Intelligence Driven Incident Response Outwitting The Adversary

Intelligence-Driven Incident ResponseOutwitting the Adversary"O'Reilly Media, Inc."
You already have the tools to make a threat intel program! With the growing number of threats against companies, threat intelligence is becoming a business essential. This book will explore steps facts and myths on how to effectively formalize and improve the intel program at your company by:* Separating good and bad intelligence* Creating a threat intelligence maturity model* Quantifying threat risk to your organization* How to build and structure a threat intel team* Ways to build intel talent from withinWith a wider array of information freely available to the public you do not want to be caught without an understanding of the threats to your company. Explore some ideas to help formalize the efforts to create a safer environment for employees and clients.
This book is written for the first security hire in an organization, either an individual moving into this role from within the organization or hired into the role. More and more, organizations are realizing that information security requires a dedicated team with leadership distinct from information technology, and often the people who are placed into those positions have no idea where to start or how to prioritize. There are many issues competing for their attention, standards that say do this or do that, laws, regulations, customer demands, and no guidance on what is actually effective. This book offers guidance on approaches that work for how you prioritize and build a comprehensive information security program that protects your organization. While most books targeted at information security professionals explore specific subjects with deep expertise, this book explores the depth and breadth of the field. Instead of exploring a technology such as cloud security or a technique such as risk analysis, this book places those into the larger context of how to meet an organization's needs, how to prioritize, and what success looks like. Guides to the maturation of practice are offered, along with pointers for each topic on where to go for an in-depth exploration of each topic. Unlike more typical books on information security that advocate a single perspective, this book explores competing perspectives with an eye to providing the pros and cons of the different approaches and the implications of choices on implementation and on maturity, as often a choice on an approach needs to change as an organization grows and matures.
Elastic security offers enhanced threat hunting capabilities to build active defense strategies. Complete with practical examples and tips, this easy-to-follow guide will help you enhance your security skills by leveraging the Elastic Stack for security monitoring, incident response, intelligence analysis, or threat hunting.
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.
Protect Your Organization Against Massive Data Breaches and Their Consequences Data breaches can be catastrophic, but they remain mysterious because victims don’t want to talk about them. In Data Breaches, world-renowned cybersecurity expert Sherri Davidoff shines a light on these events, offering practical guidance for reducing risk and mitigating consequences. Reflecting extensive personal experience and lessons from the world’s most damaging breaches, Davidoff identifies proven tactics for reducing damage caused by breaches and avoiding common mistakes that cause them to spiral out of control. You’ll learn how to manage data breaches as the true crises they are; minimize reputational damage and legal exposure; address unique challenges associated with health and payment card data; respond to hacktivism, ransomware, and cyber extortion; and prepare for the emerging battlefront of cloud-based breaches. Understand what you need to know about data breaches, the dark web, and markets for stolen data Limit damage by going beyond conventional incident response Navigate high-risk payment card breaches in the context of PCI DSS Assess and mitigate data breach risks associated with vendors and third-party suppliers Manage compliance requirements associated with healthcare and HIPAA Quickly respond to ransomware and data exposure cases Make better decisions about cyber insurance and maximize the value of your policy Reduce cloud risks and properly prepare for cloud-based data breaches Data Breaches is indispensable for everyone involved in breach avoidance or response: executives, managers, IT staff, consultants, investigators, students, and more. Read it before a breach happens! Register your book for convenient access to downloads, updates, and/or corrections as they become available. See inside book for details.
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
"Drawing upon a wealth of experience from academia, industry, and government service, this book details and dissects current organizational cybersecurity policy issues on a global scale. Using simple language, it includes a thorough description of each issue, lists pros and cons, documents policy alternatives for the sake of clarity with respect to policy alone, and dives into organizational implementation issues. It also equips the reader with descriptions of the impact of specific policy choices, both positive and negative. This book gives students, scholars, and technical decision-makers the necessary knowledge of cybersecurity policy in order to make more informed decisions"--Provided by publisher.
The only security book to be chosen as a Dr. Dobbs Jolt Award Finalist since Bruce Schneier's Secrets and Lies and Applied Cryptography! Adam Shostack is responsible for security development lifecycle threat modeling at Microsoft and is one of a handful of threat modeling experts in the world. Now, he is sharing his considerable expertise into this unique book. With pages of specific actionable advice, he details how to build better security into the design of systems, software, or services from the outset. You'll explore various threat modeling approaches, find out how to test your designs against threats, and learn effective ways to address threats that have been validated at Microsoft and other top companies. Systems security managers, you'll find tools and a framework for structured thinking about what can go wrong. Software developers, you'll appreciate the jargon-free and accessible

introduction to this essential skill. Security professionals, you'll learn to discern changing threats and discover the easiest ways to adopt a structured approach to threat modeling. Provides a unique how-to for security and software developers who need to design secure products and systems and test their designs Explains how to threat model and explores various threat modeling approaches, such as asset-centric, attacker-centric and software-centric Provides effective approaches and techniques that have been proven at Microsoft and elsewhere Offers actionable how-to advice not tied to any specific software, operating system, or programming language Authored by a Microsoft professional who is one of the most prominent threat modeling experts in the world As more software is delivered on the Internet or operates on Internet-connected devices, the design of secure software is absolutely critical. Make sure you're ready with Threat Modeling: Designing for Security.

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

Threat Intelligence is a topic that has captivated the cybersecurity industry. Yet, the topic can be complex and quickly skewed. Author Robert M. Lee and illustrator Jeff Haas created this book to take a lighthearted look at the threat intelligence community and explain the concepts to analysts in a children's book format that is age-appropriate for all.Threat Intelligence and Me is the second work by Robert and Jeff who previously created SCADA and Me: A Book for Children and Management. Their previous work has been read by tens of thousands in the security community and beyond including foreign heads of state. Threat Intelligence and Me promises to reach an even wider audience while remaining easy-to-consume and humorous.

React Hooks in Action teaches you to write fast and reusable React components using Hooks. Summary Build stylish, slick, and speedy-to-load user interfaces in React without writing custom classes. React Hooks are a new category of functions that help you to manage state, lifecycle, and side effects within functional components. React Hooks in Action teaches you to use pre-built hooks like useState, useReducer and useEffect to build your own hooks. Your code will be more reusable, require less boilerplate, and you'll instantly be a more effective React developer. About the technology Get started with React Hooks and you'll soon have code that's better organized and easier to maintain. React Hooks are targeted JavaScript functions that let you reuse and share functionality across components. Use them to split components into smaller functions, manage state and side effects, and access React features without classes—all without having to rearrange your component hierarchy. About the book React Hooks in Action teaches you to write fast and reusable React components using Hooks. You'll start by learning to create component code with Hooks. Next, you'll implement a resource booking application that demonstrates managing local state, application state, and side effects like fetching data. Code samples and illustrations make learning Hooks easy. What's inside Build function components that access React features Manage local, shared, and application state Explore built-in, custom, and third-party hooks Load, update, and cache data with React Query Improve page and data loading with code-splitting and React Suspense About the reader For beginning to intermediate React developers. About the author John Larsen has been a teacher and web developer for over 20 years, creating apps for education and helping students learn to code. He is the author of Get Programming with JavaScript. Table of Contents PART 1 1 React is evolving 2 Managing component state with useState hook 3 Managing component state with useReducer hook 4 Working with side effects 5 Managing component state with useRef hook 6 Managing application state 7 Managing performance with useMemo 8 Managing state with the Context API 9 Creating your own hooks 10 Using third party hooks PART 2 11 Code splitting with Suspense 12 Integrating data-fetching with Suspense 13 Experimenting with useTransition, useDeferredValue and SuspenseList

Get to grips with cyber threat intelligence and data-driven threat hunting while exploring expert tips and techniques Key Features Set up an environment to centralize all data in an Elasticsearch, Logstash, and Kibana (ELK) server that enables threat hunting Carry out atomic hunts to start the threat hunting process and understand the environment Perform advanced hunting using MITRE ATT&CK Evals emulations and Mordor datasets Book Description Threat hunting (TH) provides cybersecurity analysts and enterprises with the opportunity to proactively defend themselves by getting ahead of threats before they can cause major damage to their business. This book is not only an introduction for those who don't know much about the cyber threat intelligence (CTI) and TH world, but also a guide for those with more advanced knowledge of other cybersecurity fields who are looking to implement a TH program from scratch. You will start by exploring what threat intelligence is and how it can be used to detect and prevent cyber threats. As you progress, you'll learn how to collect data, along with understanding it by developing data models. The book will also show you how to set up an environment for TH using open source tools. Later, you will focus on how to plan a hunt with practical examples, before going on to explore the MITRE ATT&CK framework. By the end of this book, you'll have the skills you need to be able to carry out effective hunts in your own environment. What you will learn Understand what CTI is, its key concepts, and how it is useful for preventing threats and protecting your organization Explore the different stages of the TH process Model the data collected and understand how to document the findings Simulate threat actor activity in a lab environment Use the information collected to detect breaches and validate the results of your queries Use documentation and strategies to communicate processes to senior management and the wider business Who this book is for If you are looking to start out in the cyber intelligence and threat hunting domains and want to know more about how to implement a threat hunting division with open-source tools, then this cyber threat intelligence book is for you.

This book analyzes the security of critical infrastructures such as road, rail, water, health, and electricity networks that are vital for a nation's society and economy, and assesses the resilience of these networks to intentional attacks. The book combines the analytical capabilities of experts in operations research and management, economics, risk analysis, and defense management, and presents graph theoretical analysis, advanced statistics, and applied modeling methods. In many chapters, the authors provide reproducible code that is available from the publisher's website. Lastly, the book identifies and discusses implications for

risk assessment, policy, and insurability. The insights it offers are globally applicable, and not limited to particular locations, countries or contexts. Researchers, intelligence analysts, homeland security staff, and professionals who operate critical infrastructures will greatly benefit from the methods, models and findings presented. While each of the twelve chapters is self-contained, taken together they provide a sound basis for informed decision-making and more effective operations, policy, and defense.

Although we have been successful in our careers, they have not turned out quite as we expected. We both have changed positions several times-for all the right reasons-but there are no pension plans vesting on our behalf. Our retirement funds are growing only through our individual contributions. Michael and I have a wonderful marriage with three great children. As I write this, two are in college and one is just beginning high school. We have spent a fortune making sure our children have received the best education available. One day in 1996, one of my children came home disillusioned with school. He was bored and tired of studying. “Why should I put time into studying subjects I will never use in real life?” he protested. Without thinking, I responded, “Because if you don't get good grades, you won't get into college.” “Regardless of whether I go to college,” he replied, “I'm going to be rich.”

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

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

Three boys, who made a pact to stick together through the rough times in their impoverished Newark neighborhood, found the strength to work through their difficulties and complete high school, college, and medical school together.

As a security professional, have you found that you and others in your company do not always define “security” the same way? Perhaps security interests and business interests have become misaligned. Brian Allen and Rachelle Loyear offer a new approach: Enterprise Security Risk Management (ESRM). By viewing security through a risk management lens, ESRM can help make you and your security program successful. In their long-awaited book, based on years of practical experience and research, Brian Allen and Rachelle Loyear show you step-by-step how Enterprise Security Risk Management (ESRM) applies fundamental risk principles to manage all security risks. Whether the risks are informational, cyber, physical security, asset management, or business continuity, all are included in the holistic, all-encompassing ESRM approach which will move you from task-based to risk-based security. How is ESRM familiar? As a security professional, you may already practice some of the components of ESRM. Many of the concepts – such as risk identification, risk transfer and acceptance, crisis management, and incident response – will be well known to you. How is ESRM new? While many of the principles are familiar, the authors have identified few organizations that apply them in the comprehensive, holistic way that ESRM represents – and even fewer that communicate these principles effectively to key decision-makers. How is ESRM practical? ESRM offers you a straightforward, realistic, actionable approach to deal effectively with all the distinct types of security risks facing you as a security practitioner. ESRM is performed in a life cycle of risk management including: Asset assessment and prioritization. Risk assessment and prioritization. Risk treatment (mitigation). Continuous improvement. Throughout Enterprise Security Risk Management: Concepts and Applications, the authors give you the tools and materials that will help you advance you in the security field, no matter if you are a student, a newcomer, or a seasoned professional. Included are realistic case studies, questions to help you assess your own security program, thought-provoking discussion questions, useful figures and tables, and references for your further reading. By redefining how everyone thinks about the role of security in the enterprise, your security organization can focus on working in partnership with business leaders and other key stakeholders to identify and mitigate security risks. As you begin to use ESRM, following the instructions in this book, you will experience greater personal and professional satisfaction as a security professional – and you’ll become a recognized and trusted partner in the business-critical effort of protecting your enterprise and all its assets.

Can machine learning techniques solve our computer security problems and finally put an end to the cat-and-mouse game between attackers and defenders? Or is this hope merely hype? Now you can dive into the science and answer this question for yourself! With this practical guide, you’ll explore ways to apply machine learning to security issues such as intrusion detection, malware classification, and network analysis. Machine learning and security specialists Clarence Chio and David Freeman provide a framework for discussing the marriage of these two fields, as well as a toolkit of machine-learning algorithms that you can apply to an array of security problems. This book is ideal for security engineers and data scientists alike. Learn how machine learning has contributed to the success of modern spam filters Quickly detect anomalies, including breaches, fraud, and impending system failure Conduct malware analysis by extracting useful information from computer binaries Uncover attackers within the network by finding patterns inside datasets Examine how attackers exploit consumer-facing websites and app functionality Translate your machine learning algorithms from the lab to production Understand the threat attackers pose to machine learning solutions

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

Enterprise Cybersecurity empowers organizations of all sizes to defend themselves with next-generation cybersecurity programs against the escalating threat of modern targeted cyberattacks. This book presents a comprehensive framework for managing all aspects of an enterprise cybersecurity program. It enables an enterprise to architect, design, implement, and operate a coherent cybersecurity program that is seamlessly coordinated with policy, programmatics, IT life cycle, and assessment. Fail-safe cyberdefense is a pipe dream. Given sufficient time, an intelligent attacker can eventually defeat defensive measures protecting an enterprise's computer systems and IT networks. To prevail, an enterprise cybersecurity program must manage risk by detecting attacks early enough and delaying them long enough that the defenders have time to respond effectively. Enterprise Cybersecurity shows players at all levels of responsibility how to unify their organization's people, budgets, technologies, and processes into a cost-efficient cybersecurity program capable of countering advanced cyberattacks and containing damage in the event of a breach. The authors of Enterprise Cybersecurity explain at both strategic and tactical levels how to accomplish the mission of leading, designing, deploying, operating, managing, and supporting cybersecurity capabilities in an enterprise environment. The authors are recognized experts and thought leaders in this rapidly evolving field, drawing on decades of collective experience in cybersecurity and IT. In capacities ranging from executive strategist to systems architect to cybercombatant, Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, and Abdul Aslam have fought on the front lines of cybersecurity against advanced persistent threats to government, military, and business entities.

Is peace an aberration? The bestselling author of Paris 1919 offers a provocative view of war as an essential component of humanity. NAMED ONE OF THE TEN BEST BOOKS OF THE YEAR BY THE NEW YORK TIMES BOOK REVIEW AND THE EAST HAMPTON STAR "Margaret MacMillan has produced another seminal work. . . . She is right that we must, more than ever, think about war. And she has shown us how in this brilliant, elegantly written book."—H.R. McMaster, author of Dereliction of Duty and Battlegrounds: The Fight to Defend the Free World The instinct to fight may be innate in human nature, but war—organized violence—comes with organized society. War has shaped humanity's history, its social and political institutions, its values and ideas. Our very language, our public spaces, our private memories, and some of our greatest cultural treasures reflect the glory and the misery of war. War is an uncomfortable and challenging subject not least because it brings out both the vilest and the noblest aspects of humanity. Margaret MacMillan looks at the ways in which war has influenced human society and how, in turn, changes in political organization, technology, or ideologies have affected how and why we fight. War: How Conflict Shaped Us explores such much-debated and controversial questions as: When did war first start? Does human nature doom us to fight one another? Why has war been described as the most organized of all human activities? Why are warriors almost always men? Is war ever within our control? Drawing on lessons from wars throughout the past, from classical history to the present day, MacMillan reveals the many faces of war—the way it has determined our past, our future, our views of the world, and our very conception of ourselves.

Journalist Walls grew up with parents whose ideals and stubborn nonconformity were their curse and their salvation. Rex and Rose Mary and their four children lived like nomads, moving among Southwest desert towns, camping in the mountains. Rex was a charismatic, brilliant man who, when sober, captured his children's imagination, teaching them how to embrace life fearlessly. Rose Mary painted and wrote and couldn't stand the responsibility of providing for her family. When the money ran out, the Walls retreated to the dismal West Virginia mining town Rex had tried to escape. As the dysfunction escalated, the children had to fend for themselves, supporting one another as they found the resources and will to leave home. Yet Walls describes her parents with deep affection in this tale of unconditional love in a family that, despite its profound flaws, gave her the fiery determination to carve out a successful life. -- From publisher description.

Traditional intrusion detection and logfile analysis are no longer enough to protect today's complex networks. In this practical guide, security researcher Michael Collins shows you several techniques and tools for collecting and analyzing network traffic datasets. You'll understand how your network is used, and what actions are necessary to protect and improve it. Divided into three sections, this book examines the process of collecting and organizing data, various tools for analysis, and several different analytic scenarios and techniques. It's ideal for network administrators and operational security analysts familiar with scripting. Explore network, host, and service sensors for capturing security data Store data traffic with relational databases, graph databases, Redis, and Hadoop Use SiLK, the R language, and other tools for analysis and visualization Detect unusual phenomena through Exploratory Data Analysis (EDA) Identify significant structures in networks with graph analysis Determine the traffic that's crossing service ports in a network Examine traffic volume and behavior to spot DDoS and database raids Get a step-by-step process for network mapping and inventory

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

This book describes the people, processes, and technologies needed to extract actionable intelligence from the inside, and outside, of crime guns.

From one of America’s most popular short story writers and an Academy Award nominee: the O. Henry Award–winning tale that inspired the movie The Hunt. A subject of mysterious rumors and superstition, the deserted Caribbean Island was shrouded in an air of peril. To Sanger Rainsford, who fell off a yacht and washed up on its shores, the abandoned isle was a welcome paradise. But unknown to the big-game hunter, a predator lurked in its lush jungles—one more dangerous than any he had ever encountered: a human. First published in 1924, this suspenseful tale “has inspired serial killers, films and stirred controversy in schools. A century on, the story continues to thrill” (The Telegraph). “[A] tense, relentless story of man-against-man adventure, in which the hunter Sanger Rainsford learns, at the hands of General Zaroff, what it means to be hunted.” —Criterion

Agile continues to be the most adopted software development methodology among organizations worldwide, but it generally hasn't integrated well with traditional security management techniques. And most security professionals aren’t up to speed in their understanding and experience of agile development. To help bridge the divide between these two worlds, this practical guide introduces several security tools and techniques adapted specifically to integrate with agile development. Written by security experts and agile veterans, this book begins by introducing security principles to agile practitioners, and agile principles to security practitioners. The authors also reveal problems they encountered in their own experiences with agile security, and how they worked to solve them. You’ll learn how to: Add security practices to each stage of your existing development lifecycle Integrate security with planning, requirements, design, and at the code level Include security testing as part of your team’s effort to deliver working software in each release Implement regulatory compliance in an agile or DevOps environment Build an effective security program through a culture of empathy, openness, transparency, and collaboration

This book provides readers with up-to-date research of emerging cyber threats and defensive mechanisms, which are timely and essential. It covers cyber threat intelligence concepts against a range of threat actors and threat tools (i.e. ransomware) in cutting-edge technologies, i.e., Internet of Things (IoT), Cloud computing and mobile devices. This book also provides the technical information on cyber-threat detection methods required for the researcher and digital forensics experts, in order to build intelligent automated systems to fight against advanced cybercrimes. The ever increasing number of cyber-attacks requires the cyber security and forensic specialists to detect, analyze and defend against the cyber threats in almost real-time, and with such a large number of attacks is not possible without deeply perusing the attack features and taking corresponding intelligent defensive actions – this in essence defines cyber threat intelligence notion. However, such intelligence would not be possible without the aid of artificial intelligence, machine learning and advanced data mining techniques to collect, analyze, and interpret cyber-attack campaigns which is covered in this book. This book will focus on cutting-edge research from both academia and industry, with a particular emphasis on providing wider knowledge of the field, novelty of approaches, combination of tools and so forth to perceive reason, learn and act on a wide range of data collected from different cyber security and forensics solutions. This book introduces the notion of cyber threat intelligence and analytics and presents different attempts in utilizing machine learning and data mining techniques to create threat feeds for a range of consumers. Moreover, this book sheds light on existing and emerging trends in the field which could pave the way for future works. The inter-disciplinary nature of this book, makes it suitable for a wide range of audiences with backgrounds in artificial intelligence, cyber security, forensics, big data and data mining, distributed systems and computer networks. This would include industry professionals, advanced-level students and researchers that work within these related fields.

New York Times Best Seller How will Artificial Intelligence affect crime, war, justice, jobs, society and our very sense of being human? The rise of AI has the potential to transform our future more than any other technology—and there’s nobody better qualified or situated to explore that future than Max Tegmark, an MIT professor who’s helped mainstream research on how to keep AI beneficial. How can we grow our prosperity through automation without leaving people lacking income or purpose? What career advice should we give today’s kids? How can we make future AI systems more robust, so that they do what we want without crashing, malfunctioning or getting hacked? Should we fear an arms race in lethal autonomous weapons? Will machines eventually outsmart us at all tasks, replacing humans on the job market and perhaps altogether? Will AI help life flourish like never before or give us more power than we can handle? What sort of future do you want? This book empowers you to join what may be the most important conversation of our time. It doesn’t shy away from the full range of viewpoints or from the most controversial issues—from superintelligence to meaning, consciousness and the ultimate physical limits on life in the cosmos.

Applied Network Security Monitoring is the essential guide to becoming an NSM analyst from the ground up. This book takes a fundamental approach to NSM, complete with dozens of real-world examples that teach you the key concepts of NSM. Network security monitoring is based on the principle that prevention eventually fails. In the current threat landscape, no matter how much you try, motivated attackers will eventually find their way into your network. At that point, it is your ability to detect and respond to that intrusion that can be the difference between a small incident and a major disaster. The book follows the three stages of the NSM cycle: collection, detection, and analysis. As you progress through each section, you will have access to insights from seasoned NSM professionals while being introduced to relevant, practical scenarios complete with sample data. If you've never performed NSM analysis, Applied Network Security Monitoring will give you an adequate grasp on the core concepts needed to become an effective analyst. If you are already a practicing analyst, this book will allow you to grow your analytic technique to make you more effective at your job. Discusses the proper methods for data collection, and teaches you how to become a skilled NSM analyst Provides thorough hands-on coverage of Snort, Suricata, Bro-IDS, SiLK, and Argus Loaded with practical examples containing real PCAP files you can replay, and uses Security Onion for all its lab examples Companion website includes up-to-

date blogs from the authors about the latest developments in NSM

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

Considered by many the greatest war novel of all time, All Quiet on the Western Front is Erich Maria Remarque’s masterpiece of the German experience during World War I. I am young, I am twenty years old; yet I know nothing of life but despair, death, fear, and fatuous superficiality cast over an abyss of sorrow. . . . This is the testament of Paul Bäumer, who enlists with his classmates in the German army during World War I. They become soldiers with youthful enthusiasm. But the world of duty, culture, and progress they had been taught breaks in pieces under the first bombardment in the trenches. Through years of vivid horror, Paul holds fast to a single vow: to fight against the principle of hate that meaninglessly pits young men of the same generation but different uniforms against one another . . . if only he can come out of the war alive. “The world has a great writer in Erich Maria Remarque. He is a craftsman of unquestionably first rank, a man who can bend language to his will. Whether he writes of men or of inanimate nature, his touch is sensitive, firm, and sure.”—The New York Times Book Review

The classic story of one family torn apart by the Revolutionary War All his life, Tim Meeker has looked up to his brother. Sam is smart and brave, and is now a part of the American Revolution. Not everyone in town wants to be a part of the rebellion. Most are supporters of the British, including Tim and Sam's father. With the war soon raging, Tim knows he will have to make a choice between the Revolutionaries and the Redcoats, and between his brother and his father.

Your one stop solution to implement a Cyber Defense Intelligence program in to your organisation. Key Features Intelligence processes and procedures for response mechanisms Master F3EAD to drive processes based on intelligence Threat modeling and intelligent frameworks Case studies and how to go about building intelligent teams Book Description Cyber intelligence is the missing link between your cyber defense operation teams, threat intelligence, and IT operations to provide your organization with a full spectrum of defensive capabilities. This book kicks off with the need for cyber intelligence and why it is required in terms of a defensive framework. Moving forward, the book provides a practical explanation of the F3EAD protocol with the help of examples. Furthermore, we learn how to go about threat models and intelligence products/frameworks and apply them to real-life scenarios. Based on the discussion with the prospective author I would also love to explore the induction of a tool to enhance the marketing feature and functionality of the book. By the end of this book, you will be able to boot up an intelligence program in your organization based on the operation and tactical/strategic spheres of Cyber defense intelligence. What you will learn Learn about the Observe-Orient-Decide-Act (OODA) loop and it's applicability to security Understand tactical view of Active defense concepts and their application in today's threat landscape Get acquainted with an operational view of the F3EAD process to drive decision making within an organization Create a Framework and Capability Maturity Model that integrates inputs and outputs from key functions in an information security organization Understand the idea of communicating with the Potential for Exploitability based on cyber intelligence Who this book is for This book targets incident managers, malware analysts, reverse engineers, digital forensics specialists, and intelligence analysts; experience in, or knowledge of, security operations, incident responses or investigations is desirable so you can make the most of the subjects presented.

The only novel ever to win the Hugo, Nebula, and Arthur C. Clarke Awards and the first book in Ann Leckie's New York Times bestselling trilogy. On a remote, icy planet, the soldier known as Breq is drawing closer to completing her quest. Once, she was the Justice of Toren - a colossal starship with an artificial intelligence linking thousands of soldiers in the service of the Radch, the empire that conquered the galaxy. Now, an act of treachery has ripped it all away, leaving her with one fragile human body, unanswered questions, and a burning desire for vengeance. In the Ancillary world: 1. Ancillary Justice2. Ancillary Sword3. Ancillary Mercy

Our world is being revolutionized by data-driven methods: access to large amounts of data has generated new insights and opened exciting new opportunities in commerce, science, and computing applications. Processing the enormous quantities of data necessary for these advances requires large clusters, making distributed computing paradigms more crucial than ever. MapReduce is a programming model for expressing distributed computations on massive datasets and an execution framework for large-scale data processing on clusters of commodity servers. The programming model provides an easy-to-understand abstraction for designing scalable algorithms, while the execution framework transparently handles many system-level details, ranging from scheduling to synchronization to fault tolerance. This book focuses on MapReduce algorithm design, with an emphasis on text processing algorithms common in natural language processing, information retrieval, and machine learning. We introduce the notion of MapReduce design patterns, which represent general reusable solutions to commonly occurring problems across a variety of problem domains. This book not only intends to help the reader "think in MapReduce", but also discusses limitations of the programming model as

well. This volume is a printed version of a work that appears in the Synthesis Digital Library of Engineering and Computer Science. Synthesis Lectures provide concise, original presentations of important research and development topics, published quickly, in digital and print formats. For more information visit www.morganclaypool.com

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.

Discover the latest trends, developments and technology in information security today with Whitman/Mattord's market-leading PRINCIPLES OF INFORMATION SECURITY, 7th Edition. Designed specifically to meet the needs of those studying information systems, this edition's balanced focus addresses all aspects of information security, rather than simply offering a technical control perspective. This overview explores important terms and examines what is needed to manage an effective information security program. A new module details incident response and detection strategies. In addition, current, relevant updates highlight the latest practices in security operations as well as legislative issues, information management toolsets and digital forensics. Coverage of the most recent policies and guidelines that correspond to federal and international standards further prepare you for success both in information systems and as a business decision-maker. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.