

Experts describe the latest research in a rapidly growing multidisciplinary field, the study of groups of individuals acting collectively in ways that seem intelligent. Intelligence does not arise only in individual brains; it also arises in groups of individuals. This is collective intelligence: groups of individuals acting collectively in ways that seem intelligent. In recent years, a new kind of collective intelligence has emerged: interconnected groups of people and computers, collectively doing intelligent things. Today these groups are engaged in tasks that range from writing software to predicting the results of presidential elections. This volume reports on the latest research in the study of collective intelligence, laying out a shared set of research challenges from a variety of disciplinary and methodological perspectives. Taken together, these essays—by leading researchers from such fields as computer science, biology, economics, and psychology—lay the foundation for a new multidisciplinary field. Each essay describes the work on collective intelligence in a particular discipline—for example, economics and the study of markets; biology and research on emergent behavior in ant colonies; human-computer interaction and artificial intelligence; and cognitive psychology and the "wisdom of crowds" effect. Other areas in social science covered include social psychology, organizational theory, law, and communications. Contributors Eytan Adar, Ishani Aggarwal, Yochai Benkler, Michael S. Bernstein, Jeffrey P. Bigham, Jonathan Bragg, Deborah M. Gordon, Benjamin Mako Hill, Christopher H. Lin, Andrew W. Lo, Thomas W. Malone, Mausam, Brent Miller, Aaron Shaw, Mark Steyvers, Daniel S. Weld, Anita Williams Woolley

The U.S. Army chartered the University of Foreign Military and Cultural Studies (UFMCS) with the mission to teach Red Teaming to the U.S. Army and other authorized organizations. As the nature of warfare has evolved, so too has our curriculum and academic offerings. Version 9.0 of the Red Team Handbook represents the current state of our program. Although the contents of this volume and our courses are not official doctrine, the practices discussed directly support and are in both Joint and U.S. Army Doctrine. This handbook provides the reader with an introduction to the fundamental concepts, methods, and tools essential to the practice of U.S. Army Red Teaming.Applied Critical Thinking (ACT), provides an improved understanding of our own decision-making processes, as well as the ability to deconstruct arguments and better understand others. It helps identify assumptions, biases, and can allow us to restate ideas using an analogy to describe complex ideas more simply. Perhaps most importantly, it allows us to generate and evaluate alternatives, thereby increasing our chances of finding the path to success. ACT incorporates several fundamentals, including slowing down, asking why, seeking alternatives, and other more-advanced strategies.This compilation includes a reproduction of the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community.Chapter 1 - Introduction * Why Do We Red Team? * What is Red Teaming? * Four Principles of UFMCS * UFMCS Training * Chapter 2 - Self-Awareness And Reflection * Self-Authorship * Temperament * Emotional Intelligence * Interpersonal Communication * Interpersonal Conflict * Introspection * Chapter 3 - Fostering Cultural Empathy * Understanding Culture for the Red Teamer * Ethnocentrism * Some Cultural Definitions * Some Cultural Frameworks * Cultural Analysis For The Red Teamer * Functional Systems Approach * Cultural Relevance * Chapter 4 - Applied Critical Thinking * What is Applied Critical Thinking? * The Time Factor * Time For Red Teaming * Creating Space And Time * Summary * Chapter 5 - Groupthink Mitigation And Decision Support * Group Dynamics And Groupthink * Groupthink Mitigation * Decision Support * Chapter 6 - Thinking Creatively * The Creative

Thought Process * Stage 1: Problem-Finding * Stage 2: Preparation * Stage 3: Ideation * Stage 4: Idea Verification * Stage 5: Communication * Summary * Chapter 7 - Red Teaming Tools, Techniques, & Practices * Tools * A Technique: The Ideal Group Process * Practices * 1-2-4-Whole Group * 1 on 1, 2 on 2, Exchange Emissaries * 4 Ways of Seeing * 5 Whys * 5 Will Get You 25 * 6 Empathetic Questions * 6 Words * Alternative Futures Analysis * Analogy Suitability Analysis * Analysis Of Competing Hypotheses * Appreciative Interview * Argument Deconstruction * Assumption Sensitivity Analysis * Batna * Brainstorming * Circle Of Voices * Circular Response * Critical Variables * Cultural Perception Framework * Deception Detection * Devil's Advocacy * Divergence - Convergence * Dot Voting * Fishbowl * Frame Audit * Gallery Walk * High Impact / Low Probability Analysis * Indicators Or Signposts Of Change * Key Assumptions Check * Mind Mapping * My 15% * Onion Model * Outside-In Thinking * Premortem Analysis * Problem Restatement * Shifting the Burden * Stakeholder Mapping. * State-Elaborate-Exemplify-Illustrate (SEE-I) * Storytelling * String of Pearls * S-W-O-T Analysis * Team A / Team B Analysis * Think-Write-Share * TRIZ * Troika Consulting (Ad Agency) * What If Analysis * Who Am I? * Yes, And This handbook is an unclassified living document and regularly evolves to incorporate new ideas, approaches, and tools. It should provide a compendium of ideas from UFMCS curriculum and serve as both a reference for our graduates and a broad introduction to others.

Seize the initiative from cyber-threat actors by applying cyber intelligence to create threat-driven cybersecurity operations! Written by an intelligence professional with 40 years of experience applying intelligence to counter threats from a wide range of determined adversaries, this book provides common sense practices for establishing and growing responsive cyber intelligence capabilities customized to organization needs, regardless of size or industry. Readers will learn: -What cyber intelligence is and how to apply it to deter, detect, and defeat malicious cyber-threat actors targeting your networks and data;-How to characterize threats and threat actors with precision to enable all relevant stakeholders to contribute to desired security outcomes;-A three-step planning approach that allows cyber intelligence customers to define and prioritize their needs;-How to construct a simplified cyber intelligence process that distills decades of national-level intelligence community doctrine into a sets of clearly defined, mutually supporting actions that will produce repeatable and measureable results from the outset;-How to employ advanced analytic frameworks to apply intelligence as an operational function that can inform security design and execution to complicate actions for would be attackers.

Your one-stop guide to learning and implementing Red Team tactics effectively Key Features Target a complex enterprise environment in a Red Team activity Detect threats and respond to them with a real-world cyber-attack simulation Explore advanced penetration testing tools and techniques Book Description Red Teaming is used to enhance security by performing simulated attacks on an organization in order to detect network and system vulnerabilities. Hands-On Red Team Tactics starts with an overview of pentesting and Red Teaming, before giving you an introduction to few of the latest pentesting tools. We will then move on to exploring Metasploit and getting to grips with Armitage. Once you have studied the fundamentals, you will learn how to use Cobalt Strike and how to set up its team server. The book introduces some common lesser known techniques for pivoting and how to pivot over SSH, before using Cobalt Strike to pivot. This comprehensive guide demonstrates advanced methods of post-exploitation using Cobalt Strike and introduces you to Command and Control (C2) servers and redirectors. All this will help you achieve persistence using beacons and data exfiltration, and will also give you the chance to run through the methodology to use Red Team activity tools such as Empire during a Red Team activity on Active Directory and Domain Controller. In addition to this, you will explore maintaining persistent access, staying untraceable, and getting reverse connections over different C2 covert channels. By the end of this book, you will have learned about advanced penetration testing tools, techniques to get reverse shells over encrypted channels, and processes for post-exploitation. What you will learn Get started with red team engagements using lesser-known methods Explore intermediate and advanced levels of post-exploitation techniques Get acquainted with all the tools and frameworks included in the Metasploit framework Discover the art of getting stealthy access to systems via Red Teaming Understand the concept of redirectors to add further anonymity to your C2 Get to grips with different uncommon techniques for data exfiltration Who this book is for Hands-On Red Team Tactics is for you if you are an IT professional, pentester, security consultant, or ethical hacker interested in the IT security domain and wants to go beyond Penetration Testing. Prior knowledge of penetration testing is beneficial.

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.

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

Analyzing how hacks are done, so as to stop them in thefuture Reverse engineering is the process of analyzing hardware orsoftware and understanding it, without having access to the sourcecode or design documents. Hackers are able to reverse engineersystems and exploit what they find with scary results. Now the goodguys can use the same tools to thwart these threats. PracticalReverse Engineering goes under the hood of reverse engineeringfor security analysts, security engineers, and system programmers,so they can learn how to use these same processes to stop hackersin their tracks. The book covers x86, x64, and ARM (the first book to cover allthree); Windows kernel-mode code rootkits and drivers; virtualmachine protection techniques; and much more. Best of all, itoffers a systematic approach to the material, with plenty ofhands-on exercises and real-world examples. Offers a systematic approach to understanding reverseengineering, with hands-on exercises and real-world examples Covers x86, x64, and advanced RISC machine (ARM) architecturesas well as deobfuscation and virtual machine protectiontechniques Provides special coverage of Windows kernel-mode code(rootkits/drivers), a topic not often covered elsewhere, andexplains how to analyze drivers step by step Demystifies topics that have a steep learning curve Includes a bonus chapter on reverse engineering tools Practical Reverse Engineering: Using x86, x64, ARM, WindowsKernel, and Reversing Tools provides crucial, up-to-dateguidance for a broad range of IT professionals.

Why Red Teaming? The premise of the program at the University of Foreign Military and Cultural Studies (UFMCS) is that people and organizations court failure in predictable ways, that they do so by degrees, almost imperceptibly, and that they do so according to their mindsets, biases, and experience, which are formed in large part by their own culture and context. The sources of these failures are simple, observable, and lamentably, often repeated. They are also preventable, and that is the point of 'red teaming'. Our methods and education involve more than Socratic discussion and brainstorming. We believe that good decision processes are essential to good outcomes. To that end, our curriculum is rich in divergent processes, red teaming tools, and liberating structures, all aimed at decision support. We educate people to develop a disposition of curiosity, and help them become aware of biases and behavior that prevent them from real positive change in the ways they seek solutions and engage others. We borrow techniques, methods, frameworks, concepts, and best practices from several sources and disciplines to create an education, and practical applications, that we find to be the best safeguard against individual and organizational tendencies toward biases, errors in cognition, and groupthink. Red teaming is diagnostic, preventative, and corrective; yet it is neither predictive or a solution. Our goal is to be better prepared and less surprised in dealing with complexity. What is Red Teaming? Red teaming is a function that provides commanders an independent capability to fully explore alternatives in plans, operations, concepts, organizations and capabilities in the context of the operational environment (OE) and from the perspectives of partners, adversaries and others. A Red Team performs three general types of tasks: - Support to operations, planning, and decision support - Critical review and analysis of already-existing plans - Intelligence support (Threat Emulation) (UFMCS provides education for the first two tasks; TRADOC's Intelligence School and Center provides education on the third.) In order for a Red Team to effectively contribute to decision making all of the following elements are required: The ability to think critically about the problem. While this may seem obvious, the reality is that critical thinking is a skill set that requires training, education and tools. The Army assimilates people from different backgrounds across the nation. One of the drawbacks of that assimilation is our military tendency to reflect the same biases and perspectives. We pride ourselves in common values—which while ingrained in the Army culture are not universal outside of that culture. Thinking critically and challenging the group is an unnatural act for military staffs. Doing so effectively requires tools and methods that enable leaders to see different perspectives. Red Teams require top cover to be allowed to challenge the conventional wisdom and the organization's leaders. No matter the quality of the Red Team or the methods they employ, dictatorial or toxic leaders are incompatible with successful red teaming. Red teaming is not easy, and not everyone can do it. Red Teamers must be effective written and oral communicators. They must have credibility in the area in which they are providing red teaming insights. They must be able to constructively challenge the plan. This means focusing on what is truly important, able to explain why it is being challenged and offering some alternative ways to think about the problem.

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.

The National Bestseller "Focused and persuasive... Bray's book is many things: the first English-language transnational history of antifa, a how-to for would-be activists, and a record of advice from anti-Fascist organizers past and present."—THE NEW YORKER "Insurgent activist movements need spokesmen, intellectuals and apologists, and for the moment Mark Bray is filling in as all three... The book's most enlightening contribution is on the history of anti-fascist efforts over the past century, but its most relevant for today is its justification for stifling speech and clobbering white supremacists."—Carlos Lozada, THE WASHINGTON POST "[Bray's] analysis is methodical, and clearly informed by both his historical training and 15 years of organizing, which included Occupy Wall Street...Antifa: The Anti-Fascist Handbook couldn't have emerged at a more opportune time. Bray's arguments are incisive and cohesive, and his consistent refusal to back down from principle makes the book a crucial intervention in our political moment."—SAN FRANCISCO CHRONICLE In the wake of tragic events in Charlottesville, VA, and Donald Trump's initial refusal to denounce the white nationalists behind it all, the "antifa" opposition movement is suddenly appearing everywhere. But what is it, precisely? And where did it come from? As long as there has been fascism, there has been anti-fascism — also known as "antifa." Born out of resistance to Mussolini and Hitler in Europe during the 1920s and '30s, the antifa movement has suddenly burst into the headlines amidst opposition to the Trump administration and the alt-right. They could be seen in news reports, often clad all in black with balaclavas covering their faces, demonstrating at the presidential inauguration, and on California college campuses protesting far-right speakers, and most recently, on the streets of Charlottesville, VA, protecting, among others, a group of ministers including Cornel West from neo-Nazi violence. (West would later tell reporters, "The anti-fascists saved our lives.") Simply, antifa aims to deny fascists the opportunity to promote their oppressive politics, and to protect tolerant communities from acts of violence promulgated by fascists. Critics say shutting down political adversaries is anti-democratic; antifa adherents argue that the horrors of fascism must never be allowed the slightest chance to triumph again. In a smart and gripping investigation, historian and former Occupy Wall Street organizer Mark Bray provides a detailed survey of the full history of anti-fascism from its origins to the present day — the first transnational history of postwar anti-fascism in English. Based on interviews with anti-fascists from around the world, Antifa details the tactics of the movement and the philosophy behind it, offering insight into the growing but little-understood resistance fighting back against fascism in all its guises.

This is a book about the big questions in life: knowledge, consciousness, fate, God, truth, goodness, justice. It is for anyone who believes there are big questions out there, but does not know how to approach them. Think sets out to explain what they are and why they are important. Simon Blackburn begins by putting forward a convincing case for the study of philosophy and goes on to give the reader a sense of how the great historical figures such as Descartes, Hume, Kant, and Wittgenstein have approached its central themes. Each chapter explains a major issue, and gives the reader a self-contained guide through the problems that philosophers have studied. The large scope of topics covered range from scepticism, the self, mond and body, and freedom to ethics and the arguments surrounding the existence of God. Lively and approachable, this book is ideal for all those who want to learn how the basic techniques of thinking shape our existence.